NGI TRUST CHAIN

D1.8 ADVISORY BOARD REPORT

19/09/2024

Funded by the European Union

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

NGI TRUST CHAIN

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

D1.8 ADVISORY BOARD REPORT

Work package	WP 1
Task	Task 1.8
Due date	30/06/2024
Submission date	19/09/2024
Deliverable lead	ICS
Version	V0.4
Authors	Veniamin Boiarkin (ICS), Michal Krol (ICS)
Reviewers	Andres del Alamo (CIB), Vlado Stankovski (UL)
Abstract	Advisory Board report
Keywords	Advisory Board

Document Revision History

Version	Date	Description of change	List of contributor(s)
0.1	15/07/2024	First Draft	Veniamin Boiarkin (ICS)
0.2	15/07/2024	Review	Michal Krol (ICS)
0.3	28/07/2024	Review	Andres del Alamo (CIB), Veniamin Boiarkin (ICS)
0.4	29/07/2024	Review	Thanasis Papaioannou (AUEB), Veniamin Boiarkin (ICS)

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
9	NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS	NKUA	EL

EXECUTIVE SUMMARY

With the goal of establishing the visibility of our project and enhancing our core Consortium abilities to focus on a new decentralized internet ecosystem, we have concluded the formation of an International Advisory Board. TrustChain is a Horizon Europe Next Generation Internet (NGI) project, however, its relevance is truly international. Hence, we made efforts to select and invite eminent experts in cryptography, privacy, digital identity, blockchain, cyber and IT laws and economics of digital marketplaces which are relevant to the development of the TrustChain ecosystem. By doing so, we believe the outcome, findings and impact of TrustChain will spread across all continents, and it will allow other initiatives within and beyond Europe to join forces with our ongoing project efforts.

This deliverable outlines the context, the purpose of the AB members within the TRUSTCHAIN project, and the activities carried out with the members of this board during the first year of the project. We sought experts in specific technology and application areas that were essential for the project and included expertise in blockchain, Semantic Web, Peer-to-Peer systems, distributed computing, Cloud, Fog, and Edge computing, ecosystem economy, Artificial Intelligence, Internet of Things, software engineering, Digital Twins, integration of information systems, philosophy, ethics, human rights, legal and other essential expertise. The experts find the projects very interesting and scientifically cutting edge with innovation and impact to the society. They identified areas for improvements especially to engage more users in the early stage of the technological design and also to develop clear business models that can help to generate revenue in the short term. They identified many of the projects that were aligning them with the EU standards and developing interoperable technologies that are scalable and future proof. The final aim is to build the relevant channels to be able to efficiently and effectively engage such experts to contribute to a novel Next Generation Internet approach incorporating technology, and protocols for trustworthy content handling and trustworthy information exchange in a decentralized manner. Its also key to make sure the project aligns with international technology standards and global net zero targets to make a real impact and contribute towards the success of the digitally connected citizens of Europe.

TABLE OF CONTENTS

1 INTRODUCTION 8
2 ROLE OF THE ADVISORY BOARD 9
3 ADVISORY BOARD 10
4 THE ADVISORY BOARD FEEDBACK AFTER EIGHTEEN MONTHS OF TRUSTCHAIN IMPLEMENTATION 11
5 CONCLUSIONS 30

LIST OF FIGURES

FIGURE 1: FROM 1 TO 5, HOW CLOSE WOULD YOU ESTIMATE THE TRUSTCHAIN PROJECTS TO THE MARKET? 12

FIGURE 2: FROM 1 TO 5, HOW WOULD YOU ASSESS THE EFFECTIVENESS OF THE TRUSTCHAIN PROJECTS' BUSINESS MODELS? 14

FIGURE 3: FROM 1 TO 5, HOW WOULD YOU SCORE THE CONTRIBUTION OF THE TRUSTCHAIN PROJECTS TO DATA PRIVACY? 16

FIGURE 4: FROM 1 TO 5, HOW WOULD YOU SCORE THE CONTRIBUTION OF THE TRUSTCHAIN PROJECTS TO THE SECURE DATA EXCHANGE AND DATA MARKETPLACES? 18

FIGURE 5: FROM 1 TO 5, HOW WOULD YOU ESTIMATE THE CONTRIBUTION OF THE TRUSTCHAIN PROJECTS TO THE DECENTRALIZED TRUSTWORTHY GOVERNANCE MODELS? 20

FIGURE 6: FROM 1 TO 5, HOW EFFECTIVE WOULD YOU CHARACTERIZE THE USER-CENTRIC APPROACH OF THE TRUSTCHAIN PROJECTS? 21

FIGURE 7: FROM 1 TO 5, HOW WOULD YOU CHARACTERIZE THE CONTRIBUTION OF THE TRUSTCHAIN PROJECTS TO THE ADOPTION OF DIGITAL IDENTITY PLATFORMS FROM MARGINALIZED COMMUNITIES? 23

FIGURE 8: FROM 1 TO 5, HOW WOULD YOU RANK THE ADOPTION OF LEGAL AND REGULATORY REQUIREMENTS AND STANDARDS BY THE TRUSTCHAIN PROJECTS? 25

LIST OF TABLES

TABLE 1: ADVISORY BOARD MEMBERS 11

1 INTRODUCTION

With the consortium and TRUSTCHAIN vision formed, during the first year of the project we tried to set up the foundations of TRUSTCHAIN to gear towards involving the right experts together. The first two open calls of TRUSTCHAIN were designed to build a community of experts in various fields including:

Open Call #1 – Decentralised digital identity

The overall objective of Open Call #1 was to define and develop:

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

Open Call #2 – User privacy and data governance

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

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

During the first year of the TRUSTCHAIN project partners conducted series of dissemination activities towards key stakeholders including experts and innovators in the following domains: (1) blockchain, (2) semantic web, (3) peer-to-peer systems, (4) distributed computing, (5) ecosystem economy, (6) artificial intelligence, (7) internet of things, (8) software engineering, (9) digital twins, (10) integration of information systems, (11) philosophy, ethics, human-rights, legal and other domains which are

essentially important and have to be consulted in order to define a radical Next Generation Internet approach, technology and protocols for trustworthy content handling and trustworthy information exchange.

To further establish the visibility of our project and enhance our core Consortium abilities to focus on a new software ecosystem, the design of our TRUSTCHAIN project formed an International Advisory Board. While TRUSTCHAIN is a Horizon Europe Next Generation Internet (NGI) project, its relevance is truly international. Hence, we selected and invited eminent experts in all fields relevant to the development of the TRUSTCHAIN software ecosystem from around the World. By doing so, we spread the word about our project across all continents, as proven by the statistics of our website visits which show very high numbers of visitors from the United States and Canada.

In addition, based on the feedback received from the OC1 and OC2 calls we have emphasized the importance of the user-centric design from the early stages of the project. Additionally, we have also asked the OC3 teams to provide clearer alignment of their projects with the TrustChain vision and EU's ambition to design a truly inclusive and user centric next generation decentralized internet.

