DS-06-2017: Cybersecurity PPP: Cryptography

PRIViLEDGE
Privacy-Enhancing Cryptography in Distributed Ledgers

D5.6 – Stakeholder Engagement Report

Due date of deliverable: 30 June 2021
Actual submission date: 29 June 2021

Grant agreement number: 780477
Start date of the project: 1 January 2018
Revision 1.0

Lead contractor: Guardtime OÜ
Duration: 42 months

Project funded by the European Commission within the EU Framework Programme for Research and Innovation HORIZON 2020

Dissemination Level	
PU = Public, fully open	X
CO = Confidential, restricted under conditions set out in the Grant Agreement	
CI = Classified, information as referred to in Commission Decision 2001/844/EC	

D5.6
Stakeholder Engagement Report

Editor
Liis Livin (Guardtime OÜ)

Contributors
Mirjam Kert, Ahto Truu (GT)
Marko Vukolić (IBM)
Michele Ciampi, Mikhal Volkhov (UEDIN)
Toon Segers (TUE)
Ivan Visconti (UNISA)
Sven Heiberg (SCCEIV)
Nikos Voutsinas (GUNet)
Panos Louridas (GRNet)
Nikos Karaginnidis (I.O. Research)

Reviewers
Marko Vukolić (IBM)
Toon Segers (Technical University of Eindhoven)

29 June 2021
Revision 1.0

The work described in this document has been conducted within the project PRIViLEDGE, started in January 2018. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 780477.

Executive Summary

The "Stakeholder Engagement Report" (Deliverable 5.6) summarises the stakeholder engagement and related dissemination activities for the EU H2020 project PRIViLEDGE, including reports on all workshops and other relevant stakeholder engagement activities such as presentations at conferences. The report covers activities that were accomplished over the 42 months of the project and is connected to the communications and dissemination plans of the project (D5.1 and D5.4) that identified and classified the target audience, the outreach methods and goals.

The PRIViLEDGE project has a broad range of stakeholders drawn from our target audience sectors including academia, industry, policy and general audience. The project's engagement and dissemination activities have met the needs of all these groups. In order to achieve this, the PRIViLEDGE project's team has set up a number of channels to communicate and disseminate information in the most effective, informative way for the different stakeholder groups. These include produced content for social media and our website but also publishing research articles, blogs and news, as well as participating and organizing events such as conferences, workshops, seminars etc. During the project's lifetime PRIViLEDGE parters produced nearly 30 high-level papers, published around 40 news items on our website (blogs incl.), organized four project workshops and gave over 50 presentations about the project and related topics.

In turn, this has enabled the project to maximised the opportunities to increase engagement and to gather feedback and validate the project's results. This report pays particular attention to activities that were determined as key-vehicles to further and foster stakeholder engagement, allowing maximum interaction and input from stakeholders.

Contents

1 Introduction

This deliverable aims to demonstrate that within the project's lifetime PRIViLEDGE engaged with all the determined stakeholders relevant for validation and implementation of the project results. Both the project's communication and dissemination channels, tools and activities, as well as each partner's individual networks were used to reach this goal.

The main purpose of the PRIViLEDGE communication and dissemination strategy (D5.1 and D5.4) has been to maximize the impact created by the project. Thus, the results created under this strategy directly relate to activities described in D5.6 "Stakeholder Engagement Report''. The communication activities and established outreach channels and tools have complemented the PRIViLEDGE promotional and outreach results and enhanced its visibility to stakeholders out of the core target groups.

All consortium partners are contributors to task 5.3 "Stakeholder engagement" under WP5 "Communication, Dissemination, and Exploitation", led by Guardtime OÜ. The document begins with a description of PRIViLEDGE's stakeholder engagement objectives under Section 2, followed by an overview of PRIViLEDGE's stakeholder groups in Section 3. Section 4 reports on the channels we used and activities we conducted to engage with the stakeholders, highlighting among other things our high-level publications and the four workshops PRIViLEDGE organized. This is followed by Section 5 which is dedicated to the individual stakeholder engagement activities and results of all project partners, where they highlight the key result of their individual stakeholder engagement. Finally, Section 6 provides the overall results and assessment of the stakeholder engagement.

2 Objectives and Principles of Stakeholder Engagement

PRIViLEDGE has engaged with stakeholders to collect valuable feedback on research and innovation to advance the development and validate the results. Our engagement has been rooted in the following framework and principles (see Figure 1):

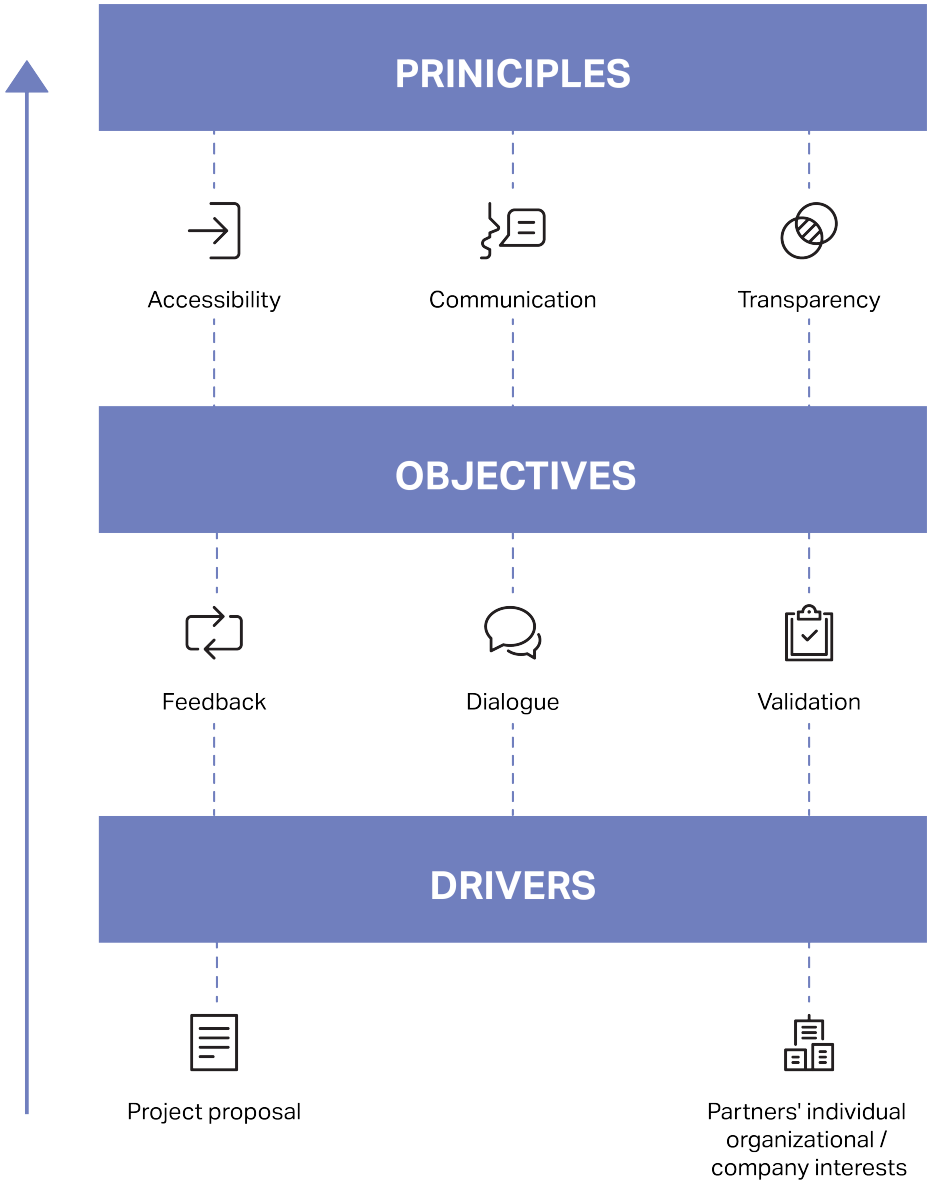

Figure 1: The framework of PRIViLEDGE's stakeholder engagement.

