NGI TRUST CHAIN

ANNEX A

GUIDE FOR APPLICANTS

SECOND OPEN CALL FOR PROPOSALS

Closing dates for proposals: 20 September 2023 at 17:00 CEST

Version 1.0 – 20 July 2023

Funded by the European Union

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

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	CITY UNIVERSITY OF LONDON	ICS	UK

TABLE OF CONTENTS

Funded by the European Union

Funded by the European Union

1 PREAMBLE

This document is the main document to support applicants in the provision of their proposals. It provides the technical details for TrustChain Open Call #2 as well as the modalities for applications, the eligibility criteria, the evaluation process, the financial support, the preparation and submission of the proposal, the support services, the indicative timelines, the information requested for the administrative part of the proposal, the necessary template to be used to draft the proposal as well as an indicative agreement that will be signed if the proposal is successful. The guide is complemented by the Open Call #2 Annexes (Section Annexes) available at https://trustchain.ngi.eu/.

Today online user platforms and websites face significant security and privacy challenges that make them untrustworthy. With huge amounts of online data collected about users' activity and choices, later to only share them with numerous third parties, the user is left with little to no choice to maintain online privacy if they want to use online services. Online user privacy and data governance face numerous challenges in today's digital landscape. Here are some key challenges:

- **Data Collection and Consent:** Many online platforms and services collect vast amounts of personal data from users, often without their full understanding or explicit informed consent. Users may be unaware of how their data is being used or shared, leading to privacy concerns.
- **Data Breaches and Security:** Data breaches have become increasingly common, with hackers gaining unauthorized access to user data. These breaches expose sensitive information, such as passwords, financial details, and personally identifiable information, compromising user privacy and leading to identity theft or fraud.
- **Lack of Transparency:** Many online companies lack transparency in how they handle user data. Users often have limited visibility into data collection practices, data sharing with third parties, and the overall data governance framework of the platform. This lack of transparency hinders users' ability to make informed decisions about their privacy.
- **Third-Party Data Sharing:** Online platforms frequently share user data with third-party advertisers, marketers, and other service providers. This sharing of data raises concerns about user consent, control over personal information, and potential misuse or mishandling of data by these third parties.
- **Profiling and Targeted Advertising:** User data is often used to create detailed profiles and enable targeted advertising. This can lead to intrusive and personalized marketing strategies that erode user privacy and create a sense of constant surveillance.
- **Cross-Border Data Transfers:** The global nature of the Internet often involves the transfer of user data across borders. Differing data protection laws and regulations among countries can create challenges in ensuring consistent privacy standards and safeguarding user data during international transfers.
- **Surveillance and Government Access:** Government surveillance programs and data requests from law enforcement agencies can infringe upon user privacy. Balancing the need for public safety and law enforcement with individual privacy rights is a complex challenge in the digital age.
- **Lack of Control and Ownership:** Users often have limited control over their own data once it is shared online. This lack of control and ownership can make it difficult for

individuals to exercise their rights, including the right to access, correct, or delete their personal information.

- **Technological Advancements:** Rapid technological advancements, such as Artificial Intelligence and Machine Learning, pose additional challenges to user privacy and data governance. These technologies can process vast amounts of data, leading to potential privacy risks if not appropriately regulated and managed.

Addressing these challenges requires a combination of technological solutions, legal frameworks, and user education. Striking a balance between data-driven innovation and preserving user privacy is essential for a more transparent and secure online environment.

Trustworthy online platforms that preserve user's data privacy and provide strong data governance frameworks are the focus of this TrustChain Open Call #2 on "User Privacy and Data Governance".

Open Call #2 welcomes applications that will clearly define, upgrade/extend the state-of-the-art, and develop the following types of solutions:

- Enhanced Consent profiles to implement transparent and user-friendly consent mechanisms that clearly explain how user data will be collected, used, and shared. A mechanism to provide users the ability to form informed consent and easily manage their privacy preferences in data sharing models,
- Data Minimization and Purpose Limitation techniques built in the web framework so that only necessary data is collected for legitimate purposes. Data owners should have means to share only data necessary to access a particular service,
- Secure data exchange and privacy-aware data processing must be the cornerstone of the new data economy. Privacy of training data, machine-learning models and model parameters should be aimed for[1],
- Developing new privacy preserving data flow techniques in line with international data sharing agreements (e.g., EU Data Spaces) so that the user has choice to tune data parameters for trading/sharing of data,
- Develop new mechanisms in line with the international data flows standards so that the data can move freely within the EU and across international borders including USA, Japan and China,
- Data identification, data provenance, data tracking mechanisms should be built so that the data that is exchanged can be tracked. Handling of the data according to the user consent provided in a data exchange should be verifiable,
- Data certification/verification methods should be developed to verify the trustworthiness of the data,
- Modern privacy enhancing technologies, such as local differential privacy and other interactive privacy techniques, taking also into account online publicly available datasets that can be linked to the original data,
- Data obfuscation, perturbation and anonymization techniques or their combination that properly address the trade-off between privacy-preservation and data utility.

[1] https://plg.eu.com/the-cross-border-data-flow-the-oecd-report-for-the-g7-digital-and-technology-pathway/https://plg.eu.com/the-cross-border-data-flow-the-oecd-report-for-the-g7-digital-and-technology-pathway/

The above system examples are only indicative, and applicants can propose solutions that integrate one or more of them. Applicants can also submit a proposal under a different example scenario, as long as it serves the overall TrustChain vision and objectives, while also fitting within the scope of human centric decentralised trustworthy Next Generation Internet protocols. Proposed solutions should utilize existing concepts and technologies already developed for data value sharing and preserving user-privacy and fit within TrustChain's vision and objectives. The solutions should be provided as open-source software desirably at TRL 7, tested and evaluated by an adequate pool of potential end-users that should be identified and mentioned in the application, as well as supported by a self-sustaining business model for exploiting the developed system at 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.

