TrustChain impact, exploitation and sustainability report

27/09/2024

Funded by the European Union

NGI TRUST CHAIN

Grant Agreement No.: 101093274
Call: HORIZON-CL4-2022-HUMAN-01
Topic: ICT-54-2020
Type of action: RIA

D5.8 TRUSTCHAIN IMPACT, EXPLOITATION AND SUSTAINABILITY REPORT

Work Package Number	WP 5
Task Number	Task 5.1, 5.2, 5.3, 5.4
Type	R – Document, Report
Dissemination Level	PU - Public
Due date (month)	Month 18
Submission date	27/09/2024
Deliverable lead	AUEB
Version	1.0
Authors	Thanasis G. Papaioannou (NKUA), Vasilios A. Siris (AUEB), George Stamoulis (AUEB)
Reviewers	Raj Muttukrishnan (ICS), Pablo Vela (ALA)
Abstract	TrustChain impact, exploitation and sustainability report
Keywords	Technical Impact, Societal Impact, Economic Impact, Exploitation, Sustainability

Funded by the European Union

Document Revision History

Version	Date	Description of change	List of contributor(s)
0.1	01/06/2024	Table of contents and outline of the document	Thanasis G. Papaioannou (NKUA), Vasilios A. Siris (AUEB), George Stamoulis (AUEB)
0.2	07/06/2024	Technical/Scientific and Societal Impact Assessment	Thanasis G. Papaioannou (NKUA)
0.3	21/06/2024	Economic Analysis Methodology and KER definition	Thanasis G. Papaioannou (NKUA)
0.4	30/06/2024	Ecosystem development, events and NGI impact	Tajana Medaković (F6S)
0.5	15/07/2024	User validation	Andres Delalamo (CIB)
0.6	31/07/2024	BM and economic analyses overview of OC1, OC2 projects	Thanasis G. Papaioannou (NKUA)
0.7	15/08/2024	OSSF business model	Thanasis G. Papaioannou (NKUA)
0.8	10/09/2024	OSSF economic analysis	Thanasis G. Papaioannou (NKUA)
0.9	20/09/2024	Abstract, Introduction, Conclusions	Thanasis G. Papaioannou (NKUA)
0.95	21/09/2024	Alastria platform exploitation	Pablo Vela (ALA)
1.0	26/09/2024	Review comments applied	Thanasis G. Papaioannou (NKUA)

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

The information in this document is provided “as is” and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. Moreover, it is clearly stated that the TrustChain Consortium reserves the right to update, amend or modify any part, section, or detail of the document at any point in time without prior information.

Copyright Notice

The TrustChain Consortium is the following:

Participant number	Role	Participant organisation name	Short name	Country
1	COO	EUROPEAN DYNAMICS LUXEMBOURG SA	ED	LX
2	BEN	F6S NETWORK LIMITED	F6S	IE
3	BEN	UNIVERZA V LJUBLJANI	UL	SI
4	**BEN**	**ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS - RESEARCH CENTER**	**AUEB**	**EL**
5	BEN	FUNDACION CIBERVOLUNTARIOS	CIB	SP
6	BEN	CONSORCIO RED ALASTRIA	ALA	SP
7	BEN	TIMELEX	TLX	BE
8	BEN	ETHNIKO KAI KAPODISTRIAKO PANEPISTIMIO ATHINON	NKUA	EL
9	AP	CITY UNIVERSITY OF LONDON	ICS	UK
10	BEN	NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS	NKUA	EL

COO = coordinator; BEN = beneficiary; AE = Affiliated entity; AP = Associated Partner

EXECUTIVE SUMMARY

In this deliverable, we describe the scientific/technical, societal and economic impact of TrustChain. We also describe its impact in terms of ecosystem building, towards the objectives of the Next Generation Internet and towards the UN Sustainable Development Goals. For the analysis of the economic impact, we identify the Key Exploitable Results (KERs) developed by third-party projects funded in the first three open calls of the project so far. We present the methodology followed by third-party funded projects for the business development of these KERs, which includes market analysis and tools such as business model canvas, value chains/networks, and SWOT models. We then overview the business models for the exploitation of the KERs that correspond to Open Calls 1 and 2. Subsequently, we deal with the sustainability of the TrustChain ecosystem. We identify that TrustChain has all necessary components to be transformed to an Open-Source Software Foundation (OSSF). We describe the business model of the TrustChain OSSF and we perform an economic sustainability analysis based on a few realistic assumptions. Based on our analysis, the TrustChain ecosystem can be economically sustainable as an OSSF.

TABLE OF CONTENTS

Funded by the European Union

Funded by the European Union

LIST OF FIGURES

LIST OF TABLES

Funded by the European Union

ABBREVIATIONS

API	Application Programming Interface
BM	Business Model
BMC	Business Model Canvas
DAO	Decentralized autonomous organization
DID	Decentralised Identifiers
DIH	Digital Innovation Hub
EEN	Europe Enterprise Network
DLT	Distributed Ledger Technology
eIDAS	electronic IDentification, Authentication and trust Services
EU	European Union
GDPR	General Data Protection Regulation
ISCC	International Standard Content Code
IRR	Internal Rate of Return
KPI	Key Performance Indicator
LoA	Level of Assurance
mDL	Mobile driver's license
NFT	Non-Fungible Token
NCP	National Contact Point
NGI	Next Generation Internet
NGO	Non-Governmental Organisations
NPV	Net Present Value
OC	Open Call
OC1	Open Call 1

OC2	Open Call 2
OC3	Open Call 3
OSSF	Open-Source Software Foundation
PKI	Public Key Infrastructure
SDG	Sustainable Development Goals
SME	Small and Medium-sized Enterprises
SSCD	Secure Signature Creation Devices
SSI	Self-Sovereign Identities
UCD	User Centred Design
VC	Verifiable Credential
VP	Verifiable Presentation
ZKP	Zero Knowledge Proof

1 INTRODUCTION

The goal of this deliverable is the description of the multifold impact of TrustChain in the first three Open Calls of the project. It overviews the scientific/technical impact, the societal impact, the contribution in the realization of the vision of the Next Generation Internet (NGI), the impact in terms of community/ecosystem building, the impact in addressing user needs, and the project contributions towards UN Sustainable Development Goals (SDGs).

The economic/business impact of TrustChain is also described at large. First, we identify the Key Exploitable Results (KERs) of the project so far. Then, we outline the methodology for business model development and economic analysis that we conveyed to all TrustChain-funded projects and trained them to follow. In the sequel, we overview the business cases towards the exploitation of the different KERs that correspond to Open Call 1 (OC1) and Open Call 2 (OC2), which were developed according to the aforementioned methodology.

Subsequently, the sustainability of the ecosystem is addressed. A potential business model for the economic sustainability of the TrustChain ecosystem is considered, namely the transformation of TrustChain to an Open-Source Software Foundation (OSSF) after the end of the project. The business model is described, and it is numerically analyzed with few basic realistic assumptions. It is found that this business model is capable to economically sustain the TrustChain ecosystem.

The remainder of this deliverable is structured as follows:

In Section 2, we recall the objectives and challenges of the 3 Open Calls of TrustChain so far, and we list the selected projects to address them.

In Section 3, we overview the impact of TrustChain project, in terms of scientific contributions, the societal challenges addressed, the contributions in the framework of the Next Generation Internet (NGI), the community/ecosystem building, the user-centered design and the end users, as well as the project contributions towards the UN Sustainable Development Goals (SDGs). In terms of economic impact, we list the Key Exploitable Results (KERs) of TrustChain so far.

In Section 4, we briefly describe the methodology for business modelling and economic analysis. The Business Model definition and economic analysis methodology. The detailed methodology can be found in the Appendix.

In Section 5, we overview the business models canvases of the KERs of OC1, OC2 that have been developed according to the methodology of Section 4. Detailed economic analyses for the different KERs of OC1, OC2 can be found in the Appendix.

Funded by the European Union

In Section 6, we describe the business model of TrustChain as a whole and study the economic sustainability of the ecosystem.

In Section 7, we conclude this report.

Finally, in Section 8, we include an Appendix with the detailed methodology for economic analysis and the economic analyses of the funded third-party projects in OC1, OC2 and OC3 of TrustChain.

2 SELECTED PROJECTS IN TRUSTCHAIN OPEN CALLS

In this section, we first overview the objectives and the challenges of Open Calls 1, 2 and 3. Subsequently, we list the projects selected to develop solutions that address these objectives and challenges.

2.1 OPEN CALL 1 SCOPE AND OBJECTIVES

This section describes the specific objectives of Open Call 1 and the challenges addressed.

2.1.1 Specific objectives

Trustworthy digital identities that also preserve privacy, in the sense that specific parts of the user identity are only exposed, are currently needed. Also, before data can be employed in blockchain smart contracts, data trustworthiness assessment is a prerequisite for online transactions.

In order to achieve TrustChain vision, it is expected that applicants will develop interoperable and sustainable digital identity management applications that are transparent and address the needs of the future decentralised internet. In particular, the following main objectives should be considered:

- Develop a framework for decentralized user-centric identity management that lies in the scope of the call and addresses the stated challenges below.
- Develop protocols for trustworthiness of entities by means of verifiable credentials and decentralized reputation systems.
- Ensure identity attributes are disclosed only with the informed consent from the data owner (i.e., data minimization requirement of GDPR).
- Develop smart oracles to assess the trustworthiness of data fed to blockchain smart contracts fetched from external systems.

Applications should cover real needs of the end-users in one of the sectors such as for example banking, education, healthcare, or e-democracy.

2.1.2 Challenges

The current ecosystem of decentralized digital identity systems experienced a rapid growth in the last couple of years. However, mainstream adoption of those systems still

encounters multiple challenges that should be addressed by the TrustChain applications.

Today's identity systems face a multitude of challenges due to the centralised nature of the internet. The internet was initially developed without the human in the loop. However, the exponential growth of the online usage, the evolution of decentralised systems and the power of cloud and edge computing have made the centralised model obsolete for many future online applications. In order to develop a usable and interoperable decentralised future internet, some of the identity challenges that exist today need to be addressed. These include the following:

- The current identity systems lack usability, privacy, transparency, interoperability and compliance with GDPR and are not inclusive in nature.
- They incorporate multitude of technologies such as zero-knowledge-proofs (ZKPs) that are not transparent to the user and not easy to integrate or deploy by the non-tech-savvy user.
- There is a lack of trust in the way the identity credentials are shared and used by multiple online services.
- Most of the authentication systems request more identity data than what is required. Hence the data minimization principle of GDPR is not observed correctly.
- Most of the existing identity systems do not provide a mechanism by which an individual can delegate their identity credentials to someone they trust for identity recovery or in an emergency scenario (i.e. social guardians).
- The systems don't maintain the privacy of the identity credentials. In addition, the user has no visibility of the audit trail of the identity credentials once shared with a 3rd party. This leads to identity fraud.
- Human has not been involved from the initial design stages of the identity eco system. This leads to lack of understanding of the new technologies (i.e. blockchain, reputation-based systems, crypto etc.) and usability issues by the end-users' restricting wider technology adoption.

With respect to those challenges, the proposed solution may include:

- the provision of public administration services,
- digital identities used in the banking (e.g., know your customer (KYC) approaches), education (e.g. micro credentials for micro competencies), healthcare (e.g. access-control mechanisms in cross-border scenarios), and other sectors,

- cross-border use of digital identities,
- digital identities used by Next Generation Internet services, and/or
- regulatory alignment of existing digital identities (e.g., in the context of EU eIDAS framework).

2.2 OPEN CALL 2 SCOPE AND OBJECTIVES

This section describes the specific objectives of Open Call 1 and the challenges addressed.

2.2.1 Specific Objectives

It has become increasingly important to minimize the amount of data needed for specific online services. As more and more organizations share business sensitive data, it is important to preserve privacy while maintaining data utility. Therefore, to give the control of their online data sharing back to the user and ensure privacy preserving ways of data exchange on the future internet is currently needed. Establishing privacy, security and consent in specific data management processes should be a pre-requisite condition of online data sharing.

The objective of this Open Call is to develop tools, cryptographic mechanisms, and other algorithms for data handling and sharing as well as for the management of data lakes in compliance with GDPR and other regulations that implement techniques such as:

Mechanisms for multi-party data sharing that lies in the scope of the call and addresses the stated challenges below,

Protocols for privacy-preserving data sharing using techniques from technologies such as federated learning both vertical and horizontal framework,

Privacy-preserving data processing, data storage and data computation techniques such as differential privacy, data obfuscation/perturbation, anonymization techniques,

Encrypted data analytics based on homomorphic encryption and Trusted Execution environment,

Protocols to verify authenticity and accuracy of data using technologies like zero knowledge proofs,

Protocols to support the digital sovereignty-based data flow and data spaces initiatives.

Data identification, data provenance, data tracking mechanisms or protocols should be built so that the data that is exchanged can be tracked, so that trustworthy data handling according to the user consent can be verified.

2.2.2 Challenges

In the current Internet, all user data is owned and managed by a few handful organizations, which dictate the terms of data exchange with third parties. In most cases, user consent is either not explicitly specified or is masked in elaborate notices. Purpose limitation and data minimization is a key data management practice that the current Internet is missing.

Today's digital systems are faced with a multitude of challenges due to the centralised nature of the Internet. The Internet was initially developed without the human in the loop. However, with the exponential growth of online usage, evolution of decentralised systems and the power of cloud and edge computing has made the centralised model obsolete for many future online applications. In order to develop effective user privacy preserving and state-of-the-art consent- based data management, the following challenges that exist today need to be addressed:

- The online data sharing model is flawed as it encourages data duplication, long term data retention and intensive data collection across service providers. There is also lack of data traceability and accountability in online data sharing,
- Privacy is important when user data is employed for training machine learning models and computation. Information leakage in training models is a persistent problem. Local differential privacy with federated learning models can be explored to address this challenge,
- Data accuracy vs privacy trade-off in privacy-preserving techniques like differential privacy is an open challenge and its solution can be key to solving many open-source data sharing issues,
- Privacy-aware data processing needs to be encouraged from the design phase of any data sharing/processing protocol,
- Similarly, illegal data copying is a big challenge in user privacy and data governance models today which needs to be addressed,
- A trust layer is missing, and it is often difficult to ensure authenticity of data. Thus, trustworthy data access and data integrity mechanisms based on SSI technologies, including decentralized identifiers and Verifiable Credentials, needs to be designed,
- In line with providing a trust layer supporting user privacy, data provenance ontologies and data transaction logging should be available to users,

- Users have little to no control over access to their personal data shared online. Therefore, automated user consent/smart user consent for data sharing needs to be implemented,
- Data owners currently do not have means to be compensated or to enable fair data value sharing with the big players in the market. When users want to participate in the data economy, they should be able to do so by means of data tokenization/trading capabilities,
- Users should be empowered to add the necessary levels of anonymity in order to share their data with a third party.

2.3 OPEN CALL 3 SCOPE AND OBJECTIVES

This section describes the specific objectives of Open Call 1 and the challenges addressed.

2.3.1 Specific Objectives

The objective of this OC is to define and build market mechanisms for data exchange and data trading as well as innovative win-win federated business models open data in compliance with GDPR and other regulations that implements techniques such as:

- Federated business models that consider fair rewarding of its participants
- Establish new or enrich the existing marketplaces. Privacy preserving data sharing on third-party platforms
- Fair data marketplaces: publish, search, discovery, other mechanisms in decentralized environments; negotiation mechanisms for data prices
- Market competition that is fair and regulated in favour of the innovators.
- Tokenization of assets and its fair trading, protection against scams such as rug pulls, initial coin offering (ICO) fraud in digital asset trading
- Establishing the value of the coins based on their quality contents; creating liquidity in the existing data marketplaces.
- Decentralized governance models that are fair and trustworthy to all the parties in a data exchange ecosystem
- Use your eIDAS2 on the EU marketplaces
- Effective data monetization strategies and business models to incentivize data providers to share their data on exchange platforms.

2.3.2 Challenges

Navigating the data exchange/trading arena proves challenging due to the involvement of multiple parties, leading to issues of trust, privacy, consent, and regulatory complexities. The existing market mechanisms for data exchange face hurdles, exacerbated by the dynamic nature of data and the digital landscape. Additionally, challenges in market competition, fair settlement practices, and determining ownership rights further complicate the ecosystem. Organizations must grapple with these challenges, ranging from establishing trust frameworks to addressing evolving privacy regulations and ensuring fair compensation for data contributors. Tackling these complexities necessitates collaborative efforts and innovative solutions to create a secure, transparent, and ethical data exchange environment. Some of the challenges to be tackled in this call are the following:

- The current form of data-sharing practises does not fairly reward the data owners/content producers. Data platform owners make decisions around the terms and conditions of data sharing.
- Accurate data discoverability on such marketplaces is a challenge. Precise matchmaking between sellers and buyers on a marketplace can significantly improve its performance.
- Data trading and exchange raise significant concerns about data privacy and security. There is a risk that sensitive or personal data could be mishandled, leading to privacy breaches, identity theft, or other malicious activities.
- Establishing enforceable data marketplace contracts for data exchange is missing; Clear and fair service level agreements for both sellers and buyers needs to be in place for a trustworthy marketplace.
- There is no standard pricing model for data, making it challenging to determine the fair market value of different data types. Mechanisms to ascertain the data quality and hence its price fairly is a challenging issue as the value of data can be subjective and context-dependent
- Issue around data provenance exist as it can be difficult to verify the data source. Techniques to inspect the provenance of a specific product, service or data is missing. Open reputation management can be one of the solutions, but it requires careful design considerations.
- Establishing clear data governance practices, including data access controls and usage policies, is essential for responsible data exchange. Data governance frameworks can be complex to implement and enforce.
- Federated marketplaces among self-interested parties emerge in various contexts, such as cloud services, IoT data exchange and more, for increasing

service coverage, availability, efficiency, etc. Providing support for trustworthy service provision logging, transparent billing, fair value sharing and coordination in resource allocation in these contexts is a challenge.

- Innovative incentive mechanisms for decentralized, coordinated outcomes, potentially involving tokenomics, in various application contexts should be provided.
- Enabling a sustainable circular economy that involves sharing, leasing, reusing existing materials and products demand data provenance on the transformation of properties of materials and on processes applied on them. Means to achieve such an economy requires innovation in terms of material traceability and digital passports.
- Marketplaces for AI/ML models trading/exchange has witnessed a rise with advancement in AI training models and fear of data exchange due to privacy violations. A comprehensive comparison of such models on marketplace remains a challenge.
- Digital solutions to enhance civic mobilisation and engagement. Such solutions can utilize real-time information, platforms for crowdsourcing ideas, and platforms for facilitating access to participatory channels, in order to transform and enhance democratic decision-making.

2.4 PROPOSALS SELECTED IN TRUSTCHAIN OC1, OC2 AND OC3

After the evaluation process, in OC1, only 13 proposals were selected out of the 87 eligible proposals submitted, leading to an overall success rate of 15%.

The 13 proposals selected in OC1 are the following:

- DidRoom: Open-source, multiplatform, multi-standard, multifunctional SSI wallet
- CreatorCredentials.cc: Decentralised Issuer Services for Verifiable Creator Credentials
- MUSAP: Multiple SSCD with Unified Signature API Library
- TREVO: Trusted Electronic Voting
- Orchestral: Identity in an ethical internet community
- The Social Wallet
- DID4EU: Decentralized identity infrastructure for Europe
- IM4DEC: Identity Management for the Digital Emergency Call

- WIDE: Web3 Identity Integration for DAOs and Education
- CLIENT-DIDs: Client-managed secret mode for DIDs
- EVI Electric Vehicle Identity: Protecting driver privacy, while streamlining transactions in public charging stations
- IS-CIS: Information Sharing: consensual, innate & sequential
- PRIVE: Privacy Respecting Identity Verification Enabler for Digital Identity Wallets

After the evaluation process of OC2, 15 proposals were selected out of the 74 eligible proposals submitted, leading to an overall success rate of 20%.

The 15 proposals selected in OC2 are the following:

- SURE: Synthetic Data: Utility, Regulatory compliance, and Ethical privacy
- ProvenAI: Proven AI
- PECS: Privacy Enhancing Car System
- OIDC PRINCE: OpenID Connect with PRIvacy-eNhanced ConsEnts
- NG-SC: Next Generation Smart Cities
- MorphMetro: Secure and privacy-preserving exchange and analysis
- of measured data based on homomorphic encryption
- LED-UP: LEVEA's Enhanced Data Governance and UserCentric Privacy in Decentralized System
- GUEDHS: Data Governance and User privacy envisioning an EHDS pilot deployment
- EIDCMP: eIDAS compliant membership platform
- DUME: Decentralised User-Centric Media Extension
- DID-IMP: Decentralized public key Infrastructure for Defended IoT data Management and Procurement
- DOOF : Data Ownership Orchestration Framework
- DGUARD : Privacy preserving data-sharing platform
- AURORA MINDS : Empowering Children with ADHD Through Privacy Preserving Data Collection
- UtiP-DAM: Utility-Preserving, Decentralized Anonymity of Mobility data

After the evaluation process of OC3, 15 proposals were selected out of the 98 eligible proposals submitted, leading to an overall success rate of 15.3%.

The 15 proposals selected in OC3 are the following:

- AI-MetaBloQ : Biosample related DLT marketplace with AI quality biosample quality assessment too
- Zkorum : Verifiable Moderation on eAgora
- DIDimo: Credential issuance/verification compliancy and marketplace
- Spark-IT: Igniting Innovation with Trust, Collaboration and Expert Mentorship
- FitChain: Empowering Personal Health Data Sovereignty through Blockchain-Enabled Monetization
- Trust City
- Flora: Federated Learning Ovulation tRacking App with Reward System
- TAC : Traceability and Trust in the Agrifood supply Chains
- Value4All: Unlocking value for all participants in a data ecosystem
- AuthBond: Authentic Bond Operating Network for DAOs
- PLD: Enhancing Democratic Decision-Making with Predictive Liquid Democrac
- TRU-IP AMICA: Trusted IP Asset Management in Cultural Aggregators
- QX Travel Wallet: The Web3 Travel Experience Wallet and SaaS / WaaS Ecosystem
- SecureOpinion: : Decentralized and Secure Public Opinion Sharing Platform using Zero-Knowledge Blockchain
- TradeOnChain : Trusted International Contract Management Framework

3 TRUSTCHAIN IMPACT

TrustChain has developed trust, privacy and user control mechanisms for exchanging and accessing personal data on the Internet. More specifically, the funded projects: PRIVE, SecurOpinion, TREVO, DGUARD, LED-UP, DID-IMP, PECS, AuthBond.

TrustChain has developed toolkits and libraries (SDKs and APIs) in the blockchain domain for assessing the trustworthiness of entities and data, as well as for coordinated rule setting. More specifically, the funded projects:: The Social Wallet, DID4EU, EIDCMP, Client-DIDs, DIDroom, Musap, WIDE

TrustChain has contributed to standards that will assure decentralised Internet protocols and mechanisms for interoperability across multiple DTLs. Specifically, the funded projects: EVI, Dume.

TrustChain has promised to fund 75 third-party developer teams to actively contribute to the development of the project platform during five open calls. During the reporting period, TrustChain has been funding 43 third-party developer teams in three open calls, specifically 15 projects in OC1, 13 projects in OC2 and 15 projects in OC3.

TrustChain has developed an active ecosystem of high-end scientists, domain experts, software developers and professionals with regular meetings, mailing lists and discussion forums (slack). In the TrustChain plenary meetings, technical presentations by team members are organized, and webinars on technical, business, legal, or UCD aspects are given by the core consortium members.

Most of the code is open source and it is available at the GitHub repository of TrustChain. The repository includes detailed documentation of the software solutions and detailed instructions for their deployment. Open APIs, and/or SDKs, and/or libraries have been provided almost by every third-party funded project as a mandatory requirement.

8 open access scientific publications have been also produced so far.

A sustainable business model, embracing all actors and results, has been developed and documented later at this deliverable to exploit the results of TrustChain in the form of a software foundation.

TrustChain web page supports and mobilises the community and investors as well as communicates, diffuses and expands the project's outcomes to the relevant stakeholders. Also, it contains media coverage, events, interviews with third-party developers, short description of third-party projects and links to demo videos of the software solutions developed within TrustChain.

3.1 SCIENTIFIC / TECHNICAL IMPACT

TABLE 1: TECHNICAL KPIS OF THE PROJECT

KPI	Target	Status (current projects providing relevant solutions)
Number of SSI/VC solutions	3+	**7:** The Social Wallet, DID4EU, EIDCMP, Client-DIDs, DIDroom, Musap, WIDE
Number of decentralized reputation systems	2+	**3:** Spark-it, ZKorum, VALUE4ALL
Number of smart oracle solutions	5+	**3:** LED-UP, EVI, TAC!
Number of privacy preserving DLT-based mechanisms implemented	8+	**8:** PRIVE, SecurOpinion, TREVO, DGUARD, LED-UP, DID-IMP, PECS, AuthBond
Data processing in Trusted Execution Environments solutions	5+	**3:** DIDroom, MUSAP, PRIVE
Number of innovative business models for data sharing	3+	**6:** AURORAMINDS, LED-UP, DOOF, GUEDHS, NG-SC, SURE
Number of solution-specific business models defined	70	28 (up to OC2), Business model for OC3 projects have not been defined yet.
Positive UX and feedback on GDPR compliance on data trading platform	20+	500+ (>>50% of the 943 users that validated TrustChain solutions so far)
Number of different bridges across chains	5+	N/A (this is the focus of OC4)
Number of semantic standards or ontologies for interchain state/value exchange	2+	N/A (this is the focus of OC4)

Number of privacy enabling mechanisms supported across blockchains	5+	**8:** Utip-DAM, MorphMetro, AURORAMINDS, DGUARD, PECS, OIDC-PRINCE, NG-SC, FLORA
Number of digital identity types supported across chains	5+	**14** different digital identity types are supported: CLIENT-DIDs supports all 11 types from Universal Registar. eIDAS is also supported by EIDCMP, eIDAS2 is supported by DIDroom. AlastriaID is also used by LED-UP. DID/VC interoperability is supported by project DIDimo. Identity transfers across chains is not yet applicable (as it is among the topics of OC4).
Number of decentralized Internet protocols	3+	**3:** SocialWallet implements an SSI/VC framework. DUME intends to extend the Solid Protocol. DID-IMP focuses on a decentralized PKI for secure and traceable data delivery in IoT.

3.2 SCIENTIFIC IMPACT

The EVI project addresses a gap in the ISO 15118 standard, which outlines direct communication between electric vehicles (EVs) and charging stations but lacks standardized methods for associating contract certificates with users and payment methods. The project proposes methods for linking contract certificates to users and digital wallets, necessary for the large-scale implementation of Plug&Charge. It introduces the EVI (EV Integration) service, which extends the Open Plug&Charge Protocol (OPCP) to allow users to generate contract certificates via authentication with their preferred wallet, reducing the need for personally identifiable information (PII).

The DUME project intends to extend the W3C Solid protocol.

Also, as part of the collaborative work done by innovators and mentors in the projects funded by TrustChain, a few paper publications have been made. Below, a list of these publications with authorship and venue names is provided.

TABLE 2: LIST OF PROJECT PUBLICATIONS

Conference / Journal	Title	Authors
IEEE/ACM CCGRID 2024, https://zenodo.org/doi/10.5281/zenodo.10785252	Efficient and Budget-Balanced Decentralized Management of Federated Cloud and Edge Providers	G. Darzanos, T. G. Papaioannou, G.D. Stamoulis, AUEB
IEEE Blockchain '24 - TrustChain workshop	A Blockchain Identity Privacy Management Framework for a Healthcare Application	Sofia Sakka (University of Ioannina, Greece), Vasiliki Liagkou (University of Ioannina, Greece), Chrysostomos Stylios (University of Ioannina/ ATHENA Research Center, Greece)

IEEE Blockchain '24 - TrustChain workshop	A Systematisation of Knowledge: Connecting European Digital Identities with Web3	Ben Biedermann (Islands and Small States Institute, University of Malta, Malta), Matthew Scerri (WIDE Consortium, Germany), Victoria Kozlova (ACURRAENT UG, Germany), Joshua Ellul (Centre for DLT, University of Malta, Malta)
IEEE Blockchain '24 - TrustChain workshop	Defining Unified Signature API for Mobile Apps to Integrate with Secure Signature Creation Devices (SSCDs)	Ammar Bukhari (Methics Oy, Finland), Jarmo Miettinen (Methics Oy, Finland), Muttukrishnan Rajarajan (City University of London, United Kingdom)
IEEE Blockchain '24 - TrustChain workshop	Designing Inclusive Technology Solutions for Global Communities	Manuel Knott (Hora eV, Austria), Sarra-Maryam Fezzani (Hora eV, Austria)

IEEE Blockchain '24 - TrustChain workshop	Enhancing Security and Scalability in Electronic Voting Through Privacy-Preserving Cryptography and Efficient Data Structures	George Misiakoulis (Konnecta Systems IKE, Greece), Harris Niavis (Konnecta Systems IKE, Greece), Stephane Kundig (Konnecta Systems IKE, Greece), Konstantinos Loupos (Konnecta Systems IKE, Greece)
IEEE Blockchain '24 - TrustChain workshop	SURE: A New Privacy and Utility Assessment Library for Synthetic Data	Dario Brunelli (Clearbox AI, Italy), Shalini Kurapati (Clearbox AI, Italy), Luca Gilli (Clearbox AI, Italy)

IEEE Blockchain '24 - TrustChain workshop, https://zenodo.org/doi/10.5281/zenodo.13618925	Towards a Blockchain-Enabled Trustworthy Market Framework	Thanasis G. Papaioannou (National and Kapodistrian University of Athens, Greece), Dimitris Mantzonis (National and Kapodistrian University of Athens, Greece), Vaios Ritas (National and Kapodistrian University of Athens, Greece)
IEEE Blockchain '24 - TrustChain workshop	User-Empowered Federated Learning in Automotive	Marcello Maugeri (University of Catania, Italy), Mirko Ignazio Paolo Morana (University of Catania, Italy), Sergio Esposito (University of Catania, Italy), Giampaolo Bella (University of Catania, Italy)

IEEE Blockchain '24 - TrustChain workshop	OIDC-PRINCE: OpenID Connect With Privacy-Enhanced Consents	Tiago Galvão (University of Coimbra, CISUC, DEI), Bernardo Arzileiro (University of Coimbra, CISUC, DEI), Bruno Sousa (University of Coimbra, CISUC, DEI

3.3 SOCIETAL IMPACT

TrustChain has funded projects dealing vulnerable communities:

- IM4DEC: DID management method, eIDAS compliant for people with disabilities and in particular for deaf or hard of hearing persons.
- LED-UP: Privacy-aware data sharing and provision of incentives for data sharing to refugees.
- AURORAMINDS: Federated learning approach to privately diagnose ADHD risk in children.
- Orchestral: Privacy-aware identity management system for marginalized citizens.

TrustChain contributes towards better quality of democracy and freedom of speech:

- Zkorum: Anonymous, yet trustworthy, discussion forums with decentralized moderation.
- Trust City: Secure digital tool for local democracy, decentralized decision making in cities.
- FlowBack: Decentralised decision making through liquid democracy with prediction markets that crowdsource social wisdom.
- TREVO: Anonymous, tamper-proof, authentic and secure e-voting for citizens.

Also, Tru-IP AMiCA helps on preservation of cultural heritage as it deals with the lifecycle management of Real-World Cultural Assets (RWCA) through the use of tokenised Digital Cultural Asset Passports (DCAP).

A collective summary of the societal challenges addressed by the OC1, OC2 and OC3 projects appear in the tables below. The tables show that the two main challenges addressed by almost all projects are those related to **"inclusive, innovative, and reflective societies"** and **"protecting freedom and security of Europe and its citizens"**. Following the above two, the next challenges addressed are **"health, demographic change and wellbeing, climate action", "environment, resource efficiency"** and **"food security, sustainable agriculture"**.

TABLE 3 : SOCIETAL CHALLENGES ADDRESSED IN OC1 PROJECTS

Societal Challenge	DIDroom	Creator Credentials	MUSAP	TREVO	Orchestral	The Social Wallet	DID4EU	IM4DEC	Wide	Client DIDs	EVI	IS-CIS	PRIVÉ
Health, demographic change and wellbeing					X	X		X					X
Food security, sustainable agriculture, marine and maritime, Bioeconomy													
Secure, clean and efficient energy										X			
Smart, green and integrate										X	X		

d transport													
Climate action, environment, resource efficiency and raw materials				X	X		X						X
Europe in a changing world - inclusive, innovative and reflective societies	X	X	X	X	X	X	X		X				X
Secure societies - protecting freedom and security of Europe and its citizens	X	X	X	X	X	X	X		X		X	X	X

TABLE 4 : SOCIETAL CHALLENGES ADDRESSED IN OC2 PROJECTS

Societal Challenge	SURE	ProvenAI	PECS	OIDC-PRINCE	NG-SC	MorphMetro	LED-UP	GUEDHS	EIDCMP	DUME	DID-IMP	DOOF	DGUARD	AURORAMINDS	UtiP-DAM

Health, demographic change and wellbeing	X						X						X	
Food security, sustainable agriculture, marine and maritime, Bioeconomy														
Secure, clean and efficient energy														
Smart, green and integrated														

transport														
Climate action, environment, resource efficiency and raw materials														
Europe in a changing world - inclusive, innovative and reflective societies		X					X						X	
Secure societies - protecting freedom and secur	X						X						X	

ity of Europe and its citizens															

TABLE 5 : SOCIETAL CHALLENGES ADDRESSED IN OC3 PROJECTS

Societal Challenge	DIDimo	Zkorum	AI-MetabloQ	Spark-IT	FitChain	TrustCity	Flora	TAC!	Value4All	AUTHBOND	FlowBack	TradeOnChain	Tru-IP AMiCA	QX Travel Experience	SecureOpinion
Health, demographic change and well being			X		X	X	X		X	X		X	X		X
Food security, sustainable agriculture, marine and mari			X					X				X			

time, Bioeconomy														
Secure, clean and efficient energy													X	X
Smart, green and integrated transport														
Climate action, environment, resource efficiency and raw materials														

European in a changing world - inclusive, innovative and reflective societies		X				X					X				X
Secure societies - protecting freedom and security of Europe and its citizens	X	X		X	X	X	X	X	X	X	X	X	X	X	X

In the process of conducting 4 Open Call campaigns (4th one being partially covered by this reporting period), TrustChain ecosystem and community around it was an

integral part of the campaigns. Focus being on the ecosystem itself, it was set up with the launch of the first Open Call at the very beginning of the project. It is important to underline that in the first year of the project, certain consortium partners from TrustChain also formed consortium in other NGI initiative projects such as Ontochain. By connecting these two projects, the community created around the first project has been successfully transitioned to TrustChain then joined by each Open Call cohort of innovators and the community following them. Additionally, consortium partners have leveraged their respective networks, initiatives and created synergies and innovators from different Open Calls are encouraged to build upon each other solutions and create other synergies in the project ecosystem. It should be noted that more details on the Open Call campaigns and their reach, collaborations, synergies, webinars and other events are reported in D2. D2.6-D2.9 Open call communication and campaigns reports, D5.1 Dissemination and Communication Report and D5.3 Value Proposition and Impact of OC1.

3.4 TRUSTCHAIN AS PART OF NEXT GENERATION INITIATIVE

In the M1-M18 period, the collaboration with NGI reflected in announcing the Open Calls on the NGI website, newsletter, newsflashes, social media and dedicated groups with a total of more than 11K followers. Additionally, through the regular meetings of the NGI Communication Task Force, calls, innovators news and events organized by the project have been communicated with NGI community including sister projects and the EC representatives. The overall purpose of the NGI Communication Task Force is to bring together representatives from all ongoing NGI projects and members of the NGI Unit at the European Commission, focusing on communication and dissemination activities. Members from ongoing NGI projects in this Task Force serve a dual purpose: they act as spokespersons for their projects, sharing initiatives, challenges, and marketing concerns, while also promoting NGI guidelines, major events, news, and other initiatives within their projects and communities. NGI Community includes EU Member States, Associated countries as well as USA and Canada. For the purposes of TrustChain Open Calls, only the first two are eligible stakeholders/entities.

The most prominent innovators and projects are also to be featured in the NGI's "Who is who" blog adding to the overall promotion of the project and its specific outcomes through the lense of a single participating project where they tackle main outcomes of their participation, synergies they have created as well as the impact. Both innovators and consortium members have participated in the NGI Forum 2023 where the project outputs were presented and chosen OC1 innovators participated in the pitch session.

Lastly, through the NGI community, TrustChain has created synergies with other projects: Ontochain, Trublo, NGI Taler, SEEBLOCKS resulting in wider reach for the dissemination and communication activities (More details on synergies in D2. D2.6-

D2.9 Open call communication and campaigns reports as well as D5.1 Dissemination and Communication Report.

3.5 OTHER INITIATIVES, EVENTS OR OPEN CALLS

As a result of the partner networks, collaborations and campaigns conducted by the project. TrustChain has been regularly presented internationally.

TABLE 6: EVENTS WHERE TRUSTCHAIN WAS PRESENTED

Conference Name	Short Conference Description
Digital Enterprise fair, Malaga (2024)	The event brought together 17.157 international digital leaders and 450 international experts, sharing their expertise and innovations linked to disruptive technologies, with the aim of meeting the requirements of today's demand.
Empodera LIVE event 2024	Over 250 experts and global leaders gathered to discuss how to decentralize technological spaces and guarantee the Internet as a fundamental right and a public good for citizens.
Turing Agenda-Setting Workshop on UK Interdisciplinary Research in Digital Identity (2024)	Agenda setting workshop launching a partnership between the Trustworthy Digital Infrastructure for Identity Systems programme at the Alan Turing Institute and the Security, Privacy, Identity and Trust Engagement NetworkPlus (SPRITE+).
IDM June 2024 conference	IDM 2024 is an enterprise-level, technology-focused series of events that at its heart is driven by the motivation to provide a platform for some of the world's leading organisations, both solution providers and end-users, who are rightly regarded as providing world-leading examples of IAM innovation.

The NGI Forum 2023	The NGI Forum 2023 delved into a wide range of topics that support the transition to the future Internet. These discussions encompass digital identity, quantum Internet, large language models and web search, decentralized social media, and the security of the open-source supply chain.
The European Blockchain Convention (EBC) (2023)	Major event for Europe's blockchain community aiming to accelerate the blockchain ecosystem, attracting thousands of attendees annually, including top speakers and innovative startups. The diverse audience of founders, investors, regulators, developers, and corporations gather to learn, get inspired, and network.
European Blockchain Week 2023	Two-day event that convened the Blockchain community from across Europe and beyond. This event was organized as a collaboration between the University of Ljubljana, the EU Blockchain Observatory & Forum, the Slovenian Ministry of Economic Development, and the Technology Park Ljubljana.
EmpoderaLIVE 2023	At EmpoderaLIVE 2023, more than 20 international leaders and researchers and around 250 experts gathered worldwide to define the new rules of the digital era, focused on the protection of citizens' rights against economic and interests of power and in improving people's lives.

Through the participation at these events the dissemination and wider social impact were possible, but it should be noted that another side-impact was created. Among the many presenters and/or stands prevalent with blockchain technology used for cryptocurrencies, among the startup pitches for the VCs; the presence of an EU-funded project that is offering equity-free funding along with mentorship and other benefits has made a perspective shift among the visitors. Therefore, even the participation in the more commercial events resulted in increased number of applications for the Open Calls, but more importantly in expanding the initial ecosystem and awareness raising among many startups.

3.6 COMMUNITY/ECOSYSTEM BUILDING

When it comes to outreach, apart from the promotion of the project itself, major outreach campaigns were conducted during Open Calls. The outreach was conducted through various channels:

- Project and partners' websites, demos, company information
- Direct emails (F6S community, Clusters, DIHs, EEN, Researchers and other databases)
- Newsletters
- Previous projects, initiatives, delegations and networks including NGI and sister projects
- Media and press contacts, media platforms and outlets
- Social media (of project, consortium partners and related stakeholders as well as external ones in connection to the project), social media groups and slack channels.
- Most of the code is open source and it is available at the Github repository of TrustChain.

TABLE 7: ECOSYSTEM DEVELOPMENT IN THE OPEN CALLS OF TRUSTCHAIN

Stakeholders / Channels	OC #1	OC #2	OC #3	OC #4
Previous projects	DAPSI, Block.IS, BlockStart, TruBlo, ONTOCHAIN: 4.166 recipients	Block.IS, TruBlo, ONTOCHAIN: 2.280	2.932 founders	*3
National Contact Points (NCP) and Europe Enterprise Network (EEN)	419 contacts	415	415	415

Digital Innovation Hubs (DIH)	179 contacts	181	181	181
Clusters	112 contacts	112	112	112
EU Delegations and Info Centres	15 contacts	10	10	16
Partner contact and networks	5 (EU Blockchain Forum, European Blockchain Association, INATBA, Blockchain for Europe) and NGI	4 (EU Blockchain Forum, European Blockchain Association, Blockchain for Europe) and NGI	4 (EU Blockchain Forum, European Blockchain Association, Blockchain for Europe) and NGI	6 (EU Blockchain Forum, European Blockchain Association, Blockchain for Europe, INATBA, Praxi Network) and NGI
Startup portals, magazines and platforms	100 + (non-paid media) contacts	106 (non-paid media)	324 (non-paid media)	183 (non-paid media)

Published articles/ blog posts/website or more prominent social media mentions	31	28	33	25
F6S Community	3273 emails/ direct messages	2,600 emails/ direct messages	2,900 emails/ direct messages	+9,263 emails/ direct messages
OC webinars	139 registered, 94 attended, 67 questions	113 registered, 86 attended, 43 questions	73 registered, 58 attended, 21 questions	66 registered, 42 attended, 19 questions
OC applications	177 started applications, 100 submitted	150 started applications, 91 submitted	172 started applications, 109 submitted	108 started applications, 59 submitted

With regard to the project website and information laid out for external stakeholders to get more information, all the project activities and public resources, including innovators' information are available and at all times displayed.

There is the full webinars' playlist, all press releases, Open Call media kits, project logo and branding package, newsletters, as well as "Selected projects" page on which all innovator teams and their respective projects are shown.

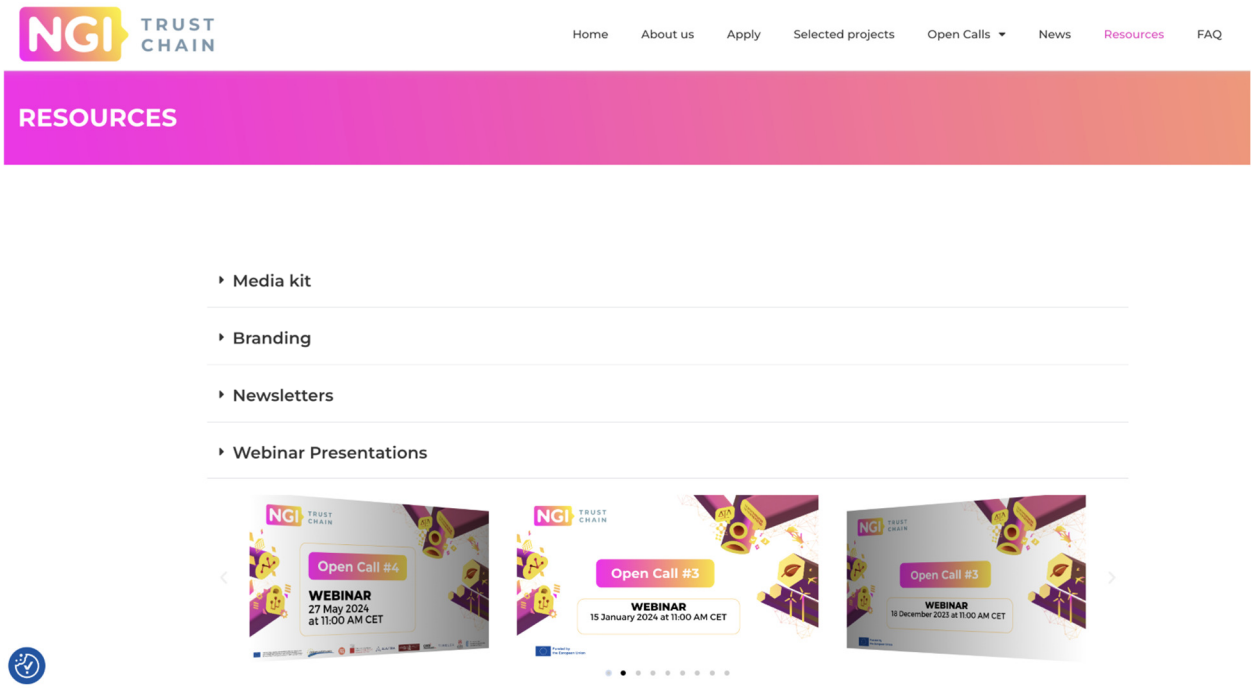


FIGURE 1: TRUSTCHAIN WEBSITE, RESOURCES PAGE

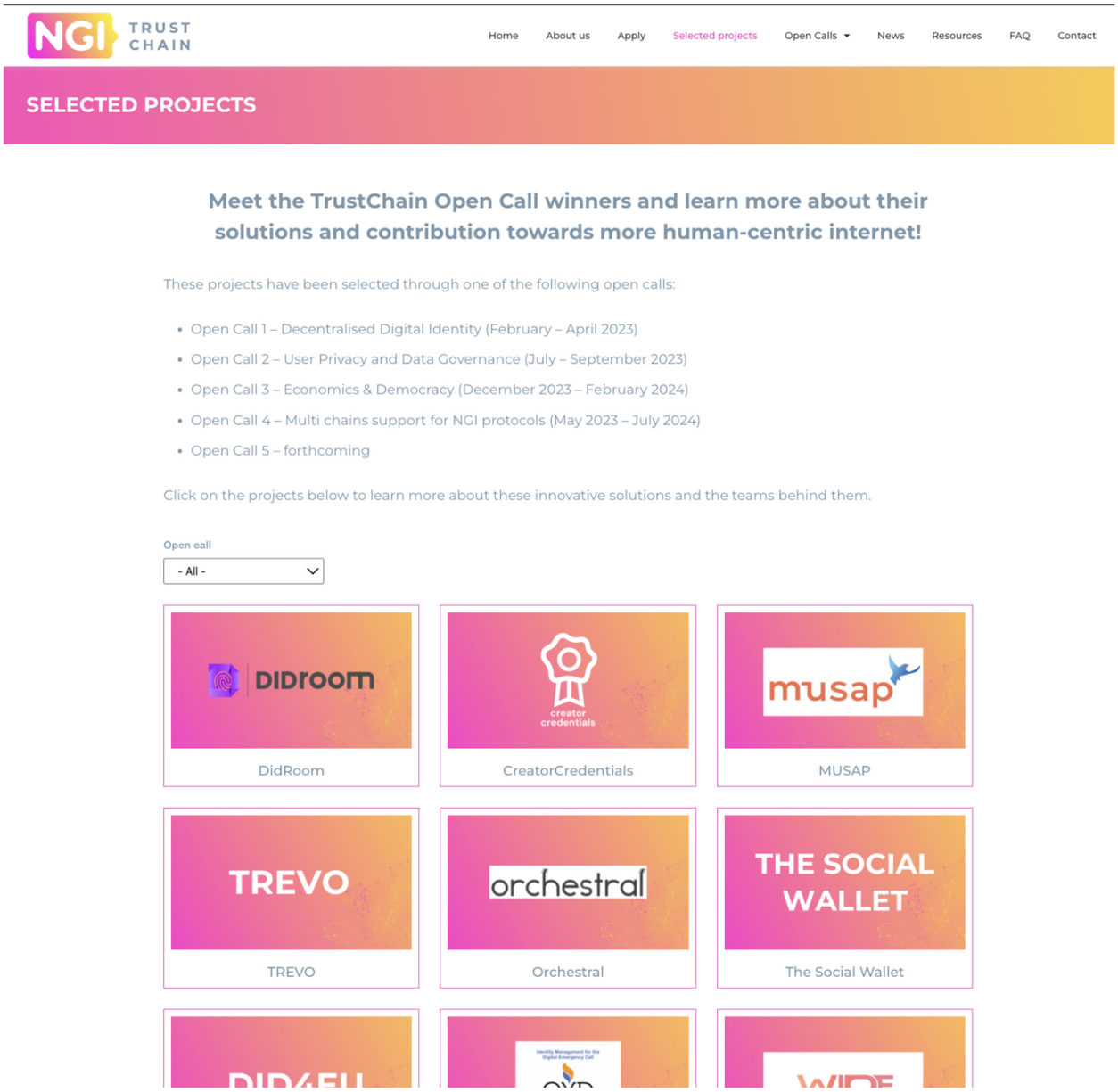


FIGURE 2: TRUSTCHAIN WEBSITE, SELECTED PROJECTS PAGE

3.7 USER-CENTERED DESIGN – END-USERS

Third-party funded project by TrustChain, employing UCD, have documented insights for the functional and non-functional requirements to empower citizens to govern their online data.

TrustChain has involved a large number of end-users in the user pilots of the different solutions developed by third-party funded projects. More specifically, in OC1 913 users have experienced and provided feedback to TrustChain solutions:

TABLE 8: NUMBER OF USERS THAT VALIDATED TRUSTCHAIN SOLUTIONS

Project Name	# of pilot users
CLIENT DIDS	239
Creator Credentials	13
DID4EU	75
DidRoom	36
EVI	10
IM4DEC	280
IS-CIS	25
MUSAP	15
Orchestral	25
PRIVE	145
The social Wallet	0
TREVO	33
WIDE	17
TOTAL	913

3.7.1 Contribution to UN Sustainable Development Goals (SDGs)

A collective summary of the contribution to UN Sustainable Development Goals (SDGs) by the OC1, OC2 projects and OC3 appears in the tables below. From these tables the five SDGs that are mainly addressed by the projects are SDG 3 – Good Health and Well-being, SDG 8 – Decent Work and Economic Growth, SDG 9 – Industry, Innovation, and Infrastructure, SDG 11 – Sustainable Cities and Communities and SDG 16 – Peace, Justice, and Strong Institutions.

TABLE 9 : UN SUSTAINABLE DEVELOPMENT GOALS 1

UN Sustainable Development Goal	DID room	Creator	MUSAP	TREVO	Orchestral	The Social	DID4EU	IM4DEC	Wide	Client DIDs	EVI	IS-CIS	PRIVÉ	SURE	PECS	OIDC PRINCE	NG-SC	MorphMetro	LED-UP	GUEDHS	EIDCMP	DUME	DID-imp	DOOF	DGUARD
SDG 1 – No Poverty						X																			
SDG 2 – Zero Hunger						X																			
SDG 3 – Good Health and Well-being						X		X					X				X			X					
SDG 4 – Quality Education					X				X					X						X					
SDG 5 – Gender Equality													X												
SDG 6 – Clean Water and Sanitation																									
SDG 7 – Affordable and Clean Energy											X													X	
SDG 8 – Decent Work and Economic Growth					X	X	X		X	X				X	X	X	X	X	X		X	X	X	X	X
SDG 9 – Industry, Innovation,	X	X		X		X	X		X	X	X	X	X	X	X		X	X		X	X	X	X	X	X

and Infrastructure																						
SDG 10 – Reducing Inequity					X	X	X		X								X	X		X		
SDG 11 – Sustainable Cities and Communities	X				X	X	X					X			X							
SDG 12 – Responsible Consumption and Production		X			X																	
SDG 13 – Climate Action							X					X										
SDG 14 – Life Below Water																						
SDG 15 – Life On Land																						
SDG 16 – Peace, Justice, and Strong Institutions	X	X	X	X	X				X	X			X		X	X				X		
SDG 17 – Partnerships for the Goals																			X			

TABLE 10 : UN SUSTAINABLE DEVELOPMENT GOALS 2

UN Sustainable Development Goal	AURORA-MINDS	UtiP-DAM	PROVENAI	DIDimo	Zkorum	AI-MetaBloQ	Spark-IT	FitChain	TrustCity	Flora	TAC!	VALUE4ALL	AUTHBOND	FlowBack	TradeOnChain	Tru-IP Amica	QX-Travel Experience	SecureOpinion
SDG 1 – No Poverty																		
SDG 2 – Zero Hunger																		
SDG 3 – Good Health and Well-being	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SDG 4 – Quality Education	X		X			X												
SDG 5 – Gender Equality					X									X				
SDG 6 – Clean Water and Sanitation																		
SDG 7 – Affordable and Clean Energy																		
SDG 8 – Decent Work and Economic Growth		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
SDG 9 – Industry,	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	

Innovation, and Infrastructure																	
SDG 10 – Reducing Inequity					X				X	X				X				X
SDG 11 – Sustainable Cities and Communities	X	X							X		X	X		X		X		
SDG 12 – Responsible Consumption and Production											X							
SDG 13 – Climate Action																		
SDG 14 – Life Below Water																		
SDG 15 – Life On Land																		
SDG 16 – Peace, Justice, and Strong Institutions			X						X					X		X		X
SDG 17 – Partnerships for the Goals					X									X				

3.8 KEY EXPLOITABLE RESULTS

Due to mentorship and coaching activities, and due to technical discussion on the different solutions, the TrustChain consortium retains a joint ownership of the IPRs of all solutions. This is mentioned in the individual contracts for the funding of the different projects.

TABLE 11: KEY EXPLOITABLE RESULTS (KERS) OF TRUSTCHAIN

ID	SOLUTION NAME	DESCRIPTION	LICENSE	OWNER(S)
1	DIDroom	Multiplatform and multifunctional Identity DID/SSI wallet, that uses a novel cryptographic virtual machine called Zenroom VM as the core component driving its mobile wallet, back-end infrastructure, and microservices. It supports multiple standards including W3C DID/VC and ISO 18013-5, and provides extensible cryptographic capabilities encompassing signatures, encryption, zero-knowledge proofs, and blockchain interoperability.	GNU Affero General Public License	Forkbomb BV
2	Creator Credentials	CreatorCredentials is a decentralised user-centric digital identity management framework specifically designed for the cultural and creative communities. This includes a software application that can be used by media organisations to issue verifiable credentials to creators and other	Not yet specified	Posth Werk BV

		rightsholders. It combines the strengths of ISCC (International Standard Content Code) and verifiable credentials.		
3	MUSAP	Unified Signature Application Programming Interface (USAPI) Library to provide a consistent and flexible interface for applications, to request digital signatures with various Levels of Assurance (LoA), regardless of the Secure Signature Creation Device (SSCD) technology or the location of the private key. This library simplifies the development of eID applications, reducing costs, accelerating time-to-market, and enhancing the security of the eID ecosystem.	Apache 2.0	Methics
4	TREVO	Advanced e-voting system that adheres to the fundamental principles of integrity, security, and reliability, leveraging cutting-edge technologies like zero-knowledge proofs (ZKPs), decentralized identities (DIDs), and blockchain.	Apache 2.0	Konnecta Systems IKE, ANAPTYXIAKI ETAIREIA DIMOU TRIKKAION ANAPTYXIAKI ANONYMI ETAIREIA OTA e-TRIKALA A.E.
5	Orchestral	Integration of decentralized identity solutions, allowing organizations to securely manage and verify digital	Not yet specified	Pangea, Universitat Politècnica de Catalunya (UPC)

		identities across multiple contexts and jurisdictions.		
6	The Social Wallet	Identity verification and management solution integrating the OID4VC stack in line with the EUDI Architecture Reference Framework, enhancing security and privacy through selective disclosure of credentials using SD-JWT signatures and DIF Presentation Exchange. It leverages keys from the SSI-SDK for Decentralized Identifiers and tokenization, incorporating web3 tokenization and SSI/VC solutions with W3C VC API and ERC-based tokenization.	Apache 2.0	Sphereon International B.V.
7	DID4EU	Comprehensive open-source identity and wallet solution, integrating major decentralized identity technologies, including self-sovereign identity (SSI), mobile driver's licenses (mDL), and non-fungible/soulbound tokens (NFTs, SBTs).	Apache 2.0	walt.id GmbH
8	IM4DEC	Identity verification and management solution in government-regulated sectors by integrating advanced technologies with practical, safety-critical applications for people with disabilities. It leverages	MIT	Verein zur Förderung der selbstständigen Nutzung von Daten (OwnYourData), Verein zur Entwicklung von

		Verifiable Credentials (VCs) to ensure trustworthy and modern digital proof of government-issued identities. The onboarding process is enhanced by integrating eIDAS2 conformant identities.		standardisierten und barrierefreien Notrufen (DEC112)
9	WIDE	Solution that combines Decentralized Identity (DID) with trusted identity frameworks and Web3, aimed at increasing data availability for decentralized autonomous organizations (DAOs) on public, permissionless distributed ledger technologies (DLTs). Existing eIDAS and Europass credential infrastructure are integrated with the decentralized identity paradigm.	EUROPEAN UNION PUBLIC LICENCE v. 1.2 EUPL	L'Università ta' Malta, acurraent UG
10	CLIENT-DIDS	Improved solution of Universal Registrar that allows creation of DIDs across different DID methods and networks with client-managed secrets decoupling DID creation with key management.	Not yet specified	Danube Tech GmbH
11	EVI	EUDI-compatible digital wallet, accessible via eIDAS2 and OIDC, based on the European Self-Sovereign Identity Framework (ESSIF) and compatible with Alastria's	MIT	EV Loader

		ID Model to store vehicle and contract certificates and integrate with public key infrastructures (PKIs) via blockchain oracles, ensuring seamless integration with the EV ecosystem while adhering to the Plug&Charge specification for EV charging.		
12	IS-CIS (ConInnSeq)	Solution for privacy-centric data management, leveraging Event-Driven Architecture (EDA) and Domain-Driven Design (DDD) principles to offer a robust and scalable framework for consent management.	Not yet specified	Keen Software S.L.U. (UST Global)
13	PRIVÉ	Solution that enables identity wallets to utilize hardware roots of trust like Hardware Secure Modules (HSMs) and Trusted Platform Modules (TPMs).	Not yet specified	Ubitech, Homo Digitalis
14	SURE	A library focusing on producing and evaluating Synthetic Data to preserve utility, privacy, and ensure regulatory compliance.	Not yet specified	CLEARBOX AI SOLUTIONS SRL
15	Proven AI	Solution for IPR management that redefines how contributors interact with AI systems. It employs decentralised identities, ensuring secure and personalised attribution for every	MIT	Ctrl+Development LP

		contribution and provides contributors with a sense of ownership and control over their knowledge data with enhanced traceability.		
16	PECS	Solution to control personal data collection from modern cars by combining together both soft and hard privacy measures.	Not yet specified	Università degli Studi di Catania, Università degli Studi di Modena e Reggio Emilia
17	OIDC PRINCE	Solution to enhance the privacy support in user consents used in OpenID Connect authentication and authorization processes.	Not yet specified	University of Coimbra
18	NG-SC	Solution to provide user privacy while incentivising users to share existing sensor data. A decentralized market is put in place to provide financial incentives for users to contribute their data.	Not yet specified	InnoRenew CoE
19	MorphMetro	Solution for secure data exchange and analysis in quality assurance across various industries.	Not yet specified	Random Red Ltd., MindMint Solutions Ltd.
20	LED-UP	Solution designed to enhance privacy, security, and user control over personal data in the digital space.	Not yet specified	Hora e.V
21	GUEDHS	A data-sharing framework for health data with	Not yet specified	Promptly Health, Instituto Pedro Nunes, Unidade

		federated learning privacy-aware data control.		Local Centro Hospitalar e Universitário de Coimbra (CHUC)
22	EIDCMP	A user-friendly DID/VC framework for issuing eIDAS compliant verifiable credentials.	Not yet specified	WallID SA, APBC, BTC-Bloq4U
23	DUME	Solution for privacy-aware media sharing by means of data sovereignty, empowering users to manage their data through personal data pods.	Not yet specified	Logimade, ARDITI
24	DID-IMP	Solution for privacy-aware data sharing through issuing and revoking credentials.	Not yet specified	Werenode
25	DOOF	Solution for orchestrating user interaction for secure data streaming and data sharing.	Not yet specified	Sidera ICTease, Nexus TLC
26	DGUARD	Framework to facilitate secure data sharing while prioritizing user privacy and security with data segmentation, provenance tracking, and robust auditability. Functionality includes consent management with SSIs, privacy-preserving authentication with ZKPs, secure data transfers and audit trails.	Not yet specified	BLOOCK HUB SL, I2CAT, beHIT

27	AURORA MINDS	Solution for privacy-aware personal data sharing with federated learning and local differential privacy.	Not yet specified	DOTSOFT SA, University of Ioannina, Greece
28	UtiP-DAM	Solution for anonymizing users in data from IoT sensor deployments, using k-anonymity.	Not yet specified	Correlation Systems Ltd.
29	AI-MetaBloQ	DLT-marketplace for privacy-aware sharing of biospecimens.	Not yet specified	Metabio
30	ZKorum	Censorship-resistant solution for anonymizing authentic opinions and decentralized moderation.	Not yet specified	ZKorum
31	DIDimo	Solution for interoperable DIDs and Verifiable Credentials	Not yet specified	Forkbomb BV
32	Spark-IT	Blockchain solution to find mentors and investors while protecting IPRs of innovators.	Not yet specified	Gheorghe Asachi Technical University of Iasi (TUIASI), Sigmatic (SIGMA APPDEV SRL)
33	FitChain	Solution for secure, privacy-preserving, and equitable exchange of personal fitness data through ZKP and blockchain.	Not yet specified	NEURON AI, LOGIKA-X
34	Trust City	Blockchain solution for local democracy where users can actively participate in shaping the city's policies, projects and initiatives.	Not yet specified	City and Me

35	FLORA	Ovulation tracking blockchain-based solution that prioritizes user privacy and data security to discover health issues through federated Learning and PETs.	Not yet specified	ATHENA Research Center, OPSIS-Research SRL
36	TAC!	Solution to track and trace the food production process and to enforce transparency by disclosing information about the products to the parties of the chain and to the end consumers through IoT and blockchain.	Not yet specified	Enismaro S.r.l.
37	VALUE4ALL	Purchasing-history data sharing, data monetization and service review solution.	Not yet specified	Arsys
38	AUTHBOND	Blockchain solution to allow a DAO to issue RFPs with identity verification through business data and eIDAS 2.0 KYB.	Not yet specified	acurraent UG
39	FlowBack	Solution for decentralised decision making through liquid democracy with prediction markets that crowdsource the wisdom of the masses and artificial agents.	Not yet specified	Digital Democracy
40	TradeOnChain	Solution for cross-border on-chain transaction among parties that have SSIs and VCs with customs integration.	Not yet specified	Intrade4you

41	Tru-IP Amica	Tokenisation mechanisms for the protection, exchange, and IPR management of cultural assets by means of lifecycle management of Real World Cultural Assets (RWCA) and tokenised Digital Cultural Asset Passports (DCAP).	Not yet specified	COMPELLIO SA
42	QX Travel Experience	Solution for travellers to provide trustworthy opinions and get rewards by use of DIDs and privacy-protecting mechanisms.	Not yet specified	QX by Qpick sp. Z.O.O, Dialog Consulting
43	SecureOpinion	Decentralised, secure, privacy-preserving openly accessible opinion-sharing platform.	Not yet specified	Innobox LTD

4 ECONOMIC ANALYSIS METHODOLOGY

In this section, we present a brief overview of the economic analysis methodology that we employ for the business development of TrustChain and the third-party projects. Webinars for the presentation of this methodology have been organized for the winning teams of OC1 and OC2, so as to be used for the business exploitation of their solutions. It has also been part of the implementation guide for all open call winners. More details on this methodology can be found in the Appendix. The notion of 'business models' has increasingly been used in recent years to describe the complex environment in which companies and organisations are operating; having to deal with new disruptive technologies, rapidly changing demand patterns, decreasing customer loyalty and constantly facing new entrants onto the market. In this environment, companies and organisations must constantly move and re-position themselves. In order to do so in a structured way, they use so called 'business models' to help them make the right choices.

The basic questions to be answered in the business model are the fundamental questions of any business:

- What does the company offer to the customer?
- Who are these customers and how should the company operate to deliver the product or service so that they can create a profitable and sustainable business?

In other words, the company needs to identify and analyse the value proposition in the intended TrustChain platform, to which customer group the service is targeted and how to organise to deliver the service in the most efficient way.

In TrustChain, process modelling will be employed for business model analysis. The process modelling focuses on the implementation of TrustChain services in an existing ecosystem infrastructure, based on realistic assumptions of costs and benefits and properly separating capital and operational expenditures.

To define, describe, select and assess the most promising business model(s) (BM) for TrustChain, the project uses different methods. The process and associated methods are outlined in Figure 3: The overall methodology for business model analysis is shown below. Market analysis concerns the overview of the global and European energy markets in terms of market value per region and per vertical, to overview the current stakeholders in the market, and to investigate existing business paradigms and models.

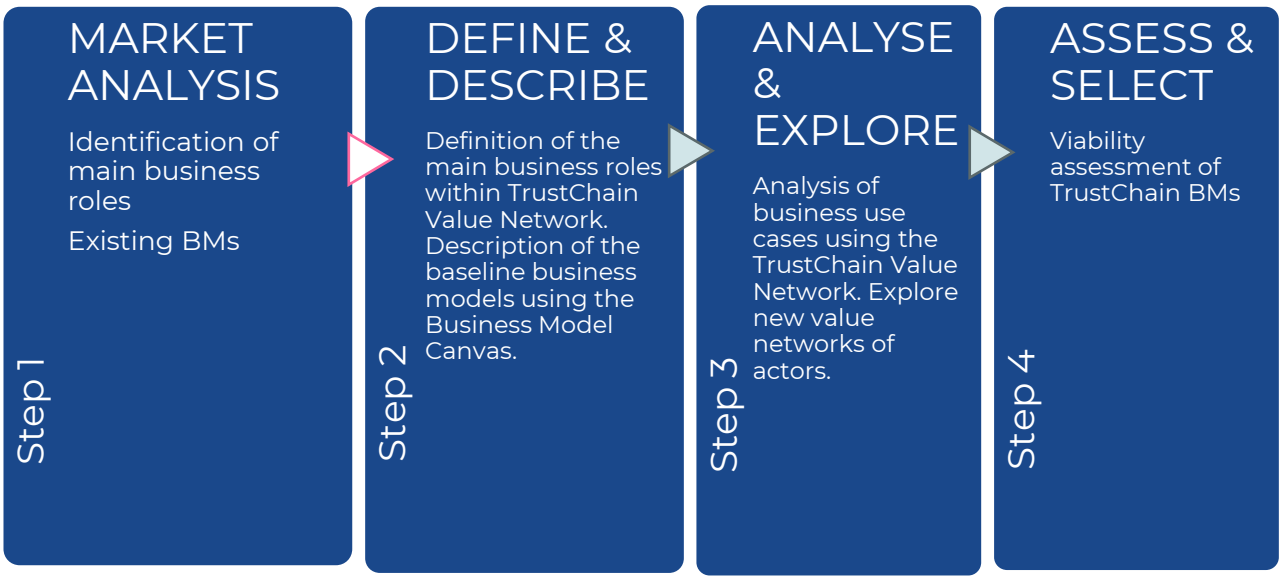


FIGURE 3: THE OVERALL METHODOLOGY FOR BUSINESS MODEL ANALYSIS.

Step 2 is about defining and describing a business model by means of a value network definition and a business model canvas. The value network concept is described in Subsection 8.1.1, while that of business model canvas in Subsection 8.1.2. In step 3, the value network defined in step 2 is analyzed to expose all values exchanged in the

Funded by the European Union

interactions of the different roles. These values may include multiple revenue or cost parameters that have to be thoroughly explored. Finally, in step 4, an economic analysis of the proposed business model is performed for a certain time horizon, as described in Subsection 8.1.3, aiming to answer questions on the profitability of the investment, on its payback period, on its deficits, etc, based on realistic assumptions on the various revenue and cost parameters found in step 3.

5 BM DEFINITIONS AND ECONOMIC ANALYSES

This section presents the business models and the economic analyses for the projects.

5.1 THIRD-PARTY BUSINESS MODELS IN BRIEF

The business models in brief for all OC1, OC2 projects are presented in the following subsections. Detailed market, business and economic analyses for these projects can be found in the Appendix.

5.1.1 DIDroom

Business model: freemium, partial/full on-premises deployment, white-labelling, relicensing and support

DIDroom is born as a multitenant white-label platform, this allows to offer multiple subscriptions options.

Free plan

Anyone can create an account (and an Organisation attached to it). The Free plan allows to (figure TBC and will change over time):

Create one Organisation and appoint a user as credential issuer manager and verifier

Invite 10 users to join the organisation as holder

Create 1-3 credential flows: the credentials issued can be configured from a template, the issuers run on a non-configurable, external microservice, managed in-house.

Create 1-3 verification flows (relying parties, according to the EUDI-ARF jargon): same as with the issuers

Issue 20 credentials per month

Verify 30 credentials per month

The Free plan is meant to allow smaller organisations to use the solution for free and larger organisations to test it and get started. The free plan offers creation and verification of credentials only using predefined microservices, hosted by Forkbomb, meaning that the keys of the issuers and verifiers are generated and kept on the platform.

Paid plans

- Invite unlimited users and credential issuing and verification
- Appoint multiple users as credential issuer manager and verifier
- Possibility to configure and use external issuer and verification microservices (based on Zenswarm or not).DIDroom offers support with setup, monitoring and maintenance (possibly individually) of the external microservices for issuing and verifying
- Web-hooks and APIs for interoperability (with web-services, DBs and blockchain), with logging
- Possibility to relicense and white-label the mobile app (AGPL3)

Target price:

- 5-50 EUR/user/month, depending on:
    - Issuer/verifier microservices (maintained or on-premises, deployed manually or automatically)
    - Usage of theW3C-DID service
    - API and web-hooks usage and logging
    - White label wallet

On-premises deployment

- Support with setup, monitoring and maintenance (possibly individually) of the back-end and admin dashboard and the microservices for issuing/verification
- Support with setup, monitoring and maintenance of theW3C-DID method
- Support with API and web-hooks for interoperability
- Support with customization (back-end, admin dashboard, mobile apps)
- Software relicensing (the whole platform is AGPL3)

- Target price: from 50K EUR year

Custom development, integration with 3rd party platforms

DIDroom is built on top of Starters (https://github.com/dyne/starters) as a modular, easy to extend and to integrate platform. Starters includes advanced features such as:

- Automatic push of updates to children project
- End-to-end testing with Playwright
- Webhooks and REST APIs
- Webauthn authentication
- Transaction email with Sendgrid

This allows the solution to be heavily customised and plugged into existing solutions. The aim is to offer custom development as an extra service, to increase functionalities and provide interoperability and integration with third-party services.

Microservice as a service

Due to the high interoperability of the platform, consideration is being given to offering microservices such as credential issuing and verification as standalone services. Which implies

- it requires integration of 3rd party solutions
- it doesn't require the whole solution to be used
- can be charged on a per hour base

This is in fact a subset of the previous revenue stream. The project is currently exploring marketplaces such as AWS and DAPPnode to publish its microservices. (AWS recently provided free credit for this purpose.)

5.1.2 Creator Credentials

TABLE 12: BUSINESS MODEL CANVAS OF CREATOR CREDENTIAL

The Business Model Canvas

CreatorCredentials.com | Posth Werk BV | 2024-01-21, v0.1

Key Partners

- **Individual creators and rightsholders** from all media sectors. incl. photographers, authors, publishers, distributors, and other stakeholders
- **Trusted entities** in the cultural and creative sectors that will act as credentials issuers
- **Technology partners** for infrastructure, security, and platform development
- Academic institutions for research and development
- Policy makers to comply with upcoming regulatory requirements

Key Activities

- Developing and maintaining the Creator Credentials software application
- Engaging with stakeholders for feedback and iterative improvements
- Promoting adoption through webinars, training sessions, and workshops
- Building and managing the legal framework for digital identity management

Key Resources

- The Creator Credentials app and associated legal framework
- The Technology stack for digital identity management
- Community of creators and users for feedback and validation

Value Proposition

- Providing a secure, verifiable **digital identity management framework**
- **Enhancing trust and transparency** in the origin and ownership of digital content
- Offering **verifiable attribution** in online media environments
- Streamlining the process for creators to **receive verifiable creator credentials**
- Supporting media organisations to **become trust services** for creators and rights holders

Customer Relationship

- Ongoing engagement with early users for feedback and improvements
- Providing **training and resources** to ensure stakeholders can effectively use the app
- **Support channels** for trouble shooting and user support
- Regular updates and workshops to keep users informed on new features

Channels

- The Creator Credentials app and website for information and access
- Direct engagement through webinars, training, and workshops
- Online platforms and social media for updates and community building
- Customer support for hands-on assistance

Customer Segments

- Creators and rights holders in the cultural and creative industries
- Trusted entities in the cultural and creative sectors that will act as credentials issuers
- Content platforms and services that rely on verified creator identities
- End-users and consumers who value verified content

Cost Structure

- Development and maintenance of the software and legal framework
- Stakeholder engagement and community building activities
- Infrastructure costs for hosting the platform and related services
- Staff costs for development, marketing, and operational support

Revenue Streams

- Subscription fees for use of the Creator Credentials app by organizations
- Transaction fees for processing and verification of credentials
- Licensing fees for the use of the platform's technology by third parties
- Possible funding or grants for supporting the creative industries

Funded by the European Union

5.1.3 MUSAP

TABLE 13: BUSINESS MODEL CANVAS OF MUSAP

Business Model Canvas	*Designed for:* NGI TrustChain	*Designed by:* Methics	*Version:* Version D3	
Key Partners	**Key Activities**	**Value Propositions**	**Customer Relationship**	**Customer Segments**
Digital identity software vendors: - On-boarding - Document signing - eWallet - SSI companies	- Produce articles andcompany visibility for potential customers/partners - Implement service components for serviceintegration with the partners **Key Resources** - Identity specialists - Sales + cost efficientintegration model - Product & Project managers	- Provide multiple LoA identities in onedevice - Enable "High" LoA - Specialized formultiple SSCDs -The project manages the documentation and certification responsibilities for theidentity product.	- Self-service tools - Support community - NGI community **Channels** - App vendor sales channel - Public tenders - Partner sales - Direct sales	- (Q)TSPs commercial - (Q) TSPs public - MNOs - Government agencies - Software vendors
Cost Structure		**Revenue Streams**		
Because of the market fragmentation, European businessmodel focuses on minimizing all costs.		Revenue is generated from charging for the use of licenses. Licensing will be based on number of instances and capabilities of each instance. Capability is a performance, functionality or availability rate of the instance.		

5.1.4 TREVO

TABLE 14: BUSINESS MODEL CANVAS OF TREVO

<table>
<tr><th colspan="5">Business Model Canvas</th></tr>
<tr><th>Key Partners</th><th>Key Activities</th><th>Value Propositions</th><th>Customer Relatic</th><th>Customer Segments</th></tr>
<tr><td rowspan="2">Government bodies
Technology providers
Legal experts</td><td>Softrware developmnet
Research and Development
Marketing
Customer support</td><td rowspan="2">Customizable e-voting system emphasizing inclusivity, low cost, automation, trustworthiness, integrity, and transparency.

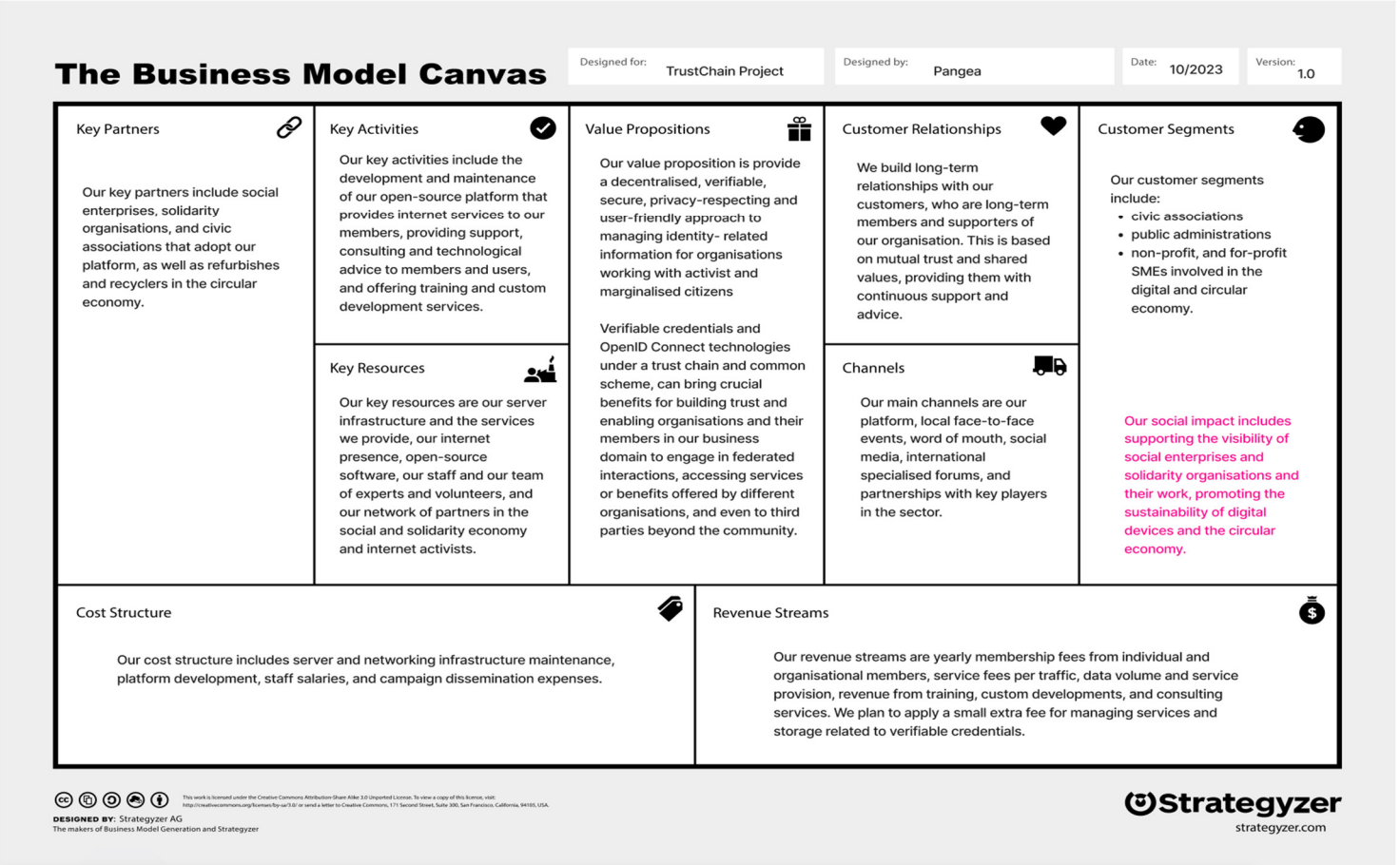
The platform ensures universal verifiability, voter privacy, and a tamper-proof voting process, without the need of a “central authority” owning/managing the solution.</td><td>Co-creation</td><td rowspan="2"><u>government bodies:</u> municipalities
educational institutions

<u>private organizations:</u>
large private companies
local unions
private consortiums</td></tr>
<tr><td>Key Resources

Expert cryptography knowledge
Legal expertise
Software developers
Hosting infrastructure</td><td>Channels
Direct
Indirect
Hybrid</td></tr>
<tr><th colspan="3">Cost Structure</th><th colspan="2">Revenue Streams</th></tr>
<tr><td colspan="3">Research & Development
Operational costs
Marketing and sales
Compliance and legal costs</td><td colspan="2">Licencing (different plans)
Pay per Election
Customization Fees (extra features)</td></tr>
</table>

5.1.5 Orchestral

TABLE 15: BUSINESS MODEL CANVAS OF ORCHESTRAL



The Business Model Canvas

Designed for: TrustChain Project | Designed by: Pangea | Date: 10/2023 | Version: 1.0

Key Partners

Our key partners include social enterprises, solidarity organisations, and civic associations that adopt our platform, as well as refurbishes and recyclers in the circular economy.

Key Activities

Our key activities include the development and maintenance of our open-source platform that provides internet services to our members, providing support, consulting and technological advice to members and users, and offering training and custom development services.

Key Resources

Our key resources are our server infrastructure and the services we provide, our internet presence, open-source software, our staff and our team of experts and volunteers, and our network of partners in the social and solidarity economy and internet activists.

Value Propositions

Our value proposition is provide a decentralised, verifiable, secure, privacy-respecting and user-friendly approach to managing identity- related information for organisations working with activist and marginalised citizens

Verifiable credentials and OpenID Connect technologies under a trust chain and common scheme, can bring crucial benefits for building trust and enabling organisations and their members in our business domain to engage in federated interactions, accessing services or benefits offered by different organisations, and even to third parties beyond the community.

Customer Relationships

We build long-term relationships with our customers, who are long-term members and supporters of our organisation. This is based on mutual trust and shared values, providing them with continuous support and advice.

Channels

Our main channels are our platform, local face-to-face events, word of mouth, social media, international specialised forums, and partnerships with key players in the sector.

Customer Segments

Our customer segments include:

- civic associations
- public administrations
- non-profit, and for-profit SMEs involved in the digital and circular economy.

Our social impact includes supporting the visibility of social enterprises and solidarity organisations and their work, promoting the sustainability of digital devices and the circular economy.

Cost Structure

Our cost structure includes server and networking infrastructure maintenance, platform development, staff salaries, and campaign dissemination expenses.

Revenue Streams

Our revenue streams are yearly membership fees from individual and organisational members, service fees per traffic, data volume and service provision, revenue from training, custom developments, and consulting services. We plan to apply a small extra fee for managing services and storage related to verifiable credentials.

