



DS-06-2017: Cybersecurity PPP: Cryptography


PRIViLEDGE
Privacy-Enhancing Cryptography in Distributed Ledgers

D5.3 – Exploitation Strategy and Roadmap

Due date of deliverable: 30 September 2018
Actual submission date: 21 September 2018

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

Lead contractor: Guardtime AS
Duration: 36 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	

D5.3

Exploitation Strategy and Roadmap

Editor

Björn Tackmann (IBM)

Contributors

Ahto Truu (Guardtime)
Toomas Krips (UT)
Michal Zajac (UT)
Michele Ciampi (UEDIN)
Berry Schoenmakers (TUE)
Ivan Visconti (UNISA)
Ivo Kubjas (SCCEIV)
Panos Louridas (GRNET)
Nikos Voutsinas (GUNET)
Peter Gaži (IOHK)

Reviewers

Luisa Siniscalchi (UNISA)
Mirjam Wester (IOHK)

21 September 2018
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.

The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

©Copyright by the PRIViLEDGE Consortium

Executive Summary

Blockchain and distributed ledger technologies (DLTs) have emerged as one of the most revolutionary developments in recent years, with the goal of eliminating centralised intermediaries and installing distributed trusted services. They facilitate trustworthy trades and exchanges over the Internet, power cryptocurrencies, ensure transparency for documents, and much more. This broad range of applications makes the market potential of DLTs substantial. While at the moment the monetarily most significant application of DLTs is in investment through cryptocurrencies and ICOs, other areas are expected to gain more importance in the future. Market analyses predict compound annual growth rates exceeding 80% in several areas such as insurances or supply-chain management.

PRIViLEDGE unites several European key players in cryptographic research and from the fintech and blockchain domains to realise cryptographic protocols supporting privacy, anonymity, and efficient decentralised consensus for DLTs. Such protocols will be needed for DLTs to support the above applications, and unlock the full market potential of DLTs. The expected importance of DLTs together with the need for advanced cryptographic solutions make them an attractive field both for academic institutions as well as innovative industry players.

This Deliverable 5.3 “Exploitation Strategy and Roadmap” describes the individual plans of the project partners for exploiting the project results, as well as a joint plan to create and use the exploitable assets outlined in the Description of Action. The plan ensures that the research results generated during PRIViLEDGE will benefit academic partners directly through, e.g., publications and teaching, but also that the protocols will be implemented in toolkits that can then be used by other partners as well as by the public. The toolkits will in particular help the industry partners in developing prototypes for their use case scenarios.

Contents

1	Introduction	1
1.1	Purpose of this Document and Relation to other Project Work	1
1.2	PRIViLEDGE Value Proposition	1
1.3	Exploitation Strategy of PRIViLEDGE	1
1.3.1	Strategy for the Industrial Partners	2
1.3.2	Strategy for the Academic Partners	3
1.4	Market Analysis and Outlook	4
2	Partner Exploitation Plans	6
2.1	Guardtime	6
2.1.1	Introduction	6
2.1.2	Exploitation Approach	6
2.1.3	Guardtime PRIViLEDGE Goals	6
2.1.4	Commercialisation	7
2.1.5	Economic Prospect of Success	7
2.2	IBM	7
2.2.1	Introduction	7
2.2.2	Exploitation Approach	8
2.2.3	IBM PRIViLEDGE Goals	8
2.2.4	Commercialisation	8
2.2.5	Economic Prospect of Success	8
2.3	University of Tartu	9
2.3.1	Introduction	9
2.3.2	Exploitation Approach	9
2.3.3	University of Tartu PRIViLEDGE Goals	9
2.3.4	Results	9
2.4	The University of Edinburgh	10
2.4.1	Introduction	10
2.4.2	Exploitation Approach	10
2.4.3	The University of Edinburgh PRIViLEDGE Goals	10
2.4.4	Results	10
2.5	Technical University of Eindhoven	10
2.5.1	Introduction	10
2.5.2	Exploitation Approach	11
2.5.3	Technical University of Eindhoven PRIViLEDGE Goals	11
2.5.4	Results	11
2.6	University of Salerno	11
2.6.1	Introduction	11
2.6.2	Exploitation Approach	11
2.6.3	University of Salerno PRIViLEDGE Goals	11
2.6.4	Results	12
2.7	Smartmatic-Cybernetica Centre of Excellence for Internet Voting	12
2.7.1	Introduction	12
2.7.2	Exploitation Approach	12
2.7.3	SCCEIV PRIViLEDGE Goals	12
2.7.4	Commercialisation	12
2.7.5	Economic Prospect of Success	13
2.8	Greek Research and Technology Network	13

D5.3 – Exploitation Strategy and Roadmap

2.8.1	Introduction	13
2.8.2	Exploitation Approach	13
2.8.3	GRNET PRIViLEDGE Goals	13
2.8.4	Commercialisation	14
2.8.5	Economic Prospect of Success	14
2.9	Greek Universities Network	14
2.9.1	Introduction	14
2.9.2	Exploitation Approach	14
2.9.3	GUnet PRIViLEDGE Goals	14
2.9.4	Commercialisation	15
2.9.5	Economic Prospect of Success	15
2.10	I.O.Research	15
2.10.1	Introduction	15
2.10.2	Exploitation Approach	15
2.10.3	I.O.Research PRIViLEDGE Goals	15
2.10.4	Commercialisation	16
2.10.5	Economic Prospect of Success	16
3	Joint Project Exploitation Strategy and Roadmap	16
3.1	Exploitable Assets	16
3.2	Active and Intended Direct Collaboration between Partners	18
4	Conclusion	18

1 Introduction

1.1 Purpose of this Document and Relation to other Project Work

The present document, Deliverable 5.3 “Exploitation Strategy and Roadmap”, aims at presenting the initial exploitation strategy and plans for the main results coming from the project PRIViLEDGE. All consortium partners contributed to this deliverable, expressing their exploitation interests according to their own organizations’ strategical interest. The document begins in Section 1 with a description of PRIViLEDGE’s value proposition and general exploitation approach, followed by an initial market analysis. Section 2 is dedicated to the individual exploitation plans of the project partners. Section 3 describes the collaborative exploitation approach of the partners. Section 4 concludes this document.

Deliverable 5.3 is part of the activities of WP5 “Communication, Dissemination, and Exploitation”. It is a public document which will be made available on the project website for those stakeholders interested in the PRIViLEDGE project. This document will be followed by Deliverable 5.5 “Report on Exploitation” toward the end of the project (M33).

1.2 PRIViLEDGE Value Proposition

Blockchain and distributed ledger technologies (DLTs) have emerged as one of the most revolutionary developments in recent years, with the goal of eliminating centralised intermediaries and installing distributed trusted services. They facilitate trustworthy trades and exchanges over the Internet, power cryptocurrencies, ensure transparency for documents, and much more.

Although based on cryptographic techniques at their core, the currently deployed DLTs do not address privacy. Indeed, the very idea of a public ledger that stores a verifiable record of transactions at first appears inherently incompatible with the privacy requirements of many potential applications, which handle sensitive data such as trade secrets and personal information. New cryptographic techniques and protocols are therefore needed to protect the data, facilitate these applications, and make DLTs deliver on their promises.