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 present Open Call is to develop tools, cryptographic mechanisms, and other algorithms for data handling and sharing as well as for the management of data lakes in compliance with 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,

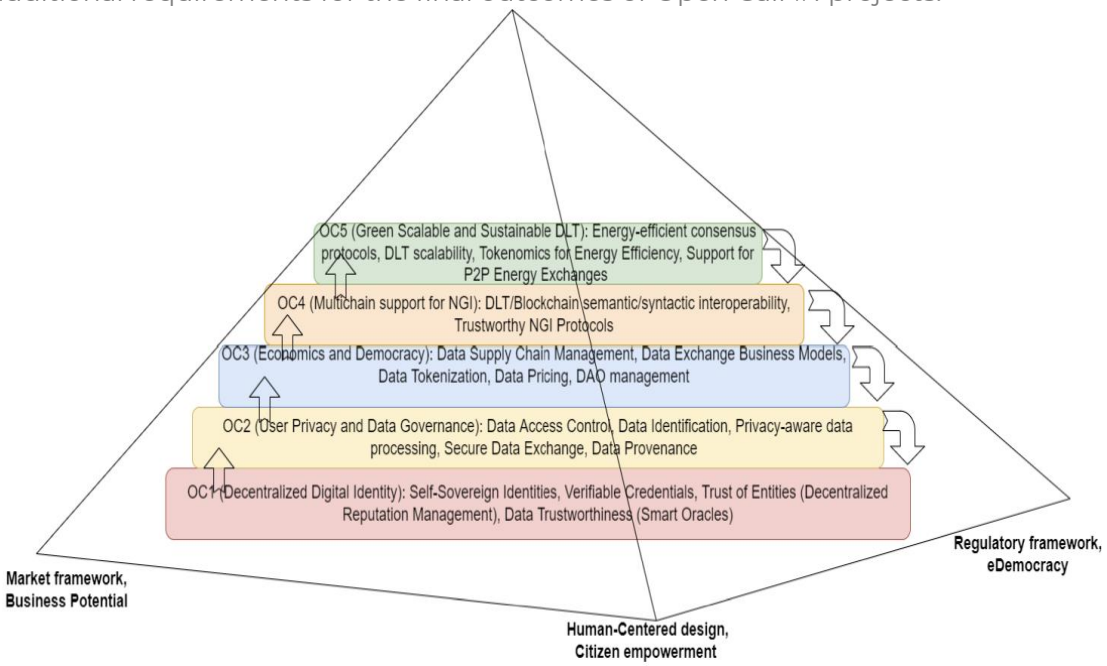
- Privacy-preserving usage of Artificial Intelligence, IoT, Cloud or combinations of those environments to provide the decentralised next generation smart digital services.

Open Call #3- Economics and democracy
The objective of Open Call #3 will be 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
Open Call #4 goal will be 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 will be a cornerstone in 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 #2 can pose additional requirements for the final outcomes of Open Call #1 projects.



In this technological framework, TrustChain Open Call #2 is thus closely related to Open Call #3 “Economics and democracy” and Open Call #4 “Multi chains support for NGI protocols”. Better solutions to user privacy and data governance will ensure better data economics and democracy and subsequently encourage ways for multi-chain interaction to exchange data/assets. Thus, knowledge created within this Open Call #2 will be transferred / integrated into future Open Call #3 and Open Call #4 calls.

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 #2 and outlines its context and its application modalities.

3 OPEN CALL #2: USER PRIVACY AND DATA GOVERNANCE

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 #3-5 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 #2 vision and objectives. Their proposed solution should consider as minimal requirement to:

- Use standard technology for full stack development,
- Be open source,
- Extend the state-of-the-art in the domain of user privacy, and/or solve existing real-world problems with 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 3.2) 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 user privacy and data governance needs or challenge they propose to address and who would benefit from it 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 #2 challenges they are going to address. Those are described in the section 3.3.

3.2 SPECIFIC OBJECTIVES

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

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

- Mechanisms for multi-party data sharing that lies in the scope of the call and addresses the stated challenges below,
- Protocols for privacy-preserving data sharing using techniques from technologies such as federated learning both vertical and horizontal framework,
- Privacy-preserving data processing, data storage and data computation techniques such as differential privacy, data obfuscation/perturbation, anonymization techniques,
- Encrypted data analytics based on homomorphic encryption and Trusted Execution environment,
- Protocols to verify authenticity and accuracy of data using technologies like zero knowledge proofs,

- Protocols to support the digital sovereignty-based data flow and data spaces initiatives.
- Data identification, data provenance, data tracking mechanisms or protocols should be built so that the data that is exchanged can be tracked, so that trustworthy data handling according to the user consent can be verified.

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

3.3 CHALLENGES TO BE ADDRESSED

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

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

- The online data sharing model is flawed as it encourages data duplication, long term data retention and intensive data collection across service providers. There is also lack of data traceability and accountability in online data sharing,
- Privacy is important when user data is employed for training machine learning models and computation. Information leakage in training models is a persistent problem. Local differential privacy with federated learning models can be explored to address this challenge,
- Data accuracy vs privacy trade-off in privacy-preserving techniques like differential privacy is an open challenge and its solution can be key to solving many open-source data sharing issues,
- Privacy-aware data processing needs to be encouraged from the design phase of any data sharing/processing protocol,
- Similarly, illegal data copying is a big challenge in user privacy and data governance models today which needs to be addressed,
- A trust layer is missing, and it is often difficult to ensure authenticity of data. Thus, trustworthy data access and data integrity mechanisms based on SSI technologies, including decentralized identifiers and Verifiable Credentials, needs to be designed,
- In line with providing a trust layer supporting user privacy, data provenance ontologies and data transaction logging should be available to users,
- Users have little to no control over access to their personal data shared online. Therefore, automated user consent/smart user consent for data sharing needs to be implemented,
- Data owners currently do not have means to be compensated or to enable fair data value sharing with the big players in the market. When users want to participate in the

data economy, they should be able to do so by means of data tokenization/trading capabilities,
- Users should be empowered to add the necessary levels of anonymity in order to share their data with a third party.

A user centric design approach should frame the developed solution carefully consider the following:

- data privacy protection,
- privacy aware data processing,
- data provenance,
- data use policies,
- data retention and data deletion, right to be forgotten, data minimization, and trustworthiness,
- data minimization and user informed data deletion.