5.1.6 The Social Wallet

The Social Wallet smartphone app is Open Source and free to use for the end users. They will be able to download the app from the App Stores and use it to work with Verifiable Credentials as a generic credential wallet, compatible with other W3C-compliant credential systems, independent of the Social Wallet platform using peer to peer communication (OID4VC)

The Social Wallet platform is Open-Source as well but will also be offered as a paid Software as a Service (SaaS).

This means that municipalities, NGOs, or other sponsors, could download and run the Social Wallet platform themselves, without any involvement of Sphereon. However, as you are aware, this is complex technology that is still changing and evolving.

It is expected that most organizations do not want to be bothered with such a burden and prefer to opt for using a SaaS offering. Or at least have some form of a commercial support services contract.

5.1.7 DID4EU

TABLE 16: BUSINESS MODEL CANVAS OF DID4EU

Key Partnerships

1. Identity ecosystems (e.g. PKIs, blockchains)
2. Consulting firms (e.g. Accenture)
3. Integrators (e.g. GFT)

Key Activities

1. Build / maintain out open source infrastructure
2. R&D / Standardization
3. Manage SaaS Platform

Key Resources

1. People (team)
2. IP / Brand (open source core, closed source extensions/cloud)

Value Propositions

1. Open Source
2. Flexibility (On-premise, SaaS)
3. Most features (ID, NFTs/SBTs)
4. Standard Compliance (interoperable, no-lockin)
5. Regulatory Compliance (e.g. eIDAS2, GDPR)

Customer Relationships

1. Open source / Freemium users:
   - Community forum / FAQs
   - Best effort support
   - Documentation
   - Code Contributions
2. Customers (paying)
   - Support / Ticketing
   - Onboarding / Training

Channels

1. Open Source (GitHub, word of mouth)
2. Content (SEO, Social)
3. Key Partnerships (consulting firms, integrators, blockchain ecosystems)

Customer Segments

Our Products enable organizations to adopt digital / decentralized identity and identity wallets.

1. Users: Developers / product teams
2. Customers: Organizations
   - Public Sector (with partners)
   - Private Sector / Enterprise (focus)
   - Private Sector / SME (SaaS)

Main verticals:

- Public Sector
- Banking / Finance
- Tech / Telco
- Education / Employment

Cost Structure

1. Personnell (80%),
2. Infrastructure and software (e.g. server)
3. Third party services (e.g. legal, tax, tech)

Our monthly costs are currently at approx. 50.000 EUR.

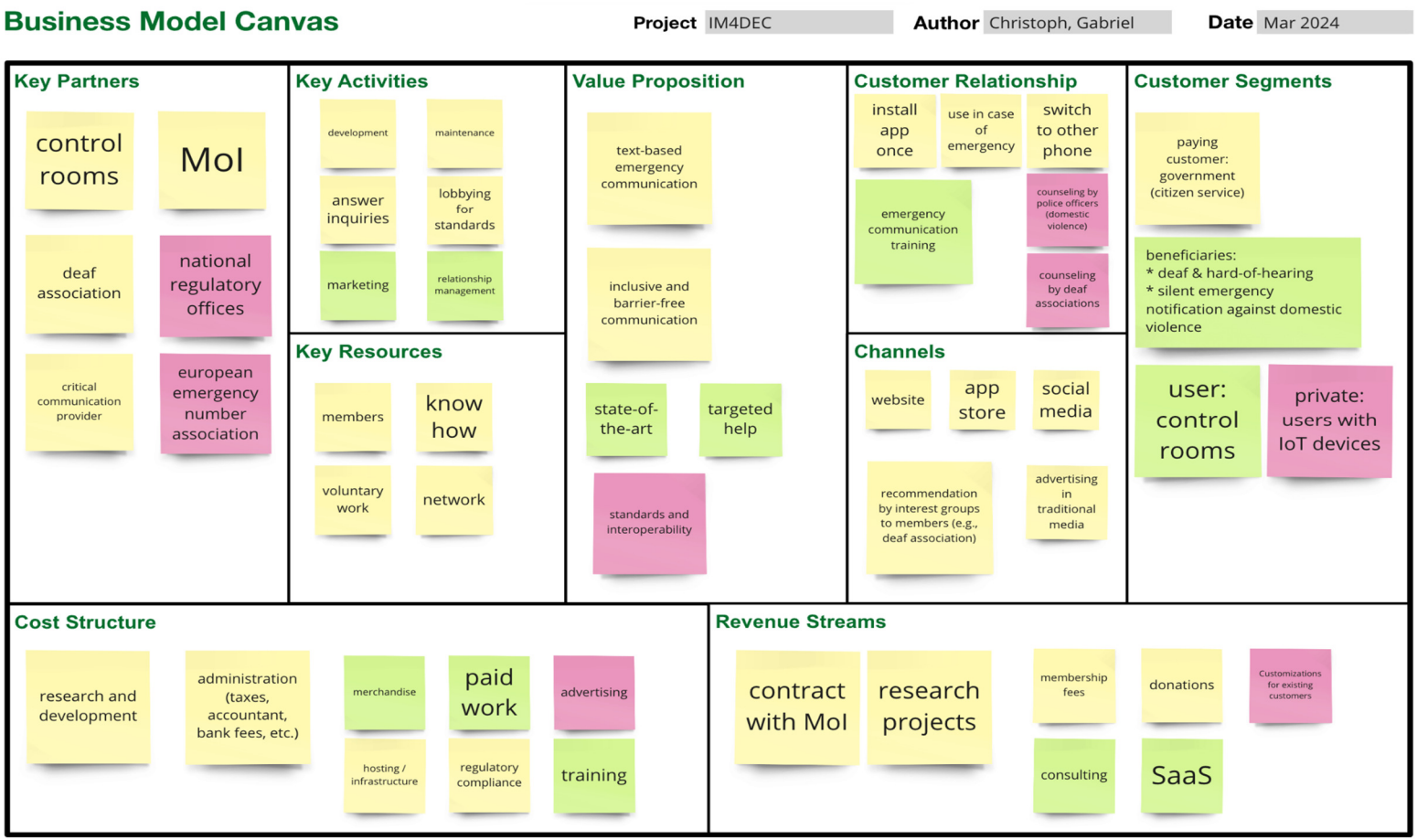
Revenue Streams

(1) Self-managed: Support contracts (annual recurring)

(2) SaaS: Transaction-based pricing (cost per credential issuance/verification; cost per active identity wallet)

5.1.8 IM4DEC

TABLE 17: BUSINESS MODEL CANVAS OF IM4DEC



5.1.9 WIDE

TABLE 18: BUSINESS MODEL CANVAS OF WIDE

Business Model Canvas

Designed For: WIDE | Designed by: NICOLE | Date: 02/04 | Version: 4

Key Partners
- ISSUERS
- THIRD-PARTY WALLET LIBRARIES
- WEB3 WALLET PROVIDERS
- CORPORATE SERVICE PROVIDERS
- DECENTRALISED AUTONOMOUS ORGANISATIONS (*E.G.* RAIDGUILD)
- RESEARCH INSTITUTES

Key Activities
- LAUNCH CREDENTIAL ATTESTATION
- INTEGRATE CREDENTIAL PRESENTATION
- IMPLEMENTATION OF PREDICATES
- BUILT SOLUTIONS ON WIDE
- INTEGRATION WITH VARIOUS SYSTEMS
- REFINEMENT OF UX / UI
- PARTNERSHIP DEVELOPMENT

Key Resources
- TECHNOLOGY INFRASTRUCTURE IN DECENTRALISED IDENTITIES
- EXPERTISE IN WEB3 AND SECURITY
- LEGAL AND REGULATORY
- STRATEGIC PARTNERSHIPS
- MARKET ANALYSIS AND STRATEGY IMPLEMENTATION
- USER-CENTRIC DESIGN AND INTERFACE

Value Propositions
- SECURE AND TRUSTED IDENTITY VERIFICATION
- INTEROPERABILITY AND FLEXIBILITY
- COMPLIANCE WITH REGULATORY AND LEGAL STANDARDS
- SUPPORT TO DAOS
- SECURE STORAGE
- SDG CONTRIBUTION
- PRIVACY PRESERVING IDENTITY CREDENTIALS

Customer Relationship
- SUPPORT AND ASSISTANCE
- COMMUNITY ENGAGEMENT

Channel
- WIDE'S PLATFORM
- B2B NETWORKS
- WORKSHOPS

Customer Segments
- EDUCATIONAL INSTITUTIONS
- PROFESSIONAL COMMUNITIES
- DAOS
- CORPORATE CLIENTS
- GENERAL PUBLIC

Cost Structure
- RESEARCH & DEVELOPMENT
- OPERATIONAL EXPENSES
- LEGAL AND COMPLIANCE COSTS
- MARKETING EXPENSES

Revenue Stream
- PUBLIC AND PRIVATE FUNDING
- SYSTEM INTEGRATION AND CONSULTANCY SERVICES
- EDUCATIONAL WORKSHOPS
- SERVICE FEES
- SUBSCRIPTION AND LICENSING PLANS
- PARTNERSHIP REVENUE

5.1.10 Client DIDs

The project pursues a model commonly known as "Open Core". This means continuing to develop and maintain the open-source Universal Registrar component, while also working on a proprietary version that adds extra features and supports additional DID methods.

This proprietary product is offered in the following ways:

- As a Software-as-a-Service (SaaS) platform. Client can use this platform eithervia a web interface, or API. Independently of whether they use the web inter-face or API, clients have to sign up for a paid subscription model with monthlyfees, organized in tiers that include different amounts of transactions that cli-ents can execute. For example, at Tier 1, clients can execute 2000 transactions
- / Month for a package fee of EUR 60. If the number of transactions is exceed-ed, extra charges apply.

- As a self-hosted on premise solution, where customers host the proprietary version of the Universal Registrar product within their own infrastructure. This approach is specifically meant for governments and large companies. In this case, annual license fees apply that also depend on the number of transactions executed using the product. Additional support fees of about 20% also apply in addition to the license fees.

There is believed to be great value in being able to create and manage DIDs in a "universal" way across different DID methods and ecosystems. With SSI on the rise inmany initiatives around the world, there is also growing interest in enabling global interoperability to seamlessly connect decentralized identity infrastructures. The Universal Registrar component is a contribution to this development.

Surveys have been conducted with industry contacts in an attempt to validate the project's thinking about the business value provided by its work, and to learn about decision factors for using a product such as the Universal Registrar, as opposed to building custom solutions. Here are some results that give insight into business considerations by potential adopters of the tools:

5.1.10.1 Factors for Opting for Hosted Services

- Feature Availability: Organizations look for robust features that cater to their specific needs.

- Maintenance and Time-Efficiency: Hosted services spare teams from the time-consuming task of maintenance, a point emphasized by OKP4.

- Cost and Support: Price and the quality of customer support are pivotal, as revealed by Trustinity.

For companies like OKP4, they spend 8-10 hours weekly on SaaS platforms due tothe time efficiency these systems offer.

5.1.10.2 Factors for On-Premise Solutions

- Technology Control: Businesses value the ability to have full control, avoiding "tech logs" as mentioned by OKP4.
- Security Measures: Security is a priority, especially for companies like Allthenticate, which specialize in it.
- User Autonomy: Autonomy over data and processes also plays a role in this preference.

When it comes to time commitment, it varies depending on customer needs and the scope of the solution.

5.1.10.3 Decision-making Process

- The decision to opt for a hosted or on-premise service predominantly lies withC-level executives, especially the CTO.
- Multiple individuals are usually involved in the decision-making process.
- Legal requirements and company policies often weigh heavily on the decision, particularly for public sector entities.

For OKP4, decision-making lies with a direction committee involving the CTO, CEO, and CPO. Trustinity emphasizes customer consultation in their decision-making process.

5.1.10.4 Industry Variations

- Larger companies and those in specific industries, such as telecommunications, are more inclined to opt for on-premise solutions.
- Smaller companies and those from less regulated industries lean more toward hosted services.

Overall, the market survey reveals a complex landscape of decision-making influenced by avariety of factors such as features, time-efficiency, control, and security. The size of the company and the industry also have significant impacts on the choice between hosted and on-premise solutions.

5.1.11 EVI

TABLE 19: BUSINESS MODEL CANVAS OF EVI

<table>
<tr>
<td rowspan="2">Key Partners

Vendors and OEMs of charging stations

Vehicle OEMs

Identity Providers/ Web3 Services

EV Roaming Networks

Hubject, Gireve e.t.c</td>
<td>Key Activities

Develop and maintain EVI services

Sales activities to owners of charging stations

Promotion to electric car drivers
Establish partnerships with Identity providers, Web3 Services, EV Roaming network</td>
<td rowspan="2">Value Propositions

Charge Point Operators/ EMSPs
Enable Plug&Charge without in-house development effort

Drivers of Electric vehicles:
Authenticate and start sessions faster, without PII dissemination, No need to use the phone when arriving in each charging stations, simply plug your vehicle</td>
<td rowspan="2">Customer Relationships

Long term for all customer segments</td>
<td rowspan="2">Customer Segments

Charge Point Operators (CPOS

Drivers of Electric vehicles

3rd party EV charge point apps</td>
</tr>
<tr>
<td>Key Resources

Developers

Software plug-ins/ libraries

cloud services</td>
<td>Channels

3rd party charge point applications

Charging Station OEMs</td>
</tr>
<tr>
<td colspan="3">Cost Structure

Payroll for software developers

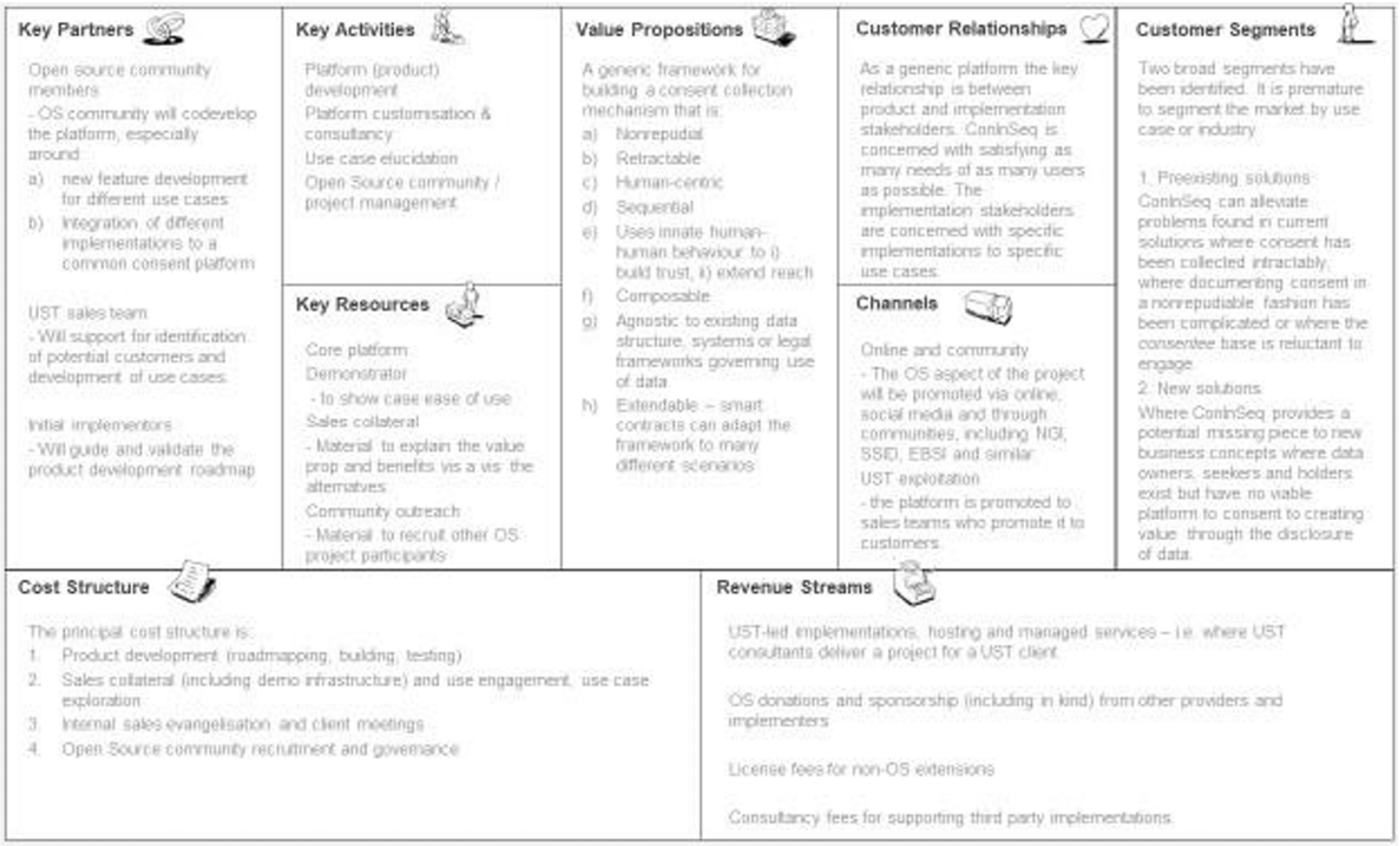
Marketing Budget to EV drivers
Cloud services
subscriptions</td>
<td colspan="3">Revenue Streams

Commission on transactions payable by owners of electric vehicle charging stations

Subscriptions paid by 3rd party apps that use issue and verification by EVI</td>
</tr>
</table>

5.1.12 IS-CIS

TABLE 20: BUSINESS MODEL CANVAS OF IS-CIS



5.1.13 PRIVÉ

TABLE 21: BUSINESS MODEL CANVAS OF PRIVÉ

Key Partners	Key Activities	Value Proposition	Customer Relationships	Customer Segments
• Wallet Service Providers • Startups in the Security and Identity management space • Established SSI Wallet Providers • Tech Companies • Universities • Governmental Bodies	• Product Development and Enhancement • Quality Assurance and Security • Customer Support and Services • Sales and Marketing • Network and Partnership Development • Legal Compliance and Risk Management • Community and User Engagement • Financial Management	• Holders have ownership of their data • Offers to the Holder a capability to control the level of the information disclosure • High Level of Assurance • Ease integration with existing SSI Wallets • Tailored for Modern Compliance	Wallet Service Providers • Dedicated Support • Continuous Updates and Improvements • Training and Resources • Community and Networking Holders • User-Friendly Interface • Customer Support • Educational Content • Feedback and Suggestions Companies for Verification • Tailored Integration Support • Verification as a Service Support Governmental Bodies • Strategic Partnership Management • Customised Implementation Support • Training and Capacity Building • Public Awareness Campaigns	• Wallet Service Providers • Governmental Bodies • Individual Holders
	Key Resources • Human Capital • Technology Infrastructure • Intellectual Property • Network and Partnerships • Financial Resources • Brand and Reputation • Knowledge and Expertise		**Channels** Wallet Service Providers or Governmental Bodies • Direct B2B sales via enterprise sales teams • Online webinars and demos • Technology and fintech conferences. Individual Holders • Advertisements • Online webinars and demos	

Cost Structure	Revenue Streams
• Research and Development • Infrastructure and Operations • Marketing and Sales • Legal & Accounting • Customer Support • Training Materials	• Licensing for Wallet Service Providers or Governmental Bodies • Subscription models for Individual Holders • Verification as a Service (VaaS) - Via the selling of the wallet in Governmental Bodies and Service Providers.

5.1.14 DOOF

TABLE 22: BUSINESS MODEL CANVAS OF DOOF

Business Model Canvas				
Key Partners NGI Research centres/universities Consulting firms and system integrators Benefits: • **normalize the approach towards integrating PETs within current enterprise IT architectures** • **minimize project deployment risks** • position themselves as **referral partners in the privacy realm** • **Resale of Ecosteer DVCO**	**Key Activities** R&D Tech support Project delivery Marketing & communication Sales **Key Resources** Technologies Personnel IP	**Value Propositions** By hiding all complexities exposed by the underlying DVCO components, as well as by any third-party Privacy Enhancing Technology populating the TrustChain ecosystem, this framework allows companies to **minimize** data exchanges deployment **costs and risks**.	**Customer Relationships** Self-service (download from GitHub) Direct support **Channels** • Internal salespeople • Through Partners' and shareholders' network • Website • GitHub & NGI • Conferences	**Customer Segments** Companies with a large customer base using consumers' data for various applications. Target sectors: energy and mobility; from 2026 financial services and healthcare Benefits: • **easily adopt PETs for IoT data sharing scenarios** of any size and across any industry • enable **GDPR and Data Act compliant** data exchanges • enhance **customers' trust and loyalty** • **minimize costs and legal liabilities related to consent management**.
Cost Structure Personnel (tech & customer support, marketing & legal) Cloud infrastructure			**Revenue Streams** With the open-source DOOF, Ecosteer will generate a second revenue stream from system integration services. The pricing model will be Project-based, with fixed fees for specific projects. Additionally, Ecosteer will offer hosting service for small size projects	

5.1.15 AURORA-MINDS

TABLE 23 BUSINESS MODEL CANVAS AURORA-MINDS

AURORA MINDS - Version 3: Independent Technology Privacy Mechanism Applicable to Any Application

Key partners
What are your key partners to get competitive advantage?

- Academics / research institutions
- Enterprise clients across various industries
- 3rd party software development companies

Key activities
What are the key steps to move ahead to your customers?

- Customizing privacy solutions for different applications
- Providing training and support for integration
- Ongoing development to incorporate the latest privacy standards

Key resources
What resources do you need to make your idea work?

- Modular privacy technology adaptable to various platforms
- Development and support teams
- Strategic partnerships with tech companies

Key propositions
How will you make your customers' life happier?

- Easy-to-integrate privacy solutions for any app
- Enhanced user trust through superior data protection
- Compliance with international privacy regulations

Customer relationships
How will you interact with your customers?

- Custom support for enterprise clients
- Community support for developers
- Regular updates and feedback mechanisms

Channels
How are you going to reach your customers?

- Direct sales teams
- Online platforms (company website, tech blogs)
- Developer conferences and tech expos

Customer segments
Who are your customers / Clients? Describe your target audience in a couple of words.

- App developers and tech startups
- Medium to large enterprises in various sectors
- Companies / Organisations requiring compliance with strict data privacy regulations

Cost Structure
How much are you planning to spend on the product development and marketing for a certain period?

- Research and technology development
- Marketing and sales operations
- Customer support and training

Revenue Streams
How much are you planning to earn in a certain period? Compare your costs and revenues.

- Subscription models for ongoing service
- One-time fees for custom integrations
- Licensing fees for technology use

5.1.16 DUME

TABLE 24: BUSINESS MODEL CANVAS OF DUME

Business Model Canvas	Designed for:	Designed by:	Date:	Version:
	DUME	Logimade Lda	25/07/2024	V0.1

Key Partners
Local Governments
Private Enterprises
Tech Companies
AI/ML Researchers
Solid Protocol Community
Data Storage Providers
Marketing Agencies
Customer Support Services

Key Activities
AI Model Training and Validation
Platform Development and Maintenance
Integration with Solid Protocol
Data Collection and Processing
Customer Support and Training
Compliance Management
Marketing and Sales Outreach
Partnership Development

Key Resources
Advanced AI/ML Algorithms
Solid Protocol Integration
High-Performance Servers and Scalable Data Storage
Skilled Development and Research Team
Customer Support Infrastructure
Marketing and Sales Teams
Regulatory Compliance Experts
Funding for Continuous R&D and Platform Enhancements

Value Propositions
Project DUME offers unmatched urban event detection with detailed characterization, including event type, severity, high-resolution images, GPS location, and continuous monitoring. The decentralized architecture ensures user data control, privacy, and security. Theia Vision's multi-applicability spans waste management, infrastructure, safety, and more, with no competition. It fosters community engagement by empowering data contributions and adheres to "privacy by design" principles, ensuring anonymity and trust.

Customer Relationships
Citizens: Empowerment through technology, data transparency, and community contribution.
Image Capturing Companies: Enhance corporate responsibility and visibility. Companies provide broad image datasets from diverse geographic areas.
Clients: Event detection and reporting, continuous monitoring, and analytical metrics.

Channels
Mobile App for direct user engagement.
API for integration with third-party systems.
Online Advertising and Social Media.
Industry Fairs and Conferences Community Events.
Customer Support Centers.
Efficient integration with existing workflows and user routines.

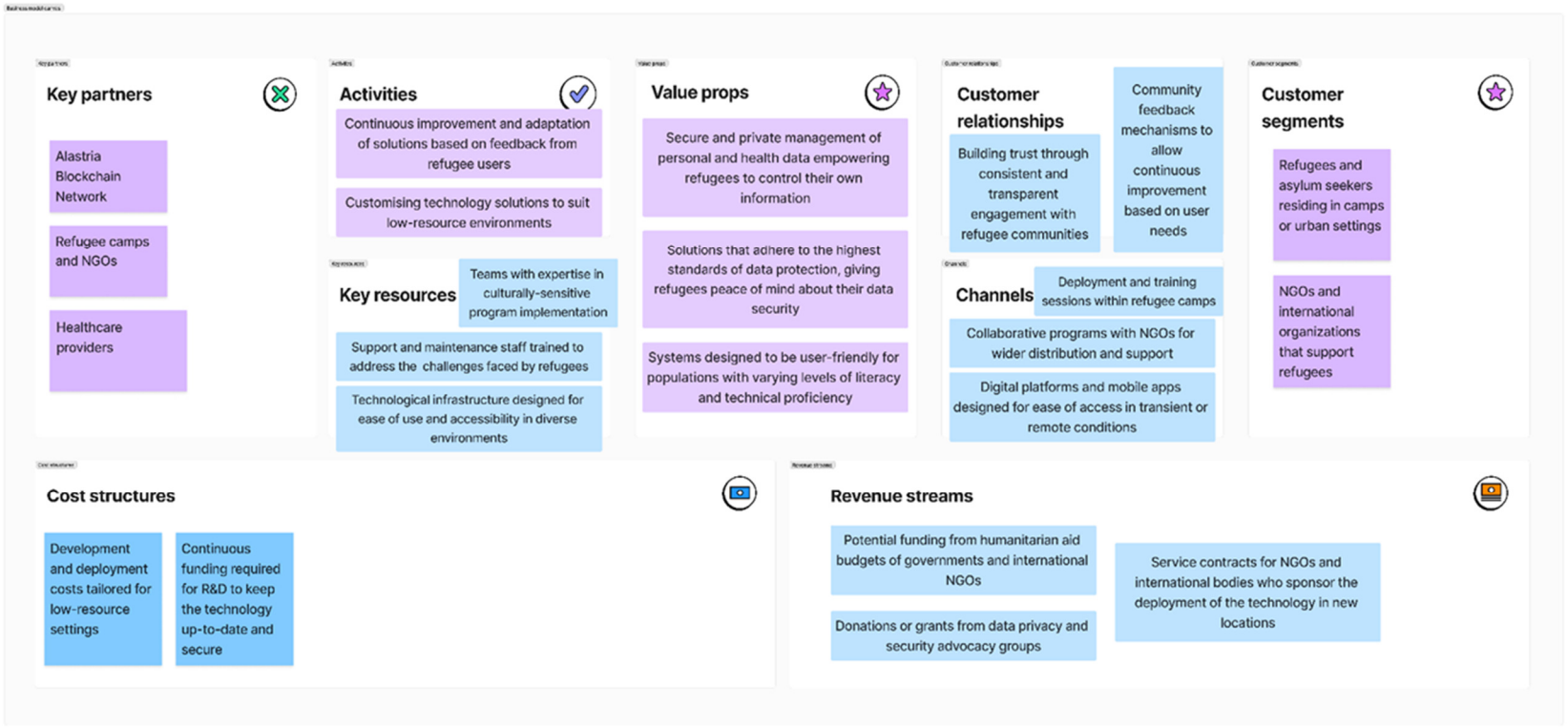
Customer Segments
Citizens: Individuals engaged in community improvement and urban management, contributing data and feedback.
Local Governments: Municipalities needing detailed urban event data for planning, services, and performance evaluation.
Private Enterprises: Companies using data for corporate responsibility, brand visibility, and operational efficiency.
Image Capturing Companies: Organizations with logistical capabilities providing extensive geographic data for analysis.
Tech Companies and Developers: Businesses integrating urban data into their applications for enhanced functionality.

Cost Structure
Project DUME is value-driven, focusing on creating a premium value proposition. The most significant costs are associated with advanced AI/ML development, Solid Protocol integration, and maintaining high-performance servers and scalable data storage. Key activities, such as continuous platform enhancements and compliance management, are also major expenses. Fixed costs include salaries for skilled development and support teams, rents, and utilities. Variable costs cover marketing campaigns and customer engagement initiatives. Economies of scale are achieved through widespread adoption, while economies of scope are realized by expanding platform functionalities and applications.

Revenue Streams
Customers value Theia Vision's advanced urban monitoring and are willing to pay for subscription plans, API access fees, and data analytics services. They currently pay through fixed pricing models, including list prices and feature-dependent subscriptions. Preferred payment methods include pay-as-you-go and fixed-price subscriptions. Major revenue streams are subscription fees, licensing for API access, and custom data analytics reports. Each stream contributes significantly to overall revenues, with subscriptions providing a stable base and API fees and analytics services adding substantial value. Pricing is primarily fixed, tailored to customer needs and usage volumes.

5.1.17 LED-UP

TABLE 25: BUSINESS MODEL CANVAS OF LED-UP



5.1.18 GUEDHS

The value proposition of GUEDHS will focus on secure data collaboration, enabling organizations to perform data analytics and identity verification without transferring or exposing their data. This ensures data privacy and security while allowing for comprehensive analytics and insights. By utilizing privacy-enhancing technologies, the project will ensure that users' identities are verified without exposing personal information, aligning with the increasing demand for privacy and data protection. Additionally, their platform will be designed to comply with global data protection regulations ensuring that data remains within legal boundaries and under the control of its owners.

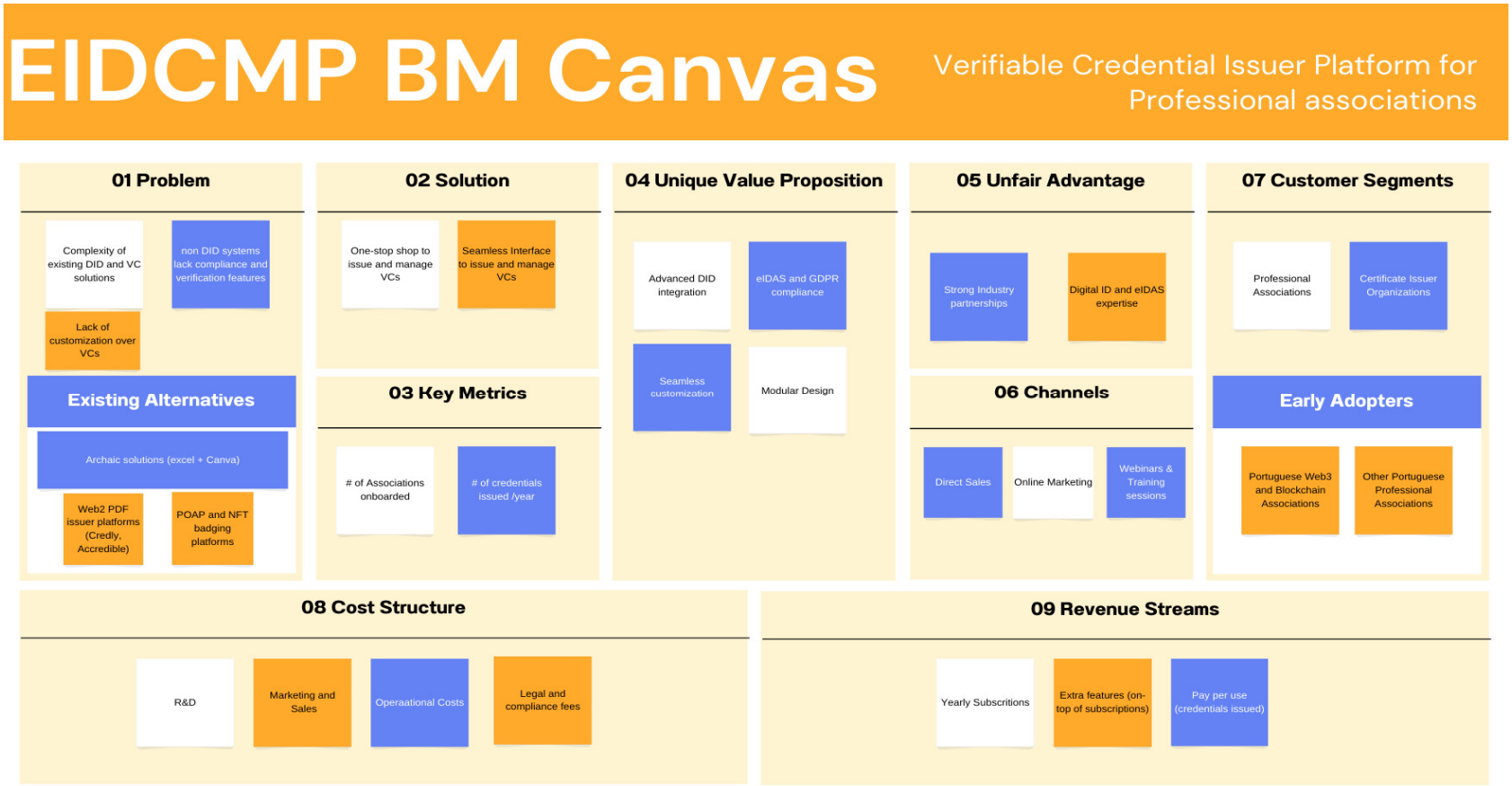
The target market of GUEDHS includes healthcare providers, who will benefit from secure and private patient identity verification and data sharing for improved healthcare outcomes and research. Pharma and MedTech companies will gain access to anonymized, large-scale datasets for drug development and medical research without compromising patient privacy. Insurance companies will be able to access comprehensive health data securely to support value-based healthcare (VBHC) agreements and underwriting processes. Financial institutions will benefit from secure and compliant identity verification services, reducing fraud and enhancing customer onboarding processes.

The revenue model of GUEDHS will incorporate subscription fees for service providers and data users accessing the platform's capabilities. A transaction fee structure will be implemented for each identity verification or data access transaction. Licensing fees will be charged for the use of the suite of Data Products, which support longitudinal data collection and analysis. Additionally, expert consulting services will be offered to help clients implement and optimize their use of the platform for various applications, such as regulatory compliance and real-world evidence (RWE) studies.

Key activities will include continuous platform development to improve security, interoperability, and scalability to meet the needs of different industries. The project will actively engage with users to gather feedback and iterate on the platform's features and capabilities. Ensuring the platform adheres to global data protection and privacy regulations will be a primary focus.

5.1.19 EIDCMP

TABLE 26: BUSINESS MODEL CANVAS OF EIDCMP



5.1.20 OIDC-PRINCE

TABLE 27: BUSINESS MODEL CANVAS OF OIDC-PRINCE

<table>
<tr><th>Key Partners</th><th>Key activities</th><th>Value Propositions</th><th>Customer Relationships</th><th>Customer Segments</th></tr>
<tr><td rowspan="3">Partners:
SSO Providers (Okta, google, Microsoft)
Risk Management (OneTrust, TrustArc, PrivacyEngine)
Suppliers:
Risk Management

Resources:
GDPR compliance proofs
Partnership:
Strategic alliance
Buyer-Supplier relationship</td><td>Activities:
Info of GDPR compliance
Info ot Service type

Distribution Channels:
website and Value-Added Resellers

Revenue:
B2C and B2B
Category:
Production, delivery of service</td><td rowspan="3">Value:
informed consents regarding the privacy risks and GDPR compliance in SSO

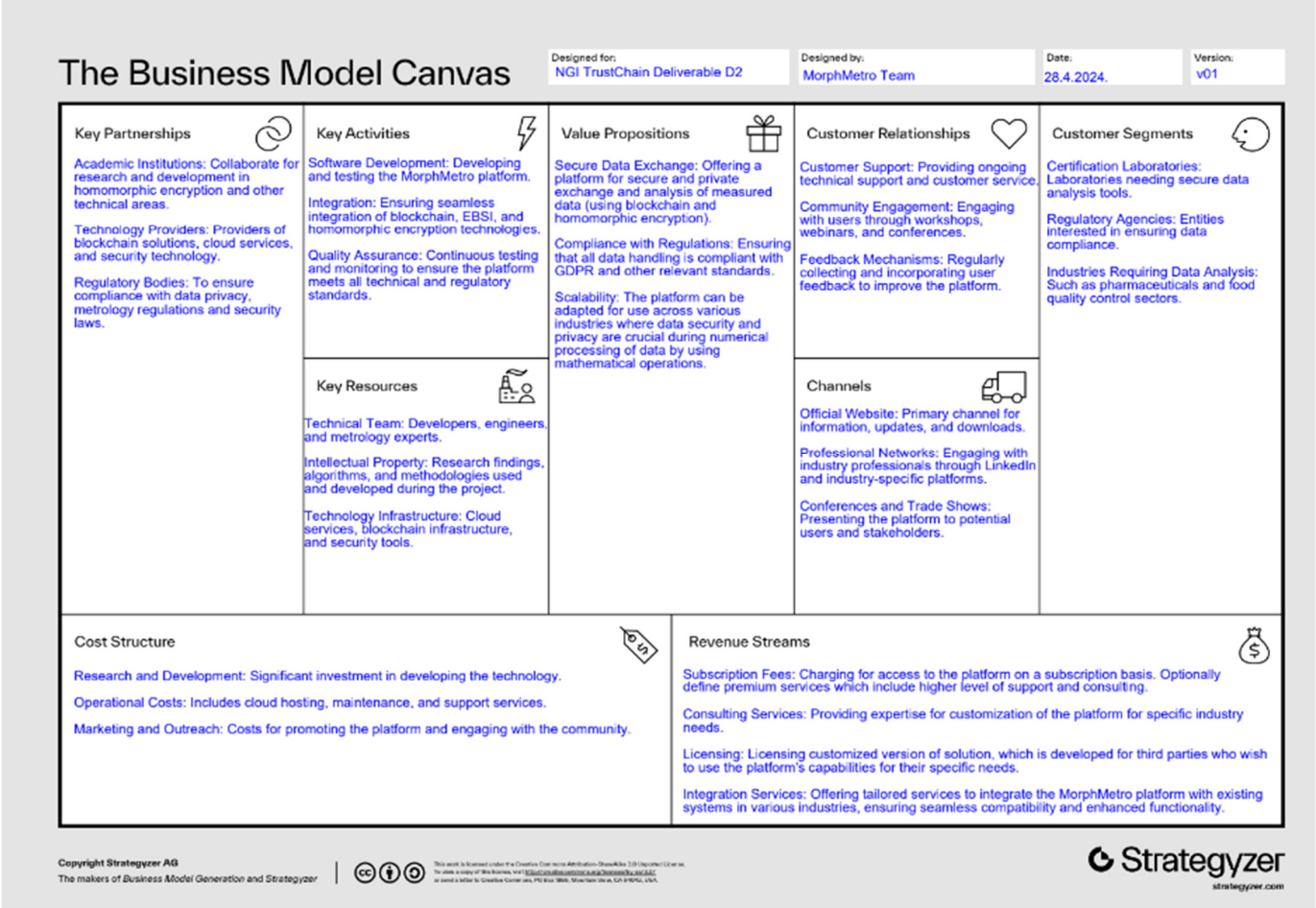
Products and services:
Service to manage privacy risk info

Customer needs:
Users are not aware of the privacy</td><td>Customer Relationships:
- Personal assistance
- Dedicated personal assistance
- Co-Creation
Price Model:
Month or annual subscription</td><td rowspan="3">Most Important customers:
- SSO providers
- Risk Management solutions

Customer Segment:
- Segmented customers like SSO, Risk Management
- Niche Markets</td></tr>
<tr><td>Key Resources
Human Resources:
Developer/Administrator
Security Engineer (DPO)
Marketing
Physical Resources:
Computational resources in cloud or physical servers
Intellectual resources:
Certification of GDPR and NIS2</td><td>Distribution Channels
Channels:
- Direct channels on B2C, D2B
- Partner channels on B2B</td></tr>
<tr><td colspan="2">Cost Structure
Important Costs:
Human Resources
Logistics
Certification</td><td colspan="2">Revenue Streams
Important Revenue Streams:
Asset Sales
Subscription Fee</td></tr>
</table>

5.1.21 MorphMetro

TABLE 28: BUSINESS MODEL CANVAS OF MORPHMETRO



The Business Model Canvas

Designed for: NGI TrustChain Deliverable D2
Designed by: MorphMetro Team
Date: 28.4.2024.
Version: v01

Key Partnerships

Academic Institutions: Collaborate for research and development in homomorphic encryption and other technical areas.

Technology Providers: Providers of blockchain solutions, cloud services, and security technology.

Regulatory Bodies: To ensure compliance with data privacy, metrology regulations and security laws.

Key Activities

Software Development: Developing and testing the MorphMetro platform.

Integration: Ensuring seamless integration of blockchain, EBSI, and homomorphic encryption technologies.

Quality Assurance: Continuous testing and monitoring to ensure the platform meets all technical and regulatory standards.

Key Resources

Technical Team: Developers, engineers, and metrology experts.

Intellectual Property: Research findings, algorithms, and methodologies used and developed during the project.

Technology Infrastructure: Cloud services, blockchain infrastructure, and security tools.

Value Propositions

Secure Data Exchange: Offering a platform for secure and private exchange and analysis of measured data (using blockchain and homomorphic encryption).

Compliance with Regulations: Ensuring that all data handling is compliant with GDPR and other relevant standards.

Scalability: The platform can be adapted for use across various industries where data security and privacy are crucial during numerical processing of data by using mathematical operations.

Customer Relationships

Customer Support: Providing ongoing technical support and customer service.

Community Engagement: Engaging with users through workshops, webinars, and conferences.

Feedback Mechanisms: Regularly collecting and incorporating user feedback to improve the platform.

Channels

Official Website: Primary channel for information, updates, and downloads.

Professional Networks: Engaging with industry professionals through LinkedIn and industry-specific platforms.

Conferences and Trade Shows: Presenting the platform to potential users and stakeholders.

Customer Segments

Certification Laboratories: Laboratories needing secure data analysis tools.

Regulatory Agencies: Entities interested in ensuring data compliance.

Industries Requiring Data Analysis: Such as pharmaceuticals and food quality control sectors.

Cost Structure

Research and Development: Significant investment in developing the technology.

Operational Costs: Includes cloud hosting, maintenance, and support services.

Marketing and Outreach: Costs for promoting the platform and engaging with the community.

Revenue Streams

Subscription Fees: Charging for access to the platform on a subscription basis. Optionally define premium services which include higher level of support and consulting.

Consulting Services: Providing expertise for customization of the platform for specific industry needs.

Licensing: Licensing customized version of solution, which is developed for third parties who wish to use the platform's capabilities for their specific needs.

Integration Services: Offering tailored services to integrate the MorphMetro platform with existing systems in various industries, ensuring seamless compatibility and enhanced functionality.

5.1.22 NG-SC

The solution developed in this project targets future smart cities initiatives. There is currently contact with the municipality of Koper for a potential deployment after the project's conclusion. Following this, plans include engaging with other municipalities interested in smart city initiatives. In addition to smart cities, the data space concept promoted by the European Union is believed to represent a significant opportunity. Data spaces provide a comprehensive and flexible framework for managing various types of data and their interrelationships, addressing the growing need for efficient data handling and utilization in diverse sectors.

Numerous platforms and services have emerged to leverage the vast amounts of data generated daily by internet-enabled devices. However, a common challenge remains: ensuring data privacy. While existing data space projects offer robust data management capabilities, they often lack built-in privacy assurance. Specialized solutions, such as those using homomorphic encryption, have been developed; however, these often fail to fully utilize the capabilities of user devices, as privacy-preserving computation still occurs on edge servers. For instance, the GAIA-X data space integrates with the Ocean Protocol's compute-to-data model to enable in-situ data processing, ensuring privacy for large, curated datasets. Nevertheless, this approach is less effective for the smaller, dispersed datasets typical of IoT environments.

NG-SC, addresses this limitation by providing a privacy-preserving solution for in-situ computation specifically designed for IoT devices. This innovation positions the solution to be adopted by existing dataspaces, enhancing their capability to handle IoT data securely and efficiently. The market potential for the solution is substantial, given the rapid growth of the IoT sector, which is expected to nearly double from 16.7 billion devices in 2023 to approximately 29 billion by 2027.

5.1.23 DID-IMP

Werenode is a for-profit software company that expects to create several revenue streams thanks to this project. The business model for a decentralized identity (DID) solution for secure automatic data transfer in IoT encompasses different revenue streams and strategic approaches to address the specific needs of IoT ecosystems. This model leverages the strengths of blockchain technology to provide a secure, reliable, and scalable solution. Here's a detailed look at the revenue model:

Subscription Model: IoT device manufacturers and service providers pay a recurring fee to access the decentralized identity infrastructure. This is priced monthly for each IoT device for which the data transfers are done through the solution. This fits well into a software as a service platform (SaaS). A licensing fee is also charged for the whole solution on a yearly basis, for the use of the proprietary software or firmware that integrates DID capabilities into IoT devices. This ensures a steady revenue stream and covers continuous access to the network, maintenance, updates, and customer support. This generates upfront revenue and also ensures that clients are invested in the platform. It also allows recovery of development costs and funds for ongoing innovation.

Transaction fees Model: Although the primary architecture might promote feeless transactions for end-users, the model can include minimal fees for high-volume enterprise transactions or advanced features. Indeed, in some use cases, it is expected that a small commission fee can be collected for certain certificate issuances, revocations, or even for some transfers. This scheme is studied for some logistics use cases of DID-IMP. This helps maintain the blockchain infrastructure and compensates for the operational costs associated with large-scale data handling.

Data Services and API Access Model: DID-IMP offers analytics and data verification services that utilize the secure, traceable nature of blockchain to provide added value from the data transferred within the network. In a second wave of developments, APIs will also be provided that enable third-party developers to build applications that interface with the decentralized identity network. Businesses benefit from enhanced data insights and integrity, creating a value-added service that justifies additional fees. The API approach fosters an ecosystem around the technology, in consistency with TrustChain ecosystem strategy, driving wider adoption and generating additional revenue from API calls.

Customization, Integration, Training and Support Model: Charge for consulting and customization services to integrate the decentralized identity system into existing IT landscapes. Offer training for developers, IT staff, and end-users, as well as ongoing technical support. This expert implementation and integration service relies on the fact that, as designers of the DID-IMP solution, the team is expected to be able to provide expert services for the integration and implementation of the solution. This offers high-margin revenue and helps clients maximize the value of their investment in the platform. Furthermore, training and support not only provide additional revenue

streams but also ensure smooth operation and customer satisfaction, fostering long-term client relationships.

Hardware Sales or Partnership Model: DID-IMP will sell the solution or partner with providers of specialized hardware that is optimized for IoT environments utilizing DID systems. The project currently consider using the DID-IMP solution to implement a smart electricity meter that will allow the development of home energy management applications in connection with the current EV charging solution and the Decentralized Energy COmmunities (DECO) project with OP Mobility. This is just an example of many other means where DID-IMP will leverage key use cases to create economical traction through hardware or partnerships. This can create a comprehensive solution offering that includes both software and hardware, optimizing the performance and security of the entire system.

Certification and Compliance Model: Provide certification services for devices and companies that meet specific security and compliance standards enabled by the DID system. Benefits: Certifications can increase the trustworthiness of the devices and services, creating a competitive edge and potentially opening new markets. By leveraging these business models, the decentralized identity solution for IoT will provide a secure and efficient means of data transfer while generating multiple revenue streams. This diverse revenue model not only stabilizes the financial footing of the initiative but also encourages broad adoption across industries by offering various ways to engage with the technology based on the specific needs and capabilities of different users.

5.1.24 DGUARD

TABLE 29: BUSINESS MODEL CANVAS OF DGUARD

KEY ACTIVITIES	CUSTOMER RELATIONSHIPS
RESEARCH AND DEVELOPMENT. To adapt to advances in the field. PRODUCT MAINTENANCE AND IMPROVEMENTS. Improvement of functionalities to increase usabilityand alignment with industry standards and maintenance to ensure service level agreements. CUSTOMER SUCCESS. Provide high-quality customer service to gather as much information as possible on improvements. MARKETING. Promoting DGUARD and maintaining the awareness ofthe brand through advertising, public relations, and relevantcontent. SALES & PARTNERSHIPS. Executea clear sales funnel and build strategic partnerships and allianceswith System Integrators and Software vendors for long term success.	Depending on the phase to position DGUARD will deal with costumers as: DIRECT SALES. DGUARD will provide self-service support through its documentation and resources once it reaches phase 3, enabling partners to integrate seamlessly. Until then, the relationship will be closely managed to gather information on necessary upgrades. DGUARD will handle personalized onboarding processes to expedite product launches and ensure market fit. Once phase 3 is reached, all direct sales efforts will be redirected to the partner ecosystem. DGUARD will prioritize automation wherever feasible, offering helpful resources, training sessions, and architectural drafts to minimizeinternal costs. SYSTEM INTEGRATORS. DGUARD willhave a partner program where to offerspecial incentives or discounts, exclusive resources and training, dedicated support, and partner recognitions through integrator certification. (Phase 3) SOFTWARE VENDORS. DGUARD willoffer an account manager that will help in terms of billing, invoicing, technical support, product updates and co-marketing campaigns for integrated platforms. (Phase 3)

KEY RESOURCES	CHANNELS
TECHNOLOGICAL RESOURCES AND LICENSES: DGUARD possesses the knowledge on the developed software, and technological tools within its ecosystem, all of which will be open-sourced. Its participants have as well several private components which DGUARD integrates with that will act as its main revenue streams. CONTRACTS with System Integrators and Software Vendors: DGUARD will maintain ownership of contracts with its network of partners and collaborators, facilitating market expansion and revenue growth. BRAND REPUTATION: DGUARD will retain ownership of its trademark and the intangible assets accumulated over time through branding, marketing, and public relations efforts. INITIAL SUCCESS STORIES. DGUARD will have the first set of success stories enabling it to position as market leader and differentiating it from competitors and newcomers.	SYSTEM INTEGRATORS. Organizations that specialize in bringing together various hardware, software, and IT services to create a system that meets specific customer needs. This might involve partnership agreements and training and sales support. INTEGRATIONS WITH SOFTWARE VENDORS. Companies that develop, market, and sell software products orapplications to end-users or other organizations. The agreements might involve partnership, bundled sales, co- marketing initiatives or resellerprograms. DIRECT SALES. Selling product directly to the end user. This might force DGUARD to develop or integratewith platforms with in-house team during phase 1-2. It is only desirable for piloting phase.

COSTS	REVENUE STREAMS
SALARIES. DGUARD will rely on its unique team to differentiate from competitors and to fulfil enhancements until phase 3. **MARKETING EXPENSES.** DGUARD will invest on advertising, promotion, and other marketing activities to attract customers and create brand awareness. **PROFESSIONAL SERVICES.** Fees paid to external experts, such as lawyers and compliance consultants, for specialized services and guidance in legal and regulatory matters. **R&D COSTS**. Expenditure on activities aimed at innovation, product development, and improving existing offerings. **SERVERS & INFRASTRUCTURES.** Investment in infrastructure, including servers and related technology.	Depending on the phase to position DGUARD will deal focus its revenue stream on: **(P1, P2) - CONSULTANCY AND DEVELOPMENT FEES.** This is not thefocus of DGUARD but is required to achieve first successful success stories, big corporations and refine the technology. **(P3) - LICENSES.** DGUARD will generate revenue from charging customers on a monthly or yearly recurring basis for the services offered based on the number of used resources on the SaaS platform.

Funded by the European Union

5.1.25 UtiP-DAM

TABLE 30: BUSINESS MODEL CANVAS OF UTIP-DAM

<table>
<tr>
<td rowspan="2">Key Partners

NGI TrustChain

Private companies including Correlation Systems' current customers, notably in Thailand

Mobility Data Space, a Gaia-X lighthouse project

Karel Neuwirt, data privacy expert</td>
<td>Key Activities

- Ensure data privacy with K-anonymization and auditing tools.

- Maintain the UtiP-DAM marketplace for data discovery and download.

- Provide an API for developers to integrate platform functionalities.

- Deploy the anonymization algorithm for data privacy at the source.

- Ensure adherence to data privacy regulations.</td>
<td rowspan="2">Value Proposition

UtiP-DAM empowers various users by providing a secure platform for mobility data.

Here's a value proposition summary:

-Ensure data privacy with auditing and anonymization. Monetize data by publishing anonymized datasets on the marketplace.

-Find valuable insights through anonymized datasets. Download data for further analysis and make data-driven decisions.

-Integrate anonymization into applications and automate data processes using the API.

-Control your data by verifying if it's included in shared datasets.

-Enhance data security with the decentralized Edge network. Streamline data management</td>
<td>Customer Relationships

Automated Service</td>
<td rowspan="2">Customer Segments

Data providers:
-Thecurrent customers who use the sensor technology to collect mobility data.
-Third-party organizations that own mobility datasets.
-Citizens (who can inquire if their data is included).

Data users:
-DPOs who ensure data privacy compliance.
-Data Consumers (researchers, businesses...) who use anonymized data from the UtiP-DAM marketplace or International Data Space.

Developers: These are individuals or organizations used to leverage the platform's functionalities in their own projects.</td>
</tr>
<tr>
<td>Key Resources

Human Resources: A team of experts in data privacy, anonymization, and blockchain technology is crucial for the development and operation of UtiP-DAM.
Technical Resources: The core technical resources include the UtiP-DAM platform itself, including the anonymization algorithms, the UtiP-DAM marketplace infrastructure, and the APIs for developer integration.</td>
<td>Channels

Direct Sales: The UtiP-DAM team can directly approach potential customers like Correlation Systems' existing customers and other data providers to showcase the platform's benefits.

Marketplace: The UtiP-DAM marketplace serves as a key channel for both data providers and data users. Data providers can publish anonymized datasets, while data</td>
</tr>
</table>

	Additionally, collaboration with partners like NGI TrustChain, Pontus-X, and Mobility Data Space provides access to valuable technical resources and expertise.	and potentially generate new revenue streams.	users can discover and download these datasets for further analysis. **Partnerships**: Collaboration with existing industry partners like NGI TrustChain, Pontus-X, and Mobility Data Space can leverage their existing channels and networks to reach a wider audience of potential data providers and users.	
Cost Structure There are two main costs: 1. Development cost: The estimated range is €165,000 to €200,000, with €115,000 covered by the project, leaving a net cost of €50,000 to €85,000. 2. Operational cost: The primary expense is an AWS t3.large server, costing around €100 per month (including storage and data transfer). Over the estimated 3-year project lifetime, this translates to a total OpEx of €3,600. In total, the system cost over 3 years is estimated to be between €53,600 and €88,600.		**Revenue Streams** Approximately three small size projects (33K Euro on average) or one medium size project (100K Euro) will bring the project to a breakeven point.		

5.1.26 PROVENAI

TABLE 31: BUSINESS MODEL CANVAS OF PROVENAI

<table>
<tr><th colspan="2">ProvenAI</th><th>Designed for:</th><th>Designed by:</th><th>Date:</th><th>Version:</th></tr>
<tr><td colspan="2">Business Model Canvas</td><td>ProvenAI</td><td>Ctrl+Space Development</td><td>01.07.2024</td><td></td></tr>
<tr><td>Key Partners</td><td>Key Activities</td><td>Value Propositions</td><td>Customer Relationships</td><td colspan="2">Customer Segments</td></tr>
<tr><td rowspan="2">Data Management Platforms: Integration with existing data management solutions
AI Development Firms: Collaboration for integrating ProvenAI into AI systems
Legal and Compliance Consultants: Partnerships for ensuring regulatory compliance
Educational Institutions
Tutor Collectives</td><td>Platform Development: Designing, developing, and maintaining
Compliance Management: Ensuring compliance with data protection regulations
Marketing and Sales: Promoting the platform, acquiring new customers, and managing relationships
Users' Support: Providing assistance, training, and troubleshooting to customers</td><td rowspan="2">Secure and transparent platform for managing AI interactions with data

Precise control over data access and usage

Compliance with regulations like GDPR

Integration with decentralized identity technologies for secure authentication</td><td rowspan="2">Personalized onboarding and support for data owners and AI developers
Continuous communication for feedback and updates
Compliance assistance and consulting services
Online knowledge base and community forums for self-help</td><td colspan="2" rowspan="2">Data Owners (enterprises, educational institutions, organizations, individuals with valuable data)
AI Developers (companies, researchers, developers creating AI models)
Regulatory Authorities (entities responsible for enforcing data protection regulations)
AI Service Providers (companies utilizing AI technologies for various applications)</td></tr>
<tr><td>Key Resources</td></tr>
<tr><td rowspan="2"></td><td>Development Team: Software engineers, AI experts, blockchain developers
Compliance Experts: Legal advisors, data privacy specialists
Marketing and Sales Team: Sales representatives, marketing specialists
Technology Infrastructure: Servers, databases</td><td>Channels</td><td>Online platform for subscription and access
Direct sales to enterprises and organizations
Partnerships with AI development firms and compliance consultants
Marketing through industry events, conferences, and online channels</td><td colspan="2"></td></tr>
<tr><td colspan="3">Cost Structure</td><td colspan="3">Revenue Streams</td></tr>
<tr><td colspan="3">• Development Costs: Salaries, software tools, infrastructure
• Compliance Costs: Legal fees, compliance audits
• Marketing and Sales Costs: Advertising, promotions, sales commissions
• Operational Costs: Office rent, utilities, administrative expenses</td><td colspan="3">• Subscription fees for data owners based on data volume and usage
• Licensing fees for AI developers based on usage and features
• Consulting fees for compliance and data governance services
• Revenue sharing from fair compensation mechanisms for data usage</td></tr>
</table>

5.1.27 PECS

The business model is provided through the following Business Model Canvas approach.

- Key Partners: MASA for integration and validation, Regulatory bodies for compliance, Industry experts for insights and best practices, Italian car brands such as Maserati, MASA end-users as well as end-users reached by crowdsourcing, TrustChain Network.
- Key activities: Gap analysis and compliance assessments, Research and development of PECSi and PECSo, Validation on MASA infrastructures.
- Key resources: Academic know-how, Technology development team, Data privacy experts, Access to MASA infrastructures.
- Key propositions: PECSi to enhance privacy awareness among end-users, PECSo to enhance privacy passively.
- Customer relationships: Online documentation and crowdsourcing support.
- Channels: Academic and Industry events and conferences, Open-source distribution.
- Customer segments: End-users, Automotive manufacturers, Infotainment software developers.
- Cost structure: Crowdsourcing, Hardware.
- Energy-Efficient Design: During the development of PECSi and PECSo, the project will prioritise energy efficiency.
- Data Minimisation: PECSi and PECSo will be designed to minimise the unnecessary collection and transmission of data, thereby reducing the energy required for data processing and transmission.
- Life Cycle Assessment: A comprehensive lifecycle assessment of the project will be conducted to identify areas where environmental impact can be reduced.
- Environmental Compliance: Project compliance will be ensured within all environmental regulations and standards in the regions where it operates.

5.1.28 SURE

TABLE 32: BUSINESS MODEL CANVAS OF SURE

Business Model Canvas	Designed for:	Designed by:	Date:	Version:
	SURE D2	Shalini Kurapati	06/05/2024	v1

Key Partners
- Technology divisions of banks and financial companies
- IT system integrators
- Privacy professionals
- Data Scientists and Innovation specialists

Key Activities
- Development and maintenance of the SURE library
- Engagement with the data science and privacy regulation communities
- Acquisition of clients for the continuous use of the SURE library and related services

Key Resources
- Human resources, especially skilled data scientists and privacy experts.
- Financial resources for ongoing development and market expansion.

Value Propositions
- Enhances regulatory compliance with data privacy standards like GDPR.
- Facilitates safe data sharing and innovative uses of data

Customer Relationships
- Direct contact and support
- Channel partnerships with IT system integrators
- Community engagement and activities

Channels
- GitHub for easy access and integration.
- Digital marketing for the online platform
- IT system integration partnerships

Customer Segments
- Data science divisions of large companies such as banks and fintech companies
- Risk and compliance divisions of large companies
- IT system integrators

Cost Structure
- HR costs for data scientists and software engineers for development and maintenance, and customisation of the library.
- Marketing, sales, and customer acquisition costs.
- Infrastructure and hardware for in-house data generation
- Office and support staff costs

Revenue Streams
- Subscription fees to access SURE library together with premium data generation libraries (Clearbox AI product)
- Consulting services for customisation and advanced integration.
- Training sessions for companies.

Template source: The Business Model Foundry (www.businessmodelgeneration.com/canvas). Word implementation by: Neos Chronos Limited (https://neoschronos.com). License: CC BY-SA 3.0

6 ECOSYSTEM SUSTAINABILITY

6.1 ALASTRIA PLATFORM FOR TRUSTCHAIN

6.1.1 Current Status

The Alastria platform is a decentralized and permissioned blockchain infrastructure aimed at providing various digital identity and data management services.

All projects that have been selected to be part of any of the OpenCalls have at their disposal any of Alastria's networks. In them, the teams can deploy their projects and perform the pilots or MVP of their developments for the duration of their participation in TrustChain. They have transactions lit at zero cost (0) of gas.

There are currently seven teams using Alastria networks: DidRoom, WIDE, MorphMetro, LED-UP, OIDC-Prince, TAC and DOOF.

6.1.2 Potential exploitation plan

After the TrustChain project concludes, the sustainability of the deployments depends on the exploitation plans crafted during the project phase. These plans would typically detail how the solutions will be maintained, scaled, or commercialized. The continuity of these deployments would likely require either integration into existing commercial services or the establishment of a foundation or entity responsible for their ongoing operation and development. The exploitation strategies should address how to maintain network integrity, user engagement, and legal compliance post-project.

The deployment of isolated networks within the Alastria ecosystem is not currently contemplated. This is true, since the blockchain networks belong to the partners and this type of decision does not depend on the project department. From a technical perspective, Alastria could help the TrustChain consortium to have its own network if necessary, but this would also have to be assessed in terms of effort.

After the end of the TrustChain project, the status of the TrustChain third-party projects deployed will have to be revisited and API-keys may be revoked. If at the end of TrustChain, third-party teams wish to continue deploying their solutions within the Alastia networks, they will have to become part of its partner network. If not, teams will be able to export their projects to any supported EVM network.

6.2 ECOSYSTEM EXPLOITATION

The TrustChain ecosystem could be exploited as an Open-Source Software Foundation (OSSF). The Open-Source Software Foundation (OSSF) is a non-profit organization dedicated to supporting, promoting, and sustaining open-source software projects. The foundation provides essential infrastructure, funding, community support, and advocacy to ensure the longevity and growth of open-source initiatives.

Here are examples of notable OSSFs along with some of their clients or users:

1. Apache Software Foundation (ASF): The Apache Software Foundation (ASF) is one of the most renowned open-source software foundations. It manages over 350 projects, including some of the most popular open-source software in the world. Key Projects include:

- Apache Hadoop (Big Data processing framework)
- Apache Kafka (Real-time data streaming platform)
- Apache HTTP Server (Web server software)

Notable clients/users are:

- Hadoop: Used by companies like Amazon, Facebook, Netflix, and eBay for big data processing.
- Kafka: Used by LinkedIn, Twitter, Airbnb, and Spotify for data streaming and real-time analytics.
- Apache HTTP Server: Powering websites and services for organizations like Adobe, Apple, and Salesforce.

2. Linux Foundation: The Linux Foundation promotes the adoption and support of the Linux operating system and hosts many other prominent open-source projects. Key projects include:

- Linux Kernel
- Kubernetes (Container orchestration platform)
- Hyperledger (Blockchain framework)
- Cloud Native Computing Foundation (CNCF)

Notable clients/users are:

- Linux Kernel: Used by Google, IBM, Oracle, and Microsoft in their cloud infrastructure, operating systems, and servers.
- Kubernetes: Adopted by companies like Google, Red Hat, IBM, and Alibaba Cloud for container management and cloud-native applications.

- Hyperledger: Used by Walmart, IBM, and J.P. Morgan for enterprise blockchain solutions.

3. Mozilla Foundation: Mozilla Foundation is a global nonprofit dedicated to building an internet that is open, accessible, and built for the public good. It is known for creating Firefox, one of the first major open-source web browsers. Key projects include:

- Firefox (Web browser)
- Rust (Programming language)
- Thunderbird (Email client)

Notable clients/users are:

- Firefox: Used globally by millions of individual users as an alternative to Google Chrome and Microsoft Edge.
- Rust: Used by companies like Dropbox, Mozilla, and Cloudflare for systems programming and performance-critical applications.

4. Eclipse Foundation: The Eclipse Foundation is a not-for-profit corporation that oversees the development of the Eclipse Integrated Development Environment (IDE) and a wide variety of other open-source projects. Key projects include:

- Eclipse IDE (Integrated development environment)
- Jakarta EE (Enterprise Java)
- Eclipse Che (Cloud IDE)

Notable clients/users are:

- Eclipse IDE: Widely used by developers and organizations like IBM, SAP, and Red Hat.
- Jakarta EE: Used by enterprises for Java-based applications in industries like banking and telecom, with clients like Deutsche Bank, Accenture, and T-Mobile.

6.2.1 TrustChain as an Open-Source Software Foundation

The key components of the value proposition of an OSSF are as follows:

1. Project Hosting and Infrastructure. Repository Hosting, i.e., hosting services for source code repositories is an essential part. We are employing Github repositories currently.

Another ingredient is the existence of code integration/deployment (CI/CD) pipelines, i.e., automated testing and deployment services. Currently, there is no CI/CD pipeline in service, however, meticulous documentation and detailed deployment instructions are provided for each piece of software. Also, there Web Hosting, i.e., hosting project websites and documentation, should be supported, which is partially done at the web site of TrustChain.

Also, there have been taken some steps towards live software deployment by agreeing with Alastria on a free deployment of TrustChain solutions for non-commercial purposes on their blockchain network. Moreover, an isolated blockchain network could be hosted at Alastria network nodes could be created in the future, if TrustChain transforms to an OSSF in the future.

2. Funding and Grants. Another key component of an OSSF is to attract funding by means of individual donations and corporate sponsorships for software projects of interest. Then, the OSSF provides grants as a financial support for sub-projects. This cascade funding scheme resembles the way that the TrustChain project currently operates by procuring new software projects in its open calls.

3. Community Building and Support. Community building is a very important component of the OSSF business model. This can be accomplished by (i) organizing events, such as conferences, meetups, and hackathons, (ii) mentorship programs, e.g., pairing experienced developers with newcomers, (iii) by means of discussion forums, i.e., hosting discussion boards and support channels. In TrustChain, there are biweekly plenary meeting where technical presentations and discussions take place. Also, TrustChain maintains slack channels for news and multi-lateral technical collaborations among different developer teams. Moreover, TrustChain offers mentorship from experienced researchers to the different software projects funded in the framework of open calls on a biweekly basis.

4. Advocacy and Outreach. An important ingredient is promotion, i.e., advocating for open-source software to businesses and institutions. TrustChain organizes an international workshop co-located with IEEE Blockchain 2024 for promoting the technology developed within its open calls. Also, educational activities by means of providing tutorials, courses, and workshops are important. Such activities happen in the biweekly TrustChain plenary sessions, e.g., tutorial on UCD, tutorial on business analysis, tutorial on data regulations, etc., and within the scrum meetings of the funded projects with their mentors.

5. Legal and Compliance Support. This component comprises licensing assistance, i.e., guidance on open-source licenses, and intellectual property management, i.e., : protecting project IP. TrustChain through Timelex core partner that is a law firm provides support on regulation issues to the teams of funded projects.

6.2.2 Revenue Streams

An OSSF may be supported by a number of revenue streams such as:

1. Donations: (i) Donations from individuals or (ii) crowdfunding, i.e., specific campaigns for projects.

2. Corporate Sponsorships: (i) Tiered Sponsorships, i.e., different levels of sponsorship with benefits, (ii) in-kind contributions, i.e., non-monetary support from corporations.

3. Grants and Subsidies: (i) Government Grants, (ii) Foundation Grants, i.e., financial support from private foundations.

4. Service Fees: (i) Consulting Services, i.e., providing expert support on open-source software. (ii) Training Programs, e.g., paid workshops and certifications.

5. Merchandising and Licensing: (i) Merchandise Sales, i.e., by means of brand establishment, (ii) Content Licensing, e.g., by licensing educational materials.

6.2.3 Costs

Costs vary based on whether the infrastructure is hosted or owned. However, the computational infrastructure for hosting the software solutions needs maintenance due to frequent hardware failures of any kind (Pineiro, Weber & Baroso, 2007), e.g., overheating, PDU failure, rack failure, disk failure, etc. Also, another cost component are the licensing costs for the software tools used in the infrastructure, e.g., hypervisor software, even though most of the software employed is open access. Note that equivalent costs arise for a hosted infrastructure, thus avoiding any capital investments, and we opt for this option. Also, a number of software engineers should be employed to do software maintenance of the infrastructure, i.e., to install updates to guide and guide and orchestrate the solution deployment.

It is important to understand that software solutions for potential clients will be crowdsourced to the software community of the open-source foundation. However, some consultants are needed for the overall design, for negotiating the contracts with clients, and for organizing developer teams for new solutions.

Moreover, another cost component is the organization of community building and promotion events. Marketing costs for promoting the brand name of TrustChain and advertisement through social media should also be taken into account.

Finally, legal costs for contract preparation, fees for legal advice, and insurance costs for mitigating liability risks have also to be considered.

6.2.4 Economic Analysis

We consider a basic scenario for our economic analysis, as follows: 10 software engineers/technicians are employed with average salary of 50,000 EUR. This is considered to be enough personnel for deploying and hosting different software solutions, and maintaining the software infrastructure for the initial 75 solutions of TrustChain. We consider that one consultant/contractor is employed with a salary of

100000 EUR, because this person should combine some high-quality technical and administrative skills.

For infrastructure rent, we consider 100,000 EUR per year, which is close to the expected cost of a cloud infrastructure of 5-7 general-purpose high-end dedicated nodes (e.g., AWS m7g) with 30% utilization for 1 year. The software licensing fees are considered to be 50,000 EUR per year.

We consider the organization of 3 conferences per year, i.e., community and exhibition events, each costing around 50,000 EUR, or equivalently 150,000 EUR for organizing events.

The cost for marketing activities is considered around 50,000 EUR on an annual basis. The legal costs for 10-15 contracts per year are considered to be around 50,000 EUR. Finally, the insurance fees for risk mitigation is taken to be 20,000 EUR, i.e., 2,000-3,000 EUR per software solution provided, assuming that 7-10 software solutions are provided annually.

To summarize, we consider:

Infrastructure Operational Costs

- Infrastructure Maintenance: €100,000/year
- Software Tools: €50,000/year

Human Resources

- Salaries: €500,000/year (for 10 full-time staff)
- Contractors and Consultants: €100,000/year

Event Management

- Conference Costs: €150,000/year
- Marketing and Outreach: €50,000/year

Legal and Compliance

- Legal Fees: €50,000/year
- Insurance: €20,000/year

Total Annual Costs: €1,020,000

Regarding revenue streams, the following assumptions are made: We assume that 500,000 EUR may arise from donations and sponsorships of the developed solutions. If we assume 10 software solutions per year, then this corresponds to 50,000 EUR donation per solution. The distribution of the donations is supposed to be split 40%-60% between individuals and corporates. Another revenue component is the grants

and subsidies for the TrustChain OSSF. Different teams and the steering group from the TrustChain community will apply for funding through national/EU calls or Open Calls of different foundations for new project proposals in related topics, employing the brand name of the TrustChain foundation. A modest annual amount of 150,000 EUR is considered to come from government grants and another 100,000 EUR from foundations. Another revenue component is consulting and training services, providing annually 100,000 EUR and 70,000 EUR respectively. Given the popular and scarce skills of the TrustChain community on decentralized technologies, these amounts for consulting/training service fees may have been underestimated. The last source of revenue is considered to be merchandise sales and content licensing, providing 30,000 EUR and 20,000 EUR annually.

To summarize, the different revenue streams considered are:

Donations and Sponsorships

- Individual Donations: €200,000/year
- Corporate Sponsorships: €300,000/year

Grants and Subsidies

- Government Grants: €150,000/year
- Foundation Grants: €100,000/year

Service Fees

- Consulting Services: €100,000/year
- Training Programs: €70,000/year

Merchandising and Licensing

- Merchandise Sales: €30,000/year
- Content Licensing: €20,000/year

Total Annual Revenue: €970,000

Note that in order to achieve financial stability, we will pursue diversified revenue streams, thus actively maintaining multiple revenue sources. Another important aspect for financial stability is the community involvement in fund raising. Engaging the community in fundraising and leveraging volunteer contributions is needed to reduce costs. Moreover, we will pursue strategic partnerships, i.e., forming alliances with corporations, educational institutions, and other non-profits to enhance resources and outreach.

6.2.4.1 Numerical Analysis

To exemplify our analysis, we calculate the revenues and costs per year as follows:

Year 1:

- Total Costs: €1,020,000
- Total Revenue: €970,000
- Net Result: - €50,000 (Initial investment or reserve funds required)

Year 2 (with 10% growth in donations and sponsorships, 5% in other streams):

- Total Costs: €1,071,000
- Total Revenue: €1,043,500
- Net Result: - €27,500 (Reduced deficit)

Year 3 (continued growth):

- Total Costs: €1,124,550
- Total Revenue: €1,123,175
- Net Result: - €1,375 (Moving towards breakeven)

The detailed economic analysis for 10 years can be depicted in the figure below.

% increase in donations and sponsorships		10.00%	10.00%	10.00%	10.00%	10.00%	10.00%	10.00%	10.00%	10.00%	10.00%
% increase in other streams		5.00%	5.00%	5.00%	5.00%	5.00%	5.00%	5.00%	5.00%	5.00%	5.00%
Market Penetration of Solutions		100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Proforma Profit & Loss	**2026**	**2027**	**2028**	**2029**	**2030**	**2031**	**2032**	**2033**	**2034**	**2035**	**2036**
Year	0	1	2	3	4	5	6	7	8	9	10
Total Revenues		970,000.00	1,043,500.00	1,123,175.00	1,209,583.75	1,303,337.94	1,405,107.33	1,515,625.45	1,635,695.75	1,766,198.46	1,908,098.11
Individual donations		200,000	220,000	242,000	266,200	292,820	322,102	354,312	389,743	428,718	471,590
Corporate sponsorships		300,000	330,000	363,000	399,300	439,230	483,153	531,468	584,615	643,077	707,384
Government Grants		150,000	157,500	165,375	173,644	182,326	191,442	201,014	211,065	221,618	232,699
Foundation Grants		100,000	105,000	110,250	115,763	121,551	127,628	134,010	140,710	147,746	155,133
Consulting services		100,000	105,000	110,250	115,763	121,551	127,628	134,010	140,710	147,746	155,133
Training Programs		70,000	73,500	77,175	81,034	85,085	89,340	93,807	98,497	103,422	108,593
Merchandising Sales		30,000	31,500	33,075	34,729	36,465	38,288	40,203	42,213	44,324	46,540
Content licensing		20,000	21,000	22,050	23,153	24,310	25,526	26,802	28,142	29,549	31,027
GENERAL EXPENSES	0%	0	0	0	0	0	0	0	0	0	0
Total Expenses (€)		1,020,000	1,071,000	1,124,550	1,180,778	1,239,816	1,301,807	1,366,898	1,435,242	1,507,005	1,582,355
Infrastructure maintenance		100,000	105,000	110,250	115,763	121,551	127,628	134,010	140,710	147,746	155,133
Software tools		50,000	52,500	55,125	57,881	60,775	63,814	67,005	70,355	73,873	77,566
Salaries		500,000	525,000	551,250	578,813	607,753	638,141	670,048	703,550	738,728	775,664
Contractors and consultants		100,000	105,000	110,250	115,763	121,551	127,628	134,010	140,710	147,746	155,133
Conference Costs		150,000	157,500	165,375	173,644	182,326	191,442	201,014	211,065	221,618	232,699
Marketing costs		50,000	52,500	55,125	57,881	60,775	63,814	67,005	70,355	73,873	77,566
Legal fees		50,000	52,500	55,125	57,881	60,775	63,814	67,005	70,355	73,873	77,566
Insurance fees		20,000	21,000	22,050	23,153	24,310	25,526	26,802	28,142	29,549	31,027
Loan repayment (A1)		0	0	0	0	0	0	0	0	0	0
ore Interest, Taxes, Depreciation, Amortization		-50,000	-27,500	-1,375	28,806	63,522	103,300	148,728	200,453	259,194	325,743
Amortizations (€)		0	0	0	0	0	0	0	0	0	0
EBIT (Earnings before Interest)		-50,000	-27,500	-1,375	28,806	63,522	103,300	148,728	200,453	259,194	325,743
Interest expenses (€)		0	0	0	0	0	0	0	0	0	0
Net Benefit		**-50,000**	**-27,500**	**-1,375**	**28,806**	**63,522**	**103,300**	**148,728**	**200,453**	**259,194**	**325,743**
Discounted Net Cash Flow	0.00	-47619.05	-24943.31	-1187.78	23698.97	49770.81	77084.16	105698.14	135674.70	167078.71	199978.15
Loan Management											
Principal		0	0	0	0	0	0	0	0	0	0
Loan Interests		0	0	0	0	0	0	0	0	0	0
Principal Payment		0	0	0	0	0	0	0	0	0	0
Total Loan Payment		**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Net Cash Flow (Net Benefit + Amortisations)	0	-50,000	-27,500	-1,375	28,806	63,522	103,300	148,728	200,453	259,194	325,743
Net Present Value (NPV)	0	-50,000	-77,500	-78,875	-50,069	13,453	116,753	265,481	465,934	725,128	1,050,871
IRR (with amortisation)	**59.81%**										
Flow (Net Benefit without amortisation) (€)	0	-47619.05	-24943.31	-1187.78	23698.97	49770.81	77084.16	105698.14	135674.70	167078.71	199978.15
NPV (€)	0	-47,619	-72,562	-73,750	-50,051	-280	76,804	182,502	318,177	485,255	685,233
PROJECT (Unleveraged) IRR (%)	**52.20%**										
Payback Period	**6.00**										

FIGURE 4: ECONOMIC ANALYSIS FOR THE BM OF TRUSTCHAIN

We assumed an inflation rate of 5%. The Net Cash Flow and the Net Present Value (NPV) are depicted below. The resulting Internal Rate of Return (IRR) is 52.2%. The payback period is found to be 6 years.

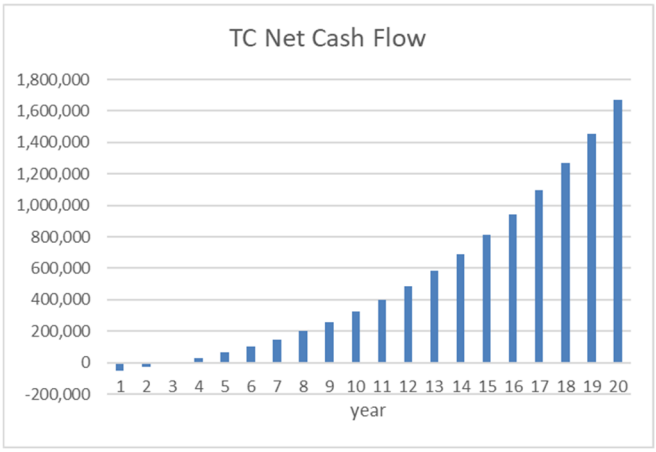


FIGURE 5: NET CASH FLOW FOR TRUSTCHAIN

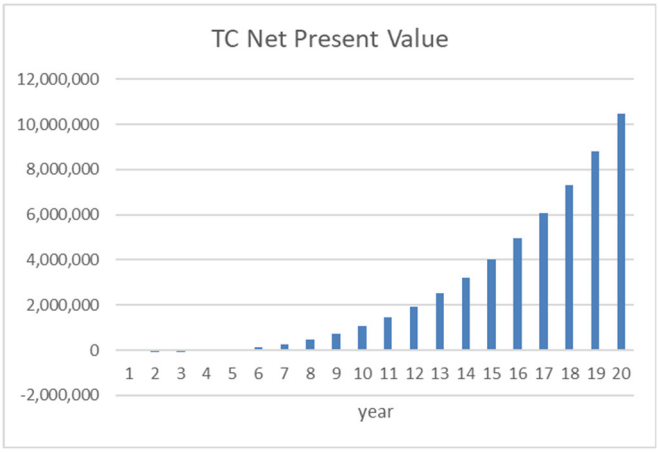


FIGURE 6: NET PRESENT VALUE FOR TRUSTCHAIN

6.2.4.2 Remarks

The OSSF aims to achieve financial sustainability through diversified revenue streams, community engagement, and strategic partnerships. Initial years might require additional funding to cover deficits, but with projected growth in donations, sponsorships, and service revenues, the foundation can move towards a stable financial footing. This model ensures that the OSSF can continue to support and promote open-source software effectively. Moreover, we will consider potential collaborations with other relevant blockchain and/or NGI projects, e.g., EBSI, Tezos, etc., and how these synergies are expected to strengthen the interoperability and adoption of TrustChain technology.

7 CONCLUSIONS

This deliverable presents the impact of the TrustChain project after the projects of the first three Open Calls have been launched. The multifold impact of TrustChain, namely scientific/ technical, societal, contribution to NGI, contribution to user needs, ecosystem development, and the contribution to the UN Sustainable Development Goals (SDGs) for each of the OC1, OC2, OC3 projects have been identified.

We also identified the economic impact of TrustChain in terms of Key Exploitable Results (KERs) and described the business model for each of them, based on a methodology for economic analysis that includes market analysis, business model convas, value network, cost-benefit analysis and SWOT. Also, towards the economic sustainability of the TrustChain ecosystem, we considered the business model of Open-Source Software Foundation (OSSF) for TrustChain after the end of the project. Based on a simple, yet realistic, economic analysis, we found that the TrustChain OSSF can be an economically sustainable endeavour.