Drivers guiding the stakeholder engagement. Our stakeholder engagement is based on the project proposal and related plans. (e.g., plans for communication, dissemination and exploitation). Additionally, each partner's organizational interests and individual motivation have been the drivers for the stakeholder engagement.

Objectives to engage with stakeholders. The abovementioned foundational drivers have been the baseline for determining the objectives for the stakeholder engagement. Our primary purpose to engage with relevant stakeholders has been to gather feedback, encourage dialogue and validate the project's progress and results.

Principles for engaging with stakeholders. In order to conduct successful stakeholder outreach and engagement PRIViLEDGE has set-up and followed three principles. Firstly, ensuring accessibility to project results has been our highest priority. Thus, we have made all the project deliverables, publications and other relevant information and references to source code available on our website and on respective GitHub project repositories. Secondly, we have also proactively and systematically communicated the project goals, activities and results through offline and online channels. And thirdly, in our presentations, discussions and feedback gathering we have always committed to fostering open and honest discourse.

3 Stakeholder Groups

PRIViLEDGE stakeholder groups correlate with the main target audiences the project has defined for communication and dissemination activities. The target audiences were defined in D5.1 "Initial Communication and Dissemination Plan", refined in D5.4 "Updated Consolidated Communication and Dissemination Plan". During the second half of the project the target audiences crystalized and thus were slightly specified and renamed. The table (see Table 1) below presents a tabular overview of both the target audiences and the related stakeholder groups we engaged with.

Target audience	**Stakeholders**	**Reason(s) to engage**
Industry	iVoting experts and election organisers, health insurance providers, higher education diplomas issuers and end-users, blockchain governance experts, developers, and product managers.	To gather feedback and validate the results, especially the ones related to use-cases.
Academia	Privacy-enhancing cryptography experts, Horizon2020 projects with strong privacy focus (e.g., CUREX, FENTEC, CHARIOT).	To exchange knowledge, foster dialogue and build upon that, to improve the research output of the project.
Policy makers	Representatives of EU institutions and initiatives (e.g., reps of EC, ECSO), governments (e.g., representatives of ministries), blockchain related associations (e.g., INATBA) and networks (e.g., NECC), privacy and industry interest groups with a strong focus on privacy (e.g., MyData Global, GSMA).	To foster dialogue on scientific and technological advances in DLT, especially from security and privacy aspects and gather feedback.
General public	Non-experts interested in electronic voting, e-diplomas, health insurance and software updates; as well as people interested in cryptography, the domain of security and privacy in blockchain and DLT and various DLT applications.	To encourage general debate on security and privacy issues and solutions of/in DLT.

Table 1: Target audiences and related stakeholder groups.

Within the **industry target audience** we have used our four use-cases as drivers and focused on the stakeholder groups that are the most relevant for gathering feedback and validation from **iVoting experts and election organisers; health insurance providers; higher education diploma issuers and end-users; and blockchain governance experts, developers and product managers** These stakeholders has been kept informed about PRIViLEDGE's research and development, we have engaged in discussions with them and used their expertise and

feedback for the developmental work in the project. We have fulfilled our aim to engage this stakeholder group with the issues addressed by the project and have invited them to use/implement the use-case outputs of PRIViLEDGE.

- This stakeholders' group engagement was achieved via website and social media, partners' existing business relationships and networks, events and presentations, blog posts, PRIViLEDGE workshops, meetings, face-to-face interactions.

Within **academia**, our primary stakeholders were researchers studying **DLT and blockchain's privacy and security issues and privacy-enhancing cryptography experts.** We have promoted both the foundational and practical impact of our achieved results, so that they could use and build on PRIViLEDGE results in future academic works and lead the way to other projects that might grow out of innovation and knowledge produced in PRIViLEDGE.

- This stakeholders' group engagement was achieved via website and social media, partners' existing academic networks, lectures, papers, events and presentations, blog posts, PRIViLEDGE workshops - especially PENCIL (see more under section 4.3), face-to-face interactions.

EC representatives, governments, blockchain related associations and networks with a strong focus on privacy from the **policy** target group have been invited to discuss the knowledge acquired during the lifespan of the project and its results with the possibility to have an impact on future policy making in the EU and beyond.

- This stakeholder's group engagement was achieved via website and social media, partners' existing policy networks, meetings, events and presentations, PRIViLEDGE workshops, especially "Data Sharing and Privacy – What Has Changed in the Era of COVID? A Deep Dive into Policy Dilemmas and New Technological Solutions" (see more under section 4.3).

Additionally, PRIViLEDGE project developments and results have been communicated to the **general audience.** We have created general support and awareness of the advantages PRIViLEDGE provides and invited external contributors to use the PRIViLEDGE solution, especially those people who are interested in **electronic voting, e-diplomas, health insurance and software updates or in cryptography in general with the focus on security and privacy in blockchain and DLT and various DLT applications.**

- This stakeholder's group engagement was achieved via website and social media, blog posts, PRIViLEDGE workshops and personal interactions.

4 Stakeholder engagement tools and activities

This section provides an overview of the dissemination tools and activities created and conducted in the project to support and drive the proactive and transparent stakeholder engagement in PRIViLEDGE. We recognise that our stakeholder groups have differing levels of knowledge and interest in our innovation and project's results, which is why we have

tailored our engagement tools and used a variety of channels, including face-to-face meetings, publications, online engagement, workshops and other types of events and networking.

This section starts with the analysis of offline engagement channels (website and social media) usage, which is followed by overviews of PRIViLEDGE stakeholder engagements during various events, workshops and publications to demonstrate the wide range of ways we have engaged with our stakeholders.

4.1 Online outreach

4.1.1 Project website

The PRIViLEDGE website is the project's key dissemination tool and the main source of information about the project, especially for the wide DLT security and privacy community and the general public. It is available at https://priviledge-project.eu

The site contains several sections: general information about the project, news and blog items, contact information and publicly available publications and project deliverables, promotional materials etc. The website is regularly updated to assure that visitors get coherent and timely information about the project as it develops. The visitor numbers of the webpage keep growing, currently having approximately 400-500 visits per month. By the end of the project, the webpage had approximately 19000 visits. It can be concluded that people visiting the PRIViLEDGE website want to know what PRIViLEDGE is about and (then) look for results.

4.1.2 Social media

The project has one social media account on Twitter. Through these channels the project's goals and advances have been shared and promoted. The purpose of PRIViLEDGE's Twitter profile (https://twitter.com/EU_PRIViLEDGE) is to reach a wide audience in a fast and efficient manner. Twitter has been used to communicate the main events, publications, as well as news related to the project. The project's partners help to enhance the project outreach by retweeting. By the end of the project PRIViLEDGE had 245 followers on Twitter. Usually, within a 28-day period PRIViLEDGE Twitter earns around 2500 impressions. Twitter impressions show how many *total* times people have seen the tweets. In total PRIViLEDGE has made close to 200 Tweets.

