NGI TRUST CHAIN

TRUSTCHAIN

OPEN CALL #4 - CALL DOCUMENT

MULTI CHAINS SUPPORT FOR NGI PROTOCOLS

Closing dates for proposals: 17 July 2024 at 17:00 CEST

Version 1.0 – 15 May 2024

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.

Document revision history

Version	Date	Description of changes
V1.0	15/05/2024	Initial version

Disclaimer

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

Copyright notice

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	NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS	NKUA	EL
9	CITY UNIVERSITY OF LONDON	ICS	UK

TABLE OF CONTENTS

1 PREAMBLE

This document provides the challenges, expected outcomes and technical details that should be addressed when preparing applications for TrustChain Open Call #4. The guide is complemented by the Open Call #4 Annexes available at https://TrustChain.ngi.eu/.

Proposed solutions should build on top of existing concepts and technologies already developed for achieving conformance of data, schemas, state transfer and other aspects of interoperability across multiple, heterogeneous wallets, applications, databases and knowledge bases, tokenization methods, blockchains, and fit within TrustChain's vision and objectives. For example, they should cover aspects of the digital identity, either based on the DID standard, the eIDAS2 or any other approaches available, privacy and security, ability to generate various proofs that can be generated and provided for verification in various circumstances and similar. The solutions should be provided as open-source software desirably at TRL 7, tested, evaluated, and validated by an adequate pool of potential end-users that should be identified and their needs addressed in the application, as well as supported by a self-sustaining business model for exploiting the developed system following the end of the project. Each proposed solution will have to use the latest technologies for full-stack development that are compatible with the current standards.

The call is open for submission from 15 May 2024 to 17 July 2024 at 17:00 CET.

2 THE TRUSTCHAIN PROJECT

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 the 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 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. Our intention is to embed in such solution's important societal goals in accordance with objective truth and therefore, trustworthiness.

TrustChain - Fostering a Human-Centred, Trustworthy and Sustainable Internet is a European project funded by the European Commission under the European Union's Horizon Europe Research and Innovation Programme and the call topic CL4-2022-HUMAN-01-03. As such, it is part of the European Commission's Next Generation Internet (NGI) initiative. Its overall objective is to create a portfolio of Next Generation Internet protocols and an ecosystem of decentralised identity management software solutions that is transparent to the user, interoperable, privacy aware and regulatory compliant that can seamlessly integrate and interoperate with any of the existing decentralised applications. **TrustChain was launched in January 2023 to address the inherent challenges within the current centralised Internet architecture that is not transparent to the user, does not protect the privacy-by-default and does not scale well through 5 Open Calls and an overall budget of 8,775 M€.**

The 5 Open Calls are the following:

Open Call #1- Decentralised digital identity
The overall objective of Open Call #1 was to define and develop:

- A framework for decentralised user-centric identity management,
- Protocols for trustworthiness assessment of entities and their data by means of verifiable credentials and decentralized reputation systems,
- Smart oracles assessing the trustworthiness of data.

Open Call #2- User privacy and data governance
The objective of the Open Call 2 was to develop tools, cryptographic mechanisms, and other algorithms for data handling and sharing as well as for the management of data lakes in compliance with the GDPR and other regulations that implement techniques such as:

- Multi-party data sharing mechanisms,
- Federated learning mechanisms considering both vertical and horizontal frameworks,
- Encrypted data analytics based on homomorphic encryption,
- Secure and privacy-preserving data analytics mechanisms based on local and global data privacy techniques,
- Privacy-preserving usage of Artificial Intelligence, IoT, Cloud or combinations of those environments to provide the decentralised next generation smart digital services.

Open Call #3- Economics and democracy
The objective of Open Call #3 was to define and build mechanisms for smarter data exchange and data trading as well as innovative win-win federated business models' open data.

Open Call #4- Multi chains support for NGI protocols
The objective of Open Call #4 is to design and build the gateways that will make it possible to transfer knowledge/metadata/data/process/requirements from one wallet, application, databases/knowledgebase, blockchain to another in a trustworthy and secure manner. Interoperability across multiple chains is a cornerstone of this call.

Open Call #5- Green scalable and sustainable DLTs
This call will build on top of all past Open Call #1-4 calls. Its objective will be to employ digital identities, trustworthy data, and already designed novel mechanisms for the ecosystems' economy, in order to achieve high energy efficiency and optimisation of DLTs. We are looking for the most appropriate, relevant and pertinent trade-offs between the use of technologies, the security of consensus protocols on one side, and the sustainability and energy efficiency requirements on the other.

The overall structure of the Open Calls is summarized in the figure below. Note that each Open Call provides key technologies that can be used as basis for development in the subsequent calls, while also the opposite interaction can be employed by later calls, e.g., Open Call #4 can pose additional requirements for the final outcomes of Open Call #1&2&3 projects.

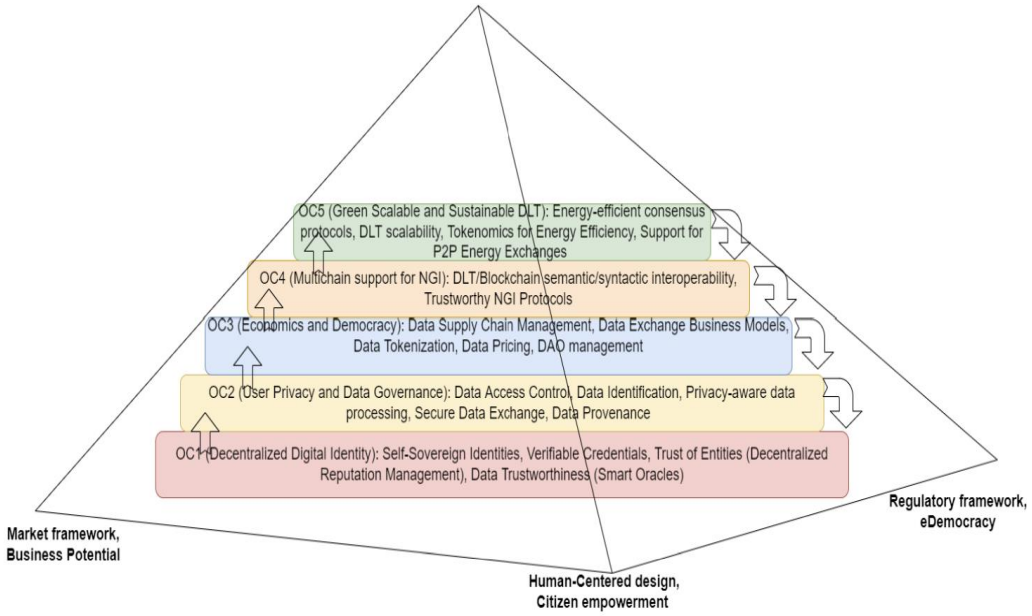

FIGURE 1: Overall structure of Open Calls

In this technological framework, TrustChain Open Call #4 is thus closely related to Open Call #5 “Green scalable and sustainable DLTs” as well as with technologies developed in Open Call #1, #2, and #3. Better solutions for interoperability across multiple chains will subsequently encourage ways for the development of green scalable, and sustainable DLTs. Thus, knowledge created within this Open Call #4 will be transferred/integrated into future Open Call #5.

Following the spirit of calls for the Next Generation Internet, the TrustChain Research and Innovation Action encourages presentation of results as open-source software and open hardware designs, open access to data, standardisation activities, access to testing and operational infrastructures as well as an IPR regime ensuring interoperability, reusability of results, lasting and sustainable with a long-term societal impact.

This guide is specifically dedicated to the Open Call #4 and outlines its context and its application modalities.

3 OPEN CALL #4: MULTI CHAINS SUPPORT FOR NGI PROTOCOLS

3.1 INTRODUCTION

It's indicative budget is 1.989.000 € and will be distributed among up to 17 selected projects led and executed by a critical number of developers, innovators, researchers, SMEs and entrepreneurs among others, actively involved in research, development and

application activities in the fields of user privacy, data governance, blockchain, semantic web, ontology engineering, software engineering, Cloud engineering, digital twins, edge and fog computing, ecosystem economics, smart applications, cryptography, standardisation, and security engineering.

Selected projects will last for a duration of 9 months. However, the TrustChain overall action lasts 36 months, and the selected projects are requested to participate after these 9 months in future Joint Meetings for knowledge and know-how transfer to TrustChain Open Call #5 and for the development of the TrustChain ecosystem.

As part of the TrustChain action, experts in diverse fields will also provide to Third party innovators selected technology development guidance, working methodology as well as access to technical infrastructure, training in business model development and data related topics, coaching, mentoring, visibility, and community building support.

Applicants are invited to submit their proposals on any topic that serves the overall TrustChain Open Call #4 vision and objectives. Their proposed solution should consider as minimal requirement to:

- Be grounded on end users needs and requirements,
- Use standard technology for full stack development,
- Be open source,
- Extend the state-of-the-art in the domain of interoperability and conformity in gradually more complex landscape of digital identity-based. This call can also be used to address existing real-world problems of interoperability and conformity data governance and provide new highly usable software solutions.