8 APPENDIX

8.1 DETAILED ECONOMIC ANALYSIS METHODOLOGY

8.1.1 The value network

The value network (VN) concept originates from Michael Porter's well-known value chain concept (Porter, 1985), which is widely used in the business literature to describe the value producing activities of an organization. The concept has been expanded by Verna Allee to include non-linear interactions between one or more enterprises, its customers, suppliers and strategic partners (The art and practice of being a revolutionary., 1999). Furthermore, these exchanges can refer to raw material, upstream services and products, information as well as financial transactions.

Value network analysis provides ways to assess both the financial and non-financial values and aspects of a business. Most forms of analysis are done in a visual form, usually through a diagram or map of the important relationships and transactions that take place between different points of each network. These points generally represent people—individuals, groups, business units, and even individual businesses in an industry.

Value networks are made up of members and their interactions while producing a product or providing a service. These connections are extremely important in identifying strong companies as well as finding a company's potential risks. For example, if a network member has a large influence, the loss of that member could devastate the entire group. This is known as intrinsic value analysis because there is value, but it is hard to put on a price tag.

Participants of the value network analysis are evaluated both individually and, on the benefits, they bring to the network. The analysis is generally depicted visually, in the form of a diagram or map (see figure below). Value networks may be internal—factors within the business—or external—factors that are outside the business.

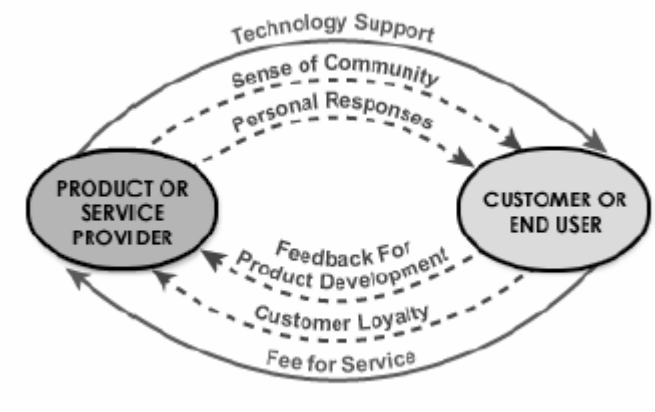


FIGURE 7: THE BASIC VALUE NETWORKS COMPONENTS.

8.1.2 Business Model Canvas

For each business role we can use the Business Model Canvas methodology in order to describe the baseline business model. The Business Model Canvas is developed by Alexander Osterwalder and Yves Pigneur in the context of the Business Model Framework (Osterwalder, et al., 2010) and is considered an established way for describing and visualising business models, by describing the rationale of how an organization creates, delivers and captures value.

The baseline business models will serve as the starting point for the TrustChain-enabled business models that will be proposed and assessed during the next phases of the TrustChain project.

The following table gives an overview of the business model canvas that will be used for describing candidate business models supported by the TrustChain ecosystem.

TABLE 33: THE TEMPLATE OF BUSINESS MODEL CANVAS

Key Partners The set of entities providing inputs (either physical or data) necessary for the service to be delivered. These partners can be upstream suppliers only, as well as peers that occasionally become downstream providers.	**Key Activities** The most critical tasks, i.e., those business processes whose details must be kept secret from rivals.	**Value Propositions** The set of products / services and their properties (e.g., low-cost, high quality) an entity offers to meet the needs of its customers.	**Customer Relationships** Customer relationships are the different types of interactions a company has with its customers. For example, a designer suit company will provide significant help for the customer, tailoring to their needs and working directly with	**Customer Segments** The exact market that the business entity is focusing on. It can be a niche market (e.g., eco-friendly home owners) or a very broad one (such as Low-Voltage households and businesses).

			them to create the suit they want.	
	Key Resources The most important inputs for the product/ service to be realized.		**Channels** The ways used for the value propositions to be delivered to customers. These can be privately owned or from third parties.	
Cost Structure The cost items that can be lump sum (such as the distribution network), repetitive but mostly fixed (for example personnel salaries), or repetitive and highly variable (like wholesale power bought).			**Revenue Streams** The sources of revenue for the entity that can be either lump sum (e.g., connection fee), repetitive but fixed (such as monthly "all you can eat" prices) and repetitive but variable (like commission from sales of power).	

8.1.3 Economic Sustainability Analysis

The main steps of economic and sustainability analysis that can be performed for product or a business model, including those of TrustChain, are as follows:

1. Define the Scope and Objectives:

- Clearly outline the purpose of the analysis. Identify the specific project, product, or business model to be evaluated for economic sustainability.
- Define the boundaries of the analysis (e.g., time frame, geographical scope, stakeholders).

2. Gather Relevant Data:

- Collect data related to costs, revenues, investments, and operational expenses; these include both historical data and projections.
- Consider external factors such as market trends, regulatory changes, and technological advancements.

3. Identify Key Economic Indicators:

- Select relevant economic indicators that align with the business model objectives. Common indicators include:
    - CAPEX (Capital Expenditure): Initial investment costs (e.g., infrastructure, equipment).
    - OPEX (Operational Expenditure): Recurring operational costs (e.g., maintenance, utilities).

- IRR (Internal Rate of Return): The discount rate at which the net present value (NPV) of cash flows becomes zero.
- RoI (Return on Investment): Ratio of net profit to the initial investment.
- Payback Time: Time required to recover the initial investment.

4. Cost and Revenue Modelling:

- Develop detailed cost models:
  - Break down costs into categories (e.g., labour, materials, overhead).
  - Estimate future costs based on historical data and market trends.
- Construct revenue models:
  - Identify revenue streams (e.g., product sales, subscriptions, licensing).
  - Estimate revenue based on pricing, sales volume, and market demand.

5. Discounted Cash Flow (DCF) Analysis:

- Calculate the net present value (NPV) of cash flows by discounting future cash inflows and outflows.
- Use the selected discount rate (often the cost of capital) to account for the time value of money.

6. Sensitivity Analysis:

- Assess the impact of variations in key assumptions (e.g., sales growth rate, cost escalation) on economic indicators.
- Conduct scenario analysis to understand different outcomes under varying conditions.

7. Risk Assessment:

- Identify risks that could affect economic sustainability (e.g., market volatility, regulatory changes, technological obsolescence).
- Quantify the potential impact of these risks on economic indicators.

8. SWOT Analysis:

- Assess the internal strengths and weaknesses of an organization, and identify the external opportunities and threats

9. Interpret Results and Decision Making:

- Evaluate the economic indicators against predefined thresholds or benchmarks.

- Consider trade-offs between short-term profitability and long-term sustainability.
- Make informed decisions based on the analysis results.

Next, we present some explanatory points about certain of the above steps of the economic sustainability analysis, and how the defined value network instances and Business Model Canvases of the involved actors are taken as an input for this analysis:

Define cost and revenue models. The cost model defines certain costs and cost drivers that affect the number of units that should be considered per cost item. It aims to capture the different Capital Expenditures (CAPEX) and Operation Expenditures (OPEX) of the TrustChain platform and of the stakeholders participating in TrustChain. CAPEX refers to long-term expenses for acquiring tangible assets such as equipment, buildings, etc., and intangible ones, like software or spectrum licenses. These costs can be recurring as well, e.g., when they refer to upgrading and maintaining those assets. On the other hand, OPEX refer to ongoing/recurring costs that a provider must spend to realise its offering. In contrast to capital expenditures, whose lifetime extends beyond the accounting period of the actual spend, the benefits derived from operational expenses are exhausted within the same accounting period/year and are not carried after that. Cost models can be useful to identify the most cost-effective architecture (e.g., functional split option) and estimating the unit cost of a service offering (e.g., when prices are cost-based). On the other hand, the revenue model aims to estimate the income of the actors involved in the service offerings, considering the prices of the different services offered by each actor and the expected demand per service which is extracted by relevant revenue drivers.

Feed figures to cost and revenue models. After defining the proposed cost and revenues models, certain inputs are required for assessing the sustainability of certain business models, i.e., for examining whether the revenue of a given actor exceeds its cost. The inputs required for the assessment are: (i) the unit cost for each cost item; (ii) the supply-side/cost drivers that affect the needed number of units per item; (iii) the price for each of the provisioned services and (iv) the demand-side drivers that determine the number of services provisioned. The relevant figures should be realistic (e.g., revenues related to actual tariffs) and in accordance to the costs expected in pilots. Note that, in certain cases, the price of each service is not given as an input and the business model's study focuses on extracting the prices that would render a business model of an actor sustainable/profitable.

Evaluate sustainability. This is accomplished for each of the business models by considering the Business Model Canvas of each actor in a given value network instance, and assessing its costs and benefits. Related sensitivity analysis should also be carried out, by re-assessing sustainability after varying certain influential parameters.

Regarding the SWOT (strengths, weaknesses, opportunities, and threats) analysis, it is a framework used in market analysis to evaluate a company's competitive position and to develop strategic planning. The main steps involved are as follows:

- Assesses internal and external factors, as well as current and future potential
- Designed to facilitate a realistic, fact-based, data-driven look at the strengths and weaknesses of an organization, initiatives, or within its industry
- Works best when diverse groups or voices within an organization are free to provide realistic data points rather than prescribed messaging
- Often synthesized to support a single objective or decision that a company is facing

The goal of a company performing SWOT analysis can be:

- Becoming more profitable
- Entering a new market
- Recovering from a setback
- Capturing market share
- Developing an R&D strategy

"Strengths" describe what an organization excels at and what separates it from the competition: a strong brand, loyal customer base, a strong balance sheet, unique technology, and so on.

"Weaknesses" stop an organization from performing at its optimum level. They are areas where the business needs to improve to remain competitive: a weak brand, higher-than-average turnover, high levels of debt, an inadequate supply chain, or lack of capital.

"Opportunities" refer to favourable external factors that could give an organization a competitive advantage. For example, if a country cuts tariffs, a car manufacturer can export its cars into a new market, increasing sales and market share.

"Threats" refer to factors that have the potential to harm an organization. For example, a drought is a threat to a wheat-producing company, as it may destroy or reduce the crop yield. Other common threats include things like rising costs for materials, increasing competition, tight labour supply, and so on.

8.2 DETAILED BUSINESS MODELS AND ECONOMIC ANALYSES OF THIRD-PARTY PROJECTS

The detailed business models, market and economic analyses of each project are presented in the following subsections.

8.2.1 DIDroom

Following a detailed business model and exploitation plan, including an in-depth economic (cost-benefit) analysis are described. This analysis should cover key financial aspects such as cost structure, revenue streams, market analysis, pricing strategy, and break-even analysis. It's crucial to demonstrate not only the feasibility of the business model but also its potential for scalability and sustainability within the context of the TrustChain project. Teams should also address how the economic landscape influences their business model and the potential risks and opportunities it presents. This section should reflect a thorough understanding of the economic environment in which the project's solution will operate, providing a realistic and comprehensive view of its financial and exploitation prospects.

8.2.1.1 Cost structure and early revenues - part time setup

Below a comparison of the current cost structure, with a forecast of the cost structure and early revenue expectations.

It is to be noted that currently the Forkbomb team, combined with the Dyne team, consists of about 15 members, half of them working full-time and the rest on a part-time based. It's worth mentioning that during the development of DIDroom within the TrustChain project, most of the team was completely focused to developing DIDroom, while for the foreseeable future DIDroom expect to be working also on its DPP platform (have just received an H2020 grant for that) as well as on cryptography and standardisation projects.

For these reasons, the project is able to guarantee at least operating the platform at minimum costs, for at least 24 months.

First development cost structure, the average monthly cost structure during the TrustChain project:

Back-end devs: 6000 EUR

Cryptography/OpenID flows devs: 5000 EUR

Front-end and mobile: 6000 EUR

UX/UI design: 2500 EUR

Product/Project/business management: 4500 EUR

Hosting and dev-ops: 1000 EUR

Total: 25000 EUR / month

Below is a list of various scenarios based on the amount of paying users (and therefore cash flow).

The scenarios represent projections with different levels of revenue and a corresponding average monthly cost structure based on the activity needed, along with the timeframe of the foreseeable scenario. The revenue and costs are monthly.

The estimate average revenue for paying user in the example is set to (bottom low) rate of 20 EUR per month per user (for limited SaaS usage) and the revenue for light customization and white-labeling to the (also bottom low) rate of 2000 EUR/month, and a rate of 6000 EUR/month for "larger" customization customers. All the figures are purposely kept very low in order to offer realistically reachable goals in the given timeframe.

DIDroom Business model	0 cost scenario	Scenario 1: M3-6	Scenario 2: M6-9	Scenario 3: M9-12	Sc.4: Break-even M12-18	Scenario 5: M18-24	Break-even w/full time
	This scenario describes the minimum cost structure if no revenue is generated, that would guarantee the hosting of the platform for around 24 months, after which some software components will start showing obsolescence and require a deeper a refactoring	500 free users, 25 Saas paying users, 0 customization/white-labeling customers, this scenario represents a possible scenario with minimal revenue	1000 free users, 50 paying users, 1 light customization/white-labeling customer: this scenario represent a possible scenario with minimal revenue	2000 free users, 100 paying users, 2 light customization/white-labeling customer: this scenario represents a possible scenario of low revenue	3000 free users, 150 paying users, light 3 customization/white-labeling customer: this scenario represents a possible scenario of low revenue, foreseeable around the month	3000 free users, 200 paying users, 3 light customization/white-labeling customer, 1 larger customization customer: this scenario represents a possible scenario of low revenue, foreseeable for the months	3000 free users, 200 paying users, 5 light customization/white-labeling customer, 3 larger customization customer
Costs							
Devs (maintenance)	-500	-1000	-1000	-1000	-1000	-4000	-7000
Devs (further dev)			-500	-500	-1000	-4000	-7000
Devs (customization)			-500	-1000	-2000	-4000	-8000
Hosting/DevOps	-250	-500	-500	-1000	-1000	-1000	-1000
Customer support		-250	-500	-1000	-1000	-1000	-1500
Inbound sales				-500	-1000	-2000	-3000
Marketing		-250	-500	-1000	-1000	-2000	-3000
Project Management/Admin				-500	-1000	-1000	-1500
Total cash burn rate	-750	-2000	-3500	-6500	-9000	-19000	-32000
Revenues							
SaaS (20 EUR user/m)		500	1000	2000	3000	4000	4000
Light customization (2000 EUR/m)			2000	4000	6000	6000	10000
Heacy customization (6000 EUR/m)						12000	18000
Total Revenues	0	500	3000	6000	9000	22000	32000
Results							
Operating result	-750	-1500	-500	-500	0	3000	0

FIGURE 8: DIDROOM COSTS AND REVENUES PLAN (LARGER VERSION IN ANNEX A)

Zero-revenue cost-structure: the minimum monthly costs to keep the software deployments running, with minimal software update (security only, minimal feature fix).

This scenario describes the minimum cost structure if no revenue is generated, that would guarantee the hosting of the platform for around 24 months, after which some software components will start showing obsolescence and require a deeper a refactoring

Result: -750 EUR/month

Scenario 1) 500 free users, 25 Saas paying users, 0 customization/white-labeling customers, 2 this scenario represents a possible scenario with minimal revenue, foreseeable for the first 3-6 months of activity.

Result: -1500 EUR/month

Scenario 2) 1000 free users, 50 paying users, 1 light customization/white-labeling customer: this scenario represent a possible scenario with minimal revenue, foreseeable for the months 6-9 of activity.

Result: -500 EUR/month

Scenario 3) 2000 free users, 100 paying users, 2 light customization/white-labeling customer: this scenario represents a possible scenario of low revenue, foreseeable for the first 9-12 of activity.

Result: -500 EUR/month

Scenario 4) (Break-even) 3000 free users, 150 paying users, light 3 customization/white-labeling customer: this scenario represents a possible scenario of low revenue, foreseeable around the months 12-18 of activity.

Result: 0 EUR/month

Scenario 5) (minimum profitability with current part time setup) 3000 free users, 200 paying users, 3 light customization/white-labeling customer, 1 larger customization customer: this scenario represents a possible scenario of low revenue, foreseeable for the months 12-18 of activity.

Result: 3000 EUR/month

8.2.1.2 Break-even point and profitability - full time setup

In the scenario of dedicating the whole team to the development and sales of DIDroom, at the current cost and head-count, the project would need to cover a cash burn-rate of 25000 EUR for the development, hosting and support, plus a 7000 EUR in sales and marketing expenses (total 32000 EUR/Month).

Realistically, DIDroom could reach this scenario with a combination of 3000 free users, 200 paying users, 5 light customization/white-labeling customer, 3 larger customization customers.

8.2.1.3 Notes about paying users and customization customers

The estimated of revenue per paying user, set at 20 EUR/user/month is represents the expectation of the average of the SaaS service the project plans to offer. The "paying user" in this case is intended as an organisation paying for a service, which is slightly above the free offer DIDroom plans to introduce.

The "light" and "larger" customization model are largely indicative and represents contracts on-going for 3-6 months. The "light" is meant to contain:

- use case study
- custom integration into 3rd party services
- support with deployment
- admin user training

The "larger" customization model contains all of the above plus:

- Support in whitelabeling
- Integration in multiple 3rd party services and databases
- Minimal feature development

The project chose to keep out of the equation larger contracts that contain more complex tasks such as ad-hoc development and integration in legacy or proprietary software, activities that the project has performed for a long time already, but are difficult to estimate.

8.2.1.4 Market Analysis

Competitive Analysis

TABLE 34: COMPETITOR ANALYSIS

Name	Description	Open source	Business	Notes
Google Wallet	Payment only	no	free	Currently payment only
Apple Wallet	Payments, US identity (mDOC)	no	free, paid support	Strong in US

Italian wallet	Italian open source wallet infrastructure	yes	no	collaboration with IPZS, EUDI–ARF compatible
IPZS wallet	Italian "Zecca" open source wallet infrastructure	Mixes source	no	EUDI–ARF compatible
MyGovID (Australia)	Australian govt. wallet	no	SaaS	Multiple services, focusing on online identification
GoodID	Hungarian ID wallet	no	SaaS	Focusing on e-signature, KYC, onboarding
Digidentity	Dutch identity wallet	no	SaaS	Focusing on KYC
Yoti	Commercial, multiple verticals	no	SaaS	KYC, Identity, signature, biometrics
Gataca	Commercial, focus on KYC	no	SaaS	KYC, Signature, Authentication
Walt.id	Modular, Identity and blockchain	yes	Paid Support, Saas	Multiple uses cases
https://authlete.com/	Focusing on Identity in Japan, US	no	SaaS	Identification, supports OpenID4VCI

Spruce ID	Modular, Identity and blockchain	yes	Paid support	Multiple use cases
https://talao.io/	Identity, support OpenID4VCI, blockchain, EBSI	yes	SaaS, paid support	based on Spruce ID

Current market situation: multiple actors, both public and commercial, offer identity wallets, some focusing on one (or few) use cases, some on multiple. The vast majority are closed source, offering SaaS and limited customization capabilities. The project found limited interoperability in most cases.

Stakeholders:

- State actors: each UE country bound to offer wallet from 2026
- Business actors: offering interoperable services for authentication, KYC, retails
- Educational: universities to offer UE (and US) interoperable Diploma credentials
- NGO/Communities: communities to offer applications required interoperable identities and credentials
- Finance/Blockchain: use wallets for KYC and signature

8.2.1.5 Opportunities and obstacles

The project tries to elaborate its market approach focusing on opportunities and obstacles.

8.2.1.5.1 DIDroom as an extensible platform

DIDroom is not a user-case type of application it is born as a platform to:

- Implement simple use cases, using the templating + no-code approach. At this point the features allowing that should be perceivable by the architecture and the GUI of the dashboard.

- as a base to implement larger use cases, that require complex integration with 3rd party software (via API or databases): the modular architecture is targeted to that
- as toolkit to use à la carte in order to perform selected features, integrated with larger 3rd party applications

The team of the project has already projects (with customers and grants) running within the latter 2 cases. The marketing approach aim to focus on the first case, in order to build a user-base that will fuel a funnel for the latter 2 cases.

The project is therefore specifically targeting:

- Organizations who need a set of features related to identity, implemented in their existing infrastructure
- Software developers (start-ups or established) who want to integrate the technology in their next products
- Organizations, with minimal or no software infrastructure, looking to offer identity related services to employees or to customers

8.2.1.5.2 Unique selling points and main opportunities

DIDroom identifies its unique selling points, and therefore largest opportunities in offering:

- Microservice-based integration
- Multitenant, open-source, identity back-end, sold SaaS
- Re-usable UI components, to be integrated in existing solutions, leading to white-labelling of mobile and web-apps

8.2.1.5.3 Software ecosystem and relicensing

DIDroom as a solution is the result of the development of a large software ecosystem, centered on the unique cryptographic virtual machine “Zenroom”. The ecosystem of components has been in development since 2017 by Dyne.org and Forkbomb BV, and only last year the team began implementing solutions, with DIDroom being the 2nd one, the first one is the DPP solution Interfacer.

DIDroom has therefore a limited amount of 3rd party dependencies, typically in secondary roles.

The whole ecosystem is licensed as AGP 3.0, implying that 3rd parties willing to use the technology in closed-source products, will require a commercial relicensing from them.

8.2.1.5.4 Obstacles

A list of specific obstacles to the success of the DIDroom, based on the current market and technology scenarios.

- Uncertainty of acceptance of the standards: based on face-to-face conversations with EC representatives, it is understood that the EC itself perceives a risk in the acceptance of the eIDAS 2.0 legal framework and the EUDI-ARF specification by the market and the member states.
    - Mitigation: While the focus is on EUDI-ARF, DIDroom also supports other specifications. There is also collaboration with actors in the US to establish a position in that market.
- Inherent complexity in the product and the architecture, makes the value proposition difficult to communication.
    - Mitigation: progressively implement multiple simple use cases, based on the user feedback and activities. Use cases are typically implemented in the DIDroom Dashboard in the form of "templates", ideally by the users. This approach allows access to user-generated data and business logic.
- Market competition: growing competition makes standing out difficult
    - Mitigation: enter and specialize into niches, grow the existing partnerships with standard maintainers and member states developers to gain technical and market knowledge along with visibility.
- Interoperability: at the current stage, no definitive interoperability protocol has been identified to work on top of EUDI-ARF, with OpenID4VCI being the most widely used.
    - Mitigation: There is limited influence possible on this issue. The focus is on growing partnerships and investing time in testing and implementing interoperability with third parties.

8.2.1.6 Pricing strategies and revenue streams

Business model: freemium, partial/full on-premises deployment, white-labelling, relicensing and support

DIDroom is born as a multitenant white-label platform, this allows to offer multiple subscriptions options.

Free plan

Anyone can create an account (and an Organisation attached to it). The Free plan allows to (figure TBC and will change over time):

- Create one Organisation and appoint a user as credential issuer manager and verifier
- Invite 10 users to join the organisation as holder
- Create 1-3 credential flows: the credentials issued can be configured from a template, the issuers run on a non-configurable, external microservice, managed in-house.
- Create 1-3 verification flows (relying parties, according to the EUDI-ARF jargon): same as with the issuers
- Issue 20 credentials per month
- Verify 30 credentials per month

The Free plan is meant to allow smaller organisations to use the solution for free and larger organisations to test it and get started. The free plan offers creation and verification of credentials only using predefined microservices, hosted by Forkbomb, meaning that the keys of the issuers and verifiers are generated and kept on the platform.

Paid plans

- Invite unlimited users and credential issuing and verification
- Appoint multiple users as credential issuer manager and verifier
- Possibility to configure and use external issuer and verification microservices (based on Zenswarm or not). The project offers support with setup, monitoring and maintenance (possibly individually) of the external microservices for issuing and verifying
- Web-hooks and APIs for interoperability (with web-services, DBs and blockchain), with logging
- Possibility to relicense and white-label the mobile app (AGPL3)

Target price:

- 5-50 EUR/user/month, depending on:
    - Issuer/verifier microservices (maintained or on-premises, deployed manually or automatically)
    - Usage of the W3C-DID service
    - API and web-hooks usage and logging
    - White label wallet

On-premises deployment

- Support with setup, monitoring and maintenance (possibly individually) of the back-end and admin dashboard and the microservices for issuing/verification
- Support with setup, monitoring and maintenance of the W3C-DID method
- Support with API and web-hooks for interoperability
- Support with customization (back-end, admin dashboard, mobile apps)
- Software relicensing (the whole platform is AGPL3)
- Target price: from 50K EUR year

Custom development, integration with 3rd party platforms

DIDroom is built on top of Starters (https://github.com/dyne/starters) as a modular, easy to extend and to integrate platform. Starters includes advanced features such as:

- Automatic push of updates to children project
- End-to-end testing with Playwright
- Webhooks and REST APIs
- Webauthn authentication
- Transaction email with Sendgrid

This allows the solution to be heavily customised and plugged into existing solutions. The aim is to offer custom development as an extra service, to increase functionalities and provide interoperability and integration with third-party services.

Microservice as a service

Due to the high interoperability of the platform, consideration is being given to offering microservices such as credential issuing and verification as standalone services. Which implies

- it requires integration of 3rd party solutions
- it doesn't require the whole solution to be used
- can be charged on a per hour base

This is in fact a subset of the previous revenue stream, the project is currently exploring marketplaces such as AWS (the project recently receive free credit from AWS) and DAPPnode to publish its microservices.

8.2.1.7 Value Network

TABLE 35: VALUE NETWORK OF DIDROOM

Entities in the Value Network	Role	Value Contribution	People/Organizations Involved
DIDroom Platform	Central entity providing decentralized identity and SSI wallet platform.	Modular, open-source solution with advanced cryptographic and blockchain functionalities, complying with standards.	-

Users	Individuals and organizations using DIDroom for identity management.	Secure and interoperable identity management, customizable solutions.	Avant Garden: Testing with 1900 users in schools, aiding pilot advancement and solution adoption.
Developers/Contributors	Individuals contributing to DIDroom's open-source development.	Continuous contribution of code, expertise, and innovation, fostering platform improvement.	Dyne Community: Support in adoption with a large network in social innovation and privacy data sovereignty.
Partnerships	Collaborating organizations for interoperability and integration.	Mutual exchange of resources, expanding DIDroom's reach through collaboration.	Avant Garden, IPZS, AGID, Dyne Community.
Blockchain Networks	Supporting blockchain networks for DIDroom's functionalities.	Enable secure transactions, multi-signatures, and interoperability with blockchain networks.	-

Regulatory Authorities	Entities overseeing compliance with identity and blockchain regulations.	Ensuring compliance, fostering trust and credibility for DIDroom.	IPZS, AGID.
Cloud Service Providers	Hosting and distributing DIDroom microservices.	Facilitating easy access to DIDroom services, leveraging cloud infrastructure for scalability.	-
Educational Institutions	Using DIDroom for issuing interoperable diploma credentials.	Providing standardized and secure platforms for issuing and verifying academic credentials.	Avant Garden: Testing with 1900 users in schools.
NGOs/Communities	Leveraging DIDroom for applications requiring interoperable identities.	Empowering communities with secure and interoperable digital identities.	Dyne Community: Support in adoption with a large network.

8.2.1.8 Cost Benefit analysis

Bases on the received feedback, the project tries to elaborate and quantify the costs for customers/developers willing to implement a similar solution and the benefits of using the solution instead.

TABLE 36: CBA COST BENEFIT ANALYSIS OF DIDROOM

Costs	Description	Quantification
Development and Maintenance	Personnel and technology costs for continuous development and platform upkeep.	The cost of Implementing a solution with a comparable minimum set of features ranges in 100s of thousands of EUR
Regulatory Compliance	Legal and compliance expenses to ensure adherence to identity with focus on EUDI-ARF and W3C-DID	Compliance and interoperability require high specialization and continuous efforts. Consultancy would cost in the 10s of thousands of EUR
Community Engagement	Resources for managing open-source community interactions and contributions.	In the scenario of implementing an open-source solution, growing and maintaining a community represents a challenge
Infrastructure and Hosting	Cloud service costs for hosting microservices on platforms like Hetzner	The microservice based architecture coupled with the multi-tenant dashboard, allows users to drastically minimize hosting maintenance costs
Custom Development and Support	Personnel and ongoing support costs for custom development services.	Zenroom's no-code approach allows non-programmers to implement simple functionalities, saving development costs.

Monitoring and Maintenance	Resources for monitoring performance and ensuring ongoing platform maintenance.	The dashboard monitoring capabilities (offered by Pocketbase and the internally developed components) allow customers to reduce cost on monitoring and maintenance
Benefits	**Description**	**Quantification**
Customers offering new services	Customers can implement use cases offering paid services..	Customers can create use case to offer paid services (e.g. event tickets) as well as offering internal services (e.g. credential based access control)
Community Contributions	Continuous improvement and innovation from the open-source community.	Contributions to the sourcecode by the community as well as to use cases by the users (via “templates” hosted on the dashboard) grows the features of the solution
Partnership development	Increased reach and potential revenue through strategic partnerships and ecosystem growth.	High Interoperability of the solution allows to create partnerships among the users
Security and cryptography impact	Market presence and social impact by providing secure digital identity solutions.	Strong cryptography security help customers establishing a branding around those values

TABLE 37: VALUE PROPOSITIONS FOR STAKEHOLDERS

Value Proposition	Description	People/Organizations Involved
For Users	Secure and interoperable identity management. Customizable solutions based on individual or organizational needs.	End Users
For Developers and Contributors	Opportunities for skill development and recognition within the open-source community.	Dyne Community.
For Partnerships	Mutual exchange of resources, expanding the reach of DIDroom through collaboration.	Avant Garden, IPZS, AGID, Dyne Community.
For Educational Institutions and NGOs/Communities	Empowering with secure and interoperable digital identities.	Avant Garden, Dyne Community.

8.2.2 Creator Credentials

The Creator Credentials project is offering a user-centric digital identity management framework that is specifically designed to serve the unique needs of the cultural and creative industries. By addressing the unique needs of these industries for a secure and trustworthy media environment, it is presenting substantial business potential for an entire ecosystem of media organisations.

8.2.2.1 Entities and Their Roles

Before describing the business model and exploitation plan in detail, it is necessary to distinguish between four (logical) entities, their roles, and relationships towards each other. This Creator Credentials ecosystem involves CREATORS, ISSUERS, HOSTS, and SERVICES. Each entity plays a critical role in the framework.

CREATORS and Rightsholders (CREATORS)

Individuals or entities such as rightsholders, including journalists, artists, musicians, who seek to verify their digital identity and rights through Verifiable Credentials (VCs).

ISSUER Organisations (ISSUERS)

Entities that issue VCs to CREATORS. These can be media companies, cultural institutions, or any organisation that holds the authority to verify and acknowledge the identity and rights of CREATORS.

HOST Organisations (HOSTS)

Entities responsible for hosting the Creator Credentials application, thereby providing the technological infrastructure and services needed by ISSUER organisations to issue VCs.

Service Organisations (SERVICES)

A specific entity, such as Liccium B.V. in the example, provides IT services to HOST organisations, ensuring the underlying infrastructure runs smoothly and efficiently.

Example

The CREATOR could be a news journalist working for "DER SPIEGEL".

The ISSUER could be "SPIEGEL-Verlag Rudolf Augstein GmbH & Co. KG".

The HOST could be "dpa – Deutsche Presse Agentur".

Liccium B.V. could be the SERVICE offering IT services to the HOST.

8.2.2.2 Relationships

1. CREATOR <--> ISSUER (A)

A direct relationship where CREATORS connect with ISSUERS to request and receive VCs, affirming their digital identity and rights.

2. ISSUER <--> HOST (B)

ISSUERS rely on HOSTS for the infrastructure to issue VCs. In some scenarios, the ISSUER and HOST can be the same entity, streamlining the process.

3. HOST <--> SERVICE (C)

HOSTS depend on service organisations for IT support and services, ensuring the infrastructure is secure, reliable, and capable of supporting the system's demands.

The following sections distinguish between HOSTS that provide the Creator Credentials services, and ISSUERS that act as the VC ISSUERS and trust service providers for CREATORS and rightsholders. However, there are scenarios where these roles merge, one organisation fulfils both functions, being HOST and ISSUER.

8.2.2.3 (A) CREATOR <--> ISSUER

8.2.2.3.1 Relationship

This foundational relationship forms between the CREATOR, acting as the customer, and the ISSUER, who provides the trust services. This dynamic is essential for the operation and integrity of the system.

8.2.2.3.2 Business Model

ISSUERS have the autonomy to define their business model for the services they offer. This could involve charging CREATORS either a one-time fee or a subscription fee. The pricing structure might vary based on factors such as user count, the volume of issued VCs, or access to additional features.

8.2.2.3.3 Revenues of ISSUER

ISSUERS can generate revenue through one or more of the following streams:

8.2.2.3.3.1 One-Time Fee

Initial Fee

Charged to confirm the identity of the CREATORS and to process the connection request.

Issuance Fee

Charged to issue a VC to the CREATORS.

8.2.2.3.3.2 Subscription Fee

Recurring fee, charged for maintaining the validity of the VC and issuing new VCs upon expiration.

8.2.2.3.4 Costs of ISSUER

8.2.2.3.4.1 Subscription Fee

Payments to HOSTS for services such as application hosting or providing support to the ISSUER.

8.2.2.3.4.2 Support and Maintenance

Involves expenses for customer support teams, training, helpdesk services

8.2.2.3.4.3 Marketing and Business Development

Includes costs for advertising, promotional activities, webinars, and outreach initiatives aimed at attracting and retaining CREATORS.

8.2.2.3.4.4 Verification

Costs associated with the proper verification of CREATOR identities and the KYC process are critical for maintaining the integrity of the system.

8.2.2.3.4.5 Administrative

Encompasses payment processing, invoicing, and day-to-day operational expenses like salaries, utilities, office space, and other overheads.

8.2.2.4 (B) ISSUER <--> HOST

8.2.2.4.1 Relationship

This section addresses the business dynamics between the ISSUERS and the HOSTS, especially relevant in scenarios where an ISSUER opts not to self-host the application but instead leverages the services provided by a HOST.

8.2.2.4.2 Business model

A HOST offers a holistic solution that alleviates the burden on media organisations of managing their own IT infrastructure. The hosted service proposition includes not just core hosting but also enhanced features like improved security, reliability, scalability, effective key management, and streamlined maintenance and updates processes.

Additionally, HOSTS can tailor its services to meet the specific needs of ISSUERS, providing premium features, support packages, and customization options for Verifiable Credentials (VCs). These services are designed to accommodate organisations seeking advanced functionalities, superior security levels, or adherence to particular regulations and standards, such as QCerts for eSeal.

8.2.2.4.3 Revenues of HOST

8.2.2.4.3.1 Subscription Fee

A recurring fee is instituted by the HOST for availing its services to the ISSUER, encapsulating the comprehensive suite of solutions offered.

8.2.2.4.3.2 Costs of HOST

The operational and developmental expenditures for the HOST are multifaceted:

8.2.2.4.3.3 Development

Costs incurred during the initial setup, development phase, addressing feature requests, and ensuring regular updates to the open-source dockerized application are significant. This category also includes continuous integration, testing, and maintaining quality assurance standards.

8.2.2.4.3.4 Hosting and Infrastructure

The financial obligations associated with hosting the service encompass server expenses, domain registration costs, data storage requirements, backup solutions, and implementing redundancy measures for enhanced service reliability.

8.2.2.4.3.5 Security and Compliance

The HOST undertakes regular audits, vulnerability assessments, and compliance checks to uphold stringent security standards. Investments in cutting-edge cybersecurity measures and tools are pivotal, along with efforts to meet regulatory requirements and secure necessary certifications.

8.2.2.4.3.6 Support and Maintenance

Expenditures related to establishing a competent customer support team, providing training, and running helpdesk services are essential. Regular software maintenance, issuing patches, and addressing bug fixes also constitute a significant portion of the operational costs.

8.2.2.4.3.7 Marketing and Business Development

Marketing initiatives, promotional activities, hosting webinars, and other outreach efforts require a dedicated budget to effectively communicate the value proposition to potential ISSUERS.

8.2.2.4.3.8 Partnerships and Licensing

Engaging in new partnerships, managing legal documentation, negotiating licensing agreements, and setting up revenue sharing models entail notable expenses.

8.2.2.4.3.9 Administrative

The day-to-day running of the HOST's operations involves overhead costs, including staff salaries, utility bills, office space rentals (if applicable), among other administrative expenditures.

8.2.2.5 (C) HOST <--> SERVICE

8.2.2.5.1 Relationship

This segment addresses the business relationship between HOSTS and SERVICES. Within this framework, any trusted media organisation has the potential to become a HOST by adopting the dockerised version of the Creator Credentials application.

8.2.2.5.2 Business Model

To sustain the Creator Credentials service, a strategy involving the provision of value-added services and customisation options is employed, all the while ensuring the core dockerised application remains open-source and freely available. This strategy guarantees on-premises, self-custodial use by HOSTS, with comprehensive support in the form of code, tutorials, and documentation accessible via GitHub and GitBook.

If needed, Liccium B.V. can provide value-added services and customisation options to trusted media organisations utilising the open-source, dockerised application to establish their own Creator Credentials service. This could encompass offering support, consultation, and implementation services to help media organisations seamlessly integrate the app into their existing workflows and systems, alongside customisation options such as branding and interface design.

The Business Model Canvas | CreatorCredentials.com | Posth Werk BV | 2024-01-21, v0.1

Key Partners

- **Individual creators and rightsholders** from all media sectors. incl. photographers, authors, publishers, distributors, and other stakeholders
- **Trusted entities** in the cultural and creative sectors that will act as credentials issuers
- **Technology partners** for infrastructure, security, and platform development
- Academic institutions for research and development
- Policy makers to comply with upcoming regulatory requirements

Key Activities

- Developing and maintaining the Creator Credentials software application
- Engaging with stakeholders for feedback and iterative improvements
- Promoting adoption through webinars, training sessions, and workshops
- Building and managing the legal framework for digital identity management

Key Resources

- The Creator Credentials app and associated legal framework
- The Technology stack for digital identity management
- Community of creators and users for feedback and validation

Value Proposition

- Providing a secure, verifiable **digital identity management framework**
- **Enhancing trust and transparency** in the origin and ownership of digital content
- Offering **verifiable attribution** in online media environments
- Streamlining the process for creators to **receive verifiable creator credentials**
- Supporting media organisations to **become trust services** for creators and rights holders

Customer Relationship

- Ongoing engagement with early users for feedback and improvements
- Providing **training and resources** to ensure stakeholders can effectively use the app
- **Support channels** for trouble shooting and user support
- Regular updates and workshops to keep users informed on new features

Channels

- The Creator Credentials app and website for information and access
- Direct engagement through webinars, training, and workshops
- Online platforms and social media for updates and community building
- Customer support for hands-on assistance

Customer Segments

- Creators and rights holders in the cultural and creative industries
- Trusted entities in the cultural and creative sectors that will act as credentials issuers
- Content platforms and services that rely on verified creator identities
- End-users and consumers who value verified content

Cost Structure

- Development and maintenance of the software and legal framework
- Stakeholder engagement and community building activities
- Infrastructure costs for hosting the platform and related services
- Staff costs for development, marketing, and operational support

Revenue Streams

- Subscription fees for use of the Creator Credentials app by organizations
- Transaction fees for processing and verification of credentials
- Licensing fees for the use of the platform's technology by third parties
- Possible funding or grants for supporting the creative industries

TABLE 38: BUSINESS MODEL CANVAS OF CREATOR CREDENTIALS

8.2.2.5.3 Revenues of SERVICES

8.2.2.5.3.1 Value-Added Services and Customisation Options

Services aimed at ISSUERS requiring assistance in implementing and hosting their version of the Creator Credentials application include:

Consultation and Implementation

Expert consultation, support, and integration services for media organisations aiming to host the Creator Credentials app.

Customization Options

Tailored branding and user interface design services.

Premium Features or Support Packages

Solutions for advanced functionalities, security enhancements, and compliance with specific regulations.

8.2.2.5.4 Costs of SERVICES

The operational costs of SERVICES encompass:

Staffing Costs

SERVICES incur expenses in providing consultants, developers, and designers necessary to deliver the aforementioned value-added services and customisation options.

8.2.2.5.5 Pricing

It is too early to come up with a proper pricing strategy and break-even analysis for the Creator Credentials project. First, the use of Verifiable Credentials as a means to provide proper attribution to content declarations and claims to content, rights or other metadata has to be established in the cultural and creative communities.

Considering, e.g. the relationship between CREATOR and ISSUER, a subscription fee model is recommended that balances affordability for CREATORS with sustainable revenue for ISSUERS. Determining the appropriate price for an annual subscription requires a comprehensive understanding of various factors, including the cost of providing the service, the value it offers to users, and the target market's willingness to pay. Without specific details on these aspects, a precise figure is challenging to suggest. However, a general approach would be to calculate the annual cost of service provision (including development, maintenance, customer support, etc.), add a margin for profit, and then adjust based on market research.

For a service like Creator Credentials, which offers significant value in terms of security, efficiency, and convenience, a starting point could be in the range of 100 EUR to 500 EUR annually for individual CREATORS or small organisations. This range accounts for the reputation and trust that is provided by the ISSUER. It's crucial to conduct market research to validate these initial estimates, understand the potential customers' budget constraints, and adjust the pricing strategy accordingly.

The insights and considerations outlined previously are broadly applicable across all roles within the Creator Credentials ecosystem. It is important to recognize that one ISSUER may have a different business and pricing model than another ISSUER, with these models potentially varying by region or specific media sector.

In addition, the commercial relevance of trust services within an entity can vary significantly; some entities may offer these services within what is sometimes called a

"cost center." This approach is strategically pursued to increase the attractiveness of other existing services, drawing customers in by offering basic trust services at minimal or no cost to encourage acceptance of more comprehensive, revenue-generating offerings.

This diversity in operational models underscores the complexity of the economic landscape in which these entities operate, necessitating flexible and adaptive strategies to adapt to the varied needs and expectations of their respective markets.

8.2.2.6 Market Analysis

8.2.2.6.1 Market Need and Opportunity

The need for trusted attribution in all media sectors is clear. Content proliferation online has made it difficult to ascertain the originality and ownership of creative works. With the rise of digital media, there's a growing demand for services that can reliably link content to its CREATORS, ensuring trust, transparency, and proper compensation.

8.2.2.6.2 Competition

After early approaches in the music industry, such as the Creative Passport, and novel projects emerging from the necessity to differentiate human-authored from AI-generated works in publishing, These new ventures are leveraging digital certificates, blockchain technology, and centralised methodologies to provide robust solutions that affirm the authorship and origin of content, addressing the growing demand for authenticity and verification in the digital landscape.

8.2.2.6.2.1 Verify Media

https://www.verifymedia.com/

Verify Media is developing a platform to assist media companies in registering their content, enabling use cases such as granting usage rights to AI platforms. The platform aims to securely associate digital content and its metadata with the actual owners, thus preventing misuse and misattribution. It leverages smart contracts for content declarations on the Polygon blockchain. Instead of integrating Polygon ID, Verify Media's method for creator identity is based on a basic root identity, represented by a signing key pair.

8.2.2.6.2.2 Polygon ID

https://polygonid.com/

Polygon ID serves as a self-sovereign identity framework developed atop the Polygon blockchain. It employs zero-knowledge proofs, enabling users to authenticate their identities while maintaining the confidentiality of personal data, thereby bolstering privacy. Operating as a decentralized identity system, Polygon ID presents potential use across a diverse range of applications, including content declaration processes.

8.2.2.6.2.3 FileProtected

https://www.fileprotected.com/

FileProtected is a digital rights management platform that focuses on providing creators with tools to protect, manage, and monetize their intellectual property (IP).

In the realm of creator identification, FileProtected is presumed to offer features enabling creators to not only affirm and validate their identity but also to integrate such identification details directly into their content. This process involves a combination of centralised copyright registration methods along with blockchain technology for added security and transparency.

8.2.2.6.2.4 C2PA

https://c2pa.org

The Coalition for Content Provenance and Authenticity (C2PA) is a consortium of members from the Content Authenticity Initiative (CAI) and Project Origin. C2PA is developing technical specifications for establishing content provenance and authenticity. They are refining a proposed international technical standard that uses capture devices within a trusted execution environment and certified software applications to certify the source and provenance of media content.

Content creators and publishers can use apps that support this standard to create and embed cryptographically verifiable metadata containing information about the asset's creation and edit actions, copyright, licences, capture device details, and software used. The assertions are designed to be hashed and gathered into a verifiable claim that is digitally signed, ensuring the integrity of the claim.

However, this method does not yet allow for the validation of the integrity of the digital media asset in cases where the metadata has been removed or tampered with, which is a common issue in online content sharing and social media platforms that strip away embedded metadata for security and business reasons.

The C2PA initiative in investigating the use of verifiable credentials.

8.2.2.7 Exploitation plan (business)

Let's apply the above to Liccium B.V. As mentioned before, Liccium B.V. will be serving simultaneously as an ISSUER, HOST, and SERVICE provider. This means:

1. Liccium B.V. will issue VCs to CREATORS;

2. Liccium B.V. will be the HOST of the Creator Credentials services running on creatorcredentials.app and encourage media organisations to become ISSUERS within this service environment;

3. To support third parties in becoming HOSTS, Liccium B.V. can offer implementation services as a SERVICE.

8.2.2.7.1 Exploitation Plan

The exploitation strategy for introducing and embedding Creator Credentials in the creative industries unfolds in three strategic steps.

Communication and Education

The initial phase involves communication campaigns to introduce Creator Credentials to stakeholders across global creative industries. This step includes presentations and workshops online and in person, using materials aimed at demonstrating the value and functionality of the product.

Initially, Liccium B.V. will play a crucial role in crafting and disseminating educational content, ensuring clarity and addressing potential concerns to facilitate understanding and eventual adoption.

This stage will be considered as an investment stage.

Media Organizations as Issuers

In the second phase, Liccium B.V. invites media organisations to issue Creator Credentials, positioning itself as a HOST that offers an implemented solution for these ISSUERS. This entails providing the platform that organisations can leverage to issue verifiable credentials, thereby enhancing trust and authenticity in the digital space.

Liccium's function is to ensure seamless integration and support for these media organisations, facilitating their transition into trusted issuers within the ecosystem.

For Liccium it will be possible to create revenues by onboarding the media organisations and charging subscription fees.

Empowering Third Parties as Hosts

The third step envisions a broader adoption where third parties assume the role of hosting the infrastructure necessary for the issuance and management of Creator Credentials.

Liccium's role evolves into providing support and expertise to media organisations that opt to host their own infrastructure or wish to adapt to specific media markets. This includes technical support, guidance on best practices, and ensuring interoperability with the broader ecosystem of Creator Credentials.

8.2.2.8 Influences of the Economic Landscape

The economic environment encompasses various external factors such as market trends, regulatory development, technological advancements, and the competitive landscape, all of which can significantly impact the project's financial viability and exploitation opportunities.

Market Trends

Emerging trends in digital media consumption and content creation can affect demand for the Creator Credentials app. Topics like fake news, disinformation or the problem of abundance of dubious digital content online due to generative AI drive the need for reliable attribution mechanisms, presenting significant opportunities for adoption and revenue generation.

Regulatory Changes

The legal environment surrounding copyright and AI play a critical role. The DSM Directive on Copyright as well as the novel AI Act, both demanding greater transparency and the respect for creators' rights certainly enhance the app's value proposition.

Technological Advancements

The pace of technological innovation, particularly in digital identity management and verification technologies, support the relevance and adoption of solutions in the creative and cultural industries.

8.2.2.9 Potential Risks

Adoption Hurdles

The core concepts of SSI, such as DIDs or Verifiable Credentials, are hard to understand for normal users. Resistance from users unfamiliar with or sceptical of VCs could slow adoption rates, affecting revenue projections.

Dependency on Third Parties

The business model may rely on partnerships with media organisations, issuers, and host entities. Failures or delays in forming these partnerships pose risks to the adoption timeline and potential financial outcomes.

8.2.2.10 Opportunities

Niche Market Penetration

By focusing on underserved segments within the media industry that have yet to adopt verifiable credentials, the app can secure early adopters as a loyal user base and establish itself as a market leader.

Strategic Partnerships

Forming strategic alliances with key industry players can accelerate market penetration, enhance the app's credibility, and provide financial stability through collaborative ventures.

Innovation Leadership

Staying ahead of technological trends and regulatory changes can position the app as an innovative leader, attracting investment and fostering trust among users.

8.2.3 MUSAP

It is believed that the primary catalyst for the expansion of identity markets stems from eIDAS and the positive outcomes derived from its use cases. As eIDAS2 advances, it presents a paradigm shift addressing the key challenges that hindered the initial eIDAS regulation's widespread adoption.

Now especially, eIDAS assurance levels can be referred to NIST assurance levels thanks to the mapping exercise by transatlantic cooperation. Methics wrote about it in the blog: https://www.methics.fi/level-of-assurance-mapping-between-eidas-nist/ .

Especially, with eIDAS2 and Digital identity standards mapping, new successful use cases, the Asia and Middle East markets growth can be accelerated. However research by KuppingerCole market sizing indicates that many sectors such as financial, government, health care already see high use of digital identity, many other industries are showing interest. Though true potential lies in embracing identity solutions which simplifies interactions of users with system. This can be perceived as meaning that there isn't a single solution that works perfectly for every situation. Additionally, all keys shouldn't be concentrated in one basket. The perspective is that identity solutions must be flexible and extensible: flexible to provide adjustable levels of assurance (LoA) for specific use cases or flows, and extensible to address interoperability needs and security considerations.

Acceptance of the European digital Identity Wallet and eIDAS 2, hinges on its user-friendliness, security, and how it provides LoA for specific use case (e.g Type 1 and Type 2 of EDIW configs).

The feasibility of achieving widespread acceptance is closely tied to the system's ease of use and its seamless operation on a global scale. MUSAP aims at easing easy implementation of EDIW by allowing both configs (LoA High and LoA Substantial) in one device and similarly many end-user apps can use MUSAP to easily interface key security.

8.2.3.1 MUSAP specific business strategy & plan

TABLE 39: BUSINESS MODEL CANVAS OF MUSAP

		Designed for:	*Designed by:*	*Version:*	
Business Model Canvas		NGI TrustChain	Methics	Version D3	
Key Partners	**Key Activities**	**Value Propositions**	**Customer Relationship**	**Customer Segments**	

<table>
<tr>
<td rowspan="3">Digital identity software vendors:

- On-boarding
- Document signing
- eWallet
- SSI companies</td>
<td>- Produce articles andcompany visibility for potential customers/partners
- Implement service components for serviceintegration with the partners</td>
<td rowspan="3">- Provide multiple LoA identities in onedevice
- Enable “High” LoA

- Specialized formultiple SSCDs
-The project manages the documentation and certification responsibilities for theidentity product.</td>
<td>- Self-service tools
- Support community
- NGI community</td>
<td rowspan="3">- (Q)TSPs commercial
- (Q) TSPs public
- MNOs
- Government agencies
- Software vendors</td>
</tr>
<tr>
<td>Key Resources</td>
<td>Channels</td>
</tr>
<tr>
<td>- Identity specialists
- Sales + cost efficientintegration model
- Product & Project managers</td>
<td>- App vendor sales channel
- Public tenders
- Partner sales
- Direct sales</td>
</tr>
<tr>
<td colspan="3">Cost Structure</td>
<td colspan="2">Revenue Streams</td>
</tr>
<tr>
<td colspan="3">Because of the market fragmentation, European businessmodel focuses on minimizing all costs.</td>
<td colspan="2">Revenue is generated from charging for the use of licenses. Licensing will be based on number of instances and capabilities of each instance. Capability is a performance,
functionality or availability rate of the instance.</td>
</tr>
</table>

Properties of each selected market vary. With the development of MUSAP, the target markets have been split into two parts: Europe and other markets.

MUSAP business model in Europe is shaped to fit and scale up for accelerated eIDAS markets in the near future. That would mean also increasing number of tenders to be answered. Additionally, it is anticipated that the complexity of these tenders will increase when customers adapt new identity technologies. In general, based on experience, each member state must be handled separately, and a local partner needs to be found in each country.

In Asian markets, the role of Certification Authority (CA) services has been firmly established for an extended period. Additionally, strong position of telecom operators allows them to either start new CA service or cooperate with existing CA service providers.

TABLE 40: SALES CHANNELS FOR MUSAP

Partner channel sales (New) Goal: Find active partners in new countries.
0. Follow EU regulations for Type 1 and Type 2 requirements
1. Partnering with Identity Wallet apps in each market segment

2. Supporting their sales activities with Type 1 or Type 2 SSCD solution • MUSAP provides easy integration for various app vendors, who can offer Methics solutions as a part of their solution for eIDAS Type 1 strong authentication. • New contract model (e.g dual license mode) and pricing model is needed
Public tender & partner sales Goal: Search for public tenders and large companies who are interested in these tenders.
0. Follow TED (Tenders Electronic Daily) and national tender portals
1. Partner for tenders • MUSAP provides a good integration point for app. Which requires eIDAS Type 1 authentication.
Direct sales Goal: Marketing and monitoring progress in various target countries.
0. Maintain a clear product vendor scope in the company web site (www.methics.fi) and provide good search material for search engines like Google and Bing.
• Customer can develop their apps independently by using MUSAP API as an integration point.

Customer relationships in the European market will get new customers via the partner network. The project offers pay as you grow licensing model for SSCDs and increase the offering by integrating new service components. To support partner success, self-service development tools like simulators for MUSAP integration are offered. **Additionally, partner-specific interfaces can be provided to speed up integration or lower maintenance costs**. Community services are to be developed on the basis of existing support services, enabling knowledge sharing between different projects.

MUSAP enables a low-cost entry for partners to incorporate different SSCDs into their products. The partner's product resolves some business problem for the TSP and MUSAP enables qualified signatures. By this way MUSAP opens a new value chain for Methics. The figure below depicts MUSAP value network in the target market. It contains key stakeholders, their interactions, and the flows of revenue and information among them. Additionally, it includes the benefits that each stakeholder brings, the relationships and dependencies for providing services and for transferring of value.

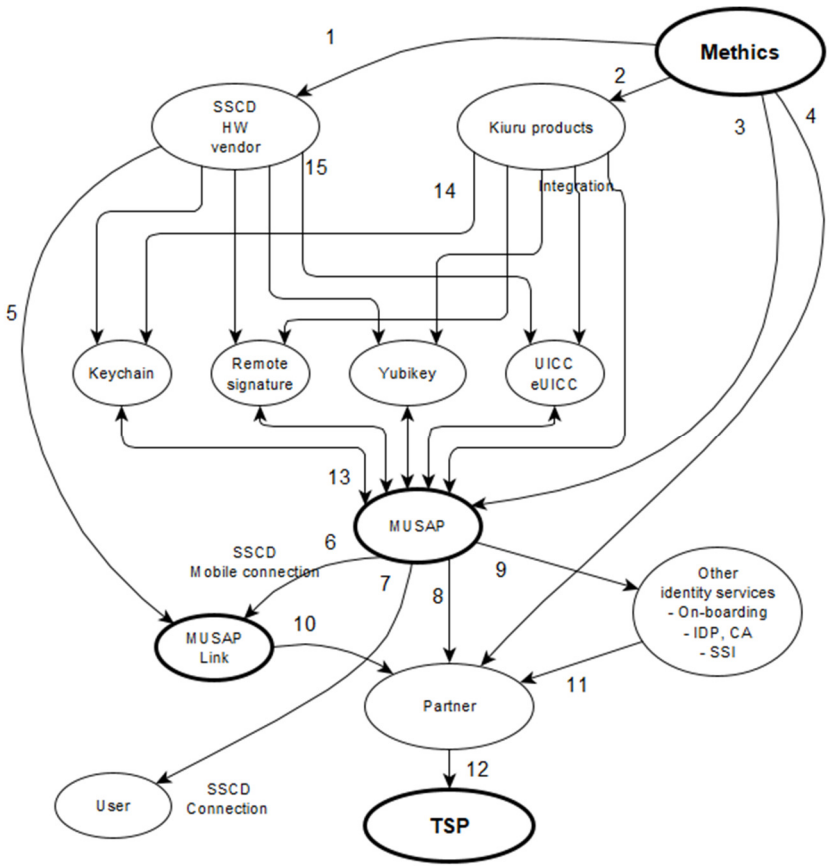


FIGURE 9: VALUE NETWORK FOR MUSAP

Among many things MUSAP Library enables end-user to have multiple identities of different LoAs. This makes it possible for user to adapt both centralized and decentralized identity, select preferred SSCD technology, LoA level, and use the solution which is best for each use-case.

8.2.3.2 Cost-Benefit Analysis

MUSAP will increase demand of standard SSCD technology and boost high LoA eID adaption. SSCD technology related service are continuously increasing e.g EDIWallet style app to support multiple LoA, option to secure your private keys, etc.

By developing standards and sharing information on SSCD constraints and security, the project makes trust-based technology using SSCD remains affordable and enable long term evolution path for the customers. Table below lists Methics products and its details.

TABLE *41*: METHICS PRODUCT PORTFOLIO

Product	Description	License type	New value proposal
Kiuru MSSP	Local signature server + orchestration	Yearly license	Orchestration for QTSP/CA, SSI and DID/VC
Kiuru SAM	Remote signature server	Yearly license	-
Alauda P38	Local signature SIM/eSIM applet	Yearly license	-
Alauda PBY	Remote signature Smartphone app/ SDK	Yearly license	-
MUSAP	MUSAP native library and MUSAP Link	Open-Source package either with Apache2.0 license.	Complete high level assurance solution for identity apps

Methics identifies different sales channels through which MUSAP can be sold as additional package to Methics existing solution, as shown in table below.

TABLE 42: MUSAP FOR NEW SALES CHANNELS ESTIMATIONS

		Per customer (unit=k euro)		
Channel	New Customer Acquisition	Costs (Customize+Project)	Initial	Recurrent (20%)
Direct sales	10%	10	180	20
Tender sales	30%	10	150	15
Partner sales	60%	30	130	20

Other markets channels based on existing product offering are defined in the following table.

TABLE 43: MUSAP FOR OTHER SALES CHANNELS ESTIMATIONS

		Per customer (unit=k euro)

Channel	New Customer Acquisition	Costs (Customize+Project)	Initial	Recurrent (20%)
Direct sales	60%	10	150	30
Tender sales	30%	10	100	15
Partner sales	10%	30	130	20

Projected consolidated Revenue for Methics in kEuros according to preliminary and partial estimates.

TABLE 44: POTENTIAL CONSOLIDATED REVENUE STREAM FOR METHICS

Year	2023	2024	2025	2026	2027	2028
Direct sales	300	300	350	350	350	300
Tender sales	0	100	100	200	150	150
Partner sales	0	0	120	300	500	700
Support & maintenance	200	240	300	500	600	750
Total	500	620	870	1350	1600	1900

8.2.3.3 Risks and opportunities

The following table describes identified risks of the MUSAP business plan.

TABLE 45: RISKS FOR MUSAP

Risk	Description	Impact
eIDAS 2 slow start	Member states' EDI Wallet start is slow	High/high
ARF	ARF still doesn't clarifty on EDI W QSCD/SSCD	Moderate

Wallet security	Wallet causes security problems	High/moderate
MUSAP security	MUSAP causes security problems	High/low
Big tech companies	Big technology companies provide corresponding or compensatory products	Moderate/moderate
Competitor mimicking	Competitors use MUSAP or similar tools	Low/low
Large scale pilots isolates	Large scale pilots isolates themselves and provide no opportunities for new parties to join	Moderate/high

The following table describes identified opportunities of the MUSAP business plan.

TABLE 46: OPPORTUNITIES FOR MUSAP

Opportunity	Description	Impact
New partners	Get new partners from completely new business areas	High/moderate
New applications	Enable new purposes for Methics products	Moderate/moderate
Extending MUSAP	More SSCDs can be added in MUSAP	Moderate

MUSAP provides a standardized and simplified way for developers to request multiple LoA signatures, regardless of the programming language, SSCD platform, or technology used. This ensure consistency and interoperability across different systems.

8.2.3.4 Business Value for Decentralized Identity

If decentralized identity services become the main trend of identity services, then MUSAP offers an interoperable route from centralized identities towards decentralized model. Using MUSAP traditional centralized systems like SIM based mobile ID can be enabled to provide authn/sign functionality.

8.2.4 TREVO

This section presents the final version of the TREVO project business model and exploitation plan. It starts by conducting a PESTLE analysis, which outlines the external macro-environmental factors that may impact TREVO operations, before delving into

the Business Model and finally providing an updated cost-benefit analysis including a break-even analysis.

8.2.4.1 PESTLE Analysis

The increasing influence of technology in lives has led to a surge in the adoption of electronic voting systems, reshaping the landscape of modern elections. These systems, leveraging advanced technology, offer substantial advantages that impact the democratic process in various ways. The availability of e-voting is associated with increased participation among abstainers and occasional voters. This underscores the potential of technology to influence civic engagement positively [1]. Below you can find a plethora of factors that address opportunities and challenges within their respective fields, regarding the integration of e-voting systems, like the one developed in TREVO, in today's evolving societies.

Political factors

Opportunities: E-voting can have several political implications that contribute to the democratic process. Firstly, it enhances accessibility and inclusivity, allowing a broader range of citizens to participate in elections. This inclusiveness aligns with democratic principles by ensuring that diverse voices are heard, potentially reducing barriers that might exclude certain groups. Additionally, e-voting has the potential to increase overall voter turnout [1]. Higher participation rates can strengthen the legitimacy of elected officials and government institutions, reinforcing the democratic mandate. Moreover, the convenience and ease of e-voting may attract younger voters who are accustomed to digital platforms, addressing concerns about generational gaps in political participation.

Additionally, the transparency and auditability feature inherent in blockchain-based e-voting systems can enhance trust in the electoral process. Auditable and tamper-proof records ensure the integrity of election results, mitigating concerns about fraud and manipulation. This heightened transparency can lead to increased public trust in the electoral system and contribute to the stability of democratic institutions. Furthermore, governments implementing e-voting may position themselves as tech-savvy and progressive, signaling a commitment to adopting innovative solutions in the public sector. This can positively impact the image of political leadership and government effectiveness, potentially garnering support from tech-oriented constituencies. In summary, e-voting holds political potential by promoting inclusivity, increasing voter turnout, enhancing transparency, and positioning governments as forward-thinking entities in the eyes of the public.

Challenges: Potential resistance to technological change and concerns about the security of electronic voting systems might pose challenges, requiring political will to address.

Economic factors

Opportunities: E-voting holds the potential for several economic benefits in the electoral process. Firstly, it can lead to cost efficiencies by reducing the need for extensive physical infrastructure associated with traditional paper-based voting systems, such as printing and distributing paper ballots and maintaining polling stations. Quicker ballot counting and result reporting mean that resources are utilized more efficiently, and election-related activities can be concluded promptly. This time efficiency can lead to cost savings in terms of personnel hours and related administrative expenses. This efficiency can lead to quicker election outcomes, saving both time and resources.

Furthermore, another notable aspect is the potential for substantial savings related to travel costs. Traditional voting methods often require citizens to travel to physical polling stations, incurring personal expenses for transportation. E-voting eliminates this need, making the voting process more accessible and cost-effective for voters. Finally, the digitization of the voting process may open up new avenues for innovation and economic growth. The development and maintenance of secure e-voting systems can foster the growth of technology and cybersecurity sectors, creating job opportunities and contributing to local and national economic development. The potential economic benefits of e-voting extend beyond immediate cost reductions, encompassing broader implications for efficiency, innovation, and economic growth.

Challenges: Initial implementation costs and the need for ongoing technological updates may pose economic challenges.

Social/cultural factors

Opportunities: E-voting systems bring forth several social and cultural benefits by fostering greater inclusivity, participation, and accessibility in the electoral process. Firstly, they can overcome physical barriers, making voting more accessible for individuals with disabilities or those who face challenges in reaching traditional polling stations. This inclusivity contributes to a more representative democracy by ensuring that diverse voices are heard. Furthermore, the flexibility of e-voting allows citizens to vote at their convenience, accommodating various work schedules and personal commitments, promoting higher voter turnout. In a cultural context, e-voting systems can adapt to the preferences of younger generations accustomed to digital platforms, potentially bridging the generational gap in political engagement.

Challenges: Resistance to technological adoption and concerns about the digital divide may hinder widespread acceptance.

Technological factors

Opportunities: Continuous advancements in electronic voting technology contribute to its favorable and prosperous environment. E-voting systems offer numerous technological advantages that can revolutionize the electoral process. Firstly, they enable secure and tamper-resistant digital authentication, reducing the risk of identity fraud and ensuring the legitimacy of each vote cast. Advanced encryption techniques can safeguard the confidentiality and integrity of the voting process, protecting

sensitive voter information and maintaining the secrecy of the ballot. Blockchain technology, often employed in e-voting systems, provides an immutable and transparent ledger, enhancing the traceability of votes and ensuring the integrity of the overall electoral outcome [2]. The use of electronic verification and tabulation streamlines the counting process, minimizing errors and providing quick and accurate results. Additionally, e-voting can facilitate remote and mobile voting, allowing citizens to participate in elections from anywhere, thereby increasing overall voter turnout.

Challenges: Cybersecurity threats pose a technological challenge, requiring robust measures to secure electronic voting systems.

Legal factors

Opportunities: E-voting systems like TREVO can contribute to various legal aspects of the electoral process. Firstly, they have the potential to enhance accessibility, ensuring that all eligible voters, including those with disabilities, can exercise their right to vote independently. Additionally, e-voting systems can provide more efficient and accurate voter registration, helping maintain the integrity of electoral rolls and reducing the risk of voter fraud. The use of advanced encryption and secure authentication methods in e-voting promotes the legal principle of a secure and tamper-resistant electoral system, safeguarding the legitimacy of election results. Furthermore, e-voting allows for quick and precise tabulation of votes, speeding up the overall electoral process and ensuring timely announcement of results. Overall, the legal benefits of e-voting lie in its capacity to strengthen the democratic foundation of elections, addressing issues related to accessibility, accuracy, security, and efficiency within the framework of established electoral laws.

Challenges: Navigating complex legal frameworks related to the adoption of electronic voting systems may pose challenges, requiring legal adjustments.

Environmental factors

Opportunities: By eliminating the reliance on traditional paper ballots, e-voting significantly reduces paper consumption, thereby lessening the environmental impact associated with paper production and transportation. The transition to digital processes minimizes carbon emissions linked to the transportation of physical ballots and materials, while also significantly reducing the need for extensive travel to polling stations and consequent fuel consumption. Additionally, the energy-efficient nature of modern e-voting systems contributes to overall energy savings compared to traditional paper-based methods. This shift toward digital, efficient, and sustainable practices not only streamlines the electoral process but also aligns with broader efforts to adopt eco-friendly technologies and minimize waste generation.

Challenges: Ensuring the environmental sustainability of the technologies used and minimizing electronic waste may pose challenges, requiring careful consideration.

Ethical factors

Opportunities: Electronic voting systems promote inclusivity by providing accessible voting options for individuals with physical disabilities or those who face mobility challenges. E-voting can enhance transparency and accuracy in the electoral process, reducing the potential for human error and intentional manipulation. Moreover, by implementing robust security measures and privacy-preserving protocols, e-voting systems aim to safeguard citizens' sensitive information and maintain the integrity of their votes. The convenience and flexibility offered by electronic voting contribute to increased voter participation, allowing citizens to engage in the democratic process more easily. Furthermore, the blockchain technology used in this system can serve as a foundational element in electronic voting systems to further enhance trust and reduce the likelihood of central entity manipulation of voting results. Additionally, the use of smart contracts on the blockchain can automate and enforce voting rules, further ensuring the integrity of the electoral process. Through the transparency and security provided by blockchain technology, stakeholders can have increased confidence in the fairness and accuracy of electronic voting systems, thus mitigating concerns related to manipulation and fraud. Overall, ethical e-voting practices prioritize fairness, accessibility, security, and the fundamental principles of democratic representation.

Challenges: Addressing concerns related to the ethical use of technology, especially in terms of cybersecurity and privacy, may pose challenges.

8.2.4.2 Business Model

TREVO envisions transforming traditional voting methodologies into a service-oriented model, embracing digitalization to foster citizen engagement. The value proposition of TREVO can be summarized as the offering of a secure, transparent, and user-friendly electronic voting solution, ensuring data integrity, voter privacy, and accessibility, while addressing the challenges faced by traditional voting systems.

The business model is designed with insights gained from the user-centric approach adopted throughout the project, heavily influenced by the gathered feedback through real-world scenarios in partnership with the Municipality of Trikala, Greece.

TREVO plans to generate revenue through licensing its voting platform to municipalities, government bodies, and organizations conducting elections. A Pay-per-Use model will also be offered, where potential users will pay a nominal fee for each election or voting event conducted via the platform, in addition to customization services tailored to specific customer requirements incurring extra charges, ensuring as such a flexible revenue model. Data analytics, providing insights into voting patterns and demographics may be also monetized.

All the above revenue streams are fundamental to sustaining the TREVO solution's maintenance and continual enhancement, which will incur significant costs. TREVO plans to continue investing to research and development towards enhancing user experience and staying up to date with the latest technological advances in fields such as blockchain and advanced cryptography. Marketing initiatives will also form a

substantial part of the costs, focusing on digital campaigns, events and community engagement to drive adoption. Operational costs will also apply, to cover for server maintenance, software updates, and customer support, ensuring seamless operations. Operational costs also include ensuring legal compliance through allocations for legal consultations and data protection assessments, aligning TREVO with voting and data related regulations. Employing the Business Model Canvas, outlined below are the specifics of the value proposition to the diverse stakeholders. The canvas encapsulates the core elements of the business model, including customer segments, value propositions and more.

TABLE 47: BUSINESS MODEL CANVAS OF TREVO

<table>
<tr><th colspan="5">Business Model Canvas</th></tr>
<tr><td>Key Partners
Government bodies
Technology providers
Legal experts</td><td>Key Activities
Softrware developmnet
Research and Development
Marketing
Customer support

Key Resources
Expert cryptography knowledge
Legal expertise
Software developers
Hosting infrastructure</td><td>Value Propositions
Customizable e-voting system emphasizing inclusivity, low cost, automation, trustworthiness, integrity, and transparency.

The platform ensures universal verifiability, voter privacy, and a tamper-proof voting process, without the need of a “central authority” owning/managing the solution.</td><td>Customer Relationships
Co-creation

Channels
Direct
Indirect
Hybrid</td><td>Customer Segments
government bodies:
municipalities
educational institutions

private organizations:
large private companies
local unions
private consortiums</td></tr>
<tr><td colspan="2">Cost Structure</td><td colspan="3">Revenue Streams</td></tr>
<tr><td colspan="2">Research & Development
Operational costs
Marketing and sales
Compliance and legal costs</td><td colspan="3">Licencing (different plans)
Pay per Election
Customization Fees (extra features)</td></tr>
</table>

8.2.4.3 COST-BENEFIT ANALYSIS

The preliminary economic analysis for the TREVO project aimed to provide an initial understanding of the cost-effectiveness and economic viability of the e-voting solution. Before delving into the estimated quantification of the costs and benefits, the initial qualitative work is presented here.

Cost Analysis:

1. Development Costs: Includes expenses related to the software development lifecycle, such as salaries for the development team, costs of technological tools and platforms, and expenses incurred during the research and development phase.
2. Operational Costs: Encompasses ongoing costs for maintaining the TREVO platform, including server costs, customer support, system updates, and security measures.
3. Marketing and Sales Costs: Pertains to the expenses related to promoting TREVO, reaching out to potential customers, and establishing a market presence.
4. Compliance and Legal Costs: Covers the costs associated with ensuring that TREVO adheres to legal standards, data protection regulations, and industry-specific compliance requirements.

Benefit Analysis:

1. Customer benefits:
   - *Efficiency Gains*: TREVO introduces significant efficiency gains for municipalities and government bodies by automating and streamlining the electoral process, reducing the need for manual intervention and minimizing the likelihood of errors.
   - *Increased Voter Participation*: By providing a user-friendly and accessible e-voting platform, TREVO has the potential to increase voter turnout, especially among demographics that have traditionally been less likely to participate due to accessibility issues.
   - *Trust and Transparency:* The integration of blockchain technology and advanced security measures in TREVO enhances the trustworthiness and transparency of the electoral process, potentially leading to a more engaged and informed electorate.

Building on the above analysis, in order to assess the viability of the TREVO solution in the market, an attempt is made here to quantify the projected costs and benefits of TREVO. The analysis starts by estimating the specific costs that TREVO would require to operate in the following years, based on the previous cost analysis and using current rates of PMs and infrastructure. The following figure presents a summary of the estimated cost breakdown:

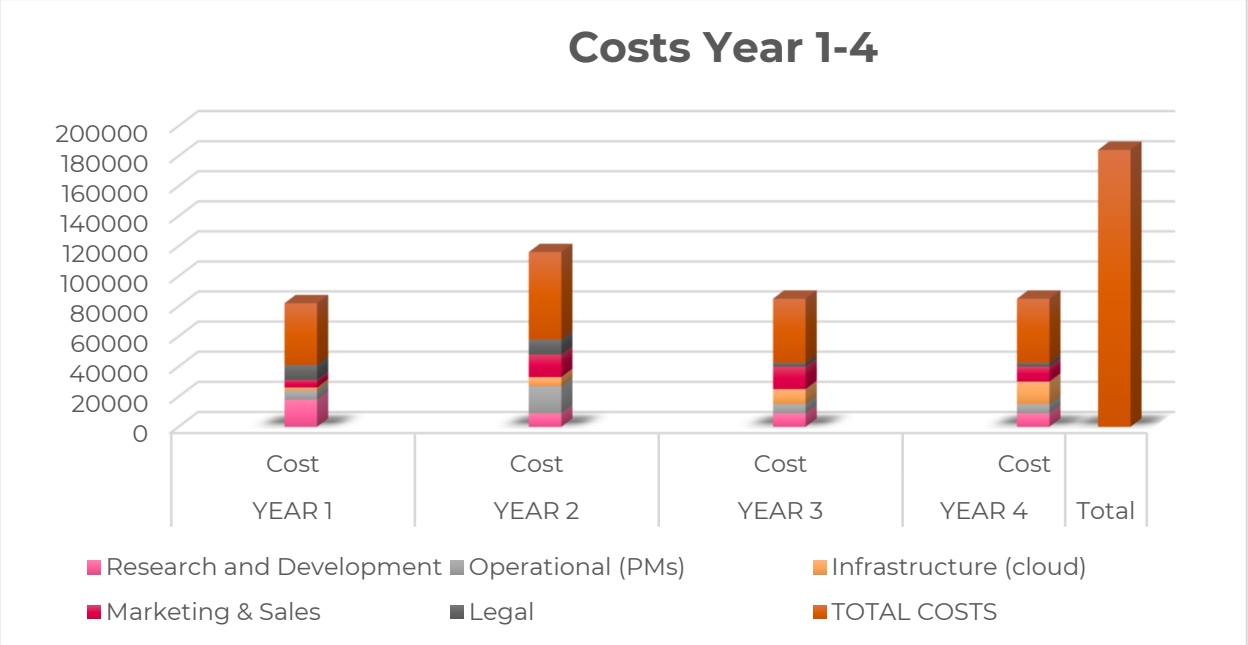


FIGURE 10. TREVO ESTIMATED COSTS (EUROS) DURING YEARS 1-4

Subsequently, the project performs a similar exercise for the expected benefits stemming from TREVO, assuming that pilot users would not be charged any costs during the first year, and also assuming a gradually expanding customer base. The table below summarizes the projected revenues, under these assumptions:

TABLE 48. TREVO ESTIMATED REVENUES (EUROS) DURING YEARS 1-4

	YEAR 1			
Customers	Enitity(ies)	Events	Votes/Event	Revenues
Municipalities	1	20	50	(not charged)
Regional	0			(not charged)
Associations / Unions	1	5	150	(not charged)
Y1 Revenue				0
	YEAR 2			

Municipalities	Enitity(ies)	Events	Votes/Event	Revenues
Regional	2	50	50	15000
Associations / Unions	1	4	50	1200
	2	3	150	2400
Y2 Revenue				**18,600.00**
	YEAR 3			
Municipalities	Enitity(ies)	Events	Votes/Event	Revenues
Regional	3	120	50	36000
Associations / Unions	2	8	50	8000
	4	8	150	8800
Y3 Revenue				**52,800.00**
	YEAR 4			
Municipalities	Enitity(ies)	Events	Votes/Event	Revenues
Regional	5	250	50	75000
Associations / Unions	3	15	50	15000
	7	21	150	23100
Y4 Revenue				**113,100.00**

Finally, using the above results, the graph below depicts the evolution of costs and revenues, superimposing as well the cumulative costs minus the cumulative benefits (darker line in Figure below), which indicate a projected break-even point for TREVO occurring after 4 years.

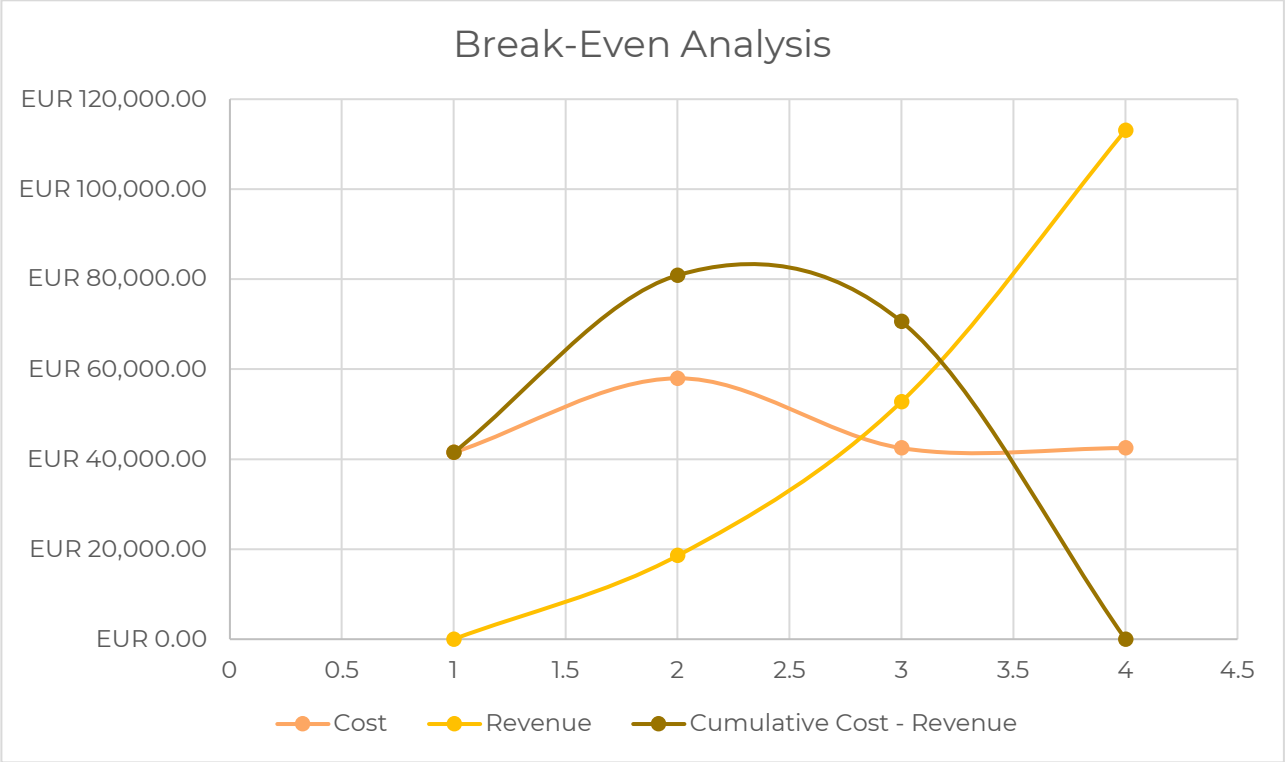


FIGURE 11. TREVO BREAK EVEN ANALYSIS

8.2.5 Orchestral

The pilots are crucial for validating the solution in real-world scenarios, which is essential for assessing the impact on the business model. These factors are integral to understanding the project's financial and exploitation prospects within the context of the TrustChain project. The pilots provide a real-world test of the solution, allowing for the gathering of data and feedback to inform future iterations and improvements. The value and demand perceived from using IdHub identity and credentials services affect the feasibility of the business model, its potential for scalability and sustainability, and the potential risks and opportunities it presents.

While a comprehensive business and exploitation plan was defined before the pilots, the pilots are still underway and progressing slowly. Working with user communities takes a long and often unbounded time, especially with volunteer participants or busy people. However, the results so far are promising as users perceive the value, but given that eIDAS2 and EBSI are not yet there, it is difficult to sharpen the details.

Moreover, the pilots are designed to address the challenges identified in the TrustChain project, such as navigating the data exchange/trading arena, which involves multiple parties and faces hurdles related to trust, privacy, consent, and regulatory complexities.

The pilots help to understand how the solution addresses these challenges in detail and how it can be integrated into the existing ecosystem of decentralised applications.

Given the open-ended nature of the pilots, which are intended to prepare for a medium-term service provided by Pangea.org, it is believed to be too early to provide a firm and more comprehensive, conclusive and realistic analysis of the business model's feasibility, scalability, sustainability, and the economic landscape's influence.

Regarding the business model, the analysis first looks at the market, with related or similar solutions, stakeholder groups and obstacles for the digitalisation of the SSE sector.

8.2.5.1 Market analysis reviewing similar solutions

The landscape is unique in the digital services for social and solidarity economy actors (SSE) working with vulnerable populations and presents opportunities and challenges.

One of the significant advantages of this niche is the lack of direct competition. Unique service offerings, like those provided by members of APC.org, which Pangea is a member of in Spain, are often difficult to replicate due to the specific needs and characteristics of the target audience. These needs often exceed what traditional platforms or services offer, making the entry barrier high for potential competitors [UN21].