PRIViLEDGE realises cryptographic protocols supporting privacy, anonymity, and efficient decentralised consensus for DLTs. In PRIViLEDGE, several European key players in cryptographic research and from the fintech and blockchain domains unite to push the limits of cryptographic protocols for privacy and security. PRIViLEDGE encompasses research and design of cryptographic protocols as well as their implementation in toolkits that will be published by the project and made publicly available. The usefulness of these toolkits will be demonstrated through four ledger-based solutions: (1) verifiable online voting; (2) contract validation and execution for insurance; (3) university diploma record ledger; and (4) an update mechanism for stake-based ledgers.

The selected use cases are diverse and represent the principal application domains of DLT. They also promote the results of PRIViLEDGE, which ensures wide reach and impact of the developed techniques beyond the immediate scope of the project.

1.3 Exploitation Strategy of PRIViLEDGE

This section outlines the exploitation approach of PRIViLEDGE after the first year of the project. As detailed in the project proposal, the exploitation effort of PRIViLEDGE is targeted at potential users of DLT in industry and the public sector, and also addresses standardisation groups. PRIViLEDGE will provide a portfolio of tools for privacy-preserving operation of distributed ledgers, for different security goals. These tools will consist of a family of modular toolkits that will be demonstrated in the context of the technology prototypes that form the use cases. The toolkits will be targeted toward, and the prototypes will be based on, widely-used open-source DLT platforms. Together, the toolkits and prototypes yield a common PRIViLEDGE *framework*, which supports compatibility and interoperability among the tools and results.

Selected building blocks will be released under open-source licenses, which simplifies their bottom-up adoption. Through the dissemination and branding efforts taken by the project, the results are expected to receive wide-spread attention.

Strategy for exploitation. The goal of exploitation in PRIViLEDGE is to ensure the sustainability of the project's results beyond the project end and to demonstrate how PRIViLEDGE has influenced the EU landscape. Exploitation includes multiple forms:

1. *Financial exploitation*, building products, projects, or services based on the project results;
2. *Research & development*, by engaging new projects (EU-funded or sponsored by other sources), based on the experiences gained in the project;
3. *Education*, e.g. courses, at the university level or in continuing education, etc.;
4. *Community-building* around the topics of the project, raising awareness for the addressed problems and the proposed solutions;
5. *Knowledge transfer*, from academia to industry, by collaboration or via employees;
6. *Contributions to open-source projects and standardisation*; through publication of open-source toolkits and participation in relevant standardisation groups.

We have created the following exploitation strategy, in order to help each partner with formulating a specific exploitation plan. These respective plans will loosely be organized along the categories outlined in the strategy. We have two broad strategies, one oriented towards the industrial partners and one addressing more the academic partners. These categories act as a guideline for the exploitation plans of the partners and the project. The two strategies are based on the exploitation strategies developed and used in the predecessor projects TClouds¹ and ESCUDO-CLOUD².

1.3.1 Strategy for the Industrial Partners

General strategy

1. Focus on the main results from the project (products, services, ...) and their commercial viability.
2. Consider new business and operating models that become possible with the project for bringing the project results to customers. Explore the role of third parties (not participating in the project) in this scenario.
3. Identify drivers for a successful exploitation and consider how those drivers can be harnessed and strengthened.
4. If there are obstacles to a successful exploitation of the project from today's perspective, address them early on.
5. Put a strong focus on how European stakeholders can profit from the exploitation of the results.
6. Develop a timeline for exploitation, showing how the exploitation can be structured in phases. Identify the prospective time frame after the end of the project to bring the results to the market.
7. Identify concrete customer needs that are addressed with the solution and product, and describe ways to quantitatively measure the success.

¹<http://www.tclouds-project.eu/>

²<http://www.escudo-cloud.eu/>

D5.3 – Exploitation Strategy and Roadmap

8. Involve marketing, product-management, and sales departments early on in the process.
9. If possible, start exploitation of intermediate results already during the project.
10. Consider synergies for exploitation with other projects, possibly also funded ones.

Economic factors

1. Aim at a quick access to the market. If necessary, create new markets for a successful exploitation.
2. Address the market for exploitation today (market analysis, prognoses, technical developments).
3. Assess the competition for the developed results, in Europe and worldwide.
4. Provide innovation in project results, ensure there are advantages compared to competitors.

Scientific and technical goals

1. Assess the impact of general technological progress on the exploitation scenarios.
2. Pay attention to non-technical developments (legal aspects, privacy aspects, ...) and their influence on exploitation.

Intellectual property

1. Consider to protect intellectual property, for example, through patents.

1.3.2 Strategy for the Academic Partners

General strategy

1. Identify drivers for a successful exploitation and consider how those drivers can be harnessed and strengthened.
2. If there are obstacles to a successful exploitation of the project from today's perspective, address them early on.
3. Put a strong focus on how European stakeholders can profit from the exploitation of the results.
4. Develop a timeline for exploitation, showing how the exploitation can be structured in phases. Identify the prospective time frame after the end of the project to bring the results to the market.
5. Identify concrete customer needs that are addressed with the solution and product, and describe ways to quantitatively measure the success.
6. If possible, start exploitation of intermediate results already during the project.
7. Consider synergies for exploitation with other projects, possibly also funded ones.

Scientific and technical goals

1. Assess the impact of general technological progress on the exploitation scenarios.
2. Pay attention to non-technical developments (legal aspects, privacy aspects, ...) and their influence on exploitation.
3. Pay attention to the competition for the developed results, in Europe and worldwide.
4. Provide innovation in project results, ensure there are advantages compared to competitors.

Intellectual property

D5.3 – Exploitation Strategy and Roadmap

1. Consider to protect intellectual property, for example, through patents.

Academic impact and education

1. Offer seminars, lectures, lab-courses and the-like with topics related to the project. Let the results of the project influence and/or improve education and training.
2. Consider to exploit the research in the project for improving the contributions to European research, like building scientific communities, organizing or participating in workshops.
3. The project should help to attract new researchers and students.
4. Engage in improved dissemination activities through the project, for presenting work in conferences (industrial and academic), journals, and so on.
5. Explore new scientific communities or try to get into other, relevant communities.

Sustainability

1. Make the results of the work available as open-source.
2. Contribute results to established open-source projects.
3. Invest in maintaining the project results after the project ended.
4. Plan follow-up projects the build on the results.
5. Form new relations during the duration of the project and engage with new partners in future collaborations.
6. Exploit the project for acquiring new projects and further funding.

Technology transfer

1. Trigger interest in the industry for your project results.
2. Ensure that students gain valuable knowledge by their work in the project, which they will take to industry.

1.4 Market Analysis and Outlook

The advent of blockchain and distributed ledger technologies (DLTs) is widely viewed as one of the most disruptive recent developments in many economic areas. Through cryptography and distributed protocols, DLTs aim at replacing central trusted entities that exist in many markets, such as stock exchanges or interbank transaction systems, but also (re-)insurances or fiduciaries, by decentralized systems that are run between the market participants. DLTs are also viewed to have the potential of improving the efficiency of processes that involve multiple authorities and that nowadays still rely on a paper trail, including global trade or letter-of-credit-type schemes in the financial industry.