4.2 Events and presentations

All the attended events have given an excellent opportunity for project partners to interact with stakeholders from different domains relevant to the project and build mutually beneficial relationships. The table (see Table 1) below gives a detailed overview of the over 40 presentations given by PRIViLEDGE partners between January 2019 and June 2021. The previous presentations were reported in D5.4.

It needs to be emphasised that, from 2020, the global COVID-19 pandemic positioned us in a situation where we had to cancel and rethink the participation at several previously planned events. Especially affected were our exhibiting plans. All in all, PRIViLEDGE managed to adjust to the situation and through adjusted presentation methods, we connected with our audiences despite the rapidly changing circumstances. The majority of the 2020 and onwards

events and related presentations were given virtually with the assistance of telecommunication tools.

Nr.	Date	Presenter(s)	Title of presentation	Venue	Audience
1.	12.02.2019	Ivan Visconti	On Deleting Data from a Blockchain	DLT Workshop 2019, Pisa, Italy	Academia & industry
2.	12.02.2019	Luisa Siniscalchi	Publicly Verifiable Argument Systems Through Generic Blockchains	DLT Workshop 2019, Pisa, Italy	Academia & industry
3.	15.04.2019	Luisa Siniscalchi	Publicly Verifiable Proofs from Blockchains	22nd edition of the International Conference on Practice and Theory of Public Key Cryptography (PKC2019), Beijing, China	Academia
4.	06.05.2019	Berry Schoenmakers	MPyC – Overview, Roadmap, and Application to Secure Ridge Regression	Talk for MPC group at TNO, The Hague	Industry
5.	18.05.2019	Michele Ciampi	Timed Signatures and Zero-Knowledge Proofs - Timestamping in the Blockchain Era	PENCIL workshop affiliated with Eurocrypt 2019	Academia
6.	18.05.2019	Björn Tackmann	Asymmetric Distributed Trust	PENCIL workshop affiliated with Eurocrypt 2019	Academia
7.	18.05.2019	Behzad Abdolmaleki	On QA-NIZK in the BPK Model	PENCIL workshop affiliated with Eurocrypt 2019	Academia
8.	18.05.2019	Toon Segers	Verifiable MPC and DLT	PENCIL workshop affiliated with Eurocrypt 2019	Academia
9.	18.05.2019	Luisa Siniscalchi	Publicly Verifiable Proofs from Blockchains and the Attacks of the Clones in Proof-of-Stake Blockchains	PENCIL workshop affiliated with Eurocrypt 2019	Academia
10.	04.06.2019	Berry Schoenmakers	Zero-Knowledge Proofs	Talk for working group at Logius, The Hague	Industry
11.	28.06.2019	Ivan Visconti	Tutorial on Blockchain	Annual Event of the Italian Group on Telecommunication Technologies, Pavia, Italy	Academia
12.	30.08.2019	Ahto Truu	A New Approach to Constructing Digital Signature Schemes	International Workshop on Security (IWSEC 2019), University of Tokyo, Tokyo, Japan	Academia
13.	12.-13.11.2019	Liis Livin, Anna-Maria Osula, Ahto Truu	Exhibition booth on PRIViLEDGE use cases	CONVERGENCE, Malaga, Spain	Policy makers & industry

14.	21.08.2019	Luisa Siniscalchi	Publicly verifiable zero-knowledge proof from **any** blockchain.	Talk at Centre for Quantum Technologies (CQT) Singapore	Academia
15.	10.09.2019	Ivan Visconti	The Rush Dilemma: Attacking and Repairing Smart Contracts on Forking Blockchains	De Cifris Seminar Series, University of Trento, Italy	Academia
16.	29.10.2019	Berry Schoenmakers	Verifiable MPC	ZKProof Community Event	Academia, industry & policy makers
17.	01.11.2019	Berry Schoenmakers	Kaplan-Meier Survival Analysis in MPyC and Other Examples of Privacy-Preserving Data Analytics	PPDS workshop, CBS, The Hague	Academia & policy makers
18.	19.11.2019	Sven Heiberg	Applying Block Chains for Electronic Voting Bulletin Boards	Webinar, Blockchain: multi-application viewpoints and opportunities, Cyberwatching.eu	General public, privacy enthusiasts
19.	21.01.2020	Ahto Truu	Verified Security of BLT Signature Scheme	9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), New Orleans, Louisiana, USA	Academia
20.	23.01.2020	Ahto Truu	Quantum-proof digital signatures	Blockchain Lab, Arizona State University, Phoenix, Arizona, USA	Academia
21.	04.02.2020	Ivan Visconti	Data Privacy in Blockchains: Theory and Practice"	3rd Distributed Ledger Technology Workshop (DLT 2020), Ancora, Italy	Academia & industry
22.	04.02.2020	Vinceno Botta	Attacking and Repairing Smart Contracts on Forking Blockchains	3rd Distributed Ledger Technology Workshop (DLT 2020), Ancora, Italy	Academia & industry
23.	21.05.2020	Markulf Kohlweiss	Secure and Private Distributed Ledgers: ZK - Saviour and Saved	ZKProof Home Edition	Standardization
24.	02.07.2020	Markulf Kohlweiss	Zero knowledge and blockchains	Cardano Virtual Summit 2020	Industry
25.	03.07.2020	Nikos Karagiannidis, Michele Ciampi, Damian Nadales, Dionysis Zindros	Decentralized Software Updates	Cardano Virtual Summit	Industry
26.	14.09.2020	Ahto Truu	Verifiable Multi-Party Business Process Automation	The Third Workshop on Security and Privacy-enhanced Business Process Management (SPBP 2020), online event due to COVID	Academia
27.	16.09.2020	Michele Ciampi	Updatable blockchains	Esorics 2020. Guildford, United Kingdom	Academia

28.	15.10.2020	Toon Segers	Privacy advances in DLT by PRIViLEDGE partners	Priviledge Virtual Workshop "Data Sharing and Privacy – What Has Changed in the Era of COVID? A Deep Dive into Policy Dilemmas and New Technological Solutions''	Policy makers & industry
29.	20.10.2020	Michele Ciampi	Timed Signatures and Zero-Knowledge Proofs - Timestamping in the Blockchain Era	18th International Conference on Applied Cryptography and Network Security	Academia
30.	15.10.2020	Ivan Visconti	Introduction to PRIViLEDGE (Moderator)	Priviledge Virtual Workshop "Data Sharing and Privacy – What Has Changed in the Era of COVID? A Deep Dive into Policy Dilemmas and New Technological Solutions''	Policy makers & industry
31.	04.11.2020	Berry Schoenmakers	Publicly Verifiable Secret Sharing and Its Use in Threshold Cryptography	NIST Workshop on Multi-Party Threshold Schemes, MPTS 2020	Academia & industry
32.	06.11.2020	Ivan Visconti	Blockchain Technology and Decentralized Contact Tracing: The Good, the Bad and the Ugly"	Launch event of the new research cluster: "Cybersecurity, Design and Human Behaviour" at RHUL	Academia
33.	01.12.2020	Ivan Visconti	The Gaze of the Gorgon, A Trojan Horse or An Offer We Could Not Refuse?	Web seminar: Contact Tracing & Giant Data Collectors: A Journey from Utopia to Dystopia?	Academia, policy makers & general Public
34.	11.12.2020	Ivan Visconti	There Is Something (Wrong) About Digital Contact Tracing	CS@GSSI/ICE-TCS webinar series	Academia
35.	09.12.2020	Ivan Visconti	Introduction to PRIViLEDGE (Moderator)	Virtual workshop at Paris Blockchain Week Summit	Industry
36.	09.12.2020	Ahto Truu	DLT Applications through Advanced Cryptography: Health Insurance	Virtual workshop at Paris Blockchain Week Summit	Industry
37.	09.12.2020	Sven Heiberg	DLT Applications through Advanced Cryptography: i-Voting	Virtual workshop at Paris Blockchain Week Summit	Industry

