NGI TRUST CHAIN

D3.7 TrustChain Support to third party innovators-Guide for Open Call implementation-1

18/07/2023

Funded by the European Union

TrustChain Project. Funded by the European Union under GA No 101093274. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

NGI TRUST CHAIN

Grant Agreement No.: 101093274
Call: HORIZON-CL4-2022-HUMAN-01
Topic: HORIZON-CL4-2022-HUMAN-01-03
Type of action: RIA

D3.7 TRUSTCHAIN SUPPORT TO THIRD PARTY INNOVATORS

GUIDE FOR OPEN CALL IMPLEMENTATION - 1

Work package	WP3
Task	3.4
Due date	30/06/2023
Submission date	18/07/2023
Deliverable lead	ALA
Version	1.0
Authors	Alexander Herranz (ALA) Iker Ruiz de Infante (ALA)
Other contributors	Maria Pretel (CIB) Caroline Barelle (ED) Thanasis Papaioannou (NKUA) Vlado Stankovski (UL) Akanksha Dixit (ICS)
Reviewers	Maria Pretel (CIB) Thanasis Papaioannou (NKUA)
Abstract	This document presents the coaching, monitoring, and evaluation activities in the context of the TRUSTCHAIN project OC1 and provide

Funded by the European Union

	the information needed for the selected applicants to successfully conduct their subproject work.
Keywords	Coaching, monitoring, evaluation of open call activities

Document Revision History

Version	Date	Description of change	List of contributors(s)
v0.1	05/05/2023	First version of the deliverable	Maria Pretel (CIB) Alexander Herranz (ALA) Thanasis Papaioannou (NKUA)
v0.2	08/06/2023	Contribution about implementation	Caroline Barelle (ED)
v0.3	06/07/2023	Preliminary final version	Iker Ruiz de Infante (ALA) Thanasis Papaioannou (NKUA) Vlado Stankovski (UL) Akanksha Dixit (ICS)
v0.4	12/07/2023	Internal review	Thanasis Papaioannou (NKUA) Maria Pretel (CIB)
v1.0	17/07/2023	Deliverable final version	Iker Ruiz de Infante (ALA)

Disclaimer

The TRUSTCHAIN project is funded by the European Union's Horizon Europe Research and Innovation programme under grant agreement no. 101093274.

COPYRIGHT NOTICE

Funded by the European Union

The TRUSTCHAIN Consortium is the following:

Participant number	Participant organisation name	Short name	Country
1	EUROPEAN DYNAMICS LUXEMBOURG SA	ED	LU
2	F6S NETWORK IRELAND LIMITED	F6S	IE
3	UNIVERZA V LJUBLJANI	UL	SI
4	ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS - RESEARCH CENTER	AUEB	EL
5	FUNDACION CIBERVOLUNTARIOS	CIB	ES
6	CONSORCIO RED ALASTRIA	ALA	ES
7	TIME.LEX	TLX	BE
8	CITY UNIVERSITY OF LONDON	ICS	UK

EXECUTIVE SUMMARY

This document presents the coaching, monitoring, and evaluation activities in the context of the TRUSTCHAIN project OC1 and provide the information needed for the selected applicants to successfully conduct their subproject work.

Funded by the European Union

TABLE OF CONTENTS

Funded by the European Union

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

AI	Artificial Intelligence
BaaS	Blockchain-as-a-Service
CCR	Cross-Cutting Requirements
DAO	Decentralised Autonomous Organization
DID	Decentralised Identifier
DLT	Distributed Ledger Technology
DT	Digital Twin
GDPR	General Data Protection Regulation
ID	Identity
IoT	Internet-of-Things
IP	Internet Protocol
KPI	Key Performance Indicator
KYC	Know Your Customer
OC	Open Call
OLA	Operational Level Agreement
SLA	Service Level Agreement
SSI	Self-Sovering Identity
TCP	Transmission Control Protocol
TR	Technical Requirement
TRL	Technology Readiness Level
VC	Verifiable Credential
WP	Working Package
W3C	World Wide Web Consortium
ZKP	Zero-Knowledge Proof

Funded by the European Union

1 CONTEXT

The Internet has pushed our existence into the digital era, revolutionising our health, our wellbeing, our social life, our education, and our information. Today we approach the Internet with our digital identities. There is a plethora of such digital identities that currently do not properly serve their purpose. Multiple threats related to truthfulness, trust, and identity (ID) arise when people interact in this digital world: delusion and manipulation, personal privacy violation and personal data exploitation, unknown provenance of information, anonymity for performing criminal activities, spread of fake news using fake identities, skills mismatches, serious breaches of security are only a few of the threats that have emerged. The spirit of the first-generation Internet based on individual freedom, material progress, and moral community is slowly turning into individualism, materialism, and moralism, diverging from essential ethical and democratic principles that should underline this technology. The design choice of the past, based on a mix of centrally managed networking and device technologies makes today's Internet obsolete when it comes to empowering all citizens to act for a more environmentally friendlier digital transformation, as well as to create a more resilient, inclusive, and democratic society, addressing inequalities and human rights, better prepared for and responsive to threats and disasters.

For TRUSTCHAIN, the current emergence of Internet of Things (IoT), Decentralised Oracles, Artificial Intelligence (AI), Cloud-to-Edge (aka Fog) Computing, Distributed Ledger (DLT) and Digital Twin (DT) technologies created the need to build democratic systems without central points of control that can establish the missing link between universally agreed objectives in the physical world, and the digital representation of the reality, thus contributing to the realisation of trusted relationships in the Next Generation Internet. This can be achieved by using various consensus mechanisms that associate proofs with digital representations and thus help humans understand the objective truth, achieve trusted relationships on the digital world, allowing them to undertake well-informed decisions, in either a manual or automated manner. The ability to arrive at the objective truth by employing democratic governance mechanisms, consensus-based proofs, verification, and certification can lead to a Next Generation Trusted Internet supporting humanity in all aspects of life. Today more than ever, challenges faced all over the world push for our society to reorganise itself to survive. The United Nations have called to reach 17 Sustainable Development Goals. Essentially, TRUSTCHAIN must be leveraged to embed in the Next Generation Internet principles of human-rights, sustainability, ethics, and other human values that have been developed and maintained through long lasting centuries of human evolution.

The key concept of TRUSTCHAIN is to embed the key humanity principles in the co-creation of the Next Generation Internet and to provide autopoietic, evolutionary, decentralised, and therefore democratic, transparent, traceable, and regulatory

Funded by the European Union

compliant mechanisms that can support any ecosystem of entities and actors participating with their digital identities. The basis for this to happen is the use of decentralised digital identity architectures together with IoT, AI, Cloud-to-Edge, DLT and DT.

In that context, TRUSTCHAIN aims to generate an ecosystem of user-centred blockchain-based solutions, processes, and business models with strong market potential in trusted blockchain-based data, metadata, ontology, knowledge, and information management to achieve trustworthy content handling and information exchange as well as trustworthy service exchange in the Next Generation Internet/social networks and for vital sectors of the European economy. The TRUSTCHAIN consortium will launch five Open Calls to fund third parties for the development of the TRUSTCHAIN blockchain ecosystem. This document concerns TRUSTCHAIN OC1 – Decentralised Digital Identity and the following activities have been performed along the TRUSTCHAIN project WP2 to implement it:

- **Preparation:** elaboration of all the open call documents: open call text, guidelines, materials, contract templates for sub-grantees and the definition of the templates for proposals (based on experience on past partners experience within Third parties financing).
- **Publication and promotion:** publish the open calls for proposals on F6S and coordinate with the Dissemination WP its promotion.
- **Evaluation:** select the evaluation board, execute a clear and transparent evaluation process.
- **Contracting:** preparation and signature of the sub-grantee agreements by the coordinator (in representation of TRUSTCHAIN consortium) and every sub-grantee will bring a set of administrative tasks that need to be done to assure the Horizon Europe principles are respected.
- **Analysis:** monitor and analyse/statistics of the open call results.

For the selected applicants of this Open Call 1 and each subsequent Open Calls, coaching, monitoring and evaluation activities will be performed under the TRUSTCHAIN project WP3, T3.4 and WP4, T4.1, T4.2, T4.3, T4.4 as follows:

- **Coaching:** Guidance and provide feedback to selected applicants regarding TRUSTCHAIN expectations.
- **Monitoring:** Follow-up experiments activities, deliverables, and outcomes.
- **Evaluation:** Define KPIs and evaluate the deliverable of selected applicants against them.

This Implementation Guide aims to explain the coaching, monitoring, and evaluation activities in the context of the TRUSTCHAIN project and provide the information needed for the selected applicants to successfully conduct their subproject work.

2 THE TRUSTCHAIN OPEN CALL 1: DECENTRALISED DIGITAL IDENTITY

2.1 TRUSTCHAIN OC1 SPECIFIC OBJECTIVES

Today, the digital identity is an essential component of any application and computing system. The digital identity is usually established by mechanisms of proving a secret that we have (e.g., password), what we possess (e.g., an identification card) or what we are (e.g., biometric data). However, in the complex world of today, a much stronger and more fine-grained Decentralised Identifiers (DIDs) are necessary to be used, in order to achieve privacy on one hand, and security on the other. Capability to autonomously manage different facets of identity brings light to Self-Sovereign Identities (SSIs). The trustworthiness and/or credentials of SSIs or DIDs cannot be taken for granted but should be assessed by means of verification from certification authorities or by means of decentralized reputation mechanisms. Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs) are currently emerging standards of the Semantic Web to ensure trustworthiness. Concomitantly, the credibility of data shared online or employed in smart contracts in the blockchain is also questionable and should also be assessed.

For this purpose, trustworthy decentralized identities and data are the focus of Open Call 1 (OC1) on "Decentralised Digital Identity". It aims to define, develop and ensure:

- **Framework for decentralized user-centric identity management that lies in the scope of the call and addresses the stated challenges below,**
- **Protocols for trustworthiness of entities by means of verifiable credentials and decentralized reputation systems,**
- **Identity attributes are disclosed only with the informed consent from the data owner (i.e., data minimization requirement of GDPR),**
- **Smart oracles to assess the trustworthiness of data fed to blockchain smart-contracts fetched from external systems within the scope of trustworthy identities as data sources.**

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

2.2 TRUSTCHAIN OC1 CHALLENGES TO ADDRESS

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 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 the 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. Develop a usable and interoperable decentralised future internet, some of the identity challenges that exist today need to be addressed. These include:

- The current identity systems lack usability, privacy, transparency, interoperability and compliant with GDPR and is not inclusive in nature;
- It incorporates multitude of technologies such as zero-knowledge-proof (ZKP) 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 onto identity fraud;
- Human has not been involved from the initial design stages of the identity eco system. This leads onto 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;

- Regulatory alignment of existing digital identities (e.g., in the context of EU eIDAS framework).

Based on the above, ensuring usage of digital identity in blockchain within Europe means for TRUSTCHAIN OC1 solutions to address the following:

- **Enhancing User-Centric Decentralized Identity Solutions**
    1. **Usability and User Experience:** Designing user-friendly interfaces and seamless experiences for individuals to easily manage their decentralized identities and interact with blockchain-based services.
    2. **Interoperability:** Ensuring compatibility and seamless integration between different decentralized identity systems and blockchain platforms to enable cross-platform usage.
    3. **Privacy and Data Protection:** Addressing privacy concerns and implementing robust security measures to protect user data while maintaining compliance with relevant regulations like GDPR.
    4. **Adoption and Awareness:** Educating the general public about the benefits and possibilities of decentralized identity solutions, fostering trust, and encouraging widespread adoption.

- **Scaling and Performance of Decentralized Identity Solutions**
    1. **Scalability:** Designing decentralized identity systems that can handle a massive number of users and transactions without compromising performance and speed.
    2. **Identity Validation and Verification:** Developing efficient methods for verifying and validating identities on the blockchain, ensuring accuracy and preventing identity fraud.
    3. **Infrastructure and Resource Requirements:** Addressing the resource-intensive nature of blockchain technology and finding solutions to reduce the computational and storage requirements for decentralized identity systems.
    4. **Network Consensus and Governance:** Establishing effective consensus mechanisms and governance models to ensure the integrity and reliability of decentralized identity systems at scale.

- **Regulatory Compliance and Legal Frameworks for Decentralized Identity**
    1. **Legal Frameworks and Jurisdiction:** Navigating the legal landscape to ensure compliance with existing regulations and adapting to emerging regulatory frameworks related to decentralized identity and blockchain technology.

2. **Cross-Border Data Transfer:** Overcoming legal barriers and challenges associated with cross-border data transfer while maintaining privacy and security in decentralized identity systems.
3. **Standardization:** Developing industry-wide standards and protocols for decentralized identity to facilitate interoperability, compliance, and regulatory harmonization.

- **Public Trust and Accountability:**

Establishing mechanisms to ensure transparency, accountability, and public trust in decentralized identity systems, especially regarding data governance, user control, and auditability.

These aspects are discussed in more detail in section 2.5 of this document and will be subject to discussion with and between selected applicants any times relevant during the supporting and coaching phase of OC1 implementation.

2.3 EXPECTED OUTCOMES AND POSSIBLE APPLICATION DOMAINS

In OC1, the application should respond to citizens' needs based on actual facts.
Hence, the expected OC1 outcomes are:

- Reliable identity retrieval (e.g., via Social Guardians);
- Flexible identity management options that will allow users to define and modify their own trust relationships;
- Guardrails ensuring that specific parts of identity information are disclosed uniquely with consent from the user in question;
- Decentralised reputation management systems;
- Smart oracles for trustworthiness assessment of real-world data.

These outcomes could be materialised by:

- Decentralised digital wallets for self-sovereign identity;
- Identity and attribute reputation management systems;
- User centric privacy preserving identity management framework;
- Decentralized (data) marketplaces;
- Automated regulatory compliance for KYC;
- EU cross-border identity portability and translation;
- Validation of EU qualifications / certifications;
- Cross-border mobility of EU citizens

Possible application domains (not limited to) are:

- Healthcare;
- Education, University diplomas etc.;
- Collaborative environments;
- Social networks (and the use of identities within such networks);
- Notarization;
- Banking;
- Creative industries;
- The aging population and their needs, e.g., taxation relief;
- Any marginalised individual and their specific needs;
- Creative industries (e.g., collaborative production of artistic and unique works);
- Entertainment, leisure, gaming industry;
- Tourism, and similar.