2 ROLE OF THE ADVISORY BOARD

The TrustChain Advisory Board is set up and operated to share its knowledge and expertise with the consortium of the project in key stages of its implementation. The overall purpose of AB members is to:

- Act as a critical mentor for the TrustChain consortium by providing valuable and independent feedback aimed at aligning project outcomes with the needs of their users and stakeholders.
- Suggest innovation actors (e.g. researchers, innovators, entrepreneurs, startups, SMEs, etc.) to participate in project activities; as well as
- Support the rollout, replication and upscale of the TrustChain software ecosystem, by informing and inviting relevant entities as and when there are potential opportunities to showcase the project findings to the wider scientific and industrial community.

3 ADVISORY BOARD

We hereby provide a list of the current members of the project's Advisory Board who are reputed community members with expertise in broad areas covered by the project.

Name	Organization	Expertise	Country
Dr Michael Zammit Maempel	MITLA Law firm	Media, Communications and Privacy law	MLT
Dr Sushmita Ruj	Head of Blockchain Group, UNSW Sydney	Cryptography, blockchain, cybersecurity and data privacy	AU
Prof Anupam Chattopadhyay	Associate Professor, Nanyang Technological University Singapore	Cyber-Security, Application-specific Architectures, Electronic Design Automation and Security	SG
Prof Ben Azvine	Head of Security Research, British Telecommunications UK	Application of AI to Cyber security, protection of critical national infrastructure, data analysis, information & knowledge management	UK
Prof Bruno Bogaz Zarpelao	Assistant Professor, State University of Londrina (UEL), Brazil	Security Analytics, Intrusion Detection, Distributed Ledger Technologies, Internet of Things	BR
Prof Pamela Briggs	Professor, Northumbria University, UK	Identity, trust, privacy and security in new social media, with a particular focus on digital inequality	UK
Prof Spyros Galanis	Professor, Durham University	Decision theory, game theory, experiments and finance	UK
Prof Theo Dimitrakos	Head of Security Research, Huawei, Germany	Information security, security policy, identity and access management, cloud computing, trust management, security risk management and cloud computing.	DE
Prof. Etienne Riviere	Professor, UCLouvain, Belgium	Distributed systems, operating systems, and privacy & security, blockchain technologies and infrastructures	BE

Prof. Stefan Dziembowski	Professor, University of Warsaw, Poland	Theoretical and applied cryptography, blockchain	PL

TABLE 1: ADVISORY BOARD MEMBERS

4 THE ADVISORY BOARD FEEDBACK AFTER EIGHTEEN MONTHS OF TRUSTCHAIN IMPLEMENTATION

On June 18 and June 19, 2024, the core consortium of TRUSTCHAIN held virtual meetings with the members of the Advisory Board to discuss the status of TRUSTCHAIN in terms of the software contributions of the selected third-party projects.

Seven out of the ten members of the Advisory Board joined this meeting. This meeting was intended to provide us with some feedback on the overall qualities or performance that the TRUSTCHAIN platform should offer to future applications for its end-users as a whole.

On each day, five projects from OC1 and OC2 presented their work and achievements with a 5-minute presentation followed by a 10-minute Q&A session, during which Advisory Board members were asking questions. Then, after the meeting, we provided the Advisory Board members with a short survey accompanied by support documents such as project presentations and slide decks. Seven members of the Advisory Boards have answered it. The results of this survey are described and discussed below.

Question 1: “From 1 to 5, how close would you estimate the TrustChain projects to the market?”

The answers to the question are depicted in Figure 1 below.

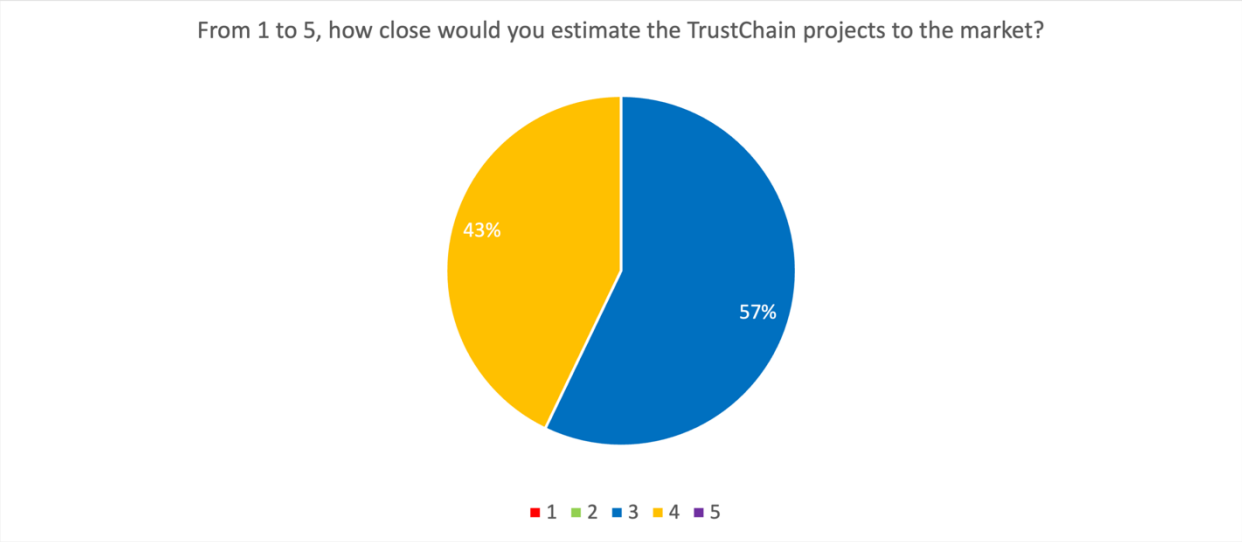

FIGURE 1: FROM 1 TO 5, HOW CLOSE WOULD YOU ESTIMATE THE TRUSTCHAIN PROJECTS TO THE MARKET?

Feedback received from Advisory Board members:

- *"The projects vary but some, such as MUSAP seem quite close to market and show good collaboration with commercial partners, whilst IM4DEC have already secured over 35k registered users. Some of the other projects are still in development, and I felt it was difficult to judge market position on some presentations."*
- *"I think there is still some work to be done to take the ideas to the market. For example, performance analysis for the blockchain projects will be important, risk assessment plan should be in place. Plans for scalability is required, because this would be an important consideration as they are launched."*
- *"It is hard to answer this question with the provided material. None of the five projects provide a clear timeline regarding large-scale testing, user-based testing, and deployment of pilots. Pilots are presented by some projects, e.g., DGuard, but without timing indicators; IM4DEC indicates plans for deployment in Austria but again without a clear timeline. For DIDRoom the technological stack seems advanced but there is no detail about large-scale validation or TRL. SURE's presentation does not allow evaluating this question. In general, all projects target ambitious technological objectives and have progressed in their realisation but the TRL may still be low at this stage (unless I am mistaken)."*

- *"Several projects did not talk much about commercialisation and marketing, they mostly talked about the main idea and proof of concept. This could also be because of the limited time of the presentation (5 minutes)."*
- *"Some projects appeared more market-ready than others, in the sense that the ideas seem to have been thought out in greater depth than in others. For instance, WIDE, Morphmetro and Werenode communicated objectives that were more clearly defined than some of the others, and consequently, they identified a need in the market that was more tangible. The projects were inconsistent in their attention to possible legal limitations to the concept and range of their project, particularly in relation to the protection of data privacy."*
- *"Most of the presented projects demonstrated a genuine concern about the feasibility of their solutions for real-world scenarios. All the projects fill gaps in the privacy/security industry and are well aligned with urgent needs. Despite these positive aspects, a few projects don't look like they have a clear perspective about how their solutions will be commercially available.*
- *"This was very good. Sure project already has some commercial engagement, more focus is needed on the business model and technology readiness level for all the projects."*

Takeaways from the Advisory Board's Feedback:

- One of the AB members felt that some of the projects were near market ready whereas others were still in the final stages of commercialisation.
- Another AB member highlighted the need for testing in real-life scenarios. Due to the limited timescales scales available for ethics approvals some projects struggled to do the market validation for a longer period with a larger end-user community.