Today's widely used DLTs are mostly related to cryptocurrencies. The economic importance of each such cryptocurrency can be measured in different ways, such as its overall capitalisation or the transaction throughput per time period. According to CoinMarketCap.com, and at the time of writing, the market capitalisation of Bitcoin amounts to €109 billion, with a trade volume of €4 billion per day. The market capitalisation of Ethereum amounts to €35 billion, with a trade volume of €1.5 billion per day. Even smaller “top-ten” systems such as Cardano still have a market capitalisation of €2.8 billion, with a daily volume of €77 million.

Another recently growing scheme is that of an ICO, or Initial Coin Offering, in which a project or company offers a token managed on a distributed ledger—often Ethereum—to investors. The token then either represents stake in the company, or it is promised to later be redeemed for services offered by the project or company. ICOs are viewed by their proponents as a new and innovative way of funding projects, whereas they also face criticism

as they may be used as a way to bypass regulation or as a tool for money laundry. According to a recent study of PwC³, in 2017 a total of 552 ICOs raised a total volume of some \$7 billion. In the first half of 2018 alone, 537 ICOs raised a total volume of more than \$13.7 billion. The average size of an ICO is estimated at \$25.5 million, with the ICO of EOS alone raising \$4.1 billion.⁴

Several classes of DLT applications are not covered by the above numbers, as they do not involve publicly traded cryptocurrencies. For the overall market including those areas, Gartner⁵ predicts that “Blockchain’s business value-add will grow to slightly over \$360 billion by 2026, then surge to more than \$3.1 trillion by 2030”. In a study focused on the blockchain in insurance market,⁶ MarketsAndMarkets.com found that the market size was \$43 million in 2017 and is projected to reach \$1.4 billion in 2023, at a Compound Annual Growth Rate (CAGR) of 84.9%. The figures are roughly comparable in other fields; blockchain in supply chain had a market size of \$82 million in 2017, and is projected to reach \$3.3 billion in 2023, at a CAGR of 87%.⁷ The fintech blockchain market size was \$230 million in 2017, and is projected to grow up to \$6.2 billion in 2023, at a CAGR of 76%.⁸

The most widely used DLTs do not guarantee data privacy beyond pseudonymity of the user, including all of the top 10 cryptocurrencies today. As more and more transactions are shifted toward DLTs, this will need to change: For one, the European General Data Protection Regulation (GDPR) guarantees to all individuals control over their personally identifiable information, and mere pseudonymisation is not sufficient to evade the realm of GDPR. Furthermore, businesses will not be willing to store their confidential production data in public, when the blockchain applications become ready for productive use. And finally, recent data breaches such as the cases of Equifax or Facebook/Cambridge Analytica appear to slowly shift the public opinion toward becoming more privacy-sensitive. Therefore, before DLTs can serve the above-described use cases and unlock the economic potential, privacy-preserving technologies must be developed and implemented in order to protect the transaction data.

Given the above, it is important for the European information technology industry to keep up with the technological advances in order to stay in par with or even move ahead of the international competition. The PRIViLEDGE project partners have assembled a strong exploitation plan that describes how each of the partners will contribute to the exploitation of the PRIViLEDGE results. The individual plans are presented in Section 2, before Section 3 will outline the joint efforts of the consortium.

³ https://www.pwc.ch/de/press-room/press-releases/pwc_mm_icoreport_de.pdf

⁴ <https://cointelegraph.com/news/moment-of-truth-for-eos-whats-next-for-4-bln-eosio-following-launch-of-v10>

⁵ <https://www.gartner.com/smarterwithgartner/the-cio-s-guide-to-blockchain/>

⁶ <https://www.marketsandmarkets.com/Market-Reports/blockchain-in-insurance-market-9714723.html>

⁷ <https://www.marketsandmarkets.com/Market-Reports/blockchain-supply-chain-market-90851499.html>

⁸ <https://www.marketsandmarkets.com/Market-Reports/fintech-blockchain-market-38566589.html>

2 Partner Exploitation Plans

This section describes the individual exploitation plans of the project partners. The plans vary based on the type of organisation and their role in the project. The exploitation of academic partners focuses on publishing research results developed in the project and using the gained insights in teaching, further research, and student supervision. While industry partners also highlight the importance of collaborative research projects for ongoing employee education, they focus on exploiting the project results for their market offerings as well as the development of their products. As the individual exploitation plans of the partners differ considerably, each partner describes their individual plans in one of the following subsections.

2.1 Guardtime

2.1.1 Introduction

Guardtime is one of the world's leading providers of blockchain solutions. Founded in 2007 in Tallinn, Estonia, the company now has 200 employees in offices in Europe, Asia, and America.

Guardtime's core technology, the KSI blockchain, has been in production service since 2008, predating the well-known Bitcoin blockchain by a year. In contrast with the Bitcoin model, the KSI blockchain is a permissioned one. This allows for much faster voting-based consensus without the need for proof-of-work. The KSI blockchain is also based on the off-chain transaction model: instead of blocks of records themselves, only their aggregate hashes are registered on the blockchain. This means the size of the blockchain grows linearly in time, irrespective of the number of clients and their transaction rates.

The platform has found applications in the defence, government, telecommunications, insurance, financial, and manufacturing sectors. Key customers include DARPA, Lockheed Martin, Ernst & Young, Verizon, Ericsson, Maersk, and SICPA, as well as the governments of Estonia, UK, USA, and China.

2.1.2 Exploitation Approach

Guardtime's primary business model is co-operating with partners from market verticals to develop specialized value-added products and services on top of the KSI blockchain platform. The primary function of the KSI blockchain in these solutions is to provide independently verifiable proof of integrity and registration time of the underlying transaction records or other data assets.

However, in many applications some form of controlled data sharing is also desirable. As the KSI blockchain does not natively provide such facilities, integrations with other distributed ledger platforms and more flexible data sharing or joint computation models could complement the offering.

2.1.3 Guardtime PRIViLEDGE Goals

One of the KSI blockchain's main characteristics is strong privacy: the blockchain provides proof of time and integrity and attribution of origin, but no data sharing facilities. At the other end of the spectrum, represented by Bitcoin among others, all data is completely public. Guardtime's main interest in PRIViLEDGE is finding a middle ground between these extremes, as limited amount of data sharing in controlled fashion is required in many business applications.

In theory, several cryptographic solutions such as homomorphic encryption, zero-knowledge proofs, and authenticated data structures could provide more controlled access in verifiable manner. In particular, zero-knowledge proofs seem attractive, as they would allow sharing verifiable claims about data without exposing the data itself. However, currently available cryptographic solutions tend to have too high overhead for practical deployment. New primitives and protocols developed in PRIViLEDGE could move these techniques into commercial viability.