2.4 TRUSTCHAIN OC1 SELECTED PROPOSALS

TRUSTCHAIN OC1 was welcoming applications that should clearly define, upgrade/extend the state-of-the-art, and develop the following types of solutions:

- Decentralised user-centric identity management framework for supporting an automated privacy preserving, legal and regulatory compliant infrastructure (e.g., GDPR) potentially in alignment with emerging European regulations and standards (i.e., eIDAS).
- Protocols for trustworthiness assessment of entities by means of verifiable credentials and decentralized reputation systems.
- Smart oracles assessing the trustworthiness of data associated with digital identities.
- Inclusive digital identity platforms focusing on marginalized communities (e.g., refugees, elderly, vulnerable).
- Social identity for delegation and recovery that drives community-based trust establishment (i.e., social guardians).
- Systems considering both public and private administration roles in issuing and managing decentralized identifiers.
- Decentralized identity systems supporting Decentralised Autonomous Organizations (DAOs),
- Use-case driven identity management system deployment (e.g., banking, publishing, healthcare, education etc).

As a result of the implementation of the evaluation process defined in the Guide for Applicants, 13 proposals were selected to join the TRUSTCHAIN project.

TABLE 1 SELECTED PROPOSAL, THEIR OBJECTIVES, EXPECTED OUTCOMES AND THE CHALLENGES THEY WILL TACKLE

Proposals	Objectives & expected outcomes	Challenges expected to be tackled
DidRoom	DidRoom aims to implement a fully open source, multiplatform, highly extendable open-source wallet, offering SSI, blockchain interoperability on top of advanced cryptography. It will be compliant with the W3C-DID and W3C-VC standards and with the current "European Digital Identity Wallet Architecture and Reference Framework" (EUDI – ARF, version 1.0.0 from January 2023).	It will add one more trust layer to the verification of data validity.
CreatorCredentials.cc	CreatorCredentials.cc aims to develop a software application and a legal framework that can be used by media organisations to provide services to issue verifiable creator credentials. The app will be based on new and upcoming W3C and ISO standards for decentralised content identification (ISCC), decentralised identifiers (DIDs), verifiable credentials (VCs), and other established online reputation systems. It will be aligned with emerging European regulations on digital identity, such as eIDAS, as well as the directives on copyright (DSM), the Digital Services Act (DSA) and Digital Markets Act (DMA).	It will help prevent the unauthorised use or misappropriation of digital media content, reduce the spread of misinformation and fake news, and promote the identification of original creative works created by human beings in the context of AI-generated content.
MUSAP	MUSAP' aims to develop a new software interface called Unified Signature Application Programming Interface (USAPI) Library that provides a consistent and flexible way for applications to request either low, substantial, or high LoA signatures, regardless of the SSCD technology or location of the private key.	It will tackle the lack of common API for smartphone apps to connect SSCD functionalities with specific consideration of the privacy of the users and their data, minimisation of Personal Identifier data, step up authentication, validation of VCs, usability, inclusivity, interoperability, standard compliance, eIDAS compliance,

		scalability.
TREVO	TREVO aims to revolutionize electronic voting systems by employing decentralized identities rooted on blockchain and an SSI approach that puts the user at the centre of the process from the early phases of the design process. It will employ blockchain technology and more specifically Decentralised Identities, Verifiable Credentials and state-of-the-art communication protocols and architectures, following the latest EU guidelines and regulations in terms of digital identities and data protection. Its framework will incorporate a mobile wallet that enables EU-wide interoperability for citizen authentication and authorization based on well-established technologies entailing trust from anchors of the public sector.	It will tackle main challenges in electronic voting that are still open, such as voter anonymity, ballot privacy, trusted tally/audit as well as verifiability.
Orchestral	Orchestral aims to co-develop an identity management system for marginalised communities built with Pangea's digital service and circular device management services. The system will allow users to manage their online identities and access community-centred internet services trusted high quality data according to their identity profile.	Integrating SSI framework in an already existing system and promoting trust and privacy online in more efficient and scalable communities. Empowering marginalised communities in their access to digital services by providing a better privacy preserving system.
The Social Wallet	The project aims to develop a solution that will provide authorities and sponsors with an efficient digital platform to request required information from socio-economically weaker and marginalized user – in a privacy-preserving manner – and to issue for them benefits. It will take the form of a fully functional modular Social Wallet ready for distribution and use in production and that uses a W3C/DIF/EUDI-compliant identity framework. It will include an easy-to-use smartphone application, focused on use by people with limited digital skills and less-than-average language- or literacy-skills as well as an easy-to-use smartphone application, focusing on use	It will support socio-economically weaker and marginalized groups by getting them from these disadvantaged. It aims as well as encouraging them to start using this application and learn new digital skills and de-risk them from being left behind.

	by providers of services.	
DID4EU	The project aims to offer developers and organizations a holistic open-source decentralized identity infrastructure that makes it easy to build applications using off-chain and on-chain technologies (e.g., SSI, m-docs, NFTs, SBTs) in a way that is ecosystem- and blockchain-agnostic and compliant with EU's existing and emerging regulation on digital identity like eIDAS2 or GDPR.	By building an open source identity & wallet infrastructure that enables any developer to build apps & use cases compliant with EU's new identity ecosystems & laws: eIDAS2 (and EBSI)., the project will tackle challenges pertaining to the lack of usability, privacy, transparency, interoperability & GDPR compliance of systems as well as the lack of trust in the way the identity credentials are shared/used while including realization of data minimization.
IM4DEC	The project aims to implements and evaluates an important advancement for Decentralised Identifiers: DID Rotation together with relevant standardisation and validation for the DID Resolution process. Furthermore, it will provide the technical (Registration Service) and legal (DPIA) basis for individuals to use DIDs. All this embedded in the highly relevant emergency services domain to support minorities and the oppressed.	It aims to face the challenge of full and equal participation of persons with disabilities, including access to communication and information services as requested by UN. It will support thanks to an appropriate solution, deaf and hard of hearing persons in Europe who currently rely on outdated technology (e.g., fax) and help from others to make an emergency Call
WIDE	The project intends to develop a Decentralized Identity (DID) bridge prototype for managing user identities, and connecting the European Commission's eIDAS 2.0 initiative with decentralized autonomous organizations (DAOs) on public-permissionless distributed ledger technologies (DLT). It will combine existing technologies from traditional finance and the cryptocurrency sector with innovative DID concepts. It will feature a novel architecture that preserves privacy and user control, while freeing users from the responsibility of managing their data directly.	The challenge is to build a novel architecture that preserves privacy and user control, while freeing users from the responsibility of managing their data directly.
CLIENT-DIDS	The project aims to improve the Universal Registrar tool, that allows creation of DIDs across different DID	Any decentralized identity application or service should consider DIDs an abstraction

	methods and networks. It offers an abstraction layer with a universal interface, which means that clients of this tool can create DIDs without having to know or implement details of the underlying DID method. The intention is to move away from a centralised approach to a decentralised client secret mode enabling them to manage certain tasks according to DIDs hence giving more control to the users. The proposed device agnostic solution will allow DIDs creation and management as well as respective wallet keys in a fully decentralised and blockchain agnostic manner.	layer and should aim at working with any DID method. However, in practice, many tools in the community often consider DIDs an "afterthought", and they often only support a small number of DID methods that have been arbitrarily selected for a subset of use cases, rather than building on top of a generic, interoperable DID infrastructure layer. Consequently, there is often very limited interoperability between different software stacks and ecosystems. CLIENT-DIDS aims to tackle this challenge.
EVI Electric Vehicle Identity	EVI aims to design and deploy a Dapp that will enable vehicle owners to generate decentralized vehicle identity certificates. These identity certificates will be stored in the drivers' digital wallet of preference and electric vehicle. 3rd parties can retrieve these certificates when a vehicle is plugged and request payments for charging sessions in public charging stations via the drivers' preferred digital wallet. In that way the drivers limit the information they are required to disperse to third parties (CPO, charging applications) and rely on a decentralized digital identity to perform charging transactions in different charging stations with less friction.	Drivers of electric vehicles (EVs) face significant data privacy risks when charging their vehicles in Public Charging Stations. Each charge point operator (CPO) uses different software to manage its stations and collect charging fees. Drivers are forced to sign up with multiple applications to start a charging session in Public Charging Stations. This further complicates drivers' experience as each application requires personal and financial data before it enables the driver to initiate a charging session. An underappreciated risk with the dispersion of information across multiple platforms is that vehicle and user data can be used to pinpoint users' locations and everyday activities. Drivers do not retain control on how 3rd parties exploit their personal data. EVI will tackle this challenge and ensure that vehicle owners have control of the type of data transmitted during a transaction in charging station.
IS-CIS	The project intends to implement a generic framework that mimics human nature in disclosure of identity. A tokenized solution for blockchain-based data sharing according to a given consent will be delivered. flexible identity	Today most of the IT-centric systems disclose information in binary fashion: all or nothing: all the data file, profile, user history, or none of it. this poses the challenge of control and repeal

	management options will allow users to define and modify their own trust relationships and guardrails ensuring that only specific parts of their identity information will be disclosed and this uniquely with their consent. IS-CIS solution will mimic natural human behaviour in releasing information successively, on a need-to-know basis, in function of trust, and in function of value in return. It will reserve control and repeal rights in the hands of the individual. It will place an onus on the asker to justify and convince the askee. It will retain a permanent record of who requested, and who granted, what and when.	rights. IS-CIS intends to give back the control to the data owner allowing them to share information sequentially and iteratively, instinctively combining "need-to-know" with "value-add" and "subjective risk" assessments on the fly.
PRIVÈ	The project aims to extend the decentralized user-centric identity management framework by building an open-source library that can be added as an extension to any SSI wallet on the Holder side to enable the use of hardware-based keys. This will offer the possibility to bind Verifiable Credentials (VCs) to the wallet of the holder and transfer the root of trust of the SSI ecosystem purely to the digital wallet by considering an underlying Trusted Component as part of the wallet, without making any assumptions on the trustworthiness of the other layers. This will enable digital identity wallets to align with emerging regulations and standards like eIDAS that require higher Level of Assurances (LoA) for services.	It will verify the integrity and origin of the presented VCs or VPs. The use of a software key-store introduces many security risks and raises trustworthiness issues, so they will introduce a hardware-based solution. Also, they aim to achieve high Level of Assurances (LoA) in isolating keys from the holder and in binding identity data to the holder, which characterize the degree of confidence in the electronic identification means, while using cryptographic mechanisms to guarantee privacy preservation.

2.5 TRUSTCHAIN OC1 REQUIREMENTS

2.5.1 Technical Requirements

When implementing their projects, all the selected projects will have to consider whenever relevant and applicable the following aspects in a technical manner according to the solution they envisioned:

- TR1 - Privacy and Data Protection
- TR2 - Identity Validation and Verification
- TR3 - Cross-Border Data Transfer

- TR4 - Infrastructure and Resource Requirements
- TR5 - Interoperability
- TR6 - Legal Frameworks and Jurisdiction
- TR7 - Standardisation
- TR8 - Usability and User Experience
- TR9 - Scalability

Each of these aspects are described in more details regarding the challenges they raised, the requirements to be addressed and the expected outcomes at the level of the envisioned solution in the tables below.

1 TR1 - Privacy and Data Protection

TR1 - Privacy and Data Protection	
Definition	Addressing privacy concerns and implementing robust security measures to protect user data while maintaining compliance with relevant regulations like GDPR.
Challenges to be tackled	• **Privacy incidents:** Number of privacy incidents reported within a given time frame. • **Compliance gaps:** Number of identified compliance gaps related to privacy regulations. • **Data breaches:** Number of data breaches that occurred, indicating potential vulnerabilities. • **Employee training:** Percentage of employees trained on privacy policies and procedures. • **Audit findings:** Number of privacy-related findings identified during internal or external audits. • **Customer complaints:** Number of customer complaints related to privacy concerns or data protection.
Requirements to be addressed	• **Consent management:** Percentage of user consents obtained and documented for data processing activities. • **Privacy policy updates:** Number of privacy policy updates made to ensure compliance with relevant regulations. • **Data minimization:** Percentage reduction in unnecessary or redundant data collected and stored. • **Privacy impact assessments (PIAs):** Number of PIAs conducted to identify and mitigate privacy risks. • **Data subject access requests (DSARs):** Average response time for handling DSARs in compliance with regulatory timeframes. • **Security controls:** Implementation and effectiveness of technical and organizational security measures to protect data.
Expected outcomes at the level of your solution	• **Compliance level:** Percentage of compliance achieved with relevant privacy regulations (e.g., GDPR). • **Data breach incidents:** Reduction in the number and impact of data breach incidents. • **Consent rates:** Increase in the percentage of users providing informed consent for data processing.

	• **Privacy awareness:** Improvement in employees' understanding and awareness of privacy policies and practices. • **Data retention policy:** Implementation and adherence to a documented data retention policy. • **Third-party risk management:** Implementation of processes to assess and manage privacy risks associated with third-party vendors or partners.

2 TR2 - Identity Validation and Verification

TR2 - Identity Validation and Verification	
Definition	Developing efficient methods for verifying and validating identities on the blockchain, ensuring accuracy and preventing identity fraud.
Challenges to be tackled	• **Accuracy Improvement Rate:** Percentage increase in the accuracy of identity validation and verification methods compared to traditional approaches. • **Fraud Detection Rate:** Percentage of fraudulent identity attempts detected and prevented through the implemented blockchain solution. • **User Adoption:** Number or percentage of users who successfully adopt and utilize the blockchain-based identity validation system. • **Compliance Assurance:** Percentage of compliance with relevant regulations and data protection laws in relation to identity validation and verification processes. • **Operational Efficiency**: Reduction in the time and resources required for identity validation and verification compared to traditional methods.
Requirements to be addressed	• **Scalability:** Ability of the blockchain-based identity system to handle a high volume of identity validation requests without compromising performance. • **Security:** Level of security provided by the blockchain system to safeguard sensitive user identity information from unauthorized access or tampering. • **User Experience:** Measurement of user satisfaction with the identity validation and verification process on the blockchain, considering factors such as ease of use and speed. • **Integration Capability:** Successful integration of the blockchain-based identity validation system with existing business processes and systems. • **Cost-effectiveness:** Reduction in costs associated with identity validation and verification compared to traditional methods, taking into account factors such as infrastructure, personnel, and maintenance.
Expected outcomes at the level of your solution	• **Identity Fraud Reduction:** Percentage decrease in instances of identity fraud due to the implementation of the blockchain-based identity validation system.