Question 2: "From 1 to 5, how would you assess the effectiveness of the TrustChain projects' business models?"

The answers to the question are depicted in Figure 2 below.

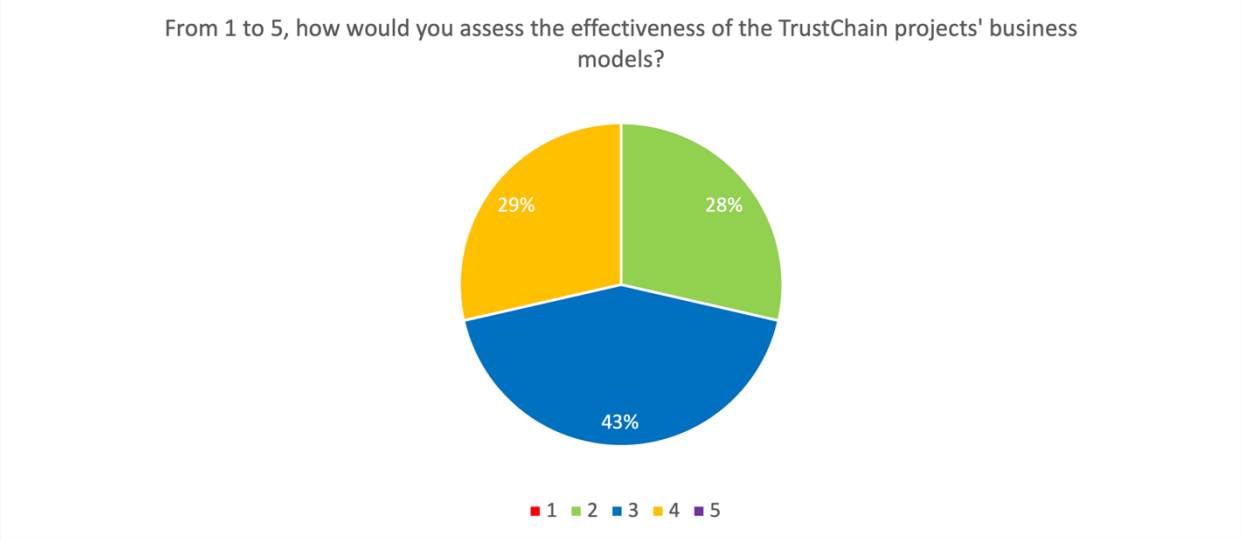

FIGURE 2: FROM 1 TO 5, HOW WOULD YOU ASSESS THE EFFECTIVENESS OF THE TRUSTCHAIN PROJECTS' BUSINESS MODELS?

Feedback received from Advisory Board members (the individual project names have been removed to maintain the anonymity of the projects):

- *"All projects seem sensitive to business interests and have been working towards some kind of launch. The business models of three funded sub-projects seem well developed."*
- *"The business models are quite effective. Some projects have used agile methodologies. I would appreciate a bit more clarity on the customers, and the source of data. What ethics checks will be performed when collecting and using public data. The projects should mention how they will build and scale, possible source of funding, collaborations and partnerships. "*
- *"This is not the strongest point of the presentations. One funded sub-project presents a business model idea that would be based on a freemium model and pay-per-use hosting of the service (for identity management and crypto operations on blockchains). Given that the project also targets open sourcing (which is good) it should explain how it will generate value by means of services or specialized developments. The other 4 projects do not present business plans. Another funded sub-project does not detail if it will have infrastructure cost or ship as a library to be hosted by clients. It does not detail how the potential costs of using difference EVM blockchains are covered. For another funded sub-project, there is limited information. The existence of registered users in Austria may not be a sufficient metric for long-term business viability.*

For another funded sub-project, the presentation is convincing regarding the need and market existence, but the exploitation is lacking. The business model only mentions that the results are open source but does not explain how value will be obtained from the results. For another funded sub-project, there is no business model presented in the presentation. The proposed tool could be sold closed source but the risks in terms of liability after a synthetic dataset is used to leak information, when it was marked as safe initially by the tool, are pretty high."

- *"There was not a lot of talk about the business model."*
- *"Although some of the projects (See previous question) identified a market need, none of the projects focused too significantly on mapping out an exploitation model or a business case."*
- *"Most projects were very concise about their business models. Some showed that they have already identified some companies that might be interested or other potential partners. However, their business plans still need to look more solid."*
- *"One funded sub-project has a viable business model based on Opensource and consultancy. Other projects also mentioned business models but not in sufficient detail."*

Takeaways from the Advisory Board's Feedback:

- Overall, this AB member felt that the projects need to demonstrate the exploitation plan and commercials in depth.
- Another AB member also identified some projects do not have a clear business model and a business plan. The mentors provide a lot of support and encourage the development of business canvas and business plans as part of the project deliverables. The Trustchain team will continue to emphasize the importance of having a robust business model and business plan in the future open call funded projects.

Question 3: "From 1 to 5, how would you score the contribution of the TrustChain projects to data privacy?"

The answers to the question are depicted in Figure 3 below.

