TRUSTCHAIN

OPEN CALL #1 - CALL DOCUMENT

DECENTRALISED DIGITAL IDENTITY

Closing dates for proposals: 10th of April 2023, 17:00 CET

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

1 PREAMBLE

This document provides the necessary details for TRUSTCHAIN Open call 1 to be implemented. Among others, it documents its specific objectives, challenges and expected outcomes. As a reminder, the indicative timelines of this first Open Call close the document.

Today, the digital identity is an essential component of any application and computing system.

However, many existing systems used by universities, governments, Internet service providers, banks and similar have not kept with the time, and do not appropriately address a plethora of user and usability requirements. Considering emerging requirements, the European legislator created a legal framework for digital identities and trust services in the EU with Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). While the TRUSTCHAIN project does not intend to limit innovation in any way, reference to the European regulatory framework concerning digital identities (i.e., eIDAS) should be clearly made by the applicants.

The digital identity is usually established by mechanisms of proving a secret that we have (e.g., password), what we possess (e.g., an identification card), or what we are (e.g., biometric data). However, in our complex world, much stronger and/or more fine-grained user-controlled Decentralised Identifiers (DIDs) may be used in order to achieve privacy on one hand and security on the other. The capability to autonomously manage different facets of one's identity brings light to Self-Sovereign Identities (SSIs). Existing SSI approaches need to be assessed in light of current requirements and should be lifted to an appropriate degree of usability in specific contexts. The trustworthiness and/or credentials made possible by SSI technology cannot be taken for granted but should be assessed by means of verifying their issuance from national and certification authorities, interconnections with a variety of digital identities used within social networks, public or private Internet services, or even by means of decentralized reputation mechanisms. Since Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs) are already W3C standards playing an important role in the Semantic Web, any new proposals will have to establish the current state-of-the-art and clearly articulate how this will be brought to a new usability level (e.g., to be used by students, disabled persons, technologically illiterate, etc.). Many of these approaches may be complemented with the use of decentralised data management infrastructures, wherever the use of such decentralised computing infrastructures makes sense from the viewpoint of benefits (e.g., privacy, security, utility) against drawbacks (e.g., energy inefficiency). **Trustworthy digital identities and data are the focus of this TRUSTCHAIN Open Call 1 (OC1) on "Decentralised Digital Identity".**

This Open Call 1 welcomes applications that will clearly define, upgrade/extend

the state-of-the-art, and develop the following types of solutions:

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

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 and fits within the scope of human centric decentralised trustworthy digital identity. It should utilize existing concepts and technologies already developed for SSI and fit within TRUSTCHAIN's vision and objectives. The solutions should be provided as open-source software achieving TRL 7, tested and evaluated by an adequate pool of potential users which 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. The proposed solution will have to use standard technology for full-stack development that is compatible with the current standards.

The call is open for submission from 8th February 2023 (12:00 PM CET) until 10th April 2023 (17:00 CEST). Its indicative budget is € 1 755 000 with up to a maximum of 15 proposals funded.

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 NGI TRUSTCHAIN relevant vision.

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 this digital world: delusion and manipulation, personal privacy violation and personal data exploitation, unknown provenance of information, anonymity for performing criminal activities, spread of fake news using fake identities, skills mismatches, serious breaches of security are only a few of the threats that have emerged. The spirit of the first-generation Internet based on individual freedom, material progress, and moral community is slowly turning into individualism, materialism, and moralism, diverging from essential ethical and democratic principles that should underline this technology. The design choice of the past, based on a mix of centrally managed networking and device technologies makes today's Internet obsolete when it comes to empowering all citizens to act for a more environmentally friendlier digital transformation, as well as to create a more resilient, inclusive, and democratic society, addressing inequalities and human rights, better prepared for and responsive to threats and disasters.

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

that have been developed and maintained through long lasting centuries of human evolution.

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

This is the main focal point of this call.

- **Open Call 2- User privacy and data governance**

The objective of this OC will be 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
- Privacy-preserving usage of Artificial Intelligence, IoT, Digital Twins, Cloud-to-Edge services, or combination of those

- **Open Call 3- Economics and democracy**

  The objective of OC3 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**

  OC4 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 OC1-4 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.

