DS-06-2017: Cybersecurity PPP: Cryptography

PRIViLEDGE
Privacy-Enhancing Cryptography in Distributed Ledgers

D5.5 – Report on Exploitation

Due date of deliverable: 31 March 2021
Actual submission date: 31 March 2021

Grant agreement number: 780477
Start date of project: 1 January 2018
Revision 0.99

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	

D5.5

Report on Exploitation

Editor
Marko Vukolić (IBM)
Contributors
Ahto Truu (Guardtime)
... (UEDIN)
Berry Schoenmakers (TUE)
Toon Segers (TUE)
Ivan Visconti (UNISA)
Sven Heiberg (SCCEIV)
Panos Louridas (GRNET)
Nikos Voutsinas (GUNET)
.. (IOHK)
Reviewers
Ahto Truu (Guardtime)
Nikos Voutsinas (GUNET)

31 March 2021
Revision 0.99

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

Blockchain and distributed ledger technologies (DLTs) have emerged as one of the most revolutionary developments in recent years, with the goal of eliminating centralized 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 one of the 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 realize cryptographic protocols supporting privacy, anonymity, and efficient decentralized 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 5.5 "Report on Exploitation" describes the individual plans and accomplishments of the project partners for exploiting the project results, as well as a joint efforts to create and use the exploitable assets outlined in the Description of Action. We report on research results generated during PRIViLEDGE as they benefited 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, in particular, help the industry partners in developing prototypes for their use case scenarios.

Contents

1 Introduction

1.1 Purpose of this Document and Relation to other Project Work

The present document, Deliverable 5.5 "Report on Exploitation", aims at presenting the final exploitation strategy and plans for the main results coming from the project PRIViLEDGE, building and extending on the Deliverable 5.3. 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 a market analysis. Section 2 is dedicated to the individual exploitation reports of the project partners. Section 3 describes the collaborative exploitation approach of the partners. Section 4 concludes this document.

Deliverable 5.5 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.

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 centralized 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. Moreover, currently deployed DLTs lack scalability which is also addressed by one of PRIViLEDGE toolkits, which will be exploited in Hyperledger Fabric.

PRIViLEDGE realizes cryptographic protocols supporting privacy, anonymity, and efficient decentralized 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 are or will be published by the project and made publicly available. The usefulness of these toolkits will be demonstrated through four ledger-based solutions (use cases): (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. As initially detailed in the project proposal, the exploitation effort of PRIViLEDGE is targeted at potential users of DLT in industry and the public sector. PRIViLEDGE provides a portfolio of tools for privacy-preserving operation of distributed ledgers, for different security goals. These tools consist of a family of modular toolkits that are demonstrated in the context of the technology prototypes that form the use cases. The toolkits targeted widely-used open-source DLT platforms, such as Hyperledger Fabric or Cardano. Together, the toolkits and prototypes yield a common PRIViLEDGE *framework*, which supports compatibility and interoperability among the tools and results.

Selected building blocks are 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 widespread 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* through publication of open-source toolkits.

PRIViLEDGE follows the exploitation strategy detailed in the following, which helped each partner with formulating a specific exploitation plan. These respective plans are loosely be organized along the categories outlined in the strategy. We followed two broad strategies, one oriented towards the industrial partners and one addressing more the academic partners. These categories acted 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 TClouds[1] and ESCUDO-CLOUD[2].

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.
8. Involve marketing, product-management, and sales departments early on in the process.

[1] http://www.tclouds-project.eu/
[2] http://www.escudo-cloud.eu/

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

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 capitalization or the transaction throughput per time period. According to CoinMarketCap.com. At the time of writing of our exploitation plan, outlined in Deliverable 5.3., the market capitalization of Bitcoin was €109 billion, with a trade volume of €4 billion per day. The market capitalization of Ethereum amounted to €35 billion, with a trade volume of €1.5 billion per day. Even smaller "top-ten" systems such as Cardano still had a market capitalization of €2.8 billion, with a daily volume of €77 million.