Using the mandatory TrustChain proposal template, applicants are expected in relation to the specific objectives identified hereafter (section 3.3) to explain in their application:

- The specific technological innovation they propose to develop and how it is clearly different from alternative solutions that are already available in the market, or developed by previous EU research and innovation actions (i.e., the EU ONTOCHAIN Project and any other projects),
- The specific interoperability and conformity needs or challenge they propose to address and who would benefit from their solution immediately and in the longer term,
- Whether the innovation will focus on the development of new solutions for existing areas, or a totally disruptive approach or idea,
- Any work they have already done to respond to this need, for example if the project focuses on developing an existing capability or building a new one,
- Any challenges or opportunities relating to equality, diversity, ethics, and inclusion arising from their project,
- Explain how their proposed solutions will align with the building blocks developed as part of the Open Call #1 call on digital identity (more details are available on the TrustChain webpage).

Applicants when applying should clearly specify the Open Call #4 challenges they are

going to address. Those are described in the section 3.2.

3.2 CHALLENGES TO BE ADDRESSED

Navigating the intricacies of data transfer between blockchains poses a multifaceted challenge rooted in the complex landscape of knowledge, encompassing rules, policies, and regulations. Achieving seamless interoperability, scalability, security, energy efficiency, and high-speed transactions demands a comprehensive understanding of the diverse blockchain ecosystems involved. Interoperability is a key aspect, as different blockchains often operate on distinct protocols and consensus mechanisms, requiring a harmonized framework for effective state transfer. Scalability is equally crucial, especially in the context of a rapidly expanding blockchain landscape, necessitating solutions that can accommodate the increasing volume of transactions without compromising efficiency. In addition, the challenge extends to ensuring the security and privacy of transferred states, as sensitive data may traverse multiple blockchains. Striking a balance between privacy and transparency becomes imperative, necessitating robust encryption mechanisms and adherence to regulatory standards. Streamlining energy consumption while maintaining the desired speed of transactions is a delicate balance that demands innovative solutions. **Some of the challenges to be tackled in this call are the following:**

- One of the fundamental challenges lies in reconciling the variations in protocols across diverse blockchains. Effectively designing gateways or bridges that can translate and adapt to these differences is crucial for ensuring seamless interoperability and facilitating smooth communication between blockchain networks whilst adhering to the European standards frameworks.
- Ensuring a consistent and trusted knowledge transfer is challenging due to the diverse consensus mechanisms and governance models utilized by different blockchains. Hence, upholding data integrity across the chains will ensure the reliability of information exchange.
- It is important to prioritize the security and privacy of transferred knowledge, requiring gateways to incorporate strong encryption and privacy-preserving techniques. Addressing this challenge is essential to safeguard sensitive data during the transfer process, ensuring a secure and confidential exchange that builds trust in information handling systems.
- Adhering to regulatory standards across various jurisdictions is challenging and requires gateways to adeptly navigate diverse regulatory landscapes. It is essential to tackle this challenge to enable a legal and compliant transfer of knowledge between blockchains, fostering a smooth and responsible exchange of information across diverse regions in Europe and internationally.
- With the expansion of blockchain networks and rising transaction volumes, ensuring the scalability of gateways becomes crucial. Innovative solutions that can meet the increased demands for data transfer while maintaining efficiency will facilitate the seamless functioning of the system.
- The complex challenge lies in achieving a balance between high-speed data transfer and energy efficiency. Gateways should minimize energy consumption while ensuring the speed and reliability of data transfers, contributing to sustainable and resource-efficient information exchange.

- Ensuring the compatibility and seamless execution of smart contracts across various blockchains is crucial. New solutions addressing this challenge will facilitate the smooth transition of smart contract logic and execution between diverse platforms, promoting interoperability and expanding the utility of decentralized applications.
- The use of semantic standards and open ontology schemas that enable the effective transfer of information and knowledge across chains is essential for cross-chain interoperability. Specific solutions that may be used to achieve interoperability and conformity may facilitate significant technology uptake.
- Ensuring the trustworthy use of digital identities across chains is required for the reliable exchange of value across chains.
- The use of multiple chains requires expert knowledge and complex configurations. Widespread cross-chain adoption can only happen when the user experience is simple and seamless.
- The intersection of AI, blockchain, IoT and cloud is very important for accountability, transparency and provenance, civil rights and citizen empowerment.
- New more trustworthy decentralized internet protocols to avoid centralization of power and trusted third parties.
- Enhancements in the blockchain, e.g., efficient blockchain bridges, more decentralized and green consensus mechanisms, app-specific consensus mechanisms, anonymous blockchains, blockchain speedups, etc.
- Provide a mechanism to operate while the user cannot have the capability to use some of the existing online identity credentials.
- Create a broker whereby the DIDs can be mapped to facilitate the interoperability challenges from multiple siloed systems.

3.3 SPECIFIC OBJECTIVES

The objective of this OC is to design and build the gateways that will make it possible to transfer knowledge/metadata/data/process/requirements from one chain to another in a trustworthy and secure manner. Interoperability across multiple chains, privacy by design, trustworthiness by design, scalability, greenness, openness, and legal compliance should be carefully considered. Innovative projects should implement techniques such as:

- Transfer of Non-Fungible Tokens (NFTs) across different chains. This might include the ability to execute contracts that depend on the state or ownership of an NFT, irrespective of which chain the NFT currently resides on.
- Semantic standards and open ontology schemas that enable the effective transfer of information and knowledge across chains and allow data interoperability.
- Mechanisms and procedures that enable the trustworthy use of digital identities across wallets, applications and blockchains or the secure binding of digital identities on multiple chains.
- Models and procedures to support simple and seamless user experience of cross-chain functionality.
- Develop techniques to carry out DID rotation and translation so that we can minimize the DID management.
- Create platforms that can build on top of the existing work that has been undertaken in Open Calls 1, 2 and 3. (Details can be found from the TRUSTCHAIN portal).

- Develop infrastructures that are inclusive, energy efficient, and usable.
- Develop platforms and infrastructures that follow European standards.

Applications should cover real needs of the end-users in one a specific sector such as for example banking, education, healthcare, or e-government.

3.4 SPECIFIC REQUIREMENTS

3.4.1 Technical Requirement

In general, a user centric design and implementation, a co-created process with citizens as well as a use case driven approach will frame the proposed innovative solution development that should carefully consider the needs for security, privacy, human-rights, sustainability, and trustworthiness. Interoperability, scalability, greenness, openness, standards, as well as legal and regulatory compliance should also be considered, calculated, and assured.

The proposed solutions are intended to be co-created with end users focusing on online user privacy and data governance, adopting a user-friendly design. Therefore, they should be designed, implemented, piloted, and validated using a specific predefined and justified set of end users in an identified use case. The co-creation and validation approach should be clearly elaborated in the applicants' proposal. A citizen digital vulnerable collectives' approach that puts in the centre the needs of the general population and vulnerable people, instead of technical/experts' users should be considered. It is intended that the solution is accessible for the general population as well as for the marginalized/vulnerable communities.

To this end, the applicant should show collaboration with an EU end-user organisation (i.e., banking, healthcare, education, policing etc.) as well as consider vulnerable groups for the evaluation /validation process if possible.

The focus should be on what is currently missing (e.g., trustworthy data access, ensuring clear and informed user content and expanding what already exists, thus scaling) rather than building something new from scratch. It is desirable that the selected projects be able to demonstrate their solution at TRL 7 in a real end-user setting. If something completely new must be built (see point above), then it should be well motivated why the nature of the problem warrants a new solution and why the state-of-the-art solutions do not solve it today (i.e., barriers to technology adoption).

The proposed solution should work within a specific business context and emphasis should be put on its scalability, on its energy efficiency and its minimum value proposition. Cross-border data sharing, moving data across EU-international borders should be carefully considered. It should be also compatible with existing data sharing frameworks, standards and demonstrate the energy efficiency through measurements that are quantifiable.

The proposal should identify and justify how the proposed solution, or specific services and/or modules provided by it, can be used by other service and application developers of the TRUSTCHAIN ecosystem.

Finally, focus should also be put on the demonstration of the technology. In particular, the applicant should demonstrate to have access to an infrastructure that is EVM compatible where it can be deployed and piloted.

Link with other Open Calls: Understanding what digital identity (Open Call #1) is, data owners privacy policies requirements and data governance (Open Call #2), market mechanisms for data exchange and trading, and federated business models (Open Call #3) is prerequisite for designing and implementing innovative and fit for purpose gateway solutions for cross-chain data exchange. Solutions to be developed in this Open Call #4 should consider some of the approaches and outcomes identified in Open Call #1, #2, and #3. Joint activities between Open Call #1, #2, #3, and Open Call #4 innovators will be facilitated by the TrustChain consortium.

3.4.2 Sustainability requirements

Various emerging technologies currently pose huge environmental impact. This negative impact should be assessed against the benefits from using these technologies. The applicants are requested to provide a short assessment of the trade-offs, considering from one viewpoint the benefits when using the technology, and from another, the potential energy-inefficiency. Various best effort solutions should be used as a baseline for providing such self-assessment.

3.4.3 Regulatory and standards requirements

New economic/business models for the ecosystem economy, user centric data management, addressing privacy aspects, legally and regulatory compliance (e.g., GDPR-compliance, verification, and certification of records of data processing activities).

3.4.4 User centricity Requirements

As mentioned above, the proposed solutions should be designed, implemented, piloted, and validated using a specific predefined and justified set of end users in an identified use case. It is paramount that a co-creation and validation approach is clearly elaborated in the applicant's' proposal and the vulnerable collectives' approach should be used for the user testing.