2.1.4 Commercialisation

In the nearest term, Guardtime expects the PRIViLEDGE outcomes to strengthen its offerings in the insurance sector, which is one of the demonstration use-cases in the project. In particular, the ability to either prove certain properties of bids and contracts without disclosing the underlying records themselves or selectively disclose parts of bids and contracts while keeping other parts confidential would bolster privacy of market participants without reducing trustworthiness of the process. However, the cryptographic techniques developed in PRIViLEDGE for those goals in the insurance use-case should be universal and thus applicable also in products and services for other verticals, most notably in the healthcare sector, in future developments.

2.1.5 Economic Prospect of Success

In the shorter term, the improved cryptographic tools developed in PRIViLEDGE are expected to bolster Guardtime's product portfolio in several privacy-conscious verticals. In the longer term the improved products and services should translate to overall increase of efficiency of business in these fields. Currently the primary advantages of the KSI blockchain over competing proposals are fast transaction finalization time (about one second on average) and low storage requirements of the main blockchain (about 2 GB per year). In order to maintain those properties, the computational efficiency of the added cryptographic primitives and protocols is of paramount importance.

2.2 IBM

2.2.1 Introduction

IBM is a globally integrated technology and consulting company headquartered in Armonk, New York. With operations in more than 170 countries, IBM attracts and retains some of the world's most talented people to help solve problems and provide an edge for businesses, governments and non-profits. Innovation is at the core of IBM's strategy. The company develops and sells software and systems hardware and a broad range of infrastructure, cloud and consulting services.

IBM Research – Zurich is one IBM's 12 research centres around the globe. This network of some 3000 scientists is one of the largest industrial IT research organisations in the world. The Zurich laboratory was established in 1956 and is home to world-class scientists representing more than 45 nationalities. Cutting-edge research and outstanding scientific achievements—most notably two Nobel Prizes—are associated with this lab. The spectrum of research activities range from exploratory research in nanoscience and -technology for future computing, to cloud and computing infrastructure, security and privacy, computational sciences, data analytics and cognitive computing. The *industry platforms and blockchain* research group at IBM Research – Zurich focuses on research and development of distributed ledger technologies for the enterprise scenario.

IBM has been a founding member of Hyperledger⁹, an organization of the Linux Foundation. IBM has contributed significantly and continuously to Hyperledger Fabric¹⁰, an advanced permissioned DLT platform developed in the context of Hyperledger. IBM continues to drive the development of Fabric, offers hosting managed platforms as a service, and also uses it as a platform in service offerings to clients. IBM also participates on other DLT-related efforts, such as the Sovrin self-sovereign identity network¹¹ or the Mobility Open Blockchain Initiative¹².

⁹<https://hyperledger.org/>

¹⁰<https://www.hyperledger.org/projects/fabric/>

¹¹<https://sovrin.org/>

¹²<https://www.dlt.mobi/>

2.2.2 Exploitation Approach

IBM offers multiple services in the context of DLT, most of which are built around the open-source Fabric project. First, the IBM Blockchain Platform¹³ is a service in which blockchain nodes are hosted in highly secure infrastructure. Then, IBM also collaborates with different business partners to build actual trade networks, such as with Walmart¹⁴ or Maersk¹⁵, with the aim of benefitting from the economic success of these ecosystems through fees earned by running the platform. Furthermore, IBM also offers the development of DLT-based platforms for specific use cases as a service to clients.

2.2.3 IBM PRIViLEDGE Goals

IBM participates in PRIViLEDGE to perform research and development tasks with the goal of advancing distributed ledger technologies, focused on, but not restricted to, the open-source platform Fabric. The two topics that IBM targets within PRIViLEDGE are flexible consensus and privacy of transactions. The importance of flexible consensus stems from the necessity of adapting DLT platforms to different use cases; the consensus mechanism represents one of the main trust assumptions of the platform, and a general-purpose platform such as Fabric must be adaptable to different scenarios, while delivering great performance in each of them. Transaction privacy is important for different reasons; one is that the confidentiality of business data requires to manage the visibility of data on a need-to-know basis, different from today's prevalent platforms that either store the data in clear (e.g., Bitcoin, Ethereum) or shield the data from everyone (e.g., ZCash). Another one is that service providers that leverage DLTs still have to comply with regulations such as GDPR, and proper cryptographic mechanisms will be needed to achieve this requirement. IBM's goal in PRIViLEDGE is to advance the Fabric open-source platform in order to support these requirements.

2.2.4 Commercialisation

IBM's main exploitation route of PRIViLEDGE results is via integration of new technologies into Fabric. As many of IBM's blockchain-related offerings build on Fabric, the outcomes of PRIViLEDGE are expected to be instrumental for this area of IBM's business. The IBM Blockchain Platform integrates new features from Fabric and offers them to clients hosting their nodes with IBM. Improved technology and features in Fabric also help IBM in developing DLT networks that fulfill the needs of trade ecosystems as well as individual clients.

2.2.5 Economic Prospect of Success

Distributed ledger technologies are expected to be a disruptive technology in different markets, from Finance through Supply Chain Management to Mobility, improving the efficiency of the markets by shifting from trusted mediators to secure decentralised technologies. IBM has been among the first major companies to understand and respond to this shift, and is today widely seen as a technology leader in the area.¹⁶ Advancing the Fabric platform that underlies many of IBM's services will allow IBM to secure this role, and to benefit from it by offering a variety of DLT-related services to companies in these markets.

From the beginning, IBM's strategy in the DLT area has been driven by the conviction that the blockchain platforms must be open source, in order to allow all participants of an ecosystem to understand and verify the correctness and security of the implemented protocols and mechanisms. This conviction has led to the contribution of the initial Fabric implementation to Hyperledger, and is also reflected in IBM's ongoing contribution to the Fabric open-source platform. IBM's commitment to the open-source idea also ensures that the outcomes

¹³<https://www.ibm.com/blockchain/platform>

¹⁴<https://www.forbes.com/sites/rogeraitken/2017/12/14/ibm-walmart-launching-blockchain-food-safety-alliance-in-china-with-fortune-500s-jd-com/#2ba380d07d9c>

¹⁵<https://www.ibm.com/blogs/think/2018/01/maersk-blockchain/>

¹⁶<https://www.juniperresearch.com/press/press-releases/ibm-ranked-no-1-blockchain-technology-leader>

of PRIViLEDGE will not only be exploited in the context of IBM projects, but will also be readily available for other organizations that build their products and services on the Fabric platform.

2.3 University of Tartu

2.3.1 Introduction

University of Tartu is an academic partner in PRIViLEDGE. At the University of Tartu, Helger Lipmaa leads a cryptography research group that studies the security and privacy-related questions of the project. It employs researchers Michał Zając and Toomas Krips and a number of PhD students. It plans to hire more researchers (with a doctoral degree) to work on the project. UT, as an academic partner, is focused primarily on research and teaching.

For the last 3 years, UT has been a partner in another Horizon 2020 project PANORAMIX, where it provides and builds know-how on privacy preserving technologies in mix-nets. UT will use some outcomes from PANORAMIX to develop new results related to PRIViLEDGE.

2.3.2 Exploitation Approach

UT is an academic, non-profit partner in PRIViLEDGE, and thus does not aim to obtain monetary gains from it. However, the project still promises certain benefits to UT. As a university, its main exploitation is the use of the project to do research, supervision and teaching in the area of privacy and ledgers.