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 be also 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.

Finally, focus should also be put on 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: This Open Call is closely related to Open Call #1 "Decentralized digital identity". Solutions to be developed in Open Call #2 should consider some of the approaches and outcomes identified in Open Call #1 for digital identity management. Joint activities between Open Call #1 and Open Call #2 innovators will be facilitated by the Trust Chain 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

Applicants are requested to present in a clear and concise manner any existing and/or emerging privacy-enhancing data sharing platform (i.e., GAIA-X & IDS, DECODE) / infrastructure standards with which they intend to comply with, or they wish to contribute to within the course of the proposed project. They should also identify how the project aligns with the Digital Services Act (DSA) and the Digital Market Act (DMA).

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. The co-creation and validation approach should be 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. Once this is done, the users should be involved in the co-creation process. Then, accessibility standards should be incorporated through the onboarding according to the vulnerable collectives' approach.

Following that, a roadmap with the appropriate methodologies should be set up. The roadmap should include the approach, objectives and phases of the testing, and sample size. The

sample needs to be representative and randomized but within the relevant characteristics of the target population.

User should be onboarded in the design process (if applicable). Proposals for improvement and insights should come from the users during the co-creation process. Complementarily, insights can be proposed by non-users (for example developers, or business partners). This decision must be justified in the corresponding deliverable.

3.5 EXPECTED OUTCOMES AND POSSIBLE APPLICATION DOMAINS

Open APIs, SDK, and libraries related to privacy-enhancing technologies and privacy-aware data sharing are expected outcomes. These outcomes should provide:

- Privacy-preserving data oracles,
- Privacy-preserving data processing techniques using technologies such as Homomorphic Encryption and Trusted Execution Environments,
- Data anonymization and perturbation techniques,
- Privacy-by-design microservice architectures,
- General-purpose DLT-based solutions for privacy and data governance,
- Smart contracts for user privacy and data governance.

Possible use-cases and application domains include the following:

- Records of data processing activities (ROPAs) with verification and certification for GDPR-policy compliance,
- Data processing in Trusted Execution Environments,
- Consent management systems,
- Collaborative secure data sharing platforms,
- Privacy-preserving social networks,
- Privacy preserving machine learning models.

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.

4 MODALITIES FOR APPLICATION

4.1 WHAT TYPES OF PROJECTS WILL BE ELIGIBLE?

Applications must be based on the Open Call #2's Proposal Description template (Annex D) and must clearly fit within the objective of TrustChain Open Call #2 described in subsection 3.1.

Furthermore, applicants should demonstrate their long-term commitment to the TrustChain Research and Innovation agenda. Selected proposals will work to demonstrate that the proposed solution progresses from the beginning of the project, reaching a higher maturity level and take-up by the end of the action. Thus, all the projects must provide evidence of substantial progress with a particular focus on the interoperability and sustainability of the outcomes according to the TrustChain framework.

Following the spirit of the calls for the Next Generation Internet, the TrustChain Research and Innovation Action encourages open-source software and open hardware design, open access to data, standardisation activities, access to testing and operational infrastructure as well as an IPR regime ensuring interoperability, reusability of results, lasting and sustainable impact. If the expected results of the proposed project cannot be released as open source, it should be duly justified in the application document.

4.2 WHAT HAPPENS AFTER THE PROPOSALS ARE SUBMITTED?

Immediately after the submission deadline (please see subsection 5.6) is over, the evaluation process begins (as described in detail in Section 6). Experts will evaluate proposals and score them according to the quality of the content presented.

The goal of the process is to select up to 17 high value proposals with the procedure defined in Section 6. The selected applicants will be invited to join the TrustChain Research and Innovation Action. The exact number of selected projects will be subject to the quality of the proposals and the funding available.

5 ELIGIBILITY CRITERIA

All applicants will have to abide by all general requirements described in this section to be considered eligible for TrustChain. **Therefore, applicants are requested to read the following section carefully.**

5.1 TYPES OF APPLICANTS

The target applicants of this call are developers, innovators, researchers, SMEs, and entrepreneurs working on different NGI relevant topics and application domains at the intersection between the technical field (e.g., Software Engineering, Network Security, Semantic Web, Cryptography, Blockchain, Digital Twin, Blockchain Security, Digital Identity, Blockchain Protocol), the Social sciences and Humanities (e.g., Social Innovation, not-for-profit sector, Social Entrepreneurship, public goods) as well as any others including economics, environment, art, design, which can contribute to the NGI TrustChain relevant vision.

Applicants can apply as individuals or linked to a legal entity. Hence, the participation is possible in several ways:

- **Team of natural person(s):**
  Team of individuals, all established in any eligible country (see subsection 5.2). This does not consider the country of origin but the residence permit.
- **Legal entity(ies):**
  One or more entities (consortium) established in an eligible country (see subsection 5.2). The entities can be Universities, Research centres, Non-Governmental Organisations, Foundations, micro, small and medium-sized enterprises (see definition of SME according to the European Commission Recommendation 2003/361/EC), large enterprises working on Internet or/and other related technologies are eligible.
- **Any combination of the above.**

In addition, the following conditions apply:

- The participating entities should not have been declared bankrupt or have initiated bankruptcy procedures.
- The entities or individuals (Team of natural persons) applying should not have convictions for fraudulent behaviour, other financial irregularities, and unethical or illegal business practices.

5.2 ELIGIBLE COUNTRIES

Only applicants legally established/resident in any of the following countries (hereafter collectively identified as the “Eligible Countries”) are eligible:

- The Member States (MS) of the European Union (EU), including their outermost regions.
- The Overseas Countries and Territories (OCT) linked to the Member States[2];
- Horizon Europe associated countries, as described in the Reference Documents and the List of Participating Countries in Horizon Europe according to the latest list published by the European Commission.

[2] Entities from Overseas Countries and Territories (OCT) are eligible for funding under the same conditions as entities from the Member States to which the OCT in question is linked.

5.3 LANGUAGE

English is the official language for TrustChain's Open Calls. Submissions written in any other language will be disregarded and not evaluated.

English is also the only official language during the whole execution of the TrustChain programme. This means submitted deliverables must be written in English in order to be accepted.