A first step is to establish target groups of users' representative of the future user base as well as clear use cases. Once this is done a plan for users to be recruited and involved in the co-creation process should be clearly presented. Also, it should be clarified who in the team will take care of both this phase and the following ones.

Following that, a roadmap that ranges from the beginning to the end of the project with the appropriate methodologies should be set up. For the approach to be complete it should include a needs assessment of the target end-users, co-creation phases and a final validation. The roadmap should include the methodological approach taken for co-creation, objectives and phases of the testing, and sample size. The sample needs to be representative either qualitatively or quantitively of the target population.

Finally, there should be an account on how users (and relevant stakeholders if applicable) would be onboarded in the design process and how their feedback will be incorporated in the development of the solution.

3.5 EXPECTED OUTCOMES AND POSSIBLE APPLICATION DOMAINS

With this OC, the following APIs or SDKs could be created, to be available for the rest of the teams, and for the European developer community, as open source:

- Cross-chain credential verification (API or SDK) to enable verification of individuals' credentials across different blockchain networks.
- Cross-chain NFT transfer (API or SDK) to enable the secure and transparent transfer of NFTs across different blockchain networks.
- Decentralized Data Governance (API or SDK) for governing the decentralized transfer of sensitive data, ensuring compliance with regulatory standards. For example, the creation of decentralized autonomous organizations (DAOs) that manage data access and permissions in different chains.
- Decentralized Asset Migration (SDK or API) to enable the movement of assets from one blockchain to another while preserving privacy, sustainability, human rights, and other user-centric considerations.

With this OC, the following outcomes are expected:

- Hybrid chain solution.
- Decentralised platforms.
- Tools for achieving interoperable schemas, conformance agreement and testing.
- Monitoring system.
- Energy optimisation system.
- Scalable gateways supporting trustworthy transfer of state and value across chains.
- Open ontologies schemas.

All this will help individuals and organisations to move data, processes and assets from one blockchain to another blockchain while achieving the same level of sustainability, human right protection, resilience, scalability, energy efficiency, and other requirements of the end users. Possible use cases and application domains include:

- Data transfer among stakeholders whose credentials lie in different chains.
- NFT transfer across chains.
- Defi and Open Banking applications.
- Defi and Open Banking applications.
- Public Sector Services Infrastructure.
- CBDC transfers across the EU and cross-border payment.
- New social media platforms for the metaverse for trading.
- Digital platforms for cross-border secure and privacy-preserving tax payments.
- Platforms for national and cross-border security and intelligence.

- Sharing of data across the supply chain and logistics.
- Carbon trading and asset management.
- Cross-border corporate digital IDs for digital trade and business.

3.6 MANDATORY DELIVERABLES

Projects selected and funded by the TrustChain consortium will have to deliver four mandatory deliverables during their lifetime. The four deliverables are defined below:

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

3.7 TRUSTCHAIN ECOSYSTEM TO DATE

The TrustChain project framework encompasses an innovative protocol suite and applications that address diverse requirements and topics. These include decentralized identity management, cryptography, secure data management, privacy-aware computation, anonymized proofs and consensus, intellectual property, data value sharing, trustworthy economics and democracy, multichain support, and solutions for more environmentally friendly, scalable, and sustainable decentralized ledger technologies. The following figure shows how these functionalities, protocols and applications should aggregate to formalise the TRUSTCHAIN ecosystem.

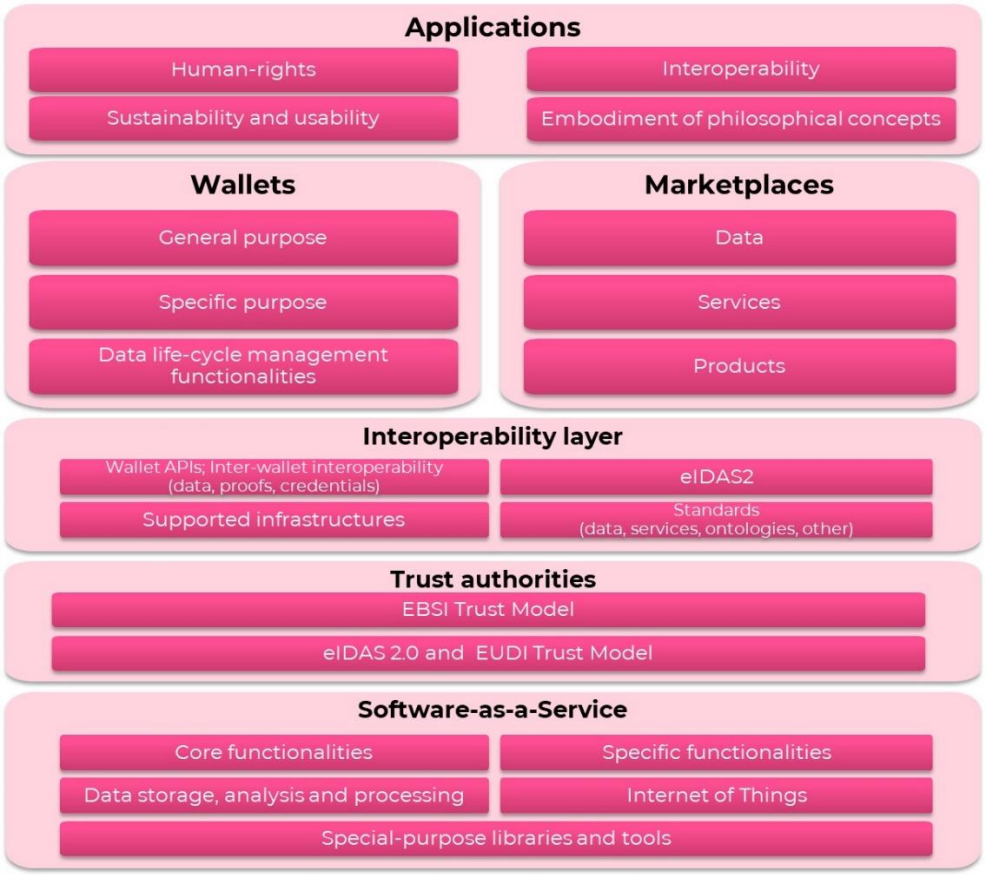

Figure 1: TrustChain Layered-Architecture

These open source functionalities, protocols and applications are developed by third parties innovators selected under TRUSTCHAIN Open Calls and as soon as implemented they are part of the TRUSTCHAIN framework and become available for the future Open call Projects.