UT will share awareness of DLTs and their fundamental privacy-related problems by organising seminars and providing a course on distributed systems, blockchain and the cryptography used therein. The course, “Distributed systems and blockchain”, will be given by Helger Lipmaa and directed to master and PhD students of computer science¹⁷. UT plans to exploit the project to establish persistent and stable scientific cooperation with other PRIViLEDGE partners, especially academic ones like the University of Edinburgh and University of Salerno. UT will offer consultancy services for companies and governmental entities planning to use DLT, yet lacking deep understanding of their security and privacy aspects. UT also considers other exploitation avenues like co-founding start-ups oriented on security and privacy in DLT. Such approaches are possible but not primary.

2.3.3 University of Tartu PRIViLEDGE Goals

UT will conduct research and publish peer-reviewed articles related to the topics of distributed ledgers and blockchain. The primary objective is to perform background research and provide know-how necessary for developing cryptographic protocols needed for WP3. As mentioned, UT will also provide a privacy and DLT-related course for students and including the course in the curriculum will hopefully make students interested in research in the related areas. To establish scientific cooperation with other partners UT would like to publish at least one article with co-authors from other PRIViLEDGE partners. Finally, UT will call exploitation successful if it manages to establish a stable environment for security and DLT research, by e.g. creating a group of cryptographic researchers and building its position as DLT-experts by publishing articles in renowned venues such as CRYPTO, Eurocrypt, Asiacrypt, Public-Key Cryptography, Financial Cryptography, CT-RSA, IEEE S& P, and ACM CCS.

2.3.4 Results

UT plans to do conduct research and publish the results, run courses, seminars, and workshops. It will collaborate with partners in order to achieve these goals, esp. academic ones like University of Salerno. UT expects several PhD defenses on related topics. All results obtained by UT will be available publicly and in open access.

¹⁷Course webpage <https://courses.cs.ut.ee/2018/infsec/spring/Main/Blockchain>.

2.4 The University of Edinburgh

2.4.1 Introduction

At The University of Edinburgh, PRIViLEDGE employs primary investigator Prof. Aggelos Kiayias and one researcher Dr. Michele Ciampi and there are plans to hire a second researcher in years 2-3.

The Blockchain Technology Laboratory (BTL)¹⁸ is part of School of Informatics and is led by Professor Aggelos Kiayias. BLT brings together academics from various disciplines and students from undergraduate to PhD level to explore the many open and wide challenges presented by blockchain systems. The areas for study bridge cryptography, algorithms, game theory, economics, regulation and compliance, business, and law. In this laboratory a number of research projects ran in parallel with high degree of synergy to PRIViLEDGE.

2.4.2 Exploitation Approach

As public institutions of higher education UEDIN is a non-profit organization that will not perform commercial exploitation of the project's results. Nevertheless, the partner has significant benefits to reap from the project results that we outline below.

The project team will incorporate material and research results of the project in courses related to the topic of the project. Among these are, most importantly, the Blockchains and Distributed Ledgers course (INFR11144), the Computer Security course (INFR10067) and the Introduction to Modern Cryptography course (INFR11131). The results of the project will enhance the course curriculums with new research and blockchain test beds for the students to experiment and will improve the training provided bringing it up to par with the current state of the art.

2.4.3 The University of Edinburgh PRIViLEDGE Goals

The results will be combined with software for e-voting which was developed by the team with previous funding from H2020 project PANORAMIX and the project DEMOS of the Greek secretariat of research and technology. The system is called Demos¹⁹, and the combination with PRIViLEDGE will greatly enhance the system's verifiability as the system's security relies on a public bulletin board. Our objective is to roll out this system as a blockchain based service for UEDIN students during the course. The project also provides valuable professional training for the researchers involved and will enable them to substantially broaden their command of distributed ledger technologies. The University of Edinburgh expects, as an outcome of this training, several publications in the top cryptographic and security venues such as CRYPTO, Eurocrypt, Asiacrypt, Public-Key Cryptography, Financial Cryptography, CT-RSA, IEEE S& P, and ACM CCS.

2.4.4 Results

Another goal is the deployment of the results of WP2 and WP3 in collaboration with industry partner IOHK with which UEDIN has a long standing collaboration via its Blockchain Technology Laboratory. This will enhance the research outputs of UEDIN in the blockchain space and buttress collaborations with other prospective industry partners.

2.5 Technical University of Eindhoven

2.5.1 Introduction

The Technical University of Eindhoven takes part in several activities that involve DLT. These include various research projects as well as some teaching activities, e.g., the course *Seminar System Architecture and Networking* will focus this year on a hands-on programming assignment using blockchains.

¹⁸<https://www.ed.ac.uk/informatics/blockchain>

¹⁹<http://www.demos-voting.org/>

2.5.2 Exploitation Approach

The Technical University of Eindhoven does not seek direct revenue from its activities surrounding DLT. Indirectly, the research and teaching activities contribute to the economic viability of the university though.

2.5.3 Technical University of Eindhoven PRIViLEDGE Goals

The goals for the Technical University of Eindhoven in PRIViLEDGE are to extend its scientific knowledge in the DLT domain, building on the existing cryptography expertise. In particular, the goal is to study the use of secure multiparty computation in the context of DLT. Advanced research results will be submitted to top-tier conferences and workshops in cryptography (mostly organized by IACR, ACM, and IEEE). Basic research results may also be integrated in advanced crypto courses taught at the TUE graduate school (master level) to keep these courses up-to-date with modern technology (e.g., in the course *Applied Cryptography*).

2.5.4 Results

Overall, the Technical University of Eindhoven seeks results in PRIViLEDGE that enhance its portfolio in privacy-protecting cryptographic protocols. Applications of secure multiparty computation with stronger security properties due to the use of DLT (e.g., by committing the inputs and outputs for secure computations using DLT) are of prime interest. Extending the MPyC²⁰ framework with such DLT links is an example of a concrete result.

Additionally, the Technical University of Eindhoven wants to strengthen its position as a knowledge partner in DLT, also at the national level within the Netherlands (through its partnership in the Dutch Blockchain Coalition²¹).

2.6 University of Salerno

2.6.1 Introduction

As an academic partner, University of Salerno is mainly interested in research and teaching. In this respect, PRIViLEDGE plays an important role for investing resources in DLT that is a cutting-edge research topic. Moreover there is a clear benefit for students that have a chance to be in touch with PRIViLEDGE through various classes that at least in part focus on cryptography. University of Salerno has contributed in the past to the design of several privacy-enhancing cryptographic primitives and protocols and this is a core component for the activities of PRIViLEDGE.

2.6.2 Exploitation Approach

Unfortunately, DLT has produced only a marginal impact on research activities in Italy so far. University of Salerno through PRIViLEDGE aims at disseminating the importance of DLT playing the role of a competence center and becoming a major academic partner for industrial projects focusing on privacy-enhancing DLT.