During PRIViLEDGE we witnessed an outstanding growth of blockchain network and DLT valuation. At the time of writing, the market capitalization of Bitcoin grew almost 8x to €870 billion, while those of Ethereum and Cardano grew respectively almost 5x (€170 billion, Ethereum) and 12x (€33.2 billion). This demonstrates the excellent timing of a PRIViLEDGE.

In Deliverable 5.3, we discussed another growing scheme, 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 study of PwC[3], 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]

Recently, and since Deliverable 5.3., blockchain and DLT industry has seen a major growth in another prominent cryptocurrency asset — NFTs or Non-Fungible Tokens. NFTs are special cryptographically-generated token that use blockchain technology to link with a unique digital asset that cannot be replicated. They are often used to represent digital art. `https://coinmarketcap.com/nfts/` tracks valuation of blockchain networks dedicated exclusively to NFTs with market capitalization exceeding, at the time of writing, €15 billion. This market capitalization does not include NFTs on less specialized blockchains and networks (e.g., Filecoin or Ethereum).

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, Gartner[5] predicts that "Blockchain's business value-add will surge to more than $3.1 trillion by 2030".

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 all contributed to strong exploitation plan that describes how each of the partners contributed to the exploitation of the PRIViLEDGE results. The individual exploitaiton reports are presented in Section 2, before Section 3 which outlines 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-cios-guide-to-blockchain/

2 Partner Exploitation Plans

This section describes the individual exploitation reports of the project partners. The exploitation reports vary based on the type of organization and their role in the project. The exploitation of academic partners focuses on published 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 described their individual exploitation reports 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, authenticated data structures, and secure multi-party computation 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 Commercialization Report

In the shorter term, Guardtime expects the PRIViLEDGE outcomes to strengthen its offerings in the insurance sector, more specifically in health insurance, which is one of the demonstration use-cases in the project. In particular, the ability to prove the efficacy of various treatments without disclosing the underlying health records would enable new payment models while preserving patient privacy.

However, the cryptographic techniques developed in PRIViLEDGE for those goals in the health insurance use-case are universal and in the longer term should able applicable also in products and services for other verticals.

2.1.5 Report on Economic Impact

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 organizations 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 Hyperledger[6], an organization of the Linux Foundation. IBM has contributed significantly and continuously to Hyperledger Fabric[7], 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 network[8] or the Mobility Open Blockchain Initiative[9].

[6] https://hyperledger.org/
[7] https://www.hyperledger.org/projects/fabric/
[8] https://sovrin.org/
[9] 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 Platform[10] 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 Food Trust [11], an ecosystem of producers, suppliers, manufacturers, retailers and others creating a smarter, safer, more sustainable food system for all; or TradeLens[12], which utilizes Fabric-based DLT to transform container logistics by freeing yourself from legacy data systems, manual document handling and poor visibility. IBM aims at benefiting from the economic success of these ecosystems through fees earned by running the platform. More recently, also based on Fabric, and in the light of the COVID-19 pandemic, IBM launched another DLT product based on Hyperledger Fabric, IBM Digital Health Pass[13] which is designed to provide organizations with a smart way to bring people back to a physical location, such as a workplace, school, stadium or airline flight. 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

Practically all use DLT use cases IBM is involved in are built on Hyperledger Fabric, which was partly developed in prior EU Horizon 2020 projects, namely SUPERCLOUD (`https://cordis.europa.eu/project/id/643964`). 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. In PRIViLEDGE, the main contributions of IBM are related to: 1) flexible toolkit for Byzantine Fault-tolerant consensus for Hyperledger Fabric which is a necessary component to power truly decentralized deployments of Fabric, and 2) privacy of transactions based on zero-knowledge proofs, targeting Fabric deployments that involve tokenization of assets.

The importance of flexible Byzantine fault-tolerant 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 Commercialization Report

With respect to the goals related to flexible toolkit for Byzantine consensus, in PRIViLEDGE IBM developed a new protocol for Byzantine fault-tolerant (BFT) consensus, called Mir-BFT[14], which allows high flexibility of the number of leaders in a BFT protocol, which in turn allows unprecedented performance at scales of about 100 nodes, which are the most relevant for permissioned blockchain systems and DLTs. In the context of work in PRIViLEDGE work package WP3, we showed that Mir-BFT outperforms state-of-the-art and orders more than 60000 signed Bitcoin-sized (500-byte) transactions per second on a widely distributed 100 nodes, 1 Gbps WAN setup, with typical latencies of few seconds.