	• **Time Efficiency:** Reduction in the time required for identity validation and verification processes, leading to faster customer onboarding and transaction processing. • **Cost Savings:** Monetary savings achieved by utilizing blockchain technology for identity validation and verification, such as reduced operational costs and fraud-related expenses. • **Trust and Transparency:** Improvement in user trust through increased transparency and accountability in the identity validation and verification process on the blockchain.

3 TR3 – Cross -Boarder Data Transfer

TR3 - Cross-Border Data Transfer	
Definition	Overcoming legal barriers and challenges associated with cross-border data transfer while maintaining privacy and security in decentralized identity systems.
Challenges to be tackled	• **Compliance Rate:** This KPI measures the level of compliance with cross-border data transfer regulations and legal requirements. It assesses the extent to which the project successfully navigates and overcomes legal barriers associated with data transfer, ensuring adherence to privacy and security regulations. • **Data Breach Incidents:** This KPI tracks the number and severity of data breach incidents encountered during cross-border data transfer. It highlights the challenges in maintaining data privacy and security, providing insights into areas that require improvement to minimize the risk of data breaches. • **Legal Disputes and Litigation:** This KPI monitors the occurrence and resolution of legal disputes or litigation related to cross-border data transfer. It indicates the challenges and obstacles faced by the project in navigating legal barriers, and the effectiveness of strategies in mitigating legal risks. • **Data Transfer Delays:** This KPI measures the time taken for cross-border data transfers to be completed successfully. Delays can be caused by legal complexities, regulatory approvals, or technical challenges. Tracking data transfer delays provides insights into the efficiency of the project's processes and identifies areas for improvement.
Requirements to be addressed	• **Compliance Framework Implementation:** This KPI assesses the successful implementation of a comprehensive compliance framework for cross-border data transfer. It measures the extent to which the project adheres to relevant regulations, standards, and industry best practices in decentralized identity systems. • **Data Encryption and Security Measures:** This KPI evaluates the implementation of robust data encryption and security measures during cross-border data transfer. It ensures that the project meets the required standards to protect data privacy and security,

	including encryption protocols, access controls, and vulnerability management. • **Privacy Impact Assessments:** This KPI tracks the completion of privacy impact assessments for cross-border data transfer. It demonstrates the project's commitment to identifying and mitigating privacy risks associated with decentralized identity systems, ensuring compliance with privacy regulations and protecting individuals' personal data. • **Data Localization Compliance:** This KPI evaluates the project's adherence to data localization requirements in different jurisdictions. It measures the project's ability to store and process data within the specified geographical boundaries, as mandated by applicable laws, while still enabling efficient cross-border data transfer.
Expected outcomes at the level of your solution	• **Increased Cross-Border Data Transfer Efficiency:** This KPI measures the improvement in the efficiency and speed of cross-border data transfer processes. It reflects the successful implementation of strategies and technologies to overcome legal barriers, resulting in streamlined and faster data transfers while maintaining privacy and security. • **Enhanced Data Privacy and Security:** This KPI assesses the level of improvement in data privacy and security measures during cross-border data transfer. It indicates the successful implementation of robust safeguards, encryption protocols, and access controls to protect sensitive information from unauthorized access and data breaches. • **Regulatory Compliance:** This KPI measures the project's adherence to cross-border data transfer regulations and legal requirements. It reflects the project's ability to navigate legal barriers effectively, ensuring compliance with privacy, security, and data protection regulations in decentralized identity systems. • **Minimized Legal Risks:** This KPI evaluates the project's success in minimizing legal risks associated with cross-border data transfer. It reflects the effectiveness of strategies, such as legal assessments, contractual agreements, and risk mitigation plans, in reducing the potential for legal disputes, litigation, and penalties.

4 TR4 - Infrastructure and Resource Requirements

TR4 - Infrastructure and Resource Requirements	
Definition	Addressing the resource-intensive nature of blockchain technology and finding solutions to reduce the computational and storage requirements for decentralized identity systems.

Challenges to be tackled	• **Time-to-Solution:** Measure the time taken to identify and address resource-intensive challenges in blockchain technology for decentralized identity systems. • **Cost Optimization:** Track the reduction in costs associated with computational and storage requirements for implementing decentralized identity systems on the blockchain. • **Scalability Improvement:** Assess the improvements achieved in the scalability of blockchain-based decentralized identity systems by mitigating resource-intensive challenges. • **Error Reduction:** Monitor the decrease in errors or inefficiencies caused by resource-intensive demands, ensuring smoother operations for decentralized identity systems.
Requirements to be addressed	• **Resource Utilization:** Measure the efficiency of resource allocation and utilization for decentralized identity systems on the blockchain. • **Hardware/Software Upgrades:** Track the implementation of necessary upgrades or modifications to infrastructure and software to meet the resource requirements of decentralized identity systems. • **Compatibility:** Assess the level of compatibility between existing infrastructure and the resource requirements of blockchain-based decentralized identity systems. • **Training and Knowledge Transfer:** Monitor the effectiveness of training programs aimed at equipping staff with the skills and knowledge required to manage the resource requirements of decentralized identity systems.
Expected outcomes at the level of your solution	• **Performance Enhancement:** Measure the improvement in the overall performance of decentralized identity systems on the blockchain after addressing resource-intensive challenges. • **Cost Reduction:** Track the reduction in operational costs associated with computational and storage requirements for decentralized identity systems. • **Increased Adoption:** Monitor the growth in adoption rates of decentralized identity systems as a result of addressing resource-intensive challenges and improving efficiency. • **Enhanced User Experience:** Assess the user satisfaction and feedback regarding the improved performance and reduced resource requirements of decentralized identity systems on the blockchain.

5 TR5 – Interoperability

TR5 - Interoperability	
Definition	Ensuring compatibility and seamless integration between different decentralized identity systems and blockchain platforms to enable cross-platform usage.

Challenges to be tackled	• **System Compatibility:** Measure the percentage of decentralized identity systems and blockchain platforms that are incompatible or face challenges in integrating with each other. • **Integration Time:** Measure the time taken to integrate different decentralized identity systems and blockchain platforms. • **Data Interoperability:** Assess the level of data compatibility and interoperability between different decentralized identity systems and blockchain platforms. • **Technical Hurdles:** Identify and track the number of technical challenges encountered during the interoperability implementation process. • **Stakeholder Alignment:** Measure the level of alignment and collaboration between stakeholders involved in the interoperability efforts.
Requirements to be addressed	• **Standards Compliance:** Monitor the adherence of different decentralized identity systems and blockchain platforms to industry standards and protocols for interoperability. • **Scalability:** Assess the scalability capabilities of the integrated systems to handle increased usage and growing demands. • **Security:** Ensure that the interoperable systems meet the required security standards and protocols. • **Performance:** Measure the performance metrics, such as transaction speed and throughput, of the interoperable systems. • **Usability:** Evaluate the user-friendliness and ease of use of the interoperable systems for end-users.
Expected outcomes at the level of your solution	• **Cross-Platform Compatibility:** Measure the successful integration and compatibility between different decentralized identity systems and blockchain platforms. • **Seamless Data Exchange:** Assess the ease and efficiency of data exchange between the integrated systems. • **Enhanced User Experience:** Monitor the improvement in user experience resulting from interoperability, such as streamlined processes and reduced friction. • **Increased Adoption:** Measure the growth in adoption of decentralized identity systems and blockchain platforms due to enhanced interoperability. • **Cost Efficiency:** Assess the cost savings achieved by leveraging interoperability, such as reduced development and maintenance costs.

6 TR6 - Legal Frameworks and Jurisdiction

TR6 - Legal Frameworks and Jurisdiction	
Definition	Navigating the legal landscape to ensure compliance with existing regulations and adapting to emerging regulatory frameworks related to decentralized identity and blockchain technology.

Challenges to be tackled	• **Regulatory Complexity:** KPI: Number of existing regulations and emerging regulatory frameworks related to decentralized identity and blockchain technology that need to be navigated and complied with. • **Legal Uncertainty:** KPI: Percentage of legal uncertainty or ambiguity regarding the application of existing regulations to decentralized identity and blockchain technology, requiring further clarification or guidance. • **Compliance Risk:** KPI: Number of compliance risks identified, such as potential penalties, fines, or legal actions due to non-compliance with applicable regulations. • **Jurisdictional Variations:** KPI: Number of jurisdictional variations in legal frameworks related to decentralized identity and blockchain technology, which may require separate compliance strategies for different regions or countries.
Requirements to be addressed	• **Legal Expertise:** KPI: Level of legal expertise and knowledge required to navigate and interpret the existing regulations and emerging frameworks related to decentralized identity and blockchain technology. • **Compliance Framework:** KPI: Development and implementation of a comprehensive compliance framework that ensures adherence to relevant legal requirements and regulatory standards. • **Regular Updates:** KPI: Frequency of updates and adjustments made to the compliance framework to address changes in existing regulations and emerging regulatory frameworks. • **Documentation and Record-Keeping:** KPI: Adequacy of documentation and record-keeping practices to demonstrate compliance with legal requirements and facilitate audits or regulatory reviews.
Expected outcomes at the level of your solution	• **Compliance Assurance:** KPI: Percentage of compliance with applicable legal frameworks and regulations related to decentralized identity and blockchain technology achieved within the project. • **Risk Mitigation:** KPI: Reduction in compliance risks associated with non-compliance, penalties, fines, or legal actions through effective navigation of the legal landscape and adherence to emerging regulatory frameworks. • **Adaptability to Changes:** KPI: Ability to adapt to emerging regulatory frameworks and changes in legal requirements related to decentralized identity and blockchain technology. • **Legal Efficiency:** KPI: Improvement in the efficiency and effectiveness of legal processes, including the ability to identify, interpret, and apply relevant legal frameworks and regulations accurately.

7 TR7 – Standardisation

TR7 - Standardisation	
Definition	Complying to standards and actively follow/contribute to standardization activities in the areas of decentralized identity systems, wallets, verifiable credentials, reputation-based identities, DAOs and/or relevant ontologies.
Challenges to be tackled	• **Adoption Rate:** Measure the percentage of organizations or industry participants that have adopted the standardized protocols for decentralized identity. This KPI reflects the level of difficulty in convincing stakeholders to embrace and implement the new standards. • **Resistance to Change:** Assess the level of resistance or pushback from industry players or organizations in adopting the standardized protocols. This KPI helps identify potential barriers or challenges that may hinder the widespread acceptance of the new standards. • **Technical Complexity:** Quantify the complexity of implementing the standardized protocols for decentralized identity. This KPI assesses the technical challenges involved in integrating the protocols into existing systems and infrastructure. • **Industry Consensus:** Gauge the level of consensus and agreement among industry stakeholders regarding the standardized protocols. This KPI measures the challenges in aligning diverse perspectives and reaching a common understanding of the protocols' importance and benefits.
Requirements to be addressed	• **Compliance Rate:** Measure the percentage of organizations or industry participants that have successfully implemented the standardized protocols for decentralized identity in compliance with the established requirements. This KPI ensures that the standards are met uniformly across the industry. • **Interoperability Level:** Assess the degree to which different systems and platforms can seamlessly interact and exchange decentralized identity information using the standardized protocols. This KPI reflects the effectiveness of the protocols in enabling interoperability among various stakeholders. • **Regulatory Adherence:** Evaluate the extent to which the standardized protocols for decentralized identity comply with relevant regulations and industry-specific requirements. This KPI ensures that the protocols meet regulatory standards and promote harmonization within the industry. • **Scalability:** Measure the ability of the standardized protocols to handle increased usage and growth in the volume of decentralized identity transactions. This KPI assesses the scalability requirements to accommodate the expanding adoption and usage of decentralized identity systems.

Funded by the European Union

Expected outcomes at the level of your solution	• Contributions to W3C standards related to DID/VC • Contributions to emerging EU standards, e.g., eIDAS2 related standards • Other possible standards from the domain of the funded projects

8 TR8 - Usability and User Experience

TR8 - Usability and User Experience	
Definition	Designing user-friendly interfaces and seamless experiences for individuals to easily manage their decentralized identities and interact with blockchain-based services.
Challenges to be tackled	• **User Adoption Rate:** Measure the percentage of users who successfully adopt and use the decentralized identity management solution. • **User Satisfaction:** Conduct user surveys or feedback mechanisms to gauge user satisfaction with the usability and user experience of the interface. • **User Onboarding Time:** Track the time it takes for new users to onboard the decentralized identity management system and interact with blockchain-based services. • **User Error Rate:** Monitor the frequency and nature of user errors or mistakes encountered while using the interface, aiming to minimize and address them. • **Training and Support Effectiveness:** Assess the effectiveness of training materials and support mechanisms in helping users understand and navigate the decentralized identity management system.
Requirements to be addressed	• **Responsiveness:** Measure the speed and performance of the interface, ensuring quick response times and smooth interactions. • **Accessibility:** Evaluate the interface's accessibility features, such as support for assistive technologies and compliance with accessibility standards. • **Intuitive Navigation:** Assess the ease of navigation within the interface, ensuring logical flow and intuitive user journeys. • **Consistency:** Monitor the consistency of design elements, layout, and terminology across the interface to provide a cohesive user experience. • **Multi-platform Compatibility:** Ensure the interface works seamlessly across different platforms and devices, such as desktops, mobile devices, and tablets.
Expected outcomes at the level of your solution	• **Increased User Engagement:** Measure the level of user engagement with the decentralized identity management system and blockchain-based services. • **Reduced User Friction:** Monitor the reduction in user friction points, such as complex registration processes or confusing user

	interfaces. • **Improved Conversion Rates:** Track the conversion rates of users successfully completing desired actions or transactions within the system. • **Enhanced User Retention:** Assess the user retention rate, indicating the ability of the interface to retain and satisfy users over time. • **Positive User Feedback:** Collect positive user feedback through surveys, reviews, or ratings, indicating a favourable user experience and satisfaction with the interface.