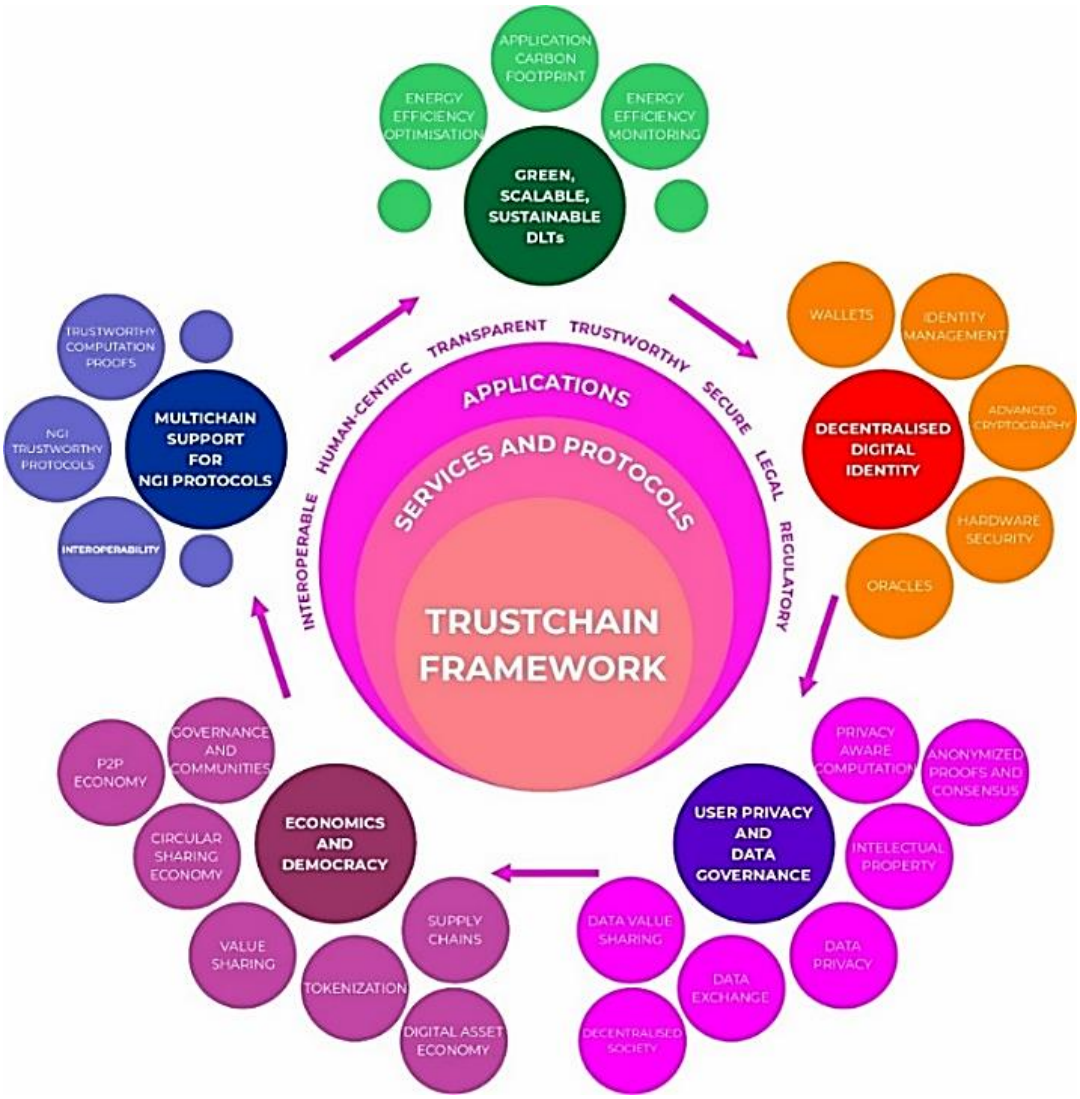

FIGURE 3: TrustChain Framework

To date, Open Call #1 related to decentralised digital identity has been achieved with 13 projects implemented and Open Call #2 projects related to user privacy and data governance are in the first phase of their development. The following section provides an overview of these Open Call #1 and Open Call #2 projects. They can serve as basis for Open Call #4 intended solutions while Open Call #4 solutions can complement them to ensure answering specific needs of end users. Complementary information about these projects can be found here: https://TrustChain.ngi.eu/selected-projects/ Open Call #3 related to economics and democracy are at the time of writing this document not yet selected.

3.7.1 Open Call #1 - Decentralised digital identity

The following figure illustrates the 13 TrustChain Open Call #1 funded projects and their corelation with the baseline TRUSTCHAIN technologies.

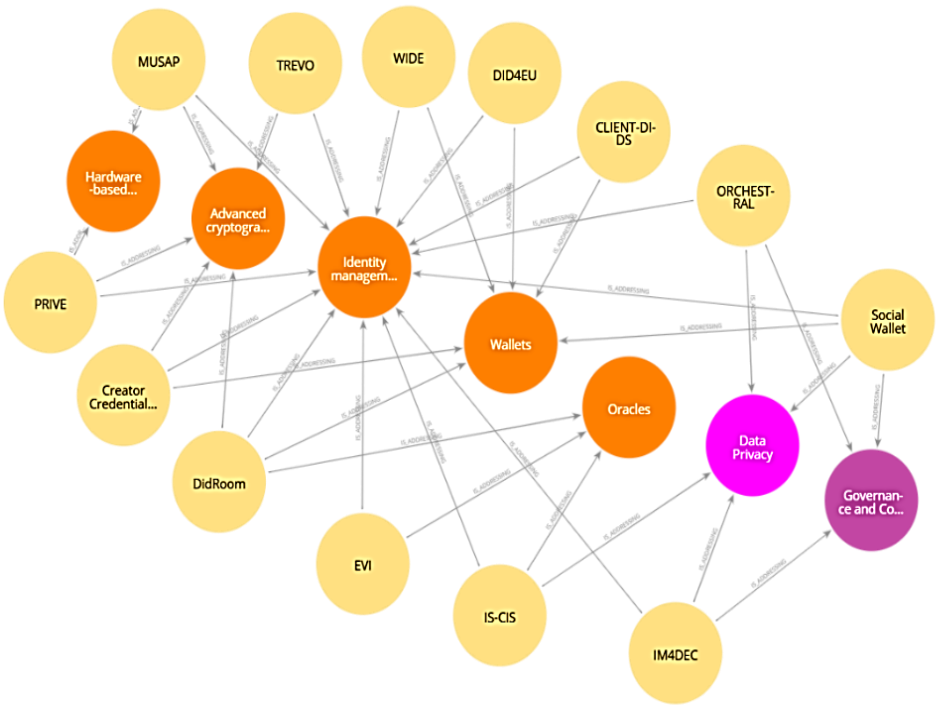

FIGURE 4: Mapping between the Open Call #1 projects and the TrustChain baseline technologies

They are further described hereafter.

DidRoom: Open-source, multiplatform, multi-standard, multifunctional SSI wallet
DidRoom is an open-source multiplatform and multifunctional Identity DID/SSI wallet, compliant with the W3C-DID and W3C-VC standards and with the current "The European Digital Identity Wallet Architecture and Reference Framework" (EUDI – ARF, version 1.0.0 from January 2023) which is the technical core of the eIDAS 2.0 regulation. DidRoom will also have advanced cryptographic and blockchain functions, including signatures, multi-signatures and blockchain interoperability (for Ethereum, Hyperledger Fabric and Sawtooth, and Planetmint).

CreatorCredentials.cc: Decentralised Issuer Services for Verifiable Creator Credentials
We propose a project to develop a decentralised user-centric digital identity management framework specifically designed for the cultural and creative industries. CreatorCredentials.cc will 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). With the app, media organisations will be able to issue verifiable credentials to creators and rightsholders in providing authentication and attribution to increase the trustworthiness of declarations and claims to digital media content online. This will increase trust and transparency of the digital media markets.

The app will be developed as an open source, dockerized service that can be installed without permission by media organisations intending to offer VC issuer services. It will facilitate the onboarding process, mutual authentication, and verification of credential issuers and creators based on novel SSI trust frameworks. The app will support the creation and issuance of various credential types and subjects, depending on the use case of the creator or rightsholder.

This dockerized service will provide a secure and efficient platform for managing digital identities and credentials, ensuring regulatory compliance, and maintaining privacy. CreatorCredentials.cc will establish a new role for public entities and organisations in digital media publishing. By extending the state-of-the-art in digital identities to the cultural and creative communities and solving existing real-world problems, the project aims to provide new and highly innovative software solutions for credential issuers and future trust services.

MUSAP project: Multiple SSCD with Unified Signature API Library

A Secure Signature Creation Device (SSCD) is a specialized cryptographic device used to generate digital signatures with high level of assurance (LoA). SSCD securely stores locally or remotely the private key which cannot be exported. When a user wants to sign a digital document, SSCD generates a digital signature using the private key and the document digest. SSCDs are used in applications that require high level of assurance, such as person authentication, identity verification, and signing legal documents, etc. To implement an SSCD, combination of hardware and software measures are required to ensure device security and signature validity.

This project 'Multiple SSCD with Unified Signature API Library: MUSAP' aims to develop a new software interface called Unified Signature Application Programming Interface (USAPI) Library.

The interface 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. USAPI simplifies the integration of various systems and services by presenting a standard set of methods and protocols for exchanging data and functionality. Project aims to work on a flexible identity management for end-users allowing them to control their trust relationships (private keys).

USAPI Library allows developers to build eID applications and Identity Wallets that can easily integrate with multiple systems without having to learn the details of each individual SSCD interface. USAPI simplifies the development process, reduces costs, and accelerates time-tomarket for new eID applications, making it particularly useful in the context of citizen's digital services, where multiple independent services need to interact with each other

seamlessly.

TREVO: Trusted Electronic Voting
Voting systems have evolved during the last hundreds of years to become more sophisticated and complex, starting from paper-based ballots up to electronic voting machines and internet voting which have been introduced as new voting technologies. However, electronic-based methods have raised concerns about security and the potential for tampering results, manipulation or hacking. The TREVO project 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 phase.

The main objective of TREVO is to tackle main challenges in electronic voting that are still open, such as voter anonymity, ballot privacy, trusted tally/audit as well as verifiability. It employs 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. The framework incorporates 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.

A mobile application is the core of the project which will be cocreated with the end-users, keeping them in the loop from the ideation and design process up to the testing and evaluation, integrating their feedback through an iterative procedure. TREVO will be deployed and evaluated/validated in real use cases of a Greek municipality (Trikala) where direct citizen feedback is needed for addressing issues such as urban planning, wider regional strategies (e.g. energy or digital transition) and e-governance, leaving no one behind, including elderly people and vulnerable groups.

The new approach is expected to increase the trustworthiness of e-voting systems in EU and across the globe and even make a step towards initiating the discussion for e-voting in national elections.

Orchestral: Identity in an ethical internet community
A group of ethical internet activists, members of the Pangea organisation, aim to co-develop an identity management system for marginalised and internet activist communities built by mature communities that work 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. The system development uses and will be open-source software. The system will be evaluated and disseminated to other communities. The system will be designed to be trustworthy and to preserve personal privacy. It will be aligned with decentralised identity models, including considering EIDAS and build on existing and emerging digital identity technology solutions, but adapted to the target and other similar communities of practice. The system will be driven by the end-user community and developed by a team of developers and researchers from Pangea and UPC. The system, extended with decentralised digital identity according to the community of practice needs, has the potential to significantly impact the lives of communities involving marginalised citizens working on digital services and circular devices. The system will give users greater control over their online identities and make accessing

essential digital services easier. The system will also help to promote trust and privacy online in more efficient and scalable communities.

The Social Wallet
We're rapidly moving into a digital-first world, which requires a different set of skills. That creates a real risk that certain groups of people will be left behind. Those with weaker socio-economic backgrounds, in vulnerable personal circumstances – old, sick, incapacitated, homeless – or are already marginalized, like certain minorities, refugees, or internally displaced. The Social Wallet project specifically supports these vulnerable people.