This document is specifically dedicated to the Open Call 1 and outlines its context and its application modalities.

3 OPEN CALL 1 (OC1): DECENTRALISED DIGITAL IDENTITY

3.1 INTRODUCTION TO OC1

The call is open for submission from 8th February 2023 (12:00 PM CET) until 10th April 2023 (17:00 CEST).

Its indicative budget is € 1 755 000 and will be distributed among up to 15 selected projects led and executed by a critical number of 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 NGI TRUSTCHAIN relevant vision.

Selected projects will last for a duration of 9 months. However, TRUSTCHAIN overall action lasting 36 months, their participation at any of the future Joint Meetings after these 9 months for knowledge and know-how transfer to TRUSTCHAIN OC2-5 and for the development of the TRUSTCHAIN ecosystem as a whole is requested.

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 OC1 vision and objectives. Their proposed solution should consider as minimal requirement to:

- Use standard technology for full stack development;
- Be open source;
- Extends the state-of-the-art in the domain of digital identities, and/or solves existing real-world problems with digital identities and provides new highly usable software solutions.

Using the mandatory TRUSTCHAIN proposal template, applicants are expected in relation to the specific objectives specified hereafter (section 3.2) to explain in their application:

1. The specific technological innovation they propose to develop and how this is clearly different from alternative solutions that are already available in the market, or developed by previous EU research and innovation actions (i.e., EU ONTOCHAIN Project & any other projects);
2. The specific digital identity needs or challenge they propose to address and who would benefit from it immediately and in the longer term;

3. Whether the innovation will focus on the development of new solutions for existing areas, or a totally disruptive approach or idea;
4. 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
5. Any challenges or opportunities relating to equality, diversity, ethics and inclusion arising from their project.

Applicants when applying should **clearly specify the Open Call 1 challenges they are going to address. Those are described in the section 3.3.**

3.2 OC1 SPECIFIC OBJECTIVES

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

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

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

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

3.3 OC1 CHALLENGES TO BE ADDRESSED

The current ecosystem of decentralized digital identity systems experienced a rapid growth in the last couple of years. However, mainstream adoption of those systems still encounters multiple challenges that should be addressed by the TRUSTCHAIN applications.

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

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

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

- **the provision of public administration services,**
- **digital identities used in the banking (e.g., know your customer (KYC) approaches), education (e.g. micro credentials for micro competencies), healthcare (e.g. access-control mechanisms in cross-border scenarios), and other sectors,**
- **cross-border use of digital identities,**
- **digital identities used by Next Generation Internet services, and/or**
- **regulatory alignment of existing digital identities (e.g., in the context of EU eIDAS framework).**

Funded by the European Union

3.4 OC1 SPECIFIC REQUIREMENTS

3.4.1 Technical Requirements

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 (e.g., identity bridges), 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 identity and trustworthiness, 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 put in the centre general population and vulnerable people needs 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. privacy preservation, reputation management and on expanding what already exists thus scaling rather than building something new from scratch. An initial TRL of 7 should be demonstrated and validated in a real end user setting. If something completely new must be build (see point above), it should be well motivated in particular with what rewards the nature of the problem and why the state-of-the-art solution does not solve it today (i.e., barriers to 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 value proposition. Cross-border identity translation, moving identities/data across borders (at least within EU) should be carefully considered. It should be also compatible with existing identity management frameworks (e.g., eIDAS), 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 showcased.

3.4.2 SUSTAINABILITY REQUIREMENTS

Various emerging technologies currently pose huge environmental impact, and they should be evaluated against any potential benefit from using these technologies. The applicants are requested to provide a short assessment of the trade-offs, from one viewpoint the benefits when using the technology, and from another, the potential energy-inefficiency. Various best effort solutions should be used as 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 identity platform (i.e., eIDAS2) / infrastructure standards with which they intend to comply or they wish to contribute in the course of the proposed projects.