5.4 PROPOSAL SUBMISSION

Proposals must be submitted electronically, using the **TrustChain Online Submission Service** accessible via https://www.f6s.com. Proposals submitted by any other means will not be evaluated.

Only the documentation included in the proposal will be considered by evaluators. It is composed by a form with administrative data (Annex C) to be completed directly in the platform and the proposal description (Annex D) attached in PDF format. **Applicants must strictly follow the proposal template provided in the annexes as well as the page limitation.**

The information provided should be actual, true, and complete and should allow the assessment of the proposal.

The preparation and submission of the proposal and other actions that follow this procedure (such as withdrawal) fall under the final responsibility of the applicant.

5.4.1 Data Protection

In order to process and evaluate applications, the TrustChain consortium will need to collect Personal and Industrial Data. F6S Network Ireland Limited, will act as Data Controller for data submitted through the F6S platform for these purposes. A Data Protection Officer (DPO) has been appointed by F6S generally, to ensure compliance with data protection regulations, such as the General Data Protection Regulation (GDPR), and that personal data is collected, processed, and stored in a secure manner.

The F6S platform's system design and operational procedures ensure that data is managed in compliance with the General Data Protection Regulation (EU) 2016/679 (GDPR)[3]. Each applicant will accept the F6S terms to ensure compliance. Please refer to https://www.f6s.com/privacy-policy to review the F6S platform's privacy policy and data security policy.

Apart from the F6S platform, data will also be stored in the F6S Google Drive, in the project repository on MS Sharepoint, and on the EasyChair platform, both managed by the project

[3] https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html

coordinator European Dynamics.

Please note that the TrustChain consortium must retain generated data until five years after the balance of the TrustChain project is paid or longer if there are ongoing procedures (such as audits, investigations or litigation). In this case, the data must be kept until the end.

5.4.2 Multiple submissions

Given the fact that this call is competitive, applicants should focus on only one specific topic as follows:

- **Only one proposal per applicant should be submitted to this call**, and only one proposal per applicant will be evaluated. In the event of multiple submissions by an applicant, only the last one received (according to the timestamp of the submission portal) will enter the evaluation process. Any other submitted proposals by the same applicant or involving the same applicant will be declared non-eligible and will not be evaluated in any case.
- **Only one proposal per individual should be submitted to this call** whether he/she applies as a member of a Team of Natural Persons or as part of a Team/Consortium. If an individual is taking part in several teams/consortiums, the members of the other teams/consortium will be informed about the participation of an individual in multiple teams/consortiums. Then, only the last proposal received (according to the timestamp of the submission portal) including the individual will enter the evaluation process. Any other submitted proposals involving this individual will be declared non-eligible and will not be evaluated in any case.

Note that the regular functioning of the F6S platform limits to one application submission per F6S user in each call. If an F6S user wishes to submit more than one application, **for example on behalf of different applicants**, the F6S user should request support from the F6S support team (support@f6s.com) at least 10 days prior to the open call deadline.

5.4.3 Participation to the five TrustChain's Open Calls and funding rules

TrustChain is an opportunity to fund truly multidisciplinary projects involving partners from different (natural and humanistic) disciplines relevant to Internet development. Thus, applicants can apply, participate and benefit from the five TrustChain's open calls but as the main objective of the action is to support a large number of third parties through open calls, **the maximum amount to be granted to each third party is 200,000.00 €** to allow cases were a given legal entity (e.g. large research, academic or industrial organisations) may receive several grants (e.g. from different calls).

5.4.4 Complaint due to a technical error of the TrustChain Online Submission Service

If you experience any problem with the application submission system prior to the deadline of the open call, you should contact F6S using the e-mail support@f6s.com, cc'ing the TrustChain

Team (trustchain@ngi.eu), and explain your problem.

If you believe that the submission of your proposal was not entirely successful due to a technical error on the side of the TrustChain Online Submission Service, you may lodge a complaint by email to support@f6s.com cc'ing the TrustChain Team (trustchain@ngi.eu) and explain your situation. For the complaint to be admissible it must be filed within **three calendar days following the day of the call closure.** You will receive an acknowledgement of receipt, in the same or next working day.

What else to do? You should secure a PDF version of all the documents of your proposal holding a timestamp (file attributes listing the date and time of creation and last modification) that is prior to the call deadline, as well as any proof of the alleged failure (e.g., screen shots). Later in the procedure you may be requested by the TrustChain IT Helpdesk to provide these items.

For your complaint to be upheld, the IT audit trail (application log files and access log files of TrustChain Online Submission Service) must show that there was indeed a technical problem on the TrustChain consortium side that prevented you from submitting your proposal using the electronic submission system.

Applicants will be notified about the outcome of their complaint within the time indicated in the acknowledgment of receipt. If a complaint is upheld, the secured files (provided to the IT helpdesk) for which the investigation has demonstrated that technical problems on the TrustChain consortium side prevented submission will be used as a reference for accepting the proposal for evaluation.

5.5 CONFIDENTIALITY

Any information regarding the proposal will be treated in a strictly confidential manner.

5.6 DEADLINE

Proposals must be submitted before 20 September 2023 at 17:00 CEST. To avoid missing the deadline, you are encouraged to submit your proposal as soon as possible.

Only proposals submitted before the deadline will be considered for evaluation. After the call closure, no additions or changes to receive proposals will be considered.

5.7 CONFLICT OF INTEREST

Applicants (even individual members of applicants) shall not have any actual or/and potential conflict of interest with the TrustChain Selection Process and during the whole programme. All cases of conflict of interest will be assessed case by case. In particular, applicants (even individual members of applicants) cannot be TrustChain Consortium partners or affiliated entities nor their employees or co-operators under a contractual agreement, nor a member of the TrustChain Advisory Board.

If a conflict of interest is discovered and confirmed at the time of the evaluation process, the proposal will be considered as non-eligible and will not be evaluated.