APC members and other digital service providers, typically organised as social enterprises or cooperatives, have effectively leveraged this advantage by offering services specifically tailored to the needs of social and solidarity economy actors and vulnerable populations [APC21]. Their ability to adapt and evolve according to the changing requirements of initiatives and projects makes them a valuable partner for other organisations looking to replicate their success.

Regarding the entry barrier, the service offering has overcome it by providing eIDAS1-compatible services that automate signing PDFs with digital certificates, which have legal validity but target manual processing and verification by human readers instead of the automated and, therefore, interactive response of automated verification procedures enabled by verifiable credentials. These signed PDF documents include a (QR) link to a modern but not yet legally valid verifiable attestation targeting eIDAS2. This innovative approach allows the services to offer organisational and individual users secure, reliable, advanced and legally compliant services.

However, it's important to note that while the digital services for social and solidarity economy actors and vulnerable populations may currently lack direct competition, this could change. Policymakers and regulators are becoming increasingly aware of the potential of these organisations. Public services may complement or compete with these organisations. Public actors can act as other issuers or verifier organisations when they complement. This is the case of the X09B or LaFede cases, where public funding agencies participate in these programs with economic incentives and benefits [DE21].

Transitioning from eIDAS1-qualified trust services to eIDAS2 based on decentralised identity and verifiable credentials presents several digitalisation obstacles in the market. The regulation, introduced in 2014, has been criticised for its limited implementation and evolving technical environment, which, together with changing user expectations, prevent it from reaching its full potential. Therefore, it is a concern how eIDAS2 can create an inclusive system that leaves no one behind.

The European Blockchain Services Infrastructure (EBSI), a public sector blockchain service enabling secure and efficient cross-border transactions between the public and private sectors, is crucial in transitioning from eIDAS1-qualified signatures towards eIDAS2 based on verifiable credentials. This would align with the goal of eIDAS2 [EI24] to move away from nationally issued digital identities towards electronic attestations of attributes that are valid at the European level. This focus on verifiable credentials provides a way to verify these claims in a decentralised manner. [EBSI24]

This change necessitates the provision of digital wallets capable of linking national digital identities with proof of other personal attributes and other tools and services for issuer and verifier roles [EP22], as well as the technological transition issues that will add to it. The project contributes working solutions adapted to the needs of the specific sector.

Lastly, the technical implementation work has started alongside the legislative process. The toolbox procedure established to guide this process involves cooperation between Member States, the Commission, and other stakeholders. However, this procedure will produce several implementing acts defining a technical architecture and reference framework, common standards and technical specifications, and common guidelines and best practices. These results will be adapted as necessary to the outcome of the legislative process [EP22], but this is a source of delay and uncertainty in the eIDAS2 scenario.

In summary the market for digitalised solutions in verifiable credentials for vulnerable people, social and internet activists, or circular device management is mainly untapped, with a growing demand for accountability and verifiability. The target market includes civic associations, public administrations, non-profit and for-profit SMEs involved in the circular economy. These organisations lack the tools to efficiently manage data related to providing, exchanging and verifying sector-relevant information, creating a substantial opportunity for the platform. Thirty years of experience in Pangea offering comparable digital services to associations and other organisations confirm that analysis and involvement with that market.

The market opportunity can be characterised in more detail as:

- **Limited competition:** Lacks direct competition due to the target audience's specific needs.
- **Growing demand:** Increasing demand for accountability and verifiability in the social sector.

- **Target market:** Civic associations, public administrations, NGOs, and SMEs in the circular economy.

Typical stakeholders in the digital services for this sector can be categorised into several groups:

1. Social and Solidarity Economy Actors: These are organisations that provide direct (direct help, advice, services) or indirect (campaigning, dissemination) support services to vulnerable populations, such as non-profit organisations, cooperatives, public services, and other entities that operate outside traditional economic profit-oriented structures. They are key stakeholders as these organisations directly use, provide or benefit from the services in digital platforms and need them to deliver their services effectively.
2. Vulnerable Population: These are individuals or groups who are particularly susceptible to exclusion from mainstream society and the economy, such as the elderly, people with disabilities, refugees, and low-income households. They are primary beneficiaries of the services offered by these support digital platforms.
3. Digital Service Providers: These are companies or individuals who create and maintain the digital platforms that facilitate transactions between social and solidarity economy actors and vulnerable populations. They play a crucial role in ensuring the smooth operation of these platforms. They tend to be small and regional in scale, which prevents the capacity to offer advanced digitalisation services. This is the case of Pangea.org and APC.org.
4. Regulatory Bodies: Government agencies and international bodies that regulate digital services, digital commerce and data protection. They are important as they set the rules and standards for all stakeholders, even this sector, as with the eIDAS1 and 2 regulations.
5. Donors and Funders: Organisations and individuals who provide financial support for developing and maintaining digital platforms and services for social and solidarity economy actors are also stakeholders. Their funding can influence the scope and functionality of these platforms. This is the case of the TrustChain project and Pangea and APC members who contribute membership funds to support these organisations.
6. Technology Partners: Companies that provide the underlying technology for digital platforms, such as housing, hosting, cloud or networking providers (that Pangea and other APC members use) and software developers (as with this project).

These stakeholders interact and complement in various ways, influencing the development and implementation of digital services for social and solidarity economy actors working with vulnerable populations. They are essential for all parties involved to address the needs and challenges of this sector collaboratively.

Several obstacles can hinder the digitalization of this sector. One significant challenge is the lack of digital skills within the sector, particularly among the vulnerable population. Older adults and migrants often struggle with mastering languages and computers, which are essential tools for accessing digital services. They may also face difficulties filling out forms correctly, answering questions accurately, and understanding the language used in official documents and the implications of digital interactions in application processes and their lives [NCBI21].

Another obstacle in using systems like eIDAS eIDs and EBSI is the challenges and issues in the generation and processing of digitally signed documents. However, initiatives like the European Union's General Data Protection Regulation (GDPR), which aims to give citizens control over their personal data, contribute to the sector's digitalisation by promoting modern, secure digital technologies [WF21].

Other obstacles include complexity in implementing digital transformation, organisational resistance to change, a skills gap in the workforce, outdated infrastructure and systems, and evolving digital landscapes. Additionally, security and privacy concerns, resource constraints, and the difficulty of measuring success can pose challenges [WF21].

Despite these challenges, many programs and initiatives contribute to the sector's digitalisation. For instance, investing in a digital adoption platform can help organisations overcome these challenges and reach their potential by empowering new digital systems and technologies [WF21]. However, this is very difficult for organisations in this sector, as resources and capacities are too limited, and staff is usually overloaded with too many critical tasks already.

8.2.5.2 High-level description of the Business Model

The Business Model proposed for the new service/application delivered by the project and the Business Model canvas is described below.

Executive Summary: This initiative is a pioneering open-source project to provide digitalised solutions and services using verifiable credentials for the social and solidarity sector. The target market consists of civic associations, public administrations, non-profit and for-profit SMEs, focusing on those involved in the social, solidarity, and circular economy. The revenue model is based on a yearly membership fee (to Pangea.org) plus service fees beyond a free tier per volume of credentials issued or verified, in addition to training, support, custom developments and consulting service fees.

Company Analysis: Pangea.org is a service provider leveraging open-source technologies to provide affordable and accessible solutions for social enterprises and solidarity organisations. The mission is to foster self-reliance and socio-economic sustainability through the service offerings. The organisational structure is designed to support the open-source model, with a dedicated team focused on support, platform maintenance, development, consulting, and technological advice.

Market Analysis: The market for digitalised solutions in verifiable credentials for vulnerable people, social and internet activists, or circular device management is untapped mainly, with a growing demand for accountability and verifiability. The target market includes civic associations, public administrations, non-profit and for-profit SMEs involved in the circular economy. These organisations lack the tools to efficiently manage data related to the subjects of their work, creating a substantial opportunity for the platform. Thirty years of experience in Pangea offering comparable digital services to associations and other organisations confirm that analysis and the involvement with that market.

Financial Plan: The primary sources of revenue are the yearly membership fees from individual and organisational members, service fees per service unit (data traffic and storage, or service units such as per person or device). Additional revenue is also generated from training, custom developments and consulting services. Costs include platform development and maintenance, staff salaries, and dissemination expenses. A steady and sustainable revenue is projected as new members are attracted and service offerings are expanded, thanks to the results of this project.

Marketing Plan: The marketing strategy is centred on raising awareness about the importance of ethical choices in internet services, self-determination in technical choices, and sustainability in device management, along with a cost-oriented approach and infrastructure sharing in the value proposition of the open-source platform. Visibility in the local community is leveraged, as well as moderate use of social media, international specialized forums, and partnerships with key players with similar organizations globally to reach the target market and target goals.

Operations Plan: Operations involve the continuous development and maintenance of the open-source service platform, providing support, consulting, and technological advice to users, as well as offering training and custom development services. Long-term goals include expanding the user base, continuously improving the platform based on user feedback and technological advancements, and fulfilling the purpose of bringing the Internet and information and communication technologies to associations, NGOs, individuals, and non-profit groups that work for change, social justice, education, peace, the environment, development, cooperation, and more.

Management Team: The team comprises experienced professionals and volunteers with expertise in open-source technologies, digital solutions, and sustainability. Their combined knowledge and skills position the team to successfully deliver on the promise of providing affordable and accessible solutions for circular device management.

Ingrid Burkett's business model canvas for social enterprises [BUR20] offers guidance to develop the canvas, a compact outline of a business model, that consists of the following sections:

Key Partners: The organizations that can help achieve success in the mission.

Key partners include social enterprises, solidarity organisations, and civic associations that adopt the platform in the social and solidarity sector.

Key Activities: The most important things the organisation must do to function effectively.

Key activities include the development and maintenance of the open-source platform that provides internet services to members, offering support, consulting, and technological advice to members and users, as well as providing training and custom development services.

Key Resources: The resources that the project needs to create value for customers.

The key resources are the server infrastructure and the services provided, internet presence, open-source software, staff and team of experts and volunteers, and the network of partners in the social and solidarity sector and internet activists.

Value Propositions: The unique value that the organisation promises to deliver to customers.

The value proposition is to provide an affordable and accessible open-source platform and infrastructure for delivering the internet services that member organizations need, fostering self-reliance and promoting the socio-economic sustainability of infrastructure as commons.

Customer Relationships: The relationship that the project establishes with customers.

Long-term relationships are built with customers, who are long-term members and supporters of the organization. This is based on mutual trust and shared values, providing them with continuous support and advice.

Channels: The ways the project communicates with and reach customers.

The main channels include the platform, local face-to-face events, word of mouth, social media, international specialized forums, and partnerships with key players in the sector.

Customer Segments: The groups of people or organisations you aim to reach and serve.

The customer segments include civic associations, public administrations, and non-profit SMEs involved in the digital, solidarity and circular economy.

Cost Structure: All costs incurred to operate the organisation.

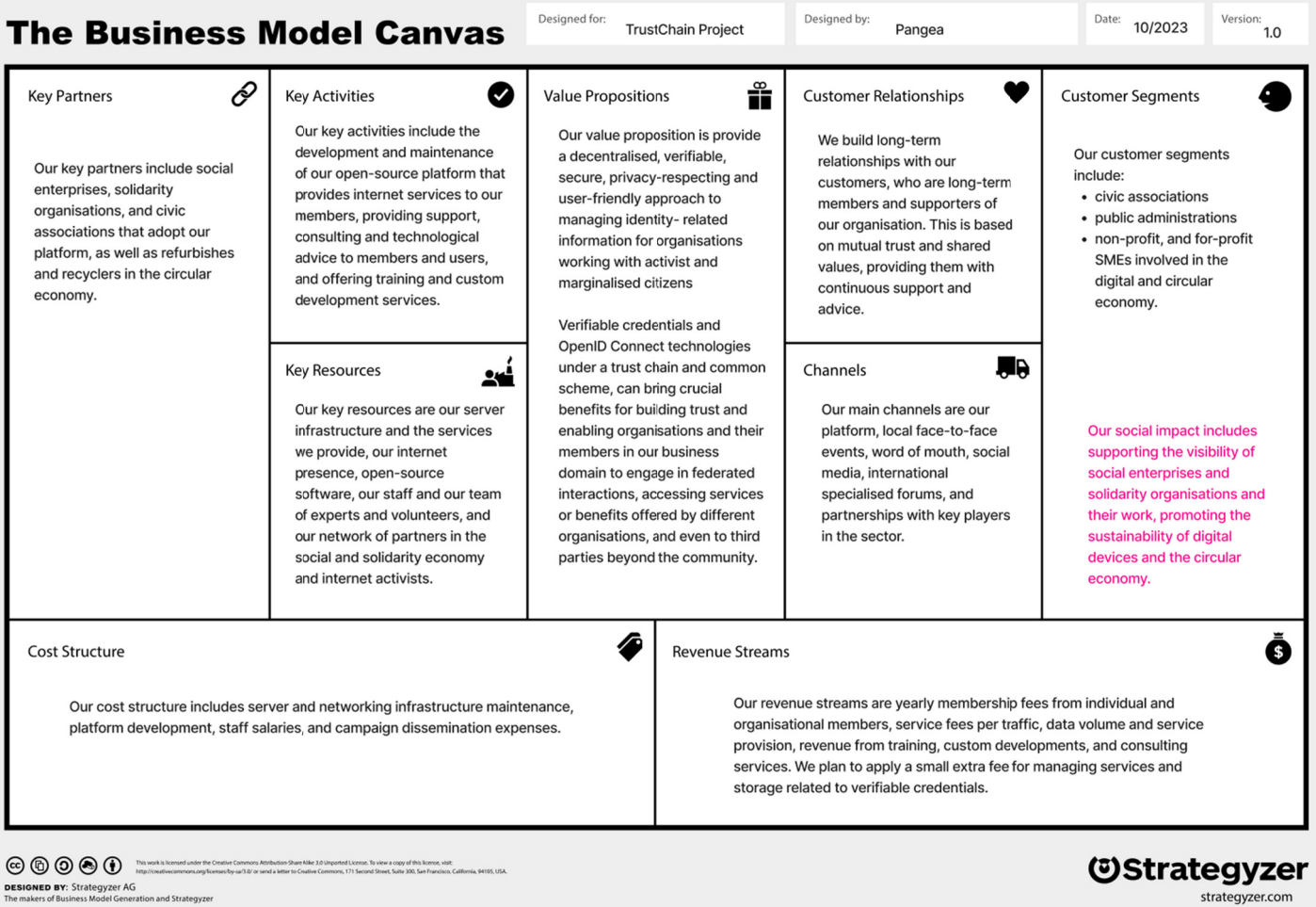
The cost structure includes server and networking infrastructure maintenance, platform development, staff salaries, and campaign dissemination expenses.

Revenue Streams: The ways the organisation makes money.

The revenue streams are yearly membership fees from individual and organisational members, service fees per traffic, data volume and service provision, revenue from training, custom developments, and consulting services.

Social Impact: The social benefits that the organisation aims to achieve according to its vision and mission.

The social impact includes supporting the visibility of solidarity organisations and social enterprises and their work and campaigns.



The Business Model Canvas

Designed for: TrustChain Project | Designed by: Pangea | Date: 10/2023 | Version: 1.0

Key Partners

Our key partners include social enterprises, solidarity organisations, and civic associations that adopt our platform, as well as refurbishes and recyclers in the circular economy.

Key Activities

Our key activities include the development and maintenance of our open-source platform that provides internet services to our members, providing support, consulting and technological advice to members and users, and offering training and custom development services.

Key Resources

Our key resources are our server infrastructure and the services we provide, our internet presence, open-source software, our staff and our team of experts and volunteers, and our network of partners in the social and solidarity economy and internet activists.

Value Propositions

Our value proposition is provide a decentralised, verifiable, secure, privacy-respecting and user-friendly approach to managing identity- related information for organisations working with activist and marginalised citizens

Verifiable credentials and OpenID Connect technologies under a trust chain and common scheme, can bring crucial benefits for building trust and enabling organisations and their members in our business domain to engage in federated interactions, accessing services or benefits offered by different organisations, and even to third parties beyond the community.

Customer Relationships

We build long-term relationships with our customers, who are long-term members and supporters of our organisation. This is based on mutual trust and shared values, providing them with continuous support and advice.

Channels

Our main channels are our platform, local face-to-face events, word of mouth, social media, international specialised forums, and partnerships with key players in the sector.

Customer Segments

Our customer segments include:

- civic associations
- public administrations
- non-profit, and for-profit SMEs involved in the digital and circular economy.

Our social impact includes supporting the visibility of social enterprises and solidarity organisations and their work, promoting the sustainability of digital devices and the circular economy.

Cost Structure

Our cost structure includes server and networking infrastructure maintenance, platform development, staff salaries, and campaign dissemination expenses.

Revenue Streams

Our revenue streams are yearly membership fees from individual and organisational members, service fees per traffic, data volume and service provision, revenue from training, custom developments, and consulting services. We plan to apply a small extra fee for managing services and storage related to verifiable credentials.

DESIGNED BY: Strategyzer AG
The makers of Business Model Generation and Strategyzer

Strategyzer
strategyzer.com

FIGURE 12. BUSINESS MODEL CANVAS

Funded by the European Union

The demonstration and validation roadmap in a real-life application has provided insights into customers' pains and gains and Pangea's maintenance cost.This is particularly critical as Pangea is an infrastructure and service provider that provides cost-oriented services to its member organisations.

As described in the project application, profit is not sought from setting up entry barriers from patenting or intellectual property (AGPL licence), but on an infrastructure and service commons model to ensure service operation, maintenance, and upgrades if possible. Given the public funding received, the goal is to offer the results for the common good.

The business model for managing services and storage related to verifiable credentials is expected to be followed. Collaboration agreements with public sector organizations are also expected to be achieved, which can partly sponsor these costs but not remove service costs, as this creates an unfeasible perception that things are free and, therefore, risk collapse in case funding stops. Ad-based funding for the software and services is not considered and is rejected, as it compromises user privacy and turns them into targets for information exploitation and manipulation.

8.2.5.3 Value network

This matrix illustrates the **value network** of the organization, showing how each stakeholder contributes to the value proposition, interacts with others, and contributes to the flow of revenue and information. It also shows the benefits each stakeholder derives from these interactions and flows.

TABLE 49. VALUE NETWORK

Stakeholder	Benefits Brought	Interactions with Other Stakeholders	Flows of revenue and information
Infrastructure and service provider (ISP) organization (e.g. Pangea)	Value-added services for their member and partner organisations and potential membership	Integration with other public and private infrastructure and service providers (e.g. EBSI)	Membership and usage fees, joint development projects, consulting, acts as data processor for user organisations
Key partners: social enterprises, solidarity organizations, civic associations, refurbishers, recyclers	Adoption of the platform, access to services, and support/guarantees (verifiability, machine readable,	They interact with the ISP organisation by adopting the platform, seeking support, and participating in the community (e.g.	They contribute to the ISP organization's revenue through membership fees and usage fees. Information flows from the ISP organization to the partners in the

	interactive) for their initiatives.	defining common credential schemas).	form of updates, news, and services.
Staff and team of experts and volunteers	Job satisfaction, professional growth, contribution to societal causes.	They interact with people and particularly vulnerable population, partners, and each other to generate, Exchange and validate credential data, the basis for providing benefits and services to.	Their compensation forms the organization's cost structure. Information flows from the organization to the staff in the form of job descriptions, project updates, and training materials.
Customers (Civic Associations, Public Administrations, Non-profit and For-profit SMEs)	Access to affordable and reliable internet services, support, and custom development services.	They interact with the organization by subscribing to services, requesting support, and engaging in the community.	They pay the organization through membership fees, service fees, and payment for custom developments. Information flows from the organization to the customers in the form of service descriptions, updates, and support materials.
Beneficiaries: vulnerable population and support NGOs	Access to affordable and reliable identity and credential services and support.	They interact with the ISP and customer organisations by subscribing to services, requesting support and benefits, accessing services, and engaging in the community.	They get free services in the form of identities and verifiable credentials. These result in information flows from issuer organisations to the beneficiaries and verifier organisations that benefit them.

8.2.5.4 Economic (cost-benefit) analysis of the offered services

As a **refined economic (cost-benefit) analysis** of the offered services, the IdHub-related services tailored to organisations engaged with activists and marginalised citizens can yield significant costs and benefits.

Costs:

1. Development costs: The initial investment for developing such a system, supported by the TrustChain project and related open-source software and infrastructure projects, includes costs for skilled developers and IT professionals, necessary hardware and software, conducting rigorous testing to ensure the system's security, reliability and compliance to policies, regulation and interoperability standards.

> Concrete detail: Beyond the development costs supported by the TrustChain OC1 project, an additional 10-20% cost is assumed to reach the market (beta testing and release). That leads to an additional cost of about 10-20 K€.

2. Software maintenance costs: Ongoing costs include regular updates to keep the system current, troubleshooting and fixing bugs, and upgrading the system to meet increasing demand or changing requirements.

> Concrete detail: As part of Pangea, with staff maintaining all services but at least requiring bug and security maintenance, an additional 5-10 K€ cost/year is assumed.

3. Infrastructure costs: Implementing web service and blockchain technology for the registry requires significant computational power and storage space, leading to recurrent costs. Verifiability, reliability, trust and other guarantees bring costly infrastructure and maintenance costs, including replication, physical and logical protection, etc.

> Concrete detail: The service and blockchain maintenance can be included in this item as part of Pangea's computing infrastructure. The infrastructure cost for an IdHub service using a medium server with multiple Docker containers and a 3-node ledger has proven to be lightweight, so it is assumed an additional 2-5 K€ cost/year.

Benefits:

1. Empowerment of organisations and their members: The proposed system would allow organisations and their members to engage in federated interactions, enabling access to services or benefits offered by different organisations within the community without compromising their personal information. This can significantly enhance the effectiveness and efficiency of these organisations and facilitate and improve life for the beneficiary population.

2. Security and Privacy: Decentralised digital identity and blockchain technology can offer superior security and privacy protections compared to traditional identity management systems. Users control their data, reducing the risk of data breaches and unauthorised access.

> Concrete detail: User-controlled data reduces data breaches and unauthorised access risk by giving users control over their data. Enhanced security and blockchain/smart contracts offer a tamper-proof way to store data, making it more secure than traditional systems.

Funded by the European Union

However, these data breaches and unauthorised access risks are hard to quantify, and their appearance is unexpected.

3. **Trust and Trustworthiness**: By leveraging blockchain technology, the system can create a trust chain that provides benefits to the community. This can enhance the reputation of the organisations involved and build trust among the community.

> **Concrete detail:** A trust chain with accreditations of organisations to issue specific credentials creates a verifiable chain of accreditation for credentials, improving trust between organisations and individuals. Reputation building: Secure and verifiable credentials can enhance the reputation of SSE actors.
>
> These data breaches are hard to quantify.

4. Cost Savings: For organisations, using such a system can significantly reduce costs associated with manual, costly, and inefficient verification processes. It can also lower the risk of liabilities, penalties, lawsuits, and serious incidents by ensuring that only qualified individuals are granted access and that interactions and data can be verified.

> **Concrete detail:** Automating otherwise manual verification processes reduces verification costs, saving organisations time and money. It also lowers the risk of liabilities by ensuring only qualified individuals have access, reducing the risk of errors and fraud.
>
> A study by the World Bank found that NGOs can spend up to 20% of their time and resources on administrative tasks such as verifying the identities of beneficiaries. The IdHub system could reduce this time by 50% or more, allowing NGOs to focus on their core mission of serving marginalised communities.
>
> Regarding reduced verification time, assuming an NGO spends 20% of its time on verification (e.g., 1 day/week for a 5-person team working with roughly 100-300 beneficiaries), a 50% reduction in verification time saves 0.5 days/week. The weekly savings = 0.5 days * 8 hours/day * €20/hour = €80, which results in annual savings (assuming 50 working weeks) = €80/week * 50 weeks = €4,000.

Given these rough numbers, the total costs range from 10 to 20 K€ for up to 4 K€ of a rough estimate of benefits for a typical medium-range NGO, among several sharing the service infrastructure.

A cost-oriented cooperative infrastructure and service-sharing model that Pangea takes is considered (member organizations can be flexible to justify post-adjustments to cover additional costs).

Tiers are defined based on local NGOs that are existing or potential Pangea members, based on the number of actors (beneficiaries or members). A minimum per holder cost would be 10 K€ / 5900 holders = 1.69 €/holder. That results in yearly costs/org ranging from 84 to close to 3384, lower than the average maximum of 4 K€ roughly expected benefits.

TABLE 50. TIERED COST MODEL FOR IDHUB

Tier	Min # holders	Max # holders	# member orgs.	Avg. tier # holders	Yearly cost/org	Monthly cost/org	Yearly tier cost contrib.
Basic	0	50	20	500	84	7	1680
Standard	50	200	8	1000	336	28	2688
Medium	200	500	4	1400	840	70	3360
Large	500	1000	2	1500	1692	141	3384
Custom	1000	2000	1	1500	3384	282	3384
Total			35	5900			14496

It is assumed that holders are not paying any wallet and service fee, nor are third-party verifier organizations.

Further important considerations:

- Economies of Scale: The more NGOs use the system, the more the costs could be spread out and lowered for everyone.
- Grant Funding: NGOs might be able to secure grants to subsidise the development of new features and the maintenance and use of this system, especially with a strong focus on security, efficiency, and benefiting marginalised communities.
- Consulting: The training on concepts and procedures, development of sectorial credential schemas, software and service maintenance, FOSS software deployment, development of custom solutions, extensions and integrations, and support can provide additional sources of income.
- Sliding Scale: Depending on NGO income or budget, a sliding scale fee could make the system accessible to smaller organisations.
- Blockchain token economy: This has been discarded as it is not technically accessible or enticing for social and solidarity economy actors, who require more decentralised, verifiable, secure, privacy-respecting, and user-friendly ways to manage identity-related information for authentication, authorisation, and accreditation. The project targets actors who are motivated towards cooperative rather than competitive models, more cost-sharing and risk avoidance, and less profit and risk-making, emphasising the importance of the decentralised and trust-based approach.
- Additional Factors: The final cost-benefit analysis will depend heavily on the specific features and implementation of the system, as well as the size and needs of individual NGOs.

8.2.5.5 Exploitation plan and Exploitability

The success of this service/application largely depends on its adoption by the organisations and the community members. If these stakeholders find value in the benefits offered by the system, they will likely use it frequently and recommend it to others. This can create a virtuous cycle of growth and success.

Furthermore, the system's exploitability lies primarily in its ability to handle high volumes of requests and transactions and in its security measures to protect user data and maintain the integrity of the blockchain and the related information details. The system may fail to attract widespread adoption if these areas are not adequately addressed.

The numbers above define a target number and tier distribution of participating organisations at the end of the first year of operation. The introduction of eIDAS2 and EBSI services in the sector will raise more requirements but, at the same time, will bring more funding sources and service demand for such services.

Value to the Broader Ecosystem:

By promoting decentralised digital identity and blockchain technology, these services/applications can contribute to the broader ecosystem by fostering innovation, improving security practices, and empowering marginalised communities. It can also provide valuable learning opportunities for organisations leveraging these technologies.

Marketing and sales plan:

The plan is to reach target customers/members through NGO associations and existing sectorial gatherings, events, partnerships, and social networks in the region where Pangea operates. Disseminating pilot results can help convince them to use the service offering. This could include developing marketing materials, attending industry events, or partnering with other organisations.

A timeline:

The reference timeline for developing and launching your system points to June 2024 to release a beta-tested software release and the first deployment open to paying user organisations, expecting to reach June 2025 with numbers as planned in the previous section.

8.2.6 The Social Wallet

The Social Wallet smartphone app is Open Source and free to use for the end users. They will be able to download the app from the App Stores and use it to work with Verifiable Credentials as a generic credential wallet, compatible with other W3C-

compliant credential systems, independent of the Social Wallet platform using peer to peer communication (OID4VC)

The Social Wallet platform is Open-Source as well but will also be offered as a paid Software as a Service (SaaS).

This means that municipalities, NGOs, or other sponsors, could download and run the Social Wallet platform themselves, without any involvement of Sphereon. However, as you are aware, this is complex technology that is still changing and evolving.

It is known that most organizations do not want to be bothered with such a burden and prefer to opt for using a SaaS offering, or at least have some form of a commercial support services contract.

8.2.6.1 Economic viability

Currently, the willingness-to-pay from municipalities such as Weert and Nederweert is known. They are charged an annual fee for the SaaS-offering based on the number of citizens in a municipality. This means a lower fee for smaller municipalities and a higher fee for larger municipalities, in line with their budgets, benefits and cost savings.

			1%	5%	10%	20%	1%
Municipalities		Avg. Fee/py					
NL	324	€ 24.000	€ 77.760	€ 388.800	€ 777.600	€ 1.555.200	€ 77.760
BE	581	€ 12.000	€ 69.720	€ 348.600	€ 697.200	€ 1.394.400	€ 69.720
		Annual revenu	€ 147.480	€ 737.400	€ 1.474.800	€ 2.949.600	€ 147.480

FIGURE 13. SOCIAL WALLET COST-BENEFIT

The calculation above lists the number of municipalities in The Netherlands and Belgium and shows that this business model will scale and will be economically sustainable.

8.2.6.2 Environmental sustainability

The alternative of running a social benefits program without the Social Wallet platform will have a much larger energy/CO2-footprint, if only because of the paper-heavy process and traditional administrative systems and processes.

The Social Wallet platform does uses (d)POS EVM blockchains (Ethereum/Polygon) and uses batching with other party's data with a PoW-blockchain (DID:ION and Accumulate anchor in Bitcoin) to minimize the environment impact, but do benefit from its proven security.

In addition to this, support for DID:EBSI methods is now also offered, which has become the preferred infrastructure for government(-related) projects in Belgium and The Netherlands.

The platform itself will be hosted on a green hosting-provider, Data Center Light (Switzerland), that has been certified to use 100% renewable energy.

After engaging in conversations with key stakeholders, it has been collectively ascertained that the original business plan remains robust and well-aligned with strategic goals and market expectations.

There is a unanimous agreement that the established revenue model continues to be relevant and applicable, embodying the same business values that are central to the TrustChain's vision.

It's important to emphasize that the strategy has been designed with the unique needs of stakeholders, especially municipalities, in mind.

The decision to maintain the existing business model, rather than shifting to a transaction-based model, is grounded in an understanding of the budgetary planning challenges faced by municipalities.

8.2.6.3 Predictability

Municipalities require predictability in their financial planning to ensure they can allocate resources effectively and comply with government regulations regarding annual budgeting. A transaction-based model, while potentially offering flexibility, introduces variability that complicates this planning process. It makes it challenging for municipalities to forecast their expenses accurately, which could lead to budgetary discrepancies and regulatory complications.

The fixed-cost model provides a solution to this problem by offering a clear, upfront cost for the implementation and use of the platform for a year. This model allows municipalities to budget effectively for the solution well in advance, ensuring they can manage their finances in compliance with government guidelines and avoid unexpected expenses that could disrupt their annual budget.

By sticking to this model, the project is not just offering a technical solution but also ensuring that it fits within the fiscal planning frameworks of stakeholders, thereby avoiding potential financial and regulatory pitfalls associated with unpredictable budgeting. This approach underlines the commitment to not only meeting the technological needs of stakeholders but also addressing their operational and budgetary constraints.

This consensus reinforces confidence in the path charted, but there is continued active gathering of insights from feedback sessions with various stakeholders and ongoing re-evaluation of the plan for any needed future revisions.

8.2.6.4 People are the First Mile

A practical example of this is an additional "gain" added to the Value Proposition based on such a feedback session; it is called "People are the First Mile":

People are the first mile in the government eServices onboarding process. And as the focus are on individuals and groups who are at risk of being left behind in the digital transition (people with socio-economic challenges, the elderly, sick, incapacitated, and marginalized groups like refugees or internally displaced individuals) which are the weakest link in the chain. They have problems with filling out forms, especially digital forms, understanding the language, what is actually asked from them to provide, where to find the information, how to ask for it, etc.

Verifiable credential wallets are the solution. They can guide people to easily get and provide the right information. Government eServices can optimize these often-complex tasks to a simple User Experience where in most cases scanning a QR-code to receive data and to share data is all that is needed. From getting access to systems (scanning a QR-code for passwordless login), to receiving and storing data on their phone (scanning a QR-code for VC issuance), to sharing what is needed by the eService from their “personal data vault” (using a Presentation Definition (PEX) to define what data is needed and simply scanning a QR-code for VP verification).

8.2.6.5 Cost- benefit analysis

It is imperative to acknowledge the inherent uncertainties surrounding the cost structure associated with advancing the Social Wallet from its current state to a more refined beta version. The initial investment in the Social Wallet project was made several years ago, marking the commencement of the journey towards creating an innovative solution for decentralized digital identity management and the efficient distribution of social benefits.

The funding received through the TrustChain grant has been instrumental in reaching a significant milestone: the upcoming launch of an alpha version of the Social Wallet.

This version serves as a foundational step, demonstrating the feasibility and potential impact of the solution. However, as the development of a beta version is anticipated, it becomes clear that further research and financial analysis are necessary to accurately determine the additional investment required.

The transition from alpha to beta entails not only enhancements in functionality and user experience but also rigorous testing, security audits, and compliance checks to ensure the platform meets the highest standards of performance and reliability. The complexity of these tasks, coupled with the dynamic nature of blockchain technology and digital identity frameworks, introduces a degree of financial uncertainty.

Maintenance and Deployment Costs:

- **Personnel:** The project plan outlines extensive tasks involving UX/UI design, platform integration, maintenance, and testing, requiring skilled personnel across multiple phases.
- **Technology:** Incorporation of DIDs, VCs, and integration with OID4VC demands advanced technology stack, including blockchain infrastructure.
- **Operations:** Continuous operation of the management platform and mobile applications, including updates and maintenance.

Hosting and Infrastructure:

- The platform uses environmentally sustainable hosting solutions and technologies, which may incur varied operational costs depending on the scale of deployment.

Compliance and Security:

- Ensuring compliance with European Architecture Reference Framework and other regulatory standards, alongside implementing robust security measures.

8.2.6.5.1 Revenue Streams

Software as a Service (SaaS) Offering:

- Municipalities and NGOs can opt for a SaaS model, paying an annual fee based on the number of citizens, ensuring scalability and economic sustainability.

Commercial Support Services:

- Optional support services for organizations preferring not to manage the technology in-house.

8.2.6.5.2 Economic Sustainability

Scale and Sustainability:

- The above-mentioned table provides a calculation for potential revenue based on municipalities in The Netherlands and Belgium, demonstrating the project's scalability and economic viability.

Environmental Sustainability:

- The project emphasizes minimizing environmental impact through the use of Proof of Stake (PoS) and Proof of Work (PoW) blockchains and hosting on green servers.

8.2.6.5.3 Cost-Benefit Analysis

- **Benefits to Users:** End-users, including marginalized groups, receive efficient, inclusive, and privacy-respecting distribution of social benefits. The user-centric design and integration with blockchain for secure identity management create a platform with high social impact.
- **Benefits to Municipalities and NGOs:** Streamlined distribution of benefits, reduced administrative burden, and increased transparency and trust in social benefit programs.
- **Economic Viability:** The SaaS model, coupled with the project's scalable design, presents a sustainable economic model. Initial investments in development and deployment are offset by the potential for substantial annual revenues from municipalities and NGOs.

8.2.7 DID4EU

8.2.7.1 Market Analysis

The project is building the infrastructure for an emerging trillion-dollar market.

8.2.7.1.1 Market Dynamics

The market for digital / decentralized identity is quickly growing:

- Decentralized identity consolidates existing ID markets like authentication, access management, ID verification, background screening. Incumbents are adopting decentralized identity and approaching to handle the infrastructure
- Decentralized identity enables new use cases that have not (really) been possible like digital passports, reusable reputation, decentralized marketplaces/apps. Governments, businesses, web3 companies (DAOs, DeFi) need these solutions to build their use cases.

8.2.7.1.2 Market Size

The project is looking at a billion-dollar market opportunity, which can be illustrated in two different ways: top-down calculations based on market research and bottom-up calculation based on the business model and pricing combined with the potential target groups (users, customers).

Top-Down Calculation

Based on research conducted by different market research firms, it is understood that the potential market for decentralized identity solutions will be a 250-billion-dollar market. If the goal of becoming a market leader is achieved, it can be expected to capture at least 10% of the market, resulting in a 25-billion-dollar opportunity:

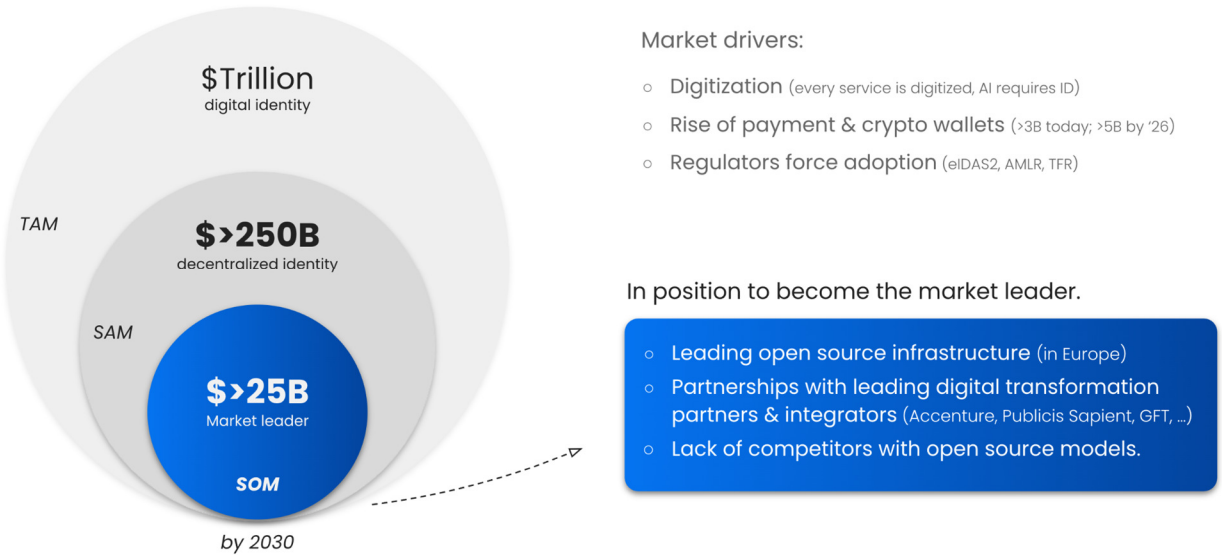


FIGURE 14. SOCIAL WALLET MARKET SIZE

Sources: Reusable Identity (Liminal Research), Grand View Research, Markets and Markets.

Bottom-Up Calculation

Aside from relying on market research, a simple calculation can be done based on discounted pricing that is already accepted by customers as follows:

- billion will have ID wallets
- 300 million organizations exist of which at least 30% will use ID wallets
- Trillions of devices exist of which at least 1 trillion will use ID wallets

Considering a pricing of $ 0.1 per wallet per year as well as 0.01 per credential issuance or verification as follows:

- 8B wallets * $ 0.1 = $ 800M / year
- 8B wallets are issued 10 new credentials / year * $ 0.01 = 800M / year
- 100M orgs verify 100 credentials / day * €0.01 = 36.5B / year

As a result, the project is looking at a +38 billion dollar market opportunity, excluding revenue from IoT.

Similarly, if it is assumed that there will be 100B daily interactions between people, organizations and things, the projection would be 35B revenue per year at an average interaction price of $0.001.

To sum up, even considering different methods for projections and pricing points, the project is looking at a +25 billion dollar market opportunity.

8.2.7.1.3 Market Drivers

The market is driven by macro trends e.g.:

- Digitization: As everything is moving digital, digital identity is becoming a big problem due to the limitations of existing approaches like federated identity.
- Adoption of payment wallets: Existing wallet infrastructure that can be used to roll out identity wallets quickly to billions.
- Rise of AI: AI is democratising online fraud and brings content authenticity problems
- Regulations: Regulators - led by the EU (eIDAS2) - force the adoption of identity wallets in public and private sector in 2024/25.

8.2.7.1.4 Target Market (SOM)

The solutions are B2B identity and wallet infrastructure for devs/organisations. Qualifications:

- GTM focus: Large buyers (SMEs adopt organically)

- Regional focus: EU (followed by US, APAC)
- Product focus: Vertical-agnostic infra for devs (not vertical-specific apps for anyone)

The project does not address markets like biometrics, traditional document or identity verification.

8.2.7.1.5 Competition

1. Overview

Competition mapped based on go-to-market strategy and organisational type:

FIGURE 15. SOCIAL WALLET COMPETITION

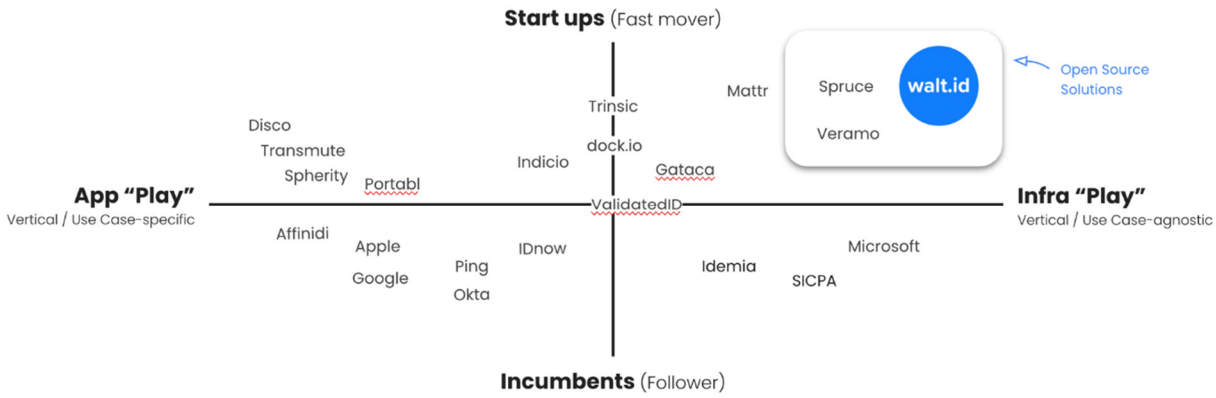


Table mapping open source competition:

		walt.id	HL Aries (AFJ)	Veramo
Model & Offering	Open Source	Yes	Yes	Yes
	Multi-Language / Platform	Yes	No	No
	Ease-of-use & docs	Industry-leading	Hard-to-use, incomplete docs (community maintained)	Hard-to-use, incomplete docs (community maintained)
	Custom development	Yes	No	No
	Support Contracts / SLAs	Yes	No (community maintained)	No (community maintained)
Products & Interop	ID Ecosystems	Agnostic (EBSI, DNS, LIs, Cheqd, custom, ...)	HL Indy	Agnostic (Indy, Ethereum, DNS)
	DID methods	>5 methods (extendable)	did:indy, did:key	>5 methods (extendable)
	Credential formats	Multiple (VCs, SD-JWTs, mDL, NFTs/SBTs)	AnonCreds, VCs	VCs
	Protocol	OIDC, DIDComm (partial)	DIDComm, OIDC (partial)	DIDComm
Deployment & Integrations	Multi-Cloud	Yes	Yes	Yes
	Keys (KMS) & Data Storage	Vendor Agnostic (Hashicorp, Oracle, MSFT, AWS, Thales ...)	Custom (HL Askar, lock-in)	Custom (lock-in)
Compliance	Standards (W3C, ISO, OIDF)	Yes	Partially	Partially
	EBSI & eIDAS2 (ARF)	Yes	No	No

Table mapping selected other (closed source) competitors:

		walt.id	Veramo	SpruceID	Trinsic	Mattr	Microsoft
Company	Team size / funding	12 / >1.5M *founded '21*	<5 *contributed to DIF*	>20 / >40M *founded '20*	12 / >8M *founded '19*	>70 / - *founded '19 (by Telco)*	<20 *Identity team*
	Strengths	best open source stack	first OSS JS stack	web3 community, funding	1st SaaS	size, funding	distribution
	Weaknesses	Team size, products not yet scalable	OSS project *(no company)*	no clear focus, founder / execs left	weak tech stack	expensive, rigid	slow, lock-in
Product	USP	holistic, customizable stack	Java Script	web3 focus (author of "Sign in with Ethereum")	Low-code, SaaS	R&D, standards	distribution, brand
	Regulated use cases, compliance	yes (#1 EU, #2 Global)	no	no	no	yes (#1 AUS/NZL, #2 EU)	yes (#1 US, #2 EU)
GTM	Open source	yes	yes	partly	no	no	no
	Initial regional focus	EU	US	US	no clear focus	APAC	US
	Customer focus	enterprise	web3	web3	SMEs	government	gov, enterprise

8.2.7.1.6 Detailed Analysis

The strongest competitors are open source frameworks (Veramo, Hyperledger Aries), SpruceID, Mattr and Microsoft. Here's why:

Veramo and Hyperledger Aries are main competitors because they are the only viable open source alternatives to walt.id (apart from SpruceID). Also, they are on the market for years.

Their main weakness is that they are *community-led efforts*, which creates various issues:

- Lack of focus and direction for developing new products and features

- No commercial organization to provide support contracts or legal assurances.
- No guarantee for ongoing compliance with laws and standards or maintenance and updates.
- Low quality of code, documentation and developer experience which creates friction for adoption and problems for (large-scale) product systems.

SpruceID is a main competitor because they are the only commercial decentralized ID vendor with comparable open source solutions. They initially focused on web3 and built a dev community around their work on the "Sign in with Ethereum" standard. Recently, they shifted focus from web3 to the US public sector e.g. providing an ID wallet for California. Finally, they've raised aggressively ($41.5M) to grow fast.

Their main weakness is a lack of focus: They invested a lot in a go-to-market strategy for web3 and launched several web3 products that are failing to translate into paying customers, while diverting attention/resources away from more promising opportunities. Also, they are facing high-employee turnover, lost a founder and several other key roles in 2023.

Mattr is a main competitor because they have the most holistic and robust solutions among all competitors. They are strong in RandD, involved in different standardization bodies and have deep technical expertise. Also, they are owned/financed by a telco (Spark, New Zealand) which allowed them to grow fast and supports their go-to-market activities in APAC (e.g. they've recently closed a large government contract with New South Wales, Australia).

Their main weakness lies in the closed source nature of their products and their expensive pricing which creates too much friction for developers and early adopters. As a result, Mattr cannot rely on organic, bottom-up adoption or build a developer community and is unnecessary limiting its market (to large public sector buyers).

Microsoft is a main competitor because of their brand, size, existing customer base and distribution channels (e.g. Entra, Azure, Authenticator).

The main weaknesses lie in its corporate nature: It is slow to adopt new features and launch new products as identity is not a top priority within the company. Moreover, Microsoft's products have a poor developer experience (based on previous work with MSFT) and are tightly integrated with their own technology stack. Microsoft is not building a vendor-agnostic solution that caters to customers' needs for using competing services (e.g. cloud, key management). Finally, their products are closed source (see resulting problems from the analyses of "Mattr") and not aligned with open standards or upcoming regulations creating interoperability and compliance issues.

Note that, one of the customers already uses the products *in addition to* Microsoft. They need walt.id for various reasons:

- Need for different deployment options (on-prem, multi-cloud, hybrid). Microsoft is only available via Microsoft's cloud ("Azure") and IAM solution ("Entra").
- Need for flexibility and control over key management or data storage. They must prevent lock-in and be able to mix/switch between different solutions (KMS, cloud) depending on business and regulatory requirements.
- Need for technologies not offered by Microsoft (e.g. mDL, NFTs).
- Need for solutions compliant with open standards to ensure interoperability between different systems/apps. Microsoft is not following most standards.
- Need for dedicated support, which is not offered by Microsoft.

Other competitors include:

Trinsic was the first company to launch a decentralized ID and wallet solution SaaS platform. They're building low-code tools for startups/SMEs and have raised $8.5M.

Their main weakness is their product, which is closed source and not fit for enterprise customers (e.g. due to a lack of flexibility for key management or data storage, lack of customizability to fit diverse requirements). Moreover, their cloud platform creates lock-in effects and is not certified. *(To use an analogy from the CRM industry: While walt.id is building "Salesforce", Trinsic is building "Pipedrive".)*

Dock.io was the first decentralized identity company to launch their own blockchain. They have a solid team and raised $20M via an ICO in 2019. Their main weaknesses stem from the fact that they run their own blockchain, which creates strategic problems: First, they cannot offer customers a blockchain-/technology-agnostic solution, which customers require. Second, running a blockchain and managing investors diverts attention from building identity products. Finally, they're products are closed source.

IDnow is an company offering traditional ID verification (KYC/AML) and digital signatures (eSignatures/eIDAS). As a result, they have experience with relevant regulations (eIDAS, AMLR) and an existing customer base (mostly banking and financial services). Recently, they launched their first decentralized ID product (ID wallet). Their weakness is their lack of technical expertise about decentralized identity. (This information is based on experience from a client project. Also, their ID wallet was not built in-house, but by "Accenture".) Additionally, they have a lack of strategic priority/urgency. (They are hesitant to cannibalize their existing business too quickly.) As a result, they move slowly.

SICPA was one of the first enterprises to offer decentralized ID and wallet infrastructure solutions. They are well funded and have a strong public sector network. (The company sells special ink required for printing money to governments.) Their weakness lies in their corporate nature: SICPA is moving slowly and inefficiently. Their solutions are closed source and expensive. Also, identity is not a strategy priority within the company (their ID products are not even mentioned as "solutions" on their website).

Ping and Okta are large vendors of ID and access management (C/IAM) solutions for businesses. As such, they focus only on the *verification* of ID credentials. They benefit from a large client base to which they can upsell decentralized ID products (for credential verification). They're different from walt.id in that they do not offer a vertical- and use case agnostic infrastructure. As a result, their products are limited to use cases related to customer or employee access management. Moreover, they don't have competing products for ID credential issuance or ID wallets. Similarly, they don't offer a solutions for non-human identity (e.g. of organizations, things, agents). Finally, their solutions are closed source.

Apple, Google, and Samsung are focused on consumer-facing wallet apps. They have no competing products for business and government customers. Note that the project is not even directly competing with them on the level of wallets. Instead, it enables banks, telcos, payment or tech companies to launch their own wallet apps and compete with Google, Apple, and Samsung.

8.2.7.1.7 Unique Selling Points:

The most holistic and flexible enterprise-grade open source infrastructure for decentralized ID.

Open-Source: The project built the best open source stack on the market because an open source strategy is the most effective way to become the de-facto industry standard and capture market leadership. Open source unlocks fast, organic bottom-up adoption (via developers), while facilitating enterprise sales (enterprise buyers prefer open source). Finally, developers love open source companies, making it easier to hire key talent.

Note that, there are only three competitors with an open source strategy: Veramo, HL Aries, SpruceID.

All-in-One: The project is the only vendor to support all major identity "flavours" or technologies (like Verifiable Credentials, mdocs/mobile driver's licence, selective disclosure, NFTs/SBTs), enabling customers to build any end-to-end use case in any industry with a unified solution.

Infrastructure Play: The focus is on building the most powerful infrastructure for developers (libraries, SDKs, APIs). The products are vertical-agnostic and focused on creating value for organisations who build vertical-specific applications and use cases.

A number of players look like strong competition (Ping, Okta, Apple, Google…) but are actually building vertical- or use case specific "off-the-shelf" solutions and focus on the application layer. As a result, they are not directly competing with the organization, but with its own customers who are building vertical or use case-specific applications.

Compliance: The products are aligned with new laws (like eIDAS2), with industry-leading expertise in this area and a unique network of policy makers and experts providing relevant insights. (The founders built this network since 2019 and co-authored

specifications for the EU and Member States which were adopted by EBSI and eIDAS2.) In addition, the company was the first to comply with all relevant technology standards (W3C, ISO, OIDF…) thanks to collaboration with standardization bodies. Note that, most competitors (Veramo, SpruceID, Mttr, Microsoft, Indicio, Trinsic, Dock, Ping, Okta) are not focused on the EU market (eIDAS2). As a result, they lack expertise about regulations and generally don't have aligned products. Standards: When starting the company in 2021, a set of standards was picked that has turned out to dominate the market today. Most competitors (e.g. HL Aries, Trinsic, Indicio) bet on a different set of standards, which have become irrelevant. As a result, many competitors are rebuilding their technology stack.

Flexibility: The project offers the most flexible solution on the market:

Customization: The modular products are easily extended to meet diverse client needs.

Multi-platform: The products work on every platform and with any language.

Deployment: The products can be deployed on-premise or in any cloud.

3rd party solutions: The products abstract various external services (PKIs, KMS, data storage, apps…) enabling clients to use different solutions and prevent lock-in.

For example, large enterprises or governments have regulatory or business requirements related to deployment options (in-prem, multi-cloud, hybrid) or technologies (KMS, data storage…). They require an open, customizable tech stack.

The reasons for winning:

Macro Perspective

Digital identity will be ubiquitous. It will become a commodity and costs will go to zero. As a result, the only way to make money is via the "masses" - from governments and large enterprise buyers to startups and SMEs. The goal is to become the *defacto standard*. Building the best (enterprise-grade) *open source* solution is the fastest way to get there.

Micro Perspective

On an operational level, the open source strategy creates a number of competitive advantages:

- People: Developers love open source companies, which gives an advantage to hire key talent over closed source competitors.
- Go-to-Market: Open source software attracts developers and drives organic bottom-up adoption from SMEs and large buyers. Customers naturally start with open source products, but require the enterprise solution (license) and/or support (annual fees) when they move to production. Also, enterprises and governments prefer (or even require) open source software.

- Product: By open sourcing the products, the company attracted thousands of developers and is building a community that provides valuable feedback to improve the products. Moreover, by building an abstraction layer based on open standards, the company maximizes interoperability for customers and allows them to use a diverse set of external services (e.g., key management, data storage, signatures, business applications like IAM tools).
- Pricing: By open sourcing the products, the company can undercut closed source competitors and take their market share. For example, organizations with restrained budgets - like startups, SMEs or large organizations who are just starting to adopt and do not yet have the required budgets - will typically pick an open source solution, everything else being equal.

In a nutshell

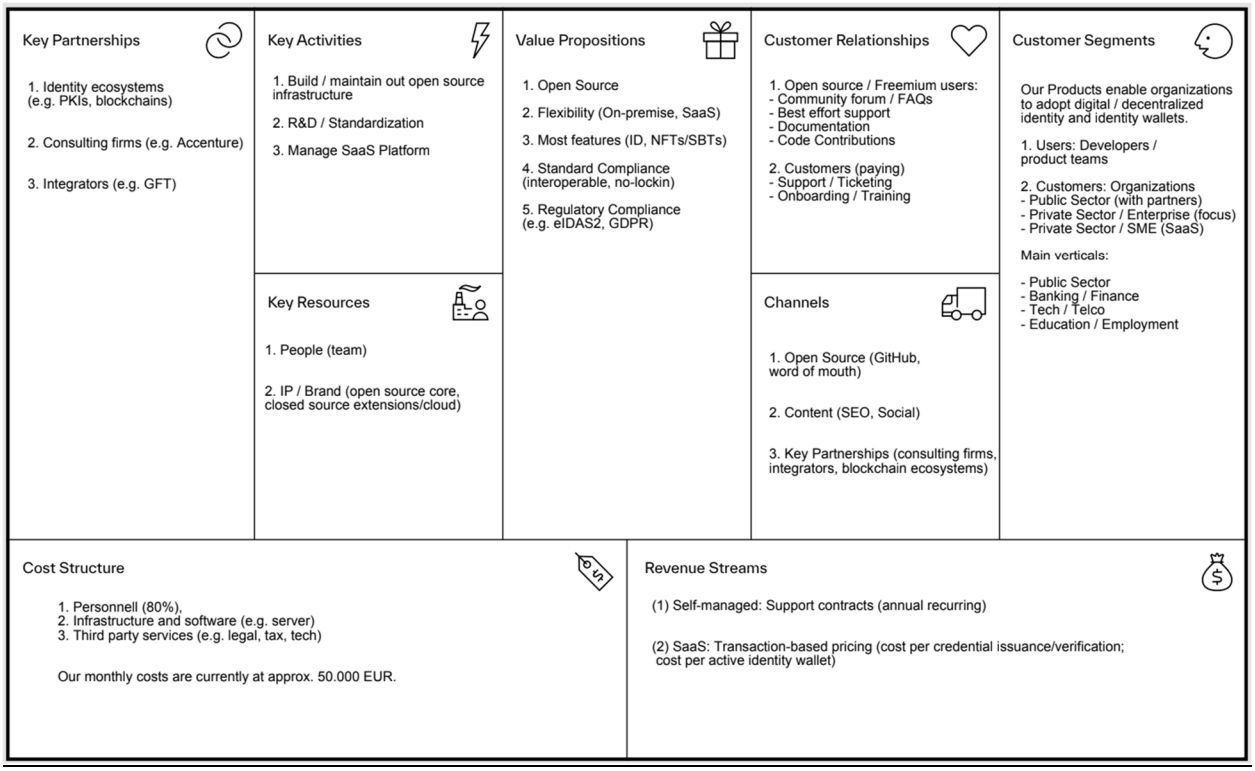
The reasons for winning against competitors, broken down:

- Veramo, HL Aries, Spruce → The company builds better open source products.
- Mattr → The open source strategy is better suited for becoming the de-facto industry standard. Their closed source approach and high prices create too much friction for adoption.
- Microsoft → The company moves faster, comply with standards and prevent lock-in (cloud, KMS...).
- Trinsic → The company is an easy choice for large buyers (Trinsic's products are built for SMEs). At the same time, it captures market share from their target segment, as SMEs often prefer OSS over closed-source solutions.
- SICPA: The company moves faster, are more effective and benefit from more traction via OSS.
- Dock: They're distracted by their blockchain, create lock-in and don't comply with new laws.
- IDnow: They move too slowly, lack expertise and urgency.
- Ping / Okta: Limitation to C/IAM-related uses cases ("credential verification").
- Apple / Google: Limitation to consumer-facing apps ("ID wallets")

Finally, none of these competitors (except IDnow) are focused on the *European market*.

8.2.7.2 Business Model

8.2.7.2.1 Canvas



8.2.7.2.2 Overview

"Open Core" and "Hosted Service" models are combined.

- Core products are open source to drive adoption and close support contracts.
- Enterprise features are offered via a licence to scale pricing for large, self-managed clients.
- The products are offered via a SaaS platform to facilitate adoption with scalable pricing.

This model has been proven by billion-dollar companies with similar products like Hashicorp.

8.2.7.2.3 Strategy

The company believes that identity will become a commodity, required by every organisation. As a result, the biggest opportunity is the market for developer infrastructure that enables organisations across industries to build products and use cases.

The goal is to be the de-facto standard for this segment, which is best served by the model:

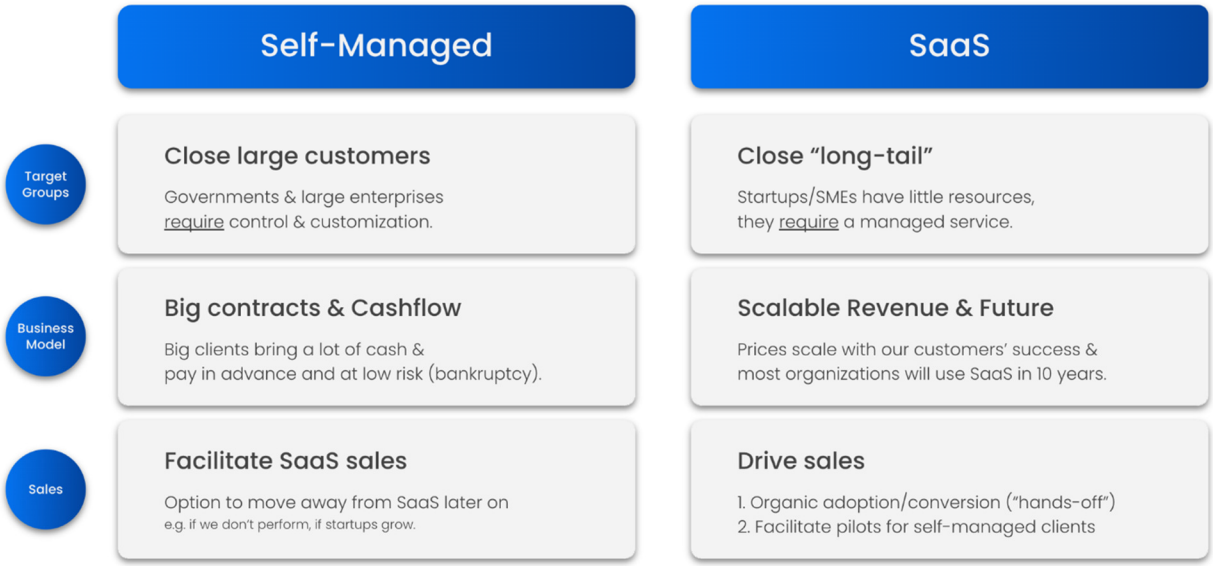
- Go-to-market: The company is fastest to market because open-source products enable bottom-up adoption and facilitate enterprise sales, as large buyers prefer open-source software.
- Pricing: Closed-source competitors, particularly those targeting small buyers, are undercut. Additionally, more revenue is brought in through support contracts than through "pay-as-you-go" pricing in the early market.
- People: Building open-source software allows for hiring great talent (devs love OSS).
- Proven by others: Companies like Hashicorp or MongoDB have comparable businesses and became billion-dollar successes following the same model.

Finally, by committing to open source early, it becomes more difficult for open-source competitors to emerge, as they typically do for foundational technologies that become commoditized.

8.2.7.2.4 Self-Managed vs. SaaS

Different product editions are offered to customers to support various deployment options:

- Self-Managed: Most of the customers (particularly large buyers) prefer to self-manage the products and deploy them on-premise or in their own cloud or hybrid environments. This flexibility and the fact that customers can "own" the products allow for closing large accounts and generating cash flow through renewing annual support contracts, which are paid in advance.
- SaaS: Later this year, a managed service will be offered to customers to expand monetizable customer segments, facilitate sales, and introduce a scalable pricing model.



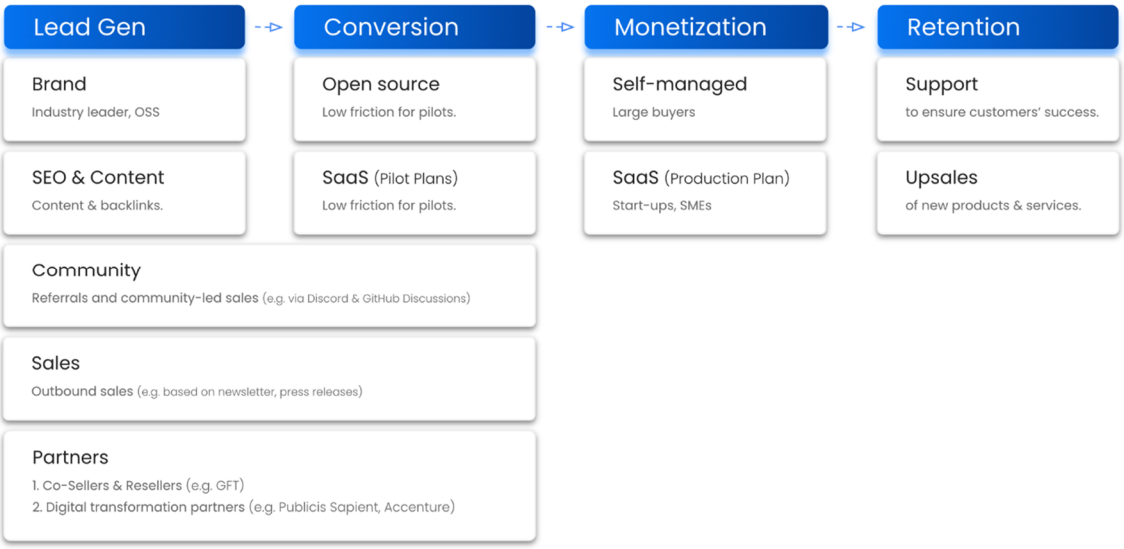
8.2.7.2.5 Adoption / Conversion

Over the year, the following repetitive adoption pattern has been observed:

- Customers start with the open source solutions to build pilots and evaluate tech.
- Once customers move to production, they need support contracts and often require the licensed enterprise products.

Later this year, the SaaS platform will allow for the expansion of monetizable customer segments by

- offering open source users a cheap alternative to self-managing the products
- attracting buyers with limited resources (cannot self-manage) or small budgets (SMEs).



8.2.7.2.6 Distribution Partners

A proven multi-channel go-to-market strategy is followed, supported by partners:

- Technology partners for co-selling
- Integrators for reselling
- Digital transformation partners for large scale projects

8.2.7.3 Pricing

Self-Managed

		Open Source Free	Support & License starting € 25.000 / year
General Limitations	Products	Community Stack	Community Stack or Enterprise Stack (license)
	Multi-Tenancy	-	Yes
	Audit logs	-	Yes
Product Limitations	UX	-	Dashboard, analytics
	Features	Core features	Enterprise features
	Integrations	Limited	KMS, data storage, IDVs, ...
	Compliance (eIDAS2)	-	Yes
Service Limitations	Onboarding	-	Yes
	Support	Community	Business hours
	SLA	-	Optional

Users require support for production systems (>25k p.a.) & licenses allow for scalable pricing.

The Enterprise Stack (licence) targets: Large buyers (via enterprise features, integrations, ...) *and* "Enablers" (via multi-tenancy, audit logs, ...).

Cloud (SaaS)

		Free	€ 99 / month	starting € 1k / month
Usage Limitations	Purpose	Pilots	Pilots	Production
	Credentials (issue, verify)	250	10k	Unlimited
	Wallets (active)	10	100	Unlimited
	Seats	1	3	Unlimited
Product Limitations	UX	-	Analytics	Audit logs
	Features	Minimum	Limited	Unlimited
	Integrations	-	-	KMS, data storage, IDV, ...
Service Limitations	Onboarding	-	-	Yes
	Support	Community	Best Effort	Business hours
	SLA	-	-	Optional

Freemium allows organic adoption. Pricing forces users to pay for production use.

8.2.7.4 Traction

Selected KPIs around traction and revenue:

The products are used by >9k developers and organizations - growing at >500% (YoY).

More than 700k in revenue has been generated, with a growth rate of over 700% year-over-year (YoY).

Annual recurring revenue (ARR) increased from "0" to 200k, with an average customer value of 32.5k.

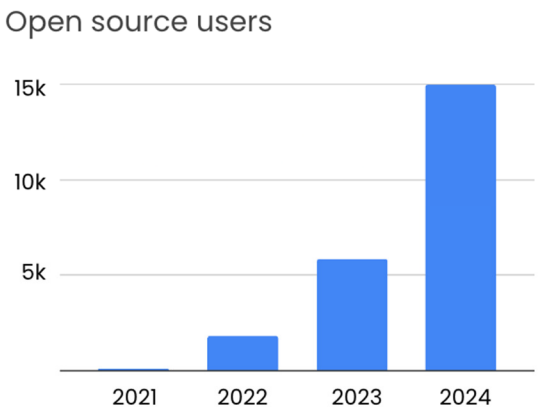
90% of all leads and more than 75% of all revenue is inbound.

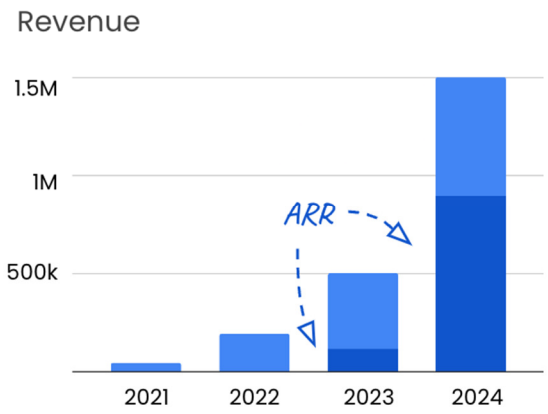
Distribution partnerships were established with digital transformation giants like Accenture and Publicis Sapient, and the first reseller agreement was closed with an integrator (GFT).

The following graphic shows traction and revenue KPIs:

User and Revenue Projections

Based on current traction and business model, the following growth projections until 2024 (first graphic) and 2026 respectively (second graphic, PandL) were created:





Income	2021	2022	2023	2024	2025	2026
Revenue						
Revenue	42,635	195,000	502,631	*1,000,000*	*4,000,000*	*14,500,000*
ARR (cumulative)	0	0	120,000	*897,000*	*3,750,000*	*14,300,000*
Self-managed (Support)	0	0	120,000	*625,000*	*2,000,000*	*5,500,000*
Self-managed (License)	0	0	0	*100,000*	*750,000*	*2,500,000*
SaaS (Subscription)	0	0	0	*172,000*	*1,000,000*	*6,300,000*
Grants						
Grants	109,214	189,696	392,891	*575,512*	*271,860*	*42,583*
Total Gross Profit	**151,849**	**384,696**	**895,521**	**1,575,512**	**4,271,860**	**14,542,583**

Operating Costs	2021	2022	2023	2024	2025	2026
People (Salaries)	140,208	460,243	594,921	*1,000,000*	*2,000,000*	*7,500,000*
Headcount (EO Year)	5	10	11	20	40	100
GTM (marketing, sales)	0	10,614	9,009	*50,000*	*250,000*	*750,000*
Contractors (hr, legal, tax)	47,734	63,231	72,158	*100,000*	*150,000*	*250,000*
Software, Hardware, Cloud	6,381	18,434	25,522	*100,000*	*600,000*	*1,200,000*
Office, Team Retreats	539	7,154	4,238	*30,000*	*100,000*	*250,000*
Total Operating Costs - Cash Flow	**194,862**	**559,677**	**705,848**	**1,280,000**	**3,100,000**	**9,950,000**

EBIT	**-43,013**	**-174,981**	**189,674**	**295,512**	**1,171,860**	**4,592,583**
Burn rate	**-3,584**	**-14,582**	**15,806**	**24,626**	**97,655**	**382,715**

Investments	2021	2022	2023	2024	2025	2026
Pre-Seed	410,000	-	-	-	-	-
Seed	-	-	-	*2,500,000*	-	-
Cash position - including Seed	**366,987**	**192,006**	**381,679**	**3,177,191**	**4,349,050**	**8,941,634**

8.2.8 IM4DEC

This is the final version of the business model and exploitation plan for the IM4DEC project.

8.2.8.1 Business Model Description

The Digital Emergency Communication Association has been diligently working on offering an effective solution for deaf individuals to enable them to engage in emergency chats. The service, as detailed on https://DEC112.at, addresses the need for accessible communication in emergencies, ensuring safety and inclusivity. With EU Regulation 2023/444 coming into effect, the business model is well positioned to fill a critical gap in emergency services.

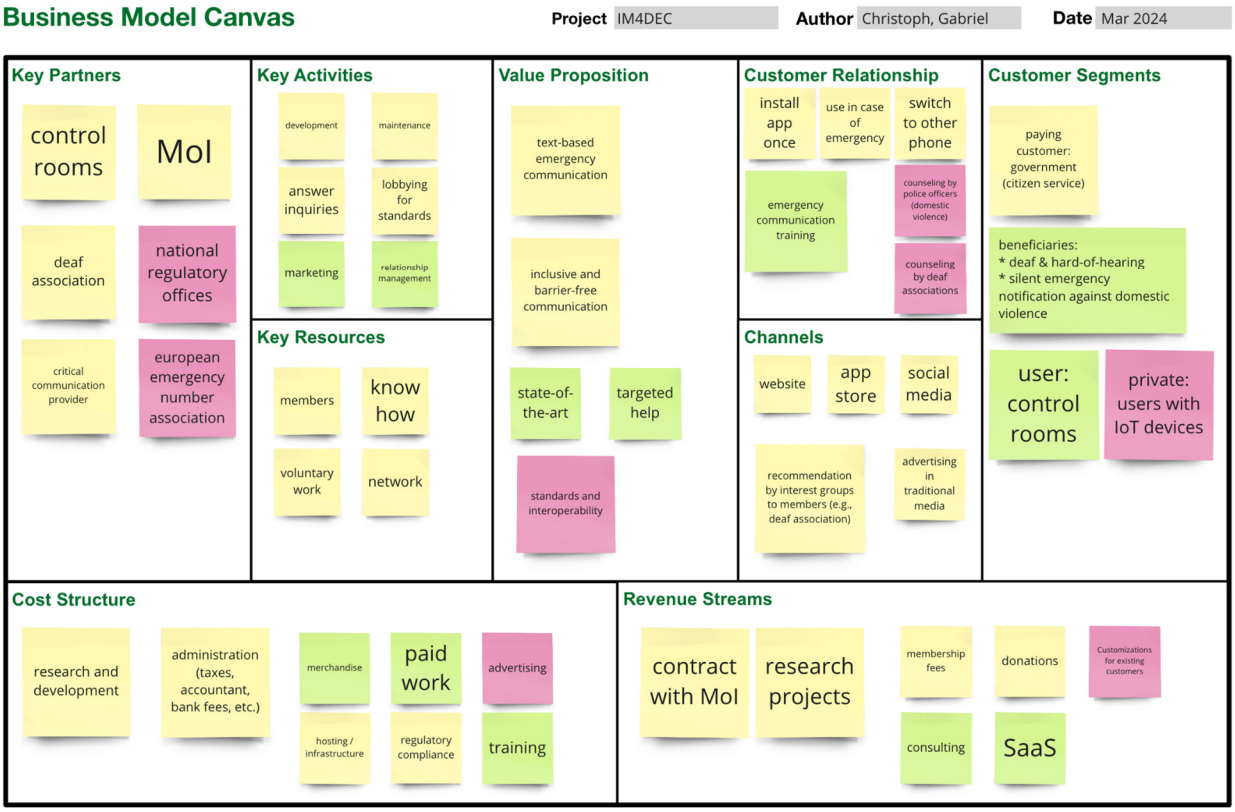


Figure 5.1: Business Model Canvas

The Business Model Canvas depicted in Figure 5.1 is the result of multiple team sessions to provide a comprehensive few of the business aspects of DEC112. Specifically, cost and revenue streams were discussed, and the remainder of the chapter provides a more detailed elaboration.

Below are the most relevant cost streams in the business model:

- Research and Development: to ensure that the service continually meets the needs of its users
- Infrastructure Maintenance: to maintain the servers, databases, and ensure the chat system's uptime
- Training & Outreach: to educate emergency service providers and the deaf community about the functionality and benefits of the platform
- Regulatory Compliance: ensuring the chat system is compliant with the EU Regulation 2023/444 and other pertinent regulations

These are the primary revenue streams:

- Licensing: partnering with emergency service providers and charging a licensing fee for integration into their systems
- Partnerships: partnering with device manufacturers to integrate the system directly, offering them a compliant solution
- Grants & Donations: as a solution catering to a specific community, there are opportunities for funding through grants and donations

8.2.8.2 Economic Analysis

Focusing on potential customers, the service targets a niche yet vital segment: around 1.8 million individuals who are deaf or are hearing impaired in Austria. However, the scope of the service transcends this group, extending to all Austrians who might find themselves in situations where a silent or text-based emergency call is necessary. This broadens the potential customer base significantly, encompassing the entire Austrian population.

When considering competitors, the landscape in Austria appears moderately competitive. There are a few organisations offering similar services (app-based emergency calling), but their number is limited to single digits. Furthermore, all competitors are just collecting additional data to an emergency, while still calling the emergency number via traditional phone call, whereas DEC112, in contrast, uses a multimedia IP infrastructure to forward emergency calls. This also allows for a direct integration of services into the respective emergency response centres, where DEC112 has already 6 control rooms connected, serving all 9 federal countries and covers fire, ambulance, police and mountain rescue services.

Regarding the role of partners, alliances have already been forged or are anticipated with a variety of entities, including emergency response centres, associations like the Deaf Association of Austria, and key organizations such as the Federal Ministry of the Interior (BMI) and the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR). These partnerships will not only extend reach but also enhance credibility and operational efficiency. Combined with the fact of being a non-

profit association, driven by innovation and not profit, DEC112 has already grown to an established entity in the Austrian landscape of emergency calling.

8.2.8.3 Business Value for the Blockchain and SSI Domain in General

The integration of Blockchain and SSI (Self-Sovereign Identity) offers enhanced security, transparency, and user control in emergency communication. Using decentralised systems, the platform can ensure user privacy and data integrity. Furthermore, as Blockchain and SSI continue to gain traction across various sectors, the project starts now to integrate the emergency communication with other platforms to create a cohesive, interoperable ecosystem, ensuring efficient and secure emergency communication.

As a very concrete contribution to the SSI domain, a collaboration between OwnYourData and the UniResolver was initiated in the course of the project to provide DID Rotation for all DID methods. Through initial discussion in the DIF WG-ID bi-weekly calls it was agreed that an adapted resolution process for DID Rotation should be implemented right in the UniResolver.

8.2.8.4 Business Value and Relevance for TrustChain

What is the link between your business and TrustChain?

TrustChain focuses on creating decentralised, transparent, and user-friendly digital services. The emergency chat system can leverage TrustChain's services to ensure that the communications between the help-seeking individual and the emergency services are secure, transparent, and incorruptible. The ongoing project evaluates the trustworthiness and dependability of other TrustChain services that might be integrated.

As a first tangible result an integration with the Sphereon Wallet was implemented and demonstrated: Users with a DEC112 Credential are now enabled to trigger a Silent Emergency Notification from the login screen.

What would the value exchange be?

For TrustChain, partnering with the solution provides a real-world use case, demonstrating its versatility and applicability in emergency services. It further strengthens TrustChains position as a leader in the domain. In return, the platform benefits from the network and available know-how of the TrustChain community.

8.2.9 WIDE

The business model of WIDE, including its financial strategy, is described in this section. The account focuses on describing revenue streams, to ensure covering both growth and sustainability considerations for an application that operates in a risky market like the digital identity sector. WIDE's approach is designed to adapt to regulatory changes

and market demands. The main risk of its early stage business model is the reliance on grants and funding to subsidise investments in the improvement and scaling of its infrastructure. WIDE addresses this risk by taking grant engagements as an opportunity to invest in research and development to diversify its offering. To that end, WIDE is actively developing additional revenue avenues, including SDK partnerships, system integration consultancy, and educational workshops, aiming to strengthen its cash flow and liquidity. Future plans include the introduction of B2B subscriptions, capitalising on WIDE's market presence and expertise. This strategic expansion is complemented by project-based funding, as open applications for a grant from the IOTA Foundation and the Qatar Research and Development Innovation (QRDI) Council Grant highlight.

8.2.9.1 Revenue Streams

WIDE's financial approach is tailored to address the evolving digital identity sector and comply with regulatory changes, ensuring both growth and sustainability. Currently, open grant applications serve as the primary revenue source, crucial for supporting ongoing research and development. However, additional revenue streams, such as consultancy services and educational workshops, are actively being developed for the near future, alongside the exploration of B2B subscriptions. These initiatives leverage WIDE's expertise and market presence, aimed at reinforcing the financial base and advancing the objectives in digital identity management.

8.2.9.2 Value Proposition

8.2.9.2.1 Systems Integration and Consultancy Services

WIDE provides custom integrations for enterprise customers, which are offered in conjunction with consultancy services aimed at facilitating the adoption and integration of digital identity solutions across both the private and public sectors. Leveraging the deep expertise in digital identity technologies, WIDE offers strategic guidance, compliance assurance, and technical integration support tailored to the distinct needs of each sector. For public sector entities, the consultancy will focus on navigating digital transformation initiatives within the context of governmental regulatory frameworks, addressing unique challenges such as data privacy, security, and citizen engagement. This comprehensive consultancy service aims to position WIDE as a key enabler of digital identity infrastructure development, fostering partnerships that drive innovation and compliance across sectors.

8.2.9.2.2 Educational Workshops

Educational workshops form a core component of the strategy to enhance understanding and application of digital identity practices among varied demographics. These workshops are designed to cater to a wide range of participants, from individuals seeking basic knowledge of digital identities and digital wallets to professionals looking for advanced insights into the WIDE solution and its potential

applications. Recognizing the diverse backgrounds and needs of the audience, workshops will be varied to ensure accessibility and relevance, incorporating hands-on sessions that foster familiarity with WIDE solutions. Special attention will be given to adapting content and delivery methods to suit different demographic groups, enhancing participants' ability to understand and leverage digital identity solutions effectively.

8.2.9.2.3 Subscription Models

In the future, B2B subscriptions will emerge as a key revenue stream for WIDE, offering various tiers of service to meet the diverse needs of businesses and public sector organisations. From basic access to advanced features and dedicated support, each subscription tier is designed to deliver value that aligns with the specific requirements and scales of operation of clients. This model encourages sustained engagement and investment in digital identity solutions, underpinning long-term relationships and a steady revenue flow for WIDE.

8.2.9.3 Pricing Strategy

WIDE's pricing strategy is integral to its service offerings, aligning with the dynamic digital identity management sector and ensuring both growth and sustainability. This strategy capitalises on WIDE's technical prowess and expert positioning in the market to provide value across various client segments.

8.2.9.3.1 Systems Integration and Consultancy Services

The system integration and consultancy services adopt a segmented pricing approach to accommodate the financial scope and specific needs of diverse clients, from nascent ventures to well-established enterprises. System integration contracts typically involve a flat fee and additional consultancy based on the below fee schedule.

Table 3: Hourly Pricing of Systems Integration and Consultancy

Segment	Indicative Pricing (EUR/H)
Pre-seed stage companies/ Public sector	45-60
Start-ups	50-75
Scale-ups	75-130
Enterprise	150-200

8.2.9.3.2 Educational Workshops

Educational workshops offer variable pricing to ensure the inclusion of various demographic groups, fostering a comprehensive understanding of digital identity solutions.