2.6.3 University of Salerno PRIViLEDGE Goals

University of Salerno aims at producing important research results on privacy-enhancing DLT. Moreover University of Salerno expects high visibility for the produced results through invited talks and participation and organization of panels, workshops and conferences. Last but not least, University of Salerno aims at starting joint projects with public or private organizations focusing on privacy-enhancing DLT. University of Salerno expects several publications from its members on important research results on privacy-enhancing DLT in top

²⁰<https://github.com/lshoe/mpyc>

²¹<https://www.dutchdigitaldelta.nl/en/blockchain>

cryptographic and security venues such as CRYPTO, Eurocrypt, Asiacrypt, Public-Key Cryptography, Financial Cryptography, CT-RSA, IEEE S& P, and ACM CCS. Moreover University of Salerno expects solid partnerships with industry and public institution.

2.6.4 Results

University of Salerno will obtain and publish scientific results, will offer courses and seminars on privacy-enhancing DLT and will expand its network of collaborations with universities and industries.

2.7 Smartmatic-Cybernetica Centre of Excellence for Internet Voting

2.7.1 Introduction

Smartmatic-Cybernetica Centre of Excellence for Internet Voting (SCCEIV) provides technology for online voting and hosts the online channel of the elections as a service. SCCEIV is a joint venture between Smartmatic, an established leader in automation of elections, and Cybernetica, the provider of online voting in Estonia since its implementation in 2005.

SCCEIV has been using distributed consensus-based storage for nation-wide elections on its IVXV platform since 2017²² and due to the success in real-life scenarios is looking for even tighter integration of online voting platform with distributed ledger technologies. SCCEIV flagship product Tivi²³ currently uses DLT for storing the submitted votes and verifying their availability.

2.7.2 Exploitation Approach

SCCEIV is planning to use DLT for being able to provide additional services and to increase the existing product line offered to potential customers. Namely, SCCEIV is looking into a possibility of offering hosting online voting services on a regular basis to private and public customers. In this approach, SCCEIV handles all the technical matters and requiring the potential customer to only set up basic information as electorate list, constituency list, choice list and any visual customisation. To prevent SCCEIV from being a trusted party, the goal is to use DLT which forces transparency and allows the customer to verify platform operations.

The second approach is to provide the election management platform as a product to public entities where local regulations require the local election bodies to provide commercial election services.

2.7.3 SCCEIV PRIViLEDGE Goals

SCCEIV as an industrial partner in PRIViLEDGE provides use-cases to the partners for constructing DLTs and implements a working prototype of an online voting platform using improved DLTs. In addition of the main goal of implementing an online voting platform prototype using DLT, SCCEIV also wishes to understand further uses and potential future developments of DLTs.

Regarding DLTs, SCCEIV expects distributed ledger technologies to provide additional transparency to on-line voting as a critical service. This means, that the voters and verifiers should be able to check that the software is working as expected. Additionally, SCCEIV expects the outcomes of the PRIViLEDGE to be more efficient in performance compared to the current solutions, allowing to run elections with millions of voters.

2.7.4 Commercialisation

The expected outcomes of PRIViLEDGE will lead to added services and products in the product line. This allows hosting many concurrent elections with the same resources while increasing the transparency. Furthermore, new products in the product line allows SCCEIV to take part in procurements and increase interest with current

²²<https://www.valimised.ee/sites/default/files/uploads/eh/IVXV-arhitektuur.pdf>

²³<https://tivi.io>

and future customers. Finally, being a member of PRIViLEDGE reinforces SCCEIV's image as a novel and transparent online election services provider.

2.7.5 Economic Prospect of Success

SCCEIV considers that distributed ledger technologies allows it to expand into new market of small- and medium-scale public and private election as a service. With the addition of new products, SCCEIV also looks forward to developments in emerging markets and being responsive in these markets. We also consider the general economic savings as a result of implementing online voting in elections due to the voters spending less time in taking part of democratic processes.

2.8 Greek Research and Technology Network

2.8.1 Introduction

GRNET's mission, when it was founded about 20 years ago, was to provide networking services to the Greek academic community, connecting universities and research centres in Greece within the country and with the rest of the world. With the infrastructure being put in place, GRNET expanded its services to grid, and then cloud computing. It now operates three data centres in Greece, allowing researchers, students, and academics, to tap into its Infrastructure as a Service offerings.

On top of the networking and computing infrastructure, GRNET has been designing, implementing, and operating integrated service solutions, like, for instance, the Zeus e-voting platform²⁴, teleconferencing services, and big data processing frameworks, among others. Lately, GRNET has embarked on leveraging recent technological developments such as DLTs, viewing them as a vehicle for end-user services for the academic community and beyond.

2.8.2 Exploitation Approach

GRNET's services are offered for free for academic and research use. Its involvement in DLTs is primarily focused on creating and delivering services that use these technologies for the benefit of its users. It also plans to use the experience gained from its involvement with DLTs to further the adoption of these technologies in Greece, in the academic community as well as the public sector.

GRNET has excellent links with research centres and universities throughout the country and the rest of Europe. These will be the foundation for the exploitation of the results of PRIViLEDGE, by using the technological know-how gained from the project to foster further collaborations as well as implementing and delivering production DLT services in Greece.

2.8.3 GRNET PRIViLEDGE Goals

GRNET is not a research organisation, but an organisation offering services to researches. The services must be of production-level quality, not proof of concepts. GRNET will use PRIViLEDGE in order to gain technological know how for the design and implementation of production-level DLT services. This includes:

- Investigation of different DLT frameworks and platforms, in relation to the requirements derived from WP1 of PRIViLEDGE.
- Investigation of different DLT smart contract approaches and languages.
- Integration of strong cryptographic protocols with DLT platforms.

²⁴<https://zeus.grnet.gr>

D5.3 – Exploitation Strategy and Roadmap

- Storage solutions for data in DLT (specifically, the trade-offs between storing in the blockchain vs. storing outside the blockchain).
- Ease of installation, deployment, and upgrades of DLT services.

2.8.4 Commercialisation

Following the above, commercialisation is not the main focus of GRNET's exploitation efforts. GRNET will instead use the results of PRIViLEDGE as an enabler for delivering production-level DLT services. Such services can be of commercial interest to others participating in them—for instance, certification and notarisation services may be of commercial interest to certification and notarisation entities. GRNET will investigate such applications with interested parties.

2.8.5 Economic Prospect of Success

While commercialisation is not the primary focus of GRNET, the economics of proposed DLT services are very important. In particular, any solutions involving DLTs must be more efficient, from an economics point of view, than other solutions using traditional technologies. That means that the resources that will be required for delivering the GRNET DLT services, in particular, the certification of university diplomas, which is the use case in which GRNET takes part, should be less than the resources required for delivering a solution with similar functionality using other technologies.

2.9 Greek Universities Network

2.9.1 Introduction

GUnet's primary goal is the development and provision of advanced network services and applications to the Greek Higher Education and Academic Institutions. One key category of GUnet's solutions consists of applications that act as a mediator of data and services that reside on authoritative systems distributed across all institutions. The services developed on the basis of those solutions target either the participant institutions and the academic community itself or third parties, with the public sector being the most notable case. In all these cases, where data and services cross the boundaries of the home organization, security, privacy and trust come at the top of the agenda. In this framework GUnet is exploring DLTs with plans to refactor existing services or build new ones that will take advantage of DLTs strengths.