DID4EU: Decentralized identity infrastructure for Europe
The goal of this project is 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. This project is building on and will extend walt.id's existing open source products in various ways, for example, by adding new capabilities as required by the eIDAS2 regulation (e.g. support for m-docs (ISO/IEC 18013-5:2021) and related data exchange protocols), by making the open source code available on every platform (all popular programming languages & mobile) and by improving overall code quality and scalability to support production deployments. Moreover, we are building vertical-specific applications with customers from different verticals to make decentralized identity accessible to organizations and end-users. Considering that the project establishes a holistic infrastructure under an open source license (Apache 2), third party developers and organizations can also use it to build applications across industries with ease. Finally, the proposed project is completely aligned with TRUSTCHAIN's mission, objectives, challenges, proposed solutions and even several illustrative examples for project ideas.

IM4DEC: Identity Management for the Digital Emergency Call
UN convention Article 9 requires countries to take measures for the full and equal participation of persons with disabilities, including access to communication and information services. Despite this, there are still about 1 million 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. DEC112 is a non-profit association that has designed and developed a standard-conform infrastructure (ETSI TS 103 479) for deaf emergency chats (ETSI TS 103 698). Since 2019, the association is now operating a system in Austria in collaboration with the Ministry of Interior that connects emergency chats to the appropriate emergency communication centre by utilising location information. However, still a number of challenges exist that are addressed in the proposal and will - in case of funding - be implemented and made available as open source.

WIDE: Web3 Identity Integration for DAOs and Education
The project proposal focuses on developing 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). This use-case agnostic solution aims to enhance credential access for Web3- native organizations and protect individuals' data privacy rights.

The solution, WIDE, aims to combine existing technologies from traditional finance and the

cryptocurrency sector with innovative DID concepts. It features a novel architecture that preserves privacy and user control, while freeing users from the responsibility of managing their data directly. Our DID bridging client relies on existing wallet solutions to empower DAOs to access user data without the need for custom integrations with individual identity solutions.

This project's anticipated impact includes a component for composable verification of verifiers to the eIDAS ecosystem and improving the composability of eIDAS Type 2 configuration-compliant solutions for improved market access of DAOs to the European Economic Area (EEA). The prototype will undergo testing in three (3) distinct scenarios: voting using EVM wallets, enabling DAOs to verify credentials, and integrating with existing DAO frameworks like DAOHaus 'Moloch v.3'.

CLIENT-DIDs: Client-managed secret mode for DIDs
In this proposal, we will improve the Universal Registrar tool, which is a well-known open-source project at the Decentralized Identity Foundation (DIF). Parallel to the Universal Resolver (which allows resolution of DIDs), the Universal Registrar allows creation of DIDs across different DID 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 (which may involve blockchains, web servers, or any other technology). This tool can be self-hosted, it should not be operated by a single centralized authority.

EVI Electric Vehicle Identity: Protecting driver privacy, while streamlining transactions in public charging stations
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. For example, CPOs can use data related to users' daily location, vehicle type and frequency of charging sessions for targeted advertising or provide these data to 3rd party advertisers that seek to target specific user groups. Most drivers do not fully understand the potential uses of their private data whenever they sign up for an EV charging application.

IS-CIS: Information Sharing: consensual, innate & sequential
We propose a generic framework that mimics human nature in disclosure of identity and has a myriad of different social and business applications. It can allow the disclosure of sensitive medical data for the purposes of recruiting a cohort of a medical trial or guide the disclosure of personal data in a social setting. It could become a de facto standard for identity disclosure from human to IT and enable complex multi-person chains of disclosure.

It reserves control and repeal rights in the hands of the individual. It allows discoverability. It places an onus on the asker to justify and convince the askee. It retains a permanent record of who requested, and who granted, what and when.

Our proposed framework does not replace validation– it does not verify the data in the system with external sources of truth – as such it is synergic with all other solutions that do provide that validation. Its purpose is to hand a safe, verifiable control to the owner of the data.

PRIVE: Privacy Respecting Identity Verification Enabler for Digital Identity Wallets
PRIVÈ extends 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 offers 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 enables digital identity wallets to align with emerging regulations and standards like eIDAS that require higher level of assurances for services. At the same time, we make sure that privacy-enhancing properties like selective-disclosure are fully supported, in order to make the wallet compliant with privacy regulations like GDPR. To this end, PRIVÈ utilizes a privacy-preserving cryptographic protocol, namely Direct Anonymous Attestation (DAA) to provide verifiable evidence and assurances about the presented VC's origin and integrity. We can now enforce that a VC can only be issued by an attested Issuer and that this VC is bound to the Holder's device (wallet), overcoming the current limitations of bare proof-of-possession of a sw-based key. PRIVÈ follows a user-centric design and implementation, co-evaluated with the end users, thus, envisioning to achieve high level of user acceptance. It is also agnostic of the wallet's implementation and the underlying VC Data Model considered.

3.7.2 Open Call #2 - User privacy and data governance

The following section list Open Call 2 projects. Their mapping with the TRUSTCHAIN baseline technologies is at the time of writing this document under development.

DOOF - Data Ownership Orchestration Framework
Today control over data visibility is centralized into the hands of data sharing platforms' owners. Rightful data owners are not actively involved in the data value chain, and this results in low trust and willingness to share data, hindering the growth of a European data market. Based on a patented multicast end-to-end encryption scheme and smart contracts, Ecosteer decentralized consent management technology – the Data Visibility Control Overlay (DVCO) – allows individuals to unilaterally grant & revoke visibility over data streams generated by their devices to selected stakeholders, as mandated by the GDPR. Additionally, a smart contract implements a compensation mechanism based on tokens, incentivizing data sharing. Within NGI TrustChain Call #2, Ecosteer will develop the Data Ownership Orchestration Framework (DOOF), a set of open SDKs, libraries and Smart Contracts that allows data owners to exercise data ownership rights – i.e. grant, revoke and monetize data visibility. In fact, the DOOF's objective is to facilitate the integration of the DVCO as well as any other consent management technology, e.g. for data sets rather than data streams, with any data source and enterprise IT system, enabling companies and institutions to deploy user-friendly data exchanges privacy-compliant by design. In this project Ecosteer will integrate its technology with smart-home sensors and distribute them among a selected group of citizens in Bolzano. Thanks to a user-friendly interface, citizens will be able to unilaterally control third party visibility over their data and to be compensated for data sharing. Such validated solution will be proposed to Utilities

to deploy their own transparent, ethical and GDPR compliant data exchanges, involving their customers and business partners. Additional data sources, e.g. energy meters, other smart home sensors, wearables, etc., can be added over time, expanding data sharing & monetization opportunities without impacting system scalability provided as-a-service by the DOOF.

UtiP-DAM - Utility-Preserving, Decentralized Anonymity of Mobility data

Understanding crowd mobility is essential for governments and businesses to prepare for long-term challenges like climate change, mid-term challenges like increasing urbanization, and short-term challenges like controlling the spread of diseases. For instance, mobility data is used to optimize public transportation, improve mobile and wireless networks and study human contacts to help public health experts track viral diseases. However, mobility data is a very sensitive type of data, since mapping the movements of individuals can reveal personal information. Anonymization cannot be limited to suppressing metadata containing the subject's identity, because the origin, the destination and even the intermediate points of a trajectory may allow re-identifying the individual who followed it (de Montjoye et al, 2013). Proper anonymization requires masking detailed spatiotemporal Information. Currently, the standard approach to building anonymized datasets is centralized: the subjects send their data to a controller, who takes care of producing an anonymized mobility data set. This requires subjects to blindly trust the controller, which is not acceptable in most cases. There is another risk inherent to mobility data, which is the possibility to re-identify individuals in anonymized datasets by cross-referencing them with other existing or newly published datasets (Srivatsa et al, 2012). Hence, the requirement for anonymity of mobility data must be controlled in consideration of publicly available data. The goals of our project are threefold: - develop a decentralized method, based on utility-preserving k-anonymity, that will allow anonymization of mobility data in a way that guarantees that even the controller cannot re-identify individuals in their datasets. - create an auditing tool that enables data controllers to audit their proprietary datasets for de-anonymization risks and anonymize the data if risks are uncovered using a centralized k-anonymity algorithm. - create a verification tool enabling individuals and companies to uncover public datasets that contain similar trajectories to theirs.

MorphMetro - Secure and privacy-preserving exchange and analysis of measured data based on homomorphic encryption

Measured data obtained by measuring devices and its subsequent analyses (measured data accuracy, errors, measurement uncertainty, regulation compliance, etc.) are pillars for quality assurance (QA) in a wide spectrum of various industries (food industry, pharmacy, etc.). Currently, there is no universally accepted protocol for the machine-interpretable structuring and digital dissemination of measurement data, leading to concerns in data governance and user privacy. Fortunately, the science of measurement (metrology) is undergoing digital transformation, as evidenced by BIPM's recent Joint Statement of Intent. Our solution builds on emerging new standards (SI-Digital, Digital Calibration Certificates, etc.) to add a crucial component for digitalizing QA reliant on measured data. We propose an open-source solution for the secure exchange of data (measured data and subsequent analyses) in use cases where one needs analysis of measured data to be carried out by a third-party data analysis service. This "third party entity" operates independently of the entity (organization, department, team) involved in data collection most often if: - there is a need to ensure an unbiased analytical perspective (often prescribed by metrology regulations) and/or - the analysis is carried out as commercial service offered on the market and/or - there is a separate "in-house" analytical department/team within the same organisation In each case it must be ensured that data

security is maintained, reducing the risk of unauthorized access or data misuse, including privacy risks if measured data contains possible Personally Identifiable Information (PII). Shortly said, our proposal has a simple input → measured data, and a simple output → analysis of measured data. However, it will use state-of-the-art technologies (blockchain, homomorphic encryption) and emerging standards and architectures established in the EU space (European Blockchain Service Infrastructure (EBSI), Alastria, Digital Calibration Certificates (DCC)) in order to make the solution trustworthy, scalable and compliant with prevailing and upcoming regulations.