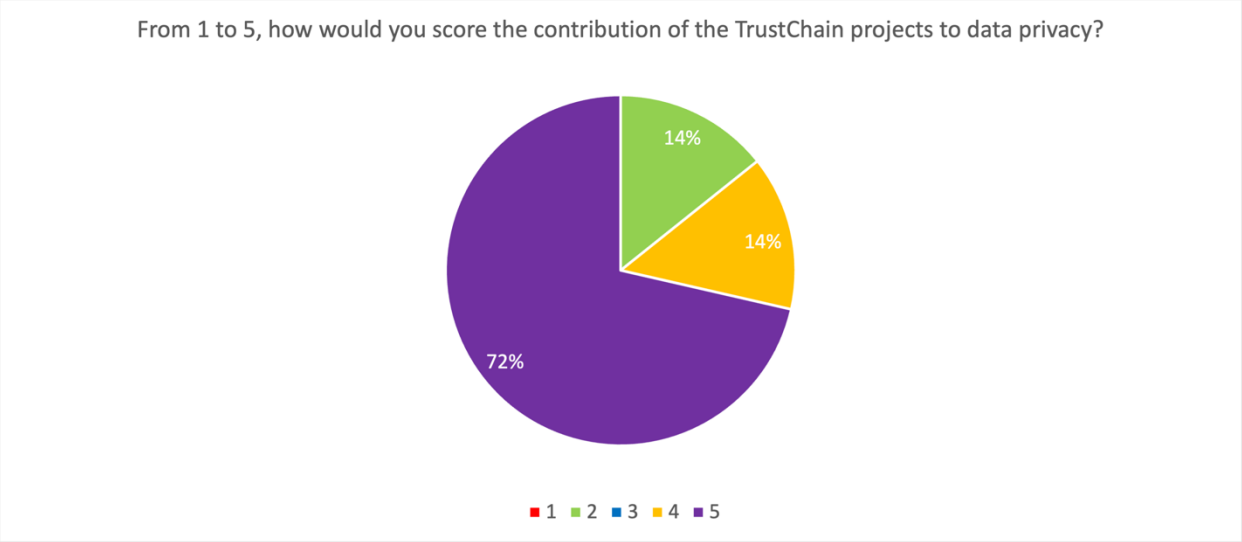

FIGURE 3: FROM 1 TO 5, HOW WOULD YOU SCORE THE CONTRIBUTION OF THE TRUSTCHAIN PROJECTS TO DATA PRIVACY?

Feedback received from Advisory Board members:

- *"All projects were making a strong contribution to data privacy, and I was impressed by the different approaches being taken. Clearly in projects using synthetic data (SURE) and medical records (BLOOCK) data privacy is paramount and I was happy to see how this was handled effectively. dGUARD was also explicit in the ways in which privacy and consent were managed."*
- *"All projects address data privacy. Utip-DAM uses k-anonymity, which might have restricted use. Morphmetro uses Homomorphic Encryption, but the smart contract design should ensure no data is stored on chain. Where node should address how they address privacy of data on-chain."*
- *"There are some nice contributions towards better data privacy in the NGI in several of the projects. DGuard and SURE are two projects that are directly related to privacy, in the context of training on sensitive data, with two different approaches (federated learning and learning on synthetic data), which could in fact be complementary. For DGuard, the core objective of the project is to allow privacy-preserving, controlled, and traceable data sharing. While the project uses building blocks that have been proposed in research (individually) their combination in an integrated framework can enhance privacy in concrete projects. The use case (e-health data sharing for federated learning) is a good example where privacy matters. With SURE, ensuring the use of "informed" synthetic data use for training can help achieve better security/privacy trade-*

off's. DIDRoom also makes interesting contributions by making SSI with privacy protection easier to integrate in applications, allowing for instance selective disclosure, a feature that is hard to implement correctly. IM4DEC does not really mention privacy as a core objective."

- *"I was satisfied with the data privacy provisions made by the projects."*
- *"Broadly speaking, privacy and the legal limits or restrictions that are posed on data processing operations was sidelined, and very few presentations explained clearly how the projects could observe the principle of privacy by design. This is not to say that the projects do not incorporate any privacy considerations: they were just not explained, or otherwise taken for granted. Utip-DAM, for instance, was somewhat unclear on how data privacy measures would be incorporated into the project and how they would operate."*
- *"As pointed out in question 1, all the projects are in line with urgent needs of the security and privacy industry. Observing different aspects of the projects such as business plans, focus on the user, technical correctness, and technical innovation, I'd say that the technical ones are the most advanced. The teams seemed to dedicate more time to the technical aspects. In terms of data privacy, I see MorphMetro as a quite promising project."*
- *"This is very good for all the projects. Sure project has an indirect link to this."*

Takeaways from the Advisory Board's Feedback:

- One of the AB members was happy with the technical merit of these projects. Highly commends the technologies such as homomorphic encryption and synthetic data that are used to achieve maximum privacy while maintaining the utility of the data.
- Another AB member could not see much spelt out by the projects around the concept of privacy-by-design principles. As this is something that all projects consider by default from the design stage they have not been explicitly mentioned. The Trustchain mentors will check in future deliverables to make sure this is clearly articulated by all the funded projects.

Question 4: "From 1 to 5, how would you score the contribution of the TrustChain projects to the secure data exchange and data marketplaces?"

The answers to the question are depicted in Figure 4 below.

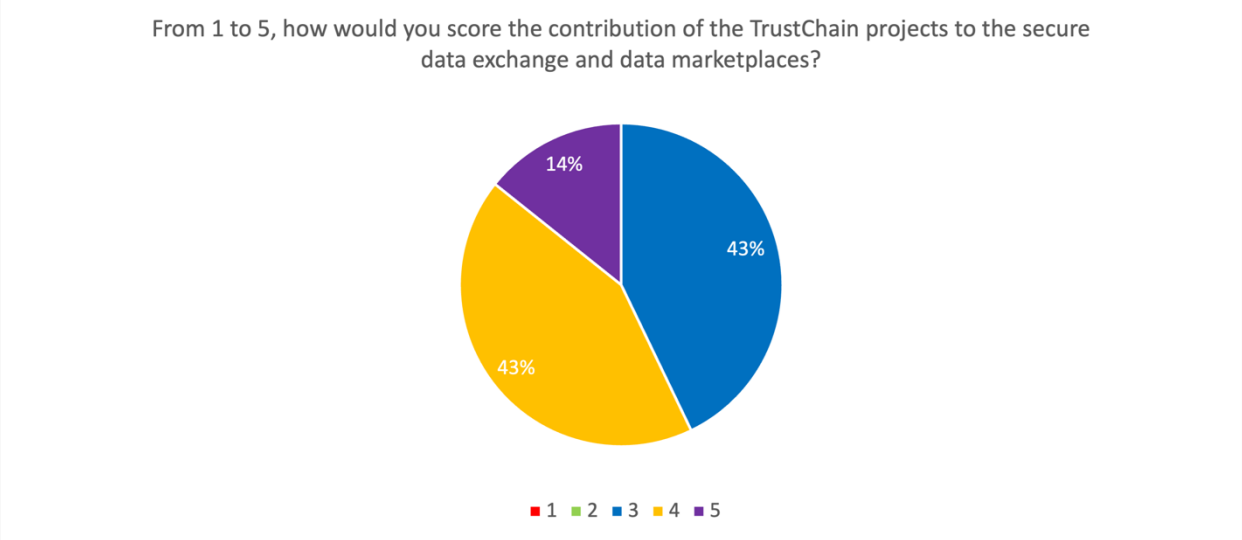

FIGURE 4: FROM 1 TO 5, HOW WOULD YOU SCORE THE CONTRIBUTION OF THE TRUSTCHAIN PROJECTS TO THE SECURE DATA EXCHANGE AND DATA MARKETPLACES?