The first step towards commercialization is open sourcing the Mir-BFT code base. The code is available at `https://github.com/IBM/mirbft` under Apache 2.0 license. In PRIViLEDGE, Mir-BFT is developed

[10] `https://www.ibm.com/blockchain/platform`
[11] `https://www.ibm.com/blockchain/solutions/food-trust`
[12] `https://www.tradelens.com/`
[13] `https://www.ibm.com/products/digital-health-pass`
[14] `https://arxiv.org/abs/1906.05552`

as a standalone library which will allow reuse of the consensus protocol across different DLTs, naturally including Fabric as well. IBM plans to complete production implementation of Mir-BFT by the end of PRIViLEDGE, or shortly thereafter.

IBM further plans to complete development of Mir-BFT under the auspices of Hyperledger Labs (`https://labs.hyperledger.org/`), which provides a space where work can easily be started without the creation of an official Hyperledger project. This will demonstrate IBM openness to sharing state-of-the-art technologies for DLTs and contribute to further visibility and impact of PRIViLEDGE results, in this case Mir-BFT library. This move of Mir-BFT to Hyperledger labs is scheduled to happen before end of PRIViLEDGE.

Once production development is fully completed IBM plans to exploit Mir-BFT in Fabric ordering service as its main consensus protocol, essentially deprecating all the others consensus mechanisms in Fabric. This is very important for the entire ecosystem. Beyond Fabric, the modularity and flexibility of the Mir-BFT consensus library will allow reuse in other DLT projects.

2.2.5 Report on Prospective Economic Impact

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.[15] 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 lead 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 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.

We expect that the toolkits developed in PRIViLEDGE, namely Mir-BFT consensus toolkit will mark a new epoch for Hyperedger Fabric, boosting IBMs visibility and presence, resulting eventually in more profits for thhe company.

2.3 The University of Edinburgh

2.3.1 Introduction

In the beginning of the project, The University of Edinburgh, PRIViLEDGE employed a primary investigator Prof. Aggelos Kiayias and one researcher Dr. Michele Ciampi. Currently, The University of Edinburgh employs, in addition to the mentioned members, the Senior Lecturer Markulf Kohlweiss, the researcher Thomas Zacharias and the PhD student Misha Volkhov.

The Blockchain Technology Laboratory (BTL)[16] 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 the this laboratory a number of research projects ran in parallel with high degree of synergy to PRIViLEDGE.

[15] `https://www.juniperresearch.com/press/press-releases/ibm-ranked-no-1-blockchain-technology-leader`

[16] `https://www.ed.ac.uk/informatics/blockchain`

2.3.2 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 has benefited from the research done during the project in terms of research and successfully incorporated part of the achieved knowledge 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 have enhanced the course curriculums with new research and blockchain which have attracted the interest of more and more students during these years.

The University of Edinburgh has therefore improved the training provided bringing it up to par with the current state of the art (more detail on the result achieved in terms of research follows).

2.3.3 University of Edinburgh PRIViLEDGE Goals

The project 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 has fulfilled the initial expectation producing several publications in the top cryptographic and security venues such as CRYPTO, Eurocrypt, Theory of Cryptography Conference (TCC), IEEE S& P, and ACM CCS. Additional result have been presented also in Financial Cryptography, Esorics, ACNS, CSF and SCN and Public-Key Cryptography, Financial Cryptography.

It is currently currently under investigation how to combine part of the result of Priviledge with the 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 Demos[17], and the combination with PRIViLEDGE will greatly enhance the system's verifiability as the system's security relies on a public bulletin board. On of our objective would be to roll out this system as a blockchain based service for UEDIN students during the course.