SURE - Synthetic Data: Utility, Regulatory compliance, and Ethical privacy

Clearbox AI, an award-winning tech startup based in Turin, Italy, specializes in facilitating AI and Analytics projects through Synthetic Data generation. Their privacy preservation and data augmentation expertise, notably in banking, finance, and healthcare, aligns seamlessly with TRUSTCHAIN's mission to establish secure and dependable data routes for responsible AI adoption. The proposal confronts the challenges posed by the rapid evolution of AI, particularly in safeguarding user privacy and data governance. AI presents distinctive privacy risks, including potential individual identification in anonymized data. Clearbox AI's solution centers on Privacy-enhancing technologies (PETs), focusing on Synthetic Data. This method preserves real-world data's statistical properties and predictive capabilities while ensuring privacy. The project's core goals involve creating an open-source library that harmonizes user privacy and data utility for AI training. It will also provide fine-grained privacy controls and uphold regulatory compliance through GDPR adherence features. Moreover, the project promotes responsible data practices, especially in the financial sector. The proposed product, named SURE, empowers users to evaluate the privacy and utility of anonymized datasets using both traditional anonymization techniques and synthetic data. Its user-friendly interface enables individuals with limited AI knowledge to evaluate and test anonymous and synthetic datasets, preserving privacy without sacrificing utility. The project's impact is poised to be significant. As AI's contributions to the global economy grow, SURE's provision of a customizable, open-source synthetic data library democratizes access to secure and privacy-respecting data solutions. It serves a diverse user base, encompassing fintech and healthcare companies, equipping them with a potent tool to bolster their data privacy practices while maintaining dataset utility. Additionally, the proposed solution dovetails with TRUSTCHAIN's fundamental objectives, cementing its status as a valuable asset in erecting secure and reliable data pathways for responsible AI adoption.

dGUARD - Privacy preserving data-sharing platform

Nowadays, there is a widespread perception that data has great value. Harnessing this value and the vast amount of data available can generate huge revenues for online service platform providers. It is common for data owners not to take advantage of this value in an adequate way and often give or share their data for free or pay with it for the use of a service. In general, these platforms offer services without preserving the privacy of users' data, without secure data exchange, without identification of the data or its provenance, or without providing mechanisms to track, explain and validate the data. The main limitation of data sharing platforms is users' lack of trust in privacy and control to manage their data. The user's perception of helplessness is increased by not knowing how their data is used and with whom it is shared. Therefore, it is necessary to preserve user data privacy and secure data exchange, in order to build trust among participants and ensure data sovereignty. Leveraging the capabilities offered by blockchain technology and the use of advanced cryptographic

technologies to ensure data sovereignty in the third-party data sharing, this project will focus on delivering four main components: 1) A consent management system based on self-sovereign digital identity authentications and interactions, 2) A privacy preserving authentication mechanism to enable privacy preserving authentications thus boosting anonymization, 3) A proxy re-encryption scheme to guarantee e2e data privacy 4) A blockchain notarized audit-trail to guarantee traceability, non-repudiation and accountability. dGUARD offers an innovative solution that harnesses the power of self-sovereign digital identity, Zero-Knowledge Proofs and proxy re- encryption with a comprehensive approach designed to revolutionize the way data exchange procedures are carried out, with a primary focus on improving consent management, strengthen data security, privacy and anonymity, while ensuring robust process accountability.

NG-SC- Next Generation Smart Cities

In the rapidly evolving landscape of the Next Generation Internet (NGI), data storage and management are undergoing a profound transformation. Historically, centralized entities and corporations held dominion over vast data stores. However, the NGI heralds a paradigm shift, prioritizing user-centric data governance, where individual users maintain control and ownership of their data, and even more intriguingly, their IoT devices become active contributors to this new ecosystem. In recent years, the idea of smart cities in which the infrastructure layer and data acquisition/storage is made available by government entities has gained significant traction. This is mostly attributed to the higher availability of cost-effective IoT devices/sensors, and growing connectivity and bandwidth of networks. However, the financial investments required to setup, and maintain the infrastructure are a high barrier to entry. Moreover, these infrastructures are commonly centralized into three layers namely, data acquisition layer, storage and computation layer, and finally the application layer in which users and companies participate in by leveraging the data. This project envisions a future where users actively participate and maintain all three core infrastructure layers. To realize this, we propose a decentralized model that allows both users and their smart devices to contribute building a decentralized infrastructure. The solution builds on a paradigm shift in the way data driven computation occurs. As such, data never leaves the device, instead computation is broken down into independent sets, and migrated across the network. This guarantees data privacy, and ownership whilst at the same time, makes use of the currently untapped computational resources of IoT devices. Our strategy involves harnessing advancements in Multi-Party Computation (MPC) technology, advancing a novel MPC protocol to a demonstrative phase. All software of the platform and the MPC protocol will be made open-source to further establish trust and inclusivity of the solution. In summary, our project seeks to empower users to actively participate and be rewarded in the data economy, fundamentally transforming data ownership in the NGI era. We propose a user-centric data governance model, fortified by cutting-edge technology, and a decentralized resource marketplace that enables users to take control of their data and computational resources. This vision aligns perfectly with the evolving landscape of the NGI, where data is not just a commodity but a democratized and user-empowering currency.

DUME - Decentralised User-Centric Media Extension

Tidy City encourages both individuals and organisations to routinely capture high-resolution images of streets and roads. The images captured with Tidy City app are then analysed by advanced AI models on centralised servers, detecting various urban challenges such as waste mismanagement or signage issues. However, like many contemporary platforms, once users

submit their data to Tidy City, they relinquish much of the control over it. Project DUME aims to change the centralised nature of digital platforms like Tidy City by: 1. Extending Solid Protocol that adeptly manages large-scale media datasets with decentralised web platforms. 2. Validating the robustness of the decentralised, user-centric features of the protocol created in 1., by implementing and testing it in Tidy City. The challenges of implementing a protocol capable of handling vast volumes of high-resolution photographs with associated metadata for streets and roads, ready for AI model training, are manyfold:

- For AI model training, swift and efficient data retrieval is essential. This involves implementing parallel data retrieval processes, batch data requests, and caching mechanisms to ensure minimal latency.
- The protocol should support rich metadata annotations, ensuring indexing mechanisms deliver quick searches and filtering based on this metadata.
- Specific AI access control ensures that AI model trainers can access the requisite data without compromising other personal or sensitive data. This involves creating specialised 'views' or 'profiles' of the data specifically curated for AI training.
- Given the dynamic nature of data (new images added constantly), the protocol must support robust versioning mechanisms, allowing users and applications to fetch historical data versions efficiently. DUME aims at creating a validated path not only for tidy city's evolution, but also for numerous other projects that depend on large amounts of media data, towards a decentralised digital paradigm where users maintain sovereignty over their media contributions.

AURORA MINDS - Empowering Children with ADHD Through Privacy-Preserving Data Collection

Aurora Minds represents a groundbreaking initiative aimed at addressing the need to early and accurately diagnose ADHD in children, while prioritizing data privacy and security. In a landscape crowded with assistive technologies for ADHD, this project distinguishes itself by integrating robust privacy measures at its core. Existing ADHD assistive technologies often overlook privacy and security concerns, leaving users vulnerable to data risks and profiling. To counter these challenges, AURORA MINDS implements a multi-layered security framework, including Identity Management (IdM) and Privacy-Enhancing Technologies (PETs). This approach enhances data security, strictly controls access to sensitive information, and ensures compliance with data privacy regulations. The project leverages machine learning techniques such as federated learning and local differential privacy to protect sensitive user data during collection and analysis, aligning with GDPR requirements. Aurora Minds adopts a human-centric design approach, tailoring personal data collection from a child while s/he interacts with a serious tablet animation game to cater a unique ADHD risk assessment process. The project benefits various stakeholders, including children, parents, educators, and clinicians. Children are examined through a specialized application supporting their behavioral unique requirements and independence. Parents receive reassurance regarding data confidentiality, gaining insights into ADHD risk assessment and relevant information to provide better support. Clinicians benefit from enhanced diagnosis capabilities, aided by qualitative and quantitative measurements. Access rights are carefully managed using the Privacy-ABCs (Privacy-Attribute-Based Credentials) approach, ensuring that each entity—child, parent, and clinician—receives appropriate access privileges. By incorporating this proposal into the TRUSTCHAIN framework, AURORA MINDS elevates TRUSTCHAIN's reputation by exemplifying

a steadfast commitment to data privacy and security. The emphasis on PETs and federated machine learning not only bolsters data privacy but also mitigates legal risks associated with data sharing, enhancing data quality for effective decision-making.