38.	09.12.2020	Panos Lourdes	DLT Applications through Advanced Cryptography: Higher Education Certificates	Virtual workshop at Paris Blockchain Week Summit	Industry
39.	09.12.2020	Nikos Karagiannidis	DLT Applications through Advanced Cryptography: Decentralized Software Updates	Virtual workshop at Paris Blockchain Week Summit	Industry
40.	15.12.2020	Michele Ciampi	Updatable Blockchains	CifrisChain seminar (online)	Academia
41.	01.03.2021	Daniele Friolo	Shielded Computations in Smart Contracts Overcoming Forks	Financial Cryptography and Data Security 2021	Academia
42.	02.03.2021	Mikhail Volkhov	Another Look at Extraction and Randomization of Groth's zk-SNARK	Financial Cryptography and Data Security 2021	Academia
43.	21.02.2021	Vincenzo Botta	Towards Defeating Mass Surveillance and SARS-CoV-2: The Pronto-C2 Fully Decentralized Automatic Contact Tracing System	CoronaDef Workshop 2021	Academia & industry
44.	03.03.2021	Nikos Karagiannidis	Efficient State Management in Distributed Ledgers	Financial Cryptography and Data Security 2021	Academia
45.	27.04.2021	Mikhail Volkhov	Snarky Ceremonies; Presentation of standardization proposal on trusted setup ceremonies for zk-SNARKs	ZKProof Workshop 4	Academia
46.	29.04.2021	Sven Heiberg	Internet Voting Technology and DLT Applications through Advanced Cryptography	Principles of Secure Software Design, University of Tartu, invited lecture	Academia
47.	09.06.2021	Nikos Karagiannidis	Decentralized Software Updates	Decrypto Seminar	Academia

Table 2: List of PRIVILEDGE presentations at various events.

4.3 PRIViLEDGE Workshops

The project has had four dedicated workshops throughout the project's lifetime. The following section gives an overview of the workshops' objectives, presented content and the stakeholders we engaged with. The workshops are listed in the topical order that was presented in the project proposal.

Workshop 1: PENCIL - Workshop on Privacy Enhancing Cryptography in Ledgers. Affiliated event of EUROCRYPT2019 in Darmstadt, Germany, 18. May 2019.

This workshop was dedicated to delivering PRIViLEDGE research results and brought together researchers and practitioners working in cryptography, security, and distributed systems from academia and industry, who were interested in cryptographic techniques for improving the privacy and security of blockchains and their applications. The main goal of the workshop was to foster information exchange between attendees from the different areas, to present new developments in cryptographic schemes and protocols, as well as applications and challenges to stimulate both use of new cryptographic techniques to improve DLT-based systems as well as future cryptographic research targeting applications in DLT.

The program included 3 invited talks, 8 presentations of results accepted (out of 23 submissions) by an international program committee chaired by PRIViLEDGE members, and 5 presentations about results presented by PRIViLEDGE members showing their initial achievements during the project.

With its 107 participants, this workshop has been the one with the highest attendance among all workshops affiliated with EUROCRYPT 2019. Participants were researchers working in academia and industry and Ph.D. students. Several results presented during the workshop have been later on published in top conferences, and thus PENCIL has been certainly useful to show the main directions in which privacy-enhancing cryptography can help the adoption of distributed ledger technology and its applications.

Workshop 2: DLT Applications through Advanced Cryptography: i-Voting, Health Insurance, Higher Education Certificates and Software Update Domains, 9. December 2020

This workshop was dedicated to delivering and demonstrating PRIViLEDGE use cases and was delivered within the framework of Paris Blockchain Week Summit 2020. The virtual event had a strong industry focus with over 3100 attendees.

The engagement goals for this workshop and result for each use-case were as follows:

1. iVoting use-case's main goal was to present the voting protocol that allows to publish cryptographic audit trails necessary for the integrity verification in such a manner that it can be made available for everyone on the public ledger without risking the ballot secrecy even in the long term. We demonstrated how in this case it would be possible for election organizers to improve availability of an election without losing the transparency and observability of paper-based elections.

   The presentation was met with interest and discussion by the participants. As the audience was more technology oriented, the focus was on DLT itself and other potential use-cases. Follow up meetings with some participants e.g., consento.org were held to dive deeper into the specifics of using DLT in use cases with privacy requirements.

2. For the health insurance use-case the main goal of the workshop was to showcase the new possibilities in healthcare contract types enabled by advanced cryptographic techniques while maintaining high standards of patient data privacy.

We made several new contacts in the distributed ledger community in France and EU. It remains to be seen whether these contacts will lead to new business for Guardtime, but at least the contacts are now aware of both Guardtime and other PRIViLEDGE partners in general and of our capabilities in the areas of privacy-enhancing cryptographic tools in particular.

3. For the diplomas use-case the main goal was to showcase how the blockchain could be used to certify diplomas in a privacy-preserving way. There are several proposals for how diplomas could be certified on distributed ledgers (and quite a bit of entrepreneurial activity as well). The focus of the presentation, therefore, was to show the differentiating aspects of the diplomas use-case: in particular, that certification happens with zero-knowledge proofs and is designated for each specific recipient, so that the privacy of the information pertaining to the diploma can be preserved. The presentation was positively received, judging from the comments and the discussion that followed.

4. The main goal for decentralized software updates use-case was twofold: a) to present at a high level our decentralized software updates framework and b) to raise awareness regarding the importance of decentralized governance for blockchain systems. To this end, the core parts of our technical solution were explained. Moreover, we have tried to highlight how important it is to identify the main decisions in the software update lifecycle that ought to be collectively decided and then provide a secure mechanism for decentralizing this decision-making process. Finally, we have pointed out the roadmap and commitment of the Cardano blockchain to decentralized governance and underlined the importance of the PRIViLEDGE results in this journey. As a main takeaway from this workshop for our use case, we identify the increasing realization from the blockchain community side of the importance of decentralized governance for self-sustaining blockchain systems and the expectation for Cardano to become soon such a system by leveraging our PRIViLEDGE results.

Workshop 3: "Close and personal with PRIViLEDGE Stakeholders" March-April 2021.

This workshop was dedicated to exploitation of PRIViLEDGE results. Within this workshop, altogether 15 interviews were conducted with the aim to:

1. investigate PRIViLEDGE's use-cases' suitability for application domain and potential users,
2. find matches/mismatches from the value propositions prepared for the end-users,
3. establish mutually beneficial and sustainable relationships with the interviewees.

The interviews of the workshop were carried out in four segments that correspond to PRIViLEDGE use-cases: iVoting, health insurance, Diplomas, decentralized software updates. The grouping of the interviews was important because each PRIViLEDGE use-case has their own specific value propositions and stakeholders with whom they engage with.

As a result, the workshop interviews provide the following key take-aways:

1. Most interviewees were able to articulate and discuss clear benefits of implementing a PRIViLEDGE use-case after they were introduced to the project and the use-case specific solution by the interviewers. They were able to see how it can be implemented one way or the other now or in the future.