9 TR9 – Scalability

TR9 - Scalability	
Definition	Designing decentralized identity systems that can handle a massive number of users and transactions without compromising performance and speed.
Challenges to be tackled	• **User Growth Rate:** Measure the rate at which the number of users in the decentralized identity system is increasing over time. • **Transaction Volume:** Track the total number of transactions processed within the system to assess its scalability in handling increasing transaction loads. • **Response Time:** Measure the time taken by the system to respond to user requests, ensuring that it remains within acceptable performance limits. • **Concurrent Users:** Monitor the number of simultaneous users accessing the decentralized identity system to ensure it can handle a large user base without degradation in performance.
Requirements to be addressed	• **Throughput:** Measure the number of transactions processed per unit of time to ensure the system meets the required performance levels. • **Latency:** Monitor the time taken for a transaction to be processed from initiation to completion, ensuring it meets the specified latency requirements. • **Scalability Testing:** Perform load and stress tests to evaluate the system's ability to handle increased user and transaction volumes while maintaining performance standards. • **Resource Utilization:** Monitor the system's resource usage (CPU, memory, network bandwidth) to ensure efficient utilization and identify potential bottlenecks.
Expected outcomes at the level of your solution	• **Scalability Index:** Develop a metric or index that quantifies the scalability level achieved by the decentralized identity system.

	• **Improved Performance:** Measure the improvement in response time and throughput compared to the system's initial performance before scalability enhancements. • **Increased User Base:** Monitor the growth in the number of users utilizing the decentralized identity system as a result of improved scalability, indicating its broader adoption. • **Cost Efficiency:** Evaluate the cost-effectiveness of the scalability enhancements by analysing the ratio of performance improvement achieved to the investment made in scaling the system.

2.5.2 Cross-Cutting Requirements

When implementing their projects, all the 13 selected projects will have to address the cross-cutting requirements according to the solution they envisioned:

- **CCR1 - User Centred Approach:** Implementation of a User Centred Approach
- **CCR2 - Legal, Regulatory and Ethical framework:** Adherence and compliance to the current legal, regulatory and ethical framework
- **CCR3 - Business Plan:** Design and evaluation of a business plan based on a detailed market and cost-benefit analysis in the TRUSTCHAIN context (see Annex 1)
- **CCR4 - Standardisation activities:** Leverage existing standards and/or contribute to standardisation activities in the TRUSTCHAIN context
- **CCR5 - Environmental sustainability:** Commitment to EU sustainable goal and six environmental objectives of the EU Taxonomy Regulation presented hereafter

1 CCR1 - User Centred Approach

CCR1 - User Centred Approach	
Definition	The approach that all the project funded by the OC1 digital identity are requested to follow is a human centred methodological path. It hast to be used in the different steps of the ICT tool development: from the definition of the use cases to the testing and piloting of the final tool. As Ortiz Crespo et al. (2020: 3) highlight, it avoids large gaps between design and reality. It is the reason why to ensure the success and, above all, the success of a decentralised digital identity tool, from a more technical point of view, the need to understand how to adapt a technology to the end-user needs and how to answer it throughout each digital identity solution. Each project will provide a trustworthy technology, behind the interface but also the effectiveness of the interface itself: content and UX wise.

	As it clearly appears in the research made by Roehrer et al. (2011) using user-centred design requires not only to involve the human from the beginning in the process and in all the steps, but it also requires a multidisciplinary work permitting the constant "translation" of the users' reality into technical requirement as to understand how to adapt the technological barriers as close as possible to the user's needs. What is important to take into account: To have a deep reflection about who are all the stakeholders, or kind of users, involved through the process and implicate them from the beginning in the process. Well, making them part of the process since the beginning may avoid making presumptions about their reality or their needs in terms of managing digital identity. As Roehrer (2011) it enables a holistic view of the problematic to be solved. To clearly link the functionality and the form (Roehrer, 2011). What does this mean for each project's methodology: **1. Concept testing and Definition of users** Starting from an extended state of the art, a qualitative approach must be followed to deeply understand the context of the specific topic that is build the decentralised digital identity. As exposed by Cremers et al. (2014: 35) cultural aspects, as are those previously mentioned, should be studied holistically, neither in isolation of their historically formed contexts, nor from one single point of view. It is the reason why, starting the research with a theoretical background is necessary, it outlines the contexts in which the problematic takes place and puts the foundations for the qualitative fieldwork in which the Human centred approach is based on. This qualitative fieldwork brings the cultural perspective within the research which allows the researcher to find out the triggers to apply within the technological projects the study is taking place. The qualitative fieldwork can take place as observation, individual or group interviews or focus groups. The best methodological tool to be used may result from the specific research questions coming out of the previously made theoretical research. **2. Definition of requirements** The outputs of the previous phase will be used as the base for defining the requirements that each project tool has to fulfil. Broader user involvement in concept thinking but also in the requirement definition may enable the findings of, otherwise, unidentified requirements (Roehrer, 2011). To define these requirements, scenarios of use will be defined looking after common patterns from the analysis of the qualitative research carried out with citizens. From these scenarios, user stories and requirement will be extracted. At this point, the multidisciplinarity of the team will be crucial in order to ensure the "translation" of the citizens need into feasible technological requirement, finding so, the correct balance. In the case it applies it may also be the moment to prioritize the requirements. **3. Platform interface design and prototype**

	Once the platform starts to be developed, mock-ups should be defined, phase by phase, to check on the flow and the design of the developed requirements. This should be done in an iterative way. Each new sprint may include the application (when possible) of the user's comments received in the previous iteration phase to test its convenience and the new designed requirements/flows may be tested. **4. Piloting** This phase takes place toward the end of the process and is more about testing the effectiveness of the concept itself, about if it responds as expected to the different stakeholders needs in a daily use. In this sense, it is very important to have its results feedback the platform definition itself. Maybe not so much the requirements themselves but how they are "translated" into the platform. It could be possible to combine quantitative methodologies during the research if it's correctly justified. But the majority the methods used must be qualitative such as focus groups, (group) interviews, observation, usability test among others. If a method will be carried out with a different sample and/or participants. It also must be correctly justified. For example, if it is more appropriate to do experts usability testing.
Challenges	There are several challenges that could appear when the projects are being carried out. Even though the qualitative and quantitative methods are complementary and necessary to have a holistic vision of the topic. It is necessary to follow a qualitative approach to deeply understand the context of the specific topic that is build the decentralised digital identity and the end-users needs. That could suppose a challenge if you have defined your sample with a wide number of participants. Another challenge could be the access to the end-users. That means that only one team, usually not the research team, has direct contact with the users. In addition, consideration has to be given to the possibility that, when dealing with digital identity issues, users may feel reluctant about the use of their data, transparency issues with developers, and so on. To avoid such reluctance in validation sessions, one possible way is to ask them to try it out without the need for them to register. Constructing a UCD, could be a challenge because the design must be empathetic. An all the sections, buttons, and functions must be fully interrelated. And, afterwards, the research team could end up with conflicting needs of different end- user groups. Analysing the common points and the dissident points will be crucial to combine the requirements and create a usable design for every end-user group. In order to overcome the challenges, it is necessary a multidisciplinary design, field research users and a collaborative design techniques.

Requirements	A decentralised user identity management that has successfully implemented a user centred approach during the parts of the project that will be developed during the OC1 work time. During the 9 months the projects need to develop their solution. To do so, implementing the UCD, the first step is to create a roadmap with the methodologies that suits better with the projects' objectives and the phase in which the project team will gather information about the participants. Once it is defined the different methods, then it needs to be defined the sample. The sample needs to be representative. Representativeness can be achieved either through sample selection or through sample size. The different methods to be followed should be mostly qualitative research methods. It is possible to complement the data collected in the qualitative sessions with other quantitative methods. These can only be complementary. Another requirement is the inclusion of users or potential users during the co-creation phase (if applicable) and the validation phase Include users or potential users during the validations and the co-creation phase of the tool. Complementarily, insights can be proposed by non-users. This decision must be justified in the corresponding deliverable. The main requirement in the Open Call 1 is that all the tools are validated by the end- users of the decentralized digital identity solution. Once the tool is ready on a TRL 7 and the use case is completely developed, it must be validated. The validation process consists of conducted usability test, could be moderated or unmoderated. The last requirement involves iteration, in the case of digital solutions that are already created with a medium TRL, at least one iteration is sought, that is, a validation round with users in which the status of the tool is acknowledged and improvements implemented. In those projects that are going to carry out a preliminary study of needs identification and/or co-creation with the end users, it is required that the feedback from the users has been correctly implemented in the development of the digital solution.
Expected outcomes	It is expected that the project team frame the sample and the ideal candidates to participate in the research. Based on the representativeness requirement. The recruitment process needs to be defined and describe either for the co-creation/ ideation stage and/or the validation stage of the project. Also, it is expected a methodological roadmap, where are defined the specific methods to answer the project objectives. Also, all the pilot execution process must be described. And the analysis may. All the decision about UCD and the iteration must be reflected and justified. All the process should result in an empathetic user centred design result of all the research, that answer the end user real needs and it accomplish the highest standards of usability.

2 CCR2 - Legal, Regulatory and Ethical framework

CCR2 - Legal, Regulatory and Ethical framework	
Definition	All the projects funded by OC1 are required to comply with the legal, regulatory, and ethical framework which is relevant to the respective projects. Compliance with the legal and regulatory framework is of course evident, considering that everyone has to comply with the law. The ethical requirements are made equally binding, however, through the Horizon Europe legal and contractual framework. The legal and regulatory framework relevant in the context of OC1 is diverse and multilayered, whereby instruments at regional, national, and supranational level govern the way in which participants set up their projects, conduct research, collaborate, collect, and manage data, develop and market solutions and publish their findings. While it is virtually impossible to identify which legal instruments will apply to all selected projects, there are several EU-level instruments which can presumed to be at the heart of every selected project considering the topic of the call: **1. General Data Protection Regulation (GDPR; Regulation (EU) 2016/679)** It is to be expected, especially considering the requirement to adhere to the human-centric approach, that each and every project will process personal data in the sense of Article 4 GDPR. The mere fact of processing personal data, even when it is limited, as part of the project will trigger the application of the GDPR in full. Every participant will therefore have to assess which personal data are being processed, what the categories of data subjects are, whether a legal basis exists for the processing of these personal data (Art. 6 GDPR) or that – in case of special categories of data – an exception can be invoked (Art. 9 GDPR), that the quality requirements for processing are complied with (Art. 5 GDPR), that data subject rights are observed (Chapter III GDPR), that the necessary agreements between all stakeholders involved are concluded (Art. 26 and 28 GDPR) and that the rules on data transfers outside the European Economic Area are complied with (Chapter V GDPR). **2. eIDAS Regulation (Regulation (EU) 910/2014)** It is safe to assume that many projects will develop and/or provide solutions which qualify as trust services under the eIDAS Regulation. Such services include, among others, the provision of means for electronic identification, website authentication, electronic signatures, etc. Depending on the level of trust required in the service developed, different technical and organisational requirements will apply. For each project the participants will have to identify the type of solution/service they are developing and assess if and to what extent the eIDAS Regulation applies to their solutions. The eIDAS Regulation is currently under review, but in the meantime, it remains applicable as-is. **3. Network and Information Security Directive (NIS; Directive (EU) 2016/1148 and Directive (EU) 2022/2555 (also known as NIS 2)**

	The Network and Information Security Directive and its successor, NIS2, include cybersecurity obligations for provides which offer digital services (NIS) or essential or important services (NIS2) to the market. It is safe to assume that each and every solution will, at least to some extent, have to comply with the NIS obligations. In contrast to the other instruments mentioned above, the NIS and NIS2 are both Directives, not Regulations, meaning that the Member States have to transpose these instruments in national law. Hence, the participants will have to determine which Member State's law applies to their solution/service and assess which requirements for said law have to be implemented in the solution/service and/or the surrounding systems and processes. Participants should also bear in mind that the European Union is in the process of putting in place the Cyber Resilience Act, a new legal instrument which imposes requirements on the design, development and putting on the market of connected products and related services with regard to the cybersecurity and vulnerability characteristics of these products and services. **4. Other rules which may be of interest** Apart from the three instruments mentioned above, other legislation which may be highly relevant, relates to consumer protection law, rules related to digital services, the protection of intellectual property and the protection of trade secrets. It is first and foremost the task of every participant to identify the legal obligations applicable to the project and act accordingly. The TRUSTCHAIN Consortium will assist, where possible, with advise whenever participants have targeted questions in relation to the legal framework applicable to them. In terms of the ethical considerations which may be relevant in TRUSTCHAIN, it would seem that concerns in relation to privacy and data protection are most pressing and relevant. Hence, participants should observe the data protection requirements under the GDPR as outlined above in order to ensure that the ethical considerations are complied with as well.
Challenges	The main challenge to overcome in relation to the ethical, legal and regulatory framework, is first to correctly identify and acknowledge which legal, regulatory and ethical obligations apply to the project. Secondly, the necessary notices, policies, procedures and contracts will have to be drafted to ensure that the legal requirements are met. Participants may need to seek assistance from legal experts to understand which rules are to be complied with when carrying out their project and to draft the aforementioned documentation.
Requirements	The participants should be able to demonstrate that the legal, regulatory and ethical requirements relevant to the project have been identified and have been complied with.
Expected outcomes	The relevant notices, policies, procedures, and contracts should have been drafted and put in place wherever necessary to ensure compliance.