Table 4: Workshop Pricing

Segment	Pricing	Notes
Varied	Starting at EUR 800 per person day (4h on-site)	Pricing varies based on workshop length and content complexity

8.2.9.3.3 WIDE as a Service (WaaS)

WaaS pricing is structured to serve an array of institutional clients, from individual verifiers to larger institutions, ensuring WIDE's solutions are accessible and scalable.

Table 5: WIDE-as-a-Service Price Structure

Subscriptions / Bundles	Number of Transactions	Price (EUR)
Basic	1x transaction	0.01
Standard	100x transactions	8.99
Premium	1,000x transactions	69.69

8.2.9.3.4 Freemium Model - For Holders

A freemium model underpins the user growth strategy, offering free access to basic features while monetizing advanced functionalities.

Feature	Price per month (EUR)
Multi-Device Access	3.99
Storage of more than 100 claims	4.99
Storage of more than 1,000 claims	29.99

Table 6: Freemium Pricing of WIDE for B2C Segment

8.2.9.3.5 B2B Subscriptions

The B2B subscription model is planned to introduce tailored service plans that align with the varying needs and capacities of the business clients.

Service Offering	Segment	Pricing Structure	Notes
B2B Subscriptions	Basic Plan	Tiered Pricing	Rates to be determined
B2B Subscriptions	Standard Plan	Tiered Pricing	Rates to be determined

Table 7: B2B Pricing Structure of WIDE

8.2.9.4 Financial Projections

The financial projections for the next three years are crafted to align with strategic goals, emphasising sustainable growth, operational efficiency, and strategic investment. The projections account for revenues primarily from grants in the first year, with expected growth in revenue through diversification and scaling of operations in subsequent years. Expenses are tightly managed, focusing on optimising salaries, regulatory compliance, and minimal marketing expenses to ensure a path towards profitability.

In the initial three years, the financial projections of WIDE are grounded in achieving sustainable growth and operational efficiency, heavily reliant on grant funding. Notably, these projections do not account for revenues from Wallet as a Service (WaaS), Freemium, and Subscription models. The exploration and integration of these models are deferred to after the three-year setup phase, allowing for the prioritization of scalability and market adaptation. This strategic choice ensures the immediate focus remains on establishing a solid foundation, thereby facilitating a more effective expansion into diverse revenue streams in the future.

8.2.9.5 Economic Analysis

Utilizing a 10% discount rate, a forward-looking estimate of the project's profitability is examined. This rate is chosen based on:

- Risk Assessment: Reflecting the inherent risks of early-stage tech and innovation projects and acknowledging potential uncertainties.
- Opportunity Cost: Representing the cost of investing in WIDE versus alternative investments, serving as a benchmark for expected returns.
- Industry Standard: A common rate in startups and technological innovations, balancing optimism with market realism.

Year 1-3 Cash Flows:

- Year 1: Grant funding of €201,600 covers exact expenses (OPEX and CAPEX), resulting in a net cash flow of €0.

- Year 2: Grant funding is estimated to double to €403,200, precisely matching the estimated OPEX and CAPEX of €409,300, leaving a negative surplus (i.e. shortfall)

- Year 3: Funding is estimated to double again to €806,400, covering the detailed expenses of €627,000, leaving a positive surplus.

Therefore:

Grant Funding:
- Year 1: €201,600 (Matching expenses)
- Year 2: Double Year 1 → €403,200
- Year 3: Arithmetic Mean of Double Year 2 and Triple Year 1 → €705,600

Surplus Calculation:
- Year 2 Surplus: Grant - Expenses = €403,200 - €409,300 = -€6,100 (Shortfall)
- Year 3 Surplus: Grant - Expenses = €705,600 - €622,000 = €83,600

Considering the above cash flows with Year 2's slight shortfall and Year 3's surplus:

1. Year 0 (Initial Investment): -€201,600
2. Year 1 Cash Flow (CF1): €0 (Break-even)
3. Year 2 Cash Flow (CF2): -€6,100 (Shortfall)
4. Year 3 Cash Flow (CF3): €83,600 (Surplus)

$$NPV = € - 146{,}171.08$$

While a negative NPV may indicate a lack of rentability, it is important to consider that the NPV represents the project at a pre-production level exclusively financed through grants. Given the long-term business model described herein, the team expects the NPV to change drastically with product-market-fit and its shift to production.

ROI for Year 3:

$$ROI_{Year\ 3} = \frac{€83{,}600}{€622{,}000} x\ 100$$

ROI (Y3) = 13.44%

The negative NPV at the end of year three suggests that when the initial investment and subsequent cash flows are discounted back to their present value, the total costs still surpass the total benefits. This reflects the high upfront costs typical in technology ventures where the payoff is long-term.

Even though the NPV is negative, the positive ROI in the same period indicates the project is starting to see some operational success. This may seem counterintuitive, but it is not uncommon in practice. ROI measures the efficiency of individual years'

investment returns, and a positive figure in the third year signals that the project is beginning to generate a return on that year's operations.

The strategy behind WIDE's financials involves a phased approach. Initially, the project's operations are heavily dependent on external funds and grants. This allows WIDE to focus on development and growth without the immediate need for profitability. It's anticipated that during the first three years, income will not come from the core business operations but rather from these external funding sources.

As the project moves forward, the aim is to leverage these funds to establish a presence in the market and to begin capturing value from various activities such as tenders, grants, and other projects. This phase is also used to actively work towards market adoption and laying the groundwork for future revenue streams.

Post the initial three-year period, the business model is expected to evolve. The intention is to have established enough of a market presence and product maturity to start generating revenues through the core business operations. This is when the diverse streams of income—beyond just grants and funding—are expected to take place, which should reflect positively in the financials.

The Break-Even point is conceptually achieved annually due to the project's structured grant funding model, which aims to match or exceed expenses each year. Specifically, Year 3's surplus following the break-even in Years 1 and 2 illustrates a fiscal strategy designed to sustain operations and invest in growth, eventually leading to profitability.

The CBA broadens the scope of the analysis to include societal benefits and costs, capturing the holistic impact of WIDE. This impact is discussed and described at length in section seven, using the PESTEL framework. While the impacts of WIDE can be described in even more depth, some of the impacts are not yet final and an extended analysis herein would preclude WIDE from measuring its full impact in terms of benefits and costs to society. Thus, the analysis in section seven is particularly focused on the potential shift in societal norms that the widespread adoption of WIDE's solutions may induce.

WIDE's financial strategy throughout the initial three-year phase is meticulously planned to support operational scaling and technological advancements, underpinned by a number of grant funding. The approach, focusing on essential operational and capital expenditures, demonstrates the project's adaptability and foresight in financial planning. Year 2, characterised by a careful balance of expenses, and Year 3, yielding a notable surplus, which highlights the project's financial resilience and potential for significant growth

The Net Present Value (NPV) analysis, considering the projected cash flows, showcases strategic planning acumen, effectively balancing the initial investments against the anticipated surplus in Year 3. This surplus not only affirms operational efficiency and strategic utilisation of grants but also signifies a pivotal move towards financial sustainability and long-term profitability. Further, the Return on Investment (ROI) calculation, incorporating Year 3's surplus, alongside a detailed Break-Even analysis,

offers a comprehensive insight into WIDE's fiscal health. These analyses confirm the dedication to sound financial management and strategic development, underlining the project's capacity to generate substantial value within the digital identity sector.

8.2.9.6 Market Adoption and Expansion Strategies

In this section, WIDE's strategic approach to market adoption is outlined. It uses a phased and focused methodology to secure market share within the digital identity sector. Recognising its position as a relatively small player, WIDE opts for a strategy that prioritises depth over breadth by targeting niche segments where it can achieve deep market integration without directly confronting the challenges posed by larger, established entities like Bundesdruckerei and Idemia.

Initial efforts are concentrated on DAOs, a strategic choice reflecting WIDE's assessment of current market gaps and opportunities, particularly in providing DAO-compatible identification solutions that are presently lacking. This strategic approach to market entry is underpinned by a reliance on partnerships rather than extensive marketing, tapping into existing contacts and networks within Web3. There, professional and private identities often intersect and WIDE can enhance user engagement with WIDE's solutions. Later on, in this subsection a segment analysis shows WIDE's ambition to extend its reach beyond the DAOs, aiming for broader application within the Web3 sector and eventually across the digital economy. This ambition is supported by a nuanced understanding of the market, identifying critical segments such as educational institutions, crypto communities, and both public and private sector organisations.

Each segment presents unique demands and opportunities, from enhancing administrative efficiencies in educational settings to addressing the cutting-edge security and privacy needs of the crypto sector. WIDE's strategy also acknowledges the importance of user-friendliness and privacy across all demographic groups, aiming to foster digital literacy and platform utilisation widely. Strategic targeting and planned expansion are central to WIDE's approach, leveraging customised solutions, collaborative partnerships, and community engagement to ensure its platform meets the diverse needs and expectations of users in an increasingly digital world.

In the following, the plan for market adoption is presented. Then, the market segmentation is explained, using both use cases and personas as a reference. Afterwards, the strategic focus of WIDE is substantiated leading into a SWOT analysis and the presentation of WIDE's business model canvas. Finally, WIDE's value flows including the economic landscape it operates in, as well as measures for achieving sustainability and scalability are explained.

WIDE employs a phased approach for achieving market adoption. More specifically, it uses market vectors to achieve adoption for one specific market segment, exhibiting a deep integration rather than aiming to capture the market at large. This approach is based on the assumption that WIDE is a small actor in the digital identity market and cannot compete with large and established market actors, such as the

Bundesdruckerei, Worldline, Idemia, Thales, and Swisscom. Following, WIDE targets the DAOs as a niche market even within Web3 before subsequently rolling out to the wider Web3 sector and finally to the digital economy at large.

Therefore, integrations that are unlikely to be targeted by large European actors, but capture deep markets are particularly interesting to WIDE. For example, a DAO-ready identification solution for grant processes allowing both European and Indian nationals to complete KYC is not currently available on the market. WIDE has ambitions to fill this gap to allow users to upload educational credentials, EUDIW-compliant credentials, and Aadhaar documents which are then structured in a privacy-preserving manner to comply with the requirements of DAOs.

As WIDE cannot rely on funding for quantitative marketing campaigns, it aims to capture a user base through partnerships. These partnerships allow users in those organisations to familiarise themselves with the solution and make them more likely to also adopt WIDE for dealing with their private matters. Web3 is a particularly suitable sector for this approach because it fuses professional and private aspects of the identities of its users, addressing users as prosumers by default.

Leveraging the University of Malta use case, WIDE recognises the immense potential within the educational sector for secure, efficient identity management solutions. This segment includes not just the institutions themselves but also their vast populations of students, from youths navigating their first digital experiences to older students seeking advanced degrees. Solutions for this segment focus on streamlining administrative processes, enhancing campus security, and providing a seamless online learning experience.

Inspired by the CryptoHub Malta community engagement, WIDE targets the burgeoning sector of cryptocurrency enthusiasts, blockchain startups, and DAOs like RaidGuild. These groups demand cutting-edge security and privacy features, alongside the flexibility to integrate with decentralised networks and services. WIDE's blockchain-based credentials offer a unique value proposition, bridging the gap between traditional identity verification methods and the decentralised ethos of the crypto space.

In response to the evolving regulatory landscape, particularly the recent updates to the eIDAS regulation, WIDE positions itself as a pivotal solution for entities requiring compliant, secure, and interoperable digital identity verification processes. This segment's broad spectrum includes government services seeking digitization and corporations across finance, healthcare, and commerce, all of which demand stringent identity verification mechanisms.

Catering to a vast range of users, from the tech-savvy younger generation to older populations acclimating to digital advancements, WIDE emphasises user-friendliness, security, and privacy. This strategy aims to foster digital literacy and adoption across all age groups, establishing trust and promoting widespread platform utilisation.

Figure 46: SWOT Analysis WIDE

8.2.9.7 SWOT Analysis

WIDE's SWOT analysis presents a straightforward view of its position. Its strengths include an innovative design and the integration with TrustChain, improving both its functionality and credibility. The focus on user needs, supported by compliance with eIDAS 2.0 and GDPR, broadens its appeal. However, integrating with existing systems presents challenges, and the reliance on rapidly changing technology like Web3 could impact its adaptability. Initial efforts to build trust are crucial for user adoption. Opportunities are evident in the growing demand for digital identity solutions, with WIDE's flexibility and potential partnerships, particularly through TrustChain, opening avenues for market penetration. Advances in Web3 technologies offer WIDE paths to enhance its offerings and stay ahead in the market.

Threats include the fast evolution of technology and a competitive market that could challenge WIDE's position. Regulatory changes could also demand adjustments in strategy. Emphasising educational workshops and targeting various user segments, WIDE aims to navigate its challenges and leverage its strengths, addressing the needs of a diverse user base in the digital identity landscape.

8.2.9.8 Competitive Advantage

WIDE distinguishes itself in the digital identity market by integrating traditional systems with the Web3 paradigm, moving beyond the centralised models of entities like Google, Microsoft, and Facebook to emphasise user control and security. This approach addresses data privacy concerns more directly than federated identity providers. Compared to decentralised projects such as Walt.id, WIDE finds its unique position by blending user-friendly experiences with cutting-edge technology, appealing to users familiar with both conventional and Web3 platforms. Unlike services such as MetaMask, which are primarily focused on cryptocurrency transactions, WIDE provides a comprehensive solution for identity management. The review of WIDE covers aspects such as technology integration, scalability, and compliance with legal standards, highlighting its competitive advantages and growth potential. The analysis includes a competition matrix to evaluate WIDE's market stance, illustrating how it navigates the challenges of delivering digital identity solutions globally while adhering to EU regulations. This matrix, shown in Table 16, aims to bolster WIDE's presence in the market by showcasing its commitment to delivering secure, flexible, and compliant identity solutions.

Feature	WIDE	Federated ID	Walt.id	MetaMask	Notes
Technology	Web3 and traditional systems integration	Centralised identity systems	Decentralised digital identity with open-source infrastructure	Digital wallet focused primarily on cryptocurrency	WIDE's modular approach provides flexibility and bridges different technologies
User Experience	User-centric with intuitive interface	Broad user base but complex privacy settings	Privacy-preserving, standards-compliant, wallet-based identity solutions	Cryptocurrency-focused wallet services, not identity management-centric	WIDE excels in offering a more comprehensive identity management experience
Scalability	Designed for efficient load handling	Highly scalable with a global user base	Provides scalable, customisable solutions for a variety of industries	Focused on digital asset management, may not address identity scalability	WIDE's architecture supports growth without performance loss
Security	Compliant with eIDAS 2.0 and GDPR	High-security measures but past data privacy issues	Aligns with global standards like W3C, ISO, and is GDPR compliant	Primarily secures transactions and digital assets	WIDE provides a secure environment for digital identity with regulatory compliance
Inter–operability	High due to modular design and Web3 integration	Limited by proprietary platforms	Offers interoperability with different	Limited to crypto transactions and interactions	WIDE's system is more adaptable and future-proof

			blockchains and ecosystems		for various digital identity use cases
Legal Compliance	Strong focus on compliance	Complies with global standards but has faced scrutiny	Compliant with standards such as eIDAS2 and GDPR	May not be primarily focused on identity compliance	WIDE's strong legal compliance is a competitive advantage in markets sensitive to privacy and data protection
Market Position	Strong due to TrustChain alignment	Dominant market presence	Utilised by developers and organisations for Web3 applications	Popular in the cryptocurrency community	WIDE's strategic partnership with TrustChain boosts its market credibility
Revenue Model	Diversified with service fees, subscriptions, and licensing	Ad-based revenue model	Open-source model with enterprise and cloud service offerings	Primarily transaction-based	WIDE has more diversified revenue streams, which may offer stability
Innovation	Continuous adaptation and user feedback	Large-scale innovation with significant resources	Offers cutting-edge, privacy-preserving login systems and open-source SSI solutions	Focuses on digital asset management innovations	Focuses on digital asset management innovations

Table 16: Competitiveness matrix of WIDE against direct and indirect competitors

8.2.9.9 WIDE's Business Model Canvas

WIDE leverages a comprehensive approach to redefine digital identity management, combining advanced blockchain technology with a deep commitment to user privacy and security. Central to this strategy is a network of key partnerships that extend across academic institutions, leading blockchain and wallet technology providers, and specialised corporate service advisors. These collaborations enrich WIDE's platform with cutting-edge capabilities and ensure adherence to stringent regulatory standards.

The platform's operations are characterised by a series of crucial activities: from credential management and the facilitation of secure credential presentation flows to the implementation of privacy-enhancing predicates. Such efforts underscore WIDE's dedication to a secure, efficient, and user-friendly experience. The integration with diverse systems, including both traditional and Web3 technologies, further illustrates the platform's versatility and its capacity to meet the multifaceted demands of digital identity management.

Resource-wise, the backbone of WIDE's offering is its robust technological infrastructure, supported by a team with specialised knowledge in Web3 technologies and security protocols. This expertise is pivotal in maintaining WIDE's edge in delivering innovative digital identity solutions. Strategic partnerships amplify WIDE's insights and reach within the market, fueling its continuous growth. WIDE's value proposition centres on delivering a platform that not only meets the highest standards of security

and privacy but also champions interoperability and user control. This makes WIDE an attractive option for anyone looking for comprehensive digital identity management solutions, from individual users to large organisations.

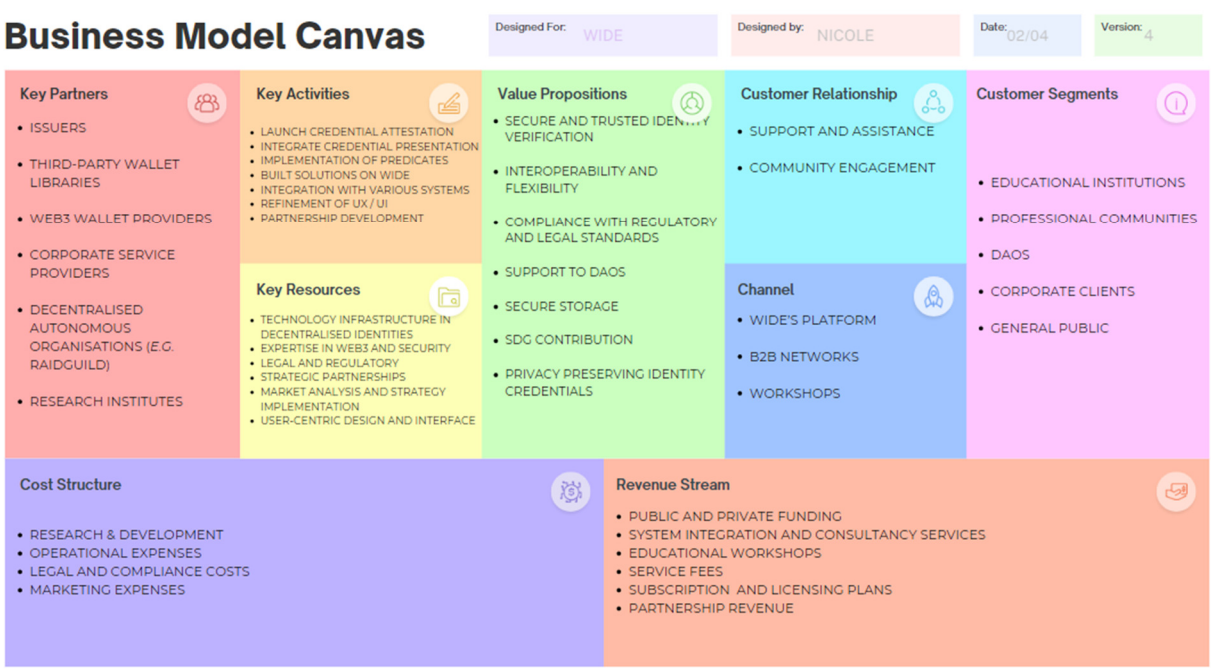


Figure 47: Business Model Canvas

To foster strong customer relationships, WIDE adopts an approach marked by active support, community engagement, and the provision of educational resources. This ensures users are well-informed and confident in utilising the platform. Channels such as online interfaces and business-to-business networks facilitate seamless interactions with WIDE's services, enhancing the overall user experience.

Targeting a broad customer base, WIDE addresses the needs of educational institutions, professional communities, DAOs, and corporate clients. This wide-ranging focus is reflected in a cost structure that prioritises research and development, operational excellence, and compliance with legal standards, ensuring WIDE remains at the forefront of digital identity management.

WIDE's revenue model initially focuses on supporting platform adoption and development through grants and project funding. Alongside this, WIDE plans to introduce additional revenue streams, including service fees for identity verification, subscriptions for premium features, and partnerships with other organisations, ensuring a sustainable financial model as the platform scales.

8.2.9.10 WIDE's Value Network

DAOs face the unique challenge of governing resources, coordinating people, and collaborating on projects without having a strict hierarchy or structure. For this reason, DAOs rely heavily on contextual knowledge and the experience of contributors. The required data, however, is often not readily available. WIDE alleviates lacking data availability by providing a standardised interface for data processing and removes the responsibility for data management from users and organisations alike. Data availability and data management that is minimal, privacy preserving and provided as a service, is a strong service offering for DAOs and entities in Web3. WIDE offers secure, encrypted storage for digital claims and credentials, significantly reducing the risk of data breaches and unauthorised access. It ensures the confidentiality and integrity of user data.

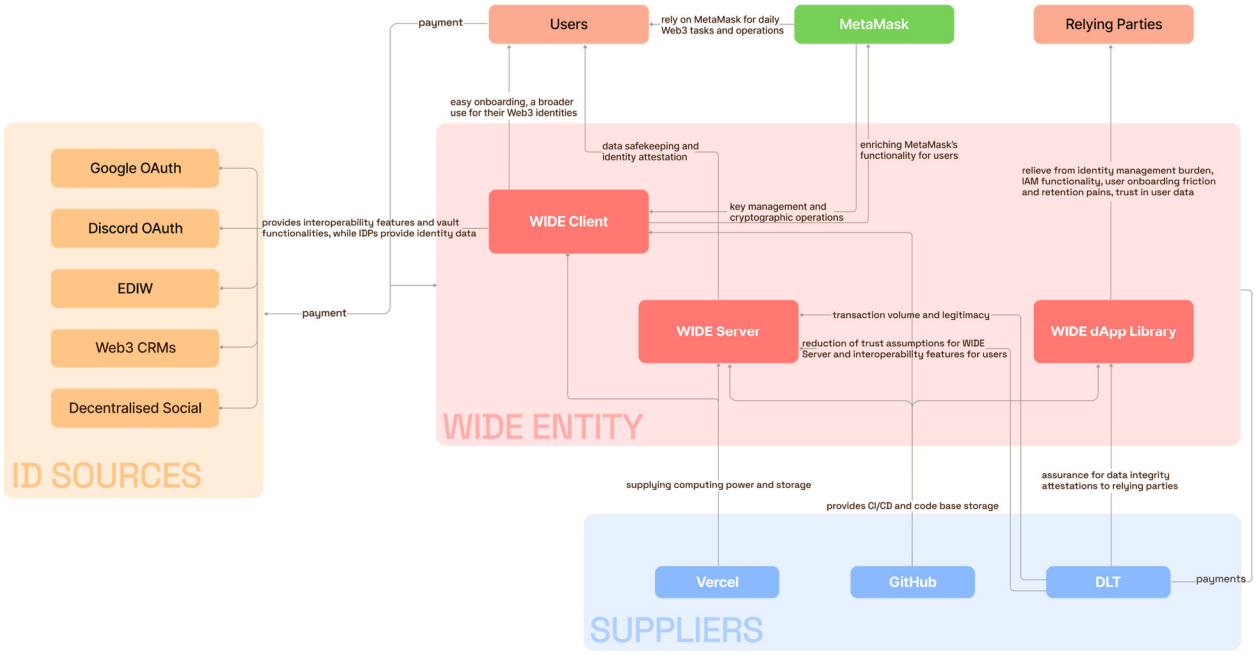


Figure 48: Value Network of the WIDE solution in the TrustChain ecosystem

8.2.10 Client DIDs

The business model for the Universal Registrar solution follows an "Open Core" approach, maintaining an open-source version of the software while also offering a proprietary version with additional features and support for more DID methods. This model allows for contribution to the decentralized identity community while also generating revenue to ensure the sustainability and continued development of the solution.

Proprietary Offering:

- Software-as-a-Service (SaaS): A hosted version of the Universal Registrar is offered, featuring a user-friendly web interface and API access. Clients can

subscribe to this service on a monthly basis, with tiered pricing based on the number of transactions. For example, Tier 1 allows up to 2000 transactions/month for a fee of EUR 60, with additional charges for exceeding the limit.

- On-Premise Deployment: For larger organizations and governments that prefer to host the solution within their own infrastructure, an on-premise version of the Universal Registrar is provided, accompanied by annual licensing fees. The fees are based on the number of transactions and include an additional 20% for support and maintenance.

Cost Structure:

Development and maintenance of the open-source and proprietary versions of the Universal Registrar

Infrastructure costs for hosting the SaaS offering

Marketing and sales expenses to promote the solution and acquire new customers

Customer support and onboarding costs

Legal and administrative expenses

Revenue Streams:

Monthly subscription fees from SaaS customers

Annual licensing fees from on-premise deployments

Additional charges for transactions exceeding the allocated limits

Potential revenue from custom development and integration services

Market Analysis:

The decentralized identity market is rapidly growing, driven by the increasing demand for secure, privacy-preserving, and user-centric identity solutions. The market is expected to reach USD 3.58 billion by 2025, with a CAGR of 71.2% during the forecast period (2020-2025). Key drivers include the need for secure identity verification, data privacy regulations, and the growing adoption of blockchain technology.

The target market includes:

Decentralized identity solution providers

Enterprises implementing self-sovereign identity solutions

Governments and public sector organizations

Blockchain and DLT platforms

Developers and system integrators

Pricing Strategy:

A tiered pricing model has been adopted for the SaaS offering, allowing customers to choose a plan that best fits their usage requirements and budget. The pricing is competitive compared to other DID management solutions in the market, while also ensuring a sustainable revenue stream for the business.

For on-premise deployments, annual licensing fees are charged based on the expected transaction volume, with an additional support and maintenance fee. This pricing model provides a predictable revenue stream and encourages long-term customer relationships.

Break-Even Analysis:

Based on projected costs and revenue streams, it is estimated that the break-even point will be reached within 18-24 months of launching the proprietary offering. This projection assumes an average monthly growth rate of 10% in SaaS subscriptions and a steady increase in on-premise deployments.

Economic Landscape and Risks:

The decentralized identity market is influenced by various economic factors, including the overall adoption of blockchain technology, regulatory developments, and the evolving landscape of digital identity solutions. Key risks include competition from other DID management solutions, potential changes in the regulatory environment, and the pace of adoption of decentralized identity solutions.

However, it is believed that the solution's unique value proposition, alignment with the TrustChain project's objectives, and strong partnerships within the ecosystem position the company well to navigate these challenges and capitalize on the opportunities in the market.

Scalability and Sustainability:

The Open Core business model ensures the long-term sustainability of the solution by balancing community-driven open-source development with a stable revenue stream from proprietary offerings. The modular, driver-based architecture of the Universal Registrar allows for easy scalability as new DID methods are onboarded and the growing customer base is catered to.

Partnerships with other TrustChain projects and the broader decentralized identity community provide a strong foundation for continued growth and innovation. As the adoption of decentralized identity solutions accelerates, the business is expected to scale accordingly, driven by the increasing demand for interoperable, user-centric, and secure identity management solutions.

In conclusion, the business model and exploitation plan demonstrate the financial viability and sustainability of the Universal Registrar solution within the context of the TrustChain project and the broader decentralized identity ecosystem. By leveraging an Open Core approach, a competitive pricing strategy, and strong partnerships, the company is well-positioned to drive the adoption of the solution and contribute to the realization of a more secure, user-centric, and decentralized digital identity landscape.

8.2.11 EVI

EVI components will be offered stand alone as SAAS to other charge point management applications that seek to verify identity certificates installed in vehicles, authorize payments via the drivers digital wallet and offer frictionless charging session initiation when a drivers plugs in a vehicle in a public charging stations. These components will be offered under monthly subscription of different cost levels based on the total number of transactions verified via EVI. The provision of the EVI components will generate recurring revenue for Parity Platform.

Main Revenue Stream:

CPOs and EMSPs that wish to include their own contract certificates list in EVI and use EVI to verify certification issued by different entities and are stored in EVI pay a monthly subscription to EVI. The monthly subscription will vary depending on the volume of certificates verified via EVI.

TABLE 51: BUSINESS MODEL CANVAS OF EVI

<table>
<tr>
<td rowspan="2">Key Partners

Vendors and OEMs of charging stations

Vehicle OEMs

Identity Providers/ Web3 Services

EV Roaming Networks

Hubject, Gireve e.t.c</td>
<td>Key Activities

Develop and maintain EVI services
Sales activities to owners of charging stations

Promotion to electric car drivers
Establish partnerships with Identity providers, Web3 Services, EV Roaming network</td>
<td rowspan="2">Value Propositions

Charge Point Operators/ EMSPs
Enable Plug&Charge without in-house development effort

Drivers of Electric vehicles:
Authenticate and start sessions faster, without PII dissemination, No need to use the phone when arriving in each charging stations, simply plug your vehicle</td>
<td>Customer Relationships
Long term for all customer segments</td>
<td rowspan="2">Customer Segments

Charge Point Operators (CPOS

Drivers of Electric vehicles
3rd party EV charge point apps</td>
</tr>
<tr>
<td>Key Resources

Developers

Software plug-ins/ libraries

cloud services</td>
<td>Channels

3rd party charge point applications

Charging Station OEMs</td>
</tr>
<tr>
<td colspan="2">Cost Structure

Payroll for software developers</td>
<td colspan="3">Revenue Streams
Commission on transactions payable by owners of electric vehicle charging stations</td>
</tr>
</table>

Marketing Budget to EV drivers Cloud services subscriptions	Subscriptions paid by 3rd party apps that use issue and verification by EVI

8.2.11.1 Economic Analysis

Globally, EVs on the road consumed over 200 TWh of electricity in 2023 at 0.35 $/ KWh for an annual estimated transaction volume of $70B. With the EV adoption rate estimated at 38% yoy until 2026 the transaction volume could reach $184B (525 TWh) globally. Europe's share of transaction is estimated at 24% of the global market volume with an addressable market at $44B by 2026. EVI aims to facilitate a subset of those charging stations taking place in public charging stations that are compatible with Plug&Charge. Serviceable market for EVI is lower than 5% of the total market since many vehicles and charging station do not support Plug&Charge. By capturing 1% of transactions in European market, that points to more than $400 million of transactions processed by EVI Wallet. Assuming a 2% net commission for EVI, this points to 8 million euros of annual revenue by the end of 2026. Wider adoption of electric vehicles, introduction discharging based transactions (vehicle-to-grid) can increase the total revenue for EVI by a factor of greater than 2 annually. from 2026 to 2030.

8.2.12 IS-CIS

Introduction

Consent management tools have become crucial in the digital landscape, especially with the rise of privacy regulations such as GDPR. These tools empower businesses to collect, manage, and respect user preferences regarding data usage.

To date, proposed consent frameworks for personal data are generally modelled as data-controller centric, and in practice almost universally. This is because they follow an inherited model of (general) data collection. Data holders most often collect data on individuals (whether PII or generic) for one of three purpose categories:

1. Required processing: Data needed as part of the service or product offered.
    a. E.g. data to personalise a product or to shape advice to the client's specific case. Consider that a custom shoe manufacturer clearly needs the feet dimensions of the customer. An e-commerce company needs to know who to ship to. A financial advisor needs to know the client's finances.
2. Profiling: Data that helps the firm segment and target the specific client or wider audience.
    a. E.g. about preferences, tastes, socio-economic group, and similar. A vehicle insurer may use information that a client is a homeowner to cross-sell home insurance. A brand understanding that most of its clients are DINK (Dual Income, No Kids) will use that information in planning publicity campaigns, etc.

Funded by the European Union

3. Resale: Data that is used to profile adverts or directly sold to third parties.
    a. E.g. The content and social network industries are almost entirely based on advertising. Data that profiles the users is invaluable for targeting the adverts, and thus many content-generation business models are based on either confirming the demographics of users or profiling users on behalf of third parties.

Under this model the same or similar data is collected simultaneously multiple times by multiple data controllers. The data is either processed by the data controller or is sent to a third party. The data controller-centric consent model collects the necessary consent for the originally envisaged purposes and, frequently, specific third-party data processors.

However, the digital realm makes it easier for data-value chains to converge. Data collected by one company for a set of specific purposes may be useful in full or in part for other companies. Retrieving the data form an existing data holder, rather than collecting it a second time from the source is more convenient, more economical, more efficient and, potentially, more accurate.

Under the current data-controller-centric consent model this is hard to do as the consent process needs to be renegotiated, and new security vulnerabilities and their accompanying legal liabilities are exposed.

Self-sovereign models turn the tables on this approach, having the data subject hold and control the data, with data processors going to source each time. This however does have scalability and coverage issues (see Misic et al[1].). Moreover, a comprehensive and widespread, ex-post migration to SS models is not supported by mature enterprise class tools due to their radical divergence from the status quo.

ConInnSeq, proposing a third alternative, splitting the data storage from the data processing consent, circumnavigates these problems by not upsetting the status quo in data storage practices (infrastructure, data base software, legal frameworks and existent business models). It is designed to allow data processors acting on behalf of the data subject to access data for separate purposes to the data controllers' own purposes.

The concept of ConInnSeq has similarities to the work of Rivas Velarde et al[2]., who built a framework that identifies consent as a compositional act. In that framework consent is composed of "a) data subjects or legal representative that provides the authorisation

[1] Scalable Self-Sovereign Identity Architecture by Jelena Misic, Vojislav B. Misic, and Xiaolin Chang, IEEE LTS, 2021

[2] Consent as a compositional act – a framework that provides clarity for the retention and use of data by Minerva C. Rivas Velarde, Christian Lovis, Marcello Ienca, Caroline. Samer & Samia Hurst; Philosophy, Ethics, and Humanities in Medicine volume 19, Article number: 2 (2024)

Funded by the European Union

of consent; b) a specific thing that is being consented to; and c) specific agent(s) to whom the consent is given". This framework is one of few pieces in the academic literature reflecting on the deficiency of the legacy data-holder centric model. In ConInnSeq the data subject (a) is provided a tool allowing them to consent to and have documented that consent, changes in (b) and (c).

The business potential, as refined over the course of the TrustChain project, for the "third way" is discussed in this section.

Initial client

ConInnSeq is in discussions with a potential client. QIoT[3] is a UK SME that has a range of connected medical devices in various stages of development. They have a prototype cardiac device and various pre-prototype devices. Their main product is a commercially available asthma inhaler and companion app that uses a proprietary post-production inhaler cap that communicates via Bluetooth to a mobile device each time the inhaler is used, thus creating a timestamp of patient behaviour and by proxy, treatment regime, and by further proxy, disease progression, responsiveness and variability. The data can be processed with other data such as local pollution or allergen data to provide further insights and a range of services can be provided such as potential warnings, data for Healthcare Professionals and more.

QIoT's purpose is patient management but it has implications for other value chains such as pharmaceutical treatment development, health service management and policy, societal development models and long-term forecasting for legislative or demand-management purposes. This initial use case will be explored further throughout this chapter.

Value proposition

> ConInnSeq allows converged data-value chains to bypass costly, error generating and time-consuming data collection and curation processes to share data when explicitly consented to by the data subject, whilst ensuring that the consent is unequivocally documented.

To break this down and to exemplify it with the QIoT use case:

[3] QIoT ltd, https://qiot.co.uk/ Hillington Park, Glasgow, Scotland, Incorporated on 31 August 2018

Funded by the European Union

- Converged data-value chains refer to where two separate value chains build value on the same data of a given data subject, and thus efficiencies or synergies are likely.
    - QIoT example: Data is collected to provide service to the asthma patient. The same asthma data can predict demand for e.g. corticosteroids and beta-agonists.
- Costly, error-generating or time-consuming costs refers to the redundancies of compiling and storing the same data multiple times, each governed by separate entities, legal frameworks and monitored independently.
    - QIoT example: The company holds objective data on the number of inhalations made by each patient and can deduce the remaining medication in the inhaler. Health service demand forecasters estimate prior and future consumption levels by combining historical data with surveys to HCPs who in turn ask patients for their estimated (subjective) consumption trends. QIoT's data could provide a more accurate, more time-sensitive and cheaper route to the same result.
- Data collection and storage refers to the entire technical and procedural lifecycle of compliantly collecting and storing data, consent to store the data, maintaining legal frameworks, and cleaning data.
    - QIoT example: the legal agreement between QIoT and its stakeholders, their inhaler-cap to database data processes, their database and infrastructure, their database management practices.
- Share data refers to providing data upon consented request to a third party for processing via any medium electronic or analogue.
    - QIoT example: sharing data with health service managers via a live dashboard.
- Explicit consent refers to the subject consenting to the specific data to be shared, purpose and processor (i.e. (b) and (c) of the Rivas Velarde model.
    - QIoT example: (proposed) consent by a patient to include their own inhalation data in an aggregated dataset shared with the health service.
- Unequivocally documented refers to the use of tokenised consent to generate an infallible audit trail as per the ConInnSeq innovation.
    - QIoT example: (proposed) a DLT audit trail showing the consent token transactions with the patient consent to the health service and to QIoT as distinguished Data Processors.

Business model

Funded by the European Union

The key business model for UST as technology developer, and based on the company profile, namely a mid-sized international technology company of some 30k employees, is to develop this technology into a product that is then customised in different niches for different industries.

Secondary business models are the development or co-development of specific industry solutions and the eventual development of independent consent hubs.

Product development

The initial focus of the operations centres around two key teams: the product development team and the opportunity team. The product development team is dedicated to refining the ConInnSeq framework, aiming to create a versatile, adaptable tool capable of addressing various use cases. On the other hand, the opportunity team comprises presales engineers who initiate connections and explore potential scenarios for specific implementations. Upon contract approval, the implementation team takes over. Their primary responsibility lies in seamlessly integrating the ConInnSeq framework into existing systems and carrying out any required customizations to meet client needs.

Each project will be uniquely crafted and interdisciplinary, integrating elements of front-end design, UI/UX development, including the creation of intuitive apps and portals. Backend development will be pivotal for establishing connections between the subject under consideration and relevant data fields and formats. Additionally, there will be an emphasis on data transfer protocols, alongside the implementation of a robust DLT governance layer.

Most profiles needed for an implementation project aren't exclusive to ConInnSeq or DLT, making the model highly scalable. These resources can be sourced internally within the organization or recruited externally without the need for specialized ConInnSeq training.

An initial product roadmap has been established to drive development, but features may be prioritized based on demand and active engagements, as the prioritization rationale is constantly updated through customer feedback.

Features and capabilities included in the roadmap are:

- Royalties' mechanisms as return value flows
- ERC1155
- Decentralised identities (Alastria-ID Model, did: web, did:eth)
- Verifiable credentials (CreatorCredentials, ValidatedID)
- SoulBound Badge

Funded by the European Union

- Account Abstraction
- Tailored Web3 UI Components.
- Digital Wallets

Return value flows is considered a particularly important aspect because it takes ConInnSeq from a framework that treats consent as a transferrable object to become a tradeable object. This provides the capability to host several innovative business models. Specifically:

- The income stream could provide an important incentive mechanism to preexisting data holders to contribute another data value chain.
    - The reward mechanism could incentivise data subjects to participate in generating value for a third party.

The value generated in an adjacent value chain could subsidise to monetise the activities of an original data-value chain.

This again can be exemplified by the SME QIoT. One of their business models that is being explored relies on these new capabilities.

Although Europe mainly has universal healthcare, many countries do not. Asthma inhalers in the USA for example cost between $50 and $100. Not all parts of the population are insured and can afford this, and the situation is more acute in many parts of the world. An impoverished market segment is not a viable market for QIoT to target with a connected device and disease self-management portal, as the costs of this will always make it a premium option.

However, QIoT has ascertained, through direct consultation with the pharmaceutical industry, that the device-generated data of their service could be worth as much as 1000 USD per patient per year to disease researchers. That top figure would apply when the data was 1) precise, 2) real time, and 3) the patient was from an uncommon segment of the population, such as for location, profile, disease state or co-morbidities, on which data is not otherwise readily available. This means that the two value chains can be converge-able as shown below. That is, the data collected by QIoT can be used as part of the pharmaceutical company's value chain.

Funded by the European Union

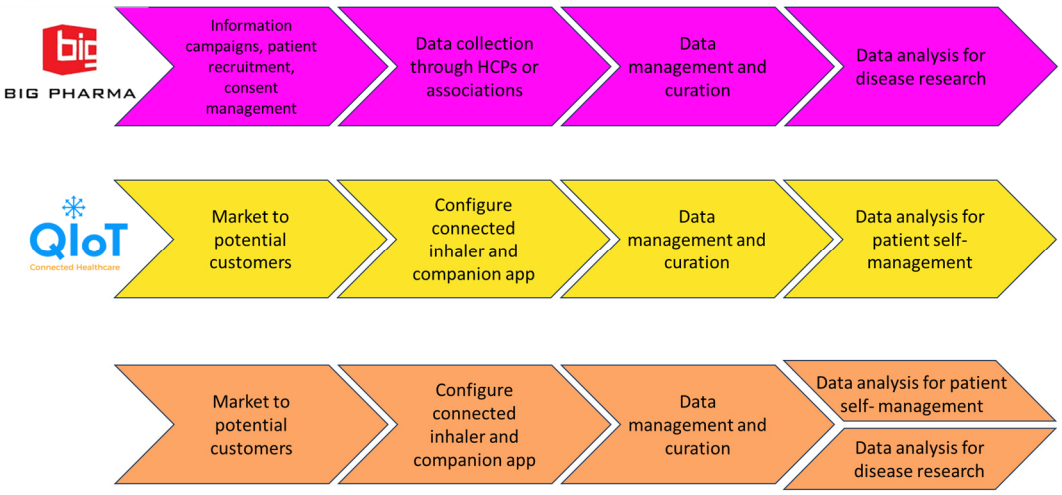


FIGURE 16: VALUE CHAIN FOR IS-CIS

This opens an exciting possibility: If QIoT can sell patient data to the pharmaceutical company, (which may be a cheaper alternative to collecting the data themselves), they could use that revenue in full or in part to subsidise the cost of their own service. In fact, if the economics were there, it could be a viable business model to provide patients with medication and the QIoT system free of charge, in return for commercialising their data. This would allow significant new populations to access healthcare. Many varieties on this model exist: the pharmaceutical company could provide the medication, QIoT could have tiered service levels (gold, silver etc).

However certain problems exist with doing this at present: QIoT cannot commercialise this data without informed consent. This may not be acceptable to all patients. Indeed, there is likely to be a spectrum of acceptance from "yes to all data", to "yes to selected data", and "no to any data". Notwithstanding any ethical considerations that may arise, ConInnSeq is an ideal platform to manage that consent because it is customisable to each user's propensity, can be altered (i.e. a patient may initially consent and then reduce the data fields they are willing to share) and can be altered in real time.

However, further complications arise:

- How does the patient earn their incentive? Hence why a return value flow, for example in the case of reward tokens or points is a high priority feature.
- How does the user know they are receiving a fair and equitable proportion of the value generated? To delve into this second point, ConInnSeq has submitted a joint bid to the TrustChain OC3, currently under evaluation.

Secondary business models

Funded by the European Union

The two secondary business models are 1) domain specific solutions, and 2) Consent hubs.

The former refers to the development, marketing and delivery of suites and tools based on the use of ConInnSeq for determined problems found repeatedly by a sector. The QIoT use case is an example of a solution that could become a UST industry solution. In this case it would develop specifically for medical consent to IOT device data and marketed directly to the healthcare sector.

At some point it would become natural to diverge from the main product roadmap and potentially fork the technology, after which back compatibility would not be guaranteed and advances in one branch might not be useable by the other. Each branch would also follow their own business plan and eventually be run separately. An industry specific solution could eclipse the generic one in which case UST might choose to disband the original plan, or alternatively divest, or set up spin outs with or without further investors and partners. Naturally, this is highly speculative, and it is illogical to speculate or plan in detail something with numerous variables. It is sufficient to identify this as a core part of the long-term thinking and that several possible scenarios have been highlighted in the brainstorming sessions within the banking, human resources and manufacturing domains.

The latter business model, consent hubs, is a concept introduced later. It appears a logical conclusion of critical mass: when sufficient data-value chains converge, monetising that convergence becomes a viable business model, rather than an efficiency saving found in the synergy of just a couple of such convergences.

To better exemplify the concept, let's return to the QIoT example. Let's imagine that they successfully enter a few territories with a business model based on subsidising medicine in return for patient data, and have established a network of buyers, from health organisations, pharmaceutical companies and others. Now, the more data they aggregate, the more data they may sell, and the more the data is valuable because now more variables can be known per patient. If they were to work with other IoT device providers, such as smart watches, diabetes monitors and heart monitors, they could leverage their existing operations to monetise that data on their behalf. At some point this may be a larger enough business that they exit the original IoT device market and concentrate solely on consent-brokering. They would have become, in essence, what is referred to as a consent hub.

The ConInnSeq vision is not, however, based on private, for profit, consent aggregators, but rather a spectrum that also includes public or not-for-profit community hubs. They do not need to generate large amounts of income to be viable if they also provide good service to all the users. For example, ride sharing would provide a community where, consenting to sharing data, may follow the ConInnSeq philosophy of Consensual, Innate and Sequential.

Funded by the European Union

For this reason, considerations are already underway regarding how, once the concept has been proven in industry use cases for paying customers, the open-source software can be adopted by communities and supported by UST and its partners. The remainder of this chapter will focus on the immediate productization exploitation path.

Cost-benefit model

Expanding on the prior cost analysis, the product development team costs have been estimated over a three-year span. This is shown below and imagines an expanding and specialising core team.

Role	Location	Costs per H including overhead and taxes					
		H1	H2	H3	H4	H5	H6
Head of project	On shore	€ -	€ -	€ -	€ 104,800.00	€ 104,800.00	€ 104,800.00
Project lead	On shore	€ 78,600.00	€ 78,600.00	€ 78,600.00	€ 78,600.00	€ 78,600.00	€ 78,600.00
Senior architect	On shore	€ 65,500.00	€ 65,500.00	€ 65,500.00	€ 65,500.00	€ 65,500.00	€ 65,500.00
Senior developer	Offshore	€ 39,300.00	€ 39,300.00	€ 39,300.00	€ 78,600.00	€ 78,600.00	€ 78,600.00
Junior developer	Offshore	€ 30,130.00	€ 60,260.00	€ 60,260.00	€ 90,390.00	€ 90,390.00	€ 90,390.00
Testing	Offshore	€ 15,065.00	€ 30,130.00	€ 45,195.00	€ 60,260.00	€ 60,260.00	€ 60,260.00
Marketing	Corporate	€ 10,000.00	€ 15,000.00	€ 15,000.00	€ 20,000.00	€ 20,000.00	€ 20,000.00
Legal	Corporate	€ 9,000.00	€ 5,000.00	€ 5,000.00	€ 5,000.00	€ 5,000.00	€ 5,000.00
Total		€ 247,595.00	€ 293,790.00	€ 308,855.00	€ 503,150.00	€ 503,150.00	€ 503,150.00

These figures are based on UST salary rates for on shore and offshore staff, consider team expansion, taxes and company overhead proportional to salary.

This team will deliver the product roadmap previously discussed. They are a pure cost function. The P&L comes from the implementation team which must cover its own costs and share of the product development.

Funded by the European Union

The implementation team naturally varies according to the scope and nature of the client and their use case, however the estimate of €1,34m over three years remains a valid figure. Of this, approximately €400k would be project margin, and €200k license costs for the ConInnSeq system, the remainder being implementation work (customising, integrating, testing, training and maintenance).

Based on estimates, the revenue per year, project margin, implementation costs, and license fees have been elaborated, considering each as an average over a three-year duration:

Year	New deals	UST Revenue	Project margin	Implementation costs	License fees
0	0	€ -	€ -	€ -	€ -
1	1	€ 1,240,000.00	€ 370,149.25	€ 669,850.75	€ 200,000.00
2	2	€ 2,580,000.00	€ 770,149.25	€ 1,409,850.75	€ 400,000.00
3	3	€ 3,870,000.00	€ 1,155,223.88	€ 2,114,776.12	€ 600,000.00
4	5	€ 6,450,000.00	€ 1,925,373.13	€ 3,524,626.87	€ 1,000,000.00
5	7	€ 9,080,000.00	€ 2,710,447.76	€ 4,969,552.24	€ 1,400,000.00

The value of the investment for UST can be considered both the project margin and any surplus on the license fees, which is shown below. As can be seen this generates a surplus in the fifth year. Until that point UST continues to invest from the project margin generated.

	Y1	Y2	Y3	Y4	Y5
Product Dev costs	€ 541,385.00	€ 812,005.00	€ 1,006,300.00	€ 1,006,300.00	€ 1,006,300.00
Fees generated	€ 200,000.00	€ 400,000.00	€ 600,000.00	€ 1,000,000.00	€ 1,400,000.00
Surplus	-€ 341,385.00	-€ 412,005.00	-€ 406,300.00	-€ 6,300.00	€ 393,700.00

The benefit for the customer is very much use case dependent, each implementation will provide a different ROI for the client. Further to the hypothetical case discussed, some estimates have been derived from conversations with the potential client QIoT:

QIOT case				
Assume the company offers 4 tiers of service, with Tier 1 refusing consent to data and Tier 4 offers full data consent.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
	Assume 10000 customers equally distributed between tiers			
n	2500	2500	2500	2500
	Assume the data value per patient is non-linear			
Value of data	€ -	€ 100.00	€ 500.00	€ 1,000.00

Funded by the European Union

	Calculate data share revenue			
Total data revenue	€ -	€ 250,000.00	€ 1,250,000.00	€ 2,500,000.00
	Estimate cost of service and client fees per Tier			
Cost of service	€ 300.00	€ 300.00	€ 300.00	€ 300.00
Client fees	€ 500.00	€ 400.00	€ 100.00	€ -
	Calculate client fee revenues			
Total fees	€ 1,250,000.00	€ 1,000,000.00	€ 250,000.00	€ -
	Subtract client costs			
Client margin	€ 500,000.00	€ 250,000.00	-€ 500,000.00	-€ 750,000.00
	Add Data revenues			
Total profit	€ 500,000.00	€ 500,000.00	€ 750,000.00	€ 1,750,000.00

Now compare two scenarios: with or without ConInnSeq

Assume without ConInnSeq they have established a price of 400€. All Tier 1 and Tier 2 users subscribe, and half of Tier 3

Without

	n	Revenues	Costs	Margin
Tier 1	2500	€ 1,000,000.00	€ 750,000.00	€ 250,000.00
Tier 2	2500	€ 1,000,000.00	€ 750,000.00	€ 250,000.00
Tier 3	1250	€ 500,000.00	€ 375,000.00	€ 125,000.00
Tier 4	0	€ 0.00	€ 0.00	€ 0.00
				€ 625,000.00

Now, compare to the scenario, including also a €1.24m investment in year 1 and a €50k cost per year thereafter.

With ConInnSeq

Revenue per year	€ 6,500,000.00
Delivery costs	€ 3,000,000.00
ConInnSeq service cost	€ 50,000
Margin	€ 3,450,000.00

Due to the project costs, the first-year margin is halved

(Note this is a simplified depiction, it excludes additional costs of business in sharing the data, managing a larger userbase, license that may be required etc. It dies however illustrate the benefit that ConInnSeq brings through innovative business models.).

Conclusion

Funded by the European Union

In this chapter, the value proposition, business model, and business plan have been explained, including the cost-benefit analysis for UST as a provider and for a potential client based on exploratory discussions of their needs. The plan to implement this is fully described and constitutes the exploitation plan.

The plan includes the vision of consent hubs. As these form, there will be greater synergies with other Next Generation Internet and TrustChain projects. Some of those synergies are already being explored. Furthermore, each individual use could find synergies with the other projects on an ad hoc basis.

The plan and forecasts are predicated on identifying key areas where ConInnSeq generates substantial value to the clients: access to new markets, new business models or greater value generation per customer. All of these are shown in the business case for QIoT.

The nature of the concept, being separate from any given business model, market or industry is not susceptible to specific shocks. Naturally it is susceptible to global economic shocks and technology trends. The primary technology trend at present is the rise of Generative AI. The analysis has not shown that to be a competitive or replacement threat: the business focuses on real data that cannot be generated by AI.

In summary, there is very strong potential for ConInnSeq as a business concept, as an NGI community concept, and for UST and its customers. It is isolated from specific market and technology shocks and a clear exploitation plan is in play comprising of: client-led projects, internal investment and further grants for specific, innovative features such as transparent value sharing.

Funded by the European Union

8.2.13 PRIVÉ

In what follows, the final version of the business model and exploitation plan is provided. First, an analysis of the competitive landscape is presented. Next, the business model is outlined, followed by a value network analysis, and an economic analysis of the implemented plan, which includes a cost-benefit analysis, risk management, and investment and funding strategies.

8.2.13.1 Introduction

This section delves deeper into the economic dynamics of PRIVÉ within the TrustChain initiative. It is designed to present a detailed, forward-looking analysis that spans cost structure, revenue streams, market examination, strategic pricing, and critical break-even points. This enriched perspective is aimed not only at establishing the feasibility of the innovative business model but also at showcasing its potential for scalability and sustainability in a rapidly evolving economic landscape.

Enhancements have been integrated, focusing on refining the two principal exploitation strategies: **Licensing fees from companies and governmental bodies** and **Playstore Downloads from individual holders**. Each exploitation avenue will be analyzed through a SWOT analysis, offering insights into their strengths, weaknesses, opportunities, and threats, thereby ensuring a holistic understanding of market position and strategic advantages.

Furthermore, the section will expand upon the competitive analysis, highlighting distinct advantages and areas for improvement in relation to key market players. This insight is pivotal for identifying strategic opportunities and reinforcing the value proposition in the decentralized digital identity ecosystem.

Additionally, the essential prerequisites for each exploitation plan will be outlined, detailing the operational, technical, and market readiness requirements necessary for successful implementation. This approach ensures that the business model not only relies on current economic realities but is also capable of navigating potential risks and capitalizing on emergent opportunities within the scope of PRIVÉ.

Through this comprehensive economic analysis, the robustness of the business model is aimed to be affirmed, underlining its adaptability and long-term viability in addressing the complexities of digital identity management applications.

8.2.13.2 Market Analysis

8.2.13.2.1 Competitive Landscape

The project delves deeper into the evolving market of decentralized digital identity solutions, with a special focus on identity wallets for both service providers and individual holders. This refined analysis not only highlights PRIVÉ's standing among crucial competitors but also emphasizes the distinct pathways through the two principal exploitation plans: Licensing and Downloads from app stores. By doing so, a

Funded by the European Union

comprehensive view of the ecosystem in which PRIVÉ operates is ensured, reinforcing strategic positioning and the value proposition.

- uPort: A self-sovereign identity platform that empowers users with full control over their identity and personal data. uPort facilitates identity verification while ensuring user privacy, using Ethereum blockchain technology.
- Sovrin: As a decentralised identity network, Sovrin provides a secure and user-centric solution for identity management. It allows individuals and organisations to create and control their digital identities, providing a robust ecosystem for trusted interactions.
- Hyperledger Indy: This platform, part of the Hyperledger suite, is specialised in decentralised identity. Indy offers robust tools and libraries for establishing digital identities rooted in blockchains or distributed ledgers, making it a significant player in the domain.
- Hyperledger Aries: Hyperledger Aries is a project under the Hyperledger umbrella focused on creating interoperable identity tools and solutions. It provides infrastructure for peer-to-peer messaging, secure data storage, and facilitates interactions involving decentralized identities. Aries is designed to enable the exchange of blockchain-based data, supporting a variety of identity solutions, and aiming to create a standardized ecosystem for digital identity.
- Jolocom: Jolocom offers a self-sovereign identity solution designed to enhance user autonomy over digital interactions. Their smart wallet enables individuals to securely manage and share their identity credentials across various services, facilitating seamless and privacy-respecting online transactions. Jolocom's approach to decentralized identity aligns with the ethos of user control and security, catering to a broad audience seeking to navigate the digital world with ease and confidence.
- Civic: Civic provides a Blockchain-based identity verification platform that allows individuals to protect and authorize the use of their identities in real time. The Civic Secure Identity App offers a way for users to establish a digital identity that they can use to interact securely with various services, emphasizing user privacy and data protection. This focus on secure, real-time identity verification makes Civic a noteworthy contender, especially for users and service providers prioritizing immediacy and security in identity verification processes.
- ID.me: ID.me offers an identity platform that simplifies how individuals securely prove and share their identity online. With a focus on accessibility and security, ID.me supports verifiable credentials for a wide range of uses, from government services to healthcare. ID.me's user-friendly approach and extensive partnership network position it as a significant player in the digital identity verification space, providing a direct benchmark for PRIVÉ's user engagement and scalability strategies.

Error! Reference source not found. provides an overview of how PRIVÉ stands out in terms of its advanced security features (such as hardware-based keys and holder

Funded by the European Union

binding), compliance alignment (GDPR and eIDAS), and its broad target audience that includes not just individual holders, but also organisational entities like Wallet Service Providers and Government Bodies. The table also illustrates how PRIVÉ differs from other competitors, especially in its approach to user control and privacy.

TABLE 52: COMPETITION ANALYSIS FOR PRIVÉ

Features/ Competitors	User Control	Privacy Features	Market Positioning	Compliance Alignment	Target Audience	Differentiator
PRIVÉ	High (Selective Disclosure, Holder Binding)	Advanced Selective Disclosure, GDPR & eIDAS aligned	High Level of Assurance, Tailored for Modern Compliance	GDPR and eIDAS	Wallet Service Providers, Holders, Verification Companies, Governmental Bodies	Integration with Existing Wallets, Enhanced Trust with Hardware Keys
uPort	User-controlled Identity Management	Privacy-centric, Limited Data Exposure	User Empowerment, Easy Integration	Varies	Individual Users, Developers	Ethereum-based, Open Source
Sovrin	Self-Sovereign Identity Management	Privacy and Security Focused	Robust Ecosystem for Trusted Interactions	Varies	Organizations, Institutions	Global Identity Network
Hyperledger Indy	Self-Sovereign Identity Management	Privacy and Security Focused	Focus on Digital Identity	Varies	Organizations, Institutions	Part of a Larger Enterprise Suite
Hyperledger Aries	Self-Sovereign Identity Management, P2P Wallet Interactions	Privacy and Security Focused, P2P Credential Exchange	Focus on Wallet Interoperability and Flexible Credential Exchange	Varies	Organizations, Institutions, Developers	Advanced Wallet Functionality, Peer-to-Peer Interactions
Jolocom	High (Self-Sovereign Identity Management)	Privacy and Security Focused, Self-Managed Identities	Open-Source, Decentralized Identity Management	GDPR Compliant	Individuals, Developers, Enterprises	Decentralized Identity with Portable Identities
Civic	User-controlled Identity Management	Privacy-centric, Biometric Verification	Secure Identity Verification, Biometric Capabilities	Complies with Various Regulations	Individual Users, Businesses	Mobile-first Approach, Biometric Authentication
ID.me	User-centric Identity Verification	Privacy Protection, Minimal Data Sharing	Verified Identity Services for Government and Business	Strong Compliance with US Laws	Government, Healthcare, Financial Services	Wide Adoption in US Government Services

This expanded analysis enriches the understanding of the competitive dynamics within the decentralized digital identity market, highlighting PRIVÉ's unique positioning, especially in terms of compliance, privacy features, and its approach to user control and market targeting.

Funded by the European Union

8.2.13.3 Business Model Description

8.2.13.3.1 Business Model Overview

PRIVÉ, a cutting-edge platform in the section of decentralised digital identity and Blockchain technology, introduces a business model tailored to the evolving landscape of digital identity management. The business model of PRIVÉ is created in a manner that enables leveraging the unique capabilities of PRIVÉ, specifically its advanced key management, selective disclosure features, and compliance with critical regulations like GDPR and eIDAS. This model is designed to respond to a diverse array of customer segments, including Wallet Service Providers, individual Holders, Companies for Verification, and Governmental Bodies, ensuring a broad market appeal.

At the core of the envisioned business model lies the strategic monetization of the technology through licensing for Wallet Service Providers and governmental bodies, subscriptions for Individual Holders and Verification as a Service (VaaS). This approach enables PRIVÉ to establish a sustainable and scalable economic foundation, while simultaneously addressing the specific needs of different market segments. In addition, it is possible to monetize other revenue streams, such as licensing for verification services.

The envisioned business model emphasises not only on technological innovation, but also on building robust customer relationships, ensuring user-friendly experiences, and strong partnerships. This approach is key to driving user adoption, enhancing customer loyalty, and creating long-term value for both PRIVÉ and its stakeholders.

8.2.13.3.2 Business Model Canvas

The canvas provided in figure below outlines a comprehensive and adaptable business model, strategically positioning PRIVÉ to capitalise on its unique offerings in the dynamic domain of decentralised digital identity.

TABLE 53: BUSINESS MODEL CANVAS OF PRIVÉ

Funded by the European Union

8.2.13.4 Value Network Analysis

8.2.13.4.1 Stakeholder Interactions and Service Provision

Expanding on the framework from Chapter 7 of D.3, PRIVÉ continues to refine its stakeholder engagement strategy, focusing on two primary exploitation plans: Licensing and Play Store Downloads. This refined focus allows PRIVÉ to cater more directly to the needs of specific groups within its ecosystem, further enhancing the utility and reach of its solutions.

- **Wallet Service Providers** act as primary integrators of the PRIVÉ library, enhancing their existing digital wallet offerings.
- **Individual Holders (End-Users):** Individuals looking for a secure, user-friendly digital wallet to manage their identities and credentials. This group is the primary focus for the Play Store downloads, offering a direct-to-consumer approach.
- **Companies for Verification** leverage PRIVÉ's technology for efficient and reliable verification of digital identities.
- **Governmental Bodies** use PRIVÉ for issuing and managing digital credentials, offering streamlined services to citizens.

Funded by the European Union

- **Technology Companies** such as Apple and Microsoft can leverage the state-of-the-art SSI library to enhance their existing digital identity solutions, filling potential gaps in their offerings and have a rapid entry into the market.

The interactions in this ecosystem are driven by the exchange of services, information, and technology, creating a value network where each participant enhances the overall effectiveness and efficiency of the system.

8.2.13.4.2 Revenue and Information Flows

The PRIVÉ platform orchestrates a sophisticated flow of revenue and information among its stakeholders, ensuring the viability and sustainability of the ecosystem.

Revenue Flows

- From Wallet Service Providers, Governmental Bodies and Technology Companies to PRIVÉ via licensing fees.
- From Individual Holders when they download the application from a store (App Store or Google Play) via subscription models.
- From Companies or Governmental Bodies for Verification via a fee per verification (Verification as a Service - VaaS).
    - It is believed that by focusing on the licensing fee through selling the product to Wallet Service Providers and Governmental Bodies, they will use the tool for verification of verifiable credentials/presentation via VaaS.

Information Flows

- Between PRIVÉ and all stakeholders for service updates, feedback, and technical support.
- Amongst stakeholders for operational data, verification information, and digital credentials.

These flows ensure that PRIVÉ can continuously invest in research, development, and service improvement while providing stakeholders with valuable services and data.

8.2.13.4.3 Prerequisites for each exploitation plan

Wallet Service Providers for licensing:

- **Integration Capability**: Existing digital platforms or wallets must have the ability to integrate third-party libraries or APIs, requiring a certain level of technical flexibility and openness.
- **High Bandwidth and Reliability**: For service providers planning to use PRIVÉ extensively, a network setup that supports high bandwidth and reliability to manage the expected traffic and data processing needs.
- **eIDAS bridge**: Wallet Service Providers need to set up an eIDAS bridge.

Governmental Bodies or Companies that will use PRIVE as a Wallet Service Provider for licensing:

Funded by the European Union

- Integration Capability: Governmental bodies should adjust their existing services with the wallet that is provided by us.

Individual Holders (End-Users)

- Compatible Mobile Device: A smartphone with the necessary specifications (e.g., operating system version) to support the PRIVÉ app downloaded from the Play Store.
- Internet Connectivity: Reliable internet access to download the app, perform digital identity transactions, and access online services.

Companies for Verification:

- High-Capacity Servers: Servers capable of supporting high bandwidth and processing large volumes of verification requests efficiently.
- Secure Data Handling: Infrastructure and protocols for secure data handling, storage, and transmission to protect sensitive user information during the verification process.

8.2.13.5 SWOT Analysis

In the tables throughout this section, the SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis for the PRIVÉ solution is provided concerning various parties and stakeholders.

TABLE 54: SWOT ANALYSIS - WALLET SERVICE PROVIDERS & GOVERNMENTAL BODIES FOR LICENSING

Strengths	**Customization and Integration:** Ability to customise and integrate PRIVÉ's solutions into existing systems, offering tailored digital identity management.
	Enhanced Security and Compliance: Leverages PRIVÉ's hardware-based keys and alignment with GDPR and eIDAS, offering a competitive edge in terms of security and legal compliance.
	Technical Support and Development: Access to PRIVÉ's expertise and continuous updates, ensuring that the solution remains at the cutting edge.
Weaknesses	**Technical Integration Complexity**: Potential challenges in integrating PRIVÉ's solutions with varied and legacy systems of different stakeholders.
	Dependence on PRIVÉ's Continuity: Reliance on PRIVÉ for continuous updates and support, which could be a concern if PRIVÉ faces operational challenges.
Opportunities	**Expanding Market for Digital Identity Solutions**: Rising demand for secure and compliant digital identity management solutions presents significant market opportunities.
	Regulatory Changes: Evolving data protection and privacy regulations could increase demand for PRIVÉ's GDPR and eIDAS compliant solutions.
Threats	**Competitive Market**: Growing competition in the digital identity space could impact market share and pricing strategies.
	Rapid Technological Changes: The fast pace of technological advancements could necessitate frequent updates and adaptations, increasing operational costs.

Funded by the European Union

TABLE 55: SWOT ANALYSIS - INDIVIDUAL HOLDERS (END-USERS)

Strengths	**Ease of Access and Use**: Direct access for users to download and start using PRIVÉ's wallet, facilitating widespread adoption.
	User Empowerment: Provides users with control over their digital identity and personal data, aligning with current consumer privacy trends.
Weaknesses	**User Trust and Adoption:** Convincing users to switch to a new digital identity solution and trust PRIVÉ with their sensitive information.
	Market Saturation: The app market is crowded, making it challenging to stand out and capture significant user attention.
Opportunities	**Growing Awareness of Digital Privacy:** Increasing consumer concern over digital privacy and data protection could drive more users towards PRIVÉ.
	Partnerships and Integrations: Potential for partnerships with app developers, online services, and platforms to pre-integrate or recommend PRIVÉ, enhancing user base and functionality.
Threats	**User Experience Expectations:** High expectations from users for seamless and bug-free app experiences can be challenging to meet continuously.
	Regulatory and Policy Changes: Changes in app store policies or digital identity regulations could impact app distribution and functionality.

TABLE 56: SWOT ANALYSIS - COMPANIES FOR VERIFICATION AS A SERVICE

Strengths	**Easy to use Solution:** Provides an immediate, ready-to-use service for verifying digital identities, saving clients from the complexity of developing or integrating similar systems.
	High Security and Compliance: Leveraging PRIVÉ's core technologies ensures a high level of security and compliance with regulations like GDPR and eIDAS, appealing to entities with stringent data protection needs.
	Scalability: Can handle varying volumes of verification requests, making it suitable for both small businesses and large institutions.
Weaknesses	**Dependence on PRIVÉ's Infrastructure:** Clients must rely on PRIVÉ's ability to maintain and scale its verification services, which could be a point of vulnerability if there are any service disruptions.
	Integration Effort: While it's an easy-to-use solution, some level of integration is required on the client's side, which could present challenges depending on their existing systems.
Opportunities	**Growing Need for Identity Verification:** The increasing importance of online identity verification across industries (e.g., banking, e-commerce, public services) presents a broad market opportunity.
	Partnerships: Opportunities to partner with a wide array of services that require identity verification, expanding PRIVÉ's reach and application scenarios.
	Increasing number of digital transactions
Threats	**Competitive Services:** The presence of competing verification services, some of which may be offered by larger, more established companies, could pose a threat to PRIVÉ's market share.
	Technological Advances: Rapid advances in technology could lead to new verification methods that are faster, cheaper, or more secure, potentially making PRIVÉ's current offering less attractive.

8.2.13.6 Economic Analysis

Funded by the European Union

8.2.13.6.1 Cost-Benefit Overview

This chapter is dedicated to the economic analysis of PRIVÉ, a platform designed to revolutionize the management and verification of digital identities. The focus here is to analyses and present the potential profitability and sustainability of PRIVÉ's varied revenue streams. This analysis is pivotal in mapping out the financial trajectory of PRIVÉ and in ensuring its long-term viability and success in the rapidly evolving digital identity landscape.

The analysis has been extended for a 36-month period, user subscriptions have been added as a revenue stream, and a Return on Investment (ROI) analysis has been created.

The approach contains a detailed examination of various economic parameters and projections, primarily emphasizing the break-even analysis and ROI. This analysis is crucial for understanding the dynamics of the cost structure against revenue generation strategies. By analyzing and presenting these financial metrics, clear insights into the economic sustainability of PRIVÉ are aimed to be offered.

One part of this chapter addresses the breakdown of the break-even analysis, exploring critical financial parameters such as Selling Price, Variable Costs per Unit, Contribution Margin Per Unit, and more. Unit sales are projected for a 28-month period for each revenue stream, accompanied by a detailed examination of monthly costs—both fixed and variable. This granular analysis aids in determining the number of units that need to be sold to reach the break-even point, a critical juncture where PRIVÉ neither makes a profit nor incurs a loss. It is worth mentioning that the variable X, used as a financial variable, aims to showcase a possible range of numerical values.

The financial narrative of this chapter is further enriched by a graphical representation of the break-even analysis. This visual aid enhances comprehension of financial projections and serves as a strategic tool in decision-making processes, enabling alignment of business strategies with market realities and financial goals.

On the other hand, the ROI analysis will take into account the initial and ongoing costs associated with development, maintenance, marketing, and operational expenses. This will be weighed against the revenue generated through licensing fees, subscription models, and service charges. A positive ROI indicates that PRIVÉ's solutions not only cover their costs but also generate a profit, underscoring their financial viability and market competitiveness. It is also indicative of the project's potential for scalability and long-term sustainability within the digital identity domain, ensuring stakeholders that the investment into PRIVÉ aligns with strategic financial goals and contributes to the overarching success of the TrustChain project.

Overall, this chapter offers a comprehensive economic analysis of PRIVÉ, laying the groundwork for its successful market entry and sustainability. Through this economic analysis, the goal is to validate PRIVÉ's financial model, ensuring that it is not only innovative in its technological aspects but also robust and viable in its economic framework.

Funded by the European Union

The use of X as a variable in the analysis represents an innovative approach to discussing financial metrics without tying the discussion to specific currencies or amounts. This allows for a dynamic interpretation of the financial model, adaptable to various scenarios and scales, providing a versatile framework for understanding the economic underpinnings of the PRIVÉ project.

TABLE 57: REVENUE STREAMS

Product Name	Selling Price (X)	Variable Costs per unit	Contribution Margin Per Unit	Contribution Margin Ration (CMR)	Break Even Units	Break Even (X)
Licensing for Wallet Service Providers	300	30	270	90.00%	9.259259259	2777.777778
Licensing for Companies or Governmental Bodies that use PRIVE as a Wallet Service Provider	400	57.5	342.5	85.63%	0	
Holders Subscriptions from App Downloads	1	0.4	0.6	60.00%	4166.666667	4166.666667
Verification as a Service (VaaS) - Per 1000 verification	1	0.3	0.7	70.00%	3571.428571	3571.428571

The analysis categorizes revenue into four primary streams: Licensing for Wallet Service Providers, Licensing for Companies or Governmental Bodies that use PRIVÉ as a Wallet Service Provider, Holders Subscriptions from App Downloads, and Verification as a Service (VaaS) - Per 1000 verifications. Table 57 provides a clear view of the diverse income sources, emphasizing the multi-faceted approach to monetization within the PRIVÉ ecosystem.

TABLE 58: FIXED COSTS

Fixed Costs	**Cost (X)**	**Percentage of Costs**
Research and Development	500	20.00%
Infrastructure and Operations	300	12.00%
Marketing and Sales	750	30.00%
Legal & Accounting	350	14.00%
Customer Support	550	22.00%
Training Materials	50	2.00%
Total Costs (X)	**2500**	

Fixed costs, including marketing and research and development expenses, are provided in Table 58 and represent the steady expenditures necessary to maintain the PRIVÉ platform's operation and growth. This section highlights the consistent investment in innovation and market presence essential for sustaining the project's competitive edge.

Funded by the European Union

TABLE 59: VARIABLE COSTS PER UNIT

Variable Costs (per unit) in X	Research and Development	Infrastructure and Operations	Marketing and Sales	Legal & Accounting	Customer Support	Training Materials	Total Per Unit (X)
Licensing for Wallet Service Providers	30	0	0	0	0	0	**30**
Licensing for Companies or Governmental Bodies that use PRIVE as a Wallet Service Provider	50	5	0	0.5	2	0	**57.5**
Holders Subscriptions from App Downloads	0	0	0	0.3	0.1	0	**0.4**
Verification as a Service (VaaS) - Per 1000 verifications	0.1	0.1	0	0	0.1	0	**0.3**

Detailed for each revenue stream over a bimonthly period, variable costs per unit (Table 59) provide insight into the operational costs directly associated with the provision of services. This granularity helps in understanding the cost structure relative to service delivery and scalability.

TABLE 60: PROJECTION OF UNIT SALES PER MONTH

Projection of Unit Sales per Month	#2	#4	#6	#8	#10	#12	#14	#16	#18	#20	#22	#24	#26	#28	#30	#32	#34	#36
Licensing for Wallet Service Providers	0	0	1	1	1	2	2	2	2	2	3	3	3	3	4	4	4	4
Licensing for Companies or Governmental Bodies that use PRIVE as a Wallet Service Provider	0	1	1	2	2	3	3	4	5	5	5	6	6	6	7	7	8	8
Holders Subscriptions from App Downloads	50	100	200	400	600	900	1300	1800	2500	4000	6000	8000	10000	13000	15000	17000	20000	23000
Verification as a Service (VaaS) - Per 1000 verification	0	20	40	40	60	60	100	100	140	140	200	200	300	400	400	500	600	700

Funded by the European Union

Projecting unit sales per month for each revenue stream (Table 60) offers a forward-looking perspective on potential income and market reception. It reflects expectations of growth and adoption rates, informing strategic planning and resource allocation.

TABLE 61: BREAK EVEN ANALYSIS

Break Even Analysis	#2	#4	#6	#8	#10	#12	#14	#16	#18	#20	#22	#24	#26	#28	#30	#32	#34	#36
Fixed Cost per Month	2500	2500	2500	2500	2500	2500	2500	2500	2500	2500	2500	2500	2500	2500	2500	2500	2500	2500
Variable Cost per Month	20	104	180	317	403	611	783	1040	1390	1990	2838	3695	4525	5755	6643	7473	8760	9990
Total Costs per month	2520	2604	2680	2817	2903	3111	3283	3540	3890	4490	5338	6195	7025	8255	9143	9973	11260	12490
Total Turnover per Month	50	520	940	1540	1760	2760	3200	4100	5240	6740	9100	11500	13600	16700	19400	21500	25000	28100
Profit Per Month	-2470	-2084	-1740	-1277	-1143	-351	-83	560	1351	2251	3763	5305	6575	8445	10258	11528	13740	15610

The analysis provided in Table 61 identifies the point at which total revenues equal total costs, highlighting the sales volume necessary to cover all expenses. The break-even point serves as a critical indicator of financial viability and sustainability.

TABLE 62: INITIAL COSTS

Initial Costs (HAPPENS ONLY ONCE)	Cost (X)	Percentage of Costs
Research and Development	2700	64.29%
Infrastructure and Operations	350	8.33%
Marketing and Sales	300	7.14%
Legal & Accounting	450	10.71%
Training Materials	400	9.52%
Total Costs (X)	**4200**	
Initial Costs (HAPPENS ONLY ONCE)	Cost (X)	Percentage of Costs

Outlining the one-time expenses incurred before the product launch, Table 63 accounts for the foundational investment in developing and deploying the PRIVÉ platform. It sets the stage for understanding the startup costs relative to ongoing operations.

TABLE 63: RETURN OF INVESTMENT

Variable Costs (per unit) in X	**Year 1**	**Year 2**	**Year 3**
Licensing for Wallet Service Providers	-66.32%	44.73%	309.78%
Holders Subscriptions from App Downloads	20000		
Verification as a Service (VaaS) - Per 1000 verifications	**4200**		

Funded by the European Union

With an illustrative investment of 20k of X, the ROI analysis of Table 63 calculates the return relative to the initial outlay. This measure evaluates the efficiency and profitability of the investment in PRIVÉ, providing a key metric for potential investors and stakeholders.

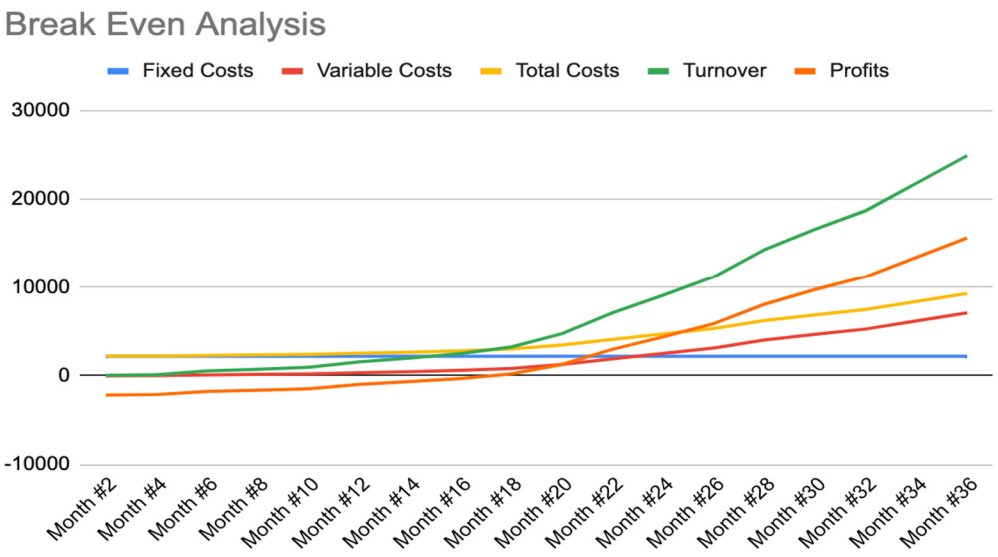


FIGURE 17: BREAK EVEN ANALYSIS

8.2.13.7 Risk Management and Mitigation

In the dynamic landscape of digital identity solutions, PRIVÉ approaches risk management with a proactive and strategic framework that identifies, evaluates, and mitigates potential risks.

Financial risks are scrutinised through cost-benefit analyses, ensuring a sustainable business model resilient to market fluctuations and capable of reaching the projected break-even point. To counteract market adoption challenges, PRIVÉ has established a multi-faceted engagement plan that leverages partnerships with established technology providers, amplifies outreach through targeted channels, and incentivizes trial via user-friendly platforms.

Furthermore, PRIVÉ continuously monitors the competitive landscape, refining its value propositions to align with Wallet Service Providers, Holders, and Verification Companies, ensuring relevance and appeal according to evolving user needs. Technological obsolescence, a crucial risk in the fast-paced tech industry, is mitigated through an agile development methodology that boosts the ongoing innovation, integration with cutting-edge advancements, and adherence to international standards like GDPR and eIDAS.

Funded by the European Union

This approach not only positions PRIVÉ at the forefront of decentralized digital identity solutions, but also ensures that it remains adaptable, future-proof, and aligned with the TrustChain project's vision for secure, private, and user-centric digital ecosystems.

8.2.13.8 Investment and Funding Strategies

In creating the financial base of PRIVÉ, a multifaceted investment and funding approach is paramount:

- Attracting **venture capital** and **angel investments** provides not only monetary support but also strategic industry insights.
- **Grants** and **subsidies** offer non-dilutive financing for R&D, promoting innovation without equity loss.
- **Strategic partnerships** with industry entities such as Wallet Service Providers and government bodies could lead to shared investment initiatives, supporting development with robust financial and collaborative support.
- **Revenue reinvestment** ensures a sustainable growth model, allowing PRIVÉ to scale operations in alignment with market receptivity.
- To complement these equity-based strategies, **debt financing** offers a leveraged means of capital infusion for expansion.

These collective strategies are tailored to the solutions developed as part of the project in order to balance growth with financial prudence, thus securing PRIVÉ's position in the dynamic domain of decentralized digital identity.

8.2.14 DOOF

8.2.14.1 Market overview

In recent years, there has been a significant increase in the interest and development of consent management, data governance, and data exchange solutions. This growth is largely fuelled by the European legislation, including the GDPR and the Data Act. These laws aim to create an inclusive, streamlined, and open data market, emphasizing the need for transparent and controlled management of personal data. They also promote streamlined data exchange across various sectors, involving numerous stakeholders and the active participation of data owners in the data value chain.

The Internet of Things (IoT) plays a significant role in the realm of data generation and its subsequent impact on society and business. The inherent potential of real-time data from IoT devices to enhance lives on both micro and macro levels is immense, particularly when considering the societal, political, and environmental challenges faced today. These challenges demand precision, speed, and a comprehensive approach in decision-making, an approach that is increasingly dependent on the intricate web of data streams produced by countless connected devices. These devices

Funded by the European Union

create a crucial link between cyberspace and real-world scenarios, providing timely and often innovative insights for problem-solving.