2. The most important benefits that PRIViLEDGE can provide according to the interviewees are integrity of elections process and higher number of voters for iVoting use-case; precise patient treatment and a more efficient health care system for health insurance use-case; digitalization of the system, tamper-proofness and process effectives (from both HE issuing and HR hiring side) for diplomas use-case; self-sustainability, decentralized governance and deep research furthering Cardano for decentralized software updates use-case.

3. The biggest barriers to implementing PRIViLEDGE according to the interviewees are technical integration aspects and general social reluctance to use emerging new technologies, i.e., due to low level of relevant communities and users understanding/being educated on the new technology/solutions the implementation might be hindered.

As a result of the workshop, it was confirmed that all the use-cases solve important problems and offer novel solutions. Also, the value offers of all use-cases match the stakeholder's expectations either completely or partially. The results of the workshop were released as a thorough report and published on PRIViLEDGE's website on 20th of May 2021.

Workshop 4: "Data Sharing and Privacy – What Has Changed in the Era of COVID? A Deep Dive into Policy Dilemmas and New Technological Solutions", 15. October 2020.

This workshop was dedicated to exploring DLT related policy issues with stakeholders from policy, industry and academia. The workshop was organized by project PRIViLEDGE individually and carried out via Zoom Webinar tool. It was attended by 54 people from 15 different countries.

With this workshop PRIViLEDGE took on the challenge and opportunity to unite the different parties from policymakers to industry and R&D representatives to explore the technological advancements and generated knowledge of PRIViLEDGE from the data security and privacy perspective. The virtual workshop facilitated numerous exchanges of ideas. The presenters explored the current data sharing "climate" and explained the different research advances and policy initiatives.

The workshop was built up in two sections. The first part focused on setting the scene with key-note panellists speaking about data sharing and privacy from governmental, public and industry perspectives. The second section of the workshop explored novel data sharing and security avenues emerging from R&D results from four H2020 projects focused on enhancing DLT, blockchain or alternative solutions. This section began with PRIViLEDGE project's presentation by Toon Segers, and was followed by CUREX project, FENTECT project and CHARIOT project.

As a result of the workshop, we re-confirmed that research, industry and policy communities need to cooperate and communicate with each other even more closely in order to tackle the present and future challenges of big data, data sharing and security. There is significant overlap in interests between these communities and the many current and upcoming EC initiatives promise to boost and support the collaboration between these stakeholders to create sustainable solutions for data sharing and privacy. It also brought into the light several nuances and caps in the EU data sharing environment from technical and practical standpoints, but also offered many innovative solutions.

4.4 Publications

4.4.1 Academic Publications

PRIViLEDGE has a strong scientific foundation and many of the research results have been published in conferences with formal proceedings and in journals. By the end of the project, we had 54[1] publications. All the publications have also been made available on PRIViLEDGE website and are thoroughly reported in D6.4 "Second Scientific & Research Impact Measurement".

Research results achieved in PRIViLEDGE include contributions about blockchains, their applications and their connections with privacy enhancing cryptography. Several publications appeared in proceedings of (prestigious in some cases) conferences and this is very typical when considering research in computer science. This section discusses a few of the achieved results by respective partners, focusing on the ones that have had the greatest impact in furthering our work in the project and on the wider DLT privacy and security spectrum.

GT. Guardtime's academic publications in PRIViLEDGE have focused on hash-based digital signatures, with new results presented at NordSec 2018, IWSEC 2019, and CPP 2020; most recently, two papers have been accepted to appear at CSF 2021 and SECRYPT 2021. Additionally, we presented our results on verifiable business process execution at SPBP 2020.

TUE. TUE researcher publications have focused on extending applications and supporting primitives for Secure Multiparty Computation (MPC), in particular efficient protocols for: matrix decomposition; comparison of medium-sized inputs; linear and ridge regression; Moore-Penrose pseudoinverse; finite group operations, focusing on applications in threshold cryptography; verifiable MPC, i.e., proving in zero-knowledge the correctness of an MPC computation. TUE implemented all the above protocols on top of its open-source MPyC library, which was launched and extended extensively during the course of PRIViLEDGE, introducing many new secure types and arithmetic (e.g., finite fields, integers, fixed-point, floating-point, oblivious lists).

UEDIN. In collaboration with I.O. Research, the research team has contributed to defining and modelling software updates for blockchains. The result of this research has been presented to ESORICS 2020. The University of Edinburgh has also studied new notions of security related

[1] This number includes journal and conference papers and technical reports published by the end of the project, as well as papers confirmed to be published after the project.

to the timestamping problem. The output of this research consisted of a new security notion of timestamping that can be realized by using the blockchain as a setup, and in an analysis that formally captures the unpredictable values generated during the lifetime of blockchain systems like bitcoin. These results have been presented to ACNS 2020. The team has also provided a universally composable formalization of private smart contracts and provided a realization of them. These results are collected in a paper presented at IEEE Computer Security Foundations Symposium 2021. The team continued investigating the notion of sidechains, presenting a result in the proof of stake setting at IEEE Security & Privacy 2019. A work on improving setup ceremonies for zk-SNARKs is accepted at ZKProof 2021 workshop. Another work on analyzing and improving security and performance properties of one of the most popular zk-SNARKs was published at Financial Cryptography 2021.

UNISA. In IACR PKC 2019 and IACR PKC 2021 the research team contributed to a novel form of privacy-preserving (i.e., witness indistinguishable and zero knowledge) proof systems that leverage blockchains using them as a decentralized setup. Similarly, in IACR EUROCRYPT 2020 the research team exploited some unpredictability derived from the decentralization of blockchains to produce a weak form of randomness beacon that is a useful functionality for protocol designers. In CoronaDef 2021, the research team showed that blockchains can be leveraged to construct transparent privacy-preserving contact tracing systems. In ACNS 2021 smart contracts are designed to exploit vulnerabilities of currently deployed contract tracing systems (e.g., SwissCovid). In FC 2021 the research team has shown how to tackle vulnerabilities due to forks of blockchains without delaying computations because of slow block confirmations.

SCCEIV. In E-Vote-ID 2018, the SCCEIV team published its research on applying public permissionless block chain for electronic voting bulletin boards.

4.4.2 Blog posts

In addition to the above-mentioned publications, all PRIViLEDGE partners were dedicated to writing and publishing **blog posts** targeted for general audience.

By the end of the project, we published 29 blog posts on various topics related to the project that are suitable for a general reader with interest in the field of DLT. The blogs helped the project followers to gain further insight into the project research and the development of different use cases.