2.9.2 Exploitation Approach

GUnet's exploitation plan is organized across two pillars. The first one is the development of know-how in the field of DLTs and stay ahead of technology shifts. The acquired knowledge will be used in the design and development of its own solutions and at the same time it will be diffused to all its member institutions of Higher Education. The second one is the evaluation of the outcome of the diploma's registry use case towards implementing a corresponding service for all Higher Education institutions of Greece.

2.9.3 GUnet PRIViLEDGE Goals

GUnet's main goal from PRIViLEDGE is to stress the underlying blockchain technologies and early identifying its strengths, limitations and applicability in real world scenarios. Namely GUnet will focus in the performance aspects of the technology, the functionality limitations that might occur and the comparison of DLTs with other technologies in terms of efficiency for use in services that involve Student Information Systems. GUnet's secondary goal is the establishment of the APIs that will connect the Student Informations Systems where diplomas records are initialized and the application layer of the diplomas registry.

2.9.4 Commercialisation

There is no commercialization plan in the strict sense. However, GUnet has a long history of offering complete software products—with no price-point attached to them—which are being widely used in production environments by educational organizations and other 3rd parties. Therefore GUnet’s goal is to invest further in the use of DLTs, using and expanding on the results of PRIViLEDGE, towards productizing the use case of diplomas registry and include it in the portfolio of platforms available to its members.

2.9.5 Economic Prospect of Success

Being a non profit company GUnet is not looking for creating a new revenue stream using the results of PRIViLEDGE. The benefits from PRIViLEDGE results will come from the fact that the anticipated impact of DLTs in the field of Higher Education is expected to fundamentally transform some of GUnet’s existing services and create opportunities for new ones.

2.10 I.O.Research

2.10.1 Introduction

I.O.Research is a European subsidiary of Input Output Hong Kong (IOHK). IOHK is an international research and engineering company focused on blockchain protocol design and development. It is a leader in the blockchain sector and develops blockchains and cryptocurrencies for government entities, research institutions and private corporations. IOHK plays a central role in the technical development of the Cardano blockchain, currently the largest public proof-of-stake blockchain by market capitalisation.

The vision for I.O.Research is to be a leading institution in the academic study of blockchain and to establish a reputation for tackling difficult research questions and for building a strong foundation in the blockchain industry. The business goals of I.O.Research match those of IOHK.

2.10.2 Exploitation Approach

As a research division, I.O.Research greatly benefits from maintaining and extending the technical expertise of its employees and in-house researchers. This is in particular true given the extremely quick development in the novel field of Distributed Ledger Technologies.

The participation of I.O.Research in PRIViLEDGE will allow the company to keep up-to-date with the latest research findings, contribute to them, and apply them in the development of IOHK’s products. It also provides a stage to foster the existing research collaboration between I.O.Research and the Blockchain Technology Laboratory at University of Edinburgh, which also participates in PRIViLEDGE.

2.10.3 I.O.Research PRIViLEDGE Goals

I.O.Research expects the PRIViLEDGE project to contribute, in accordance with the project’s goals, to a better general understanding of the methods for maintaining privacy on a decentralized ledger, as well as methods for secure updating of the ledger protocol. The hope of I.O.Research is that these methods will be (directly or indirectly) applicable to the Cardano blockchain maintained by IOHK, as well as other DLT projects that IOHK is involved in.

Both of these problems are highly relevant in the context of permissionless blockchain systems. While there exist several deployed permissionless blockchains providing some privacy guarantees to its users, none of these uses proof of stake as its underlying consensus mechanism. The reason is that the combination of privacy-preserving constructions and stake-based consensus (where the stake is recorded on the privacy-preserving ledger itself) introduces additional technical challenges. I.O.Research hopes to benefit from the research performed in the course of the PRIViLEDGE project when addressing these challenges for Cardano.

2.10.4 Commercialisation

I.O.Research expects that given the above-described research outcomes, their implementation in the Cardano blockchain by IOHK may provide a competitive advantage to the project, increasing its commercial success. This expectation is based on the current understanding that both privacy-supporting features, as well as a secure update mechanism, are seen as important (and often missing) aspects of existing projects in the cryptocurrency space.

2.10.5 Economic Prospect of Success

A measure of the economic success of the Cardano blockchain (which can be supported by the outcomes of the PRIViLEDGE project) will be the rate of adoption of the underlying cryptocurrency ADA by broader public.

3 Joint Project Exploitation Strategy and Roadmap

This section describes the PRIViLEDGE approach to joint exploitation of the project results. The first avenue of joint exploitation is through the explicit results of the project. The foundational research results on security properties and models will feed into the following research on schemes and protocols by the same or other partners. Schemes and protocols will then be implemented in toolkits that will be made available to all project partners and also publicly. The toolkits will in turn be used by the use case prototypes implemented in the project. The second avenue is through direct collaboration of project partners during the course of the project.

3.1 Exploitable Assets

The project will develop several toolkits that are relevant for the project use cases and beyond. These toolkits have been listed in the project proposal and are described in more detail here.

Cryptographic protocols for anonymous authentication (IBM): A distributed ledger system must ensure that only authorised parties can initiate transactions. In permissionless ledgers for cryptocurrencies, a transaction must be authorised by the key(s) controlling the assets used as an input to a transaction. In permissioned systems, this is often achieved by checking the authorisation of the registered identity of the transaction initiator. The authorisation must be publicly verifiable and is therefore stored on the ledger. One attempt to still preserve privacy is to use authentication schemes based on non-interactive zero-knowledge proofs, such as those used in Identity Mixer²⁵. The toolkit developed in the course of PRIViLEDGE will be based on research performed in WP2 and improve the privacy-preserving authorisation of transactions in the open-source Hyperledger Fabric platform, with the aim of including the developed code as part of the standard distribution of the platform.

Toolkit for flexible consensus protocols in Hyperledger Fabric (IBM): A core component of any distributed ledger platform is the consensus protocol that allows the nodes to agree on an order of the transactions recorded on the ledger. The consensus protocol must be chosen to suit the trust assumptions that the participants of the ledger system are willing to make. Since these trust assumptions may well differ between use cases, several ledger platforms such as Hyperledger Fabric or Corda support multiple consensus protocols. At the moment, the production release of Fabric only supports centralised or crash-fault tolerant consensus. Other consensus methods such as Byzantine-fault tolerant (BFT) consensus, BFT consensus with flexible quorums as in Ripple or Stellar, or stake-based consensus each represent trust assumptions relevant in different use cases. The toolkit developed in the course of PRIViLEDGE will be based on research on consensus methods performed in WP3 and extend Fabric's consensus mechanism, focusing on the flexible-quorum-type of BFT consensus. The aim is to make it available as open source and evaluate an inclusion in the standard Fabric distribution.