2.3.4 Report on Exploitation Results

The UEDIN has made a significant joint effort with the industry partner IOHK with which UEDIN has a long standing collaboration via its Blockchain Technology Laboratory. Currently UEDIN and IOHK are still collaborating to deploy of the results of WP2 and WP3. One of the most relevant work is related to the UC4 (software update for blockchains). The research outputs of UEDIN comes from the collaboration with other research and industrial partners, in particular with UNISA.

2.4 Technical University of Eindhoven

2.4.1 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.

2.4.2 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.

[17] `http://www.demos-voting.org/`

The supported members of the research team (one Associate Professor and two PhD students) have benefited from the research done during the PRIViLEDGE program. Particularly, the support helped to advance research in privacy-preserving secure computation techniques (see PRIViLEDGE publications), to extend the open-source MPC toolkit MPyC `https://github.com/lschoe/mpyc`, and to evolve the TU Eindhoven course on Cryptographic Protocols (2DMI00).

2.4.3 Technical University of Eindhoven PRIViLEDGE Goals

The project provided valuable professional training for the researchers involved and will enable them to substantially broaden their command of distributed ledger technologies. TU Eindhoven has produced several publications in important cryptographic venues such as the RSA Conference.

2.4.4 Report on Exploitation Results

TU Eindhoven collaborated closely with industry partner Guardtime on the proof of concept application of verifiable MPC (combining MPC with zero knowledge proofs) in the PRIViLEDGE Health Insurance Case use-case 2. It also collaborated closely with University of Salerno on the joint delivery of the MPC toolkit for cryptographic ledgers.

During the project, the company Roseman Labs was founded by two members of the TUE research team, dr. Niek Bouman and Toon Segers. Niels de Vreede, who worked on PRIViLEDGE while employed by TUE, also joined the company. Roseman Labs is advised by Berry Schoenmakers and applies open-source research on MPC from PRIViLEDGE, particularly the concept of "Secure Groups" (see also PRIViLEDGE Deliverable 2.3). The focus of Roseman Labs is production grade software for MPC.

2.5 University of Salerno

2.5.1 Introduction

As an academic partner, University of Salerno is mainly interested in research, teaching and knowledge transfer activities. In this respect, PRIViLEDGE plays an important role conveying resources towards DLT that is a cutting-edge research topic. 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.

2.5.2 Exploitation Approach

Through scientific publications and dissemination activities connected to PRIViLEDGE, University of Salerno is now a more established institution for skills and experience on DLT. This can attract more qualified students, scientific collaborations and partnerships with industrial partners.

2.5.3 University of Salerno PRIViLEDGE Goals

A primary goal is to leverage competence increased during PRIViLEDGE in order to then produce more relevant scientific results in this field. Through scientific results and dissemination activities focusing on DLT, University of Salerno also aims at establishing new connections with both academic and industrial partners to the embark in joint projects and other forms of collaboration.

2.5.4 Results

The research group at University of Salerno involved in PRIViLEDGE activities produced several research papers (some of them already published in well known conferences) presenting new results of both theoretical and practical relevance for DLT. Moreover University of Salerno established collaborations with industrial partners interested in the use of confidential data in DLT.

There has been a clear benefit for students that had a chance to be in touch with PRIViLEDGE in various forms (e.g., classes, theses). Moreover University of Salerno joined the Algorand Foundation's Global University Program, that includes only some selected universities in the world.

2.6 Smartmatic-Cybernetica Centre of Excellence for Internet Voting

2.6.1 Introduction

Smartmatic-Cybernetica Centre of Excellence for Internet Voting (SCCEIV) is a private company established in 2014, dedicated to the development of online voting systems and providing online voting services. The company is owned by Smartmatic (https://www.smartmatic.com/), world leader in the automation of elections, and Cybernetica AS (https://www.cyber.ee/), the Estonian R&D intensive ICT company that built the online voting system used in Estonia.

SCCEIV is developing the online voting system TIVI (https://tivi.io/) and is participating in the support & development of Estonian verifiable online voting system – IVXV.

The TIVI system is used to provide services to diverse set of customers – governmental, municipal and organizational elections of different kind can be carried out with the TIVI technology. All these customers require some level of transparency and verifiability for their elections under the condition of secret ballot.