In the context of **smart cities**, IoT devices like air quality sensors offer valuable data that can lead to improved public health, infrastructure maintenance, and environmental monitoring. This example illustrates the tangible impact of IoT on urban life. Moreover, IoT data has the power to transform not only collective societal structures but also individual experiences. The smart home concept, where IoT assists in daily living, adapting to changing needs over time, is a testament to this transformation.

According to the United Nations Technology and Innovation Report 2021, IoT stands as one of the most lucrative frontier technologies, with sales potentially escalating from $130 billion in 2018 to $1.5 trillion in the near future. The Vodafone IoT Barometer 2019 reinforces this potential, highlighting significant revenue growth and competitive advantages for IoT adopters. However, the real value lies not in the devices themselves but in the data they generate. Yet, referring to 2018, Gartner estimated that 80% of IoT implementations missed opportunities for real innovation by focusing on narrow use cases and analytics.

In light of this scenario, where the volume of data generated by IoT devices is colossal, the development of efficient and effective data exchange tools becomes crucial. Even given this single scenario, the data from the air quality sensors not only contributes to better environmental and health outcomes but also has profound implications for businesses and individuals. The recent surge in data exchange and management technologies is a response to this burgeoning demand. Yet, the current trend in these technologies leans heavily towards centralized and vertical models. This centrality, while offering certain advantages in policy execution and data handling, also brings its own set of challenges and limitations.

The centralized model focuses on policy execution and typically involves a central entity responsible for two main areas: physical data sharing activities and consent management. When consent management is handled centrally, the data intermediary mediates between data owners and data recipients. Data owners specify their preferences for data visibility through data intermediaries, who then communicate these preferences to potential data recipients and vice versa. This process is often lengthy, consuming significant time and resources. Moreover, policy-based consent management can delay outcomes and places all legal liabilities associated with consent management on the data intermediary.

Centralized data management also implies that data intermediaries may have visibility over the data shared on their platforms. This visibility can conflict with the concept of data ownership, as these companies control data access, effectively removing this control from individuals. While intermediation is a common aspect of many services, it is unusual for intermediaries to have complete control over the actual asset, rather than just its value or representation. Current data management solutions require users to surrender their data in its entirety to ensure its protection or to manage access control.

Funded by the European Union

Furthermore, **current solutions often lack a separation of concerns regarding the levels of operations they offer, such as physical data sharing and consent management**. These functions are typically closely linked, leading to vertical, closed-off solutions rather than facilitating, horizontal technologies. This limitation hinders the easy movement of data and the development of a robust and dynamic data market.

Most of the identified players operate both in realm of DVCO, which is out of the scope of this project, and DOOF, meaning both in the realm of data visibility control and consent management. The differences between these technologies and DVCO won't be highlighted in this document.

Ecosteer Data Ownership Orchestration Framework allows to separate physical data sharing and consent management. It is a set of SDKs, libraries and Smart Contracts that allows any organization to deploy automated, scalable consent management technologies for sharing both data streams and data sets, easily implementing data exchanges that are GDPR compliant and Data Act ready.

8.2.14.2 Market Analysis

The **privacy enhancing technology market** size is projected to reach US$ 25.8 billion by 2033 at a CAGR of 26.6% during the 2023-2033 period. Organizations are increasingly finding the need to adopt **privacy-enhancing technologies (PETs)** as they look to safely and securely share data with their partners. This is fuelled by the IoT market growth and by the European legislation, including the GDPR and the Data Act.

A Gartner report stated that by 2025, 60% of large organisations will adopt PET for processing data in untrusted environments and (multi-party) data analytics use cases.

Considering GDPR compliance only, it costs between £300-450 per employee and it causes 8.1% drop in profit (Tech Monitor 2022[2]). Cost of non-compliance can cause a huge reputation damage and up to €20 million in fines or 4% of global annual turnover.

Despite the promising advantages of privacy-enhancing technologies the complexity associated with implementing and integrating these sophisticated technologies into existing systems hinder their widespread adoption. PETs often require specialized expertise, both in terms of understanding the underlying technologies and adapting them to specific use cases. The lack of skills leads to slower adoption rates. Additionally, striking the right balance between robust privacy measures and maintaining computational efficiency remains a significant challenge, as organizations need to ensure that the adoption of these technologies does not compromise overall system performance. Overcoming these implementation and performance-related hurdles is crucial for the broader acceptance and integration of PETs across diverse industries.

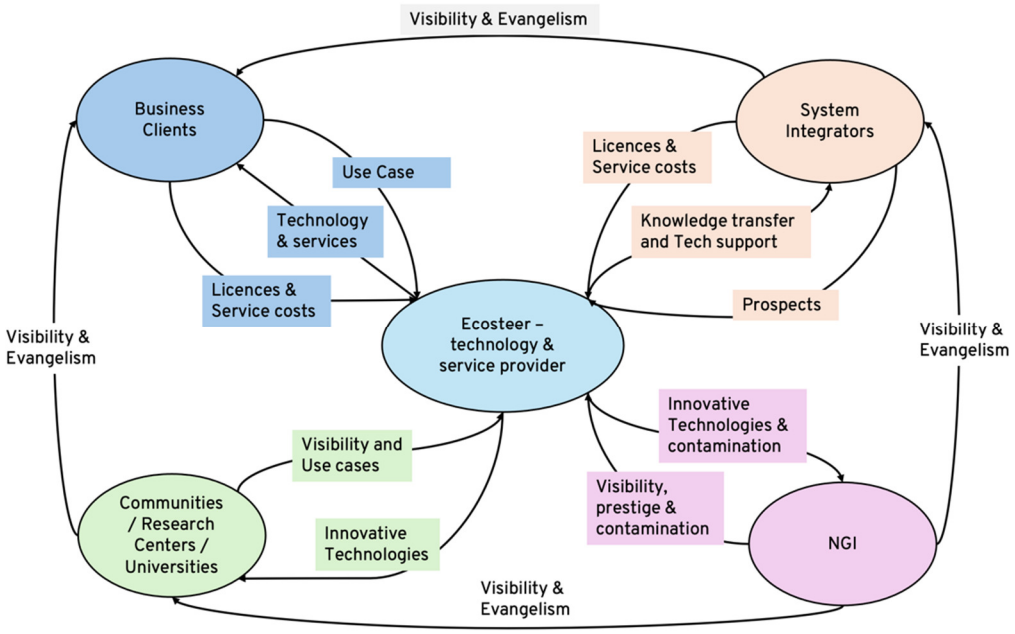
Consent management solutions – either integrated in data marketplaces or provided separately – are seen as competitors from a market point of view. Data marketplaces such as Dawex or Here Technologies provide their platforms integrated with a consent management tool. Even when consent management tools are provided separately to

Funded by the European Union

be integrated in existing corporate systems, they are not designed to separate access control to the data sharing infrastructure from visibility control over the data that crosses it. These tools simply aim at collecting user consent that is required for processing their personal data. According to this paradigm, the data sharing platform's owner manages third party data visibility on behalf of data owners, who do not have any technical means to control which third parties have visibility over their data. Without a separation of physical data sharing from consent management, these solutions lead to vertical applications, difficult to scale in size and business scope.

By decoupling physical data sharing from consent management, Ecosteer DOOF allows companies to easily adopt innovative PETs, implementing data ownership at a low risk and cost.

8.2.14.3 Value Network



This model will help Ecosteer to grow and establish itself as the long-term leader in the Data Ownership field.

Below the stakeholders and the interactions among themselves:

Business Clients. DOOF is a horizontal solution for integrating PETs that correspond to underlying requirements (see section 7.4.1 FACILITATING ADOPTION OF PRIVACY ENHANCING TECHNOLOGIES of D2) in any sector. Initial target sectors are energy and mobility with companies that have revenues of at least 1Bn/year. With initial clients Ecosteer will manage the entire sale cycle, from lead generation to project deployment. The client will select a system integrator or a consulting firm for business case definition and front-end development. Project will provide back-end

Funded by the European Union

extension for DOOF integration with Client's IT systems and for realizing the designed UX/UI, technical documentation, technical support to system integrator/consulting firm. Ecosteer will charge a yearly license fee for its proprietary PET technology – the Data Visibility Control Overlay –and a project-based fee for the DOOF. The price for the DOOF will be calculated according to the size of the projects – i.e. number and kind of data sources, number of intended use of data and new functionalities for the front-end.

System integrators and consulting firms. After initial projects, Ecosteer will partner with system integrators and consulting firms that will act as an additional channel to market – fundamental to reach big corporations and guide them in defining the business case for the selected PET technology. These players will also manage the solution deployment within Clients' IT infrastructure. Ecosteer technologies contributes to the innovative offering of these players, who will resell the license of the Data Visibility Control Overlay and use the DOOF to facilitate the project deployment. Ecosteer will provide them all the needed Know-how and technical support for project delivery.

Communities, Universities and research centres. Thanks to the DOOF communities, universities and research centres will be able to easily adopt Ecosteer Data Visibility Control Overlay for their innovative projects. Indeed, new technologies contribute to advanced research capabilities, enhance collaborations with private and public entities and improve publication and dissemination. In return, Ecosteer will obtain visibility and prestige.

NGI. Being selected by Next Generation Internet initiative means being recognized as an innovator in the field of trust and security for data sharing. Visibility, prestige and contamination from the community are the main benefits of being part of NGI. In return, the community will be able to use the DOOF to easily deploy PETs within Clients' IT infrastructure. Additionally, Ecosteer will share its knowledge and competences in the field of consent management, Data Act and GDPR compliance by technology and multicast ned-to-end encryption.

8.2.14.4 Business Model Canvas

Funded by the European Union

TABLE 64: BUSINESS MODEL CANVAS OF DOOF

Business Model Canvas				
Key Partners NGI Research centres/universities Consulting firms and system integrators Benefits: • **normalize the approach towards integrating PETs within current enterprise IT architectures** • **minimize project deployment risks** • position themselves as **referral partners in the privacy realm** • **Resale of Ecosteer DVCO**	**Key Activities** R&D Tech support Project delivery Marketing & communication Sales **Key Resources** Technologies Personnel IP	**Value Propositions** By hiding all complexities exposed by the underlying DVCO components, as well as by any third-party Privacy Enhancing Technology populating the TrustChain ecosystem, this framework allows companies to **minimize** data exchanges deployment **costs and risks**.	**Customer Relationships** Self-service (download from GitHub) Direct support **Channels** • Internal salespeople • Through Partners' and shareholders' network • Website • GitHub & NGI • Conferences	**Customer Segments** Companies with a large customer base using consumers' data for various applications. Target sectors: energy and mobility; from 2026 financial services and healthcare Benefits: • **easily adopt PETs for IoT data sharing scenarios** of any size and across any industry • enable **GDPR and Data Act compliant** data exchanges • enhance **customers' trust and loyalty** • **minimize costs and legal liabilities related to consent management**.
Cost Structure Personnel (tech & customer support, marketing & legal) Cloud infrastructure			**Revenue Streams** With the open-source DOOF, Ecosteer will generate a second revenue stream from system integration services. The pricing model will be Project-based, with fixed fees for specific projects. Additionally, Ecosteer will offer hosting service for small size projects	

8.2.14.4.1 Value proposition

Ecosteer DOOF provides a standard framework to normalize the approach towards integrating Ecosteer DVCO as well as other PET technologies – such as those developed by other companies within NGI programs – within current enterprise IT architectures, enabling user-centric and privacy-compliant data exchanges.

By hiding all complexities exposed by adopted PET technology, this framework allows companies to minimize data exchanges' deployment costs and risks.

8.2.14.4.2 Customer segments

Ecosteer targets **companies with a large customer base using customers' data generated by smart devices/apps for various applications**. For these companies the compliance with the GDPR is not only a legal obligation but also an opportunity to enhance customer trust and loyalty.

Thanks to the DOOF, Companies can **easily adopt PETs for IoT data sharing scenarios** of any size and across any industry, turning their data sharing infrastructure into GDPR and Data Act compliant data exchanges. Privacy-centric data exchanges **enhance customers' trust and loyalty, while minimize costs and legal liabilities related to consent management**.

Being already on the market with a patented Privacy Enhancing Technology, the DVCO, Ecosteer will target those sectors where it can leverage an industry-specific

Funded by the European Union

knowledge and an established network of contacts. Initial target sectors are **energy** and **mobility**, followed by healthcare and financial services starting from Q1 2026. In terms of geography, Ecosteer will **start from the Italian market**, where it can leverage an already existing network of contacts, partners, and clients.

8.2.14.4.3 Channels

After the 9-month project the DOOF commercial development activities will be financed by Ecosteer.

Ecosteer will generate qualified leads through online and offline channels. To achieve these goals Ecosteer will update its website presenting the DOOF technology and will structure a content and social media marketing plan for Linkedin, YouTube and Medium channels. Ecosteer will scout and apply for calls for speakers in industry-focused events and conferences to present its technologies. A marketing and communication agency will be also engaged to support Ecosteer dissemination plan.

In addition, Ecosteer will also exploit the GitHub and NGI communities.

Ecosteer directly offers its technologies and services to target clients. To increase market reach Ecosteer is looking to partner with system integrators and large consulting firms who will provide both new channels to market and project delivery services. Additionally, Ecosteer also leverages its advisors to reach the target companies of a list that is continuously updated, according to market and competitive analysis.

8.2.14.4.4 Customer relationship

DOOF components can be directly downloaded from GitHub.

Beside the R&D team, Ecosteer will create internal dedicated technical sales and project delivery teams to manage the entire sales cycle for consulting services – from lead generation to project definition and delivery, until technical support. This team will be responsible also for knowledge transfer to system integrators and consulting firms.

8.2.14.4.5 Partners

Ecosteer will partner with system integrators and business consulting firms who will provide both new channels to market and project delivery services. Ecosteer can already leverage the formal partnership based on a reselling agreement with NTT Data, part of NTT Docomo, a multinational company providing system integration and IT services in different sectors such as mobility and energy. Furthermore, Ecosteer will partner with universities and research centres to obtain visibility, while contributing to their advanced research capabilities, their collaborations with private and public entities and to their publication.

DOOF allows partners to **normalize the approach towards integrating** Ecosteer **DVCO**, as well as any **other privacy enhancing technology, within current enterprise IT architectures, minimizing project deployment risks**. This technology will support Partners in **selling innovative projects**, enabling them to position as **referral partners in the privacy realm**.

Funded by the European Union

Ecosteer will offer them training and technical support for DOOF adoption in PET projects. This technology will spin up revenues from DVCO licenses – if this is the underlying selected PET technology. They can generate revenues also from resale of Ecosteer DVCO.

8.2.14.4.6 Key Activities

R&D activities aim at executing the Product Development Roadmap. At the end of this project DOOF will be in TRL7. Starting from Q4 2024 the product will undergo industrialization, optimization and further development activities.

To directly support clients willing to adopt the DOOF, Ecosteer will create a dedicated Delivery Engineers team to cover all the **technical & project management activities** along the entire project cycle, also **supporting Partners**.

Marketing & communication activities aim at increasing company visibility and product awareness across all channels. A detailed marketing and communication plan will be drawn up.

By leveraging marketing activities, the **sales** team will structure and execute the commercialization plan.

8.2.14.4.7 Key resources

The fundamental resource of any successful business is its people. Ecosteer will hire dedicated resources for R&D, technical support, project delivery, marketing, and sales activities.

Ecosteer technologies and its IP are the other key resources.

Additionally, Ecosteer will use a Cloud infrastructure for R&D and small size projects (typically pilot projects), as well as for offering hosting services.

8.2.14.4.8 Revenue streams

With the open-source DOOF, Ecosteer will generate a second revenue stream from system integration services. The pricing model will be project-based, with fixed fees for specific projects. Based on a daily tariff of €800 for junior resources, €1300 for senior resources and €1800 for the Head of R&D, Ecosteer will charge €38.700 for small size projects, € 77.4000 for medium size projects and €148.300 for large size projects.

Additionally, Ecosteer will offer hosting service for small size projects (€20000/each with 20% of margin).

Ecosteer's main revenue stream will be generated by its DVCO, offered as a yearly software license priced per number of devices where is the DVCO API is installed. Thanks to the DOOF Ecosteer will provide a standard framework to normalize the approach towards integrating Ecosteer DVCO within current enterprise IT architectures. This standardization will speed up DVCO adoption, expected to achieve 90K DVCO enabled devices by 2027, i.e. ca. 0,05% SOM (Italian market). With this market

Funded by the European Union

penetration, Ecosteer expects software license revenues to be about €5.8M. The DOOF will increase Ecosteer total revenues by about 20%, in line with software.

8.2.14.4.9 Costs

The cost structure of IT consulting services mainly encompasses:

Personnel, that is the major cost item. Ecosteer will hire 22 people by 2029; salaries, benefits, and other compensation for the employees, including R&D people, delivery engineers, and marketing and sales.

Marketing and business development activities;.

Travels for client meetings and onsite work.

Cloud infrastructure for R&D and small size projects

8.2.14.5 SWOT Analysis

Strenghts • Universal framework for any Privacy Enhancing Technology and any use case • Data Ownership focus • Open source	Weaknesses • Difficult to cover functionalities for all verticals
Opportunities • Usable by any sector • New Partnerships • Legal compliance	Threats • Insufficient financial resources for quick scale up

8.2.14.6 Cost-Benefit Analysis

(based on realistic tariffs/costs and market penetration scenarios)

Funded by the European Union

	Junior Resources	Senior Resources	Head of Tech			
	€ 800	€ 1.300	€ 1.800			
S Project	38	5	1	€ 38.700		
M Project	76	10	2	€ 77.400		
L Project	152	15	4	€ 148.300		
Proforma P&L	2024	**2025**	**2026**	**2027**	**2028**	**2029**
n.of small projects		2	5	8	13	18
n.of medium projects		1	3	5	9	12
n.of large projects		0	1	3	5	8
Revenues from services		€ 154.800	€ 574.000	€ 1.141.500	€ 1.941.200	€ 2.811.800
Hosting service (only for small projects)		€ 40.000	€ 100.000	€ 160.000	€ 260.000	€ 360.000
Total Revenues		€ 194.800	€ 674.000	€ 1.301.500	€ 2.201.200	€ 3.171.800
# personnel		1	2	2	4	5
Personnel R&D		€ 45.000	€ 110.000	€ 110.000	€ 220.000	€ 300.000
# personnel		1	2	4	5	8
Personnel Delivery		€ 45.000	€ 90.000	€ 180.000	€ 225.000	€ 360.000
# personnel		1	1	2	2	2
Personnel Marketing & Sales		€ 45.000	€ 55.000	€ 110.000	€ 110.000	€ 120.000
		76%	75%	79%	80%	83%
Other S&M costs		€ 24.000	€ 36.000	€ 36.000	€ 48.000	€ 48.000
Other G&A costs		€ 6.000	€ 24.000	€ 24.000	€ 24.000	€ 24.000
Other R&D costs		€ 11.600	€ 23.600	€ 44.000	€ 64.000	€ 84.000
Total costs		€ 176.600	€ 338.600	€ 504.000	€ 691.000	€ 936.000
EBITDA	-€ 84.000	€ 18.200	€ 335.400	€ 797.500	€ 1.510.200	€ 2.235.800
Net present value	3.554.916 €					
IRR	6%					

1.1.1.1.1 Costs

Ecosteer initial investment for developing the product is €199000. This cost is partially covered by NGI financing of €115000.

The main ongoing cost is personnel (15 people in total by 2029) for R&D, delivery services and sales and marketing (more than 80% of costs).

Among other R&D costs there is Cloud infrastructure.

Among other sales and marketing activities there are marketing & communication agencies, events and travels for S&M employees.

1.1.1.1.2 Benefits

From a business point of view, this technology will spin up the sales of Ecosteer DVCO and will increase company total revenues by about 20%, in line with software vendors' revenue split between software licenses and professional services. DOOF will also generate indirect benefits such as improved customer satisfaction due to less costs and risks of PET projects implementation.

Additionally, thanks to DOOF Ecosteer will gain overall operational efficiency for technology development and delivery.

8.2.14.7 Business Value and Relevance for TrustChain

Funded by the European Union

Ecosteer's DOOF framework being developed within the TrustChain ecosystem exemplifies an alignment with the core missions of both entities, promising a mutual enhancement of value and impact (please see section 9 INTEGRATING WITH GLOBAL OBJECTIVES OF TrustChain of this document). DOOF, by design, confronts the pressing issues of data ownership and control which are central to TrustChain's objectives under the European Commission's Next Generation Internet initiative. This synergy is grounded in shared commitments to ethical data governance, user empowerment, and fostering a decentralized digital society.

TrustChain ecosystem may benefit from the adoption of DOOF. Ecosteer's universal framework not only simplifies the integration of Privacy Enhancing Technologies (PETs) developed within TrustChain but also extends the reach and applicability of these technologies across various industry verticals. This capability amplifies TrustChain's mission to establish a resilient, secure, and trustworthy digital infrastructure that is inclusive and democratic.

In turn, by embedding TrustChain's principles, the DOOF framework enhances its market relevance and fortifies its position as a leader in ethical data exchange. Moreover, Ecosteer's participation in TrustChain's ecosystem facilitates access to a network of innovators, investors, and experts, accelerating product development and adoption through valuable feedback and peer collaboration. This interaction not only fuels Ecosteer's growth but also contributes to the collective advancement of TrustChain's goals, including the development of new business models and the removal of market barriers for decentralized technologies.

Thus, the partnership between Ecosteer and TrustChain creates a dynamic ecosystem where innovative solutions are not only conceptualized but are also actively implemented, tested, and refined. This establishes a robust foundation for continuous innovation, underpinned by shared values of privacy, security, and user-centric governance, ensuring that both parties propel each other towards achieving a more ethical and user-empowering digital future.

8.2.15 AURORA-MINDS

The Business Model Canvas (BMC) is a strategic management tool used to quickly and easily define and communicate a business idea or concept. It is a visual chart with elements describing a firm's value proposition, infrastructure, customers, and finances, assisting businesses in aligning their activities by illustrating potential trade-offs. Developed by Alexander Osterwalder and Yves Pigneur, the BMC provides a clear, structured format that allows organizations to brainstorm and map out the key activities, resources, partnerships, customer interactions, and revenue streams needed to make a business successful.

The widespread use of the Business Model Canvas can be attributed to its simplicity and effectiveness. It breaks down the fundamental elements of a business into easily understandable and manageable components, making it an excellent tool for both startups and existing businesses to explore new strategic directions. It also facilitates

Funded by the European Union

communication and understanding across different departments and stakeholders, ensuring that everyone is aligned on the business model and strategic path.

For the case of AURORA MINDS, the project team opted for creating at this stage three (3) different versions of the Business Model Canvas based on the following rationale:

- Exploring Strategic Alternatives: Each canvas can represent a different strategic path, showcasing alternative ways of creating value for customers and capturing revenue. This exploration can reveal new opportunities or highlight potential risks and challenges that might not be apparent with a single approach.
- Adaptability to Changing Conditions: Having multiple business models prepared allows a company to be flexible and adaptable, ready to pivot or adjust its approach in response to market feedback, technological changes, competitive pressures, or other external factors.
- Stakeholder Engagement: Different versions can cater to the interests or concerns of various stakeholders, including investors, partners, and key customers. This helps in securing support and resources from these stakeholders by presenting tailored strategies that align with their expectations or objectives.

Based on the above, next section describes three alternative business models and corresponding business model canvases, in order to effectively plan multiple strategic routes, ensuring preparedness and adaptability in today's dynamic business environment.

8.2.15.1 BUSINESS MODEL DESCRIPTION

In this section, three different versions of the business model canvas for future market exploitation of AURORA MINDS are explored. These models are described below:

- Version 1: Privacy for Health Risk Diagnosis or Monitoring Tool

  This version of the Business Model Canvas emphasizes the application of privacy technologies in health risk diagnosis or monitoring tools, offering robust data protection as a primary feature.

  By concentrating on the technological strengths and superior privacy features of the project, this business model aims to attract business clients as well as involved "consumer stakeholders" (parents, patients, etc.) looking for the most secure and effective health risk diagnosis and monitoring solutions available, ensuring a strong competitive position in a tech-driven market.

  The rationale for this strategic business model lies in the following:

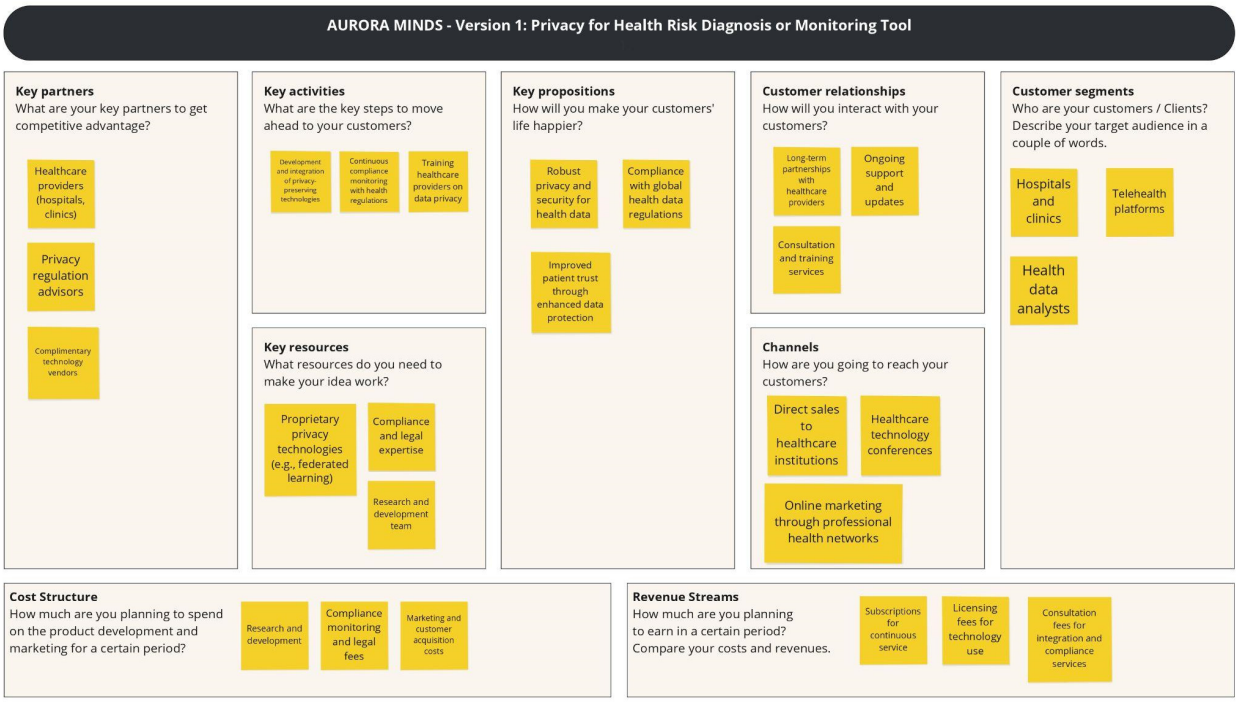
  - Core Focus on Health Data Privacy: This approach harnesses cutting-edge privacy technologies like federated learning and encryption to ensure that patient data remains secure and private. This is crucial in healthcare, where data breaches can have serious consequences.

Funded by the European Union

- **Compliance with Healthcare Regulations**: Ensuring compliance with global healthcare regulations such as HIPAA in the U.S. and GDPR in Europe enhances trust and marketability. This strategic compliance is not only about following laws but also about leveraging these standards as a key market differentiator.
- **Partnerships with Healthcare Providers**: Establishing partnerships with hospitals, clinics, and telehealth platforms can accelerate adoption by integrating the technology directly into existing workflows, making it a seamless part of the healthcare provision.
- **Subscription and Licensing Revenue Model**: Charging healthcare providers a subscription fee for using the platform, or licensing the technology to other companies, creates a continuous revenue stream while encouraging long-term commitments.

This model is designed to appeal directly to healthcare providers and organizations looking for secure, compliant, and efficient tools to handle sensitive health data, thereby improving patient outcomes while safeguarding privacy.

TABLE 65: BUSINESS MODEL CANVAS OF AURORA-MINDS – VERSION 1



Funded by the European Union

- Version 2: Privacy Mechanism for Citizen Data Integration in Smart City Platforms

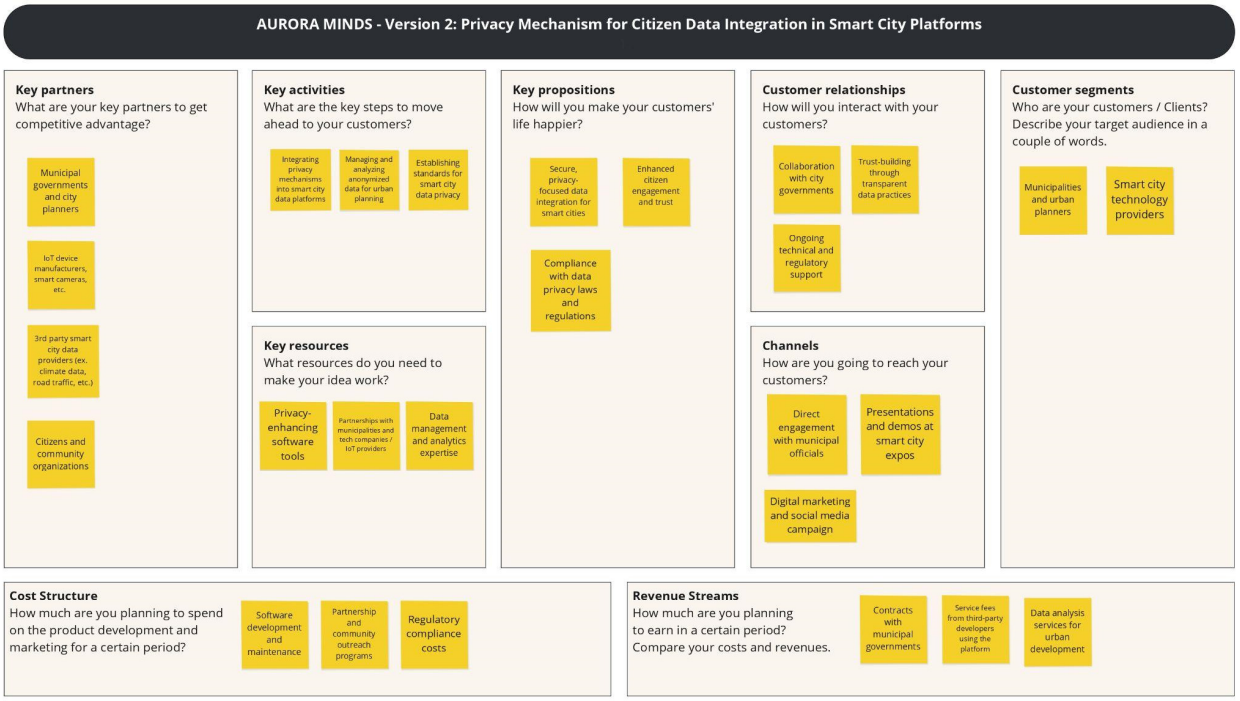
  This version is focused on integrating privacy mechanisms into smart city platforms, ensuring that citizen data is used responsibly and securely for urban management and services. The key rationale for this option includes the following:

  - Smart City Collaboration: Partnering with city planners and municipal governments to integrate the privacy mechanism into existing and new smart city infrastructures. This includes data from IoT devices, public Wi-Fi, mobility and transportation systems, city portal apps, etc.
  - Enhanced Citizen Trust and Engagement: By ensuring that citizen data is handled with utmost privacy, the project aims to increase public trust and encourage greater participation in smart city initiatives.
  - Diverse Revenue Streams: The AURORA MINDS approach allows for various revenue streams such as government contracts, public-private partnerships, and service fees from data analytics companies that benefit from the anonymized, aggregated data.
  - Compliance and Standardization: Adhering to international standards on data privacy and actively contributing to the development of new standards can position the project as a leader in smart city privacy solutions.

  This business model leverages the increasing demand for smart city solutions that prioritize citizen privacy, catering to government bodies and urban planners who need to balance technological advancements with privacy concerns.

Funded by the European Union

TABLE 66: BUSINESS MODEL CANVAS OF AURORA-MINDS – VERSION 2



- Version 3: Independent Technology Privacy Mechanism Applicable to Any Application

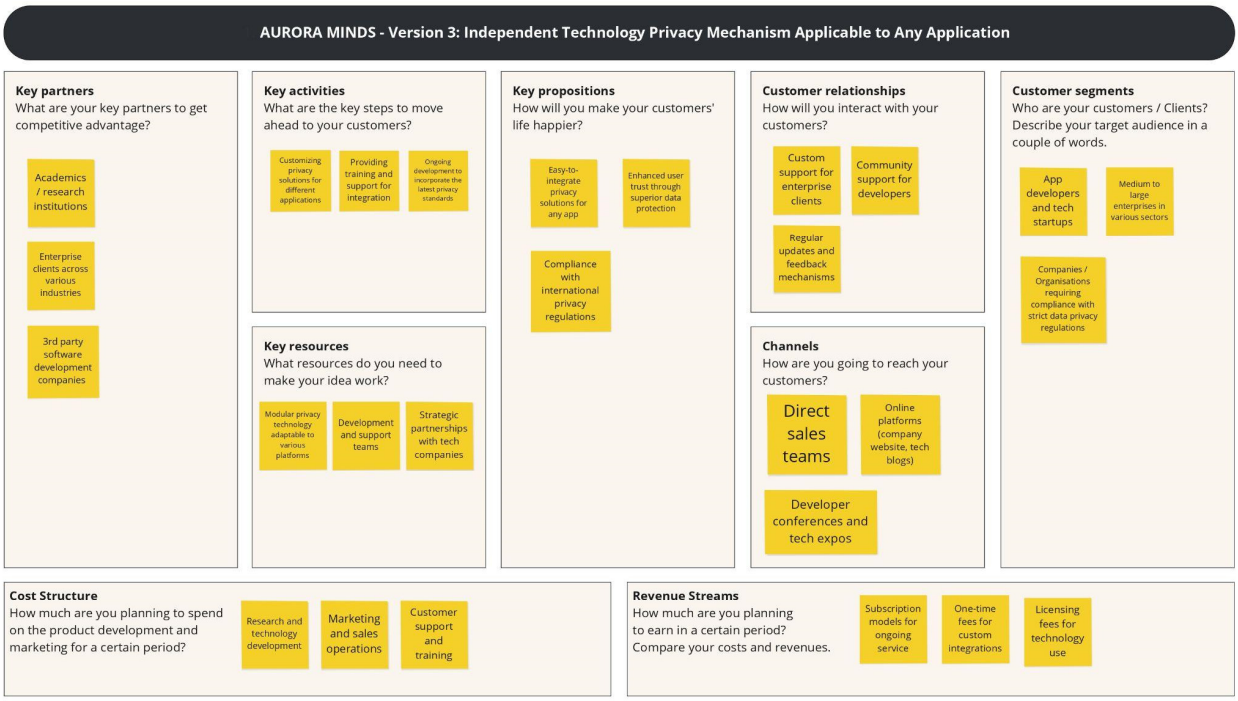
  The third version focuses on creating a versatile privacy mechanism that can be implemented across various applications, regardless of the industry, enhancing user trust and data security. The key rationale behind this option is as follows:

  - Broad Market Application: The technology is marketed as an independent solution that can be integrated with any existing application, from mobile apps to enterprise software, making it extremely versatile.
  - Focus on Developer and Corporate Partnerships: Building relationships with other software developers and corporate IT departments to embed the privacy technology in their applications from the ground up.
  - Flexible Pricing Models: Offering a range of pricing models, including pay-as-you-go, subscriptions, and premium packages, which can be tailored to the size and scope of the customer's needs.
  - Strong Emphasis on Innovation and Compliance: Continuously updating the privacy mechanisms to handle new types of data breaches and compliance requirements, thus staying ahead in a rapidly evolving tech landscape.

Funded by the European Union

This model aims to capture a broad market by offering a privacy solution that can be easily adopted by any application developer or company, thereby addressing the universal need for data privacy across sectors.

TABLE 67: BUSINESS MODEL CANVAS OF AURORA-MINDS -VERSION 3



8.2.15.2 SWOT analysis

The sections that follow provide an initial overview of the projected revenues as well as the forecasted costs for market exploitation of the project. Before estimating the key figures and project parameters, this section involves a preliminary SWOT analysis as part of the strategic planning process, in order to identify and understand the Strengths, Weaknesses, Opportunities, and Threats related to the business of the project. SWOT analysis helps organizations in assessing both internal and external factors that could impact their objectives.

Methodologically, a SWOT analysis is based on identifying the following:

- Strengths: Positive attributes that are within the control of the organization and upon which it can capitalize.
- Weaknesses: Factors that are within the organization's control that detract from its ability to attain the core goal or advantage.
- Opportunities: External attractive factors that represent reasons for an organization to exist and prosper.

Funded by the European Union

- Threats: External factors beyond your control that could place the project or organization's mission or operation at risk.

A SWOT analysis is crucial because it provides insights into where an organization currently stands and how it can advance towards future goals. This analysis is particularly valuable in strategic planning, as it helps to:

- Identify core competencies: Understanding what the organization does best and how it stands out in the marketplace.
- Minimize risks: Recognizing external threats allows organizations to form contingency plans.
- Leverage opportunities: By knowing the landscape, the organization can better spot and exploit growth opportunities.
- Address weaknesses: Identifying internal weaknesses gives the organization a chance to fix them or develop strategies to mitigate their effects.

The following table summarizes the SWOT analysis for the project AURORA MINDS:

TABLE 68: SWOT ANALYSIS

STRENGTHS	WEAKNESSES
• **Innovative Technology**: Use of federated learning, privacy-enhancing technologies, and blockchain for secure digital identities • **Compliance with GDPR**: Ensures data privacy and security, enhancing trust among users • **Focused Application**: Tailored specifically for the a specific health issue diagnosis	**Complex Technology**: High complexity of the technology might hinder user adoption or require significant user education. **Dependency on Third Parties**: Relies on collaborations with healthcare providers and educational institutions for data and pilot testing **Technological Dependence**: Dependence on 3rd party TRUSTCHAIN applications may hinder further market scalability
OPPORTUNITIES	**THREATS**
• **Growing Market for Health Diagnostics**: Increasing awareness and need for health and behavioral diagnostic tools. • **Potential for Expansion**: Ability	**Competitive Market**: High competition from existing digital health solutions and new entrants **Regulatory Changes**: Changes in

Funded by the European Union

to extend technology into other areas of health diagnostics or applications requiring privacy sensitivity, such as smart city / citizen applications • **Regulatory Trends Favoring Privacy**: Increasing regulations on data privacy could make AURORA MINDS more attractive to organizations seeking compliant solutions.	privacy laws and health regulations could affect operational capabilities **Technological Advances**: Rapid advancements in technology could render AURORA MINDS's current solutions obsolete if not continuously updated.

8.2.15.3 Competition

Regarding ADHD, there are numerous applications available that offer various approaches. Some of these focus on providing valuable information, promoting education, and ensuring high-quality care using checklists, such as Psychiatry-Pocket, and Adult-ADHD. Other apps offer mobile quizzes for diagnosing ADHD, while others help track and manage symptoms. Additionally, there are apps focused on using games for ADHD treatment. For example, Jumpy-Car and Magic-Land. Currently, there is a proliferation of digital applications and frameworks designed for diagnosing ADHD. These applications may not always adhere to established diagnostic criteria, leading to the potential for misdiagnosis or overdiagnosis. Some of these digital solutions have already been presented in Table VII of this report.

In the figure below, a direct comparison of the relevant apps to the proposed solutions in terms of machine learning algorithms utilization and privacy enhancements is provided. It is important to note that the current solution, Smartspeech, which serves as the baseline for AURORA MINDS, is also included in the comparison.

Funded by the European Union

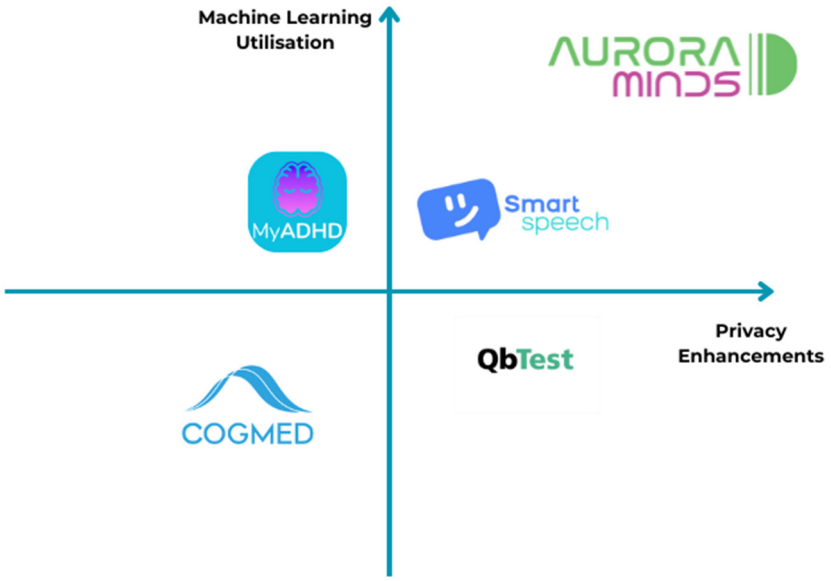


FIGURE 63: COMPARISON WITH EXISTING SOLUTIONS

8.2.15.4 Projected Revenue Streams

The project revenue streams can be generated by two main sources:

- monthly subscriptions of the AURORA MINDS secure / privacy preserving system and methodology, or
- lump sum project revenues generated by clients seeking a secure solution for ensuring high standards for privacy and compliance with protocols for personal data and dynamic consent management.

The table that follows demonstrates an estimation of the forecasted revenue streams.

Funded by the European Union

TABLE 69: FORECASTED REVENUE STREAMS

Sales forecast	Year 1	Year 2	Year 3
Client sales / monthly	8	12	23
Units /months (monthly subscription model)	67	100,8	193
Unit Pricing/month	3.700,00 €	3.700,00 €	3.700,00 €
Annual Sales from monthly subscriptions	**248.640,00 €**	**372.960,00 €**	**714.840,00 €**
Client sales / lump sum	7	10	20
Unit Cost / Lump Sum	24.000,00 €	24.000,00 €	24.000,00 €
Annual Sales from lump sum sales	168.000,00 €	240.000,00 €	480.000,00 €
Total Sales	**416.640,00 €**	**612.960,00 €**	**1.194.840,00 €**

8.2.15.5 Forecasted Costs

The table that follows depicts the main economics of the costs involved:

TABLE 70: FORECASTED COSTS

Cost of sales	83.328,00 €	122.592,00 €	238.968,00 €
Gross margin	333.312,00 €	490.368,00 €	955.872,00 €
Nr. of employees	5	7	9

These costs involve:

- direct inputs necessary to create the product or service
- Direct labor costs associated with the production of goods or delivery of services
- overheads, which may include utilities, maintenance, and costs of manufacturing equipment
- Marketing and sales expenses directly attributed to the selling of services or products
- handling costs
- Costs related to technology infrastructure, such as servers or cloud services

Funded by the European Union

- Payments for software used in providing services to clients
- sales commissions

The number of employees indicates labor costs, which would typically include:

- Salaries and wages
- Benefits and taxes
- Training and development

8.2.15.6 Key Parameters and Indicators

In this section, a preliminary strategic assessment of the AURORA MINDS project is described. Overall, the provided data suggests that the project has a solid financial strategy with substantial revenue growth and effective cost management. However, maintaining this trajectory will require careful monitoring of market conditions and customer behavior. Specifically, based on the Year 1 to Year 3 Revenue and Cost Analysis, the following summary can be made:

Revenue and overall cost analysis

- Revenue Growth: Revenue is projected to nearly triple from €416,640 in Year 1 to €1,194,840 in Year 3. This indicates a strong upward trend in sales both from monthly subscriptions and lump sum payments.
- Increasing Client Base: Both the monthly and lump sum client bases are growing, with monthly sales more than doubling and lump sum sales almost tripling by Year 3. This is a positive sign for market acceptance and demand.
- Price Stability: Unit pricing remains constant at €3,700 per month, however, it may be necessary to adjust this pricing year by year.
- Cost of Sales and Margin: While costs are increasing, the gross margin is increasing at a higher rate, which suggests the project is achieving some economies of scale or improved efficiency.

Economical Health

- Profitability: The business is profitable across all three years, with a significant increase in profitability over time.
- Cost per Employee: This trajectory suggests improving operational efficiency.
- Scalability: The model suggests scalability, with the costs not growing as rapidly as revenues, indicating that the business can grow without a proportionate increase in costs.

Strategic Observations:

Funded by the European Union

- **Lump Sum Sales**: A substantial portion of revenue is coming from lump sum sales, which might pose a risk if there's overreliance on what could be one-off contracts.
- **Sustainability**: The subscription model provides a predictable, recurring revenue stream, which is generally favorable for long-term sustainability.
- **Cost Management**: The increase in employees is relatively modest compared to revenue growth, which suggests good cost management.

Potential Risks and Considerations:

- **Market Saturation**: As the business grows, the business strategy adopted must be wary of market saturation. Strategies for new market penetration or product diversification may be necessary.
- **Customer Retention**: Retaining monthly subscribers is crucial. The cost of acquiring a new customer versus retaining an existing one should be carefully balanced.
- **Competitive Pricing**: If competitors emerge, the company exploiting AURORA MINDS may need to review its pricing strategy.
- **Economic Factors**: External economic factors, such as inflation and purchasing power, can affect both costs and sales.

8.2.15.7 VALUE NETWORK

In the scope of analysing the business value of the AURORA MINDS system, in this section, a business value network diagram is illustrated.

In principal, a **value network diagram** is a graphical representation of the actors and roles involved in a business ecosystem, as well as the interactions and relationships between them. It illustrates the flow of objects, knowledge, and money between the different stakeholders in the ecosystem, and shows how they collaborate to create and deliver value. The diagram is used in business modelling to understand the interdependencies of stakeholders and to design sustainable business models that contribute to the achievement of Sustainable Development Goals (SDGs). The diagram is also used to assess the sustainability of the business model, by analyzing the cost and revenue models of each actor in the ecosystem. By examining the revenue and costs per year over an investment period, economic indices of value such as Internal Rate of Return, Net Present Value, and Payback Period can be calculated to determine the economic sustainability of the business model.

To illustrate the business value network, the focus will now be on the first version of the Business Model Canvas, titled "Privacy for Health Risk Diagnosing and/or Monitoring Tool." The business value network illustrates the interactions between the different actors and roles in the ecosystem, based on the value proposition, key partners,

Funded by the European Union

customer segments, and other components defined in the business model canvas. The value network diagram provides a visual representation of the relationships and interactions between the different actors in the ecosystem, and helps to identify opportunities for collaboration, innovation, and streamlining processes throughout the value chain. By understanding the value network, businesses can develop more effective strategies for creating and delivering value to their customers and stakeholders.

The value network diagram for Aurora Minds, as depicted below, demonstrates the interactions between the various stakeholders involved in the system, including children, parents, educators, clinicians, and the Digital Identity Provider. The diagram also illustrates the flow of data, knowledge, and money between these stakeholders, highlighting the key components of the system, such as federated learning, local differential privacy, and Privacy-ABCs.

Here are the main components of the diagram:

- **Stakeholders**: key stakeholders in the Aurora Minds ecosystem for the health communication disorder use case includes children, parents, educators, clinicians, as well as the Digital Identity Provider.
- **Actor Roles**: Data Provider children subjects, parents, educators) Service providers), infrastructure provider.
- **Value Network**: subscriptions from clinicians to the service provider, data collection from children subjects, output to clinicians and parents & educators.
- **Federated Learning**: local model parameters are shared between clinicians to perform federated learning and increase the accuracy and generalization ability of the model while preserving raw data privacy.
- **Identity Provider (IdP) System**: the IdP System verifies the identities of end-users and the ones from clinicians, enabling data sharing and consent.
- **Data Collection**: data generation through children's interactions with the gamified mobile app as well as through surveys completed by parents.
- **Selective and Minimum Disclosure**: users having full control over which parts of their sensitive data they are willing to reveal to whom, and the ability to check whether certain relying parties are eligible to request certain pieces of information.
- **Anonymity**: when necessary, anonymity is used to maximize user privacy.

The following figure depicts the way different stakeholders interact with each other and the core application / system to support secure consent management and access rights or data related with the use case of the risk diagnosis for communication in young children.

Funded by the European Union

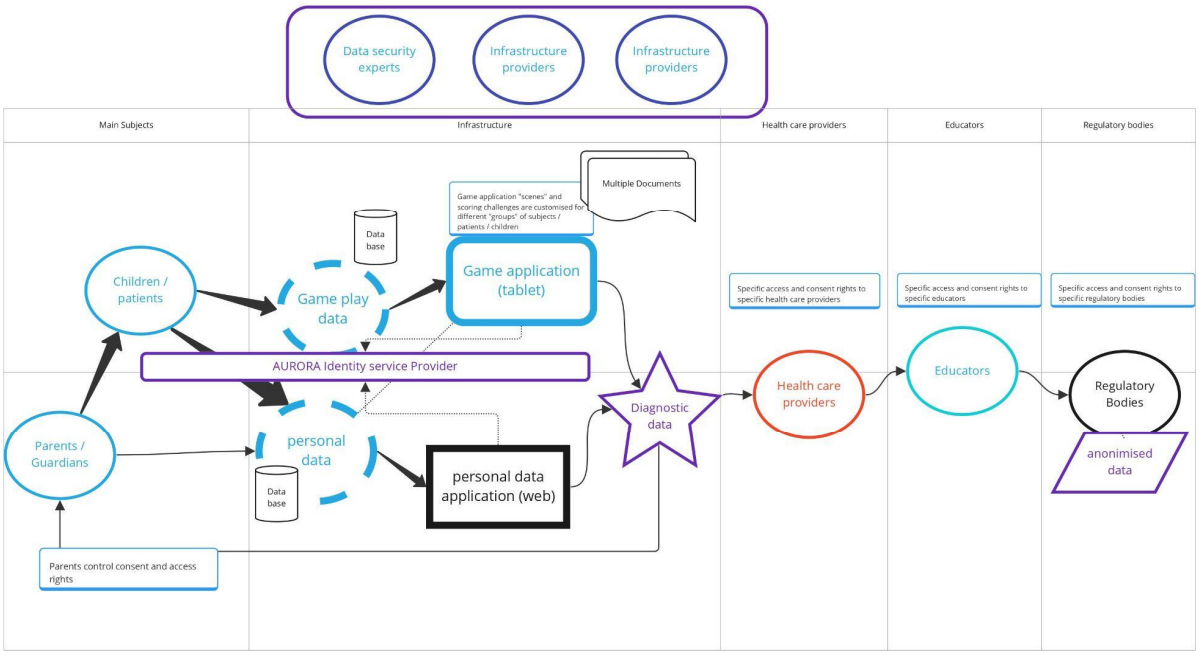


FIGURE 64: APPLICATION'S DIFFERENT STAKEHOLDERS

To perform a strategic assessment of the value of the business proposition created, a map is created that analyzes the value network of the AURORA MINDS system within its ecosystem, allowing for analysis of the exchange from an organic, dynamic, and systemic perspective. This map seeks to represent a wide territory network of the roles and interactions that generates the business "good" of the AURORA MINDS system. This map, named as a value network, provides a human -centric, role-based, network view of any business activity involved. The value network for AURORA MINDS is as follows:

Funded by the European Union

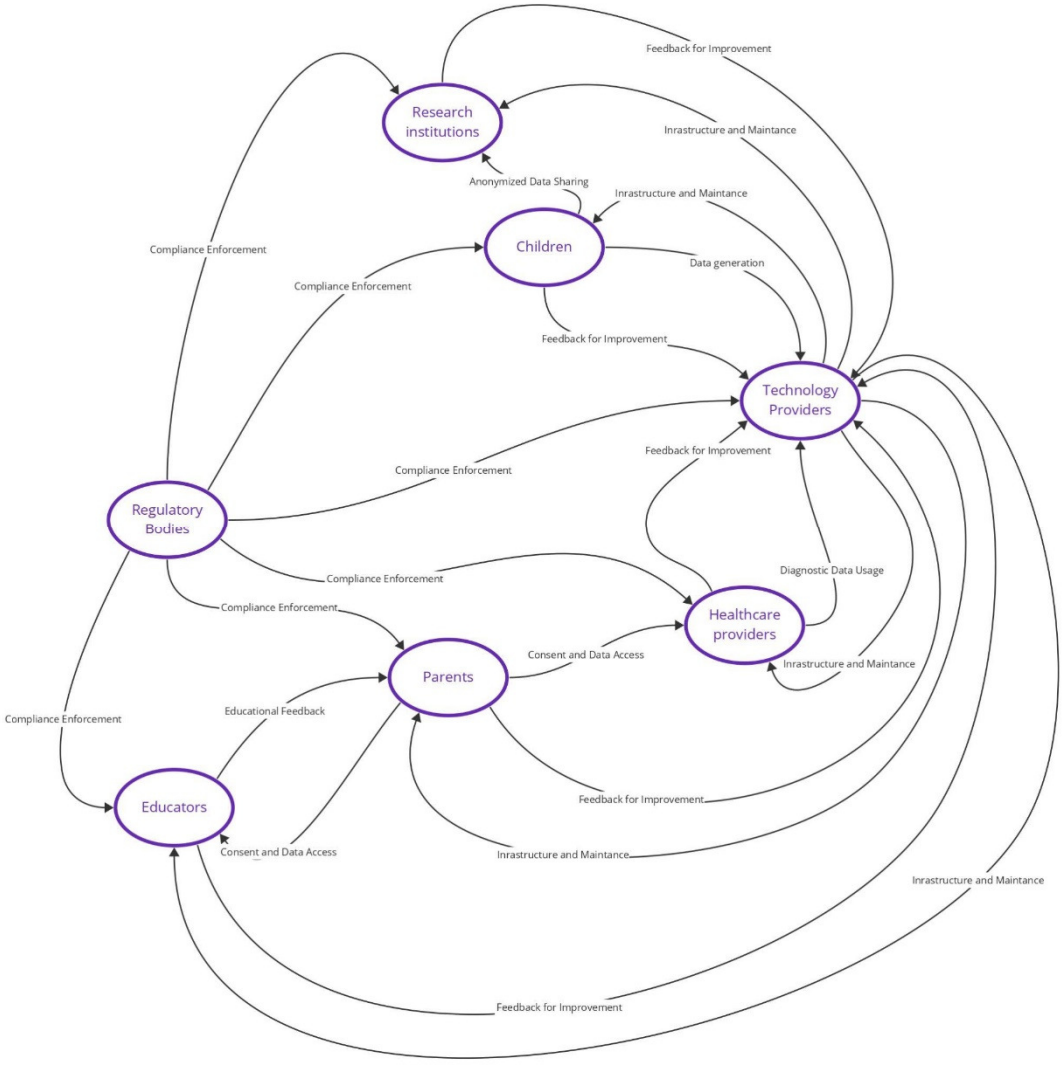


FIGURE 65: VALUE NETWORK DIAGRAM

The diagram appears to be a value network for the AURORA project, showcasing how different stakeholders interact with one another and the types of value exchanges that occur between them.

- **Children**: At the center of the network, they provide behavioral data through interaction with the system. Their data is used by Research Institutions for analysis and by Healthcare Providers for diagnostic purposes.
- **Research Institutions**: Receive anonymized data from Children for study and provide feedback for system improvement to Technology Providers.

Funded by the European Union

- Healthcare Providers: Utilize diagnostic data to treat and support Children and also contribute feedback for the improvement of the Technology Providers' systems.
- Parents: Grant consent and access to Children's data for Healthcare Providers and Educators, and receive educational feedback from Educators.
- Educators: Access data to aid in the educational support of Children, based on the consent provided by Parents.
- Regulatory Bodies: Enforce compliance across the network, ensuring that all interactions and data exchanges adhere to legal and ethical standards.
- Technology Providers: Offer the infrastructure and maintenance for the system used by all stakeholders and receive feedback for system improvements from various sources within the network.

8.2.16 DUME

8.2.16.1 Market analysis

Urban management and waste collection efficiency are critical components of smart city initiatives globally. Civic Engagement Platforms like NYC311, FixMyStreet, and MeinBerlin have paved the way for citizen engagement in urban management, but they come with limitations including underreporting, false reporting, and non-uniform citizen participation. These platforms rely heavily on manual inputs from citizens, which can lead to data inaccuracies and inefficiencies.

Theia Vision introduces a novel approach by automating the detection and classification of urban occurrences, using AI-driven analysis of massive image collections from public spaces. This not only enhances accuracy but also reduces the dependency on citizen reporting, addressing the core limitations of current Civic Engagement Platforms.

8.2.16.1.1 Competitor Analysis

In the competitive landscape of urban management technologies, Theia Vision stands out with no direct competitors currently matching its comprehensive approach. The technologies discussed below represent the closest parallels in the market, each contributing unique solutions to aspects of waste management and environmental monitoring. However, it's important to note that none of these technologies compete directly with Theia Vision. Instead, they address related challenges with differing focuses and technologies. This analysis highlights how Theia Vision differentiates itself by integrating advanced AI to automatically detect, classify, and manage urban occurrences in public spaces—a groundbreaking approach that these indirect competitors have not yet adopted.

Funded by the European Union

Bigbelly Core Offerings: Bigbelly is known for its network-connected solar-powered waste and recycling stations, which compact waste and communicate status to collection crews to optimize pick-up schedules.

Comparison with Theia Vision:

- Technology: Bigbelly's focus is on hardware solutions to optimize physical waste collection logistics. In contrast, Theia Vision integrates advanced AI algorithms to analyze images for detecting various urban waste types and other environmental issues, providing a broader scope of urban management solutions.
- Community Engagement: Bigbelly lacks features for direct community interaction through a mobile app, which Theia Vision offers, enabling real-time reporting and monitoring of urban cleanliness and safety issues by residents.
- Market Focus: While Bigbelly is primarily focused on reducing the frequency of waste collection and associated costs, Theia Vision aims to enhance the quality of urban environments comprehensively, including public health and safety through its automated detection system.

Rubicon Global

Core Offerings: Rubicon Global provides a technological platform for waste, recycling, and smart city solutions to businesses and governments, designed to improve waste and recycling operations.

Comparison with Theia Vision:

- Service Scope: Rubicon focuses mainly on commercial entities and offers solutions tailored for business waste management logistics and recycling processes. Theia Vision, however, targets a broader spectrum including public spaces, thus contributing directly to urban public health and aesthetics.
- AI Utilization: Unlike Rubicon, which primarily uses digital platforms for operational optimization, Theia Vision employs AI to actively monitor and classify types of waste and environmental hazards in public areas, making it more dynamic and responsive to urban management needs.
- User Interaction: Rubicon's platform is used by businesses and government entities without direct citizen involvement. Theia Vision encourages active citizen participation through its mobile app, enhancing community engagement and responsiveness.

Nordsense

Funded by the European Union

Core Offerings: Nordsense provides sensor-based waste bin monitoring solutions that enable cities and waste operators to manage waste collection more efficiently.

Comparison with Theia Vision:

- Technological Approach: Nordsense uses IoT sensors to monitor waste bin levels to optimize the logistics of waste collection. Theia Vision takes a more comprehensive approach by using AI to detect and analyze waste directly from images taken in public spaces, offering insights into waste types and locations rather than just bin levels.
- Data-Driven Solutions: While Nordsense offers data on waste levels for operational optimization, Theia Vision provides actionable insights based on visual data, which can be used for more strategic urban planning and environmental management.
- Scope of Application: Nordsense's solution is limited to waste bins, whereas Theia Vision's capabilities encompass a wider range of public space monitoring applications, making it more versatile.

Enevo

Core Offerings: Enevo focuses on optimizing waste collection routes through ultrasonic sensors that measure the fill-level of waste containers and predict the optimal collection times.

Comparison with Theia Vision:

- Innovative Technology: Enevo's approach, while innovative in optimizing collection routes, does not provide the broader environmental monitoring that Theia Vision's image analysis and AI capabilities offer.
- Real-Time Monitoring and Classification: Enevo lacks the real-time monitoring and classification of waste types in public spaces that Theia Vision provides, which can significantly enhance urban management strategies beyond just waste collection.
- Public Engagement: Enevo operates primarily with municipal and private waste management services, with no direct engagement model for the public. Theia Vision's platform empowers citizens to actively participate in maintaining and improving their urban environments.

8.2.16.1.2 Stakeholders and Potential Partners

The stakeholders and potential partners for Theia Vision encompass a broad range of entities, each contributing uniquely to the platform's ecosystem and benefiting differently from its deployment:

Funded by the European Union

1. Citizens: Individuals with an interest that their neighborhood and city is kept clean and safe. They are the primary beneficiaries of Theia Vision's functionalities, directly experiencing in their daily lives the improvements in urban management.

2. Image Capturing Companies: Companies possessing extensive capabilities to capture images over vast urban areas, such as logistics companies and personal transport services. These stakeholders have an interest in enhancing their corporate social responsibility by visibly improving the communities and cities they operate in.

3. Clients (Notification Recipients): Entities such as local governments, advertising companies, utility companies, recycling companies, and urban planners, who benefit from real-time notifications of urban events affecting their operations and responsibilities.

4. Local Governments: Local government bodies are primary stakeholders in public space management, with vested interests in maintaining cleanliness and ensuring efficient operations within urban settings. Theia Vision offers local governments a technology-driven solution to monitor and manage public spaces more effectively. By automating the detection and classification of urban waste and other environmental issues, Theia Vision can help these entities save on labor costs, optimize resource allocation, and enhance responsiveness to urban cleanliness issues. Furthermore, the data collected can aid in policy formulation and urban planning, providing insights into problem areas and the effectiveness of current policies.

5. Environmental Agencies: These agencies are committed to preserving natural resources and ensuring sustainable urban development. Theia Vision can serve as a vital tool for these agencies by providing detailed, real-time data on various environmental parameters such as the prevalence of waste or the health of urban greenery. This data can be crucial for environmental impact assessments, enabling these agencies to monitor the effectiveness of sustainability programs and make data-driven decisions to improve environmental policies and practices.

6. Community Organizations: Non-profits and community groups play a crucial role in mobilizing local populations and fostering civic engagement. These organizations can partner with Theia Vision to promote citizen participation in urban cleanliness initiatives. By using Theia Vision’s mobile app, community members can actively contribute to monitoring and reporting on local urban issues, creating a more engaged and responsible citizenry. This partnership not only helps in maintaining cleaner public spaces but also empowers individuals by making them active participants in their community's welfare.

7. Technology Providers: Collaboration with companies that specialize in AI, IoT devices, and software development is essential for the continuous improvement of Theia Vision’s capabilities. Technology providers can offer the latest

Funded by the European Union

advancements in image recognition, data processing, and device integration, enhancing Theia Vision's accuracy and expanding its functionality. For instance, IoT device manufacturers can supply advanced sensors and cameras that improve the quality and frequency of data collection, while AI firms can refine the algorithms that analyze this data, leading to more precise occurrence detection and classification. Also, companies like Inrupt, Inc., which supports Solid open-source technology, are crucial for maintaining the platform's technological edge.

8.2.16.1.3 Opportunities

- **Smart City Initiatives**: Many cities worldwide are investing in smart technologies to improve urban living, which represents a significant opportunity for Theia Vision.
- **Sustainability Focus**: Increased global emphasis on sustainability can drive adoption of AI-based, efficient waste management solutions.
- **Technological Advancement**: Rapid advancements in AI and IoT present opportunities for continuous improvement and integration of new technologies into Theia Vision.

8.2.16.1.4 Challenges

- **Technology Adoption**: Resistance from traditional waste management entities and local bureaucracies could slow down adoption.
- **Data Privacy Concerns**: Collection and analysis of public space images must comply with stringent data protection regulations, which could pose implementation challenges.
- **High Initial Costs**: Deployment of AI technologies and the necessary infrastructure might require substantial initial investment.

8.2.16.1.5 Final remarks

The market for urban waste management solutions is ripe for disruption by innovative technologies like those proposed in Theia Vision. By addressing the shortcomings of current civic engagement platforms and offering a technologically advanced solution, Theia Vision is well-positioned to lead this new market segment. However, successful market penetration will depend on strategic partnerships, adept handling of regulatory challenges, and effective community engagement to foster widespread acceptance and use.

8.2.16.2 Business Model

Funded by the European Union

In the rapidly evolving landscape of urban monitoring and management, Project DUME, through the platform Theia Vision, presents a robust and sustainable business model designed to ensure both financial viability and exceptional service delivery. This comprehensive model delineates diverse revenue streams and managed cost streams, crafted to address the needs of various stakeholders ranging from local governments to private enterprises. By leveraging advanced technological capabilities and adhering to rigorous financial planning, Theia Vision aims to improve urban data analytics while maintaining operational excellence and growth potential.

The revenue streams of Theia Vision have been strategically diversified to maximize financial sustainability. This is achieved through a mix of subscription plans, API access fees, and tailored data analytics services. These revenue channels are carefully designed to meet the distinct needs of different sectors, providing flexible and scalable solutions that cater to specific operational demands and budget constraints. The varied subscription packages, comprehensive API access, and detailed data analytics offerings ensure that Theia Vision remains a valuable asset for all its users.

Simultaneously, Logimade, the driving force behind Theia Vision, incurs various costs essential to sustaining and enhancing this innovative urban management platform. These costs, categorized into development, operational, and market expansion expenses, are crucial for maintaining the platform's efficiency, security, and user satisfaction. By investing in continuous development, robust operational infrastructure, and proactive marketing and sales strategies, Logimade ensures that Theia Vision not only meets current demands but also anticipates future needs, solidifying its position as a leader in urban monitoring solutions.

8.2.16.2.1 Revenue Streams

Theia Vision has strategically diversified its revenue streams to maximize the platform's financial sustainability and service delivery. This is achieved through an offering of subscription plans, API access fees, and data analytics services, each tailored to meet the distinct needs of various stakeholders ranging from local governments to private enterprises:

Subscription Plans: Subscription plans are designed to cater to different sectors by offering customized packages that vary in terms of event type coverage, geographic area, number of events, feature access, and validity periods. These plans ensure flexibility and scalability, allowing users from different sectors to choose services that best fit their operational needs and budget constraints.

API Access Fees: Theia Vision provides API access that enables third parties to integrate its advanced urban monitoring capabilities into their own systems. This service is crucial for tech companies looking to enhance their applications with real-time urban data analytics, thereby generating a steady stream of revenue from API licensing.

Data Analytics Services: Tailored data analytics services offer clients custom reports and insights specific to urban management tasks. These services are essential for decision-

Funded by the European Union

makers requiring detailed analytics on urban trends, event impact assessments, and operational planning.

The paid service packages of Theia Vision are available directly through the mobile and backoffice applications, and include the following types of packages:

Issues/Events Packages:

- Access to Detected Issues/Events: Users can view detailed information about each event, including type, location, and associated imagery.
- Event Reports for Decision Support: These reports provide critical insights such as the frequency of occurrences over time, average resolution times, and hotspots for different types of events.

Street Navigation with Up-to-Date Images:

- This service offers a navigation interface similar to Google Street View but features much more recent images. It is particularly valuable for companies in the utilities sector that depend on up-to-date geographic data for daily operations.

API Package:

- Broad Access for Integration: Users purchasing this package can access Theia Vision's comprehensive API for integrating urban image data and metadata into their systems.
- Target Audience: This package is especially beneficial for AI companies and developers looking to create custom solutions or enhance their services with Theia Vision's data.

Pricing Modalities:

- Pay-As-You-Go: This flexible pricing option allows users to pay for only the services they use, ideal for smaller entities or sporadic needs.
- Fixed-Price: Offering predictable costs, this modality is suited for larger organizations requiring consistent access to Theia Vision's services.

8.2.16.2.2 Cost streams

In order to sustain and enhance Theia Vision innovative urban management platform, Logimade incurs various costs associated with development, operations, and market expansion. Understanding and keeping these costs under control is crucial for maintaining the platform's efficiency and effectiveness, while ensuring strategic financial planning and resource allocation.

Development Costs:

Funded by the European Union

- AI Capabilities Enhancement: There's an intrinsic need to continuously invest in improving Theia Vision artificial intelligence systems to enhance event detection accuracy and expand the range of detectable urban issues. This involves funding advanced research, algorithm optimization, and the integration of the latest AI technologies.
- Platform Functionalities: Regular updates and upgrades are essential to keep the platform responsive to user needs and technological advancements. This includes developing new features, improving the UI, refining existing services, and ensuring the platform's architecture can scale with growing user demands.
- Solid Pod Server Integration: Continuous development efforts are required to integrate and maintain compatibility with Solid Pod Servers. This includes adapting to updates in server technology and ensuring that Theia Vision's platform can effectively interact with these servers for storing and retrieving high-resolution, georeferenced images and associated metadata.
- Authentication and Authorization Mechanisms: The Solid protocol uses Web Access Control (WAC) lists for authentication and authorization, which necessitates regular updates to Theia Vision's systems to align with new security practices and standards introduced in the Solid community. This includes implementing and updating mechanisms that handle ACLs to ensure secure and flexible data access controls within the platform.
- Metadata Synchronization: As Theia Vision handles extensive datasets involving urban management, ensuring effective metadata synchronization across different components of the Solid architecture is crucial. This involves developing systems that can efficiently manage RDF metadata updates, deletions, and queries in real-time, aligning with the decentralized nature of the Solid protocol.
- Image Data Cache Mechanism: Critical for AI training modules within Theia Vision, the image data cache mechanism requires ongoing development to optimize data retrieval speeds and processing efficiency.

Operational Expenses:

- Server Maintenance: Robust server infrastructure is critical for the real-time processing and storage of large volumes of image data and user interactions. Regular maintenance ensures high availability and performance, which are critical for user satisfaction and service reliability.
- Data Storage: As a data-intensive application, Theia Vision requires substantial investment in secure and scalable data storage solutions to handle the increasing influx of urban data from multiple sources.
- Customer Support: Providing timely and effective customer support is essential for maintaining user trust and satisfaction. This includes staffing support centers,

Funded by the European Union

training customer service personnel, and implementing support software solutions.

- **Compliance Management:** With a strong commitment to privacy and data security, Theia Vision invests in compliance with various data protection regulations such as GDPR. This involves regular audits, compliance training for staff, and updates to security measures to safeguard user data.

Marketing and Sales:

- **Outreach Initiatives:** To capture a larger market share and engage with potential users, Logimade must create various marketing campaigns across digital and traditional media platforms. This includes online advertising, social media campaigns, public relations efforts, and participation in industry fairs and conferences.
- **Engagement Initiatives:** Building and maintaining strong relationships with existing users and partners is crucial for long-term success. Engagement activities might include community events, webinars, training sessions, and user conferences designed to increase platform loyalty and user activity.
- **Sales Operations:** Developing and sustaining an efficient sales team to handle inquiries, negotiate contracts, and close deals with potential clients, especially in targeted sectors like government and large corporations, which require dedicated account management.

Funded by the European Union

8.2.16.2.3 Business Model Canvas

TABLE 71: BUSINESS MODEL CANVAS OF DUME

Business Model Canvas	Designed for:	Designed by:	Date:	Version:
	DUME	Logimade Lda	25/07/2024	V0.1

Key Partners	Key Activities	Value Propositions	Customer Relationships	Customer Segments
Local Governments Private Enterprises Tech Companies AI/ML Researchers Solid Protocol Community Data Storage Providers Marketing Agencies Customer Support Services	AI Model Training and Validation Platform Development and Maintenance Integration with Solid Protocol Data Collection and Processing Customer Support and Training Compliance Management Marketing and Sales Outreach Partnership Development	Project DUME offers unmatched urban event detection with detailed characterization, including event type, severity, high-resolution images, GPS location, and continuous monitoring. The decentralized architecture ensures user data control, privacy, and security. Theia Vision's multi-applicability spans waste management, infrastructure, safety, and more, with no competition. It fosters community engagement by empowering data contributions and adheres to "privacy by design" principles, ensuring anonymity and trust.	**Citizens**: Empowerment through technology, data transparency, and community contribution. **Image Capturing Companies**: Enhance corporate responsibility and visibility. Companies provide broad image datasets from diverse geographic areas. **Clients**: Event detection and reporting, continuous monitoring, and analytical metrics.	**Citizens**: Individuals engaged in community improvement and urban management, contributing data and feedback. **Local Governments**: Municipalities needing detailed urban event data for planning, services, and performance evaluation. **Private Enterprises**: Companies using data for corporate responsibility, brand visibility, and operational efficiency. **Image Capturing Companies**: Organizations with logistical capabilities providing extensive geographic data for analysis. **Tech Companies and Developers**: Businesses integrating urban data into their applications for enhanced functionality.
	Key Resources Advanced AI/ML Algorithms Solid Protocol Integration High-Performance Servers and Scalable Data Storage Skilled Development and Research Team Customer Support Infrastructure Marketing and Sales Teams Regulatory Compliance Experts Funding for Continuous R&D and Platform Enhancements		**Channels** Mobile App for direct user engagement. API for integration with third-party systems. Online Advertising and Social Media. Industry Fairs and Conferences Community Events. Customer Support Centers. Efficient integration with existing workflows and user routines.	

Cost Structure	Revenue Streams
Project DUME is value-driven, focusing on creating a premium value proposition. The most significant costs are associated with advanced AI/ML development, Solid Protocol integration, and maintaining high-performance servers and scalable data storage. Key activities, such as continuous platform enhancements and compliance management, are also major expenses. Fixed costs include salaries for skilled development and support teams, rents, and utilities. Variable costs cover marketing campaigns and customer engagement initiatives. Economies of scale are achieved through widespread adoption, while economies of scope are realized by expanding platform functionalities and applications.	Customers value Theia Vision's advanced urban monitoring and are willing to pay for subscription plans, API access fees, and data analytics services. They currently pay through fixed pricing models, including list prices and feature-dependent subscriptions. Preferred payment methods include pay-as-you-go and fixed-price subscriptions. Major revenue streams are subscription fees, licensing for API access, and custom data analytics reports. Each stream contributes significantly to overall revenues, with subscriptions providing a stable base and API fees and analytics services adding substantial value. Pricing is primarily fixed, tailored to customer needs and usage volumes.

8.2.16.2.4 Value network

Theia Vision orchestrates a comprehensive value network that leverages technology to enhance urban management through community engagement and data-driven insights. This network creates a synergistic environment where citizens, companies and public authorities interact, sharing resources and information to collectively improve urban spaces. The platform facilitates this by offering advanced analytics, real-time data, and a decentralized framework, ensuring all participants—citizens, image capturing companies, and clients—benefit from enhanced operational efficiencies and community welfare.

Funded by the European Union

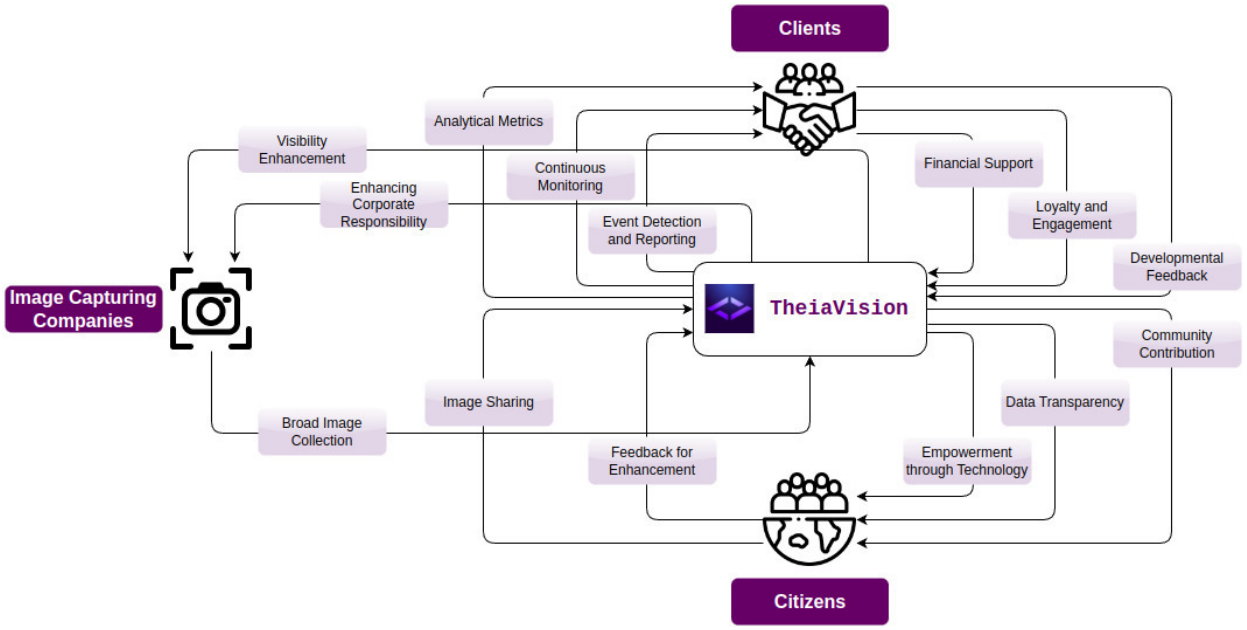


FIGURE 18 – VALUE NETWORK

Interactions with Citizens:

- From Theia Vision to Citizens:
  - **Empowerment through Technology:** Provides citizens with the tools to actively keep their neighborhoods clean and safe, fostering a proactive community environment.
  - **Data Transparency:** Offers objective data on local government performance, helping citizens understand and evaluate service efficacy.
  - **Community Contribution:** Enhances citizens' sense of involvement and impact within their community by allowing them to contribute directly to urban management.
- From Citizens to Theia Vision:
  - **Image Sharing:** Citizens contribute by sharing targeted sets of images from localized areas, capturing specific events that directly affect their daily lives.
  - **Feedback for Enhancement:** Citizens provide essential feedback that informs continuous product development, ensuring the platform meets their evolving needs.

Interactions with Image Capturing Companies:

Funded by the European Union

- From Theia Vision to Companies:
    - **Enhancing Corporate Responsibility:** Assists companies in boosting their social responsibility profiles by documenting their contributions to urban improvement.
    - **Visibility Enhancement:** Increases public visibility of the companies' efforts, reinforcing their brand image among public authorities, consumers, and other stakeholders.
- From Companies to Theia Vision:
    - **Broad Image Collection:** Companies with extensive logistical capabilities (e.g., fleet vehicles) provide large datasets of geographically diverse images, albeit with a lower frequency of event-specific captures.

Interactions with Clients (Notification Recipients):

- From Clients to Theia Vision:
    - **Financial Support:** Clients pay for services, providing the financial backbone for the platform's operational sustainability.
    - **Loyalty and Engagement:** Clients offer loyalty which helps in building long-term relationships and continuous service enhancements.
    - **Developmental Feedback:** Clients contribute to product refinement by providing detailed feedback based on their professional use and requirements.
- From Theia Vision to Clients:
    - **Event Detection and Reporting:** Delivers precise and actionable information on urban events, including GPS location, event type, and high-definition imagery.
    - **Continuous Monitoring:** Provides tools for ongoing monitoring of urban events, allowing clients to track resolutions and ongoing issues effectively.
    - **Analytical Metrics:** Offers comprehensive metrics on event occurrences over time, aiding clients in strategic planning and resource allocation.

8.2.16.3 Preliminary economic (cost-benefit) analysis

Logimade plans to launch and expanding Theia Vision across various European markets, starting from the Autonomous Region of Madeira in 2025 and progressively reaching out to the rest of Portugal, Spain, and other European countries by 2029.

The sustainability assessment covers the previously presented revenue streams generated through distinct service packages offered by Theia Vision, including

Funded by the European Union

Issues/Events Packages, Street Navigation with Up-to-Date Images, and the API Package. These services are designed to cater to a diverse client base, ranging from local governmental bodies and utility companies to AI developers and, perhaps, even general public users interested in active urban management.

This assessment outlines a comprehensive analysis of projected revenues and costs associated with development, operations, and marketing. Additionally, it explores three financial scenarios — basic, optimistic, and pessimistic — to provide a balanced view of potential outcomes. These scenarios consider varying degrees of market acceptance and operational efficiency, offering insights into the expected payback periods and internal rates of return.

By carefully analyzing these elements, Logimade aims to ensure that Theia Vision not only achieves financial sustainability but also meets the strategic goals of enhancing urban environments through technology-driven solutions and community engagement. This assessment is intended to guide strategic decision-making and resource allocation as the project moves forward with the implementation and scaling of Theia Vision across designated markets.

Theia Vision's revenue streams from various service packages are projected to grow as the platform expands geographically from the Autonomous Region of Madeira in 2025 to other parts of Portugal in 2026, Spain in 2027, and additional European countries by 2028 and 2029.

Revenue Projections by Package:

1. Issues/Events Packages:
    - 2025 (Madeira only): €200,000
    - 2026 (Portugal): €600,000
    - 2027 (Spain): €1,000,000
    - 2028-2029 (Other EU countries): €1,500,000 annually
2. Street Navigation with Up-to-Date Images:
    - 2025 (Madeira only): €100,000
    - 2026 (Portugal): €300,000
    - 2027 (Spain): €500,000
    - 2028-2029 (Other EU countries): €800,000 annually
3. API Package:
    - 2025 (Madeira only): €150,000
    - 2026 (Portugal): €450,000

Funded by the European Union

- 2027 (Spain): €750,000
- 2028-2029 (Other EU countries): €1,200,000 annually

Cost Projections:

- Development Costs: Annual development costs (including updates to AI capabilities, platform functionalities, and Solid protocol integration): €500,000 annually, increasing by 10% each year to accommodate expansion and inflation.
- Operational Expenses: Server maintenance, data storage, customer support, and compliance management: Starting at €300,000 in 2025, increasing by 15% annually due to expanding operations.
- Marketing and Sales: Initial cost: €200,000 in 2025, increasing by 20% annually to support expansion and enhance market penetration strategies.