Feedback received from Advisory Board members:

- *"Again, the projects show a good range of approaches, but secure data exchange was at the heart of each of them, with dGUARD providing a good example. Some were (e.g. DIDROOM) were more technical than others, and so hard for me to evaluate given my lack of technical expertise."*
- *"Some of the projects like Coninnseq and InnoRenew and Morphmetro will be important for data marketplace and data exchanges. However, a proper incentive model has to be in place for all the projects. "*
- *"Only DGuard is directly targeting this thematic. The project builds a secure data exchange. It does not seem to be designed as a marketplace, but elements of its architecture can form sound building blocks. SSI and identity management as targeted by several projects is orthogonal to data exchange but important. The synthetic data training in SURE could be an interesting approach to exchange sanitized data with certificates in marketplaces."*
- *"There was not a lot of talk about data interoperability and common standards. For example, with DGuard I can extract my data, but how easy it is to insert them on a different data service? Otherwise, one creates different data silos that do not communicate with each other. However, because most projects build on a blockchain, data security should be good."*

- *"The projects that were presented for review set valid aims and objectives for how secure data exchanges and data marketplaces can be exploited and used to improve quality of life."*
- *"Here, we have the same as the last question. All the projects seem fine from the technical angle. In terms of secure data exchange and data marketplaces, I'd say the projects Next Generation Smart Cities and IMP-DID are quite promising."*
- *"The projects don't address this aspect directly, but they are linked to this area indirectly."*

Takeaways from the Advisory Board's Feedback:

- One of the AB members highlighted many projects do not show how they align with the standards and regulations especially looking at the data protection and NIS security standards.
- Another AB member also identified the lack of clarity around scalability and interoperability which should be clearly defined by all the projects. The Trustchain mentors will take this feedback on board and ask all current and future projects to clearly demonstrate the interoperability and scalability of their developed protocols/systems etc with the Trustchain ecosystem.

Question 5: "From 1 to 5, how would you estimate the contribution of the TrustChain projects to the decentralized trustworthy governance models?"

The answers to the question are depicted in Figure 5 below.

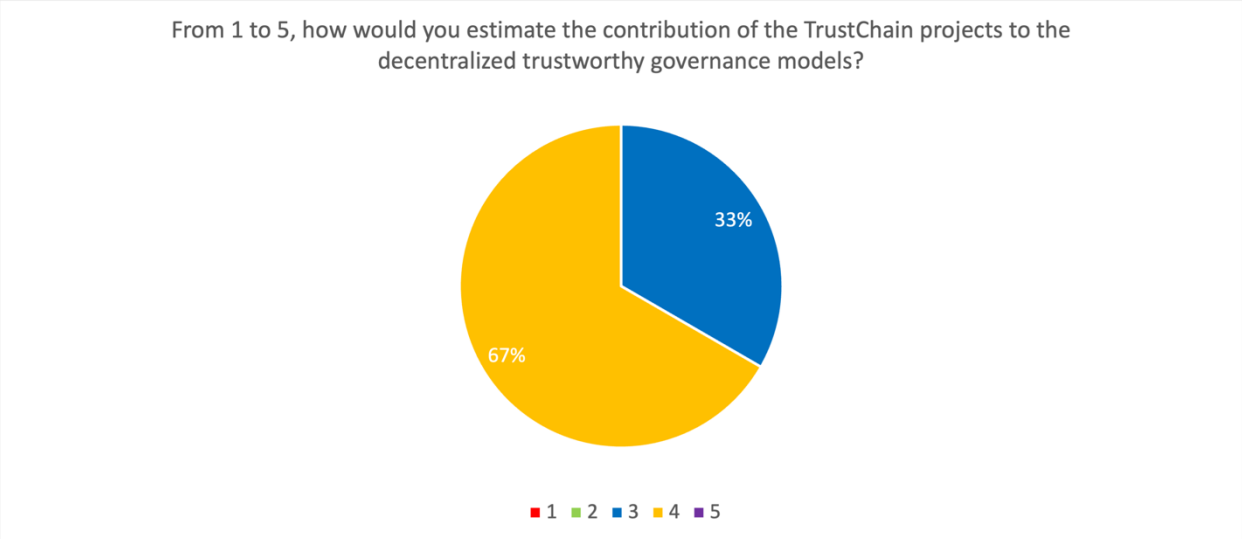

FIGURE 5: FROM 1 TO 5, HOW WOULD YOU ESTIMATE THE CONTRIBUTION OF THE TRUSTCHAIN PROJECTS TO THE DECENTRALIZED TRUSTWORTHY GOVERNANCE MODELS?

Feedback received from Advisory Board members:

- *"Some projects were more explicit about this than others, but again, given my lack of technical expertise in this matter it was hard for me to comment."*
- *"Some projects like InnoRenew have decentralized trustworthy governance models in place and are backed by peer-reviewed publication. Not all projects are decentralized in nature which is ok. Some like WIDE, Morphmetro, Werenode reply on blockchains, but not all have a governance model. "*
- *"None of the projects directly target this thematic. Supporting sovereign identities and SSI, as made easier by DIDRoom and MUSAP, is important to enable trustworthy governance solution, but not sufficient."*
- *"At least 3 out of 6 projects showed a special concern in terms of decentralized governance: WIDE, Next Generation Smart Cities, and IMP-DID."*
- *"There is good contribution across the projects. DIDRoom provides services to incorporate digital ID into applications."*

Takeaways from the Advisory Board's Feedback:

- One of the AB members observed that some projects are clearly articulating the governance framework whereas others are not demonstrating the decentralisation aspects clearly.
- Its noteworthy to see how some projects are clearly showing their contributions through publications and dissemination to the wider end user community.

Question 6: "From 1 to 5, how effective would you characterize the User-Centric Approach of the TrustChain projects?"

The answers to the question are depicted in Figure 6 below.

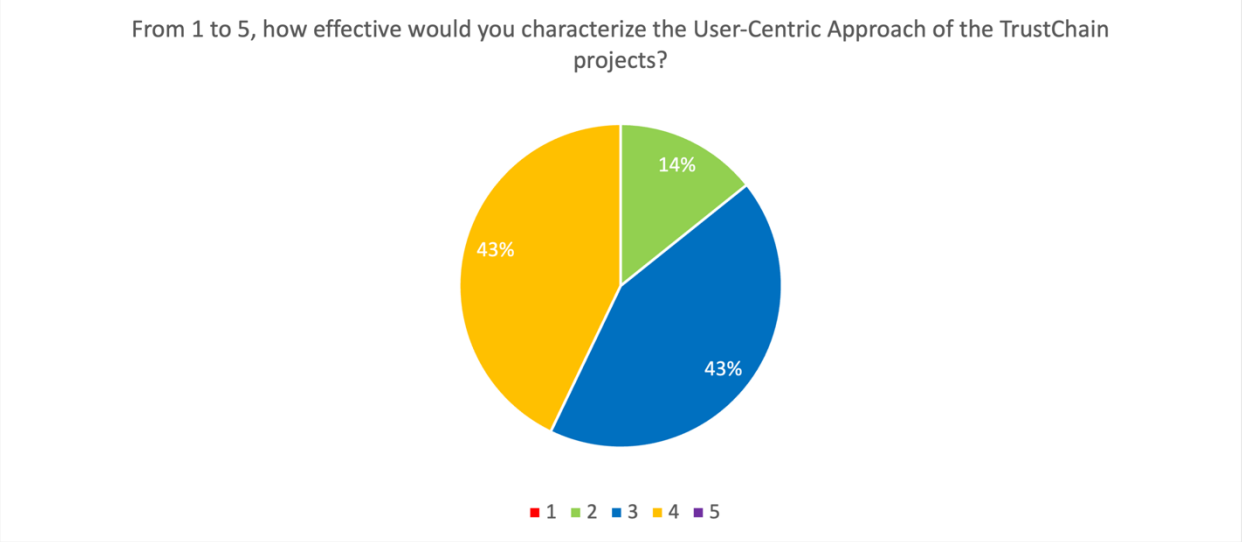

FIGURE 6: FROM 1 TO 5, HOW EFFECTIVE WOULD YOU CHARACTERIZE THE USER-CENTRIC APPROACH OF THE TRUSTCHAIN PROJECTS?