3.5 EXPECTED OUTCOMES AND POSSIBLE APPLICATION DOMAINS

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

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

These outcomes could be materialised by :

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

Possible application domains (not limited to) are:

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

3.6 OC1 MANDATORY DELIVERABLES

Projects selected and funded by the TRUSTCHAIN consortium will have to deliver four deliverables during their participation process. These deliverables are mandatory. They are defined below:

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

4 SUPPORT SERVICES PROVIDED BY TRUSTCHAIN TO THIRD PARTIES

Selected participants will receive support with the following services:

- **Access to Infrastructure:**

Applicants will be provided with Alastria blockchain infrastructure (two different networks, T Network based on GoQuorum and B Network based on Hyperledger Besu), compliant with Ethereum, for demonstration purposes for those that may 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 need for them to install any 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 selected third-party innovators to exploit their use cases and successfully reach the market, different trainings and sessions with mentors will be organised. Depending on the team profile, aspects such as Value Proposition, pitching or IPR (among others) will be explored.

- **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.
  - connect with a vibrant ecosystem of innovators, investors, industry players and public authorities.

Each third party selected will be assigned one or more mentors from the TRUSTCHAIN consortium to follow their progress and support them with specific expertise (technical, user centric, legal aspects, business aspects) all along their project on a regular basis.

5 ANNOUNCEMENT

Submission to the TRUSTCHAIN Open Call 1 will open on the **8th February 2023 (12:00 PM CET) and close the 10th April 2023 (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 1 will take place.

Call Announcement	8th February 2023 at 12:00 PM CET
Call closure and submission deadline	10th April 2023 at 17:00 CEST
Total EU funding available for OC1	€ 1 755 000
Evaluation Period	Until end of May 2023
Signature of Sub-grant Agreement	First week of June 2023
Expected duration of projects	From June 2023 to February 2024, 9 months
Task description	In order to achieve TRUSTCHAIN vision, it is expected that applicants will develop interoperable and sustainable digital identity management applications that are transparent and address the needs of the future decentralised internet. In particular, the following main objectives should be considered: ○ Develop a framework for decentralized user-centric identity management that lies in the scope of the call and addresses the stated challenges below, ○ Develop protocols for trustworthiness of entities by means of verifiable credentials and decentralized reputation systems, ○ To ensure identity attributes are disclosed only with the informed consent from the data owner (i.e., data minimization requirement of GDPR), ○ Develop smart oracles to assess the trustworthiness of data fed to blockchain smart-contracts fetched from external systems. [identity-related explanation] Applications should cover real needs of the end-users in one of the sectors such as for example banking, education, healthcare or e-democracy (Not limited to).
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 the TRUSTCHAIN Consortium and the TRUYSTCHAIN Advisory Board Members.
Further information	Further details are available at: https://trustchain.ngi.eu/apply

6 SUPPORT TO APPLICANT

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-1
- 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

The TRUSTCHAIN Open Call 1 supported material is the following:

- **The TRUSTCHAIN Open Call 1 text**

The present document.

- **The TRUSTCHAIN Guide for applicant**

This document provides in details the information to help apply to the TRUSTCHAIN

Open Call 1 such as an abstract of the TRUSTCHAIN action, a description of the TRUSTCHAIN open call 1, 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: It is available at: https://trustchain.ngi.eu/apply

This document also contains in annex the administrative forms preparation template, the proposal description template and the TRUSTCHAIN additional applicant's template.

- **The TRUSTCHAIN Application material**

  - **Administrative forms preparation template**: which presents the list of administrative information that you need to fill in directly in the F6S portal.
  - **Proposal description template:** a mandatory and editable document to describe your proposal.
  - **Additional applicant's template:** In case your proposal has more than 3 applicants participating as individuals (Natural persons) or/and more than 3 applicants participating as organisations (Legal entities), you will have to fill in this document and upload it in section 3 of the F6S form.

- **Indicative sub-grant agreement form**

This document provides a template of the sub-grant agreement that only the selected applicants will be requested to sign. It is not necessary to send this document at the time of application.

All documents are available at: https://trustchain.ngi.eu/apply