Financial Scenarios

Basic Scenario:

- Assumes steady growth with no major market disruptions. Expected internal rate of return (IRR): 8%.
- Net Present Value (NPV) considering a 6% discount rate: €2,500,000 by the end of 2029.

Optimistic Scenario:

- Assumes higher adoption rates and successful marketing campaigns. Expected IRR: 12%.
- NPV considering a 6% discount rate: €3,500,000 by the end of 2029.

Pessimistic Scenario:

- Factors in potential market resistance and slower adoption rates. Expected IRR: 4%.
- NPV considering a 6% discount rate: €1,000,000 by the end of 2029.

Payback Period Analysis

- Basic Scenario: Estimated payback by mid-2028.
- Optimistic Scenario: Payback by early 2028.

Funded by the European Union

- **Pessimistic Scenario:** Payback potentially extending beyond 2029.

8.2.16.4 Sensitivity Analysis

The Sensitivity Analysis evaluates how changes in key variables affect Theia Vision's financial performance under different scenarios. This analysis helps identify the robustness of the business plan developed by Logimade and underscores potential financial risks. The critical variables assessed here include market penetration rates, operational costs, and revenue streams.

Sensitivity to Market Penetration Rates:

- **Assumption Variations:** Changes in the adoption rate of Theia Vision services can significantly impact revenue. For instance, the basic scenario assumes a steady uptake by new markets each year. However, if market penetration is slower due to unforeseen resistance or competition, the revenues could be substantially lower than projected.
- **Impact Analysis:** A 10% decrease in market penetration rates could delay the payback period by an additional year and decrease the Net Present Value (NPV) by 15-20%. Conversely, a 10% increase could enhance NPV by an equivalent margin and shorten the payback period.

Sensitivity to Operational Costs:

- **Assumption Variations:** Operational expenses such as server maintenance, data storage, and compliance management are based on current estimates. An increase in these costs due to new regulations, higher energy costs or higher-than-expected data usage can alter the financial outcomes.
- **Impact Analysis:** A 20% increase in operational costs could reduce the annual net income by approximately 10%, impacting both the IRR and NPV negatively, which might extend the payback period.

Sensitivity to Revenue Streams:

- **Assumption Variations:** Revenue projections are based on current service pricing and package adoption rates. Changes in competitive dynamics or less-than-expected utility from the packages could affect these projections.
- **Impact Analysis:** If actual revenues are 15% lower than projections due to reduced API package adoption or lower interest in updated street navigation images, the NPV could drop significantly, affecting overall project sustainability.

Funded by the European Union

The successful implementation and growth of Theia Vision hinge on navigating several critical risks that could potentially impact the platform's market performance and operational stability. Identifying these risks early and developing robust mitigation strategies are essential for ensuring the long-term sustainability of the business.

The major risks outlined in this section encompass challenges in market adoption, technology integration, regulatory compliance, and economic stability. Each of these risks carries implications that could disrupt Theia Vision's service delivery and financial outcomes.

By proactively addressing these risks, Logimade aims to fortify Theia Vision's market position and enhance its capability to deliver innovative urban management solutions effectively. This proactive risk management approach ensures that Theia Vision not only anticipates potential setbacks but is also well-prepared to respond swiftly and effectively, thereby safeguarding its business objectives and customer commitments.

1. Market Adoption Risks:
    - Risk Description: Resistance to new technology or slower-than-expected adoption rates among target customers.
    - Mitigation Strategy: Intensify marketing efforts, enhance customer engagement, and adjust pricing strategies to increase market penetration.
2. Technology Integration Risks:
    - Risk Description: Potential integration issues with Solid Protocol or delays in development schedules impacting product launch and updates.
    - Mitigation Strategy: Implement rigorous testing phases, involve potential users in early development stages for feedback, and develop contingency plans for technological setbacks.
3. Regulatory and Compliance Risks:
    - Risk Description: Increased operational costs due to new data protection regulations or compliance requirements.
    - Mitigation Strategy: Stay updated with regulatory changes, allocate resources for compliance management, and engage in proactive advocacy.
4. Economic Risks:
    - Risk Description: Economic downturns affecting client budgets, leading to reduced spending on new technologies.

Funded by the European Union

- Mitigation Strategy: Diversify the client base, develop lower-cost packages to maintain affordability, explore new application areas, and tighten financial controls.

8.2.17 LED-UP

The LED-UP project aims to revolutionise data governance and user privacy through a decentralised platform. Leveraging the Alastria B Network, the project combines DDI, advanced encryption, and data tokenization to create a secure and transparent data management solution. The open-source project will monetize its offerings through a premium version that includes compensation for data sharing, providing a sustainable revenue stream. LED-UP's mission is to empower individuals and organisations with innovative solutions that prioritise data privacy and governance through decentralised technology, ensuring users can benefit economically from their data. The business model revolves around monetizing the open-source LED-UP project by offering a premium version with advanced features for data tokenization and compensation alongside services such as support, custom solutions, and training. The growing demand for data privacy and decentralised solutions presents significant market opportunities. Initial deployment focuses on refugee camps with potential expansion into healthcare, finance, and other sectors.

The core open-source offering is the basic LED-UP framework, which provides decentralised data sharing and governance features that are available for free, encouraging widespread adoption and community contributions. Monetized premium services include data tokenization and compensation, where users can tokenize their data and receive compensation when accessed or purchased by third parties. Premium support services are offered in different tiers: Basic Support with email support and a 48-hour response time, Professional Support with priority email and phone support and a 24-hour response time, and Enterprise Support with dedicated account managers, 24/7 technical assistance, and on-site support options. Consulting and custom solutions provide expert consulting to tailor the LED-UP framework to specific organisational needs, including integration with existing systems and custom feature development. Enterprise features offer enhanced security protocols, compliance modules, and premium analytics tools. Training and certification programs provide comprehensive training programs and certification courses for organisations and individuals.

Combining the flexibility and innovation of an open-source project with professional-grade services and support ensures users can maximise their privacy and data governance capabilities while benefiting economically from their data. The target market includes organisations and sectors requiring robust data governance solutions, such as healthcare, finance, NGOs, and government agencies. Their marketing strategy focuses on community building, engaging with the open-source community through forums, GitHub, and social media to foster contributions and spread awareness. Content marketing involves publishing case studies, whitepapers, and blog posts

Funded by the European Union

showcasing successful implementations and use cases. Partnerships with technology companies, NGOs, and academic institutions will expand reach and credibility. Events and webinars will demonstrate the capabilities and benefits of LED-UP.

LED-UP's sales strategy includes direct sales through targeted outreach to potential enterprise clients and organisations needing customised solutions, channel partners by developing partnerships with technology resellers and consulting firms, and an online platform to offer premium services, training programs, and support packages. The operational plan outlines development phases starting with initial setup and community engagement in the first month, establishing the open-source repository, engaging with the community, and gathering initial feedback. In months 1-3, service development will develop premium support structures, consulting packages, and enterprise features. Testing and quality assurance in months 3-5 will ensure high-quality standards through rigorous testing of premium features and services. Training and documentation in months 4-5 will create comprehensive training materials, user manuals, and certification programs. Deployment and expansion in months 5-9 will launch premium services, begin offering consulting, and start enterprise sales.

Resources include a team of developers, support engineers, consultants, and trainers, advanced cryptographic tools, decentralised platforms, and cloud infrastructure, along with partnerships with academic institutions and industry experts for continuous improvement and validation. Risk management involves mitigating market risks by securing strategic partnerships and building a strong community, ensuring compliance with KYC/AML and securities laws through legal consultation and robust procedures, and implementing a clear roadmap and transparent communication to maintain community trust.

Revenue projections are based on premium support subscriptions, consulting fees, enterprise feature licences, and training program enrollments. Initial funding through grants and seed investment will support development and marketing efforts. Expense management will prioritise efficient use of resources, community engagement, and development of monetized services. Break-even analysis estimates the time required to cover initial investments through revenue generation from premium services and consulting. The LED token (LED) serves multiple purposes within the ecosystem, including incentivizing data sharing, accessing premium features, staking for governance, and transaction fees.

To launch the commercial initiative of LED-UP, an Initial Coin Offering (ICO) will be realised. The initial token distribution involves a total supply of 1 billion LED tokens. The distribution is structured with 40% allocated to community and ecosystem, 20% to team and advisors, 15% to foundation and governance, 10% to reserve, and 15% to token sale. The ICO launch strategy includes pre-ICO phase activities such as finalising tokenomics and legal compliance, launching marketing and PR campaigns, and opening whitelist registration. During the ICO phase, the project will conduct a private sale to secure strategic investors and open a public sale with clear communication of funding goals and token utility. Post-ICO phase activities include distributing tokens to

Funded by the European Union

participants, listing tokens on exchanges, and continuing community engagement and transparency efforts.

The market analysis for decentralised digital identity platforms highlights several key players, emerging trends, and critical insights into the opportunities and challenges within this sector. Major platforms such as Microsoft's ION, Sovrin, uPort, Polygon ID, and Lifeform are leading the decentralised digital identity market, each offering unique features that enhance security and user control over personal data. Microsoft's ION is built on the Bitcoin blockchain and provides decentralised identifiers (DIDs) that allow users to manage their digital identities independently of centralised authorities. Sovrin focuses on creating a global public utility for self-sovereign identity, enabling secure and independent identity management. uPort, developed by ConsenSys, leverages the Ethereum blockchain to offer decentralised identity solutions that integrate seamlessly with decentralised applications (dApps). Polygon ID uses ZKPs to ensure user privacy while enabling secure identity verification, allowing users to manage credentials directly on their devices. Lifeform integrates hyper-realistic 3D avatars with decentralised digital identity capabilities, catering to Web3 users who wish to manage their digital identities interactively (Expert Market Research, 2023; Shoemaker, 2024).

The market is rapidly growing, driven by increasing concerns over data privacy and security. North America currently dominates the market due to technological advancements and supportive regulatory frameworks such as the California Consumer Privacy Act (CCPA). However, the Asia Pacific region is expected to experience the fastest growth, fueled by rising cybersecurity awareness and proactive government initiatives promoting digital identity solutions. Europe also presents a significant market with regulatory frameworks like the General Data Protection Regulation (GDPR) supporting the adoption of decentralised identity technologies (Gujar & Kathoke, 2023; iMarc Group, 2023).

Key stakeholders in the decentralised digital identity market include technology providers, regulatory bodies, enterprises across various sectors, and end-users demanding greater control over their personal data. Potential partners for the LED-UP project could include companies like Microsoft, IBM, Accenture, and innovative startups such as Lifeform and Polygon ID, which are actively developing advanced digital identity solutions. Collaborations with these entities could enhance interoperability and integration capabilities, fostering broader adoption and market penetration (KuCoin Learn, 2024; Liu, 2022).

The opportunities in this market are substantial, particularly in sectors such as finance, healthcare, and government, where secure identity verification is crucial. For instance, the healthcare sector can benefit from decentralised identity solutions by streamlining patient data management and enhancing privacy. Financial institutions can use these solutions to improve KYC processes and reduce fraud. Governments can leverage decentralised identities to provide secure and efficient public services. However, challenges remain, including the need for interoperability standards, the complexity of integrating decentralised identity solutions with existing systems, and addressing user

Funded by the European Union

adoption barriers due to the technical knowledge required (Expert Market Research, 2023; iMarc Group, 2023).

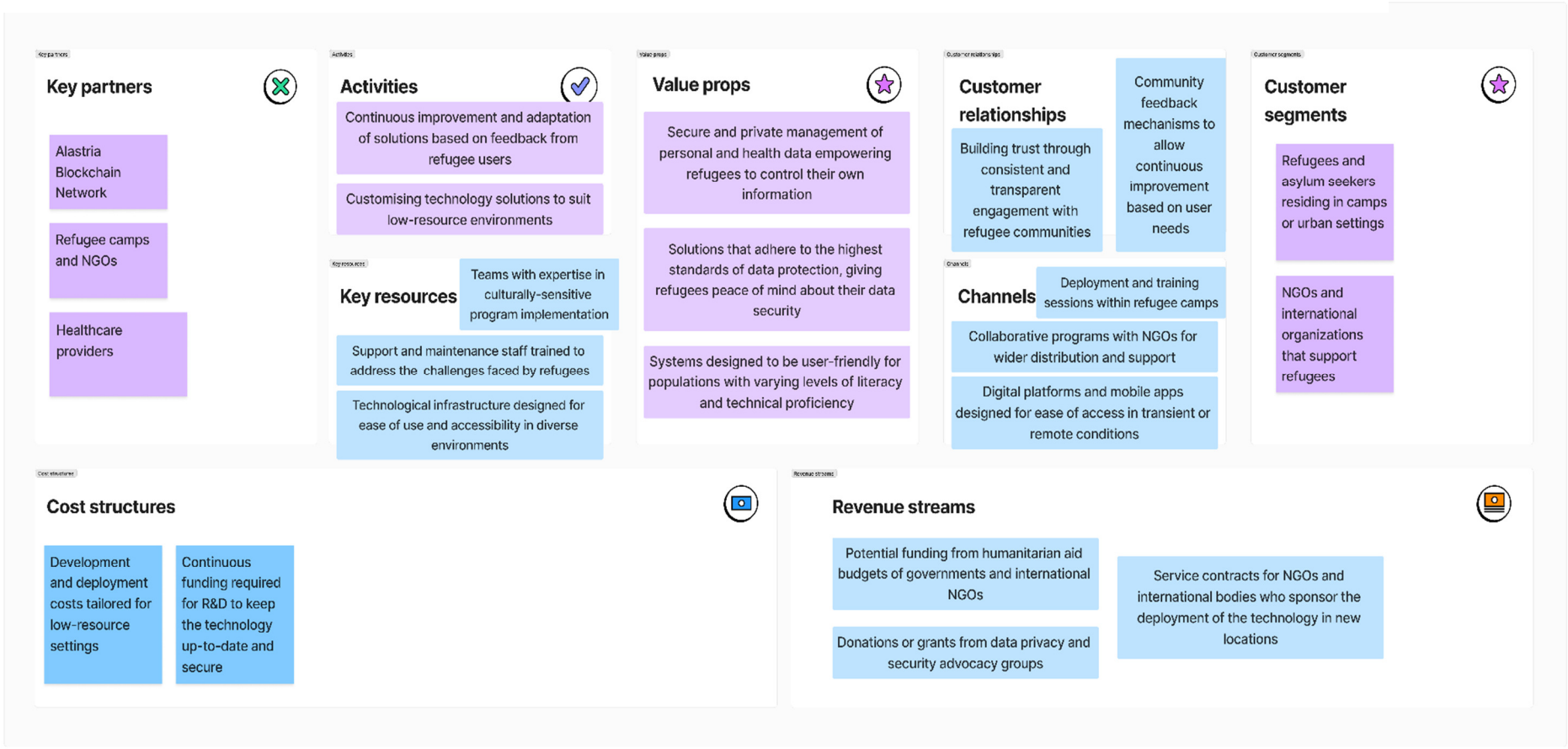
In summary, the decentralised digital identity market offers significant growth and innovation opportunities. Successful market entry requires addressing interoperability issues, ensuring seamless integration with existing digital infrastructures, and fostering partnerships with key industry players. The positive trajectory of this market underscores its potential to transform digital identity management, creating a more secure and user-centric digital ecosystem.

The business model for the LED-UP project is designed to create a sustainable ecosystem that leverages decentralised digital identity and blockchain technology to provide robust data governance and privacy solutions. The proposed service/application focuses on monetizing its offerings through a premium version that includes advanced features such as data tokenization and compensation for data sharing. This business model ensures multiple revenue streams while promoting user-centric data management.

The core value proposition is to empower individuals and organisations with innovative solutions that prioritise data privacy and governance. This is achieved by providing a decentralised platform that combines DDI, advanced encryption, and data tokenisation. The primary stakeholders include end-users, enterprises, technology providers, and regulatory bodies.

Funded by the European Union

TABLE 72: BUSINESS MODEL CANVAS OF LED-UP



Key Partners

- Technology Providers: Alastria Blockchain Network essential for the blockchain infrastructure.
- Strategic Partners: Refugee camps and NGOs, crucial for deployment and providing real-world application feedback. Healthcare providers are also key partners for testing and implementation within medical environments.

Key Activities

- Development and Maintenance: Continuous improvement and adaptation of solutions based on feedback from refugee users.
- Customisation: Tailoring technology solutions to suit low-resource environments, ensuring the platform is accessible and usable under diverse conditions.

Key Resources

- Expert Teams: Composed of individuals with expertise in culturally sensitive program implementation.
- Support Infrastructure: Includes support and maintenance staff trained to address the challenges faced by refugees, along with technological infrastructure designed for ease of use and accessibility in diverse environments.

Value Propositions

- Secure and Private Data Management: Empowering refugees to control their own personal and health data, providing secure and private management that meets the highest standards of data protection.
- User-Friendly Design: Systems are specifically designed to be user-friendly for populations with varying levels of literacy and technical proficiency.

Customer Relationships

- Trust and Engagement: Building trust through consistent and transparent engagement with refugee communities, facilitated by community feedback mechanisms that allow for continuous improvement based on user needs.

Channels

- Training and Deployment: Deployment and training sessions conducted within refugee camps, utilising collaborative programs with NGOs for wider distribution and support. Digital platforms and mobile apps are designed for ease of access in transient or remote conditions.

Customer Segments

- Primary Users: Refugees and asylum seekers residing in camps or urban settings.
- Organisational Users: NGOs and international organisations that support refugees and are actively involved in deploying and utilising the LED-UP system.

Cost Structure

Funded by the European Union

- Development and Operational Costs: Includes the development and deployment costs tailored for low-resource settings and ongoing funding required for R&D to keep the technology up-to-date and secure.

Revenue Streams

- Funding and Donations: Potential funding from humanitarian aid budgets of governments and international NGOs, alongside donations or grants from data privacy and security advocacy groups.
- Service Contracts: Revenue also comes from service contracts for NGOs and international bodies who sponsor the deployment of the technology in new locations.

8.2.18 GUEDHS

The value proposition of GUEDHS will focus on secure data collaboration, enabling organizations to perform data analytics and identity verification without transferring or exposing their data. This ensures data privacy and security while allowing for comprehensive analytics and insights. By utilizing privacy-enhancing technologies, GUEDHS will ensure that users' identities are verified without exposing personal information, aligning with the increasing demand for privacy and data protection. Additionally, GUEDHS platform will be designed to comply with global data protection regulations ensuring that data remains within legal boundaries and under the control of its owners.

The target market of GUEDHS includes healthcare providers, who will benefit from secure and private patient identity verification and data sharing for improved healthcare outcomes and research. Pharma and MedTech companies will gain access to anonymized, large-scale datasets for drug development and medical research without compromising patient privacy. Insurance companies will be able to access comprehensive health data securely to support value-based healthcare (VBHC) agreements and underwriting processes. Financial institutions will benefit from secure and compliant identity verification services, reducing fraud and enhancing customer onboarding processes.

The revenue model of GUEDHS will incorporate subscription fees for service providers and data users accessing the platform's capabilities. GUEDHS will implement a transaction fee structure for each identity verification or data access transaction. Licensing fees will be charged for the use of their suite of Data Products, which support longitudinal data collection and analysis. Additionally, GUEDHS will offer expert consulting services to help clients implement and optimize their use of the platform for various applications, such as regulatory compliance and real-world evidence (RWE) studies.

Key activities will include continuous platform development to improve security, interoperability, and scalability to meet the needs of different industries. GUEDHS will

Funded by the European Union

actively engage with users to gather feedback and iterate on the platform's features and capabilities. Ensuring the platform adheres to global data protection and privacy regulations will be a primary focus.

Data privacy and security will be maintained through federated learning techniques, allowing data to be analyzed locally while sharing only the insights and not the data itself. Advanced encryption and data anonymization methods will protect user data during processing and transmission. Modular privacy-enhancing technologies will be implemented to ensure compliance with data privacy regulations and build trust among users.

8.2.19 EIDCMP

Market Analysis:

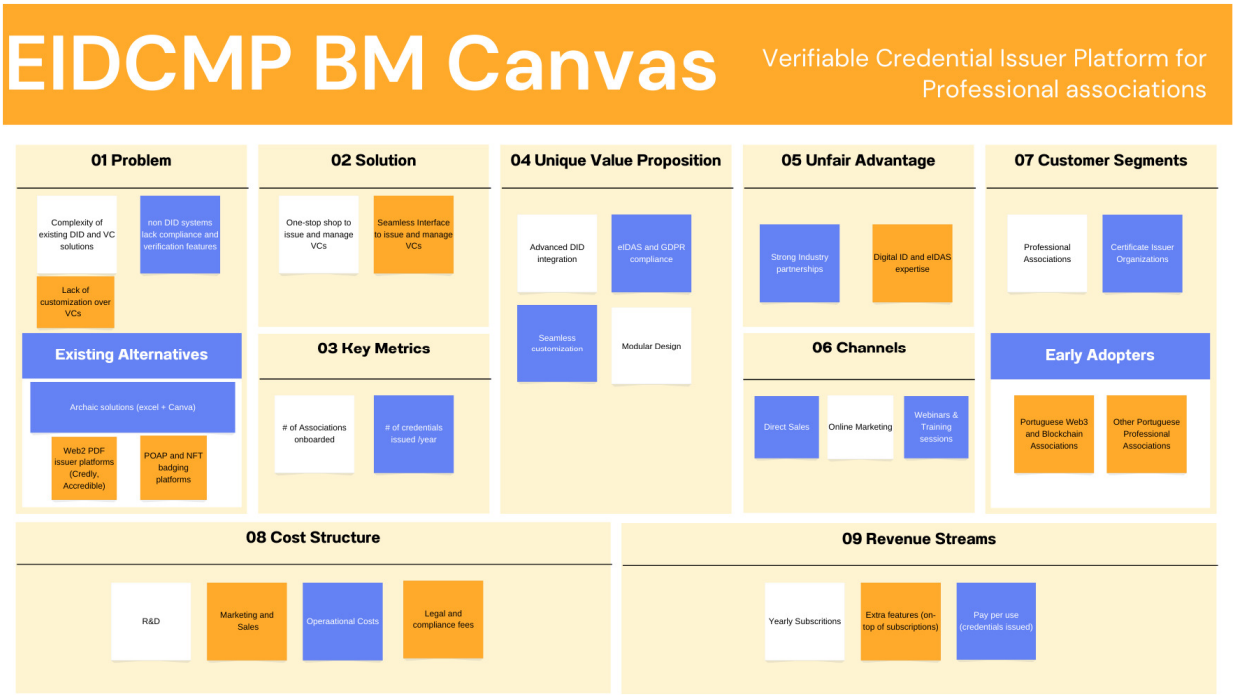
The landscape of membership management and credential issuance within professional associations remains dominated by traditional, often archaic tools. From their research and pilot interactions, it's evident that many associations still rely on manual systems like spreadsheets for member data management and basic graphic design tools like Canva for creating certificate images. One standout case, Immunefy, revealed their use of Quota Path for membership management. However, they expressed significant dissatisfaction with its complexity and its inadequacies in credential composition and issuance capabilities.

The analysis of EIDCMP also identified several platforms that manage membership for associations, such as MemberClicks and Wild Apricot, which focus broadly on membership management without specializing in the issuance of verifiable credentials. This is where EIDCMP differentiates itself by concentrating on credential issuance using decentralized digital identity and blockchain technologies, offering a more secure, compliant, and versatile solution compared to competitors like Credly and Accredible. These platforms, while popular for digital credentialing, lack the robust compliance features and the enhanced security and transparency provided by DID and VC protocols integrated within the EIDCMP solution.

Funded by the European Union

Business Model:

TABLE 73: BUSINESS MODEL CANVAS OF EIDCMP



Value Network:

The go-to-market strategy of EIDCMP is a top-down approach, identified as the most effective during their pilot phase. One significant barrier to the widespread adoption of DID solutions is the lack of network effects, which can make these solutions less viable outside specific issuing environments. To overcome this, EIDCMP initially targets top-hierarchy associations, such as industry leaders and umbrella organizations like AIP, that oversee other associations. Starting with small, internal pilots, EIDCMP plans to gradually expand the application of their solutions across all certificates they issue. This strategy ensures that top associations not only adopt their platform themselves but also encourage subordinate associations within their network to follow suit, creating a robust value network. This network effect facilitates widespread adoption and standardization across the industry, enhancing the platform's value and utility.

Preliminary Economic Analysis:

The economic viability of EIDCMP is underpinned by its ability to reduce the costs associated with traditional credential issuance methods while enhancing security and

Funded by the European Union

compliance. The preliminary cost-benefit analysis of EIDCMP indicates substantial savings for associations in terms of reduced labour and material costs and minimized risks of credential fraud. This economic benefit, coupled with the advanced capabilities of blockchain and decentralized identity technology, positions EIDCMP as a lucrative solution for professional associations.

The integration of decentralized digital identity and blockchain not only enhances the security and efficiency of the EIDCMP platform but also significantly contributes to its market appeal and competitiveness. By aligning with the latest advancements in technology and adapting to the specific needs of professional associations, EIDCMP is well-positioned to lead in the digital credentialing space, offering unmatched value to the broader ecosystem.

8.2.20 OIDC-PRINCE

The business model is presented considering the value proposition, an analysis of the market, the value network and preliminary simulations considering 3 distinct scenarios.

8.2.20.1 Value proposition

The main value proposition for OIDC-PRINCE is informed consents regarding the privacy risks and GDPR compliance in Single Sign On (SSO) processes.

OIDC-PRINCE fills a gap in the SSO process, as users are not aware of the privacy risks related with the consents they provide when providence consent to access personal fields. For instance, a service not compliant with GDPR (or other privacy regulation) may simply share personal identifiable information (PII) with other entities for profit reasons (marketing). Also, users are not fully aware of the privacy risks, and their initial surveys with users demonstrates this.

8.2.20.2 Market analysis

There is a big market in SSO solutions, due to the flexibility and convenience of such methods for authentication, the following table provides a summary of the main players in the SSO market.

The market analysis is focused to the direct competitors of OIDC-PRINCE and identify new ones.

TABLE 74: SSO SOLUTIONS AVAILABLE IN THE MARKET

Solution	Solution	Description	Price	Cost	Additional

Funded by the European Union

Provider	Name		Model		information	
PrivacyEngine	PrivacyEngine	Privacy Risk Management with SSO	Per year	€15,64	linkA	
SecureAuth	Arculix	Risk Engine on top of other SSO solutions including Microsoft and google	per user per month	€1,38	linkA	linkB
OneTrust	OneTrust	Platform with support for privacy automation, consent & preferences management, risk management, security & privacy compliance	Per feature per month	€30,00	linkA	linkB
TrustArc	TrustArc	Data Privacy Management Platform	Per year per user	10000	linkA	linkB

The business model of SecureAuth with the Arculix product is mainly devoted for the risk management associated with the SSO process. The risk management mainly considers the identification of legitimate access attempts or device posture pre-authentication, during authentication and post-authorization processes. The service provided by Arculix is built on top of others SSO solutions, which **indicates the viability of providing the intended services of OIDC-PRINCE in a B2B model.**

The **direct competitor of OIDC-PRINCE is PrivacyEngine**, which provides privacy risk management, considering SSO processes and others. Analysing this service with more attention, one can observe that the solution of PrivacyEngine is quite complete in terms of Privacy Risk management, as it supports among other the several functionalities like: Record of Processing Activities, Data Breach Management, Data Retention, Risk Management and Data Protection Impact Assessment (DPIA).

Nonetheless, the solution from PrivacyEngine does not support the envisioned functionalities of OIDC-PRINCE, since PrivacyEngine is more focussed on the Business sector to allow the analysis of information flows of the diverse processes (e.g. authentication, invoices, etc), collects evidences to analyse GDPR compliance and establish the respective privacy risk. In this regard, there is not a direct competition with

Funded by the European Union

OIDC-PRINCE, and indeed PrivacyEngine can be used to provide the GDPR Compliance proofs which are used by OIDC-PRINCE.

The **TrustArc** solution provides Data Privacy Impact Assessments (DPIA) or Privacy Impact Assessment (PIA), using AI to perform auto identification of privacy compliance issues, allowing therefore to automate risk assessment, besides supporting compliance reporting, which facilitates auditing. The risk assessment can be performed using provided templates, which can be customized to the needs of a client/organization. As per PrivacyEngine, the TrustArc solution provides more functionalities than OIDC-PRINCE, nonetheless TrustArc can be employed as a mean to provide the GDPR Compliance proofs for OIDC-PRINCE, through the reporting integration.

The **OneTrust** solution also provides support for PIA and DPIA, in the same line as TrustArc. Additional features are provided, which include Privacy Incident Management (PIM) that includes assistance on incidents and data breaches. Along with this, there is support for compliance automation on privacy and risk management standards like SOC 2, ISO 27001 and GDPR. In terms of GDPR OneTrust allows to demonstrate the accountability of GDPR requirements and enforce governance of data. As per the remaining competitors OneTrust can be employed as a mean to provide the GDPR Compliance proofs for OIDC-PRINCE.

The **main opportunities** to go to market are:

1. Users are concerned with the privacy risks on the Internet and the information they share with existing services. OIDC-PRINCE has a narrowed scope for login processes with OpenID Connect, allowing the authentication flow to be parameterized according to the privacy risk information in terms of GDPR compliance and consent information from services. OIDC-PRINCE establishes a risk module that allows to secure the login process for end-users considering the privacy risks that can be associated with certain service profiles and requested claims.
2. The devised architecture of OIDC-PRINCE allows it to be integrated with existing Risk Management platforms either to receive information from these, or to complement the existing risk information with the privacy risk calculated by OIDC-PRINCE.

The **potential obstacles** to go to market are:

3. Privacy Impact Assessment is integrated in Risk Management platforms to monitor the overall risk of the different processes within an organization. Privacy Risk is not considered only for single processes like Single Sign On. OIDC-PRINCE has a narrowed scope that is for login through OpenID Connect, which may reduce the interest from organizations, since it only supports a specific process that is the SSO login.

Funded by the European Union

4. Unwillingness of major risk and privacy management vendors[4] (OneTrust, TrustArc, PrivacyEngine) to perform business liaisons with OIDC-PRINCE or any type of integration. These liaisons can foresee bidirectional flow of information: input to OIDC-PRINCE, for instance the GDPR compliance proofs; output from OIDC-PRINCE regarding the risk information in the login process to the integrated risk management platforms.

5. Unwillingness of major SSO providers[5] (Okta SSO, Google SSO, Microsoft SSO) to perform business liaisons with OIDC-PRINCE or any type of integration. The integration/liaison in this situation is unidirectional, where OIDC-PRINCE provides risk information to the SSO platforms to complement existing risk management policies.

8.2.20.3 Business Model Canvas

The Business Model Canvas (BMC) considers diverse aspects as documented in each subsection. The overall view of the OIDC-PRINCE BMC is provided in the table below, while the details of each component in the BMC are provided in the following subsections.

[4] Note that this is assumption, no contacts or demonstrations have been performed with such vendors.
[5] Note that this is assumption, no contacts or demonstrations have been performed with SSO providers.

Funded by the European Union

TABLE 75: BUSINESS MODEL CANVAS OF OIDC-PRINCE

<table>
<tr><th>Key Partners</th><th>Key activities</th><th>Value Propositions</th><th>Customer Relationships</th><th>Customer Segments</th></tr>
<tr><td>Partners:
SSO Providers (Okta, google, Microsoft)
Risk Management (OneTrust, TrustArc, PrivacyEngine)
Suppliers:
Risk Management

Resources:
GDPR compliance proofs
Partnership:
Strategic alliance
Buyer-Supplier relationship</td><td>Activities:
Info of GDPR compliance
Info ot Service type

Distribution Channels:
website and Value-Added Resellers

Revenue:
B2C and B2B
Category:
Production, delivery of service</td><td>Value:
informed consents regarding the privacy risks and GDPR compliance in SSO

Products and services:
Service to manage privacy risk info

Customer needs:
Users are not aware of the privacy</td><td>Customer Relationships:
- Personal assistance
- Dedicated personal assistance
- Co-Creation
Price Model:
Month or annual subscription</td><td>Most Important customers:
- SSO providers
- Risk Management solutions

Customer Segment:
- Segmented customers like SSO, Risk Management
- Niche Markets</td></tr>
<tr><td></td><td>Key Resources
Human Resources:
Developer/Administrator
Security Engineer (DPO)
Marketing
Physical Resources:
Computational resources in cloud or physical servers
Intellectual resources:
Certification of GDPR and NIS2</td><td></td><td>Distribution Channels
Channels:
- Direct channels on B2C, D2B
- Partner channels on B2B</td><td></td></tr>
<tr><td colspan="3">Cost Structure
Important Costs:
Human Resources
Logistics
Certification</td><td colspan="2">Revenue Streams
Important Revenue Streams:
Asset Sales
Subscription Fee</td></tr>
</table>

The **key partners** include SSO providers and Privacy Risk Management solution providers, these can include:

- SSO providers like: Okta, Google, Microsoft
- Risk Management solution providers like: OneTrust, TrustArc, PrivacyEngine

The **key suppliers** mainly include Risk management operators, which can provide information regarding GDPR compliance. These operators would mainly provide the GDPR compliance proofs as **resources** that are used in OIDC-PRINCE to determine risk.

The **types of partnership** are mainly reduced to two possibilities:

- **Strategic alliance**, at the beginning OIDC-PRINCE would be registered as a startup and would establish formal agreements with other companies to collaborate on the privacy risk management. This alliance can be performed with different entities that include SSO providers and Risk Management solutions providers. With SSO providers the alliance would include the use of OIDC-PRINCE to enhance policies in SSO processes supported by OpenID Connect

Funded by the European Union

and with Risk Management solution providers by integrating the GDPR compliance proof for the privacy risk free login in SSO with OIDC-PRINCE.

- **Buyer-supplier relationship**, as OIDC-PRINCE is established as a recognized supplier of privacy risk free login in SSO processes, the aim is to be acquired by a major player, so that OIDC-PRINCE is integrated into existing SSO or Risk Management platforms in the market

The **key activities** for the value proposition mainly require:

- **Information of GDPR compliance**, the information of GDPR compliance in a DPV format, which is maintained in a decentralized EVM blockchain, and that can be obtained in an audit process regarding GDPR compliance.
- **Information of type of service**, which is required to assess which fields make logic to be requested consent to the user. This information can also leverage on AI models that can perform this type of classification, nonetheless this is out of scope from the time being.

The **distribution channels** include mainly two types:

- **Website** with the official OIDC-PRINCE service, which will also be used to make the interaction with customers, and to announce pricing models, support clauses, among other aspects. Associated with the website, the social media will also be employed to promote marketing campaigns. On such case the **revenue** will be based on the direct relation with customers, Business to Client (B2C), which can have different profiles, for instance SMEs aiming to manage the privacy risk in their SSO solutions.
- **Value-Added Resellers** (VARs) like the SSO providers or/and the Risk Management solution providers that include the OIDC-PRINCE services in their own platforms according to the established partnership type. In such case the revenue will be based on the partnership that is established, relying mainly on a Business to Business (B2B) relationship

The **category** mainly includes the delivery of services, that is OIDC-PRINCE is provided in the as a service either in the B2C or B2B revenue streams.

The **value** that OIDC-PRINCE delivers is informed consents regarding the privacy risks and GDPR compliance in Single Sign On (SSO) processes.

Funded by the European Union

OIDC-PRINCE provides a **service** to fill a gap in the SSO process to manage the privacy risk information. **Users** are not aware of the privacy risks related with the consents they provide when providence consent to access personal fields. A service not compliant with GDPR (or other privacy regulation) may simply share personal identifiable information (PII) with other entities for profit reasons (marketing). Also, users are not fully aware of the privacy risks, and their initial surveys with users demonstrates this.

Potential customers expect **personal assistance** to customize how privacy risk information can be determined. Specific implementation can include specific fields of information, which are not part of the standard claims of OpenID Connect. Additionally, how the service can be configured regarding the input for GDPR information can require **dedicated personal assistance**.

Co-creation has already been employed with users to formulate the design and presentation of interfaces regarding risk information.

As stated, the most important customers include SSO providers and Risk Management service providers, which can include Okta, Google, Microsoft, OneTrust, TrustArc, PrivacyEngine among others. The customers can also include SMEs, but these represent the minority.

The customer segment type includes **segmented customers**, either dealing with SSO or Risk Management. OIDC-PRINCE is positioned for **Niche markets** dealing with privacy management in SSO processes, which can impact SMEs, enterprises but also other customers providing SSO and Risk management solutions.

The OIDC-PRINCE solution requires different type of resources, which can include:

- **Human resources** OIDC-PRINCE requires:
    - an Informatics Engineer working as a developer and an administrator
    - a Security Engineer to act as the Data Privacy Officer (DPO)
    - a Marketing Expert (ME) to manage the contracts with clients and business entities
    - a Human Resources (HR) Expert to manage human resources.
- **Physical resources**, OIDC-PRINCE service requires computational services, which need to be accommodated in servers, either through cloud computing or through dedicated servers.
- **Intellectual resources**, OIDC-PRINCE itself needs to be certified as being GDPR compliant, to be integrated with other platforms.

The **most important costs** are related with the development and certifications of the OIDC-PRINCE solution. The development of features in the dedicated personal

Funded by the European Union

assistance represents a considerable cost, as the OIDC-PRINCE needs to be adapted to the customer needs (i.e., support of specific claims). The development costs are related with the costs of the human resources, related resources required for this task.

The costs in OIDC-PRINCE are structured into 3 main categories:

- Human Resources, this category includes costs with the human resources (Engineers and Experts).
- Logistics this category includes costs with equipment, consumables, water, electricity and cloud resources
- Certification this category includes the costs with the required certifications, namely the compliance with GDPR, which can be renewed each 3 years [SPRINTO].

The main revenue stream is based on two models:

Asset sales – assuming that OIDC-PRINCE is integrated in the products of SSO providers or Risk Management solution providers

Subscription Fee – The solution of OIDC-PRINCE is provided in a subscription model, where clients pay each month for each service. OIDC-PRINCE establish a price model per service per month in the options documented in Table 76.

TABLE 76: SUBSCRIPTION OPTIONS

Subscription pack	Details	Value per Month	Note
Basic	Per service	€ 2,50	
Basic Enterprise	Pack with 10 services	€ 20,00	
Advanced	Per service	€ 50,00	Support for private features of OpenID Connect
Advanced Enterprise	Pack with 10 services	€ 400,00	Support for private features of OpenID Connect and High Availability

Funded by the European Union

Customers prefer to be reached via **direct channels**, thus OIDC-PRINCE establishes a web site to provide information regarding updates, documentation information and also to provide a owned channel to communicate with customer, in a B2C perspective.

The website will also include a B2B support channel for clients, where the OIDC-PRINCE is deployed according to business liaisons. The final clients, in this situation will be managed through **partner channels**.

8.2.20.4 Value network

OIDC-PRINCE has the potential to be associated a value network composed of:

- **Technology Providers**: who can certify the compliance of services regarding GDPR and provide such compliance in decentralized systems. For instance, the EUGDPR Institute [EUGDPR], can emit proof of GDPR compliance in the DPV format.
- **Regulatory Bodies**: OIDC-PRINCE has already established synergies with the working group of Data Privacy Vocabulary (DPV) [DPV]. This synergy has been mainly on a specific use case for DPV, which was deemed as necessary by the chair of the work group (in the person of Harshvardhan J. Pandit).
- **Strategic Alliances**: with SSO providers and Risk Management solution providers. These alliances will provide enhanced services to their client base using the solutions provided by OIDC-PRINCE.
- **Clients** from direct channels, through the help of UC Business unit (which establishes a relationship with SMEs, big enterprises, and Instituto Pedro Nunes (IPN) which is focused on technology transfer and has incubation units.

8.2.20.5 Preliminary Economic Analysis

The Preliminary Economic analysis mainly considers the subscription fee model, and the different options documented in Table 76.

Different simulations are considered, for a period of 5 years, where it is expected that the number of clients doubles each year, starting on 20 in year 1, 40 in year 2, 80 in year 3, 160 in year 4 and 320 in year 5.

- Simulation A, this scenario considers that all the subscription options have the same ratio (25%).
- Simulation B this considers a higher ratio of basic
- Simulation C this considers a minimum of advanced enterprise

Funded by the European Union

The costs associated with OIDC-PRINCE are documented per category, as summarized in Table 77.

TABLE 77: TOTAL COSTS OF OIDC-PRINCE

Category	Item	Cost por mor	Cost per Yea	Total Value
Human Resources	Informatics Engineer	€2 120,00	€27 560,00	
	Security Engineer	€3 500,00	€45 500,00	
	Human Resources Expert	€2 120,00	€27 560,00	
	Marketing Expert	€2 120,00	€27 560,00	
				€128 180,00
Logistics	Installations - Rent (assuming incubation in 5 years)			
	Electricity	€300	€3 600	
	Water	€200	€2 400	
	Consumables	€400	€4 800	
	Alojamento Cloud	€200	€2 406	
	Alojamento Cloud (premium)	€876	€10 506	
				€23 712
Certification	GDPR compliance certifications and renewal		€10 000	
				€10 000
			TOTAL per year	**€161 892,21**

The total cost per year is estimated around **161 892,21 €**. The GDPR Certification is a process that needs to be performed for a three-year period, its cost is variable, but has been considered costing 30 000,00€. This cost has been divided by three (validity of certification) to be considered as an annual cost [SPRINTO].

8.2.20.5.1 Simulation A

The sets of simulation A are documented in Table 78.

TABLE 78: SIMULATION A

Simulation A Equal ratio		25%	25%	25%	25%		
Year	# Clients	Basic Associated Costs	Basic Enterprise Costs	Advanced Costs	Advanced Enterprise	Total revenue per year	Total Cost per year
1	20	5 € 150,00	5 € 1 200,00	5 € 3 000,00	5 € 24 000,00	€ 28 350,00	€ 161 892,21
2	40	10 € 300,00	10 € 2 400,00	10 € 6 000,00	10 € 48 000,00	€ 56 700,00	€ 161 892,21
3	80	20 € 600,00	20 € 4 800,00	20 € 12 000,00	20 € 96 000,00	€ 113 400,00	€ 161 892,21
4	160	40 € 1 200,00	40 € 9 600,00	40 € 24 000,00	40 € 192 000,00	€ 226 800,00	€ 161 892,21
5	320	80 € 2 400,00	80 € 19 200,00	80 € 48 000,00	80 € 384 000,00	€ 453 600,00	€ 161 892,21

Funded by the European Union

Picturing the values of Table 78 in Figure 19, one can perceive that in the middle of the third year there is already a positive margin. But for this, the number of clients need to increase per year and opt for the different packs considered in the business plan.

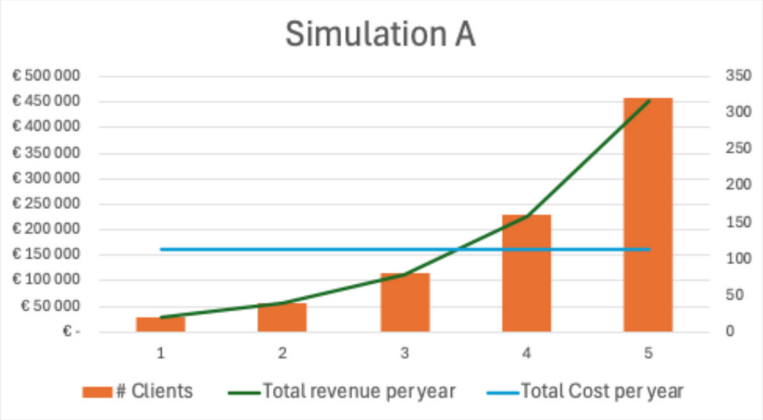


FIGURE 19 - SIMULATION A GRAPHIC

8.2.20.5.2 Simulation B

The sets of simulation B are documented in Table 79.

TABLE 79: SIMULATION B

Simulation B More basic		40%		30%		20%		10%			
Year	# Clients	Basic Associated Costs		Basic Enterprise Costs		Advanced Costs		Advanced Enterprise		Total revenue per year	Total Cost per year
1	20	8	€ 240,00	6	€ 1 440,00	4	€ 2 400,00	2	€ 9 600,00	€ 13 680,00	€ 161 892,21
2	40	16	€ 480,00	12	€ 2 880,00	8	€ 4 800,00	4	€ 19 200,00	€ 27 360,00	€ 161 892,21
3	80	32	€ 960,00	24	€ 5 760,00	16	€ 9 600,00	8	€ 38 400,00	€ 54 720,00	€ 161 892,21
4	160	64	€ 1 920,00	48	€ 11 520,00	32	€ 19 200,00	16	€ 76 800,00	€ 109 440,00	€ 161 892,21
5	320	128	€ 3 840,00	96	€ 23 040,00	64	€ 38 400,00	32	€ 153 600,00	€ 218 880,00	€ 161 892,21

Picturing the values of Table 79 in Figure 20, one can perceive that in the middle of the fourth year there is already a positive margin. But for this, the number of clients need to increase per year and opt for the different packs considered in the business plan.

Funded by the European Union

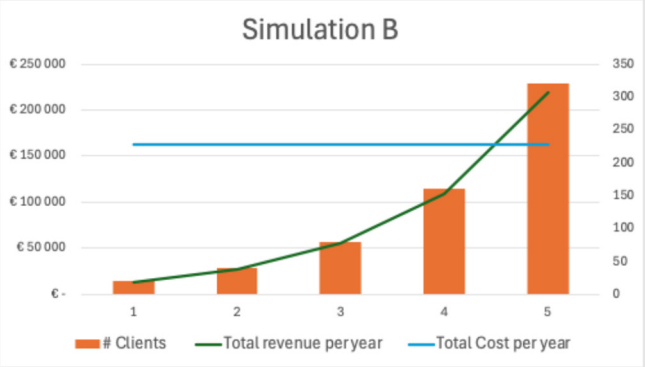


FIGURE 20 - SIMULATION B GRAPHIC

8.2.20.5.3 Simulation C

The sets of simulation C are documented in Table 79.

TABLE 80: SIMULATION C

Simulation C Mimimum A		40%		45%		10%		5%			
Year	# Clients	Basic Associated Costs		Basic Enterprise Costs		Advanced Costs		Advanced Enterprise		Total revenue per year	Total Cost per year
1	20	8	€ 240,00	9	€ 2 160,00	2	€ 1 200,00	1	€ 4 800,00	€ 8 400,00	€ 161 892,21
2	40	16	€ 480,00	18	€ 4 320,00	4	€ 2 400,00	2	€ 9 600,00	€ 16 800,00	€ 161 892,21
3	80	32	€ 960,00	36	€ 8 640,00	8	€ 4 800,00	4	€ 19 200,00	€ 33 600,00	€ 161 892,21
4	160	64	€ 1 920,00	72	€ 17 280,00	16	€ 9 600,00	8	€ 38 400,00	€ 67 200,00	€ 161 892,21
5	320	128	€ 3 840,00	144	€ 34 560,00	32	€ 19 200,00	16	€ 76 800,00	€ 134 400,00	€ 161 892,21

Picturing the values of Table 80 in Figure 21 , one can perceive that more than five years are required to obtain a positive margin, considering the number of clients. This scenario really urges the need to have a higher number of clients or a high number of Advanced subscriptions.

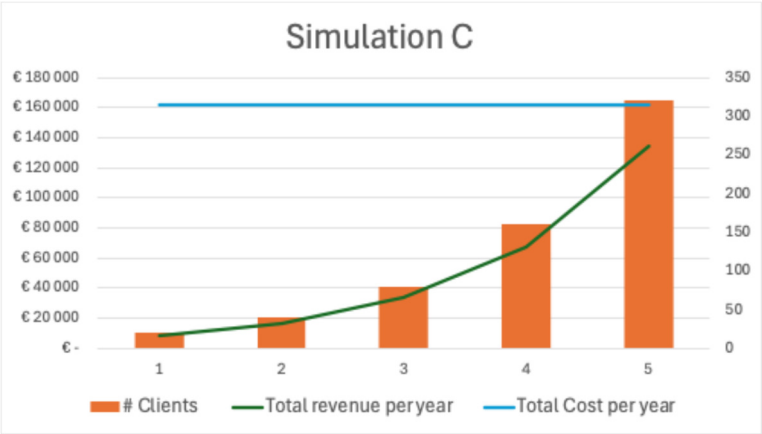


Figure 21 - Simulation C graphic

Funded by the European Union

8.2.21 MorphMetro

8.2.21.1 Market Analysis

MorphMetro solution provides secure and privacy-preserving analysis of measured data. This is achieved through the use of homomorphic encryption. Within the MorphMetro project focuses on ensuring data privacy and protection in proficiency testing (PT) and interlaboratory comparisons (ILC) in legal metrology. Each laboratory in the legal metrology ecosystem must undergo periodical proficiency testing (PT) and interlaboratory comparisons (ILC).

There are a number of different PT/ILC service providers on the market. NAB (National Accreditation Body) for each country provides a list of suitable PT/ILC service providers (example for NAB Malta: https://nabmalta.org.mt/proficiency-testing-and-interlaboratory-comparisons/), and there are also some worldwide databases with service providers. Links to a few examples are given below.

EPTIS is a worldwide database for PT service providers. It helps laboratories find a suitable proficiency testing (PT) scheme. At present, a listing on the database is only open to PT providers from countries that are covered by their so-called coordinators: https://www.eptis.org/

EU also has its own list of PT/ILC service providers for each "topic" – example for GMO testing laboratories in EU: https://gmo-crl.jrc.ec.europa.eu/proficiency-tests

All these PT/ILC service providers operate with more or less the same principle. They send the measuring sample to the laboratory. Laboratory then conducts measurements and sends its measured values back to the PT/ILC service provider. Service provider then analyses the data and writes a report with results of proficiency testing. So, the laboratory is always sending its raw unencrypted data to the PT/ILC service provider. This is recognized as a potential problem, which can be seen from the statements that different service providers are putting out:

"Deltamu, among other services, provides ILC calls and acts as an ILC coordinator. The laboratories that take part in ILC are **anonymized** in the final report.", https://deltamu.com

"Results are available through **secure section** of web site.", https://proficiencytesting.fapas.com

"In order to ensure **confidentiality**, participants in all schemes are allocated a unique laboratory reference number. This number enables results to be reported without divulging the identities of participant laboratories. Only staff within the proficiency

Funded by the European Union

testing team and the laboratory itself will know this number.", https://www.lgcstandards.com/GB/en/support/faq#proficiency-testing

"As a participant, you must agree to **respect the confidential information** GUEDHS have to disclose to you to make the proficiency testing scheme work. The confidential information disclosed to the participants is primarily: The preceding participant, who sent the artefacts to you and the next participant, to whom GUEDHS requests you send the artefact.", https://www.hn-proficiency.com/terms.htm

"The technical advisors assigned to a proficiency test **do not have access** to client data. The technical advisors are given raw data only. One of the most important factors in designing meaningful proficiency tests is the involvement of technical advisors. One of the strengths behind NAPT's success is the technical experts that assist them on a daily basis. The technical advisor is an expert in the field for which they provide assistance.", https://proficiency.org/

"Characteristics of their PT programs: Independence of the organiser, **Confidentiality** of laboratories, Ongoing performance monitoring, Diversity of matrices, Fast publication of results, Robustness of assigned values, International participation.", https://www.bipea.org/proficiency-testing/.

As mentioned earlier, in many use cases, the company providing PT/ILC service also provides the physical samples that are measured by each laboratory. To do so, the PT/ILC providers are cooperating with referent laboratories which manufacture the samples.

The PT/ILC service providers on the market have a strong network of their users (laboratories that are participating in PT/ILC tests) and their suppliers (sample manufacturers).

In order to bring the MorphMetro solution to the market, the most viable path is to form partnerships with established PT/ILC providers by licensing their solution or by charging a fee per PT/ILC test. By using MorphMetro's homomorphic approach, the PT/ILC providers would offer increased value for their clients by providing a secure and privacy preserving PT/ILC service. Their greatest advantage is that MorphMetro enables PT/ILC with fully encrypted data, a feature that no one is currently offering and it is not available on the market, but all PT/ILC service providers have recognized the need for it.

Potential market size is quite large where PT/ILC service providers are working with 13 000 participating PT laboratories[6] with over 200 different PT tests (https://www.bipea.org/proficiency-testing/).

Another channel to access PT/ILC providers is their ongoing collaboration with EuroLAB (https://www.eurolab.org/) which has the support of over 9000 laboratories within the

[6] https://www.lgcstandards.com/GB/en/support/faq#proficiency-testing

Funded by the European Union

EU. Namely, Kruno Milicevic (Random Red Ltd.) is member of EuroLAB's Working Group "Digitalization" and through this has good insight into the needs of EuroLAB members/laboratories.

8.2.21.2 A HIGH-LEVEL DESCRIPTION OF THE BUSINESS MODEL

The proposed business model for the MorphMetro platform focuses on delivering a secure and scalable solution for data exchange and analysis, leveraging advanced technologies such as blockchain and homomorphic encryption. The platform is designed to cater to industries where data security and privacy are paramount, including pharmaceuticals, food quality control, certification laboratories, and regulatory agencies. By collaborating with academic institutions for R&D, technology providers for infrastructure, and regulatory bodies for compliance, MorphMetro ensures robust development and regulatory adherence. The primary revenue streams include subscription fees for platform access, consulting services for customization, licensing for tailored solutions, and integration services to ensure compatibility with existing systems. The business model emphasizes continuous quality assurance, user engagement through workshops and conferences, and active feedback mechanisms to iteratively enhance the platform. This comprehensive approach aims to provide a high-value proposition by ensuring data privacy, regulatory compliance, and adaptability across various sectors requiring secure numerical data processing.
Business model canvas:
https://drive.google.com/file/d/1t0036HWiKIlVMaXCB7fEtZCoPi8yMWId/view

8.2.21.3 VALUE NETWORK

The value network of MorphMetro involves an interplay of various stakeholders, each contributing distinct benefits and engaging in reciprocal value exchanges through the provision of services, information, and revenue flows.

Stakeholders and Their Contributions:

1. Academic Institutions:

- **Benefits:** Provide research and development in homomorphic encryption and other technical areas.
- **Relationships:** Collaborate with MorphMetro for innovation and technical advancements.
- **Value Exchange:** Contribute cutting-edge research in exchange for real-world application opportunities and funding support.

2. Technology Providers:

- **Benefits:** Supply blockchain solutions, cloud services, and security technologies.

Funded by the European Union

- **Relationships:** Partner with MorphMetro to ensure seamless technology integration.
- **Value Exchange:** Receive revenue from providing infrastructure and services, gain market insights from practical deployments.

3. Regulatory Bodies:

- **Benefits:** Ensure compliance with data privacy, metrology regulations, and security laws.
- **Relationships:** Engage with MorphMetro to maintain and enforce regulatory standards.
- **Value Exchange:** Obtain secure and compliant technological solutions that enhance regulatory oversight capabilities.

4. Certification Laboratories and Regulatory Agencies:

- **Benefits**: Utilize secure data analysis tools to ensure data integrity and compliance.
- **Relationships**: Act as primary users and validators of the MorphMetro platform.
- **Value Exchange:** Provide feedback to MorphMetro, ensuring continuous improvement and regulatory alignment, and pay subscription fees for platform access.

5. Industries Requiring Data Analysis (e.g., Pharmaceuticals, Food Quality Control):

- **Benefits**: Implement secure and private data analysis solutions tailored to their specific needs.
- **Relationships:** Engage as key customers, benefiting from MorphMetro's sector-specific solutions.
- **Value Exchange**: Pay subscription and consulting fees, contributing to MorphMetro's revenue, and provide valuable use-case feedback.

6. TrustChain Ecosystem:

- **Benefits:** Leverages advanced cryptographic and blockchain solutions developed by MorphMetro.
- **Relationships:** Interacts with MorphMetro for ecosystem-wide innovation and development.
- **Value Exchange**: Mutual exchange of technologies and expertise, fostering growth and innovation across the network.

7. Alastria Blockchain Network:

Funded by the European Union

- **Benefits:** Enhances data integrity and security for various sectors through blockchain integration.
- **Relationships:** Integrates with MorphMetro to offer sector-specific blockchain solutions.
- **Value Exchange:** Receives advanced cryptographic libraries and contributes to broader adoption of blockchain technology.

Flows of Revenue and Information:

· Revenue Flows:

- Subscription fees from industries and regulatory bodies provide a steady revenue stream to MorphMetro.
- Consulting and integration services generate additional income, especially from industries needing tailored solutions.
- Licensing fees for customized versions of MorphMetro's solutions also contribute to revenue.

· Information Flows:

- Continuous feedback from users helps refine and enhance MorphMetro's platform.
- Academic institutions and the technical team exchange research and practical insights to drive innovation.
- Regulatory bodies and certification laboratories provide compliance and usage data, ensuring the platform meets all necessary standards.
- Benefits to Stakeholders:

· MorphMetro:

- Gains advanced cryptographic and blockchain solutions, revenue, and market credibility.
- Enhances product offerings through collaborative R&D and user feedback.
- Increases visibility and alignment with EU initiatives, such as TrustChain.

· Stakeholders:

- Receive cutting-edge, compliant solutions tailored to their needs.
- Benefit from collaborative development, reducing individual R&D costs and time.

Funded by the European Union

- Gain access to a broader infrastructure and support network, facilitating market penetration and operational efficiency.

Dependencies and Relationships:

- **Academic Institutions and Technical Team**: Depend on each other for R&D and practical application of innovations.
- **Technology Providers**: Depend on MorphMetro for market applications of their infrastructure solutions.
- **Regulatory Bodies and Certification Laboratories**: Depend on MorphMetro for secure and compliant data analysis solutions.
- **Industries**: Rely on MorphMetro's platform for operational efficiency and regulatory compliance.
- **TrustChain Ecosystem and Alastria**: Depend on mutual collaboration for the development and deployment of advanced blockchain and cryptographic solutions, enhancing overall ecosystem value.

This value network illustrates the synergistic relationships and dependencies among stakeholders, ensuring the successful provision of MorphMetro's services and the continuous transfer of value, information, and revenue within the ecosystem.

8.2.21.4 PRELIMINARY ECONOMIC (COST-BENEFIT) ANALYSIS

The analysis considers the costs associated with development, deployment, and maintenance against the expected benefits and revenue streams.

Cost Analysis

The initial investment in developing the MorphMetro platform involves several key components:

1. **Research and Development (R&D)**: Significant resources are allocated to developing the underlying technologies, including homomorphic encryption and blockchain integration. This includes salaries for developers, engineers, and cryptography experts, as well as the costs of collaborating with academic institutions.
2. **Technology Infrastructure**: Ongoing expenses for cloud services, blockchain infrastructure, and security tools are necessary to ensure robust and secure operations.
3. **Compliance and Regulatory Alignment**: Ensuring compliance with GDPR and other regulatory standards involves legal consulting fees and regular audits.
4. **Quality Assurance and Testing**: Continuous testing to maintain high standards of security and functionality, including user feedback incorporation.

Funded by the European Union

5. **Marketing and Outreach:** Costs for promoting the platform through industry events, professional networks, and targeted campaigns.

Benefit Analysis

The benefits of the MorphMetro platform are realized through multiple revenue streams and value propositions:

- Data Brokerage Fees: Charging a commission for securely facilitating data exchanges between parties.
- Subscription Services: Offering tiered subscription packages to access premium features, support, and updates.
- Integration Services: Providing services to enterprises and laboratories for integrating MorphMetro into their existing systems.
- Consulting and Training: Engaging in consultancy and training sessions to assist organizations in digitalization.
- Data Analysis Services: Supplying tailored analysis and insights from metrology data, in compliance with data privacy regulations.

Given the commercialization plans outlined for MorphMetro, here is a breakdown of potential revenue streams across the specified categories over the next five years. The percentages will shift over time, reflecting the company's growth, market penetration, and diversification of services.

	. Year 1	Year 2	Year 3	Year 4	Year 5
Data Brokerage Fees	10%	15%	20%	25%	30%
Subscription Services	15%	20%	25%	30%	35%
Integration Services	30%	25%	20%	15%	10%
Consulting and Training	25%	20%	15%	10%	5%
Data Analysis Services	20%	20%	20%	20%	20%

Summary of Revenue Trends

Funded by the European Union

- Data Brokerage Fees: Steadily increase as the network grows and more data exchanges are facilitated.
- Subscription Services: Consistent growth as the user base expands and more features are added.
- Integration Services: Decrease over time as the initial wave of integrations is completed.
- Consulting and Training: Decline as organizations become more self-sufficient.
- Data Analysis Services: Remain steady, with ongoing demand for specialized insights.

This structure reflects a shift from initial heavy reliance on integration and consulting services towards a more balanced revenue model driven by data brokerage and subscription services as MorphMetro matures and scales. In conclusion, the preliminary economic analysis of MorphMetro demonstrates a business case with strong potential for exploitation and sustainable revenue generation.

Cost-Benefit Comparison

The upfront and ongoing costs are justified by the substantial and diversified revenue streams, supported by a strong value proposition:

- Increased Adoption and User Base: By addressing critical needs in data security and compliance, MorphMetro is positioned to rapidly grow its user base across multiple industries.
- Scalability: The platform's scalable architecture allows for expansion without proportionate increases in costs, improving profitability as the user base grows.
- Market Differentiation: The use of cutting-edge technologies like homomorphic encryption and blockchain provides a competitive edge, attracting clients who prioritize data security and regulatory compliance.
- Positive Externalities: Enhancements in data privacy and security contribute to broader societal benefits, such as increased trust in digital services and reduced fraud, which can further drive adoption.

Economic Impact

Funded by the European Union

The platform's economic impact extends beyond immediate revenue:

- **Job Creation:** The expansion of the MorphMetro platform is likely to create new jobs in software development, system maintenance, user support, and cybersecurity.
- **Environmental Sustainability:** By enabling secure remote work and reducing the need for physical data transport, MorphMetro contributes to environmental sustainability, which can be a significant value proposition for environmentally conscious clients.

Next steps

- In order to prepare for long-term sustainability, the MorphMetro team is exploring several routes towards commercialization:
- Random Red has been invited to the IMEKO World Congress (which features up to 800 cutting-edge presentations from over 50 countries) to present the MorphMetro project, including the EBSI implementation, at the Digitalization Workshop[7].
- The large number of visitors and the event's relevance will facilitate further collaborations, including commercial opportunities.
- The PTB (German National Metrology Institute) has expressed willingness to be a partner organization in the ongoing EBSI Early Adopter Programme, which is also a component of their MorphMetro solution:
- https://www.linkedin.com/feed/update/urn:li:activity:7233813463821680641/
- https://www.linkedin.com/posts/sascha-eichstaedt-ptb_lets-hear-about-advancements-in-the-metrology-activity-7236072723146244096-dhOA/
- MorphMetro has arranged a presentation of on the 10th of September at BIOCentre (https://www.biocentre.hr/). BIOCentre is the EU-funded first biotech incubator in the Republic of Croatia, where several biotech laboratories operate. This venue will be highly relevant for their ILC/PT use-case:
- https://www.linkedin.com/feed/update/urn:li:activity:7237021621125865472/
- In addition to ILC/PT, they have also identified "Smart Standards" as a potential use-case and contacted the ISO team for Smart Standards (https://www.iso.org/smart) and arranged a meeting for the 11th of September.
- Having this additional use-case provides their solution with sufficient flexibility and diversity. It is important to note that ISO is the most important global

[7] https://www.linkedin.com/feed/update/urn:li:activity:7234092293366968320/

Funded by the European Union

standardization organization, composed of representatives from the national standards organizations of member countries. ISO has published over 25,000 international standards covering almost all aspects of technology and manufacturing and operates over 800 technical committees (TCs) and subcommittees (SCs) for standards development.

- Currently, the team members are preparing further project proposals linked to technologies used and developed in MorphMetro (homomorphic encryption and Alastria/EBSI blockchain), which will ensure their continuous development and expand their network of collaborators. For example, an NGI Sargasso (https://ngisargasso.eu/) proposal developed with a US-based partner/university, where usage of homomorphic encryption will be applied in transcontinental data exchange (between EU and US).
- In long term it is also important to mention that the team is a part of HMD's, IMEKO's and Eurolab's Digitalisation Workgroups: o HMD is Croatian Metrology Society and it represents numerous metrology companies and laboratories in Croatia.
- IMEKO is an international non-governmental federation of 42 Member Organizations individually concerned with the advancement of measurement technology.
- EUROLAB is an international not-for-profit organisation composed of 25 national associations all over Europe and beyond, grouping more than 3.000 conformity assessment bodies members, over 9.000 accredited laboratories and representing over 150.000 professionals.

So, through these organizations, MorphMetro can continuously monitor the needs of end users and appropriately improve their solution.

Funded by the European Union

8.2.22 DID-IMP

TABLE 81: COMPETITOR ANALYSIS

COMPETITOR	Decentralization	Scalability	Feeless	Maturity	Ease of use (App)	Reliable identification of devices
Nexus Group	-	+	+	+	+	+
Helium	+	+	-	+	+	+
Kalima	+	+	-	+	-	-
IOTA	+	+	+	+	-	-
Slock.it	+	+	-	-	+	-
Filament	+	+	-	+	-	-

8.2.22.1 EVALUATION CRITERIA

Decentralization: true to the concept of DIDs, the solution should operate in a decentralized manner, avoiding single points of failure and ensuring that no central authority can compromise the integrity of the network nor has an unbalanced predominant role.

Scalability: given the potential vast number of devices in IoT, the solution should be able to handle a large and rapidly growing number of identifiers and a very large amount of data transfers.

Funded by the European Union

Feeless: IoT devices are often resource-constrained. A good DID solution should be efficient in terms of blockchain gas consumption to ensure that all types of devices can use it and to allow easy manageability. Indeed, blockchain gas refuelling add a significant operational constraint.

Maturity: the maturity of the solution is its current development status, taking into account its TRL, access to market, number of customers and turnover.

Ease of use (App): it is the assessment of the user experience quality through the application.

Reliable identification of devices: this is the core value of the solution. Minuses in the reliability column are based on the fact that devices lose their reputation only after the actual commission of a harmful action.

8.2.22.2HIGHLIGHTED PROJECTS

All platforms listed use blockchain technology to secure data transmission. Blockchain technology provides the following security benefits: Immutability, Authentication, Privacy. However, they differ in terms of data transmission technology, cost, and target audience. Helium uses radio frequency spectrum for data transmission. This allows it to provide wider network coverage and lower latency than platforms based on blockchain technology. However, radio frequency spectrum can be limited and expensive. IOTA also uses blockchain technology for data transmission. However, it uses a more efficient algorithm than other platforms, which allows it to provide higher speed and scalability. However, IOTA requires transaction fees, which may be a drawback for some users. Slock.it also uses blockchain technology for data transmission. However, it is targeted at a narrower audience than other platforms and requires some technical expertise to use. Filament is a framework for developing web applications that uses blockchain technology to ensure the security and decentralisation of data. However, it is not very convenient for IoT device management. The usability of the platforms depends on their target audience. Platforms such as Helium and Kalima are focused on developers and require some technical expertise to use. Platforms such as IOTA and Slock.it have a simpler interface and are designed for a wider range of users.

8.2.22.3REVENUES AND COSTS

Funded by the European Union

Werenode is a for-profit software company that expects to create several revenue streams thanks to this project. The business model for a decentralized identity (DID) solution for secure automatic data transfer in IoT encompasses different revenue streams and strategic approaches to address the specific needs of IoT ecosystems. This model leverages the strengths of blockchain technology to provide a secure, reliable, and scalable solution.

8.2.22.3.1 Revenues

SUBSCRIPTION SERVICES & LICENSING FEES

Model: IoT device manufacturers and service providers pay a recurring fee to access the decentralized identity infrastructure. This is priced monthly for each IoT device for which the data transfers are done through the solution. This fits well into a software as a service platform (SaaS). DID-IMP also charges a licensing fee for the whole solution on a yearly basis, for the use of their proprietary software or firmware that integrates DID capabilities into IoT devices.

Benefits: This ensures a steady revenue stream and covers continuous access to the network, maintenance, updates, and customer support. This generates upfront revenue and also ensures that clients are invested in the platform. It also allows recovery of development costs and funds for ongoing innovation.

TRANSACTION FEES

Model: Although the primary architecture might promote feeless transactions for end-users, the model can include minimal fees for high-volume enterprise transactions or advanced features. Indeed, in some use cases, it is expected to be able to collect a small commission fee for some certificate issuance or revocation or even for some transfers. This scheme is studied for some logistics use cases of DID-IMP.

Benefits: This helps maintain the blockchain infrastructure and compensates for the operational costs associated with large-scale data handling.

DATA SERVICES AND API ACCESS

Funded by the European Union

Model: DID-IMP offers analytics and data verification services that utilize the secure, traceable nature of blockchain to provide added value from the data transferred within the network. In a second wave of developments, it will also provide APIs that enable third-party developers to build applications that interface with the decentralized identity network.

Benefits: Businesses benefit from enhanced data insights and integrity, creating a value-added service that justifies additional fees. The API approach fosters an ecosystem around the technology, in consistency with TrustChain ecosystem strategy, driving wider adoption and generating additional revenue from API calls.

CUSTOMIZATION, INTEGRATION, TRAINING AND SUPPORT SERVICES

Model: Charge for consulting and customization services to integrate the decentralized identity system into existing IT landscapes. Offer training for developers, IT staff, and end-users, as well as ongoing technical support. This expert implementation and integration service relies on the fact that as designers of the DID-IMP solution, it is expected the team to be able to provide expert services for the integration and implementation of the solution.

Benefits: This offers high-margin revenue and helps clients maximize the value of their investment in the platform. Furthermore, training and support not only provide additional revenue streams but also ensure smooth operation and customer satisfaction, fostering long-term client relationships.

HARDWARE SALES OR PARTNERSHIPS

Model: They will sell their solution or partner with providers of specialized hardware that is optimized for IoT environments utilizing DID systems. They currently consider using the DID-IMP solution to implement a smart electricity meter that will allow the development of home energy management applications in connection with their current EV charging solution and their Decentralized Energy COmmunities (DECO) project with OP Mobility. This is just an example of many other means where DID-IMP will leverage key use cases to create economical traction through hardware or partnerships.

Benefits: This can create a comprehensive solution offering that includes both software and hardware, optimizing the performance and security of the entire system.

CERTIFICATION AND COMPLIANCE

Model: Provide certification services for devices and companies that meet specific security and compliance standards enabled by the DID system.

Benefits: Certifications can increase the trustworthiness of the devices and services, creating a competitive edge and potentially opening new markets.

Funded by the European Union

By leveraging these business models, their decentralized identity solution for IoT will provide a secure and efficient means of data transfer while generating multiple revenue streams. This diverse revenue model not only stabilizes the financial footing of the initiative but also encourages broad adoption across industries by offering various ways to engage with the technology based on the specific needs and capabilities of different users.

8.2.22.3.2 COST STRUCTURE

Implementing DID-IMP systems in IoT involves a variety of costs across several categories. Development costs include the creation of the blockchain solution, security measures to protect the data and identities, and possibly fees for consulting services. Infrastructure costs are associated with running blockchain network operations, including transaction fees (such as gas on Ethereum, though in the TrustChain framework there is currently no cost to use the Alastria network), possibly costs for running full nodes, and additional storage needs for larger data sets, which may utilize decentralized storage solutions like IPFS. Blockchain expenses are fees, legal (licenses, documents etc).

TABLE 82: COSTS BREAKDOWN

Costs	2024	2025	2026	2027	2028
IT&RD	3 500	89 200	102 652	293 113	491 867
Blockchain	200	1 600	20 000	125 000	300 000
Customer support	3 800	19 000	190 000	950 000	1 900 000
Sales&Marketing	9 000	84 500	201 180	793 652	1 525 619
Autres	80 175	125 400	257 320	549 206	607 791
Total	**96 675**	**319 700**	**771 152**	**2 710 972**	**4 825 277**

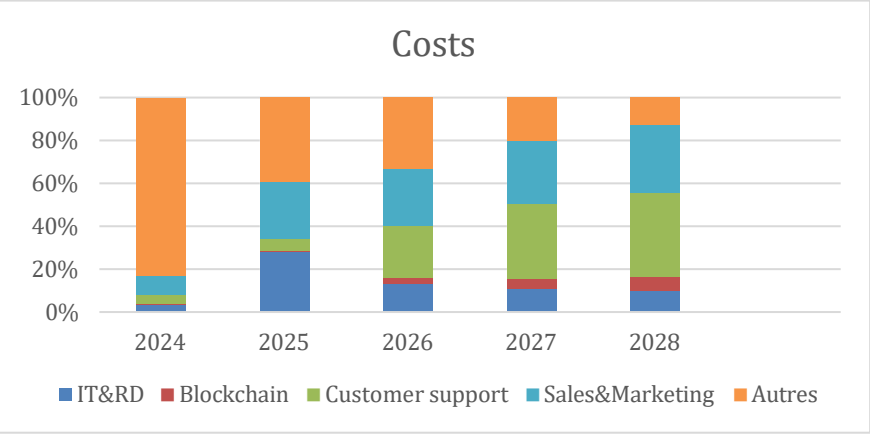


FIGURE 22: COSTS BREAKDOWN

Funded by the European Union

Integration costs involve expenses to update or modify IoT devices for blockchain compatibility and the costs to integrate the blockchain with existing IT systems. Operational costs cover the ongoing maintenance of the blockchain network, support, and training for users and staff. There are also significant regulatory and compliance costs to ensure the solution meets data protection standards like GDPR and obtains necessary industry certifications. Lastly, miscellaneous costs include marketing to promote adoption and continuous research and development to keep the technology up-to-date. Each of these cost factors must be meticulously managed to ensure the blockchain solution is both functional and financially sustainable.

TABLE 83: HUMAN RESOURCES EXPENSES

Five years plan (€)	2024	2025	2026	2027	2028
Team scenario (FTE)					
DG	0,25	0,50	0,50	1,00	1,00
CTO	0,50	0,50	1,00	1,00	1,00
CIO	0,00	0,00	0,50	1,00	1,00
DAF/COO	0,00	0,00	0,00	1,00	1,00
Development & IT / smart contracts	1,00	2,00	3,00	6,00	9,00
Marketing, sales, administration	0,00	1,00	1,00	3,00	5,00
Total	**2**	**4**	**6**	**13**	**18**
Team costs (including employee social charges but excluding employers social charges)					
DG	84 615	89 692	95 074	100 778	106 825
CTO	76 923	81 538	86 431	91 617	97 114
Confirmed Engineer	61 538	65 231	69 145	73 293	77 691
Development & IT / smart contracts	53 846	57 077	60 502	64 132	67 980
Marketing, sales, administration	38 462	40 769	43 215	45 808	48 557
Total	**113 462**	**240 538**	**401 903**	**897 843**	**1 252 766**

Developing a decentralized identity blockchain-based solution for an IoT Secure Automatic Data Sharing (SADS) system requires a diverse and skilled team. At the core, Blockchain Developers are essential for crafting the underlying blockchain architecture, writing and testing smart contracts, and ensuring their interoperability with IoT devices. IoT Engineers play a crucial role in integrating blockchain technology with physical IoT devices, adapting existing firmware, and managing real-time data flows securely. Additionally, Support and Training Staff are necessary for educating users and maintaining system efficiency post-deployment, while Marketing and Business Development Managers work to promote the solution, identify strategic business opportunities, and drive adoption across the IoT ecosystem.

Funded by the European Union

TABLE 84: OTHER COSTS (FIVE YEARS PLAN)

Total expenses (equipment and services)	**21 675**	**86 500**	**411 600**	**1 805 800**	**3 562 800**
Equipment purchases	**3 000**	**12 000**	**17 000**	**29 500**	**39 000**
Servers	1 500	6 000	8 000	10 000	12 000
Miscellaneous material	500	2 000	3 000	6 500	9 000
IT equipment	1 000	4 000	6 000	13 000	18 000
...					
Operational and external expenses	**18 675**	**74 500**	**394 600**	**1 776 300**	**3 523 800**
Legal fees for shareholding management	0	1 000	5 000	5 000	5 000
Other legal fees / contracts	1 000	5 000	10 000	20 000	25 000
Accounting	1 000	1 000	2 000	15 000	20 000
Renting	1 000	5 000	5 000	10 000	20 000
Insurances	500	1 000	1 000	2 000	4 000
IT developments	1 000	5 000	10 000	20 000	20 000
Patents					
Telephone	175	400	600	1 300	1 800
Digital marketing	5 000	10 000	15 000	20 000	30 000
Sales incentives	2 000	10 000	15 000	20 000	30 000
CPA cost per acquisition	2 000	11 500	115 000	575 000	1 150 000
Supply chain					
Blockchain transaction fees	200	1 600	20 000	125 000	300 000
Customer support	3 800	19 000	190 000	950 000	1 900 000
Travels	1 000	4 000	6 000	13 000	18 000
...					

8.2.22.4 BUSINESS CONTEXT

8.2.22.4.1 Overview

The Internet of Things (IoT) is playing an increasingly central role in data production globally, with projections suggesting that nearly half of the world's data will soon come from IoT devices. As of 2020- 2021, the big data market, which encapsulates a wide array of industries and technologies, was estimated to have a value between $138.9 billion and $156 billion. This market is expected to grow substantially, driven by the widespread adoption of mobile technologies and an ever-growing need for efficient data sharing mechanisms. In particular, the sector focused on automated IoT data sharing is seeing a significant uptick in interest and investment, setting the stage for substantial growth in the near future.

Allied Market Research has highlighted the IoT payments market as a specific area of interest. Valued at $7.6 billion in 2018, this market is expected to soar to $27.8 billion by 2026, growing at a compound annual growth rate (CAGR) of 17.6%. This surge is largely fuelled by the global shift towards cashless transactions, an increase in smartphone usage, and the need for more robust payment security measures. These factors are not just enhancing existing applications but are also paving the way for new innovations in how IoT devices handle and transfer financial data.

The anticipated expansion of the IoT payments market is indicative of a broader trend in which IoT technologies are revolutionizing industries by enabling more streamlined, secure, and efficient operations. The integration of IoT devices with advanced data analytics and machine learning is transforming big data from a sheer volume of information into actionable insights that can drive efficiency and innovation across

Funded by the European Union

various sectors, including healthcare, automotive, manufacturing, and urban development.

Furthermore, the integration of blockchain technology in IoT data sharing provides an added layer of security and reliability, offering tamper-proof systems for transmitting sensitive information across networks. Blockchain not only enhances data security but also introduces greater transparency and efficiency in processes such as supply chain management, asset tracking, and compliance monitoring.

As IoT technologies continue to evolve, the potential for new applications and business models seems almost limitless. Companies that are able to leverage IoT capabilities effectively are likely to gain a significant competitive edge in the rapidly evolving digital economy. This is particularly true for those that invest in integrated solutions that not only improve data flow but also enhance the security and reliability of these data exchanges.

Overall, the growth of the IoT sector and its integration with big data and blockchain technologies is creating a dynamic ecosystem where advanced data sharing and processing capabilities are becoming crucial for business success. This trend is expected to accelerate, underpinning a wide range of innovations that could transform daily life and business operations across the globe.

The accessible market corresponds to the cumulated markets of SADS systems for Smart Home Devices, Industrial IoT, Automotive industry, Healthcare, Supply Chain and Logistics and Smart Cities, whereas their first target market corresponds mainly to Smart Home Devices and Industrial IoT.

TABLE 85: MARKET FOR SECURE AUTOMATIC DATA SHARING

	2022	2025	2030
TAM	1.02 B$	3.9 B$	10.8 B$
SAM	0.34 B$	2.92 B$	10.8 B$

Funded by the European Union

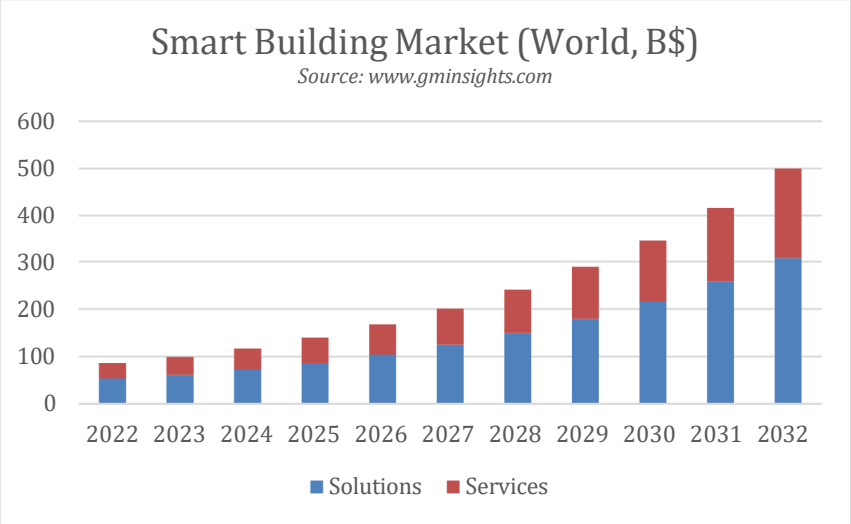


FIGURE 23: – EXAMPLE OF SMART BUILDING SYSTEMS & SOLUTIONS (B$)

DID-IMP is built to be easily scalable globally. Furthermore, premium features or add-ons can be added later to improve the market value of the solution.

8.2.22.4.2 MARKET SEGMENTS AND CUSTOMER PROFILES

DID-IMP, as decentralized identity (DID) blockchain-based solution for an IoT Secure Automatic Data Sharing (SADS) system targets several key market segments, each with unique needs and opportunities for integration. First the segment of Smart Home Devices includes IoT devices used in residential settings, such as smart thermostats, security systems, and home assistants. A DID system enhances privacy and security in data sharing between devices and service platforms, allowing homeowners to control who accesses their data.