The list of published blog posts is as follows:

1. Looking back and looking ahead
2. Zero Knowledge
3. It's time to stamp time
4. Asymmetric Distributed Trust
5. Successful first project workshop
6. Alice proves to Bob that she has graduated with diploma
7. Introducing TIVILEDGE: Next Generation Blockchain Online Voting
8. Toolkit for post-quantum secure protocols in ledgers
9. Software Developers vs Blockchain Application Developers
10. Introducing ‘The World’s Billionaires Problem’

11. Privacy Challenges and Requirements in the Diploma Record Ledger
12. What did 2019 deliver to PRIViLEDGE and PRIViLEDGE to 2019?
13. How decentralized are your software updates?
14. Reasoning about privacy in smart contracts
15. Privacy meets accountability in token payment systems
16. Safe storage of data on ledgers
17. Auditable Multi-Party Computation
18. Property testing a software update mechanism
19. Introducing TIVILEDGE: Next Generation Blockchain Online Voting, Part II
20. Updatable Blockchains
21. Blockchain Technology and Decentralized Contact Tracing: The Good, The Bad and the Ugly
22. Privacy Advances by PRIViLEDGE Partners
23. eDiplomas platform reaches new heights in Greek legislative policy and digital transformation of Higher Education Institutes
24. PRIViLEDGE 2020 flashback
25. Linear Relations on QAP Polynomials
26. MPC company Roseman Labs puts academic results from PRIViLEDGE into practice
27. Toolkit for Secure Multi-Party Computation on Ledgers
28. Mir-BFT goes Hyperledger Labs: high-throughput and scalable open-source consensus for decentralized networks
29. Achievements of the PRIViLEDGE project

5 Stakeholder engagement report by partner

In this section all the project partners report on their individual stakeholder engagement activities throughout the project lifecycle. Firstly, each partner gives an overview of the stakeholder groups they engaged with, combined with the activities they carried out to reach out to and engage with designated stakeholders. This is followed by showcasing the key results and future work with relevant stakeholders. It should be noted that concerning the diplomas use-case, lead jointly by GUNet and GRNet, this section includes GUNet's report, as the former was responsible for stakeholder engagement out of the two partners.

5.1 Guardtime

Through-out the project Guardtime (GT) has prioritized the stakeholders from the industry target audience. Guardtime has been engaging with the **producers of pharmaceuticals**, **health insurance funds** (e.g., Estonian and Swedish Health Insurance Funds), **medical centres** (e.g., North Estonia Medical Centre Foundation) to gather feedback and understand the need for privacy and security of data in the sector in more depth. This has been valuable feedback also for the use case development. Guardtime has been actively engaging with Roche, AstraZeneca, and Takeda. There are ongoing discussions for collaboration and further enhancement of the work done so far.

Guardtime's target stakeholder groups in academic context are: 1) **researchers** in relevant fields for exchange of ideas, primarily to further our work on hash-based digital signatures, and 2) **students, as potential future employees**. We have engaged with the former by publishing and presenting at conferences and with the latter by giving guest lectures at several universities. In order to engage with the academic stakeholder Guardtime has presented its results in multiple international forums, like NordSec 2018, IWSEC 2019, and CPP 2020. Moreover, as also reported above, two papers have been accepted to appear at CSF 2021 and SECRYPT 2021. Additionally, we presented our results on verifiable business process execution at SPBP 2020. We also gave talks on those topics at industry conferences (the ACCU conference in 2019 and 2021) and in several universities (Tartu University and Tallinn University of Technology in Estonia, Arizona State University in USA).

From the policy perspective Guardime has had an active attendance and discussions about our work done within the project in various cybersecurity and blockchain related organizations, initiatives and networks, both on national and international level. Guardtime is a active member of INATBA, ECSO, the North European Cybersecurity Cluster (NECC) and the Estonian Information Security Association (EISA), and a contributor to the work of European Blockchain Partnership, EU Blockchain Observatory and Forum, Energy BRIDGE as well as the CEN/CLC/JTC 19 Blockchain and Distributed Ledger Technologies standardisation committee, and the EIT Digital ecosystem. Guardtime has been actively engaging in these organisations meetings as well as presenting the project and discussing various topics related to PRIViLEDGE such as DLT's and data integrity.

As key results of stakeholder engagement Guardtime:

- gathered vital feedback to further develop our use case and adjust to the needs of the users,

- created market visibility,
- established a good network of expertise in the healthcare domain,
- improved its understanding of the methods and challenges on data sharing within the healthcare domain,
- expanded its deep knowledge on multi-party computation and zero-knowledge proofs.

In the future Guardtime continues negotiations and work with the stakeholders established in PRIViLEDGE and will use them in the next phase of developing our use-case as well as our academic work. Guardtime has a dedicated team working on healthcare solutions and the work done throughout the PRIViLEDGE project will be explored further with the aim of developing it into a commercial solution. Furthermore, besides the current use-case, Guardtime will also look for other areas besides health-care where the cryptographic techniques developed in PRIViLEDGE could be implemented.

5.2 IBM

All IBM contributions developed in the context of PRIViLEDGE are dedicated for inclusion in one of the Hyperledger projects (mainly Hyperledger Fabric) or planned as a standalone contribution that can be leveraged in multiple Hyperledger projects. Thus, the engaged stakeholder groups that are impacted by IBM's work in PRIViLEDGE can be broadly summarized as the **organizations that are interested in the Hyperledger ecosystem** which consists of more than 200 members. As an example of the latter, IBM has promoted one of the key outcomes of PRIViLEDGE, a toolkit for flexible consensus, based on a novel BFT protocol called Mir-BFT as a Hyperledger Lab (https://github.com/hyperledger-labs/mirbft). Mir-BFT was foreseen in PRIViLEDGE as the basis for a toolkit for flexible consensus in Hyperledger Fabric, but the interest in it grew beyond Hyperledger Fabric, which is why IBM promoted it to a full-fledged standalone Hyperledger Lab. As such, Mir-BFT can impact a broader community than that of Fabric. Furthermore, IBM has given numerous invited talks about Mir-BFT including academic organizations such as University of Cambridge and University of California at Davis, general venues such as 2020 Hyperledger Global Forum, as well as at industrial organizations such as Facebook Novi.

As a key result of stakeholder engagement IBM:

- established the Mir-BFT Hyperledger Lab in April 2021 for a wider promotion of the flexible consensus toolkit developed in PRIViLEDGE. As Mir-BFT is expected to power a variety of IBM blockchain and distributed ledger offerings, including Hyperledger Fabric, the importance of this stakeholder engagement is very high.

In the future, IBM will continue to invest in Mir-BFT and Fabric ecosystems, communities and stakeholders even after the end of the PRIViLEDGE project. As the main goal, IBM plans to work in a community-oriented manner towards finalizing production ready implementation of the Mir-BFT library, as a Hyperledger Lab, which is then expected to be used as consensus in many blockchain and DLT projects within and outside the Hyperledger family.

5.3 The University of Edinburgh

The University of Edinburgh (UEDIN) engaged both with the general public of blockchain enthusiasts (including in particular Cardano community) and entrepreneurs as well as the academic community. In addition, we engaged the ZK proof standardization community as well as open-source communities.

UEDIN representatives attended and presented at various events to engage with the stakeholders. For example, the 2nd ZK Proof online workshop and the 4th ZKProof online workshop were essential to engage with the ZK proof community. Additionally, UEDIN has been engaged with ZK Proof online community via Telegram group and the community reference document[2]. UEDIN researchers have also given talks on general zero-knowledge protocols, Ouroboros crypsinous, and private smart contracts.

Moreover, in 2020 the UEDIN team helped to organize the Advances in Blockchain Technology-Scotland event for Blockchain enthusiasts and entrepreneurs. The event was organised by the Blockchain Technology Lab in partnership with the Bayes Centre at the University of Edinburgh and had keynotes by Charles Hoskinson (CEO of IOHK) and Dale Chrystie (FedEx). In addition, UEDIN members of Privilege gave talks and participated in discussions. UEDIN also regularly presented PRIViLEDGE accomplishments in joint seminars on zk-SNARKs with University of Bergen and Simula Laboratory.

UEDIN also engaged with the wider spectrum of open-source communities through the International Association of Cryptographic Research (IACR) and participated in events like Theory of Cryptography Conference 2020, Financial Cryptography 2020, Conference on Practice and Theory of Public-Key Cryptography, 2020, 2021.