Feedback received from Advisory Board members:

- *"This was very variable. For some projects (e.g. SURE) there was good consideration of different user perspectives (e.g. data analyst vs. data protection officer) and there were also plans in place to do more advanced user testing. Some projects had mapped the user journey well and others (e.g. DIDROOM, MUSAP) were more focused on technical rather than user issues."*
- *"Some projects are quite user centric like Coninnseq, Werenode and WIDE."*
- *"A common trait of the five projects is the complexity of the proposed solutions targeting end users (an exception is SURE that targets experts, DPOs and data*

scientists, willing to assess the privacy-utility tradeoffs of synthetic datasets). This complexity is a risk to the adoption of solutions. It is also intrinsic to decentralized solutions and to the complex European landscape (and some projects like MUSAP and DIDRoom aim to reduce this landscape complexity with technical solutions). It is unclear from the presentation is end users were involved in the early stages of the design or in early test campaigns. There are projects with test cases in deployments of the solution (e.g., DGuard or MUSAP) but the development seems quite technology centric. For IM4DEC, the solution that targets vulnerable and impaired users is complex (e.g., require a wallet, following a complex workflow as shown in the demo video, etc.) and may be a risk for adoption and uptake, as compared to a simpler, government-provided solution for emergency calls. For DGuard, the project involves a test case with actual users. There is little detail about the implication of users in the design phase or on the user interface design and simplicity. For DIDroom, the project presentation is not user-centric but focuses more on the technology and cryptography. There is no evidence in the documentation of taking users into account (e.g., through scenarios or early testing), e.g., to develop the mobile applications. The demo focused on the administration panels and configuration. For MUSAP, the integration of the many solutions for European Digital Identity Wallet (EDIW) using multiple SSCD (Secure Signature Creation Device) could benefit users, but the overall complexity of the process may be a hindrance (e.g., to select amongst multiple backends for managing identities and storing crypto material). There is no evidence in the slides that the development of the solution was driven by end user tests and analysis. Finally, for SURE, target users are data scientists and DPOs. The presentation does not detail if these were involved in the design and analysis phase of the project."

- *"I think all projects had a good user-centric approach."*
- *"Although after re-reading and re-viewing the presentations a second time, it becomes easier to understand how the end-user is at the centre of the projects, this was not always communicated effectively during the presentations themselves. As a general comment, all projects should consider re-assessing how user-centrism is communicated and explained as being a fundamental part of each respective project."*
- *"All the projects mention their solutions are user centric, but I saw only a few things that are solid in this sense. The projects should be clearer on how they are empowering the users in terms of controlling their privacy and how the projects can meet users' specific needs. Relying on decentralized approaches like SSI and DLTs obviously helps make users more powerful, but the projects need to elaborate on how they will make this feasible. Also, pointing out that the projects will be evaluated by real users don't ensure they will be user centric."*

- *"This is OK. IM4DEC is focused on helping people in an emergency who cannot speak. dGuard provides mechanisms for users controlling the use of their data."*

Takeaways from the Advisory Board's Feedback:

- One of the AB members did not get a clear sense if all projects had users involved from the early design phase. Some AB members were able to identify whereas the others could not understand the importance of the user-centric aspect of the project. This should be clearly identified and presented to the AB in future projects.
- Another AB member could not understand the scale in which this end user engagement happened to understand the feasibility of deploying these solutions in real world applications. The project team will address this by asking projects to clearly show the numbers that were involved in each stage of the user engagement and validation.

Question 7: "From 1 to 5, how would you characterize the contribution of the TrustChain projects to the adoption of digital identity platforms from marginalized communities?"

The answers to the question are depicted in Figure 7 below.

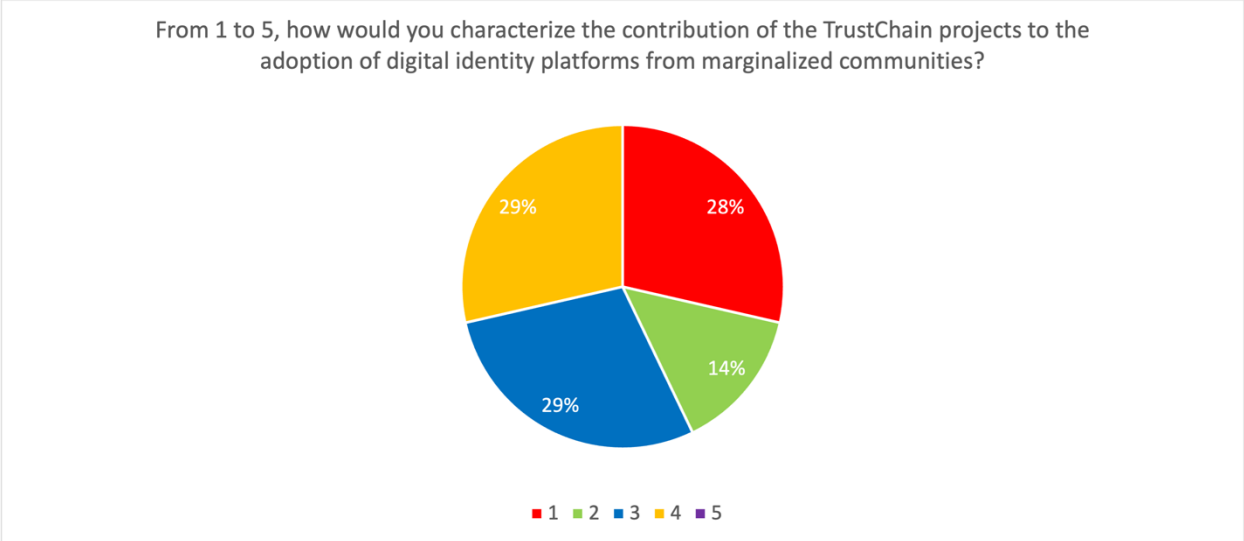

FIGURE 7: FROM 1 TO 5, HOW WOULD YOU CHARACTERIZE THE CONTRIBUTION OF THE TRUSTCHAIN PROJECTS TO THE ADOPTION OF DIGITAL IDENTITY PLATFORMS FROM MARGINALIZED COMMUNITIES?