Nevertheless, their business priority is industrial IoT (IIoT). Indeed, factories and industrial setups use IoT for predictive maintenance, operational efficiency, and safety enhancements. DIDs ensure secure, tamper-proof communication between machines and management systems, facilitating trust and data integrity in environments that often involve sensitive or proprietary information. This is a critical market as the ESG pressure on the industry is currently huge and implies to deploy emergency action to be able to analyse, monitor and improve many key indicators that utilize IoT sensors. This is especially true in the automotive industry where additionally, connected cars and autonomous vehicles use IoT systems for navigation, safety, and entertainment

Funded by the European Union

features. DID-IMP can manage identities and permissions for data sharing between vehicles and infrastructure, improving security and personalization.

This shouldn't cancel any interest for the huge market for healthcare. IoT devices in healthcare, such as wearable health monitors and connected medical devices, benefit significantly from DID solutions by safeguarding patient data and supporting compliance with strict regulatory standards for data protection and privacy.

However, supply Chain and Logistics use extensively IoT for tracking and managing goods. DID- IMP keeps a keen eye on this segment to provide a solution to verify device data across the supply chain, enhancing transparency and reducing fraud.

Finally, IoT devices in smart cities manage everything from traffic control to pollution monitoring. DID-IMP can help secure the vast amounts of data these devices generate, ensuring that city managers and authorized entities can leverage this data for planning and public safety without compromising privacy. These diversified market segments demonstrate the broad applicability of DID blockchain solutions across various industries, emphasizing their role in enhancing security, privacy, and efficiency in the IoT ecosystem.

Concerning customer profiles, there are some first feedbacks that would lead them to believe that their first customers will probably be SME which are trying to innovate with new efficient solutions for smart buildings or factories.

8.2.22.4.3 Acquisition Channels & Marketing Strategy

DID-IMP partners with Greendoy, a company that is specialized in realizing carbon footprint assessment of small companies. They provide reports and analysis of the carbon impact of these companies, which then position this company ideally to propose action plans for such carbon footprint reduction. DID-IMP then takes its full place as a candidate component to build a dynamic capacity for monitoring the carbon footprint of the company.

8.2.22.4.4PERSPECTIVES

The marketing strategy and acquisition channels will be coupled with TrustChain ecosystem. It also primarily targets digital communication channels using communities favourable to the development of web3.0.

From there, they can draft forecast the development of the project for the next five years:

Funded by the European Union

TABLE 86: REVENUE AND CASH FLOW FORECAST

Number of target buildings in the accessible markets	40 000	48 000	57 600	69 120	82 944
Number of customer buildings	20	100	1 000	5 000	10 000
Number of IoT devices / building	100	160	200	250	300
Monthly service fee / IoT device	0,60	0,62	0,64	0,66	0,68
Annual licence fee / building	590,00	650,00	690,00	690,00	690,00
Average cost / IoT device	0,45	0,41	0,37	0,33	0,29
Average solution cost / solution / year	500,0	450,0	400,0	380,0	360,0
SaaS gross margin	25,0%	33,7%	41,9%	49,7%	57,1%
Full solution gross margin	15,3%	30,8%	42,0%	44,9%	47,8%
Annual turnover	**26 200,0**	**183 656,0**	**2 217 696,0**	**13 284 543,0**	**31 210 990,3**
Total Annual Turnover	**26 200**	**183 656**	**2 217 696**	**13 284 543**	**31 210 990**
EBITDA	-129 252	-267 235	-26 014	1 488 944	4 040 428
Free Cash Flow	-156 175	-324 312	-116 766	1 296 550	3 734 521
Fund raising	600 000	0	0	0	0
Cash at the end of fiscal year	443 825	119 513	2 747	1 299 297	5 033 817

This development plan relies on partnerships with key players to develop quickly the DID-IMP concept. They also especially target companies working in energy management systems for smart buildings like charging stations and solar panels installations to distribute and promote the DID-IMP solution.

Funded by the European Union

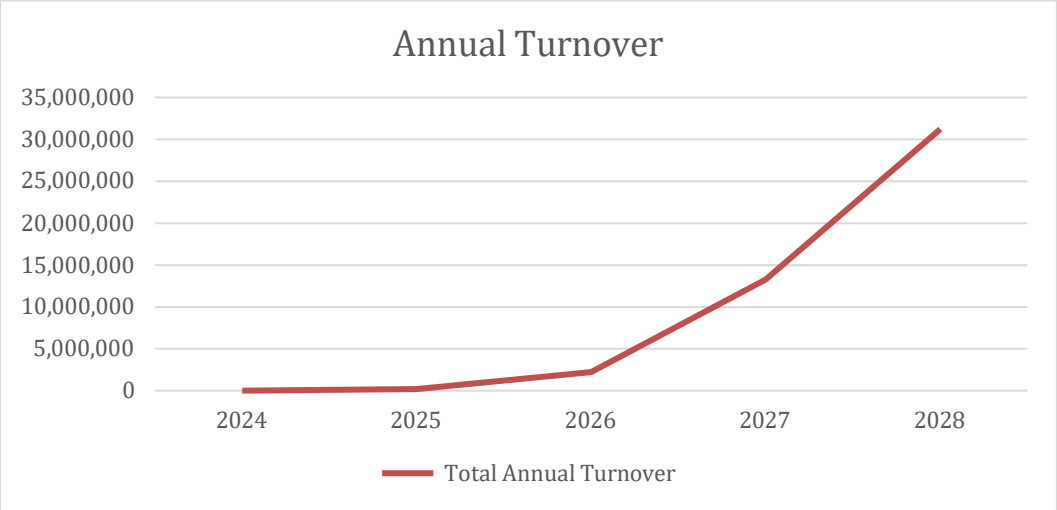


Figure 17 – Total Annual Turnover

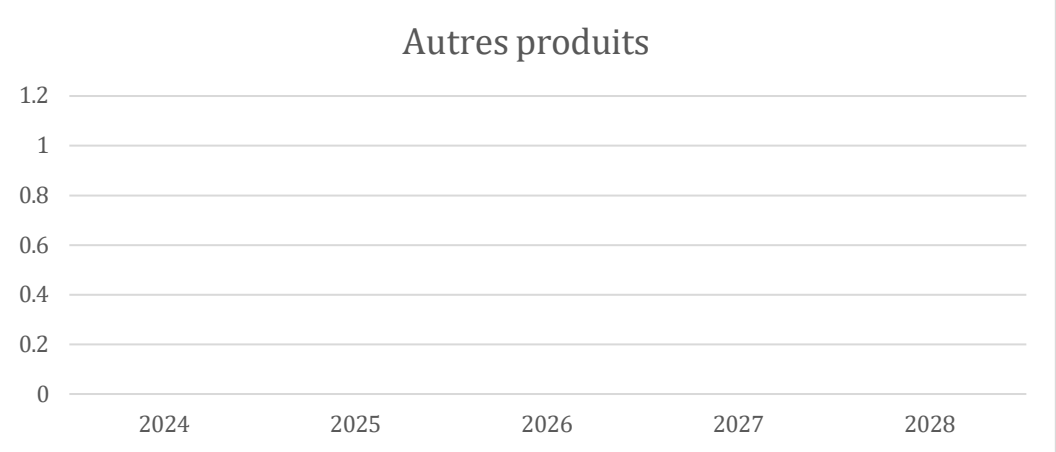


Figure 18 – Gross Operating Profit

As a Web3.0 solution, DID-IMP is part of the TrustChain program, so it will leverage all the marketing and efforts of promotion. The NGI initiative is a strong framework to push

Funded by the European Union

forward the projects so the economic impact should be greater than if DID-IMP was a standalone platform. Indeed, their vision is resolutely oriented towards the new frontier of the digital economy. Web3.0 is very concretely built on the decentralization of infrastructures as well as the decentralization of the value chain that irrigates them. DID-IMP firmly believes in the ability of Web3.0 technologies, particularly the Blockchain, to put an end to the "winner takes all" situation that clogs the global economy, pushing players like GAFA to the rank of global economic superpowers.

Their solution is natively international and can be easily deployed everywhere, both in developed and developing countries.

8.2.22.4.5 BUSINESS PROTECTION

To prevent someone from cloning their contract and setting up slightly cheaper transaction fees, they have to ensure that their product offers a comprehensive suite of features beyond just smart contracts. This includes an intuitive dashboard, an integrated wallet, robust security measures, and continuous updates. These additional components and the seamless user experience they provide create a significant value proposition that isn't easily replicated by simply lowering transaction fees.

8.2.22.5 ECONOMIC ANALYSIS

The economic analysis of a decentralized identity (DID) blockchain-based solution for an IoT Secure Automatic Data Sharing (SADS) system revolves around its potential to enhance efficiency, reduce costs, and open new revenue streams, balanced against initial and ongoing investment requirements.

Cost Reduction: Implementing DID can significantly lower operational costs by automating identity verification processes, reducing the need for intermediaries, and minimizing fraud and data breaches. These efficiencies decrease both direct costs, such as labour and transaction fees, and indirect costs, such as those associated with data breaches and compliance penalties.

Initial Investment: The upfront costs for developing and deploying a DID system are substantial. These include expenses related to technology development, system integration, security measures, and initial training for users. These costs are offset over time through operational savings and efficiency gains.

Revenue Generation: By providing robust data security and privacy, DIDs enhance trust in IoT systems, potentially increasing user adoption and enabling businesses to charge premiums for secure services. Additionally, the system can facilitate new business models, such as data monetization through secure data marketplaces.

Funded by the European Union

Market Differentiation: Companies that adopt DID solutions can differentiate themselves from competitors by offering enhanced security and privacy, appealing to privacy-conscious consumers and compliance-focused industries.

Scalability and Flexibility: The decentralized nature of blockchain allows for scalability without significant additional costs associated with traditional centralized systems. This adaptability is economically beneficial for growing IoT networks.

In summary, the long-term economic benefits derived from operational efficiencies, new revenue potentials, and competitive advantages present a compelling case for the large adoption of DID-IMP.

8.2.23 DGUARD

To ease the process of defining the business model and operational strategy, DGUARD will commence by methodically delineating their proposal and underlying hypotheses. Through a systematic approach, they intend to validate these hypotheses incrementally throughout the duration of this study. Subsequently, they will articulatea coherent strategy designed to harmonize with prevailing market dynamics and regulatory frameworks. By subjecting their assumptions to rigorous scrutiny and refinement, they aim to establish a resilient foundation upon which to structure their business and operational initiatives.

Outcomes:

The project aims to provide a framework for consent management and privacy - among data sharing through a platform that provides a Self-Sovereign Identity (SSI) whilst preserving privacy using zero knowledge proofs among authentications and proxy re-encryption to ensure control of usage of data. Furthermore, the platform incorporates a blockchain-notarized audit trail to guarantee the traceability and accountability of data management procedures which is meant to be cross-industry, easily integrable and user-friendly. More precisely the outcomes expected for this project are the following components and modules:

1. Back-end API: It includes modules for self-sovereign digital ID, consent management, and audit trail logging. The self-sovereign digital ID module enables credential provisioning and authentication using Zero Knowledge Proofs (ZKPs). Consent management orchestrates secure data exchange, while the audit trail log tracks platform actions, ensuring traceability and accountability.

2. User-friendly Front-end: Implemented as a static web app, it provides modules for user management & sign-in, consent management, and verifiable logs of activity. Users can log in using an authentication protocol, manage consent preferences, and validate platform actions.

Funded by the European Union

3. SDKs: Facilitates integration of platform features into external applications. Modules include client-side ZKP authentication and proxy re-encryption, allowing secure data sharing while preserving confidentiality and integrity.

What it aims to solve:

1. Lack of control over access to personal information. Individuals sharing personal data and data consumers will be provided direct control over data access and verification of authenticity and consent. Establishing a trust mechanism empowering both parties (data producer and consumer) for consent management and data authenticity, independently of third-party involvement (data controller).

2. Lack of anonymity and privacy. By leveraging ZKP authentication and proxy re-encryption data will be shared guaranteeing anonymity and privacy. This will be accomplished by providing a privacy-preserving authentication mechanism. That allows users to reliably anonymize data on the client side. Additionally, deploying encryption schemes like proxy re-encryption will enable users (data producers) to maintain control over their data, even when it is held by third parties (data controllers / consumers).

3. Lack of data traceability and accountability. Data sharing procedures will be traceable, with well-defined accountability mechanisms in position. All digital interactions related to data sharing will be traceable and notarized to ensure maximum transparency and non-repudiation, reinforcing the accuracy and verifiability of data sharing procedures.

Where is it meant to be applied:

While DGUARD's technological capabilities are meant to have cross-industry relevance and compatibility with various existing platforms, their strategic vision leans towards focusing their efforts initially within a specific market segment. By concentrating on a singular market with identifiable pain points and significant growth potential, they aim to establish a strong foothold. This approach allows them to refine and tailor their solution to meet the specific needs of this market while also laying the groundwork for future expansion into other data sharing markets associated with data spaces. They have selected the healthcare data space as the first vertical to be dealt due to the following factors:

1. Solution fits the market pains. In the healthcare domain, where the stakes are notably higher due to the sensitivity of the data involved, the challenges surrounding data privacy are particularly pronounced. This sector, which serves as the primary focus of their ground-breaking solution, faces intensified pressure to address these issues effectively. Despite significant advancements in protocols and techniques such as OpenEHR for encrypted standardized record-keeping, k-Anonymity for data indistinguishability, Differential Privacy for enhanced privacy protection, and the FHIR Protocol for secure data exchange,

Funded by the European Union

the persistent hurdles of centralized trust requirements and technological barriers loom large.

2. Forecasted grow of the potential market. The utilization of AI in medical applications is currently undergoing a rapid expansion. Projections indicate that by 2030, investments in AI development for medical purposes will soar to an estimated $69.8 billion. This surge is fueled by several factors, including the escalating prevalence of chronic diseases and the increasing availability of medical data. Moreover, there is a growing emphasis on the importance of trustworthy AI, with investments expected to reach $11.3 billion by 2023. This focus on trustworthiness aims to address concerns surrounding bias and discrimination within AI systems, ensuring fair and equitable outcomes. Specifically, within the realm of dermatology, the application of AI is poised for significant growth, with an anticipated market value of $1.2 billion by 2028. This growth is driven by the rising demand for early detection of skin diseases, highlighting the potential of AI technologies to revolutionize diagnostics and improve patient outcomes.

3. Prior experience in the space. DGUARD credibility and potential is significantly reinforced by the extensive expertise and proven track record of BeHit & Top Doctors, who plays a major role in the specific sector know-how of this project. Their wealth of experience and success in navigating the intricacies of the healthcare landscape instils confidence in their ability to deliver impactful solutions. Entities in this project are in collaborative initiatives with entities like Evidenze Groups and Grifols, which does not only deepen their insights into the sector but also foster a broader understanding of its complex dynamics. These partnerships facilitate knowledge exchange, fuel innovation, and position them at the forefront of addressing evolving needs and opportunities in the healthcare industry and market positioning.

8.2.23.1.1 SWOT Analysis

Once the solution and its potential market is defined, an initial SWOT analysis can be presented to identify key factors of DGUARD exploitation plan and its business model as well to identify risks and validate their initial exploitation hypothesis.

TABLE 87: OPPORTUNITIES AND THREATS FOR DGUARD

SWOT	
OPPORTUNITIES	THREATS

Funded by the European Union

- GROWING DEMAND. As priorly stated, there's a growing demand of privacy preserving and compliant solutions worldwide in the space of data sharing and specially in data sensitive sectorssuch as healthcare. - REGULATORY ALIGNMENT. Europe is currently in the process of redefining its regulatory framework, encompassing directives such as eIDAS, Data Acts, andIA Acts, among others. Particularly in healthcare with the Approval of the EHDS (European Healht Data Space). This endeavor aims to harmonize the utilization of emerging technologies for the betterment of its citizens, thereby generating increased demand in relevant sectors, particularly healthcare. - NEW ECONOMY SPACE WITH ALIGNED INCENTIVES. The data landscape is fostering the development of a fresh economic ecosystem where all stakeholders are incentivized to share information. Over time, this proves advantageous for each party involved, thereby facilitating the establishment of a value proposition tailored to every stakeholder.	– COMPETITION. A large volume of vendors already provide access to solutions and infrastructure that may fit the same category of products as, although none of them providethird-party independent guarantees. – ACCEPTANCE OF TECHNOLOGY. There is still frequent reluctance of some companies to start working with decentralized technologies due to regulatory uncertainty, privacy concerns, misunderstanding of the technological basis of SSI and concernsrelated to user experience and usability. - TRANSITIONING TO PRODUCTIVE ENVIRONMENTS. The timeline for implementing comprehensive regulations and foundations remains uncertain, resulting in a prolonged onboarding process for customers in the short and medium term as they adjust to the evolving landscape.

TABLE 88: STRENGTHS AND WEAKNESSES FOR DGUARD

SWOT	
STRENGTHS	WEAKNESSES
- COMPLETENESS. DGUARD offers the easiest route for enterprises to leverage decentralized technologies for secure and compliant data exchanges that	- CHALLENGING FOR NON-TECHNICAL PROFILES TO GRASP. Despite DGUARD's intended accessibility for non-specialized users, comprehending

Funded by the European Union

cover the whole range of needs for consent management and user privacy.

- USABILITY. DGUARD does not just provide an integration layer but also a predefined interaction dashboard to manage consents thus easing data producers and consumers experience while dealing with data sharing procedures.

- SCALABILITY, INTEROPERABILITY AND PRIVACY. DGUARD covers by default the major technological concerns and risks to be considered when integrating with decentralized technologies.

– ENHANCED INTEGRATION CAPABILITIES. DGUARD platform can seamlessly integrate with existing systems and processes, making it easier for businesses to adopt as they do not require to change its technological stack.

- MARKET KNOWLEDGE. DGUARD team has prior experience and already existing relations with the targeted market, thus easing pilot and at-scale deployments.

- STANDARIZATION. All DGUARD components are standardized under international and regulations criteria, thus accelerating interoperability and comprehension.

the underlying cutting-edge technologyrequires delving into various aspects such as ZKP, SSI, PRE, and so on. This might be required by a buyer persona to evaluate among other solutions.

- TECHNOLOGY READINESS AND FUTURE DEVELOPMENTS. While the solution is expected to be fully operational, given its innovative nature,it is anticipated the need for several adjustments and enhancements in the short and medium term to meet industry standards. These adjustments will primarily involve piloting various adaptations and upgrades to ensure widespread industry acceptance.

- PARTIALLY ADDRESSABLE MARKET SIZE: The DGUARD platform encompasses a vast array of key players,necessitating a partnership-oriented approach due to limitations in their team's capacity to directly engage with all stakeholders. This strategy entails collaborating with distribution channelsand software providers to extend their reach effectively.

Funded by the European Union

From this analysis the following conclusions can be undertaken:

Healthcare as a target market. The choice of sector is grounded in a thorough analysis of expertise, market growth projections, and identified market needs. Alignment with sectors is ensured where the team's skills are most relevant and where there are promising opportunities for innovation.

Prioritization of DGUARD values. The value proposition must center on addressing pain points, emphasizing ease of deployment, usability, and regulatory compliance. DGUARD focus on making their solution easy to use and compliant with relevant regulations to build trust with their customers.

High-touch approach launch: During the initial phase, they must prioritize engaging closely with customers and stakeholders to develop tailored pilot programs. These programs will serve as a testing ground for their technology, allowing them to gather feedback and make iterative improvements that align with market needs.

Importance of dissemination and simplifications: They must articulate their solution in a clear and understandable manner to overcome complexity barriers. By simplifying complex concepts, they effectively communicate their value proposition and build trust with the market.

Long-term success requires alliances for mass deployment: They recognize the importance of forging alliances to expand their reach and onboard additional stakeholders. Collaborative partnerships enable them to leverage sources, expertise, and networks to accelerate growth and solidify their position as a market leader.

8.2.23.1.2 EXPLOITATION PLAN

Based on the conclusions drawn and the data gathered during the previous analyses, they segment their plan for successful exploitation into three main phases, with a fourth transversal category that intersects with all operations.

8.2.23.1.2.1 (P1) Validation and development

During this initial phase, their primary focus will be on developing the framework for their solution and conducting a pilot in a controlled environment as outlined in point P2 to validate the solution. This phase also entails comprehensive market research and validation efforts. These activities are crucial for ensuring that their solution aligns with the specific needs and regulatory requirements of the healthcare sector, laying a solid foundation for subsequent phases of their exploitation plan once they have an initial functional version of the software developed which can be applied to other enterprises and cases.

Funded by the European Union

(P2) Piloting, refinement and alignment with regulations and required criteria

Once the foundational elements are established and an initial pilot confirms the validity of the solution, their objectives include developing a well-structured pilot program tailored to address the specific needs and intricacies of the healthcare sector.This entails collaborating closely with selected healthcare organizations to jointly design and implement pilot initiatives, focusing on real-world challenges and demonstrating the effectiveness of their solution.

Simultaneously, DGUARD will focus on the refinement and iteration of their technology. Thisinvolves continuously refining and iterating on their technology based on insights gathered from pilot programs and user feedback. The team will incorporate user feedback and market intelligence to enhance the usability, scalability, and interoperability of their platform, ensuring it aligns with evolving industry standards.

Furthermore, ensuring regulatory compliance is paramount. They will remain informed about evolving regulatory requirements within the healthcare sector, ensuring strict compliance with data privacy laws such as GDPR and HIPAA. This will involve working closely with legal experts to navigate regulatory complexities and obtain necessary certifications or approvals for their solution's compliance.

In this second phase, the business approach will be more linked to closed projects than to a fully SaaS model as it will require the involvement of their teams to deal with integrations, adaptations, and improvements.

(P3) Scaling and expansion

Once the solution reaches its optimal refinement and meets the stringent standards of quality aligned with market needs, their focus will pivot towards expanding its market reach and penetration. This pivotal phase entails leveraging the invaluable asset of customer testimonials while concurrently initiating a strategic partnership approach. Their strategic agenda involves a gradual expansion of operations, strategically building upon the achievements of pilot programs and the favourable feedback garnered from their valued customers. Through this, they aim to not only attract additional institutional investors but also to engage with potential distributors who can help amplify their solution's visibility and accessibility across diverse markets and regions.

In this third phase, the business approach will be more linked to licenses based on usage of the platform as their channels will be the ones executing the integrations once the software is stabilized.

8.2.23.1.3 MARKET ANALYSIS

TABLE 89: ANALYSIS OF OTHER SOLUTIONS IN THE MARKET

Solutions	Interoperability (FHIR, HL7, OpenEHR)	Personalisation	DaaS	Traceability

Funded by the European Union

TopDoctors	Strong ELT tool featuring HL7 FHIR, HL7 v2 and openEHR.	Highly customizable: interface, templates, KPIs, information display, data protocol, settings such as on premises - cloud build... Also personalised services tailored to the specific needs of clinics, health practitioners, and healthcare providers.	DaaS platform integrated with patients' EHR. Personalised healthcare based on patient data. NVIDIA Flare SDK integration for federated learning.	Integration with blockchain.
Cerner	Wide range of integrations with EMR, LIS, HIEs and	Highly customizable: interface, templates,	DaaS platform focused on clinical research. Integration with	Data traceability and clinical research. System aimed at security
Solutions	**Interoperability (FHIR, HL7, OpenEHR)**	**Personalisation**	**DaaS**	**Traceability**
	other healthcare systems.	workflows, order sets and API access for custom integrations.	EHR for research and analysis.	and information monitoring.
Veradigm	Wide range of integrations as an Open Network solution.	Specialty-specific. Hundreds of preloaded templates and protocols. Learning specific order habits.	Real-world data solutions for research. Access to more than 180 million patient records.	High level based on system functionalities (EHR, patient portal, analytics, etc.).

Funded by the European Union

DXC	Compliance with the three standards. Platforms: DXC Connect, DXC Open Health Connect, DXC Rhapsody. Member of the Health Interoperability Initiative. Success story: Implementation of regional HIEs.	Adaptable to the needs of suppliers. Customization of workflows, interface and functionality.	Lack of information about DaaS. However, DXC's expertise in data engineering, infrastructure, and life cycle management, as well as their emphasis on data-driven insights, suggests a strong foundation that could support effective DaaS functionalities within their EHR solution.	Strong technical capacity for tracking and integrations.
Maxims	HL7 and FHIR support. Commitment to interoperability.	High degree of customization. Adaptable and configurable interfaces.	There's no specific DaaS platform but their focus on interoperability and adherence to standards (HL7, FHIR) suggests potential for data exchange and potential	Traceability in EPR systems. Compliance with standards such as NHS Digital DCB0129.
Solutions	Interoperability (FHIR, HL7, OpenEHR)	Personalisation	DaaS	Traceability
			integration with DaaS solutions.	
Meditech	Traverse Suite for data exchange with external sources, use of CommonWell Health AllianceÆ, bidirectional interfaces, openness to a partner ecosystem.	Specific tools for doctors (Expanse Virtual Assistant) and nurses (Expanse Point of Care), considering the needs and workflows of each role.	Expanse as a scalable DaaS platform. Traverse Tool makes it easy to connect to various data sources, internally and externally.	Prioritization of traceability through complete documentation and registration of changes and accesses. Order and results tracking functionality.

Funded by the European Union

System C	It supports various interoperability capabilities, third-party integrations, data access and communication through exchange protocols. Extensive experience in interfaces with clinical and administrative systems.	The platform focuses on adaptability, but information on the level of customization of the EPR system is not specific. It includes functionalities for medication management, clinical support, patient administration, etc.	Does not offer DaaS. Medical records migration and deployment services.	Integration of record sharing innovations into CareFlow. Access to information from the healthcare community. Optimized workflow for admissions and discharges.
Nervecentre	Architecture designed for interoperability. Access to patient information in real time. Mobile approach and usability to update data from the point of care.	Customized solutions that address the entire patient flow, integrating mobile devices and offering real-time data.	Does not offer DaaS. It focuses on ìData-Driven Hospitalsî and facilitating access to data for doctors.	Access to patient information in real time, allowing for recording and updating data at the point of care. Intelligent algorithms for sepsis identification. Emphasis on traceability for decision making.
Solutions	**Interoperability (FHIR, HL7, OpenEHR)**	**Personalisation**	**DaaS**	**Traceability**
TPP	Wide range of interfaces with medical devices, mobile applications, clinical software, and infrastructure such as NHS SPINE. Complies with HL7 and FHIR standards.	Clinical Development Kit (CDK) that allowsthe creation and modification of clinical records. Customizable dashboards, questionnaires, and templates.	It does not explicitly offer DaaS. Facilitates access to anonymized datafor research through researchservices. Collaborate on projects such as OpenSAFELY and Born in Bradford.	Establishes traceability with a shared electronic medical history system that consolidates interactions with health services. Mobile access for patients.

Funded by the European Union

Phreesia	Wide range of integrations with EMR, LIS, CRM and medical devices.	Highly customizable: survey content, questions, workflows, interface design and permission settings. Creationand integration ofcustom applications.	Scalable and secure DaaS platform with analysis and reporting tools.	Complete traceability of patient data: interactions, changes, and access.
Salesforce	Wide range of integrations with EMR, CRM, medical device managementsystems, and other Salesforce applications.	Highly customizable: survey content, questions, workflows, interface design, permission settings, and custom app creation and integration.	Scalable and secure DaaS platform with analysis and reporting tools.	Complete traceability of patient data: interactions, changes, access,and security.
Jane Software	Limited interoperability withother healthcare systems.	Limited customization: survey content, questions, and workflows. It does not allow the creation of custom applications.	Does not offerDaaS.	Limited traceability of patient interactions.
Solutions	**Interoperability (FHIR, HL7, OpenEHR)**	**Personalisation**	**DaaS**	**Traceability**
Universal Software Solutions	Limited interoperability withsome third-party systems, such as imaging solutions.	Moderate customization:survey content,questions, and workflows. Advanced customization may require additional development.	Does not offer DaaS. Third party cloud storage can be integrated.	Moderate traceability of patient data: interaction and changes. Limited auditing capabilities.

Funded by the European Union

8.2.23.1.4 BUSINESS MODEL DESCRIPTION

Based on the exploitation strategy, the following business model is outlined at this business canvas model.

TABLE 90: BUSINESS MODEL CANVAS OF DGUARD

KEY ACTIVITIES	CUSTOMER RELATIONSHIP
• **RESEARCH AND DEVELOPMENT.** To adapt to advances in the field. • **PRODUCT MAINTENANCE AND IMPROVEMENTS.** Improvement of functionalities to increase usability and alignment with industry standards and maintenance to ensure service level agreements. • **CUSTOMER SUCCESS.** Provide high-quality customer service to gather as much information as possible on improvements. **MARKETING.** Promoting DGUARDand maintaining the awareness ofthe brand through advertising, public relations, and relevant content. • **SALES & PARTNERSHIPS.** Execute a clear sales funnel and build strategic partnerships and alliances with System Integrators and Software vendors for long term success.	Depending on the phase to position DGUARD will deal with costumers as: **DIRECT SALES.** DGUARD will provide self-service support through its documentation and resources once it reaches phase 3, enabling partners to integrate seamlessly. Until then, the relationship will be closely managed to gather information on necessary upgrades. DGUARD will handle personalized onboarding processes toexpedite product launches and ensure market fit. Once phase 3 is reached, all direct sales efforts will be redirected to their partner ecosystem. DGUARD will prioritize automation wherever feasible, offering helpful resources, training sessions, and architectural drafts to minimize internal costs. • **SYSTEM INTEGRATORS.** DGUARD will have a partner program where to offer special incentives or discounts, exclusive resources and training, dedicated support, and partner recognitions through integrator certification. (Phase 3) • **SOFTWARE VENDORS.** DGUARD will

Funded by the European Union

	offer an account manager that will help in terms of billing, invoicing, technical support, product updates and co-marketing campaigns for integrated platforms. (Phase 3)
KEY RESOURCES	**CHANNELS**
• TECHNOLOGICAL RESOURCES AND LICENSES: DGUARD possesses the knowledge on the developed software, and technological tools within its ecosystem, all of which will be open-sourced. Its participants haveas well several private componentswhich DGUARD integrates with that will act as its main revenue streams. • CONTRACTS with System Integrators and Software Vendors: DGUARD will maintain ownership of contracts with its network of partners and collaborators, facilitating marketexpansion and revenue growth. • BRAND REPUTATION: DGUARD will retain ownership of its trademark and the intangible assets accumulated over time through branding, marketing, andpublic relations efforts. INITIAL SUCCESS STORIES. DGUARD will have the first set of success stories enabling it to position as market leader and differentiating it from competitorsand newcomers.	• SYSTEM INTEGRATORS. Organizations that specialize in bringing together various hardware, software, and IT services to create a system that meets specific customer needs. This might involve partnershipagreements and training and sales support. • INTEGRATIONS WITH SOFTWARE VENDORS. Companies that develop, market, and sell software products or applications to end-users or other organizations. The agreements mightinvolve partnership, bundled sales, co-marketing initiatives or reseller programs. DIRECT SALES. Selling product directly to the end user. This might force DGUARD to develop or integratewith platforms with in-house team during phase 1-2. It is only desirable for piloting phase.
COSTS	**REVENUE STREAMS**
SALARIES. DGUARD will rely on its unique team to differentiate from competitors and to fulfil	Depending on the phase to position DGUARD will deal focus its revenue stream on:

Funded by the European Union

enhancements until phase 3. **MARKETING EXPENSES.** DGUARD will invest on advertising, promotion, and other marketing activities to attract customers and create brand awareness. **PROFESSIONAL SERVICES.** Fees paid to external experts, such as lawyers and compliance consultants, for specialized services and guidance in legal and regulatory matters. **R&D COSTS.** Expenditure on activities aimed at innovation, product development, and improving existing offerings. **SERVERS & INFRASTRUCTURES.** Investment in infrastructure, includingservers and related technology.	- (P1, P2) - **CONSULTANCY AND DEVELOPMENT FEES.** This is not the focus of DGUARD but is required to achieve first successful success stories, big corporations and refine the technology. - **(P3) - LICENSES.** DGUARD will generate revenue from charging customers on a monthly or yearly recurring basis for the services offered based on the number of used resources on the SaaS platform.

In overview, DGUARD's cost structure is primarily influenced by several key factors:

Personnel and Expert Professional Services: Investment in skilled personnel and external professional services will be significant. This includes hiring specialized talent to drive innovation, development, and implementation of thesolution, as well as engaging legal and compliance experts for regulatory guidance.

Marketing and Sales: Another substantial area of expenditure will be marketing and sales activities. DGUARD will allocate resources to promote itssolution, raise brand awareness, and acquire customers. This encompasses various marketing channels, advertising campaigns, and sales efforts topenetrate the market effectively.

Operational Expenses: Operational costs, particularly infrastructure expenses related to hosting and maintaining the SaaS platform, will also contribute to overall expenditures. This involves investing in server infrastructure, data storage, network resources, and other technology components essential for thesmooth functioning and scalability of the platform.

On the revenue side, dGUARD anticipates multiple streams of income depending on the phase:

Phases 1-2: During these initial phases, revenue will stem from grants and consultancy fees. DGUARD will engage in consultancy and tailored projects forvarious clients to

Funded by the European Union

customize the solution according to industry standards and specific requirements. These projects aim to demonstrate the solution's effectiveness, establish success stories, and build momentum within the targetmarket.

Phase 3: Subscription fees will become the primary revenue stream as DGUARD transitions to a subscription-based model. Customers will pay recurring fees to access and utilize the platform's services on an ongoing basis.This subscription model ensures a steady and predictable revenue stream for DGUARD, facilitating sustainable growth and long-term viability.

8.2.24UtiP-DAM

The core business model of Correlation Systems (CS) is based on selling sensors and systems (backends) for crowd analytics.

Utip-DAM is supporting the following business models:

1. The customer purchases a full system which include sensors and backend (physical server with software), and install the system in his own permissions - this module is typically used by government agencies
2. Similar to the first option - however, the backend is installed on a cloud service provided by the customer
3. The customer is purchasing the sensor and subscribes to a cloud service provided and managed by Correlation Systems. In this case, the client may have his own server or he may share the server with other customers (SaaS module)
4. Limited time rental - a customer is renting the system for a specific time period and by the end of the time period he returns the system. This module is typically used in cooperation with their distributors in order to provide service for a specific event.

It is planned to offer UtiP-DAM as a complementary service (free of charge) for all the aforementioned customers. This will allow them to provide the customers with raw data which is currently not available for systems that are maintained and operated by Correlation Systems due to the privacy risk.

This will also allow customers to share the data with third parties via UtiP-DAM (typically companies during data analytics and big data systems for the municipality) without limiting the use of the data.

In addition, their free anonymised data sharing service will help them discover potential partners worldwide, as typically organisations that have a mobility dataset are potential end users and distributors for their system.

Funded by the European Union

8.2.24.1 Market Analysis (Stakeholders, Partners, Competitors, Opportunities & Obstacles)

8.2.24.1.1 Stakeholders

UtiP-DAM involves a variety of stakeholders, each with a unique interest in crowd data collection and user privacy. Among these stakeholders are individuals, (also referred to as “humans”, “citizens”), who prioritise data protection and privacy.

For example, Sarah, a concerned individual, wants to ensure her location data is not misused by third parties.

> UtiP-DAM addresses these concerns by offering robust privacy protection measures that safeguard personal data against unauthorised access and exploitation.

Organizations also form a significant segment of UtiP-DAM's stakeholders. This group includes Correlation Systems’ customers, third-party dataset owners, data privacy officers, and developers. Third-party dataset owners require secure data handling solutions to prevent unauthorised data access and misuse. Data privacy officers are professionals dedicated to ensuring their organisations adhere to data privacy regulations and best practices, while developers focus on integrating privacy protection mechanisms into software and applications.

Researchers are also important stakeholders. They are deeply interested in advanced anonymization techniques that balance data privacy with utility.

The actors within the UtiP-DAM ecosystem include the interdisciplinary UtiP-DAM team, led by Erel Rosenberg, responsible for developing state-of-the-art privacy tools and conducting user case analyses. The team's expertise and commitment drive the project’s success in delivering high-quality privacy solutions. University students in North Tel Aviv also play a vital role by actively participating in demonstrations and providing valuable insights into privacy concerns and data threats. Their involvement ensures that UtiP-DAM's solutions are user-centric and address real-world issues. Additionally, public organisations like municipalities, that currently use mobility data solutions from Correlation Systems, collaborate with UtiP-DAM in use-case analyses, helping to validate UtiP-DAM's solutions and demonstrate their practical applicability.

8.2.24.1.2 Partners

UtiP-DAM's partners include universities and research institutions, privacy experts, and technology providers, such as the Mobility Data Space. These collaborations enable the UtiP-DAM tools to be developed in closer fit with market expectations, as well as maximise the project’s impact.

8.2.24.1.2.1 Research Institution

Correlation Systems has a very close relationship with Brno University of Technology in the Czech Republic and members of the faculty dedicated to research on privacy enabling technologies.

Funded by the European Union

This collaboration enables discussion with their researchers on anonymity methods and validation of the project outcomes by these stakeholders.

8.2.24.1.2.2 Privacy Expert

Correlation Systems has engaged with Karel Neuwirt for an expert opinion on K-anonymity, in the context of legal compliance and more generally, on privacy protection.

Who is Karel Neuwirt?

Dr. Karel Neuwirt is the former Data Protection Commissioner of the Czech Republic. For many years he has devoted himself to the protection of personal data in the environment of new information technologies.

In 2002 he was appointed the Vice-President of the Project Group on Data Protection (CJ-PD), the highest Council of Europe´s body for personal data protection and later he was elected for the Council of Europe Data Protection Commissioner (2007). Since 2006 he worked as the team leader of the EU CARDS project on personal data protection in North Macedonia. Currently, he works as an independent consultant for personal data protection providing training and analysis of compliance with the EU data protection legislation (GDPR) for both public and private institutions.

8.2.24.1.2.3 Technology Provider

UtiP-DAM partners with the Mobility Dataspace for the sharing of anonymized mobility data. The CS team also participates in events organised by the Mobility Data Space (as detailed previously - see part 5) to maximise opportunities generated by this partnership.

8.2.24.2 Competition

The competitive landscape for UtiP-DAM includes companies like Privacy Analytics, HERE Technologies and the EU-funded ANYMOS project. However, unlike UtiP-DAM, none of these offer a tool designed for individuals willing to check the anonymity of their mobility data.

Indeed, Privacy Analytics offers data anonymization services primarily for the healthcare and research sectors and it uses a risk-based approach to anonymize data, removing personal information while preserving business value. This method builds trust, prevents privacy violations, and maintains data utility, enabling organizations to innovate and grow confidently.

Unlike simple data masking, Privacy Analytics' approach considers the data's context, ensuring it remains useful for innovation and revenue generation. Their methodology, recognized globally since 2007, aligns with international standards.

Privacy Analytics evaluates data identifiability based on its intended use, users, and access environments to determine necessary measures for maintaining privacy and

Funded by the European Union

utility. Proprietary algorithms and proven processes de-identify data to appropriate thresholds, ensuring compliance and protection.

On the other hand, HERE Technologies has introduced an enterprise-grade anonymization tool available for self-hosted, cloud, and hybrid environments. This tool processes real-time and historical location data, ensuring data privacy while preserving business value. It enables businesses to maintain control over personal location data and comply with privacy regulations such as GDPR, CPRA, and APPI.

The HERE Anonymizer allows flexible deployment, functioning with or without an internet connection, and can be used on-premises, in hybrid setups, or in public clouds like AWS, Azure, or Google. This capability is crucial for sectors handling sensitive location data, such as retail, telecommunications, automotive, and logistics.

Privacy is defined as a core focus by HERE Technologies, which holds multiple certifications, including HITRUST Risk-based, 2-year (r2) Certified status, ISO/IEC 27701:2019, ISO 27017, and ISO 27018. Their anonymization tool is part of a comprehensive suite of location services, supporting customers across various industries worldwide.

Lastly, the NextGenerationEU project named ANYMOS also represents a serious competitor for UtiP-DAM. Indeed, The ANYMOS cluster focuses on integrating anonymization techniques into data-driven future mobility solutions while maintaining data usability. This initiative addresses the challenge of using personal data, which is essential for mobility solutions but subject to strict data protection regulations.

ANYMOS aims to establish anonymization as a key technology to mitigate uncertainties about complying with data protection laws when sharing and using data. The project seeks to reinforce Germany's leadership in automotive and public transport innovation. To achieve this, ANYMOS is developing a process model to help companies identify anonymization needs and options for mobility use cases, select appropriate methods, apply them correctly, and systematically evaluate re-identification risks.

The ANYMOS project, which began on November 15, 2022, and will run until November 14, 2025, aspires to reduce the uncertainties surrounding data protection compliance without compromising the data's utility for specific applications.

Funded by the European Union

8.2.24.3 Business Model

TABLE 91: UTIP-DAM BUSINESS MODEL CANVAS

<table>
<tr>
<td rowspan="2">Key Partners

NGI Trustchain

Private companies including Correlation Systems' current customers, notably in Thailand

Mobility Data Space, a Gaia-X lighthouse project

Karel Neuwirt, data privacy expert</td>
<td>Key Activities

- Ensure data privacy with K-anonymization and auditing tools.

- Maintain the UtiP-DAM marketplace for data discovery and download.

- Provide an API for developers to integrate platform functionalities.

- Deploy the anonymization algorithm for data privacy at the source.

- Ensure adherence to data privacy regulations.</td>
<td rowspan="2">Value Proposition

UtiP-DAM empowers various users by providing a secure platform for mobility data.

Here's a value proposition summary:

-Ensure data privacy with auditing and anonymization. Monetize data by publishing anonymized datasets on the marketplace.

-Find valuable insights through anonymized datasets. Download data for further analysis and make data-driven decisions.

-Integrate anonymization into applications and automate data processes using the API.

-Control your data by verifying if it's included in shared datasets.

-Enhance data security with the decentralized Edge network. Streamline data management and potentially generate new revenue streams.</td>
<td>Customer Relationships

Automated Service</td>
<td rowspan="2">Customer Segments

Data providers:
-Our current customers who use our sensor technology to collect mobility data.
-Third-party organizations that own mobility datasets.
-Citizens (who can inquire if their data is included).

Data users:
-DPOs who ensure data privacy compliance.
-Data Consumers (researchers, businesses...) who use anonymized data from the UtiP-DAM marketplace or International Data Space.

Developers: These are individuals or organizations used to leverage the platform's functionalities in their own projects.</td>
</tr>
<tr>
<td>Key Resources

Human Resources: A team of experts in data privacy, anonymization, and blockchain technology is crucial for the development and operation of UtiP-DAM.

Technical Resources: The core technical resources include the UtiP-DAM platform itself, including the anonymization algorithms, the UtiP-DAM marketplace</td>
<td>Channels

Direct Sales: The UtiP-DAM team can directly approach potential customers like Correlation Systems' existing customers and other data providers to showcase the platform's benefits.

Marketplace: The UtiP-DAM marketplace serves as a key channel for both data providers and data users. Data providers can publish</td>
</tr>
</table>

Funded by the European Union

	infrastructure, and the APIs for developer integration. Additionally, collaboration with partners like NGI Trustchain, Pontus-X, and Mobility Data Space provides access to valuable technical resources and expertise.		anonymized datasets, while data users can discover and download these datasets for further analysis. **Partnerships**: Collaboration with existing industry partners like NGI Trustchain, Pontus-X, and Mobility Data Space can leverage their existing channels and networks to reach a wider audience of potential data providers and users.	

Cost Structure	**Revenue Streams**
There are two main costs: • Development cost: The estimated range is €165,000 to €200,000, with €115,000 covered by the project, leaving a net cost of €50,000 to €85,000. • Operational cost: The primary expense is an AWS t3.large server, costing around €100 per month (including storage and data transfer). Over the estimated 3-year project lifetime, this translates to a total OpEx of €3,600. In total, the system cost over 3 years is estimated to be between €53,600 and €88,600.	Approximately three small size projects (33K Euro on average) or one medium size project (100K Euro) will bring the project to a breakeven point.

8.2.24.4 Positive role of decentralised technologies

While UtiP-DAM does not directly incorporate blockchain or self-sovereign identity (SSI) technologies, the project is part of a broader decentralised ecosystem that can leverage its outcomes.

The project's emphasis on privacy, transparency in data collection and open data sharing aligns strongly with the vision of human-centric decentralised technologies. For instance, the integrated auditing tool, empowers individuals to verify if their location data is included in mobility datasets. This approach not only enhances individual rights but also builds trust in the overall data ecosystem.

Moreover, UtiP-DAM's EDGE-based decentralised anonymization method is compatible with blockchain-based solutions for data exchange and data provenance tracking. This alignment creates an opportunity to explore the integration of blockchain technology into the UtiP-DAM architecture. While beyond the scope of this

Funded by the European Union

project, a potential future extension could involve transforming edge devices into blockchain nodes, thereby creating a decentralised network for recording and verifying mobility patterns, where each EDGE device could add to the ledger information on the anonymized mobility patterns it generates.

Finally, through collaboration with the Mobility Data Space, UtiP-DAM is actively contributing to the development of a decentralised data economy.

8.2.24.5 Value Network

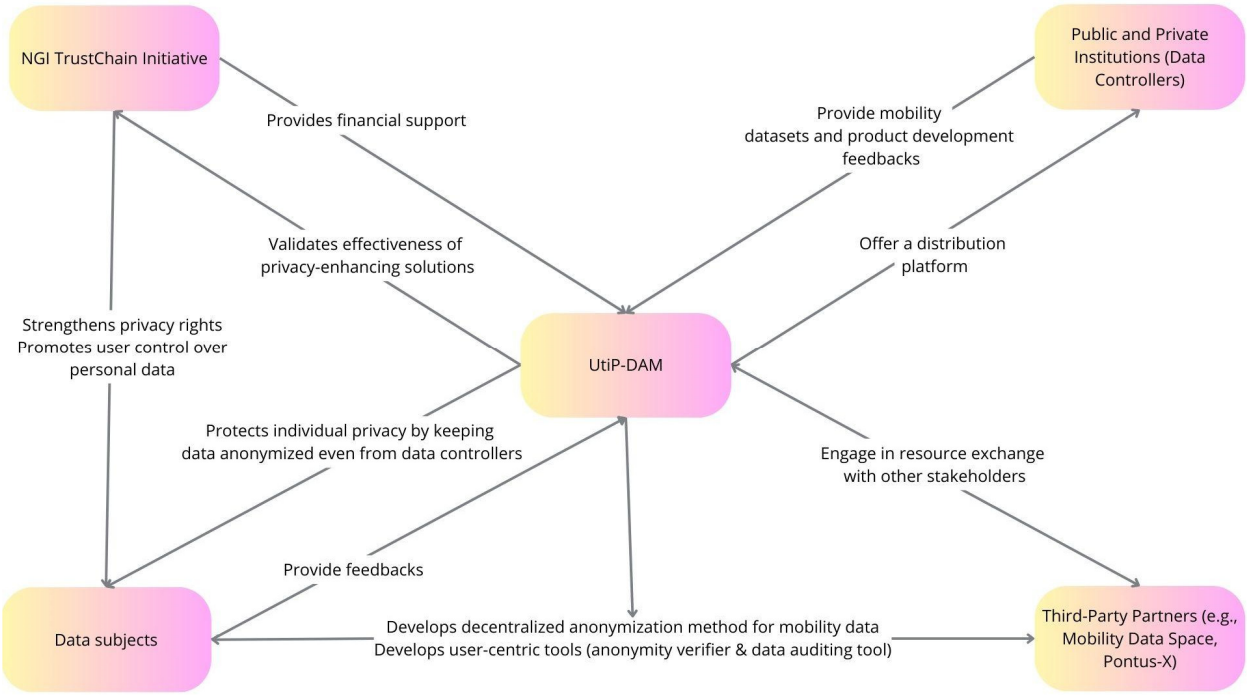


Figure 9 - UtiP DAM's value network

8.2.24.6 Economic Analysis

8.2.24.6.1 Cost Analysis

The cost of the system includes two key elements: development cost (CapEx) and operational costs (OpEx)

- CapEX: The initial development costs are estimated between 165,000 to 200,000 Euro from which 115,000 Euro will be covered by the project.
- OpEX: Their operational costs are mainly one AWS t3.large server which cost around 100 Euro per month (including storage and data transfer)

Funded by the European Union

Parameters:

- Product lifetime: It is estimated that the project (ngi.cs.co.il) will operate for three years (from the end of the development) as technology for data de-anonymization and data collection are changing very fast.
- Interest rate: a 10% is being used as the effective interest rate that the company needs to pay in case an external loan will be required.

8.2.24.6.2 Revenue stream

Approximately three small size projects (33K Euro on average) or one medium size project (100K Euro) will bring the project to a breakeven point.

8.2.24.7 Return of investment

Following the presentation of the project to their partners in Thailand it estimated that only in Thailand Utip-DAM will be able to get 3-5 medium size projects based on data sharing module within 1-3 years

It is expected to return the investment in the project in one year and to get around 200% return of investment during the 2nd year.

Funded by the European Union

8.2.24.8 SWOT Analysis

TABLE 92: UTIP-DAM SWOT ANALYSIS

Strengths	Weaknesses
Unique value proposition: UtiP-DAM fills a gap in the market with a multi-users, multi-faceted platform designed to answer the needs of various stakeholders in the anonymization, auditing and sharing of mobility datasets. **Open-source K-anonymity:** Distributed in open-source, the UtiP-DAM tools enable researchers and developers to generate anonymized mobility datasets that ensure the right to privacy of their data subjects. **Modular architecture:** Enables scalability, flexibility, and easier integration with external applications. **User-centricity:** User-centric development (with continuous user engagement through surveys and interviews) ensures that the platform answers user requirements. **Future-oriented design:** The distributed anonymity design through an IoT edge network is a novel architecture, which could inspire other IoT companies to anonymize their data in a decentralised manner.	**New entrant**: UtiP-DAM needs to establish itself and gain traction within a competitive data management landscape. **Reliance on data providers**: The platform success depends on our capacity to attract data owners to populate the marketplace with their datasets. **Limited awareness of privacy issues**: While most companies and researchers in the EU especially realise the importance of legal compliance, they may be satisfied with the strict minimum (e.g: storing poorly anonymized private data on secured servers) without understanding that true compliance consists in not collecting nor storing (even securely) identifying data. **Technical complexity**: Balancing data privacy, utility, and scalability is a technical challenge that some companies may not want to tackle.
Opportunities	**Threats**
Growing demand for mobility data: Increasing demand for anonymized mobility data across various sectors like transportation, urban planning, and location-based services creates a significant market opportunity for UtiP-DAM. **Evolving legal landscape:** Laws, in the EU and beyond, tend to emphasise greater privacy guarantees, which will make the UtiP-DAM tools increasingly attractive to companies that collect personal data. **Potential for new features:** The platform can be extended to incorporate new features like data analysis tools or visualisation dashboards, based on platform adoption and user feedback. **Partnerships:** During D2, CS has signed a collaboration agreement with the Mobility Data Space, a Gaia-X lighthouse project, which will enable UtiP-DAM users to push their datasets on the Mobility Data Space, providing greater visibility and UtiP-DAM and datasets anonymized via UtiP-DAM.	**Stringent data privacy regulations**: Despite guaranteeing a good level of anonymity K-based anonymization of mobility dataset is contingent on (i) the end-user actually choosing a high enough K (e.g: K =2 is not sufficient to safeguard anonymity) and (ii) other publicly available datasets which may be distributed post-anonymization. Hence, there is still a risk that datasets anonymized via UtiP-DAM will not meet data privacy laws. **Competition:** Existing data management platforms (e.g: International Data Space and Gaia-X projects) or new entrants focusing on mobility data will inevitably become a competitive threat.

Funded by the European Union

8.2.25 SURE

8.2.25.1 Market analysis

The synthetic data and privacy-preserving technologies market is rapidly growing, driven by increasing regulatory demands and the need for secure data sharing. AI, which is largely data-driven, will bring about enormous economic benefits to societies and will be largely powered by synthetic data by 2030. The Total Addressable Market (TAM) of the synthetic data market is expected to converge with the big data and analytics market with various segmentations in terms of data types. It can be considered a gateway to a structured data market of about 195 B dollars by 2030, which can be unlocked with responsible data sharing of synthetic data with high privacy and utility attributes.

The competitive landscape features several established and emerging companies. Clearbox AI, based in Italy, specializes in high-quality synthetic data generation for privacy preservation. The project's team has listed a competitor analysis in Table 9. These competitors highlight the diverse approaches and applications of synthetic data technologies in the market. Clearbox AI's unique combination of privacy, utility, open-source accessibility, and regulatory compliance sets it apart in the synthetic data market. By providing robust, privacy-preserving synthetic data solutions that maintain data utility and adhere to regulatory standards, Clearbox AI supports secure data sharing and innovation across various sectors. This comprehensive approach ensures that Clearbox AI's solutsolutions are not only technically advanced but also trusted and widely adopted.

TABLE 93: COMPETITORS ANALYSIS

Company, country	About	Data type	Use case and industries	Product /Pricing	Opensource modules
Clearbox AI clearbox.ai Italy,synthetic data since	High quality synthetic data generator for data quality augmentation, privacy preservation and bias mitigation.	csv, time series, relational databases	Data sandbox, data sharing Finance, energy, telco, healthcare	On-prem, private cloud solution. + On-demand generation	Yes
2021					
Israel, 2018	An end-to-end, self-service synthetic data platform that generates visual data. Data as Code.	Images, 3D data	AR/VR, Security, Automotive, Robotics, Manufacturing	SaaS/ price on request	N/A

Funded by the European Union

USA, 2019	Developer Stack for Synthetic Data for privacy preservation.	csv	Privacy preservation, industry agnostic	SDK, monthly fee or custom license	Yes
Austria/USA, 2017	Synthetic data generator for building AI and software applications	csv, text	AI training, software testing, NLP, banking, insurance, telco	SaaS/price on request	Yes
Italy, 2018	Synthetic data platform for analytical applications	csv	Data value chain, Finance, Healthcare, retail, govtech	Saas and on premises	No

Despite the promising opportunities, such as regulatory compliance, innovation in financial services, and healthcare advancements, there are obstacles to market entry. Low awareness and market readiness for synthetic data solutions, as well as the need for specialized technical knowledge, pose significant challenges. Addressing these obstacles through targeted education and strategic partnerships will be crucial for successful market penetration. The project has detailed tech business model framework and strategy in the following section.

8.2.25.2Business model of SURE proposal

The proposal has significant business potential, considering the increasing demand for secure, GDPR-compliant data solutions in multiple sectors, including finance and healthcare. The open-source nature of the synthetic data library facilitates wide adoption, establishes them as thought leaders, and creates a user base that can evolve into a customer base for premium features.

In the business canvas template illustrated in Figure 6:

While the core library will be open-source, the revenue model will include Consultation Services, Premium Features, Custom Solutions and Training: Workshops and courses to upskill employees in the proper usage and customization of the library.

In the business, the team of the project envisions two different customer segments: Tech and data science divisions of small and medium companies that are accustomed to working with cloud-based solutions/SaaS and larger companies that require private cloud or enterprise solutions on-premises, and large companies that require completely data sovereign product requirements with on-prem installation.

For segment 1, users are offered a free plan with a limited number of operations and computing credits. Users can choose to pay a premium to unlock premium features and extra computational power. For segment 2, Companies can request an on-prem

Funded by the European Union

installation, and the process is coordinated by a dedicated account manager for such clients with additional services, including training and onboarding.

The next steps for economic sustainability include user community building, strategic product partnerships with companies in target sectors as well as continuous product updates to provide value to the premium users.

In terms of sustainability, since synthetic data can be generated on demand, the need to store massive datasets is significantly reduced, thereby reducing energy consumption and costs. Privacy-preserving mechanisms of synthetic data can improve remote working possibilities due to easier data access. It also promotes responsible data collection and use and reduces the carbon footprint of data collection and storage facilities.

A detailed business model is as follows.

The project describe the business mode of SURE using the business model canvas template shown in Figure 6.

The stakeholders and value network of SURE shown in Figure 6 encompasses various stakeholders, including technology providers, financial and healthcare institutions, regulatory bodies, and end-users. Technology providers supply the necessary infrastructure and tools for data generation and processing. Financial and healthcare institutions utilize synthetic data for compliance and innovation, while regulatory bodies ensure adherence to data protection standards. End-users, including data scientists and DPOs, benefit from the privacy-preserving capabilities of the SURE library.

Interactions among these stakeholders facilitate the flow of revenue and information, ensuring each brings value to the ecosystem. For instance, technology providers enable data generation and processing, financial and healthcare institutions leverage synthetic data for compliant data sharing and innovation, regulatory bodies ensure legal compliance, and end-users drive continuous improvement through feedback and utilization. This network fosters enhanced data privacy and compliance, secure data sharing, and trust in blockchain technologies.

Funded by the European Union

TABLE 94: PRELIMINARY BUSINESS MODEL CANVAS OF SURE

Business Model Canvas

Designed for:	Designed by:	Date:	Version:
SURE D2	Shalini Kurapati	06/05/2024	v1

Key Partners
- Technology divisions of banks and financial companies
- IT system integrators
- Privacy professionals
- Data Scientists and Innovation specialists

Key Activities
- Development and maintenance of the SURE library
- Engagement with the data science and privacy regulation communities
- Acquisition of clients for the continuous use of the SURE library and related services

Key Resources
- Human resources, especially skilled data scientists and privacy experts.
- Financial resources for ongoing development and market expansion.

Value Propositions
- Enhances regulatory compliance with data privacy standards like GDPR.
- Facilitates safe data sharing and innovative uses of data

Customer Relationships
- Direct contact and support
- Channel partnerships with IT system integrators
- Community engagement and activities

Channels
- GitHub for easy access and integration.
- Digital marketing for the online platform
- IT system integration partnerships

Customer Segments
- Data science divisions of large companies such as banks and fintech companies
- Risk and compliance divisions of large companies
- IT system integrators

Cost Structure
- HR costs for data scientists and software engineers for development and maintenance, and customisation of the library.
- Marketing, sales, and customer acquisition costs.
- Infrastructure and hardware for in-house data generation
- Office and support staff costs

Revenue Streams
- Subscription fees to access SURE library together with premium data generation libraries (Clearbox AI product)
- Consulting services for customisation and advanced integration.
- Training sessions for companies.

.

While the entire SURE library is open source, designed to promote accessibility and foster community collaboration, it has been built upon a foundation of previously developed algorithms, expert staff, and substantial financial investments, the approach enhances the library's capabilities while maintaining a robust framework. This strategic integration of proprietary resources with the open-source commitment ensures the delivery of a high-value, versatile tool that supports a broad range of applications. This combined approach offers both accessibility, transparency and provides commercial pathways to future users and clients. These value propositions are communicated to clients either directly, or through digital activities, as well as channel partnerships with other system integrators. Distribution channels include direct downloads via GitHub, supplemented by workshops, webinars, and a strong online presence to engage users. The cost structure of SURE is dominated by investments in research and development, marketing to attract and retain users, and operational costs associated with customer support and staff salaries. Revenue streams are diversified across subscription fees for premium features, consulting services for custom solutions, and training programs that educate users on the effective use of the library.

For any business model, it is important to highlight its main internal strengths and weaknesses along with the external opportunities and threats it faces in the dynamic

Funded by the European Union

market environment. Therefore, the team of the project has created a SWOT analysis for the SURE library business model in Table 12.

TABLE 95: SWOT ANALYSIS FOR SURE

Strengths	**Weaknesses**
1) Advanced and highly scalable solution for data privacy and utility 2) Expertise in data science and privacy. 3) Strong industry and academic partnerships.	- Reliance on specialised technical expertise. - Low awareness, and market readiness on the topic may deter broader adoption.
Opportunities	**Threats**
• Increased demand due to stricter regulations like AI act • Expansion into healthcare and public administration	1) Rapid technological changes require constant updates 2) Competitors undercut costs

The SURE project will capitalise on its strengths in scalability and data privacy expertise by expanding its team's skills and enhancing market awareness through targeted educational initiatives. Leveraging opportunities from stricter data regulations, SURE aims to penetrate healthcare and public administration sectors with compliant solutions. The project is also staying agile to navigate rapid technological changes and competitive pressures, focusing on demonstrating superior value over lower-cost alternatives.

8.2.25.3Preliminary Economic Analysis

A preliminary cost-benefit analysis of SURE's synthetic data offerings indicates significant economic advantages. By generating synthetic data on demand, organizations can minimize the need for extensive data storage, which directly translates to reduced storage costs and lower energy consumption. For example, synthetic data reduces storage requirements by up to 50%, lowering operational costs and decreasing energy consumption associated with maintaining large datasets. This

Funded by the European Union

method not only enhances cost efficiency but also supports environmental sustainability by reducing the carbon footprint of data storage facilities (MIT).

Furthermore, the privacy-preserving mechanisms embedded in synthetic data facilitate remote work by enabling secure and easy data access without compromising privacy. This capability reduces the need for physical data storage and enhances operational flexibility, allowing organizations to comply with stringent data privacy regulations while maintaining productivity. By promoting responsible data collection and usage practices, synthetic data significantly boosts economic sustainability.

8.2.25.4 Exploitation plan and updates

The SURE library's business model can be enhanced by leveraging its users as ambassadors, promoting the library within their networks. Revenue will be generated through subscription models and consulting services, particularly in highly regulated sectors such as healthcare and finance. Additionally, SURE is actively engaging in contracts, such as the one with a technology provider, to evaluate AI-ready datasets, which represents a significant revenue stream.

8.2.25.5Early costumers

Early adopters of the SURE library could be organizations involved in AI and data privacy, particularly those in healthcare and finance, where data security and compliance are critical. These customers will benefit from the SURE library's capabilities in ensuring data privacy while maintaining data utility.

8.2.25.6Technology Readiness Level (TRL)

Technology Readiness Level (TRL):

The SURE system is currently at a TRL of 6-7, indicating it has been demonstrated in a relevant environment but is not yet fully operational. Future development aims to advance SURE to TRL 8-9, where it will be fully tested and deployed in real-world settings

8.2.25.7Opportunities and future work

In addition to these revenue strategies, there is potential to integrate blockchain technology to create a transparent and verifiable ledger for datasets, enhancing trust in the use of synthetic data. This integration remains a future work opportunity, potentially to be developed by other teams within the TrustChain ecosystem.

Integrating decentralized digital identity and blockchain technologies potentially enhances the value of SURE's offerings by ensuring secure, private, and transparent handling of data. Decentralized digital identity management enables individuals to control their personal information, reducing risks of identity theft and fraud, which is

Funded by the European Union

crucial for maintaining high data privacy standards (MIT Computational Law Report).. Furthermore, decentralized identity systems can uniquely identify and authenticate users while enabling attributes to be assigned to an identity for additional descriptions, ensuring data accuracy and reducing redundant data storage across multiple platforms (MIT Computational Law Report). These integrated technologies could allow SURE to offer robust, secure, and compliant data-sharing solutions, fostering trust and promoting innovation across various sectors. Although these integrations are beyond the scope of the current project, they lay the foundations for future impactful projects.

8.2.26 PECS

8.2.26.1 Market analysis and innovation potential

The possible competitors of PECS, to the team's knowledge, are PRICON, by academia, and Privacy4Cars, by industry.

PRICON. It consists of two main components: a user interface that uses a privacy calculation model to predict privacy-related adoptions based on privacy-related costs and usage-related benefits is being developed. The first step in this process is the analysis of a connected car usage scenario, which leads to the formulation of an information architecture that considers the user choices and expectations. The user is guided in choosing privacy settings via the UI. The user may choose from four pre-defined privacy profiles and manage what information is shared across various services. Every service is subject to the profiles. Custom settings are an option for the user, though.

While there are some features that both solutions have in common, such as preset privacy levels, the ability to customise preferences for each application, and the ability to choose which personal information to share, PECS goes above and beyond by protecting those data with PETs and identifying in real-time if some applications are violating user policies.

The ability of the solution to confirm whether an application is attempting to transmit data that the user has specifically forbidden is an intriguing feature and it is available for all applications, not just those that are fully-compatible with PECS. In this situation, PECS notifies the user via their preferred method, which was previously configured during the initial PECS onboarding. The user may make their choice through a variety of notification options, such as haptic input on their steering wheel, visual indicators, or auditory cues. It appears that PRICON is not carrying out these checks, therefore it is unable to notify the user when a violation occurs.

Moreover, the way PECS approaches the problem of obfuscating data produced inside of cars underscores its dramatic innovation potential. A specific type of information such as location-based data has drawn a lot of attention recently since it is necessary for many services to function properly. However, location can be considered very

Funded by the European Union

relevant personal data. PECS attempts to ensure the privacy preservation of any data that flows to apps and to the cloud through the use of the PECSo module and the compliance tier system.

Privacy4Cars. Customers may view privacy information about a car through the vehicle identification number (VIN), including the Personal Information (PII) that the manufacturer collects, distributes, and sells. This information includes identifiers, biometric data, geolocation, data from synced phones, and user profiles. Every Vehicle Privacy Report consists of two parts: the Vehicle Privacy Label, a set of ten clickable icons that summarises the data collection, sharing, and selling practises of vehicle manufacturers, and the Vehicle Privacy History, a list of acknowledged actions companies have been taken to protect the privacy of 14 of their clients. Furthermore, it identifies and references the available information from the manufacturer as well as the time and level of education needed for the typical customer to independently go through all pertinent terms and privacy policies. By including the Report tool into their sales websites, car dealers may appropriately reveal the data practices of auto corporations for each specific vehicle on their lot. The information and badges specific to individual VINs will be immediately updated on the Vehicle Detail Pages of those "Privacy Care" dealerships' websites.

It is clear that PECS exceeds Pivacy4Cars not only in terms of the sheer functionalities that each provides. Most importantly, PECS establishes a fully user-centric approach to empower the user with full control over their own choices over the processing of their personal data, both in terms of soft and of hard privacy measures. It follows that the outcomes of PECS bear huge innovation potential, promoting an entirely new automotive data ecosystem whose main currency lies in the hands of the legitimate owner: personal data is fully controlled by the physical person it belongs to.

8.2.26.2Business model

This section showcases the business model Canvas.

- **Key Partners**: MASA for integration and validation, Regulatory bodies for compliance, Industry experts for insights and best practices, Italian car brands such as Maserati, MASA end-users as well as end-users reached by crowdsourcing, TrustChain Network.
- **Key activities**: Gap analysis and compliance assessments, Research and development of PECSi and PECSo, Validation on MASA infrastructures.
- **Key resources**: Academic know-how, Technology development team, Data privacy experts, Access to MASA infrastructures.
- **Key propositions**: PECSi to ensure a privacy friendly experience and PECSo to enhance the data obfuscation experience among end-users.
- **Stakeholders:** Service providers, infrastructures and end-users.

Funded by the European Union

- **Customer relationships**: Online documentation and crowdsourcing support.
- **Channels**: Academic and Industry events and conferences, Open-source distribution, Exhibitions, Real-Worl Demonstrations.
- **Customer segments**: End-users (Drivers), Automotive manufacturers, Infotainment software developers, Mobile app developers.
- **Cost structure**: Software development, service provision, maintainance.
- **Energy-Efficient Design**: PECSi and PECSo prioritise energy efficiency.
- **Data Minimisation**: PECSi and PECSo will be designed to minimise the unnecessary collection and transmission of data, thereby also reducing the energy required for data processing and transmission.
- **Life Cycle Assessment**: A comprehensive lifecycle assessment of the project will be conducted to identify areas where environmental impact can be reduced.
- **Environmental Compliance**: Project compliance will be ensured within all environmental regulations and standards in the regions where it operates

The business model canvas just provided revolves around its key propositions. In other words, and put more simply, the PECSi and PECSo modules bear a huge potential for business and exploitation through spin-offs.

In particular, PECSi abides by the cost structure given above. As services require more and more detailed privacy policies, PECSi will have to evolve coherently to reflect the modifications and the required extensions necessary to continue to offer drivers a friendly management of their privacy choices.

Beside PECSi lies PECSo with its strong, inherent requirement for customisation, hence with its enormous business potential, which is explained in the following. The team of the project has seen the two PECSo modules prototyping respectively Federated Learning and Secure Multi-Party Computation. The team also discussed Tier3 compliance signifying that a service provider has to deliver a new interface for its apps, an interface capable of receiving inputs in the form of FL models or of SMPC outputs. The counterpart to make obfuscation work at Tier3 is the PECSo-APP, which receives information from PECSi and controls the user data through the specific obfuscation technique that the user chose to be used with the given service.

It is also made clear that using Federated Learning to obfuscate the data that a user traditionally sends to a service requires availability of a model specifically trained over that very type of data. Similarly, using Secure Multi-Party Computation requires the encoding of the specific output to compute in a privacy-preserving way, output such as average, min, max and so on.

The obvious implication is that for every service that opts to become Tier3 compliant, there needs to be some coding effort to tailor the PECSo-APP to it. For the sake of

Funded by the European Union

demonstration, there is a potential need for components such as PECSo-FL-Service1, PECS-SMPC-Service1, PECSo-FL-Service2, etc.

It is behind the software development and maintenance effort that the team see huge, clear potential for a PECS spin off.

8.2.26.3Preliminary economic analysis

- Production Costs:
    - Go-to-Market costs: EUR 30,000 (Development and Deployment of PECS prototypes into actual products – one developer year for the first year)
    - Fixed Spin Off Costs: EUR 20,000 annually (Accounting and Administration)
- Revenue Projections:
    - Price per Unit: EUR 10,000 (Customisation of PECSi and PECSo for specific service that wants to become Tier3 PECS compliant)
    - Sales Forecast: 10 units in the first year
- Break-Even Analysis:
    - Break-Even Volume: 5 units in the first year
- Profit Margins:
    - Gross Profit Margin: EUR 50,000 under Sales Forecast

8.2.27 ProvenAI

ProvenAI's strategy for implementing data tracking and privacy within Retrieval Augmented Systems (RAG Systems) revolves around several pivotal components:

- Data Tracking in GenAI Systems (Retrieval Augmented Systems):
    - **Existing Provenance Tools:** Traditional provenance tools often focus on tracking entire datasets or documents overlooking the granularity required for tracking individual document pieces, especially in unstructured data. For example, a data tracking system might log whena file is accessed or modified, but it may not differentiate between individual sections or components within the file.
    - **Verifiable Credentials:** In a decentralized identity framework, verifiable credentials are used to authorize data transactions. For instance, consider a scenario where a researcher wants to access a specific topicof research. Verifiable credentials associated with the researcher's decentralized

Funded by the European Union

identity and the AI Agent's identity can grant them access to only the relevant papers related to the specific knowledge field and purposes.

- **ISCC Codes:** The International Standard Content Code (ISCC) enables the unique identification of individual documents and their sections within a document. For example, each paragraph, image, or table within a research paper can be assigned a unique ISCC code.

- Utilization of SSI and Decentralized Identities in AI Systems:
  - **Decentralized Identities (DIDs):** Decentralized identities, represented by DIDs, provide individuals and entities with control over their digital identities. For instance, consider a student who owns a decentralized identity. This identity can be used to authenticate the student's access to educational resources and track their learning progress securely.
  - **EU Standards:** European Union standards such as eIDAS (Electronic Identification, Authentication and Trust Services) and the EU AI Act provide regulatory frameworks for identity management and AI governance. These standards ensure that AI systems adhere to data protection and privacy regulations while leveraging decentralized identities for user authentication.
  - **Decentralized Identities in AI Systems:** In AI systems, decentralized identities play a crucial role in ensuring data privacy and security. For example, an AI Agent system may authenticate Agents using their decentralized identities before providing personalized learning recommendations. This ensures that only authorized users have access to certain educational data.
  - **AI Agents:** AI Agents, such as language models like GPT-4, are evolving entities with specific roles and purposes. For instance, an AI Agent may serve as a language tutor, providing assistance with grammar and vocabulary. By uniquely identifying AI Agents using DIDs, ProvenAI enables accountability and traceability in AI interactions, allowing policymakers to regulate AI usage based on the creators' identities.

8.2.27.1 Market Overview

ProvenAI operates at the intersection of data management, AI development, and blockchain-based identity solutions. This market analysis reviews similar platforms, services, and applications to identify stakeholders, potential partners, and competitors. The analysis highlights opportunities for market entry and potential obstacles.

8.2.27.1.1 Similar Platforms and Services

Funded by the European Union

TABLE 96: MARKET ANALYSIS FOR PROVENAI

Application	Category	Description	ProvenAI leverage/upgrading level of existing solutions
LangChain	RAG – AI Agent	LangChain is a framework that enables creation of AI Agents supported by Retrieval Augmented Generation, that integrates external tools and external data sources, enhancing AI applications with more versatile and context-aware responses.	- AI Agents are not identified globally - No data-owner consent mechanismexists ProvenAI incorporates these capabilities
OriginTrail DKG	RAG	OriginTrail Decentralized Knowledge Graph (DKG) is a blockchain-powered framework that facilitates the secure and interoperable exchange of data across different networks, enhancing the trust and verifiability of shared information.	- Unstructured data pieces identification (sections of documents) is not possible. ProvenAI incorporates these capabilities
AI-tutor.app	AI Education	AI tutor is a personal tutoring app that resolves questions on the spot by simply taking a photo of theproblem or explanation andsending it to Discord.	-AI Tutors are pre-defined ProvenAI is forming a community of actively engaged educators, and is the TOOL that educators will use to CREATE their AI Tutors

Funded by the European Union

Khanmingo	AI Education	Khanmigo is an AI-powered personal tutor and teaching assistant from trusted education nonprofit Khan Academy. For learners and families, Khanmigo offers engaging, on-topic, and effective learning for students, and is ethically designed with safety and learning as a top priority. Unlike other AI tools such as ChatGPT, Khanmigo doesn't just give answers. Instead, with limitless patience, it guides learners to find the answer themselves.	+AI Tutor assistance -closed community, that does not enhance knowledge exchange and sharing -AI Tutors are pre-defined ProvenAI is forming a community of actively engaged educators, and is the TOOL that educators will use to CREATE their AI Tutors

8.2.27.1.2 Established Partners

TABLE 97: PARTNERS FOR PROVENAI

Walt.id wallet/issuer	SSI standards	Walt.id specializes in Self-Sovereign Identity (SSI) solutions compliant with European standards like eIDAS, facilitating secure digital identity management and verification within a regulatory framework, ensuring user privacy and data integrity.	+ secure digital identity managementand verification withina regulatory framework ProvenAI utilizes the infrastructure provided to quickly issue & verify credentials compliant with SSI/W3C/EU standards

Funded by the European Union

International Standard Content Code (ISCC)	Standard	The ISCC is a free, open-source universal identifier for digital content, currently in the process of becoming an ISO standard. It uses algorithmic fingerprints to enhance content identification and management across decentralized sectors, signaling a significant step towards standardization.	+ content identification ProvenAI uses ISCC Code to identify sections of documents contributing to an AI generated answer

8.2.27.1.3 Potential Partners

1. Data Management Platforms

- Description: Companies specializing in secure data storage and management solutions.
- Potential Collaboration: Integrate ProvenAI to offer enhanced data interaction and compliance features.

2. AI Development Firms

- Description: Companies developing AI models and applications.
- Potential Collaboration: Partner to integrate ProvenAI's data management capabilities with AI development workflows.

3. Educational Institutions

- Description: Universities, colleges, schools, and other educational organizations.
- Potential Collaboration: Use ProvenAI to manage and share educational data securely, improve teaching methodologies with AI insights, and ensure compliance with data protection regulations.

4. Tutor Collectives

- Description: Groups or associations of private tutors.
- Potential Collaboration: Utilize ProvenAI for managing and sharing educational content, providing a platform for collective learning, andensuring proper compensation and credit for contributed content.

Funded by the European Union

5. Online Learning Platforms

- Description: Platforms like Coursera, Udemy, and Khan Academy.
- Potential Collaboration: Incorporate ProvenAI's data management and AI interaction features to enhance their educational offerings and ensure compliance with data protection regulations.

6. EdTech Companies

Description: Companies developing educational technology solutions.

Potential Collaboration: Integrate ProvenAI into their existing platforms to provide secure data management, AI-enhanced educational tools, and compliance with regulations.

8.2.27.2Value Network for ProvenAI

TABLE 98: VALUE NETWORK FOR PROVENAI

Stakeholder	Role	Value Provided	Interactions	Revenue/Information Flow
Educational Institutions	Data Providers	Provide educational content and resources	Data sharing, feedback	Subscription fees, data usage analytics
Tutor Collectives	Content Creators	Create and share educational content	Content creation, feedback	Compensation for content usage, analytics
EdTech Companies	Technology Partners	Integrate ProvenAI into their platforms	Technology integration, feedback	Licensing fees, shared revenue from content usage
Online Learning Platforms	Distributors	Distribute ProvenAI's AI tools and resources	Content distribution, feedback	Licensing fees, shared revenue from content usage
AI Development Firms	AI Developers	Develop AI models and applications	AI integration, feedback	Licensing fees, shared revenue from AI model usage
Regulatory Authorities	Compliance Enforcers	Ensure data protection compliance	Compliance audits, feedback	Consulting fees, compliance management fees

Funded by the European Union

8.2.27.3SWOT Analysis

TABLE 99: SWOT ANALYSIS FOR PROVENAI

Strengths	Weaknesses
Advanced AI technology	High initial development costs
Strong data privacy controls	Market competition
Compliance with GDPR	Educators' reluctance to adopt new tech
Integration with decentralized identities	
Opportunities	**Threats**
Growing demand for AI in education	Regulatory challenges
Potential for strategic partnerships	Market adoption resistance
Leveraging blockchain for security	Competing platforms and tools
Technological advancements	

TABLE 100: BUSINESS MODEL CANVAS FOR PROVENAI

ProvenAI		*Designed for:*	*Designed by:*	*Date:*	*Version:*
Business Model Canvas		ProvenAI	Ctrl+Space Development	01.07.2024	
Key Partners	**Key Activities**	**Value Propositions**	**Customer Relationships**	**Customer Segments**	
Data Management Platforms: Integration with existing data management solutions **AI Development Firms:** Collaboration for integratingProvenAI into AI systems **Legal and Compliance Consultants:** Partnerships for ensuring regulatory compliance **Educational Institutions** **Tutor Collectives**	**Platform Development:** Designing, developing, and maintaining **Compliance Management:** Ensuring compliance with data protection regulations **Marketing and Sales:** Promoting the platform, acquiring new customers, and managing relationships **Users' Support:** Providing assistance, training, and troubleshooting to customers	Secure and transparent platform for managing AI interactions with data Precise control over data access and usage Compliance with regulations like GDPR Integration with decentralized identity technologies for secure authentication	Personalized onboarding and support for data owners and AI developers Continuous communication forfeedback and updates Compliance assistance and consulting services Online knowledge base and community forums for self-help	**Data Owners** (enterprises, educational institutions, organizations, individuals with valuable data) **AI Developers** (companies, researchers, developers creating AI models) **Regulatory Authorities** (entities responsible for enforcing data protection regulations) **AI Service Providers** (companies utilizingAI	

Funded by the European Union

			technologies for various applications)
	Key Resources **Development Team:** Software engineers,AI experts, blockchain developers **Compliance Experts:** Legal advisors, data privacy specialists **Marketing and Sales Team:** Sales representatives, marketing specialists **Technology Infrastructure:** Servers,databases	**Channels** Online platform for subscription and access Direct sales to enterprises and organizations Partnerships with AI development firms and compliance consultants Marketing through industry events, conferences, and online channels	
Cost Structure • **Development Costs: Salaries, software tools, infrastructure** • **Compliance Costs: Legal fees, compliance audits** • **Marketing and Sales Costs: Advertising, promotions, sales commissions** • **Operational Costs: Office rent, utilities, administrative expenses**		**Revenue Streams** • Subscription fees for data owners based on data volume and usage • Licensing fees for AI developers based on usage and features • Consulting fees for compliance and data governance services • Revenue sharing from fair compensation mechanisms for data usage	

TABLE 101: ECONOMIC ANALYSIS FOR PROVENAI

Funded by the European Union

Category	Description	Year 1	Year 2	Year 3	Year 4	Year 5
Costs						
Development Costs	Salaries for developers, AI experts,blockchain developers	100.000	100.000	100.000	100.000	140.000
Compliance Costs	Legal fees, compliance audits, dataprivacy specialists	5.000	5.000	5.000	5.000	5.000
Marketing and Sales Costs	Advertising, promotions, sales commissions	3.000	5.000	6.000	10.000	15.000
Operational Costs	Office rent, utilities, administrative expenses	2.000	3.000	3.500	10.000	15.000
Support and Training Costs	Customer support, training materials, workshops	2.000	5.000	10.000	10.000	15.000
Total Costs		112.000	119.500	125.500	135.000	190.000
Benefits						
Subscription Fees	Revenue from end-users based on usage (monthly subscription -50% for tutors – 50% for Ctrl+Space Labs)	12.000	36.000	60.000	90.000	120.000
Licensing Fees	Revenue from AI Firms (solution Integration)	30.000	40.000	50.000	80.000	100.000
Consulting Fees	Revenue from compliance and data governance services	50.000	50.000	50.000	70.000	80.000
Increased Efficiency	Cost savings from streamlined operations and improved data management	0	5.000	10.000	20.000	30.000
Total Benefits		82.000	131.000	170.000	260.000	330.000
Net Benefits (Costs)		**-30.000**	**+11.500**	**+44.500**	**+125.000**	**+140.000**

Funded by the European Union

REFERENCES

Osterwalder, A. & Pigneur, Y. (2010). Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers.

Pinheiro, E., Weber, W.-D., & Barroso, L. A. (2007). Failure trends in a large disk drive population. In Proc. of 5th USENIX Conference on File and Storage Technologies (FAST' 07), San Jose, CA, USA.

Porter, M. (1985). The Competitive Advantage: Creating and Sustaining Superior. New York, Free Press.

Funded by the European Union