5.8 OTHER

Each applicant must confirm:

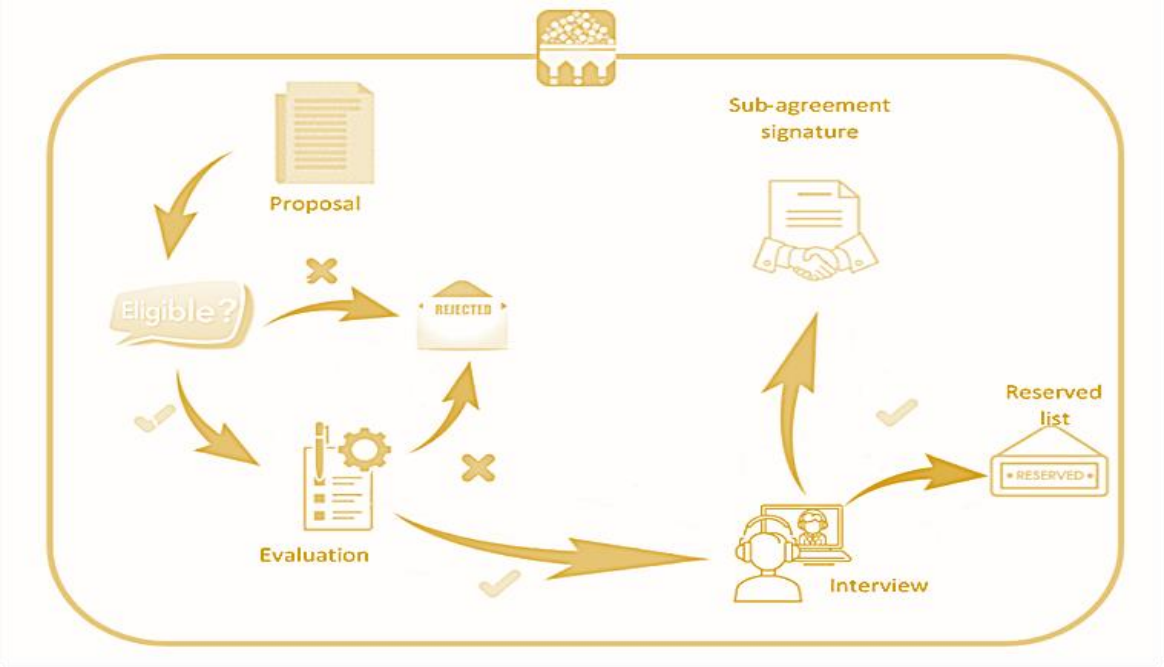
- It is not under liquidation or is not an enterprise under difficulty according to the Commission Regulation No 651/2014, art. 2.18,
- Its project is based on the original works and going forward any foreseen developments are free from third party rights, or they are clearly stated,
- It does not receive extra funding for the development of its proposal from any other public or private entity,
- It is not excluded from the possibility of obtaining EU funding under the provisions of both national and EU law, or by a decision of both national or EU authority,
- Via the principal investigator that he/she agrees with the terms presented in Annex B – Model Sub-grant Agreement draft template.

6 PROPOSAL EVALUATION AND ACCESS TO TrustChain FUNDING

6.1 EVALUATION PROCESS

Proposals are submitted in a single stage and the evaluation process is composed of three stages as presented hereafter.

- **Stage 1**: Admissibility & eligibility check
- **Stage 2**: Proposals evaluation
- **Stage 3**: Online interviews and final selection



6.1.1 Admissibility and eligibility check

Admissibility and eligibility criteria for each proposal are performed by the TrustChain Consortium staff. A proposal may be declared ineligible or inadmissible at any stage.

To be considered admissible, a proposal must:

- Be submitted in the electronic submission system before the call deadline,
- Be compliant with the specific eligibility conditions set out in the relevant parts of this guide (see Section 5). The eligibility filter enables the creation of a shortlist of proposals to be evaluated,
- Be readable, accessible and printable,
- Be completed and include the requested administrative data, and any obligatory supporting documents specified in the call (following the template presented in Annex D, compulsory, and Annex E, if necessary),
- Include the proposal description. Applicants must strictly follow the template instructions as well as the page limitations for drafting the research proposal that are included in this guide (Annex D). A proposal will only be considered eligible if its content corresponds specifically to the objective of the TrustChain Open Call #2 or is proposed as an “open topic” and demonstrates that it aims to advance the state-of-the-art especially with regards to the TrustChain Open Call #2 Framework and application domain.

6.1.2 Proposal evaluation

The evaluation of proposals is carried out by the TrustChain Consortium with the assistance of independent experts. TrustChain Consortium ensures that the process is fair and in line with the principles contained in the European Commission's rules on Proposal submission and evaluation. To facilitate the independent experts and the evaluation process, the EasyChair platform (https://easychair.org/) will be used.

Experts perform evaluations on a personal basis, not as representatives of their employer, their country or any other entity. They are required to be independent, impartial, and objective, and to behave throughout the process in a professional manner. The experts sign an expert contract, including a declaration of confidentiality and absence of conflict of interest, before beginning their work.

All experts must declare beforehand any known conflicts of interest and must immediately inform the TrustChain Consortium if they detect a conflict of interest during the evaluation. The expert contract also requires experts to maintain strict confidentiality with respect to the whole evaluation process. They must follow all instructions given by the TrustChain Consortium to ensure this. Under no circumstance may an expert attempt to contact an applicant on his/her own account, during the evaluation process. Confidentiality rules must be always adhered to before, during, and after the evaluation.

Each proposal is evaluated by a set of 2 experts (one from the TrustChain Consortium and one independent) according to the following criteria:

1-Excellence and innovation (40% weighting)

- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context and credibility of the proposed methodology including the User Centric Approach
- Extend that the proposed work is beyond the state of the art, and demonstrates innovation potential in relation to TRUSTCHAIN objective (e.g. ground-breaking objectives, novel concepts and approaches, new products, services or business and organisational models)
- Evaluate the degree to which the human centric methodology is clearly described and sound.
- Evaluate the appropriateness and soundness of the technical approach.