3 CCR3 – Business Plan

CCR3 - Business Plan	
Definition	All projects funded by OC1 are expected to deliver mature prototype solutions in an operational environment (TRL7), which are close to the market. Towards the business exploitation of the OC1 project results, the projects should study and report on their market context in terms of market size, their value proposition, their potential competitors, their potential partners, and the business models of their competition. The OC1 projects should collect realistic cost and benefit parameters from the market to employ in their economic analysis. More information on the business analysis methodology will be found in the Annex.
Challenges	The main challenge is for projects to clearly describe, their customers, their competitive advantage, and their added value, as related to the competition, and their projected market share or market penetration in a convincing way. Another challenge would be to identify all the cost and revenue parameters so that they define cost and revenue streams for their solution, as well as different customer channels. Last but not least, their business model should be defined.
Requirements	The participants should perform a comprehensive market analysis and clearly position their solution to the market. Also, specific realistic market penetration scenarios should be defined. Economic analysis tools such as business model canvas, value chain/network, SWOT/TOWS analysis, cost/benefit analysis, and more should be employed.
Expected outcomes	Each OC1 project should deliver (at least) the following: • Market overview • Business model canvas • Value network • Cost-Benefit Analysis (based on realistic tariffs/costs and market penetration scenarios) • Risk analysis

4 CCR4 - Standardisation activities

CCR4 - Standardisation activities	
Definition	TRUSTCHAIN intends to contribute to industry-wide standards and protocols for decentralized identity to facilitate interoperability, compliance, and regulatory harmonization in particular for DID/VC in relationship to eIDAS2
Challenges	Integrate ability for DID methods to serve aspects of the digital identity
Requirements	Proofs (e.g. proofs of location, proofs of presence, proofs of passed examination) Zero-knowledge proofs (e.g. the final outcome of a process that only asserts that the goal has been achieved without providing any details about the process and its data)

	Reputation management (e.g. data which is not connected to the actual identity and does not allow the identity to be discovered in any way) Integration of Smart Oracles (e.g. the use of Internet of Things sensors in the processing of DID/VC methods) Proximity solutions (e.g. the use of DID/VC methods when no connection to the Internet is possible) High-level ontology that can be used to address process, cost, proof, and any other aspect of the TRUSTCHAIN use cases
Expected outcomes	Contribution towards the DID/VC standards of the W3C

5 CCR5 - Environmental sustainability

CCR5 - Environmental sustainability	
Definition	The TRUSTCHAIN ecosystem is intended to be designed in a way it is not significantly harming any of the six environmental objectives of the EU Taxonomy Regulation presented hereafter. • Mitigation means making the impacts of climate change less severe by preventing or reducing the emission of greenhouse gases (GHG) into the atmosphere. • Climate change adaptation means altering our behaviour, systems, and—in some cases—ways of life to protect our families, our economies, and the environment in which we live from the impacts of climate change. The more we reduce emissions right now, the easier it will be to adapt to the changes we can no longer avoid. • Ocean sustainability embodies the approach required to manage our oceans and the services they provide. The oceans and in particular their coastal areas are an essential component of the Earth's ecosystem hosting between 500,000 and 10 million species that provide a wide range of ecosystem services. • Circular economy is an economic system based on the reuse and regeneration of materials or products, especially as a means of continuing production in a sustainable or environmentally friendly way. • Pollution Prevention means eliminating or reducing the amount and toxicity of potentially harmful substances at their sources, prior to generation, treatment, off-site recycling or disposal. • Biodiversity conservation protects plant, animal, microbial and genetic resources for food production, agriculture, and ecosystem functions such as fertilizing the soil, recycling nutrients, regulating pests and disease, controlling erosion, and pollinating crops and trees.
Challenges	The EU Taxonomy Regulation on Environmental Sustainability has been invented to provide directions that could be complemented with Key Performance Indicators (KPIs).

Funded by the European Union

	TRUSTCHAIN technologies, due to their inherent decentralization, may stimulate new solutions to provide a sustainability level that has been beyond humanity reach until this point. The challenge that we face is therefore to implement our TRUSTCHAIN solutions to tackle the environmental objectives of the EU Taxonomy Regulation.
Requirements	Solutions which, as compared to alternative ones, satisfy one or more of the following: • Consume less energy. • Have a longer life expectancy and reusability potential. • Enable the peer-to-peer and/or the circular economy. • Save costs in terms of human activity and energy. • Promote/incentivise sustainable objectives in the energy, society or economy domains. • Enable other specific sustainable solutions.
Expected outcomes	New innovations that can be used to educate, stimulate, or incentivize people in the context of Environmental Sustainability and the goals of humanity in this context, or innovations that enable sustainable outcomes in economic, energy and/or the societal terms.

2.5.3 Key Performance Indicators

The following tables summarize overall the KPIs of the selected projects with their assessment grid. They should be assessed on a regular basis by the selected innovators. Some of the KPIs might not be relevant to some selected projects. In that case, it must be justified and discussed with the TRUSTCHAIN consortium. In any case this assessment should be submitted to the TRUSTCHAIN consortium each time requested (see section 5).

1 KPIs towards a more trustworthy and privacy-aware evolution of the internet

KPI	Can apply to your project? (Yes/No)	Specify your contribution (In a quantifiable and measurable way; Less than 30 words)
Which is the Trust Assessment Effectiveness, e.g., accuracy for labelling/inference of the trustworthiness subjects or for		

content, for your solution.		
How can you assess the privacy/anonymity of your solution? E.g., employing probabilistic metrics, anonymity set size, entropy, etc.		
Security guarantees on trustworthiness/privacy, e.g., security proofs.		
Did you employ/ implement zero knowledge proof protocols?		
How does your solution improve security and privacy, comparing with existing solutions?		

2 KPIS towards a more decentralized ngi

KPI	Can apply to your project? (Yes/No)	Specify your contribution (In a quantifiable and measurable way; Less than 30 words)
Did you implement new decentralised computing technologies for storing and accessing data, e.g., via the OAI-PMH protocol, that achieve high reliability, availability, Quality of Service, and similar properties necessary to realise new decentralised services?		
Did you implement new decentralised social networks?		
Did you implement new decentralised publishing platforms?		

Did you implemented new Digital Twin technologies that can help establish digital representation of the reality in specific circumstances where needed?		
How does your solution improve decentralization, and how that impacts with user experience, comparing with existing solutions?		
Have you investigated the scalability of your decentralized solution?		

3 KPIS towards sustainable business

KPI	Can apply to your project? (Yes/No)	Specify your contribution (In a quantifiable and measurable way; Less than 30 words)
Market penetration potential? # of pilot users, # of potential customers, # of competitors, # of partners, etc.		
Business model defined? Details should be mentioned, such as # of Business Use Cases (BUCs), # of BM canvases, # of BUCs analysed		
Profitability, e.g., ROI, NPV, payback period, etc.		
Crypto strategy? Token type? Crypto distribution?		

4 KPIS towards new forms of human-centered interaction and immersive environments for ngi users

KPI	Can apply to your project? (Yes/No)	Specify your contribution (In a quantifiable and measurable way; Less than 30 words)
Task Success rate. % of participants that successfully complete a task.		
User Adoption Rate. How many new users does the tool have? What percentage represents the new users?		
User Satisfaction. How satisfied are the users with the solution? What is the % of satisfaction?		
User error rate. How frequently users make mistakes during a specific task? Where the users face difficulties with the product?		
Time on task. How much time is the total learning time spent by the user to know how to use the solution?		
Navigation vs. search What the users prefer to do? Is the navigation process clear? How often do the users use the search function?		
System Usability Scale (SUS) questionnaire. How usable is your solution for the users?		

Net promoter Score. What is the % of likelihood that the users recommend the solution?		

5 KPIS related to the pilot studies

KPI	Can apply to your project? (Yes/No)	Specify your contribution (In a quantifiable and measurable way; Less than 30 words)
User Experience (UEQ questionnaire)		
# of pilot users		
User Engagement (# of transactions per user, freq. of use, etc.)		
# of interested users in future business collaboration		
# of paying users		
List of use cases in the pilot.		
User story: List of actions accomplished by users to complete the different use cases.		

6 Interoperabilty and standardization

KPI	Can apply to your project? (Yes/No)	Specify your contribution (In a quantifiable and measurable way; Less than 30 words)
Did you propose or could/will propose standards/drafts?		
Describe international events on standardization activities participated/contributed		
What digital identity standards to you focus on?		

What standards related to credentials do you focus on?		
Which Blockchain network(s) and Smart Contract language(s), did you use?		
Interoperability standards employed (syntactic interoperability)? Ontologies employed (semantic interoperability)?		
What interoperable data formats or communication protocols were used if any in the implementation?		
Importance of interoperability in your solution? E.g., # of cross-chain transactions?		

7 Legal and ethical compliance

KPI	Can apply to your project? (Yes/No)	Specify your contribution (In a quantifiable and measurable way; Less than 30 words)
All users are informed about the processing of their personal data. An information notice has been put in place.		
Users' consent is asked and stored whenever consent is the relevant legal basis to be used.		
The purposes for processing personal data have been well-defined, specified and are communicated to the users and		

no personal data is processed beyond what is needed for these purposes.		
Retention periods for users' personal data are well-defined and are communicated to the users.		
Personal data are kept accurate, complete and up to date.		
The necessary technical measures are taken to protect the personal data processed. Personal data are encrypted in transfer and at rest, where appropriate.		
All processors engaged provide adequate assurances and guarantees as required and the appropriate data processing agreements have been completed and signed.		
The processes are put in place to ensure compliance with data subject rights (e.g., right of access, correction, erasure, limitation, opposition, etc.).		
Personal data are only transferred to third countries to the extent that adequate protection can be foreseen.		
A record of processing activities is drawn up for the project and kept up to date.		
The necessary approvals and authorizations from the competent ethics and/or		

governmental bodies for the processing of personal data are sought and obtained.		

8 KPIS TOWARDS A GREENER NGI

KPI	Can apply to your project? (Yes/No)	Specify your contribution (In a quantifiable and measurable way; Less than 30 words)
Carbon footprint, e.g., greenhouse gas emissions comparing with existing solutions		
Consumption of energy		
Supply chain miles		
Saving life, improving biodiversity		
Waste reduction and recycling rates		
Sustainable outcomes in economic, energy and/or the societal terms achieved		
Environmental sustainability standards and policies, e.g., Green Energy Generation Initiatives, Sustainable Development Goals		
Addressing climate change? (yes/no)		

9 KPIS TOWARDS INNOVATION

KPI	Can apply to your project? (Yes/No)	Specify your contribution (In a quantifiable and measurable way; Less than 30 words)
Did you implement new innovative TRUSTCHAIN use cases?		
Did you implement new innovative TRUSTCHAIN reasoning technologies?		
Did you make any inventions in the framework of your project, in terms of patents, copyrights, design rights, trademarks, trade secrets, etc?		
Which are the most disruptive technology components of your solution?		

10 KPIS RELATED TO THE IMPLEMENTATION

KPI	Can apply to your project? (Yes/No)	Specify your contribution (In a quantifiable and measurable way; Less than 30 words)
Code simplicity (analyser used and results)		
Testability Coverage (method/tool used for testing and results)		

3 SUPPORT FOR THE OPEN CALL #1 WINNERS

To ensure an adequate integration of the technologies/solutions proposed by the selected applicant teams into the TRUSTCHAIN ecosystem, different layers of support have been defined:

- Coaching support
- Technical support with Alastria infrastructure
- Communication support

3.1 COACHING SUPPORT

3.1.1 Head coach role

A TRUSTCHAIN head coach is assigned to each OC1 winner (see section 3.1.2). The coach is the main TRUSTCHAIN contact point for the assigned applicant team, and will have the responsibility to support, guide, provide feedback, motivate, understand, and challenge the applicant team. More specifically, the head coach:

- Schedule weekly monitoring calls with their assigned selected innovator(s) (as described in detail in Section 5);
- Update the monitoring tool (described in Section 6.3);
- Connect their assigned selected innovator(s) with relevant other innovators to establish TRUSTCHAIN platform interoperability;
- Ensure that deliverables and milestones are submitted by their assigned selected innovator(s) at the end of each sprint (timekeeper);
- Engage their assigned selected innovator(s) on TRUSTCHAIN events;
- Liaise with the relevant TRUSTCHAIN partners based on their assigned selected innovator(s) needs;
- Attend the biweekly meeting for coaches to share experience and foster the support between coaches.

3.1.2 Head coach distribution per projects

The assignment of the selected projects per head coach and coaching team (TRUSTCHAIN consortium partner) is depicted in the table hereafter.

TABLE 2: SELECTED PROPOSALS AND ASSIGNED HEAD COACH

Proposals	Head Coach
DidRoom	AUEB
CreatorCredentials.cc	ALA
MUSAP	ICS
TREVO	AUEB
Orchestral	UL
The Social Wallet	ALA
DID4EU	UL
IM4DEC	ICS
WIDE	UL
CLIENT-DIDS	UL
EVI Electric Vehicle Identity	ICS
IS-CIS	ALA
PRIVÈ	NKUA

3.1.3 Coaching and collaboration organigram - Communication flow

One of the key points for the success of all the TRUSTCHAIN initiatives in the OC1 Frame as well as for coaching and different collaboration activities is good communication between the different parties. To assure this, a workflow of communication between the different stakeholders is proposed in the following figure.

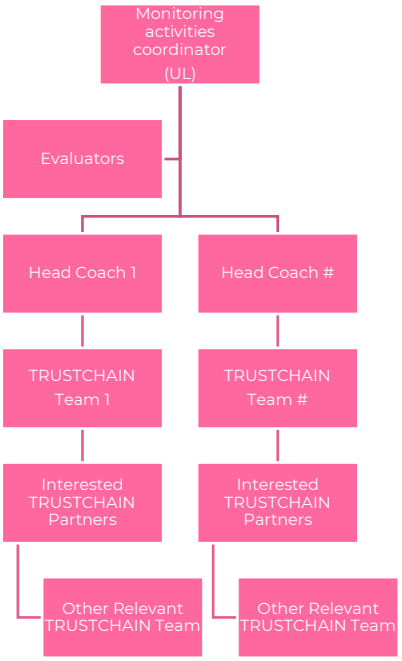


FIGURE 1: ORGANOGRAM OF THE COACHING/COLLABORATION ACTIVITIES IN TRUSTCHAIN.

3.2 TECHNICAL SUPPORT WITH ALASTRIA INFRASTRUCTURE

The available infrastructure, described in the Alastria's blockchain infrastructure for TrustChain document, will be live since the start of the first OC until the end of the last OC, with great system performance and uptime, improving every day with work of their employees and most active members. During this time any TrustChain participant will have access to this infrastructure in a Blockchain-as-a-Service (BaaS) manner, described in the Alastria Quick Reference for TrustChain document.