Feedback received from Advisory Board members:

- *"Some projects were explicit about their value to marginalized or global south communities and for others it was more implied. Interesting examples included MUSAP being rolled out in Kenya and IM4DEC's consideration of victims of domestic violence and of disabled users (e.g. deaf/mute). Obviously, given the medical context, some of the examples of dGUARD would also be highly relevant for marginalized communities. "*
- *"It is not clear from the presentation how this would cater to marginalized communities. From the presentation they seem to be agnostic. Digital literacy in marginalized communities is assumed but may not be true. So, this issue needs to be addressed. Apart from this, I don't see any obstacle that will hinder marginalized communities to use these applications successfully."*
- *"This aspect seems orthogonal for DGuard and MUSAP."*
- *"The SSI solutions allowed by DIDRoom enable selective disclosure which I believe is a useful tool to fight discrimination, which can be a more prevalent problem for marginalized communities. It is not certain it will raise adoption directly, but perception may change (with lots of pedagogy). IM4DEC supports emergency calls by chat, useful for people with hearing or speaking disabilities. It is unclear if a decentralized solution using wallets is necessary for this, especially when identity management is already procured by a centralized state-sponsored system. For SURE: minorities are often the most at risk with re-identification attacks. Assessing the risk of re-authentication in synthetic data sets surely helps marginalized communities given the overlap, but it is unclear if it will increase adoption amongst them."*
- *"The projects are open to everyone, so this should help the adoption by marginalised communities. However, there was not any mentioning of specific efforts/initiatives to attract marginalised communities. The project IM4DEC is an exception, because by default it is intended to help marginalised communities (those who cannot speak and need to communicate by text) and make it easier for them to launch an emergency call."*
- *"Generally, there seemed to be little focus by the projects (collectively) on marginalized communities."*
- *"No projects showed a real concern about this topic."*
- *"There isn't specific focus on this, however IM4DEC is focused on helping people in an emergency who cannot speak, this is an important group and affects people with disabilities."*

Takeaways from the Advisory Board's Feedback:

- One of the AB members identified only one project that involved marginalised communities in the design phase. This project was targeted at designing technological solutions for the marginalised communities. The project team will advise projects to be more inclusive in the design phase of the projects.
- There is also a discussion around the types of marginalised communities and how this can be adopted by various communities. This is a challenging task to achieve as there are several ethical issues that needs to be addressed before such feasibility studies can take place which can be an issue for a short-term projects such as the ones funded by Trsutchain.

Question 8: "From 1 to 5, how would you rank the adoption of legal and regulatory requirements and standards by the TrustChain projects?"

The answers to the question are depicted in Figure 8 below.

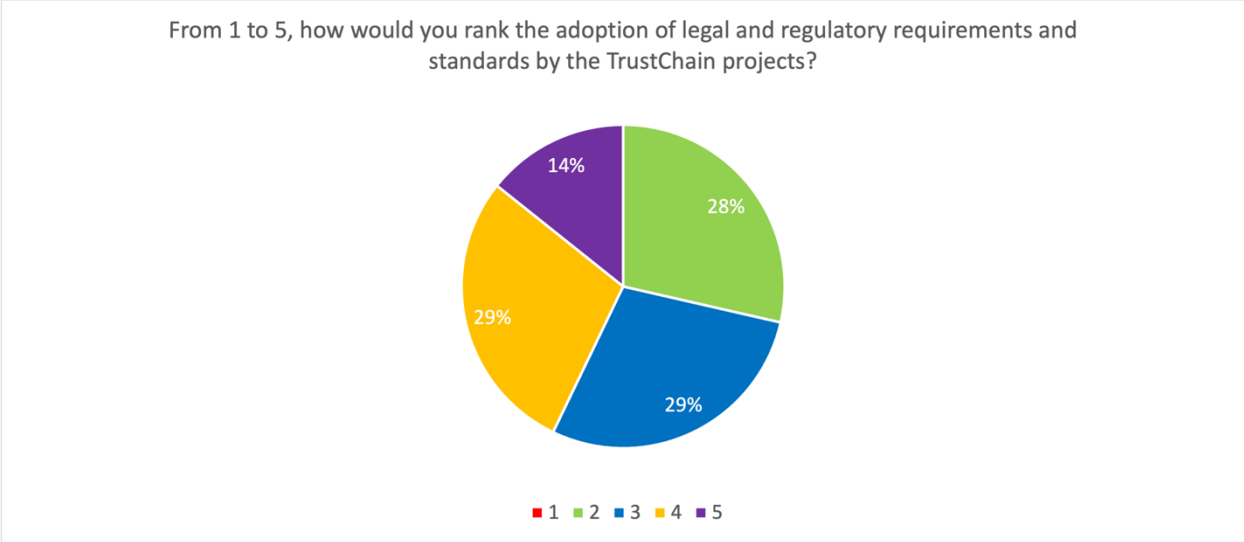

FIGURE 8: FROM 1 TO 5, HOW WOULD YOU RANK THE ADOPTION OF LEGAL AND REGULATORY REQUIREMENTS AND STANDARDS BY THE TRUSTCHAIN PROJECTS?

Feedback received from Advisory Board members:

- *"All projects seemed well aware of regulatory standards, but again this is not my area of expertise."*

- *"Not much was discussed about regulatory requirements. However, data collection, storage, use all need to be DPA. The projects should mention how they would adhere to DPA and should have proper consent in place while collecting and using data. It should address how and where data is stored."*
- *"This is not the strongest point of the project, but please take my evaluation with a pinch of salt as this is not my core domain of expertise. The constraints linked to regulations are only partially addressed by the projects. Several projects, on the other hand, focus on promoting standards and interoperability. Dguard: mentions that the platform will allow complying with GDPR but there are little details about how this happens. The project does not mention the possible tension between this compliance and storing traceability information in blockchains. DIDroom does not mention legal requirements and standards, but efforts are made to support SSI standards (e.g. w3c) and identity management good practices. The MUSAP project targets the ENISA standards or proposals for identity management. It does not mention legal concerns or their implications. For SURE, the project should consider legal risks with synthetic datasets that are declared "safe" by the tool and lead to re-identification attacks later, and what contractual/legal obligations this entails."*
- *"It is difficult to comment on this, as I would need to read about the specific details of how they implement their project. For example, DGuard is about patients' health data records. There would need to be a very thorough process to ensure that data privacy and GDPR provisions are met. DGuard mentions in the presentation that GDPR provisions are met, but in this short amount of time for the presentation it is impossible to give details."*
- *"In terms of technical standards, most projects follow well known practices and justify their choices. As for regulatory requirements, I see specially two projects that may be climbing a slippery slope: Utip-DAM and Next Generation Smart Cities. They handle personal location data as part of their core, which is always tricky."*
- *"Almost all projects make reference to legal and regulatory requirements."*

Takeaways from the Advisory Board's Feedback:

- One of the AB members identifies many projects are trying to comply with the GDPR regulations to protect the consumer data. They are all convinced the data collection is done in line with the regulations.
- Some AM members feel that more focus is around technology and standards and less focus is on the regulatory aspects. The Trustchain consortium has a dedicated legal team and most of the projects do seek regular advice from the legal experts to make sure their projects comply with the EU regulations.

Question 9: "Name two application domains of the TrustChain projects that you found the most interesting and promising."