As a key result of stakeholder engagement UEDIN:

- significantly improved the wider understanding of ZK and its applicability thanks to the stakeholder engagements, combined with social media communications and participation in industry relevant events.
- built a successful course of “Blockchains and Distributed Ledgers” held at the University of Edinburgh.

In future UEDIN’s stakeholder engagement and collaboration plans include the following three streams. 1) Ongoing implementation of “Mining for Privacy” work done by T. Kerber, A. Kiayias, M. Kohlweiss in partnership with IOHK, with the intention of producing a protocol that allows running a decentralized SRS procedure for Sonic zk-SNARK. Such a solution would benefit many protocols and solutions that intend to use Sonic or other updateable SNARK systems such as PLONK or Marlin. 2) Continuing the process of ZKProof standardization. One important resource is the ZK PRoof community reference into which UEDIN’s work on “Snarky Ceremonies” is yet to be integrated. The reference document is intended for both academic and practical users, and in general addresses a wide auditory -- its purpose is to both provide an introductory description of concepts used in the community of ZK experts, as well as to provide a set of reasonable defaults for practical implementations of ZK related algorithms.

[2] https://docs.zkproof.org/pages/reference/reference.pdf

UEDIN's contribution should help a wide set of practitioners who want to run their own trusted setup ceremony for a pairing-based SNARK, such as Groth's 2016 SNARK. 3) Also, the work on private smart contracts in Kachina is influencing the privacy design for smart contracts. The collaboration with IOHK is expected to result in better understanding of mechanics of smart contracts, especially with respect to the programming language area; that is, it is likely to influence IOHK's smart contract language solutions and blockchain projects that use these solutions.

5.4 The Technical University of Eindhoven

The Technical University of Eindhoven (TUE) has identified several specific stakeholder groups from the target audiences with whom they have engaged with throughout the project. From the academic domain, TUE has prioritized engaging with research groups and academic communities focused on secure multi-party computation (MPC) to exchange research findings. While engaging with the industry TUE's focus has been on (potential) partners who operate with or develop applications of MPC. TUE has also informed policy makers on privacy technology and MPC especially.

TUE engaged with the scientific community on PRIViLEDGE related topics, particularly, e.g., during the ZKProof workshop and the NIST Workshop on Multi-Party Threshold Schemes. TUE also engaged with industry partners such as TNO, Royal Philips (e.g., on MPC in digital health), the Dutch government (Logius) etc.

As a key result of stakeholder engagement TUE:

- improved significantly the wider understanding of MPC and its applicability, with the support of established stakeholder relationships, combined with social media communications and participation in industry relevant events.
- founded a spin-off company, Roseman Labs, a company focusing on secure multi-party computation that is valorising the project's open access MPC research output.

In the future, TUE continues to engage with academic, government and industry partners to innovate and promote privacy technologies, particularly MPC.

5.5 The University of Salerno

The University of Salerno (UNISA) engaged with stakeholders from industry, academia and policy. From the industry target audience UNISA engaged with **companies interested in permanently storing documents in ledgers**, in using ledgers to provide transparency in supply chains. Amongst the academic communities, UNISA engaged with **researchers** interested in joint research projects and in disseminating t**echniques for security and privacy in blockchains**. journalists, and policy makers interested in transparency and decentralization issues in digital contact tracing.

Members of the UNISA research team presented their work and role in PRIViLEDGE in both national and international workshops/conferences and advertised its activities on the Web and social networks. UNISA's representative (Ivan Visconti) has been the coordinator of Italian

group “CifrisChain” that includes cryptographers working in industry and academy and are interested in cryptographic aspects of blockchains, which has given for UNISA an outstanding opportunity to engage with stakeholders on the national level. UNISA is also a member of the academic advisory body of INATBA and has contributed to its activities related to private data in blockchains.

As a key result of stakeholder engagement UNISA:

- the company Farzati Tech funded a 6-month scholarship to support a study on formalizing the features added by ledgers to food-oriented supply chain management systems.
- UNISA research team members conducted new joint research with new national and international researchers focusing on ledgers and their applications.
- several students have been supervised for their master theses on exploiting ledgers and their applications at the University of Salerno, M.Sc. in computer engineering.

In the future UNISA aims to submit grant proposals to the forthcoming Horizon Europe program, building on the relationships and cooperation with PRIViLEDGE stakeholders. There is also a growing interest from industry towards the final results of the project, including the toolkits, that UNISA will try to push forward.

5.6 Smartmatic-Cybernetica Centre of Excellence for Internet Voting

Smartmatic-Cybernetica Centre of Excellence for Internet Voting (SCCEIV) engaged with stakeholders from different groups including academic, industry and policy making. More precisely, SCCEIV discussed the DLT for online voting in general and the approach taken in the PRIViLEDGE project in detail with members of the academic community (computer science, security, University of Tartu) and the value proposition of the PRIViLEDGE project results with its industrial partners (Cybernetica, Smartmatic). Also, SCCEIV discussed the applicability of the DLT for online voting with policy influencers and election organizers (from Estonia and UK, including them in the PRIViLEDGE workshop wiith stakeholder interviews) and SCCEIV introduced the results from the PRIViLEDGE project to more general audiences in the workshops (PBWS, Cyberwatching.eu).

To engage with the stakeholders mentioned above, SCCEIV used various tools and performed several activities. SCCEIV conducted stakeholder engagement interviews with research, industry and policy people, published a research paper about the work with the DLT, wrote a BSc thesis at the University of Tartu. SCCEIV also carried out internal seminars about the TIViLEDGE online voting system for the industrial partners and introduced the PRIViLEDGE project to prospective customers as part of marketing meeting/tender or request for information response. SCCEIV representatives gave multiple presentations to engage with the both the academic and industry stakeholder, e.g., Cyberwatching.eu webinar on “Blockchain: multi-application viewpoints and opportunities” and Paris Blockchain Week Summit. Additionally, SCCEIV wrote several blog posts for the general audience that were released on the project’s website.

As a key result of stakeholder engagement SCCEIV:

- realized the importance of finding proper balance between various parameters such as security, usability, environmental compatibility, etc. The stakeholders come with

often conflicting ideas even within the specific stakeholder groups. As an example - there are stakeholders who consider privacy a most important property to achieve democratic elections, whereas there are stakeholders who say that privacy in elections is mostly over-hyped and a secondary requirement. Both of these stakeholders, at the same time, consider transparency about achieving the correctness of the election result utmost important.

- found out that, although the cryptographic mechanisms for achieving transparency are important, there is also the usability aspect which has not been in the focus in the development of the TIViLEDGE.
- concluded that the application of DLT for securing the elections at governmental level requires a paradigm shift, since the kind of distribution of government duties across different organizations for shared responsibility is not the model that works currently with mostly centrally managed elections.

In the future the most important step for SCCEIV is the conversion of the experimental work done in the PRIViLEDGE project into a packaged solution for both existing and future customers. This means additional work in the following areas: (1) usability of cryptographic transparency features from layman perspective and (2) the organizational changes and agreements needed to apply the distribution of the ledger to certain election types/settings.