The following subsections include the description of the TrustChain consortium's Service Level Agreement (SLA) and Operational Level Agreement (OLA).

3.2.1 SLA: Service Level Agreement

Blockchain network scope

Alastria networks, based on Consensys' GoQuorum and Hyperledger Besu

technologies, are available to deploy blockchain based use case implementations.

Available IT infrastructure

Alastria's available IT infrastructure will ensure that there will be a different number of servers up to run the different needed nodes of Alastria networks. In addition, Alastria will ensure that enough servers will be up and running and up to date to enable good performance and great user experience for the selected projects that will use Alastria networks.

Available nodes

Regarding the available nodes, there will be a different number of nodes available. Alastria will ensure that enough nodes are active, updated and synchronised to enable good performance and great user experience.

SLA-related services

As part of the SLA, the TrustChain consortium will provide the following SLA-related services:

- **Documentation and examples about developing and deploying use cases:** Alastria will provide enough documentation in the form of guides, tutorial, and practical examples, already available in public GitHub repositories.
- **Support by email and Slack channels:** Alastria will provide support via email as well as the dedicated Slack channels, where the developers could send their questions and request. Support will be available during the on-boarding period as well as the rest of the Open Call, during the use cases deployment on the blockchain networks.
- **Maintenance:** Maintenance is performed daily on Alastria networks to make sure that the network is active and updated all the time. Alastria will maintain the IT infrastructure, based on servers, and the hosted nodes to keep the network up and synchronised.
- **Issue reporting and tracking:** Alastria will internally track any issue reported by the available channels (email and Slack).

3.2.2 OLA: Operational Level Agreement

Selected teams can contact Alastria for any issues or questions on the networks in any of the following ways:

- **Direct contact via email or the dedicated Slack channels:** Support will be

available from 9:00 – 14:00 CET during workdays (Monday to Friday) except public holidays in the EU. Regarding response times, Alastria technical experts will provide an answer within 4 hours via email or on Slack.

- **Specific help request:** If any TrustChain participant could need special support, video calls could be scheduled to help them to successfully use the Alastria blockchain networks.

Incidents will be tracked and resolved internally. Alastria will inform when the issue is received, when work on it is started and when it is resolved.

3.2.3 Alastria networks monitoring and maintenance

Monitoring

Regarding networks monitoring and to be aware of the network use and status, as well as to solve potential issues as soon as possible, Alastria will monitor the networks with the help of different software tools.

Maintenance

As for networks maintenance and to ensure the optima health status and availability of the networks, and solve potential issues as soon as possible, Alastria will work every day in the networks, testing new components, updating software and solving bugs and other issues.

Availability

Alastria will work on the networks during work days from 9:00-17:00 CET (Monday to Thursday) and 9:00-14:00 CET (Friday). **24x7 support is not granted.**

3.3 COMMUNICATION SUPPORT

Each OC1 team will receive a communication toolkit from the F6S team, reference for all their communication/dissemination activities.

This kit is composed of the following:

- Press release template
- Social media content
- Co-branding suggestions
- NGI, TRUSTCHAIN and EU logos
- NGI textual recognition
- Official credits of the EU support

- Social media engagement information

For all other matters related to communication activities and community building, OC1 winners can refer to F6S.

4 MONITORING, FOLLOW-UP AND EVALUATION

4.1 DAY-TO-DAY COMMUNICATIONS

All OC1 team members will be invited to join a private Slack workspace where they can engage with the TRUSTCHAIN consortium members, coaches, and other participants. Slack is the preferred platform for day-to-day communications such as requesting help or asking questions to the other participants.

Three specific channels are open to OC1 innovators in Slack for communication.

 # TRUSTCHAIN-general

The **TRUSTCHAIN-general channel** is the one of the TRUSTCHAIN Community. The TRUSTCHAIN consortium, the OC1 Innovators and later on the innovators of the next OCs are all members of this channel. This is the place to share about TRUSTCHAIN in general, open discussion with OC1 innovators, exchange on specific orientations with all the TRUSTCHAIN Community, exchange experience and lessons learned.

 # OC1-general

The **OC1-general channel** is the one of the TRUSTCHAIN consortium and the OC1 Innovators. This is the place to share about TRUSTCHAIN OC1 in general. All information to be spread about TRUSTCHAIN OC1 to the consortium and/or to OC1 innovators are shared in this channel.

 # [project]

The **[project] channel** is a private channel only devoted to the direct sharing of information on the project itself between the related project team and its head coach and/or coaches that have been invited to the channel.

OC1 Team leaders are encouraged to provide their head coach with the list of team members who should be invited to this Slack workspace.

4.2 MONITORING, FOLLOW-UP AND EVALUATION PROCESS

In TRUSTCHAIN OC1, the monitoring, the follow-up and the evaluation activities will be sequenced by various reports and meetings defined hereafter.

The **kick-off meeting** will mark the start of the OC1 projects and will be held on the 14th of July, 2023. It aims to present the TRUSTCHAIN OC1 framework within the TRUSTCHAIN project and the implementation approach (e.g., support, coaching/monitoring, activities assessment, KPI etc.), expected outcomes for OC1 innovators, as well as to get to know with OC1 innovators. For this last purpose, OC1 innovators will take the floor to describe their project of the support, coaching/monitoring, and evaluation activities (OC1 Monitoring Supervisor and Head Coaches).

The **TRUSTCHAIN community meeting**, following the model of the kick off meeting intends to strengthen the links within the TRUSTCHAIN Community and ensure that TRUSTCHAIN overall goals are achieved. OC1 project outcomes will be presented to the whole community. This type of meeting, including the kick off meeting, is planned to take place a total of 3 times within the duration of OC1 projects.

To explore collaboration opportunities between relevant OC1 projects, coaches will elicit a collaboration intention report after the kick-off event where applicants state up to five projects that they would consider collaborating with and then encourage and organize meetings among them. Specifically, each applicant should explain in their collaboration intention report the following:

- The synergies with their selected five projects.
- The quality of the synergies.
- The level of the interoperability with these projects.
- The added value for TRUSTCHAIN of these synergies.

Overall, all along the OC1 implementation, OC1 innovators will be monitored and guided following a **SCRUM methodology** depicted in the following figure.

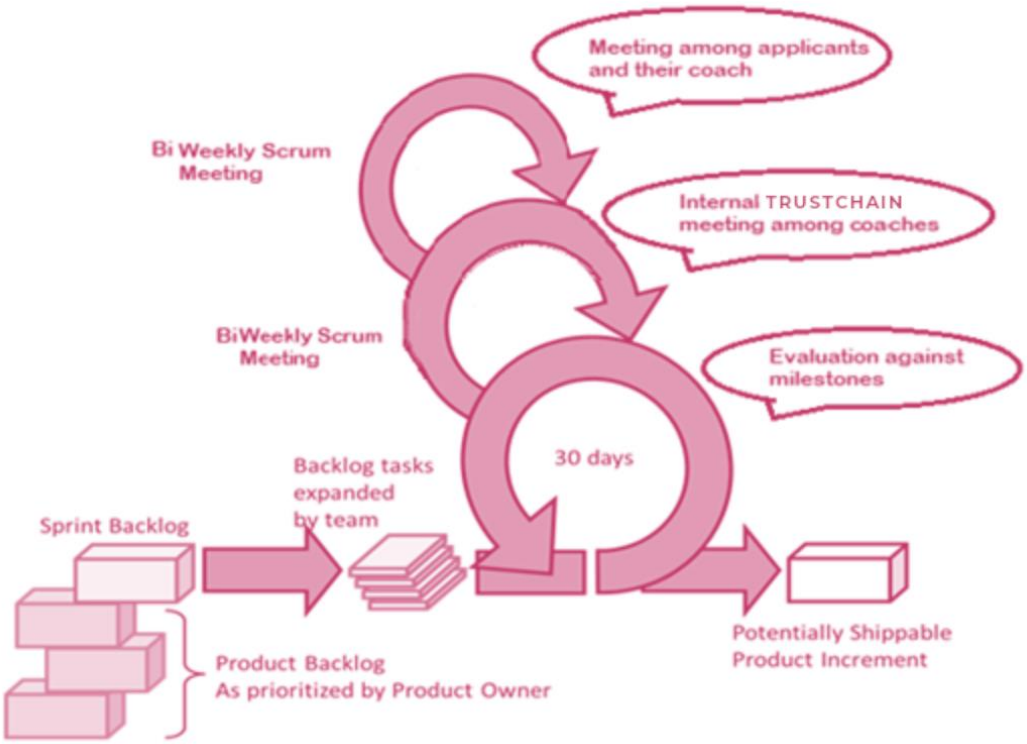


FIGURE 2: SCRUM GUIDANCE AND EVALUATION METHODOLOGY

Sprint phases have been defined for which the duration has been set to one month. Each OC1 team has defined milestones in their submitted proposals and agreed on KPIs with their Head Coach. These are the basis for monitoring and evaluating their work progress during the execution of their projects. On top, 4 deliverables are requested according to contractual terms and will be evaluated as described in the next section.

A sprint phase includes the following meetings:

- **Biweekly SCRUM meeting** with head coaches. The goals of these meetings are to assess OC1 teams progress since the previous two weeks and offer specific assistance (e.g., technical, business, communication or administrative) when needed. During these meetings, participants discuss current blockers. Head Coaches can suggest solutions in accordance with OC1 goals in real time or take the time for reflection and advice from other TRUSTCHAIN coaches (reasonable duration before the next scrum meeting) to unlock the issue quickly and in a relevant way according to OC1 goals. Different communication tools can be used for this purpose, but all-important items/tasks identified in each scrum meeting will be reported in the TRUSTCHAIN monitoring board of the considered sub

project i.e., Agile board template of the GitHub KANBAN software (see section 6.3 Monitoring tool)

Frequency: recurring biweekly meeting. A meeting slot should be identified between the Head Coach and the team and be available on a biweekly basis. In case no team member can join the biweekly scrum meeting, they must inform their coach at least 24 hours before the planned time and provide availability for the next 72 hours.
Who: The Head Coach and the team, other coaches if deem necessary.
Tool: Any communication/video conference tool as far as agreed by the Head Coach and the Team (virtual meeting room to be agreed) and the GitHub KANBAN project Agile board to report on.
Duration: No more than 30 minutes.

- **SPRINT meeting**: SPRINT meeting is no more than a particular SCRUM meeting. They occur the last week of each sprint at the usual time slot defined for the biweekly SCRUM meeting. The selected OC1 team:
  - present an overview of the work accomplished in the previous sprint as compared to the planned one,
  - show the progress in the respective phase of the project against the KPIs.
  - expose the synergies with their selected five projects, the level of the interoperability with these projects, the added value for TRUSTCHAIN of these synergies.
  - discuss any deviation and how they are handled.
  - answer questions from the coaches.
  - Receive feedback from the coaches.
  - prioritize tasks for the next sprint.

  The typical duration of this sprint meeting is however of a maximum of 1 hour.

- **Coaches' Biweekly meetings** will be held online among all TRUSTCHAIN coaches to update each other on the progress of the OC1 projects that they supervise, to identify common challenges, outline improvement strategies, share experiences and good practices. Any project will be summarised in a slide by the project head coach, followed by a discussion. The project head coach will record the minutes of the discussion about the concerned project and take adequate action for the OC1 project.

  Frequency: Recurring biweekly meetings.
  Who: The Head Coaches only.
  Tool: Any communication/video conference tool agreed between the Head Coaches.
  Duration: No more than 30 minutes.

- **Biweekly Plenary Meetings:** TRUSTCHAIN intend to embed key humanity principles in the co-creation of the Next Generation Internet and to provide autopoietic, evolutionary, decentralised, and therefore democratic, transparent, traceable, and regulatory compliant mechanisms that can support any ecosystem of entities and actors participating with their digital identities. With that respect, cross-cut aspects related to the user centricity of the ecosystem, to the legal & regulatory framework around digital decentralised identity and data sharing, to standards, interoperability and greenness of the ecosystem or business plan is crucial. To follow up on these aspects and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network, biweekly plenary meetings will also take place.

  Goal: Consensus on common approaches and technologies to be used in the project; Discussion about any open issues proposed by any parties whether about the User Centric design, the legal regulatory framework, the business aspects, or standards to follow/contribute to; to strengthen a common vision about the TRUSTCHAIN ecosystem; to foresee a common understanding of the TRUSTCHAIN business models, etc.
  Frequency: Recurring biweekly meetings.
  Who: Organised by the TRUSTCHAIN technical coordinator with the following participants: TRUSTCHAIN consortium, whole TRUSTCHAIN community.
  Tool: Virtual meeting room to be agreed.
  Duration: maximum 1 hour.

TABLE 3: MEETING TYPES IN OC1.

Meeting name	Meeting objectives	Frequency	Head Coach (Rapporteur)	Coaches	OC1 Innovators	Community
TRUSTCHAIN Community Meeting	Socialize and fulfil TRUSTCHAIN overall goals	3 times	Everyone			
Scrum meeting	Heads up	Bi-weekly	✓	✓	✓	
Sprint retrospective / planning	Planning	Monthly	✓	✓	✓	
Coaches Meeting	Progress tracking	Bi-weekly	✓	✓		
Plenary Meetings	Plenary Topic-Specific Sessions	Bi-weekly	✓	✓	✓	

4.3 EVALUATION OF OC1 DELIVERABLES

During TRUSTCHAIN OC1, 4 deliverables must be released by each OC1 Team. **According to the deadlines confirmed by the Head Coaches, OC1 teams will release their deliverables via email to their head coach and save them in their OC1 own repository in SharePoint** (see Section 6.1). TRUSTCHAIN evaluators will then evaluate them, have respective meetings with the OC1 teams if necessary and produce an evaluation report to approve or disapprove the submitted deliverables with recommendation for improvement action when needed. Financial support will be only granted if the deliverables have been approved by the evaluators. The deadlines of the various deliverables are depicted in Table below.