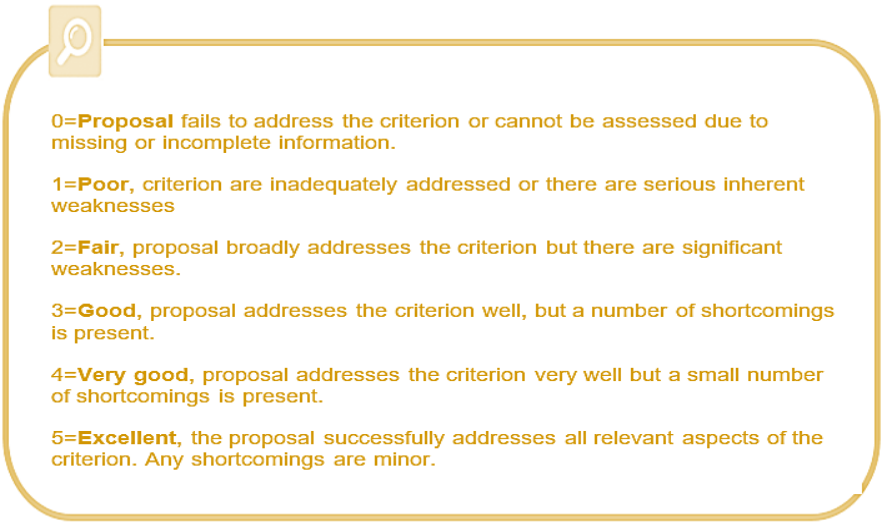
2-Expected impact and value for money (30% weighting)

- Contribution to TRUSTCHAIN overall goal 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.
- Impact of the innovation on the needs of European and global markets is clearly provided and relevant KPIs are available.
- Quality of the proposed measures to exploit and disseminate the project results (including management of IPR), and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.

3-Project Implementation (30% weighting)

- Quality and effectiveness of the work plan, including extend to which the resources assigned to the work are in line with its objective and deliverables and milestones.
- Required mandatory deliverables are provided.
- Quality and effectiveness of the management procedures including risks and mitigation management.
- Integration of the solution to the overall TRUSTCHAIN ecosystem.
- Team is properly established and includes the key expertise to achieve the objectives.

Experts will score each award criterion on a scale from 0 to 5 (half point scores may be given):



For each criterion, the minimum threshold is 3 out of 5 points. The default overall threshold, applying to the sum of the three criteria scores with the corresponding weight each, is 10.

Each expert prepares an individual evaluation report.

Following the individual evaluations by the two experts, a consensus meeting, typically mediated by the evaluation tool is organised between the two experts to achieve a consensus between them on the quality of the proposal based on the two evaluation reports. Comments and scores are validated by the two experts in a consolidated evaluation report.

When necessary, an additional review of projects for which there was a lack of consensus in terms of scoring by the two experts or for which additional clarifications are required is undertaken by the TrustChain Call Referent (member of the TrustChain Consortium). In this case, an additional independent evaluator is appointed to review the proposal. The final score is obtained based on the consensus of the 3 evaluators, one internal and 2 externals to the consortium.

The TrustChain Consortium then formally approves the ranking list.

The admission to the online interview for applications follows this rule: **the 20 highest-ranked proposals are admitted to the online interview.** The TrustChain Consortium may decide to invite more proposals to be part of the online interview stage in case for example of *ex-aequo*.

In any case, all proposals admitted to the online interview must reach all score thresholds.

Regarding the communication of the results, each applicant will receive via e-mail a letter informing them of the decision, which can be either a rejection decision supported by an Evaluation Summary Report or an invitation to the online interview session.

Funded by the European Union

6.1.3 Online interview and final selection

According to the rules, the top projects at the end of the proposal evaluation stage will be invited to the final selection stage. The applicants invited to the online interview will receive via e-mail, an invitation letter the online interview as well as relevant guidelines. **It is worth mentioning here that an invitation to the interview is not a formal invitation for funding.** The interview aims to better understand the project concept, scope, and centrality to the TrustChain vision, the team skills and competencies, capacity, and willingness to exploit the results under a commonly agreed plan with the rest of the TrustChain ecosystem and TrustChain partners. Most importantly, the online interview aims to clarify still unclear aspects of the proposal which have been identified during the proposal evaluation. The proposal evaluation report is not circulated to the applicants before the interview but forms the basis for the interaction with them.

In practice, the interview will be carried out by the evaluation board composed of the TrustChain core partners and the TrustChain advisory board members. It will be recorded to assure maximum transparency. It is based on 10 minutes pitch presentation and 20 minutes of Q&As to clarify some aspects regarding the quality of the proposal and its relevance for TrustChain, as well as to reach a final agreement about scores and the Evaluation Summary Report (ESR). The comments on the ESR are taken into consideration for the preparation of relevant questions during the online interview and they are not communicated beforehand to the applicants.

The ESR will be structured according to the 3 criteria mentioned in the previous section (i.e., excellence and innovation, expected impact and value for money, project implementation) and will consolidate the comment of the proposal evaluation and the clarifications and overall impression obtained during the online interview. Based on the final consolidate score, the short list of winners will be produced and only at this stage the final ESR will be communicated to the applicants.

Remaining proposals will be maintained on a reserve list and potentially be later admitted in case of withdrawal or failure of one of the projects initially admitted to successfully complete any phase of the contract signing process.

The list of selected projects is then submitted to the European Commission for final screening and validation.

6.1.4 Scientific misconduct and research Integrity

Issues of scientific misconduct and research integrity are taken very seriously. In line with the Horizon Europe Rules for Participation, appropriate action such as disqualification of the application, termination of the Grant Agreement Preparation phase or, if the Grant Agreement has been signed, the implementation of liquidated damages and financial penalties, suspension of payments, recoveries and termination of the Grant Agreement, will be taken against any applicants/beneficiaries found to have misrepresented, fabricated or plagiarised any part of their proposal.

6.2 THE AGREEMENT PROCESS

The objective of the agreement process is to fulfil the legal requirements between the TrustChain consortium and each selected project of the call. It covers essentially the status information of the beneficiaries. The legal requirements for legal entities and natural persons are provided in the table hereafter.