²⁵https://www.zurich.ibm.com/identity_mixer/

Toolkit implementing post-quantum secure protocols for distributed ledgers (Guardtime): Most existing ledger platforms make extensive use of public-key cryptography. Much of it, in particular digital signature schemes whose security rests on the difficulty of the discrete logarithm problem, will become irreparably insecure with the advent of universal quantum computers. The long-term evidentiary value of KSI signatures, on the other hand, depends only on properties of cryptographic hash functions, which are believed to be much more resilient to quantum adversaries. With that in mind, the ability to make calls from other ledger platforms to the KSI blockchain might be a desirable feature. To test this approach in practice, PRIViLEDGE will provide an integration toolkit allowing users of Hyperledger Fabric easier access to the KSI service. KSI signatures provide proof of integrity and signing time, and will be able to indemnify the current state of data against future quantum adversaries. They also provide forward-secure attribution of origin, but lack non-repudiation properties. To amend that, Guardtime is developing the BLT signature scheme²⁶ which is also fully hash-function based. Thus, BLT could be a viable replacement to the elliptic curve based signature schemes to keep the ledgers going in the post-quantum era as well.

Toolkit for zero-knowledge proofs for ledgers (UT): Although some distributed ledgers, like Zerocash, use zero-knowledge proofs to provide, e.g. anonymity of transactions, none of them allow for this cryptographic primitive to be used for more complicated ledger operations. Lack of ledger-executable zero-knowledge proofs is notably pinching in smart contracts. Currently, no distributed ledger offers the option to use zero knowledge to provide privacy of a contract – that is, all ledger users must know the contract rules and conditions required for its execution. The toolkit developed during PRIViLEDGE will include various zero-knowledge proofs that secures privacy of advanced ledger operations. Among the proofs, zk-SNARKs will be emphasized as a primitive of great efficiency.

Toolkit for ledger-oriented secure two/multi-party computation (UNISA): The power of secure multi-party computation is only partially exploited by Hyperledger Fabric and this generates in turn various functional and security limitations. For example in Hyperledger Fabric a chaincode (i.e., a smart contract) must be deterministic simply because the execution of a chaincode must be identically replicated. Obviously with such a limitation many natural applications of the distributed ledger technology (e.g., a public draw, a raffle, a card game) are problematic to implement in Hyperledger Fabric. The toolkit developed in the course of PRIViLEDGE will show how to use secure two/multi-party computation for some interesting functionalities in order to improve the security and the features of Hyperledger Fabric. The aim is to make the toolkit available as open source.

Toolkit for privacy-preserving applications on top of ledger technology (GRNET): Privacy-preserving applications require strong cryptographic protocols. Their implementation requires deep software engineering experience, as well as expert cryptographic knowledge. GRNET will leverage the cryptographic knowledge of the research partners and will capitalise on its own long engineering experience to develop a toolkit which programmers will be able to use in order to develop and deploy their own privacy-preserving services on ledgers. The toolkit will include both server-side and client-side libraries, to facilitate the development and the integration of front-end and back-end DLT applications.

The project will furthermore produce solutions for four use cases as described in the project proposal. These use cases are based on business needs of the respective use case partners. The use cases will also take up PRIViLEDGE results in the form of research results and toolkits.

Verifiable online voting with ledgers (SCCEIV): SCCEIV will develop a prototype of online voting platform which uses DLT for storing the ballots in an immutable way. The platform will make use of the distributed nature of DLT to remove the need for trusting the service provider completely. In addition, the prototype will use currently known best practices in voting protocols as individual and universal verifiability, mixnets

²⁶Named after the inventors: Ahto Buldas, Risto Laanoja, Ahto Truu

and zero-knowledge proofs. This prototype would be a basis for an Election-as-a-Service (EaaS) platform and as an independent product offered to the customers.

Distributed ledger for insurance (Guardtime): Guardtime and Ernst & Young, in co-operation with Maersk and a number of insurance partners, have developed and deployed a blockchain-backed platform to support marine insurance applications.²⁷ However, the offering could be more attractive to more market participants with more flexible privacy options. Bidding on insurance contracts is a highly competitive activity and neither insurers nor buyers want to disclose more data than is required to close the deal. On the other hand, lack of shared view of the coverage conditions is the leading cause of delays in claims processing, and distributed ledger technologies have the potential to tremendously decrease processing times and associated costs.

University diploma record ledger (GRNET/GUNET): GRNET and GUNET will provide a DLT service for the certification of university degrees. The technology that will be used for implementing the diploma record ledger, however, will be of much broader application. It will be general enough so that it will be straightforward to develop other notarisation and certification services on top of it. In this way, the university diploma record ledger will function as an example and reference application of the technologies that will be available for use for certification and notarisation services beyond the end of the project.

Cardano stake-based ledger (IOHK): IOHK will develop a general framework for software updates in ledger systems and then will develop a prototype for use by the Cardano ledger. The prototype will allow any participant (with sufficient stake) of the Cardano ledger to make update proposals and have a vote on them, and will orchestrate an efficient and secure deployment of successful proposals. The mechanisms for handling proposals, voting and deployment of updates will leverage the built-in consensus mechanism of the blockchain itself.

3.2 Active and Intended Direct Collaboration between Partners

Beyond the exploitation of the concrete and tangible project outcomes described in Section 3.1, PRIViLEDGE also benefits the project partners by fostering ongoing and long-term collaboration. Such collaborations often even outlast the immediate timeframe of the project, leading to further joint project applications or research. We therefore also consider ongoing or intended direct collaborations between partners as results of the project.

University of Edinburgh and University of Salerno are actively collaborating on new efficient constructions of non-interactive zero-knowledge argument systems. IBM and University of Salerno are starting a collaboration on researching privacy-preserving mechanisms in the context of Hyperledger Fabric; this collaboration shall support University of Salerno in producing their toolkit on secure two-party/multi-party computation and IBM in Fabric-based privacy-preserving applications. IBM and IOHK are evaluating a possible integration of stake-based consensus protocols and Hyperledger Fabric. IOHK/I.O.Research and University of Edinburgh are already collaborating through the Blockchain Technology Laboratory hosted at the university.

4 Conclusion

PRIViLEDGE generates research results as well as toolkits and prototypes in the area of privacy-preserving DLTs, an area that is expected to be of significant economic importance. Beyond that, new requirements for cryptographic schemes that stem from DLT applications require considerable advances in cryptographic research.

Academic partners benefit from PRIViLEDGE in several ways. The research results obtained during PRIViLEDGE are planned to be published at high-level academic venues, improving their reputations. Results developed and experiences gained during PRIViLEDGE will help advancing existing or developing new courses, and

²⁷<https://www.insurancejournal.com/news/national/2018/05/25/490345.htm>

D5.3 – Exploitation Strategy and Roadmap

thereby improve teaching. Beyond the courses, student projects and theses in popular areas such as DLTs also attract additional students to the involved research groups.

Industry partners mainly benefit through the generation of assets which they can exploit in their offers as well as in future product developments; this in particular refers to the toolkits and prototypes developed throughout the project. The partners additionally benefit through ongoing education of their employees, through interaction with the other partners in PRIViLEDGE.

Last but not least, the toolkits developed in the project will implement the research results and be available as open source. This ensures that not only the PRIViLEDGE partners will be able to benefit from the work performed during the project, but that the results will also be readily available for use by the public.