2.6.2 Exploitation Approach

SCCEIV customers fall into two major categories – customers who purchase a license to the platform for extended period of time and unlimited elections and customers who purchase platform and services for a single event.

Period license – with these customers the approach is to set up a version of the TIVI platform in such a manner that the customer can manage all election related aspects (key generation, election configuration, voter lists, decryption etc.) themselves. In order to facilitate verifiability, these platforms are co-hosted with the customer, such that certain components are solely under the control of customer.

Single event – with these customers there is no standard approach, however they are less likely to be interested in participating in technical hosting of the platform and more likely in requesting election-as-a-service, rendering the service provider a trusted third party.

In both of these cases the protocol and approach proposed by the PRIViLEDGE, implemented as part of the TIVI platform lowers the bar on making election data available to independent auditors. For customers with periodic license this simplifies addition of external auditors to the existing deployment scheme. For the single event customers the technical complexity of required controls is reduced due to the everlasting privacy of the voting scheme.

2.6.3 SCCEIV PRIViLEDGE Goals

All TIVI customers require transparency and verifiability for their elections under the condition of secret ballot. This calls for the application of cryptographic protocols that enable independent auditors to verify the claims about the correctness of the voting result without violating ballot secrecy. From the auditor's perspective there is a question about the authenticity and integrity of the data provided as a basis of the analysis. From the election organization's perspective there is a question about the risks rising from the data being made available to the third parties.

SCCEIV main goal in the project is to gain knowledge about making data proving election integrity publicly available in distributed manner without jeopardizing the confidentiality properties. The protocol and proof-of-concept implementation from the PRIViLEDGE can be integrated with the TIVI to offer this to the customers as part of SCCEIV portfolio.

2.6.4 Commercialization Report

SCCEIV expects the project outcomes to become part of its portfolio and proposal to its customers, giving SCCEIV a competitive advantage in cases where strong verifiability and transparency are expected by the customers.

In longer term SCCEIV may integrate the techniques from the PRIViLEDGE into its platform TIVI, which will make them available to its customers as a standard offering.

2.6.5 Report on Economic Impact

The COVID-19 pandemic has increased interest towards online voting mostly among large organizations that rely on elections in the process of their decision making. These organizations move quicker and decide faster in comparison to governmental customers. Nevertheless, a key elements in introducing online voting to their processes are transparency, verifiability and auditability. The outcomes of the PRIViLEDGE, if integrated into a product, improve auditability and remove one more obstacle from the way for online voting, making decisions to go for the technology easier for the organizations.

2.7 Greek Research and Technology Network

2.7.1 Introduction

As set out in D5.3, 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. Since the outbreak of the COVID-19 pandemic, GRNET has been tasked with developing and providing online government and administrative services, under the auspices of the Ministry of Digital Governance. GRNET has developed the `gov.gr` portal, where a host of administrative procedures, which previously could be carried out only in person, are now offerred digitally, online. The number of the services grows continuously, as more processes are adopted for digitisation. The `gov.gr` portal, in operation for almost a year, has been a resounding success, with millions of digital documents and procedures carried out by citizens, resulting in huge savings (apart from contributing to reduced physical contacts).

The services put in production by GRNET to this date do not use DLT technologies. That is not required, as the validity of documents and procedures is certified by law, centrally, by the technological infrastructure of the Ministry of Digital Governance (part of it operated by GRNET itself). Therefore there is no notion of distributed trust or of any disputes; in essence the law prescribes exactly how code (implemented through GRNET services) is legally binding. In this background, GRNET is actively exploring the outcomes of PRIViLEDGE for extending the existing services or developing new services that will benefit from a decentralized trust model, as we explain below.

2.7.2 Exploitation Approach

GRNET's services are offerred free; the exploitation therefore focuses on ease of adoption of new services and interoperability with other services and initiatives.

GRNET participates actively in the European Blockchain Services Infrastructure (EBSI), representing the Greek government as an entity overseen by the Ministry of Digital Governance. In EBSI, Greece has declared interest in implementing four use cases: European Self-Sovereign Identity Framework (ESSIF), Diplomas, Notarization, and the handling of Asylum applications. It is already operating an EBSI network node in Athens and has entered in a CEF-TELECOM project for supporting and extending the infrastructure and services of the "Hellenic Distributed Ledger Technologies Infrastructure—ELEDGER".