<table>
<tr><th>For legal entities</th><th>For teams of natural persons</th></tr>
<tr><td>A legal existence:
Company Register, Official Journal and so forth, showing the name of the organization, the legal address and registration number and, if applicable, a copy of a document proving Intra EU VAT registration (in case the VAT number does not show on the registration extract or its equivalent)
Specifically for SMEs:
1. A proof of the SME condition is required:
- If the applicant has been fully validated as an SME on the Beneficiary Register of the H2020 Participant Portal, the PIC number must be provided.
- If the applicant has not been fully validated as an SME on the H2020 Participant Portal, the following documents will be required to prove the status as an SME:
2. In the event the beneficiary declares being non-autonomous, the balance sheet and profit and loss account (with annexes) for the last period for upstream and downstream organizations is required.
3. Status Information Form. It includes the headcount (AWU), balance, profit & loss accounts of the latest closed financial year and the relation, upstream and downstream, of any linked or partner company.
4. Supporting documents. In cases where either the number of employees or the ownership is not clearly identified: any other supporting documents which demonstrate headcount and ownership such as payroll details, annual reports, national regional, association records, etc.</td><td>A copy of the ID-card or passport of participant(s) in the project team will be required.

A proof for each participant in the project that (s)he is legally established and working in an eligible country (see section 3.2).</td></tr>
<tr><td colspan="2">Bank account information:
The account where the funds will be transferred will be indicated via a financial information form signed by the entity, individuals, and the bank owners. The holder of the account will be the legal entity and/or all the individuals or the coordinator of the group on its own (consortium of legal entities or consortium of legal entities and natural persons) if allowed by the other team members.</td></tr>
<tr><td colspan="2">Sub-grantee funding agreement:
Signed between the TrustChain Consortium (represented by its coordinator European Dynamics), and the beneficiary/ies.
Have a careful look at the document in Annex B.</td></tr>
</table>

This information will be requested by the TrustChain consortium according to specific deadlines. Failure to meet the deadlines requested will directly end the agreement process. These deadlines will be announced in the decision letter sent to successful applicants.

6.3 MONITORING PROCESS ALL ALONG THE SUB-PROJECTS DURATION

For the monitoring of the progress and proper evolution of the selected projects, selected Third Parties will have to attend several mandatory internal events organised with the TrustChain Consortium. Indicatively, they are the following:

- Kick-off event devoted to knowing the different selected Third Parties and their foreseen contribution to TrustChain,
- Meeting for setting-up clear KPIs that will be linked to the funding of the selected Third Parties,
- Midterm event devoted to following-up the progress of the Third Parties according to the defined KPIs, with a pitch contest where the Third Parties will present their project outcomes and in particular their prototype and their deployment scenarios,
- Final event with a pitch contest where the Third Parties will present their solutions and in particular their modularised software components ready for distribution and a demo of their solution.

6.4 FINANCIAL SUPPORT

Open Call #2 budget totals 1.989.000,00 € to support up to 17 projects.

6.4.1 Indicative distribution of the funds

Selected third party innovators will become part of the TrustChain programme and will go through an exhaustive sequential process which will last 9 months. The maximum amount of the fund will vary depending on the type of team (see sub-chapter 3.1) as indicated in the table below and providing that all the phases have been completed.

Type of team	Maximum funding
Team of natural persons	97K € + 2K €
Legal entity or consortium of legal entities or combination of legal entities and natural persons	115K € + 2K €

Payments will be done in 4 instalments based on concrete results (a prefinancing, two interim payments and a final payment). A detailed evaluation process will be presented in the TrustChain Open Call #2 guide for implementation for the related periods. **The 2,000.00 € extra funding will be provided in case of the project outcome results in a peer reviewed journal publication with a minimum impact factor of 2.5.**

- **Beginning of the implementation and pre-financing:**
  During the first weeks of the project implementation, each team will define with their

coaches a set of clear and objective KPIs to be achieved and linked with the funding. These KPIs are different for each team and are related to the solution to be implemented. They will help measure the project progress, but also the commitment and involvement of the third party innovator (i.e., their consistency in attending periodic call meetings with the coaches, meeting the deadlines for reporting, among other criteria). After the definition of the KPIs, **a pre-financing of 30% of the sub-grant amount will be released**.

- **First midterm review and second instalment:**
  At first midterm of the project implementation, the coaches will assess the KPI's percentage of execution of the project based on the evaluation of the deliverable D2. A 100% completion of the KPIs for the related period will unlock the total of the 2nd payment which is **20% of the total sub-grant amount**. A lower completion of the tasks will launch the proportional payment. If the KPIs for the related period are met by less than 50%, the payment will be retained until the KPIs for the period are assessed as completely reached. If less than 25%, the third party innovators will be automatically disqualified from the process.

- **Second midterm review and third payment:**
  At the second midterm of the project implementation, the coaches will assess the KPI's percentage of execution of the project based on the evaluation of the deliverable D3. A 100% completion of the KPIs for the related period will unlock the total of the 2nd payment which is **30% of the total sub-grant amount**. A lower completion of the tasks will launch the proportional payment. If the KPIs for the related period are met by less than 50%, the payment will be retained until the KPIs for the period are assessed as completely reached. If less than 25%, the third party innovators will be automatically disqualified from the process.

- **Final review and final payment:**
  At the end of the project implementation, third parties will be paid according to their overall completion of KPIs materialised by the deliverable D4. A final event will be used to evaluate third parties on a face-to-face pitch contest. The third parties will present their implemented solution, and their business plan in the context of TrustChain. A panel of evaluators consisting of the TrustChain Consortium and Advisory Board members, will assess the third-party innovators to release the final payment (**remaining 20% of the sub-grant amount**). In the case of an underperformance below 25%, the team will be disqualified, and no further payment will be released.

6.4.2 Summary of the funding per type of beneficiary

	Project			
	Pre- financing 30% of the total funding	Interim Payment 20% of the total funding	Pre- financing 30% of the total funding	Final Payment 20 % of the total funding
Indicative dates	M2	M4	M7	Project end
Team of Natural persons	29 100 €	19 400 €	29 100 €	19 400 €
Legal Entity(ies) or combination of legal entities or combination of legal entity (ies) and individual(s)	34 500 €	23 000 €	34 500 €	23 000 €

These numbers are indicative, detailed payment schedule and payment conditions will be settled in the Sub-grant Agreement (Annex B) at the time of the signature.