5.7 Greek Universities Network

Greek University Network (GUNet) engaged stakeholders from industry, academia and policy streams. GUnet has launched a pilot service where a citizen can get a verifiable digital copy of her diplomas or authorize a third-party organization to request and receive a verifiable digital copy of her diplomas. Via this pilot service GUnet was able to signal the **industry (e.g., Vivartia Food Services)** about the new digital channel in this field and mobilize consumers and technology providers both from the public and private sector. Additionally, GUnet has engaged with various **academic institutions (e.g., National and Kapodistrian University of Athens)** in an effort to keep them in the loop on the latest developments, gather feedback as far as the inclusion of DLT in the architecture of the digital diplomas service is concerned and achieve consensus from the main institutions. In the ecosystem the academic institutions play the role of the diplomas issuers and their involvement is critical for the success of the endeavour. Finally, the **policy makers (e.g., Hellenic Ministry of Digital Governance, Greece)** couldn't be kept away from the process. They were engaged in a series of discussions with the goal to proceed with the legal and policy framework that will accompany the service. The goal here was to bring up the privacy issues that arise when personal information is to be shared and how technology can close the gap between functionality and privacy in an efficient way.

GUnet has developed and launched eDiplomas.gr pilot service with the Ministry of Education and has presented the service and its development status to all Greek High Education Institutes in scheduled technical meetings. In addition, jointly with the Ministry of Digital Governance and the Ministry of Education, GUnet presented the eDiplomas solution to higher education institutions rectors, during two meetings held at Thessaloniki (21/10/2020) and Chania (5/11/2020).

As a key result of stakeholder engagement:

- the Greek legislation was extended to cover the use of digitally verifiable diplomas and diplomas information sharing, which was a prerequisite for the launch of the eDiplomas platform. While the legislation doesn't specify the explicit use of DLTs it touches upon citizen's privacy issues and establishes a digital alternative to exchanging diplomas data.
- four Greek High Education Institutes, covering more than 40% of the available 1st degree university diplomas, have already joined the digital diplomas service making available over 250K diploma titles to the general public.
- GUNet realized that academic stakeholders had concerns regarding the necessity of using DLTs but were able to refocus and find efficient methods to integrate their Students Information Systems with the eDiplomas platform and establish the necessary organizational changes and procedures to accommodate the data quality requirements of the service.

In the future, as far as the HEIs engagement is concerned in their role as diploma issuers, the goals include the expansion of the platform deployment across more Greek HEIs. Furthermore, GUnet will pursue collaborations with other technology companies in the private sector and research teams coming from its member Universities.

5.8 I.O. Research

As I.O. Research is building a solution (a prototype) for a decentralized software updates mechanism, which captures the lifecycle of a software update end-to-end -from the ideation phase to the activation on the main-chain- that is to be incorporated with the Cardano node software, it is natural that all their stakeholders are somehow related to the Cardano ecosystem. I.O Research has identified five major groups of stakeholders. The first group is the **Cardano product management team**, responsible for the Cardano line of products and especially for the main product which is the Cardano blockchain. Naturally, in order to leverage our PRIViLEDGE results for Cardano, we needed the consensus of the product team. The second group is the **Cardano Foundation**, a non-profit organization that provides custodial oversight to Cardano and strives to advance and support the global Cardano community through various inclusive programs and endeavours. The decentralization of Cardano governance is a main part of their work and thus, since I.O. Research PRIViLEDGE results are a significant piece in this decentralized governance puzzle, the Foundation was engaged early in the project. The third group of stakeholders is the **Cardano Treasury system research team**. The Treasury system is another piece of the Cardano decentralized governance landscape that solves the problem of proposal funding. Intuitively some software update proposals might require funding and so there needs to be some sort of "collaboration" between the software updates process and the Treasury process. The fourth group of stakeholders are the **Cardano blockchain developers** - engineers that maintain the Cardano code. Any new software update mechanism must go through them and thus it was deemed very important to engage with them especially for achieving the integration of the update mechanism into the Cardano node. Finally, the fifth group of stakeholders is the **broader Cardano community**. The latter are ada holders and stake pool operators that actively

participate in the network, but also Cardano enthusiasts in general, who have embraced the Cardano vision. These stakeholders eventually will become the end-user consumers of our work.

To engage with the above stakeholders I.O. Research initiated and carried out several activities. It should be noted that the Cardano future release's code-name is "Voltaire". Therefore, a "Voltaire task force" has been created with participants from all stakeholder groups and representatives of I.O Research's PRIViLEDGE team. This task force meets regularly and communicates via online channels to discuss all Voltaire related issues in detail. Moreover, another regular meeting has been established with the Cardano formal methods team. This is the team of engineers that design (using formal methods techniques) and do property-based testing on Cardano. This close collaboration with them has helped to adjust our solution to the Cardano node and design an effective integration architecture. In fact, the benefit has worked both ways since there have been significant improvements in the Cardano code-base due to this engagement. One notable example is the revision of the Cardano ledger layer to accommodate a pluggable software update mechanism. Finally, in order to engage with the broader Cardano community we have utilized participation in public blockchain events (e.g., Paris Blockchain Summit) and more focused on Cardano, we have presented our work in the yearly Cardano Summit event.

As a key result of stakeholder engagement I.O. Research:

- got confirmation that software updates in blockchain are hard but decentralized software updates are even harder.
- learned that decentralized governance is a very difficult problem and there is no silver bullet
- learned that the stake for a blockchain update system is incredibly high. You cannot afford to get this right.
- learned that it is important to identify all the distinct decisions one must make in the lifecycle of a software update and decide how to decentralise this process in each one.
- learned that decisions on software updates should go through a gradual refinement so that when one reaches activation, one really knows what will be activated and have the participant's consensus on that.
- learned that low participation in the software update protocol is potentially high risk.
- realised that the community embraces the Cardano vision for decentralized governance (a part of which are software updates)
- proved that the property-based testing techniques used for Cardano have been proven invaluable for validating our prototype.
- Concluded that the integration of the update mechanism into the Cardano node software should aim at a decoupled and modular ledger-layer/update system architecture.

In the future the primary goal for I.O. Research is to exploit the use-case's results into Cardano. I.O Research will continue their close engagement with all stakeholders to influence work done for the Cardano Voltaire release as much as possible. A successful decentralized governance story in Cardano will inevitably benefit the whole blockchain space, which is I.O Research's greatest aspiration.

6 Conclusions

The PRIViLEDGE's stakeholder engagement activities were on track throughout the project, even considering that during the last 1,5 years we had to conduct our engagement activities during COVID-19. This entailed a level of replanning our activities early 2020 to mitigate the risks and carry them out with maximum effort. Prevailing, we made great effort in reaching out to the project's stakeholders and use their feedback to evaluate our work.

During the lifespan of the project, we updated our website and social media regularly to inform all our audiences promptly about our regularly achieved milestones. The website was constantly updated and served as an essential vehicle to bring our results to both general audience and to our specific target groups and stakeholders. We used actively our internal and external networks to promote PRIViLEDGE and used the social media channels for the project to spread project related news.

What is more, we complemented the scientific literature with 24 publications, covering a variety of scientific publication types, with the attempt to make PRIViLEDGE results available for different types of academic audiences and readers interested in DLT privacy and security issues and DLT applications. We also dedicated 28 blog post to a general audience interested in cryptography and DLT related topics.

We took part at numerous events where we presented PRIViLEDGE results and had a chance to engage with our stakeholder. The four PRIViLEDGE workshops, each dedicated for a specific topic and stakeholder group, were especially important to establish new stakeholder relationships, have elaborate discussions and validate the achievements of the project.

To sum up, the PRIViLEDGE consortium was successful in building meaningful stakeholder relationships throughout the project and will utilize many established connections beyond the project as well. This was achieved through well-established communication practices and the overall transparency and accessibility of the project's results.