The aim of EBSI is to develop cross border services in Europe leveraging blockchain technologies; for instance, even though diploma certification services may already exist (or come to exist) in different countries, blockchain technologies can be used to ensure their interoperability and smooth integration for the users.

GRNET will continue to follow the developments in EBSI and look for synergies with PRIViLEDGE outcomes that will allow services in Greece to be integrated with services at the European level with cutting-edge technologies.

2.7.3 GRNET PRIViLEDGE Goals

In the course of PRIViLEDGE GRNET has been working on various different DLT technologies. GRNET goals are to investigate whether, and if yes how, they can be adopted for use in real-world digital services, potentially (but not exclusively) those pursued by the EBSI:

- We have explored distributed storage technologies that can be used in conjunction with blockchains for off-ledger storage. This can be instrumental for storing data when existing, or centralized storage is not desired. For instance, in `gov.gr` GRNET has already immplemented and deployed digital vaults, where citizens and public administrator agencies store documents. The digital vaults are currently stored in GRNET's premises; however, this does not exclude decentralized storage solutions (like citizen's wallets) being used in the future.
- We have developed and implemented a privacy-preserving diplomas certification protocol. The EBSI is developing a diplomas certification service in the Diplomas Use Case. As the EBSI Diplomas Use Case develops we will seek synergies between the protocol and the technologies we have used in PRIViLEDGE and those of the use case.
- In PRIViLEDGE we have worked with the University of Tartu, and are have also been working with the University fo Edinburgh in zkSNARK implementations. Our particular interest is in facilitating the creation of Common Reference Strings (CRS); practical methods for CRS generation can obviate the need for onerous ceremonies. This can be instrumental for the adoption of new, CRS-based mixnets that have the potential of very significant speed ups for the mixing of votes in Zeus (`zeus.grnet.gr`), GRNET's e-voting service that is used by thousands of institutions and groups around the world.

2.7.4 Commercialization Report

GRNET does not currently seek to commercialize the services it develops. As explained, a large number of them are services offered to citizens, and these are not the subject of commercial exploitation. As noted in D5.3, production-level services built on DLTs may be of commercial interest to other parties. GRNET can investigate such applications with interested parties. Moreover, GRNET is committed to open source and the provision of data and services through open Application Programming Interfaces (APIs), which can fertilize commercial exploitation of added-value services building on top of them.

2.7.5 Report on Economic Impact

The COVID-19 pandemic has given the incentives for moving processes online, and GRNET has been instrumental in making progress in this area in Greece, resulting in substantial savings, from reducing time in transport and in-person appointments (millions of administrative procedures have now been conducted remotely). This has happened without leveraging the technology of PRIViLEDGE. Gains from PRIViLEDGE technologies will be realized via their adoption in extending digital services, as outlined in 2.7.2 and 2.7.3; however, it is not possible to estimate the potential economic impact at the present time.

2.8 Greek Universities Network

2.8.1 Introduction

The Greek Universities Network is a non-profit civil company and its members are all the Greek higher education and academic institutions. GUNET's mission is the provision, diffusion and promotion of advanced information

technologies and applications in the broad academic and research community in Greece. As a software provider, GUNET develops its own software platforms and delivers bespoke solutions aiming at servicing the operational needs of its members. As a solution integrator and service provider, GUNET delivers production services targeting the 25 institutions of the higher education in Greece. In parallel, because of its affiliation with the research groups at universities, GUNET has been an early adopter of many emerging technologies.

2.8.2 Exploitation Approach

GUNET's exploitation approach is twofold. The immediate benefits from the PRIViLEDGE results will be realized via the planned advancements in the eDiplomas platform (https://ediplomas.gr) that GUNET has developed for the Greek HEIs. Furthermore, because of GUNET's central role as the provider of Identity and Access Management solutions for the Greek HEIs, is exploring mixtures of emerging Identity Management technologies such as DIDs, SSIs with DLTs towards building a trustworthy, inter-operable, and standards-based identity management solution for individuals and organizations.