OIDC PRINCE - OpenID Connect with PRIvacy-eNhanced ConsEnts

The OIDC PRINCE project aims to enhance the privacy support in user consents used in OpenID Connect authentication and authorization processes. Nowadays the consent to access the claims about end-user and authentication events (e.g., gender, birthdate, phone number), may have associated privacy issues. Users need to be informed regarding the potential risk of providing consent for the personal information access by services/entities that may not be trusted by the user and the OpenID Provider, which is responsible to manage the authentication and authorization. OpenID PRINCE introduces the proof of privacy regulations compliance (e.g., compliance with GDPR) in the OIDC discovery and registration processes using data privacy vocabulary (DPV) specification that can be certified by entities external to the OIDC authentication process. These proofs can be stored securely in a EMV compliant blockchain. OIDC PRINCE also enables privacy analysis to assess the risk of services accessing the end-user private information. This analysis, performed by Fuzzy Logic models considers the claims which access is being requested and the profile of the service requesting the access, for instance if it is a service associated with acquisitions or a service for education and learning. OIDC PRINCE contributes to enhance the support of privacy in OpenID connect by enabling informed consents, and by minimizing the data sharing with entities that are not trusted, or that do not provide evidence of being trustworthy in terms of privacy management.

PECS - Privacy Enrooted Car Systems

People's privacy control over the personal data that they generate and consume while they drive modern cars is extremely weak at present. There is historical as well as recent evidence that car brands harvest a variety of personal data from drivers and, arguably, full compliance of their processing with the European General Data Protection Regulation is questionable. PECS revolutionises modern car ecosystems for what concerns the processing of personal data. It does so by advancing, tailoring to the specific domain and, ultimately, combining together both soft and hard privacy measures. The project raises drivers' soft privacy through the PECS interface for static and dynamic control of personal data, so that drivers can decide what to share and with whom and when, as well as follow and control the flows of data at service run time by means of multy-sensory media techniques. Hard privacy thrives in the project through a combination of obfuscation techniques including Federated Analytics, Secure Multi Party Computation and Pseudonymisation, so that drivers are enabled to keep their personal data opaque to anyone from the outset. All developments proceed from the established academic laboratories of UNICT-UNIMORE, then are demonstrated in the operational environment of MASA-UNIMORE, reaching TRL7. The PECS results stem from the open-source, open-Internet approaches, hence bear huge technical, societal and industrial impacts, bringing Europe at the forefront of data protection, at least in the automotive domain. PECS also brings forward a whole new range of business opportunities such as various forms of software support for its technologies, and of renewed car services leveraging privacy-by-design-by-default. Finally, PECS provides the necessary grounds favouring the inception of a new breed of services that would be naturally enrooted on drivers' sensitive data such as sexual, religious and political orientations, e.g. apps for dating, praying and debate on political topics.

EIDCMP - eIDAS compliant membership platform

WalliD and the Portuguese Blockchain and Cryptocurrencies Association (APBC) are forging a dynamic partnership to develop an advanced membership platform, poised to revolutionize the verification and credential issuance processes for Professional and Governmental Associations. Our platform will enable these associations to seamlessly verify member IDs and issue dynamic, verified credentials, all while accommodating new data updates. Crucially, this system will operate in full compliance with eIDAS regulations and adhere to the latest industry standards. In this project, our primary approach is to leverage existing technology and established standards, ensuring accessibility for all associations. Our comprehensive system will:

- Verify member ids with meticulous adherence to eidas regulations, harnessing the power of digital ids and digital wallets.
- Issue verifiable credentials in strict compliance with w3c standards and the eidas directive.
- Enable user management and sharing of credentials.
- Safeguard user data throughout the entire process, from verification to credential issuance, ensuring a secure and private environment.

With WalliD and APBC at the helm, this initiative will pioneer a new era of streamlined and secure membership management, providing associations and institutions with a powerful tool to enhance their services and compliance, while safeguarding the privacy of their members.

DID-IMP - Decentralized public key Infrastructure for Defended IoT data management and procurement

The DID-IMP project is building a decentralized public key infrastructure to allow any connected object to be able to deliver or procure secured and traceable data. To achieve this, Werenode is leveraging blockchain technologies to remove the need for a classical hierarchical structure with players like the Certificate Authority (CA) and the Registration Authority (RA). For DID-IMP, we replace these administrator-like trusted third parties (RA & CA) with a feeless blockchain smart contract. The blockchain is also used as a Certificate Store on which services providers can issue and manage revocable certificates and credentials. Such a lean architecture is especially well adapted for Internet of Things (IoT) Secure Automatic Data Sharing SADS. Indeed, SADS can be used in various ways to simplify and streamline data sharing processes, and to secure and trace data transfers. Some of the main use cases include: Connected Cars: DID-IMP-enabled cars can automatically share data for tolls, parking, vehicle recharging (electricity or hydrogen), and other transportation-related processes, making the service more convenient for drivers. They can automatically deliver maintenance data with selected relevant bodies. Remote healthcare: SADS systems can enable remote healthcare services, such as telemedicine and patient monitoring, improving access to healthcare. Sensors can also collect data on patient health and behavior and control the delivery of this data with specific accredited personas. Cognitive Cities: IoT plays an important role in creating smarter, environment conscious and more efficient cities. Applications like smart traffic management, water and waste management, and public safety rely on secure data transfer to optimize operations and protect citizens' data. Energy Management: IoT devices in the energy sector, such as smart meters and grid sensors, transmit data about energy consumption and distribution. Secure data transfer helps utilities ensure data accuracy and protect against unauthorized access. It's also a key component to be able to build local and

decentralized energy communities. And also, Smart Homes, Maintenance, Logistics... In a nutshell, we build a Trust Chain for IoT secure data sharing, bringing better traceability to data, securing their flow and allowing companies to reduce administrative overhead, save time and money, and offer a better protected data sharing experience for final customers. Indeed, users can retain ownership and control over their IoT data while granting access to specific parties through permissioned credentials. Additionally, our SADS-enabled solution can help to manage the flow of sensitive data and the compliance to the new European and Global regulations, thanks to the native traceability features provided by blockchain technologies combined with the process proposed by this DID-IMP project, which implies a traced blockchain transaction for each data transfer, also tracking the main regulatory characteristics of the data exchanged.

GUEDHS - Data Governance and User privacy envisioning an EHDS pilot deployment

The Covid-19 crisis has significantly raised the urgency for efficient use of health data beyond the healthcare providers' borders. It has also highlighted the importance of joint European health initiatives and data-sharing scenarios, as the ones promoted by the European Health Data Space (EHDS). Data can improve patient outcomes (primary use of data) while fostering research, and accelerating the development of new health services (secondary use of data), but only if it is shared securely and reused by stakeholders. In this process, privacy must be respected, data usage control enforced and transparency ensured. Establishing the EHDS is an integral part of building a European Health Union and the GUEDHS project will pilot it, at an interregional scale. As the epidemic risks increase globally, and to fast-forward crisis preparedness and resilience, GUEHDS project will present a solution leveraging existing concepts and technologies developed for data value-sharing in respiratory infections scenario. Promptly will bring a federated learning framework, while IPN will adapt a cybersecurity tool, for fast deployment of a Federated Network in action. This solution will enable data custodians to grant and revoke permissions on the data they control, and monitor the data used by FL tasks at the different data nodes. The testing data partners — CHUC and CHUdSA – will pilot-test GUEHDS solution within a clinical study on the epidemiological trends of respiratory viruses. This pilot will establish the ground for the Portuguese Observatory for Respiratory Diseases, an initiative that can be scaled at a European level together with Regulators (EMA) and Life Science Companies.

ProvenAI - Provenance in AI

Imagine a world where every piece of data, every article, and every contribution has a traceable lineage. Where, instead of AI models indiscriminately assimilating vast volumes of data, every fragment has a unique identifier and provenance. ProvenAI promises such a world, aspiring to construct a Decentralised Provenance Platform tailored specifically for unstructured data. It doesn't stop at mere identification; the objective is to ensure knowledge creators can trace how their content is utilised while receiving just compensation. Traditional platforms offer limited utility in the evolving realm of Generative AI and semantic searches. ProvenAI distinguishes itself by segmenting massive unstructured datasets into semantically relevant sections, ensuring only pertinent data segments respond to specific AI queries. This not only promotes data minimization but also protects against unwarranted data exposure. In this rapidly advancing age of information, ProvenAI stands as an ally to ethical AI development and data governance. By valuing the rights of content creators and emphasising user privacy, it seeks to redefine the dynamics of knowledge acquisition and compensation in the AI sphere. With ProvenAI, we're not just building a technology; we're nurturing a vision where innovation

aligns seamlessly with integrity, accountability, and respect for every byte of knowledge contributed. As we move forward, ProvenAI seeks to play a pivotal role in shaping a digital landscape that is both equitable and transparent, ensuring that the digital footprints of today become the trustworthy paths of tomorrow.