The answers to the question are as follows:

- Synthetic Data and Sharing of Medical Data,
- Consent management and data Sharing for next generation smart cities,
- Identity management and Privacy-preserving machine learning,
- Secure exchange of IoT data and Privacy-preserving data analysis,
- Healthcare and emergency services.

Feedback received from Advisory Board members:

- *"Synthetic data is a fascinating subject, and the SURE team were well positioned to consider the delicate balance between data privacy and data utility – I found this an exciting presentation. Medical data exchange is well-worn ground but the dGUARD team did have a convincing approach to the problem and had considered privacy and security issues well."*
- *"Consent management is very important for all projects in data sharing and data management. Next generation smart cities have important challenges that needs to be addressed. These two domains are closely related to many other problems like managing credentials, privacy preserving data sharing, etc."*
- *"I like IM4DEC because it has a very specific use case that can help vulnerable people. It is also in alignment with EU regulations, and it can fit with the pan-European tools for emergency calls. I think SURE is taking on a very interesting and difficult problem. I would have like to see more details on what distinguishes them from other solutions and how they can measure how much information is lost, depending on the particular ML/empirical analysis that the end user wants to conduct."*
- *"(1) We (academia and industry) are all still struggling to understand how we can use securely all this data IoT sensors have been collecting. So far, big techs have got more benefits than anyone else, and we've got to change this game. Making IoT data exchange easier, more decentralized, and profitable for more companies and people is key to that. (2) Outsourcing of data analysis tasks has great potential, and assuring data privacy here is critical."*

Takeaways from the Advisory Board's Feedback:

- One of the AB members likes the outcome of the projects focussing on consent management and data privacy especially using synthetic data. Projects which address inclusive design is also highlighted as a positive outcome of some of the projects. The AB felt more details should be provided to help the readers understand the gap in the current technology landscape.
- The comparison with existing technologies and how these projects differentiate themselves can be demonstrated in projects' competitor analysis task. The projects will be advised to clearly demonstrate this aspect going forward to the AB board.

Question 10 "What do you think are the two main contributions of TrustChain to the development of the Next-Generation Internet?"

The answers to the question are as follows:

- *"Placing privacy and security concerns at the heart of digital exchange."*
- *"The use of Web3, and the focus on privacy and data sharing"*
- *"Bridging the gap between privacy-enhancing technologies design/research and their actual use in applications / Easing the integration of advanced and more secure identity management solutions, something that is currently hard."*
- *"Use cases for decentralized digital identity / Promoting the building of applications on the blockchain."*
- *"Innovative thinking / Harnessing technology to improve quality of life."*
- *"(1) Demonstrating the real potential of DLT-based solutions. During the blockchain hype, we saw many solutions including blockchain only as a buzzword. TrustChain is showing that DLTs have great potential for multiple applications. (2) Helping the transition of some techniques like homomorphic encryption and self-sovereign identities from academy to industry."*
- *"Sharing confidential data, protecting user data."*

Feedback received from Advisory Board members:

- *"I was impressed that the projects showed real variation in both context and approach, but that all were very focused on ways to ensure data security and privacy at every point."*
- *"Most of the projects have addressed privacy and data sharing which is very important for the next generation Internet. The next generation internet will be data-centric, so these projects are very timely and effective."*

- *"Technology continually outpaces itself – so maintaining an innovative way of looking at technology and thinking out how it can be harnessed to improve quality of life is a challenge that runs in parallel with that face pace of change. The projects successfully showed how critical thinking can be applied to new technologies to achieve objectives that are needed and useful to society."*

Additional comments provided by Advisory Board members:

- *"The 5-minute presentation is very short, and it is difficult to get a lot of information about the projects. Maybe it would be more helpful if, in addition, the projects provided short answers on a few standardized questions (e.g. what is your main commercialization strategy, what are the main points of your business plan, how have you complied with GDPR regulations etc). This is not to burden the projects in providing lengthy answers, but if they have a short answer, we could pick it up on the Q&A session, after the presentation, or even after the entire session with an email. This is of course only if the projects would consider this to be helpful."*
- *"It would be helpful if, to compare the projects on a like-with-like basis, the presentations followed the same order (for instance: description of objectives, description of logic, description of technologies used, legal considerations, etc). Some presentations gave varying importance to different aspects of their projects, and a like-with-like comparison was therefore harder to make."*
- *"Overall, it was exciting for me to see all the great ideas and applications that have been discussed and developed in TrustChain projects. They are technically sound and address relevant issues in our industry. Additionally, I saw motivated teams, which are clearly trying to come up with innovative products. To improve their solutions, the teams should focus a bit more on user experience (UX). All the proposed solutions are quite complex and will demand a significant design effort to translate all that complexity into friendly and effective applications."*
- *"Describing the state of each project in terms of TRL's would be beneficial to assessing the impact and choosing the appropriate business model for all the projects."*

Takeaways from the Advisory Board's Feedback:

- One of the AB members has highlighted how the projects are well aligned to meet the objectives of the Trustchain project. Most of the AB members are well impressed with the technical merit in these projects. They are also identified the UX aspects and user centric aspects are key to the development of next

generation decentralised internet and commend that many projects have tried to achieve this overarching goal of Trustchain.

- Another AB member has felt the timings were too short for each project presentation and the this will be improved in the future presentations to the AB. The AB also suggested to have a logical structure for all presentations so that they can compare the merits of each project against certain specific criteria. The project mentors will take this onboard and will prepare a standard template for future presentations to AB and also increase the timings of the presentation to 10 mins per project.

5 CONCLUSIONS

This report presents the context, objectives, composition, and activities done during the first year of the Trustchain Advisory Board engagement. The main technological challenges towards the realization of the Trustchain framework are discussed and the feedback received by the Advisory Board on the progress of our project and the desirable performance properties of the envisioned software are presented. Overall, the Trustchain progress was perceived quite positively by the members of the Advisory Board. The Advisory members commended the progress to market, contributions to data privacy and the decentralized trustworthy governance models, and the user-centric approach used by the project, At the same time, the adoption of the legal and regulatory requirements as well as focus on marginalized communities received relatively lowest scores.

The AB also highlighted the need for projects to demonstrate the interoperability and scalability of their proposed systems/tools. They highlighted the need for more inclusive design so that the needs of the marginalised communities are captured in the design phase. The AB also felt that the projects lacked clear business/revenue models.

Our next steps will be to organise thematic workshops with the Advisory Board members to inform them about the ongoing project activities and about the areas of needed contributions and collect feedback on the current arrangement of the third call (i.e. OC3) and any necessary corrective actions. In addition, we will invite the AB to the final selection of the OC4 projects to seek their views. Furthermore, we will emphasise the legal/regulatory aspects and focus on marginalized communities with our incoming project cohorts. The project mentors from the Trsutchain consortium will organise focussed meetings in regulatory aspects, business and governance models and go to market strategies. We will bring external experts to deliver seminars in some of these businesses focussed topics to assist the project to explore commercialisation strategies. The project team are also organising events in next

generation topics such as homomorphic encryption, post quantum cryptography and deepfakes to help the project think a bit more out of the box.