TABLE 4: PROJECT DELIVERABLES DESCRIPTION AND DEADLINES

Title	Deadlines
D1. State of the art overview, use case analysis and preliminary technical specification of the solution. The document should clearly specify how the proposed solution extends and/or upgrades the state-of-the-art.	M2
D2: Detailed technical specification of the solution, software implementation work plan, demo scenarios, the number of end users that will be involved in any pilots, and preliminary business plan.	M4
D3: Implementation, deployment in an appropriate TRUSTCHAIN platform, testing, demonstration, and validation roadmap in a real-life application (i.e., banking, education, healthcare, utilities, defence, or cross-border travel).	M7
D4: Modularised software components ready for distribution, full documentation for developers/users, final business plan and result of the validation process.	M9

- **For the Deliverable 1 "State of the art overview, use case analysis and preliminary technical specification of the solution." (D1) the expected outcomes are:**
  - User stories and use case analysis.
  - Clear explanation of the proposed functionality/application and why it is needed.
  - Clear specification of background (software) and foreground (developments within TRUSTCHAIN)

- Software design and analysis, component specification (preliminary)
- Detailed work plan for implementation and deployment (preliminary)

The KPIs for this deliverable are:
- Adequate review of related solutions and relevant state of the art.
- Draft solution specification and explanation of innovation as compared to the state of the art.
- Clear motivation for the proposed solution.
- Use case description detail.
- High-level software design quality.

- **For the Deliverable 2 "Detailed technical specification of the solution, software implementation work plan, demo scenarios, the number of end users that will be involved in any pilots, and preliminary business plan." (D2) the expected outcomes are:**
  - User stories and use case analysis.
  - Software design and analysis, component specification (final)
  - Detailed API specification (preliminary)
  - Detailed work plan for implementation and deployment (final)
  - Risk Analysis in the implementation work plan.
  - Cost and revenue streams and parameters.
  - Business Model and Exploitation plan (early)
  - Early User Engagement Plan (particularly for applications)
  - Sample definition for the end-user validation.

  The KPIs for this deliverable are:
  - Technical Depth (Excellence and Completeness): Functionality, Technical Soundness, Detail of Specification, Low Solution Complexity
  - Impact (Business Value for TRUSTCHAIN (including BM) and any other impact, e.g., Technological, Socio-Economic, Environmental, etc.), and
  - Implementation plan (Feasibility, Modularity, Interoperability within TRUSTCHAIN, Proximity/Relevance to Blockchain)

- **For the Deliverable 3 "Implementation, deployment in an appropriate TRUSTCHAIN platform, testing, demonstration and validation roadmap in a real-life application (i.e., banking, education, healthcare, utilities, defence or cross-border travel)." (D3) the expected outcomes are:**
  - Detailed API specification (final)
  - Software code of the solution
  - Evaluation Methodology and/or Experimental Design
  - Roadmap of the pilot studies with real users/ customers
  - Description of Pilot Studies with Real Users/Customers (mandatory for all applications, desirable for core functionalities)

- Early Demo and/or Initial Experimental (or Analytical) Results

The KPIs for this deliverable are:
- Software code delivery (mandatory)
- API specification and software documentation (mandatory)
- Demonstration of Prototype Software and/or Experimental (or Analytical) Results (mandatory)
- Clear and viable plan for pilot experiments with real users
- Moreover, D3 should evaluate the solution outcomes according to the KPIs provided in the Annex (when applicable)

- **For the Deliverable 4 "Modularised software components ready for distribution, full documentation for developers/users, final business plan and result of the validation process." (D4) the expected outcomes are:**
  - Full software documentation
  - Clean software code of production quality (TRL 7)
  - Final Demo
  - Business Model and Exploitation plan (final)
  - Economic analysis
  - Impact Assessment
  - Pilot Studies Results (mandatory for all applications, desirable for core functionality)

  The KPIs for this deliverable are:
  - Final software code delivery (mandatory)
  - Full API specification and software documentation delivery (mandatory)
  - Solution demonstration
  - Positive Pilot Studies Results
  - Impact Assessment and Business Potential
  -

5 TIMELINE

Weekly SCRUM meetings are omitted from the table below for clarity. The meeting dates must be treated in a tentative manner, while the deliverable deadlines are hard.

TABLE 5: MEETINGS AND DEADLINES TIMETABLE

Sprint #	Activity	Description	When	Who is involved
1	Projects kick-off	Presentation of TRUSTCHAIN project, TRUSTCHAIN Architecture, services and functionalities, OC1 project pitches, OC1 guidelines for implementation	**14/07/2023**	OC1 Beneficiaries, TRUSTCHAIN Coaches, TRUSTCHAIN Projects Coordinator
1	Sprint Planning Meeting	Online meeting to assess the subproject progress	**17-21/07 /2023**	One OC1 Team and their Coaches
1	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**24-28/07 /2023**	OC1 Coaches
1	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**24-28/07 /2023**	OC1 Beneficiaries, Coaches
1	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**07-11/08 /2023**	OC1 Coaches
1	Biweekly Plenary Meetings	Follow up the integration activities and elicit	**07-11/08 /2023**	OC1 Beneficiaries, Coaches

Funded by the European Union

		challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network		
2	Sprint Planning Meeting	Online meeting to assess the subproject progress	**14-18/08 /2023**	One OC1 Team and their Coaches
2	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**21-25/08 /2023**	All Coaches
2	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**21-25/08 /2023**	OC1 Beneficiaries, Coaches
2	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**04-08/09 /2023**	All Coaches
2	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**04-08/09 /2023**	OC1 Beneficiaries, Coaches
2	Delivery of the D1		**08/09/2023**	OC1 teams

3	Sprint Planning Meeting	Online meeting to plan the subproject progress	**11-15/09 /2023**	One OC1 team and their Coaches
3	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**18-22/09 /2023**	All Coaches
3	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**18-22/09 /2023**	OC1 Beneficiaries, Coaches
3	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**02-06/10 /2023**	All Coaches
3	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**02-06/10 /2023**	OC1 Beneficiaries, Coaches
4	Sprint Planning Meeting	Online meeting to assess the subproject progress	**09-13/10 /2023**	One OC1 Team and their Coaches
4	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**16-20/10 /2023**	All Coaches

4	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**16-20/10 /2023**	OC1 Beneficiaries, Coaches
4	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**30/10/2023 - 03/11/2023**	All Coaches
4	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**30/10/2023 - 03/11/2023**	OC1 Beneficiaries, Coaches
4	Delivery of the D2		**03/11/2023**	OC1 teams
5	Sprint Planning Meeting	Online meeting to assess the subproject progress	**06-10/11 /2023**	One OC1 Team and their Coaches
5	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**13-17/11 /2023**	All Coaches
5	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of	**13-17/11 /2023**	OC1 Beneficiaries, Coaches

		the TRUSTCHAIN ecosystem/network		
5	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**27/11/2023 - 01/12/2023**	All Coaches
5	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**27/11/2023 - 01/12/2023**	OC1 Beneficiaries, Coaches
6	Sprint Planning Meeting	Online meeting to assess the subproject progress	**04-08/12 /2023**	One OC1 Team and their Coaches
6	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**11-15/12 /2023**	All Coaches
6	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**11-15/12 /2023**	OC1 Beneficiaries, Coaches
6	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**25-29/12 /2023**	All Coaches

6	Biweekly Plenary Meetings	*Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network*	**25-29/12 /2023**	OC1 Beneficiaries, Coaches *Beneficiaries, Coaches*
7	Sprint Planning Meeting	Online meeting to assess the subproject progress	**01-05/01 /2024**	One OC1 Team and their Coaches
7	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**08-12/01 /2024**	All Coaches
7	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**08-12/01 /2024**	OC1 Beneficiaries, Coaches
7	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**22-26/01 /2024**	All Coaches
7	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**22-26/01 /2024**	OC1 Beneficiaries, Coaches

7	Delivery of the D3		**26/01/2024**	OC1 teams
8	Sprint Planning Meeting	Online meeting to assess the subproject progress	**29/01/2024 - 02/02/2024**	One OC1 Team and their Coaches
8	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**05-09/02 /2024**	All Coaches
8	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**05-09/02 /2024**	OC1 Beneficiaries, Coaches
8	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**19-23/02 /2024**	All Coaches
8	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**19-23/02 /2024**	OC1 Beneficiaries, Coaches
9	Sprint Planning Meeting	Online meeting to assess the subproject progress	**26/02/2024 - 01/03/2024**	One OC1 Team and their Coaches
9	Biweekly meeting for coaches	Online meeting to collectively assess	**04-08/03 /2024**	All Coaches

		the monitoring activities		
9	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**04-08/03 /2024**	OC1 Beneficiaries, Coaches
9	Delivery of the D4		**15/03/2024**	OC1 teams
9	Final Review Meeting (Community meeting)	Online meeting to collectively assess the monitoring activities	**18-22/03 /2024**	All OC1 Long Projects Beneficiaries, Coaches

6 Repositories

6.1 PROJECT REPOSITORY

A specific OC1 repository has been created in SharePoint. In this repository, there is:

- **OC1-General:** Where all documents and material to be shared between TRUSTCHAIN consortium and OC1 projects can be stored (e.g., the contact list of OC1 Innovators, the OC1 guide for implementation and the OC1 Kick off meeting presentations are part of this repository.)

- **OC1-[Project]:** Each project has its own dedicated folders only accessible by the project itself and TRUSTCHAIN core members. The folder name is composed by the OC topic number and the project acronym as depicted in the previous figure. It is decomposed in six subfolders:

1. **Proposal:** Where the proposal submitted by the respective OC1 selected innovators is saved, and which contains the project details.
2. **Contract:** After the signature of the sub-grant agreement a copy of it will be saved in this folder.
3. **Deliverables:** The place to save the OC1 4 deliverables requested according to the agreement.
4. **Communication:** The folder to save all relevant material related to the OC1 innovators communication activities.
5. **Monitoring:** The folder to save any kind of material related to the follow-up and progress monitoring of the project.
6. **Evaluation reports:** The folder to save the different evaluations reports done by the evaluators in reference to the different deliverables.

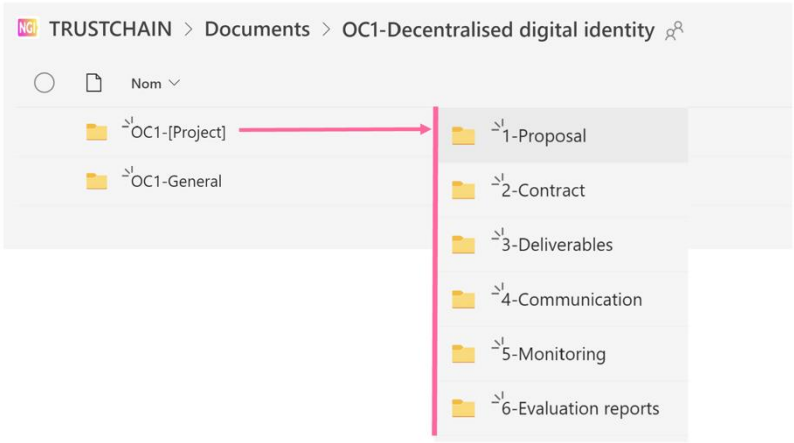


FIGURE 3: TEAM OC1 REPOSITORY

6.2 SOFTWARE REPOSITORY – GITHUB

TRUSTCHAIN has created its official GitHub organization: https://github.com/NGI-TRUSTCHAIN.

A private software repository for each applicant project has been created in TRUSTCHAIN GitHub organization, namely: https://github.com/NGI-TRUSTCHAIN/PROJECT-ACRONYM

An **Issue Tracker** per project for Feedback and Support can be found at: https://github.com/NGI-TRUSTCHAIN/PROJECT-ACRONYM/issues

Each individual project's repository must take into account the followings:

- **README.md:** A detailed and well-written README file for providing an overview of the project that includes information about the purpose, goals, and key features. Additionally, it should contain instructions on how to set up and run the project, any dependencies, and relevant documentation links.
- **Project structure:** Organising the codebase in a well-structured manner and that makes possible navigating it in an intuitive and/or easy way.
- **Documentation:** Comprehensive documentation to help understand the codebase and its functionality: components, APIs, interfaces, and any other relevant information.
- **Usage examples:** Usage examples and code snippets to demonstrate how to use the project and to show the capabilities and potential of the project.
- **Tests:** A comprehensive suite of tests that cover the major functionalities and use cases of the project.
- **Licensing and Acknowledgement:** The licensing terms under which the project is released and the acknowledgement about all contributions to the project (including dependencies).

TRUSTCHAIN members and applicants will add material there (documentation, guides, etc).

6.3 MONITORING TOOL

Specially designed to support the OC1 monitoring activities, a specific template GitHub KANBAN board is available for each project. The responsibility of maintaining the monitoring tool belongs to the core members of the SCRUM team and mainly to the selected OC1 projects. Note that a SCRUM team comprises the OC1 team members and the coach(es) from the TRUSTCHAIN consortium. The main lists of the GitHub KANBAN board are depicted in the figure below.