6.4.3 Origin of the Funds and specific Provision regarding multiple beneficiaries

Any selected proposer will sign a dedicated Sub-Grant Agreement (Annex B) with the TrustChain project coordinator (on behalf of TrustChain Consortium).

Specific provision regarding contracting in case of multiple beneficiaries:

In the case of projects with multiple beneficiaries (Team of natural persons, combination of legal entities, combination of legal entities and individual(s)), a Team/Consortium Agreement that designates among other the Coordinator/Authorized representative of the Team/Consortium must be adopted and signed by all the beneficiaries prior to the signature of the TrustChain Sub-grant Agreement.

The Coordinator/Authorized representative of the Team/Consortium signs the TrustChain Sub-grant Agreement on behalf of the multiple beneficiaries.

The Coordinator/Authorized representative receives the funding and must distribute the payments between the beneficiaries according to the conditions set in the Team/Consortium Agreement.

The funds attached to the Sub-Grantee Funding Agreement come directly from the funds of the European Project TrustChain, and the TrustChain consortium is managing the funds according to the Grant Agreement Number 101093274 signed with the European Commission.

As will be indicated in the Sub-Grant Agreement, the relation between the sub-grantees and the European Commission through the TrustChain project carries a set of obligations to the sub-grantees with the European Commission. It is the task of the sub-grantees to accomplish these obligations, and of the TrustChain consortium partners to inform about them.

7 PREPARATION AND SUBMISSION OF THE PROPOSALS

The submission will be done through the F6S platform (https://www.f6s.com) which is directly linked with the TrustChain Programme. The applicants are required to register a profile at F6S to be able to submit a proposal.

The documents that will be submitted are:

- **Application form (Annex C):** administrative questions to be completed directly in the F6S platform. In addition, some general questions for statistical purposes and tick boxes to be clicked by the third parties confirming they have read the conditions and agree with the conditions defined in this document. In addition, an Annex E will be uploaded in case that more than 3 applicants participate as individuals (natural persons) or/and more than 3 applicants participate as organisations (Legal entities) filled with the information about the applicant(s) that do not fit in the application form.
- **Proposal description (Annex D)**: document in PDF format containing the description of the project. It will include three sections:
  (1) Project Summary,
  (2) Organisation background,
  (3) Detailed proposal description.

The project proposals must strictly adhere to the template provided by the TrustChain consortium via the F6S platform, which defines sections and the overall length.

Participants are requested to carefully read and follow the instructions in the form. Evaluators will be instructed not to consider extra material in the evaluation.

Additional material, which has not been specifically requested in the online application form, will not be considered for the evaluation of the proposals. Data not included in the proposal will not be considered.

It is strongly recommended not to wait until the last minute to submit the proposal. Failure of the proposal to arrive in time for any reason, including communication delays, automatically leads to rejection of the submission. The time of receipt of the message as recorded by the submission system will be definitive.

TrustChain offers a dedicated support channel available for proposers at trustchain@ngi.eu for requests or inquiries about the submission system or the call itself. Those received after the closure time of the call will neither be considered nor answered.

8 APPLICANTS COMMUNICATION FLOW

8.1 GENERAL COMMUNICATION PROCEDURE

Applicants will receive communications after each step of the evaluation process indicating whether they passed or not. A communication will also be sent to applicants rejected, including the reasons for the exclusion.

8.2 APPEAL PROCEDURE

If, at any stage of the evaluation process, the applicant considers that a mistake has been made or that the evaluators have acted unfairly or have failed to comply with the rules of this TrustChain Open Call, and that her/his interests have been prejudiced as a result, the following appeal procedures are available.

A complaint should be drawn up in English and submitted by email to trustchain@ngi.eu.

Any complaint made should include:

- Contact details.
- The subject of the complaint.
- Information and evidence regarding the alleged breach.

Anonymous complaints or those not providing the aforementioned information will not be considered.

Complaints should also be made within **five** (calendar) days since the announcement of the evaluation results to applicants.

As a general rule, the TrustChain Team will investigate the complaints with a view to arriving at a decision to issue a formal notice or to close the case within no more than twenty days from the date of reception of the complaint, provided that all the required information has been submitted by the complainant. Whenever this time limit is exceeded, the TrustChain Consortium will inform the complainant by email of the reasons for the unforeseen delay and the subsequent steps.

9 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.

10 INTELLECTUAL PROPERTY RIGHTS (IPR)

The ownership of IPR created by the beneficiaries, via the TrustChain funding, will remain with them. Results are owned by the Party that generates them.

The Sub-Grant Agreement (Annex B) will introduce provisions concerning joint ownership of the results of the sub-granted projects.

11 COMMUNICATION OBLIGATIONS

Any communication or publication of the beneficiaries shall clearly indicate that the project has received funding from the European Union via the TrustChain project, therefore displaying the EU and project logo on all printed and digital material, including websites and press releases. Moreover, beneficiaries must agree that certain information regarding the projects selected for funding can be used by the TrustChain consortium for communication purposes.

12 SUPPORT FOR THE APPLICANTS

For more information about the TrustChain's Open Calls, please check the Frequently Asked Questions (FAQs) section included at https://trustchain.ngi.eu/faq/.

For further information on the Open Call #2, in case of any doubt regarding the eligibility rules, the information that is to be provided in the Application Form, or if you encountered technical issues or problems with the Application Form, please contact TrustChain Technical Helpdesk email: trustchain@ngi.eu

13 INDICATIVE TIMELINES

Submission to the TrustChain Open Call #2 will open on 20 July 2023 (13:00 CEST) and close on 20 September 2023 (17:00 CEST). The table below presents the indicative dates during which each phase of TrustChain Open Call #2 will take place.

Description	Indicative dates*
Call Announcement	20 July 2023 at 13:00 CEST
Call closure and submission deadline	20 September 2023 at 17:00 CEST
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
Projects duration	9 months

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

ANNEXES

Other important documents can be consulted at https://trustchain.ngi.eu/apply

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 Applicant(s) template (read only)

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