LED-UP - LEVEA's Enhanced Data Governance and User-Centric Privacy in Decentralized Systems

Amid the digital evolution, a pressing need has emerged to bolster user privacy and data governance. This is especially palpable for people forced to live in refugee camps who require robust, private, and transparent health data management. Our groundbreaking proposal, built upon the Alastria B Network, aims to redefine the way we approach these challenges. Using pioneering tools like Decentralized Digital Identity and Homomorphic Encryption, coupled with DAO structures, we offer a framework where data privacy is not just a feature but the very foundation. While the current digital landscape offers decentralized solutions, many fail to put user privacy and data governance at the forefront. Our model diverges, ensuring every data interaction prioritizes user consent, traceability, and security. This commitment extends beyond mere encryption; it reshapes how data is stored, shared, and accessed, always keeping the user's rights at the centre. Through consistent collaboration and feedback loops with users and stakeholders, especially those from vulnerable settings like refugee camps, we craft a solution inherently aligned with their needs. Our co-creation ethos guarantees that our framework is not only technologically advanced but also deeply empathetic, understanding, and responsive to real-world user challenges. Moreover, our proposed framework introduces a paradigm where data sharing is both transparent and potentially beneficial for users, marrying user privacy with data governance seamlessly. This harmony between privacy and governance is pivotal in sectors beyond healthcare, finding resonance in finance, real estate, and more. Together as Hora e.V. with our industry-leading members, we are able to realise a paradigm shift on how user privacy and data governance is handled in a decentralized world. Thereby, we are in sync with TRUSTCHAIN's vision, which seeks to set a transformative benchmark.

4 SUPPORT SERVICES PROVIDED BY TRUSTCHAIN TO THIRD PARTIES

Selected participants will receive support with the following services:

- **Access to Infrastructure:**

  Access to the Alastria blockchain infrastructure (two different networks, T Network based on GoQuorum and B Network based on Hyperledger Besu), compliant with Ethereum, for demonstration purposes, will be provided to the Applicants that request to use it for testing their proposed solution. This will be made available by Alastria through TrustChain, at no cost for the third-party innovators selected, in a BaaS model without requiring that the Applicants install their own blockchain node.

- **Use of token:**

The TrustChain consortium understands that the ultimate value of a new and innovative application should be shown in business context, for example, by demonstrating that the users (physical persons or companies) are willing to pay for using the service. In this context, the TrustChain core consortium partners are willing to consider the possibility of issuing a crypto-token for the purpose of demonstration of the applications' business value, should such an interest be expressed by the applicants.

- **Business support services:**

  To support the third-party innovators to exploit their use cases and successfully reach the market, different training events and sessions with mentors will be organised. Depending on the team profile, aspects such as Value Proposition, pitching or IPR (among others) will be addressed.

- **Communication support services:**

  Major visibility, promotion and networking opportunities are offered as part of the TrustChain project and the Next Generation Internet initiative. Selected third party innovators will:

  - have access to communication tool kits and co-branding materials,
  - be showcased in the TrustChain project website,
  - be interviewed and promoted on relevant media channels,
  - be invited to participate in top events, and
  - connect with a vibrant ecosystem of innovators, investors, industry players and public authorities.

5 ANNOUNCEMENT

Submissions to the TrustChain Open Call #4 will open on 15 May 2024 (13:00 CEST) and close on 17 July 2024 (17:00 CEST). Dates for the different phases are outlined below but may be subject to change if any modifications in the project's schedule occur.

The table below presents the indicative dates during which each phase of TrustChain Open Call #4 will take place.

Call Announcement	15 May 2024 at 13:00 CEST
Call closure and submission deadline*	17 July 2024 at 17:00 CEST
Total EU funding available	1.989.000 €
Evaluation Period*	Up to three months after the call closure
Signature of Sub-grant Agreement*	Up to one month after the announcement of the final list of

	selected projects
Expected duration of projects	9 months
Task description	Navigating the intricacies of data transfer between blockchains poses a multifaceted challenge rooted in the complex landscape of knowledge, encompassing rules, policies, and regulations. Achieving seamless interoperability, scalability, security, energy efficiency, and high-speed transactions demands a comprehensive understanding of the diverse blockchain ecosystems involved. Interoperability is a key aspect, as different blockchains often operate on distinct protocols and consensus mechanisms, requiring a harmonized framework for effective state transfer. Scalability is equally crucial, especially in the context of a rapidly expanding blockchain landscape, necessitating solutions that can accommodate the increasing volume of transactions without compromising efficiency. In addition, the challenge extends to ensuring the security and privacy of transferred states, as sensitive data may traverse multiple blockchains. Striking a balance between privacy and transparency becomes imperative, necessitating robust encryption mechanisms and adherence to regulatory standards. Streamlining energy consumption while maintaining the desired speed of transactions is a delicate balance that demands innovative solutions. Some of the challenges to be tackled in this call are the following: • One of the fundamental challenges lies in reconciling the variations in protocols across diverse blockchains. Effectively designing gateways or bridges that can translate and adapt to these differences is crucial for ensuring seamless interoperability and facilitating smooth communication between blockchain networks whilst adhering to the European standards frameworks. • Ensuring a consistent and trusted knowledge transfer is challenging due to the diverse consensus mechanisms and governance models utilized by different blockchains. Hence, upholding data integrity across the chains will ensure the reliability of information exchange. • It is important to prioritize the security and privacy of transferred knowledge, requiring gateways to incorporate strong encryption and privacy-preserving techniques. Addressing this challenge is essential to safeguard sensitive data during the transfer process, ensuring a secure and confidential exchange that builds trust in information handling systems. • Adhering to regulatory standards across various jurisdictions is challenging and requires gateways to adeptly navigate diverse regulatory landscapes. It is essential to tackle this challenge to enable a legal and

	compliant transfer of knowledge between blockchains, fostering a smooth and responsible exchange of information across diverse regions in Europe and internationally. • With the expansion of blockchain networks and rising transaction volumes, ensuring the scalability of gateways becomes crucial. Innovative solutions that can meet the increased demands for data transfer while maintaining efficiency will facilitate the seamless functioning of the system. • The complex challenge lies in achieving a balance between high-speed data transfer and energy efficiency. Gateways should minimize energy consumption while ensuring the speed and reliability of data transfers, contributing to sustainable and resource-efficient information exchange. • Ensuring the compatibility and seamless execution of smart contracts across various blockchains is crucial. New solutions addressing this challenge will facilitate the smooth transition of smart contract logic and execution between diverse platforms, promoting interoperability and expanding the utility of decentralized applications. • The use of semantic standards and open ontology schemas that enable the effective transfer of information and knowledge across chains is essential for cross-chain interoperability. Specific solutions that may be used to achieve interoperability and conformity may facilitate significant technology uptake. • Ensuring the trustworthy use of digital identities across chains is required for the reliable exchange of value across chains. • The use of multiple chains requires expert knowledge and complex configurations. Widespread cross-chain adoption can only happen when the user experience is simple and seamless. • The intersection of AI, blockchain, IoT and cloud is very important for accountability, transparency and provenance, civil rights and citizen empowerment. • New more trustworthy decentralized internet protocols to avoid centralization of power and trusted third parties. • Enhancements in the blockchain, e.g., efficient blockchain bridges, more decentralized and green consensus mechanisms, app-specific consensus mechanisms, anonymous blockchains, blockchain speedups, etc. • Provide a mechanism to operate while the user cannot have the capability to use some of the existing online identity credentials. • Create a broker whereby the DIDs can be mapped to facilitate the interoperability challenges from

	multiple siloed systems. **Applications should cover real needs of the end-users in one a specific sector such as for example banking, education, healthcare, or e-government.** **A user centric design approach should frame the development of these solutions**
Submission and evaluation process	Proposals are submitted in a single stage and the evaluation process is composed of three phases as presented hereafter: • **Phase 1:** Admissibility & eligibility check • **Phase 2:** Proposals evaluation carried out by the TrustChain Consortium with the assistance of independent experts. • **Phase 3:** Online interviews (10 minutes pitching & 20 minutes of Q&As) and final selection carried out by TrustChain Consortium and TrustChain Advisory Board Members.
Further information	Further details are available at: https://TrustChain.ngi.eu/apply

***NOTE:** Dates for the different phases are indicative and may be subject to change if any modifications in the project's schedule occur.

6 SUPPORT TO APPLICANTS

The TrustChain consortium will provide information to the applicants only via TrustChain@ngi.eu. No binding information will be provided via any other means (e.g., telephone or email).

More info at: https://TrustChain.ngi.eu/apply
Apply via: https://www.f6s.com/TrustChain-open-call-4
Support team: TrustChain@ngi.eu
Personal Data Protection Policy available at: https://TrustChain.ngi.eu/privacy-policy/

The TrustChain consortium will also organise webinars to connect with interested applicants so stay updated and get involved!

7 KIT FOR APPLICATION

TrustChain Open Call #4 supported materials can be found at https://TrustChain.ngi.eu/apply and are the following:

Open Call #3 – Call document

The present document.

Annex A - Guide for Applicants

> This document provides in detail the information to help apply to the TrustChain Open Call #4, such as an abstract of the TrustChain action, a description of the TrustChain Open Call #4, the modalities for application, the evaluation process, the scheme of the funding support, the IPR aspects related to TrustChain and how to prepare and submit a proposal.

The kit also includes the Model Sub-grant Agreement (draft template only), Administrative form (read only), Proposal description and the Additional Applicants templates, as follows:

Annex B – Model Sub-grant Agreement – draft template only
Annex C - Administrative Form – read only
Annex D - Proposal Description template – read only
Annex E - Additional Applicants template – read only

Note: Word templates (Annex D and Annex E) are available at the F6S Submission System.