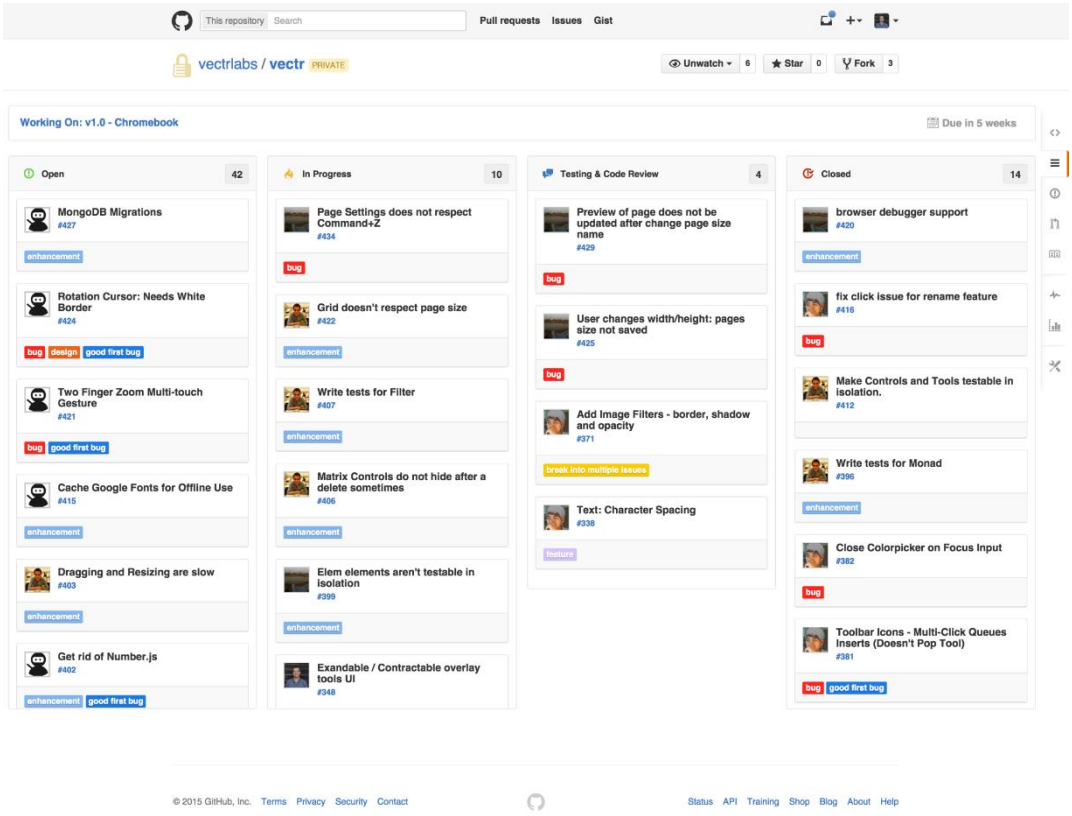


FIGURE 4: GITHUB KANBAN BOARD FOR PROJECT MONITORING

The GitHub KANBAN board for Agile project monitoring is composed by the following lists:

- **Contacts:** A list of the contacts involved in each OC1 project. For each contact, a full name (first name, last name), an affiliation, a role, an email, and a phone number are required.
- **Backlog:** In this list, each project should put all microtasks that will be completed within the project. A microtask can ideally fit in the timeframe of one sprint, here one week. The approach to define microtasks employs the identification of user stories or use cases for the envisioned system, identify all needed functionality, define tasks to accomplish functionality and then split tasks to microtasks that ideally fit into one week, and necessarily are not longer than two weeks (two sprints). A first prioritization of tasks, not binding, can be agreed among members of the SCRUM team (including the product owner -

the coach), which is not binding. Each microtask may be tagged with a colormap for prioritization or categorization.

- **Current Sprint:** This is the list where the microtasks to be performed for next week are removed from the backlog and put into during the weekly scrum meeting. The actual selection of the microtasks from the backlog represents the current work prioritization of the project. Moreover, an assignment of each microtask is made to a specific team member and the microtask is tagged with a colormap for prioritization or categorization.
- **In Progress:** In this list, the team puts microtasks from the current sprint that started. When a microtask is completed, then it is moved to the Done list. If a microtask is not completed within a sprint, then it will be discussed in the next SCRUM meeting, and it may be planned for the next sprint.
- **On hold:** This is the list where the team puts any microtasks that have been blocked for any reason, e.g., task dependency, lack of information, medical emergency, etc. with a description on the blocker. Microtasks that are on hold may go back in the In-Progress list, if possible, or otherwise discussed in the next SCRUM meeting and planned for the next sprint.
- **Done:** In this list, all accomplished microtasks are put. Eventually, the SCRUM process should result in the migration of all microtasks from the Backlog list to the Done list. If the microtasks are well defined, then the number of microtasks in the Done list over the number of sprints (weeks) provides an indication of the productivity rate of the team.
- **Questions:** Any questions that arise between SCRUM meetings are put in this list and discussed in the next SCRUM meeting.
- **Would Love to Do** - Manifest: In this list, team members put ideas for future work or activities not initially conceived or anticipated in the project proposal. These are discussed in the next SCRUM meeting, and they may become microtasks and put in the backlog or they may be kept as notes.
- **Room for Improvement:** In this list, the team members can put thoughts or suggestions for accomplished microtasks in the Done list, where there is "Room for Improvement", describing in detail the value of the suggested improvement.
- **Deliverables:** A list of the pending deliverables with their respective deadlines. Moreover, the status of their evaluation can also be reported there.
- **Invention:** This is a list to report all invention activities, such as patent applications. An initial request for invention should be reported to TRUSTCHAIN first, so that the innovation potential is established through an internal search by patent experts. The information to be reported includes Invention identifier, Invention title, Inventor, Affiliation, Initial description of the contribution, Notification date to the TRUSTCHAIN, amended description of the inventor

contribution after internal search report, Intention confirmed after search report (Y/N), Date of the conclusion of the internal search report.

- **Dissemination Activities:** To report all dissemination activities such as presentations in workshops/conferences, paper publications, active participation in venues, media coverage, press releases, etc., by each OC1 team. Necessary information to be reported is Name, Title, Venue, Date, Audience, Feedback, Abstract, Link and more detailed description may be provided if needed.
- **Software components:** To track all different software components and their software versions delivered by each OC1 team. The necessary information to be filled for each component is Component Name, Owner, Architectural Components, Code Release (Y/N), version, source file(s) and/or binaries, license, checkbox for it being uploaded in the GitHub repository, documentation (link/file(s)).
- **Participation in project events/meetings:** To track all the relevant events/meetings attended by each OC1 team (excluding SCRUM meetings). Necessary information to be reported is Event Name, Date, Purpose, Participants, Main Outcomes. For example: Event Name: Kick-off OC1 Event, Purpose: Introduction, Date: October 14, 2022, Participants: TRUSTCHAIN community, Main Outcomes: Project Kickstart
- **Awesome Things - WINS!** This is a list for reporting some activity of high impact or value that does not fit into any of the other categories.
- **Resources:** The resources available for each team and any respective changes should be reported here. For example, a new team member should be announced in this list. Acquiring the license of a certain useful software should also be reported here.
- **Marketing Ideas - Icebox:** This list serves as a placeholder for aggregating and storing specific ideas on the future market exploitation of the results of the project.
- **Recycle Bin:** Microtasks or cards in general that have been created in GitHub KANBAN boards cannot be removed, and normally should not! If for any reason, the team decides to remove a certain card, then this card can be moved into the Recycle Bin list.

The prioritization or categorization of microtasks can be labelled as depicted below.

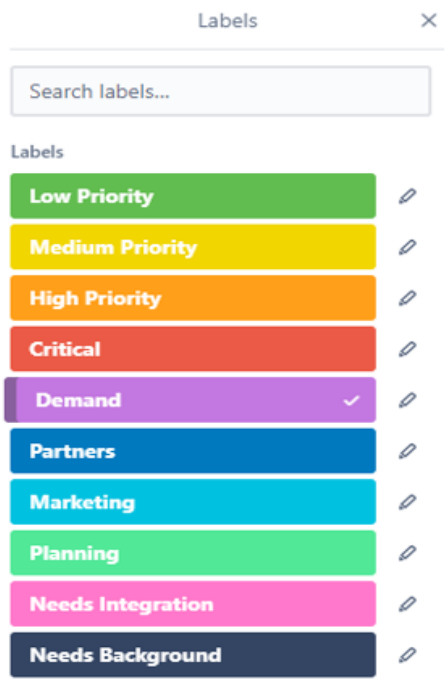


FIGURE 5: GITHUB KANBAN LABEL OPTIONS

7 MAILING LISTS

OC1 winners' mailing list: TRUSTCHAIN_OC1winners@eurodyn.com

TABLE 6 PROJECTS CONTACT LIST

Project Acronym	Contacts
DidRoom	andrea@forkbomb.eu
CreatorCredentials.cc	sebastian@posth.me
MUSAP	jarmo.miettinen@methics.fi
TREVO	antonis.mygiakis@konnecta.io
Orchestral	suport@pangea.org
The Social Wallet	sfboender@sphereon-int.com

DID4EU	dominik@walt.id
IM4DEC	christoph@ownyourdata.eu
WIDE	matthew.scerri@gmail.com
CLIENT-DIDS	markus@danubetech.com
EVI Electric Vehicle Identity	c.stefanatos@parityplatform.com
IS-CIS	daniel.field@ust.com
PRIVÈ	agiannetsos@ubitech.eu

TRUSTCHAIN coaches' list: TRUSTCHAIN_coaches@eurodyn.com

TABLE 7: COACHES MAILING LIST

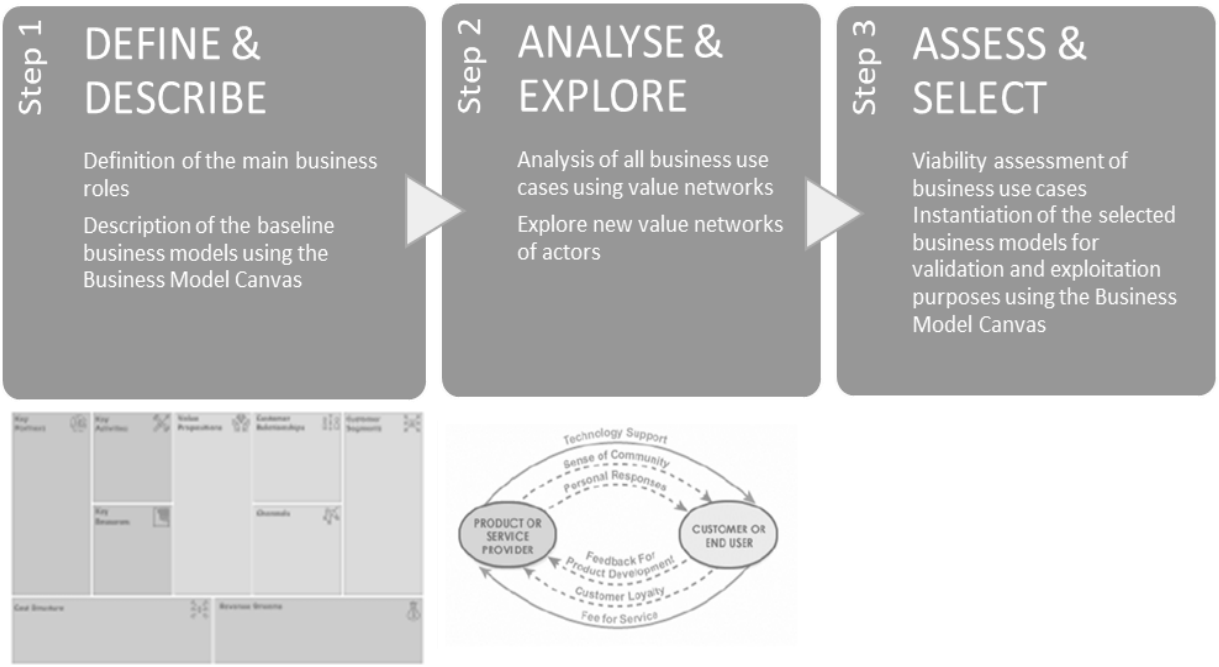
TRUSTCHAIN partners	Head Coach details
ALA	Alexander Herranz (alexander@alastria.io) Iker Ruiz de Infante (iker@alastria.io)
UL	Vlado Stankovski (vlado.stankovski@fri.uni-lj.si) Petar Kochovski (petar.kochovski@fri.uni-lj.si) Arvin Jušić (arvin.jusic@fri.uni-lj.si) Iztok Škof (iztok.skof@fri.uni-lj.si) Gaber Polajnar (gaber.polajnar@fri.uni-lj.si) Pouriya Miri (pouriya.miri@fri.uni-lj.si)
AUEB	Vasilis Siris (vsiris@aueb.gr) George Stamoulis (gstamoul@aueb.gr)
ICS	Muttukrishnan Rajarajan (r.muttukrishnan@city.ac.uk) Michal Krol (michal.krol@city.ac.uk) Akanksha Dixit (akanksha.dixit@city.ac.uk)
NKUA	Thanasis Papaioannou (atpapaioannou@uoa.gr)
TLX (legal & regulatory aspects)	Ruben Roex (ruben.roex@timelex.eu)
CIB (User Centric design)	María Pretel (maria.pretel@cibervoluntarios.org)

ED (administrative duties)	Caroline Barelle (caroline.barelle@eurodyn.com)

APPENDIX

ANNEX 1 - BUSINESS MODEL ANALYSIS METHODOLOGY

To define, describe, select and assess the most promising TRUSTCHAIN-enabled business models (BM), the project uses different methods. The process and associated methods are outlined in the figure below. Each step and its methods are described in the following sections.



The business modelling steps and methods

STEP 1: DEFINE BUSINESS ROLES AND DESCRIBE BASELINE BUSINESS MODELS

To define the main business roles and describe the baseline business models, use the Business Model Canvas methodology. 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 & Pigneur, 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.

Funded by the European Union

The baseline business models will serve as the starting point for the TRUSTCHAIN-enabled business models that will be proposed. The following table gives an overview of the business model canvas that will be used for describing candidate business models.

The template of the Business Model Canvas

<table>
<tr>
<td rowspan="2">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.</td>
<td>Key Activities
The most critical tasks, i.e., those business processes whose details must be kept secret from rivals.</td>
<td rowspan="2">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.</td>
<td>Customer Relationships
Automated & personalised relationships and gamification techniques.</td>
<td rowspan="2">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).</td>
</tr>
<tr>
<td>Key Resources
The most important inputs for the product/ service to be realized.</td>
<td>Channels
The ways used for the value propositions to be delivered to customers. These can be privately owned or from third parties.</td>
</tr>
<tr>
<td colspan="3">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).</td>
<td colspan="2">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).</td>
</tr>
</table>

STEP 2: Generic 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 (Allee, 1999). Furthermore, these exchanges can refer to raw material, upstream services and products, information as well as financial transactions.

A generic value network

STEP 3: COST-BENEFIT ANALYSIS

Based on the value network, realistic cost and revenue parameters, and a market penetration scenario, an economic analysis is performed to assess the business viability and profitability of the solution, usually using spreadsheets. Economic indicators of interest include the Return on Investment (ROI), the Net Present Value (NPV) and the payback period in years.

REFERENCES

Allee, V. The art and practice of being a revolutionary. Journal of knowledge management, 3(2), 121-131, 1999

Osterwalder, A., & Pigneur, Y. Business model generation: a handbook for visionaries, game changers, and challengers. John Wiley & Sons, 2010

Porter. "The Competitive Advantage: Creating and Sustaining Superior Performance". New York, Free Press, 1985