2.8.3 GUnet PRIViLEDGE Goals

While eDiplomas is built around conventional cryptographic technologies so as to deliver a production ready solution today, it is modular enough to incorporate DTLs in order to replace its central hub architecture for various core functions. In particular, GUNET's participation in PRIViLEDGE has led to the enrichment of eDiplomas roadmap with:

- a HyperLedger based permissioned yet public blockchain, to host the open data that compose the public part of the diplomas templates, i.e. the part of diploma that does not include PII or issuing dates, a total of more than 4K records dating back from the year 2000, from more than 40 issuing institutions.
- a permissioned private blockchain supplementary subsystem, to provide the accountability and auditability of the messages exchanged through eDiplomas, in a privacy preserving way as required by the legislation.

The achievement of the above goals would be a quantum leap in the evolution of the eDiplomas and will better position the platform in the relative market.

2.8.4 Commercialization Report

GUNET is a non-profit civil company founded by the Greek universities and its objectives are determined by the needs of its members. In that discipline GUNET's efforts are not focused on the commercialization of the provided solutions. However, GUNET's participation and active engagement in the technological evolutions in the field of DLTs is essential for reinforcing its leading position in the Greek Higher Education as a service provider as well as for introducing new citizen-centric data channels and immutable accounting and audit functions to its core application platforms. This way GUNET will be able to participate in broader collaborations across Europe and attract public funding.

2.8.5 Report on Economic Impact

The forecasted direct and indirect cost savings from the PRIViLEDGE enhancements in the eDiplomas platform will be significant, mostly because issuing institutions and service consumers are expected to welcome any additional technical measures that will help them minimize the risk of a GDPR incident. This will further expedite the adoption of the eDiplomas solution and provide significant cost savings by transforming the recruitment and hiring processes at the consumer side and alleviate the burden of manual diploma's verifications from the university personnel.

2.9 I.O.Research

2.9.1 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.

2.9.2 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.

In particular, IOHK anticipates results from PRIViLEDGE regarding the decentralization of software updates. This is because the Cardano blockchain aspires to become a community-governed, self-sustaining blockchain. Decentralized governance is the key factor to achieve this goal, a core component of which is the software updates system. The research results on the problem of decentralized software updates developed within PRIViLEDGE, as well as the corresponding prototype implementation, will greatly influence the future version of Cardano that will enable decentralized governance.

Last but not least, I.O.Research's participation in PRIViLEDGE 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.

2.9.3 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.

In particular, the low-hanging fruit of PRIViLEDGE that I.O.Research aims to leverage is to influence as much as possible the decentralized governance roadmap of the core blockchain product of IOHK, namely the Cardano blockchain. Decentralized governance in Cardano comprises three main components: a) The Cardano Improvement Proposal (CIP) Process, an off-chain process for formulating ideas for change. b) The Treasury system, a decentralized blockchain-based system for funding proposals and c) The decentralized software updates system. Indeed, the decentralized software update system is a core part of the decentralized governance landscape of Cardano. The primary goal of I.O.Research is to exploit the relevant PRIViLEDGE research and work in the relevant prototype in order to influence Cardano along the following dimensions:

- Definition of an end-to-end software updates mechanism that will cover the full *lifecycle* of a software update and will include all types of software updates (protocol changes, parameter changes, common software updates)
- Definition of *secure activation protocols* for consensus protocol updates that will ensure a secure transition from the current ledger to the upgraded one, without chain splits, or other security risks.

- Exemplary integration of a new update mechanism within the Cardano blockchain and propose a modular architecture for the relevant core Cardano node software components (Ledger layer, Consensus layer).

Our ambition is with our work in PRIViLEDGE to benefit the future release named "Voltaire" that will enable decentralized governance and community-based decision making for Cardano.

2.9.4 Commercialization Report

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 decentralized governance is a major milestone in the Cardano blockchain product roadmap, which has been announced from the early beginning and is greatly anticipated by the Cardano community. We expect that this will significantly increase the value of the Cardano blockchain, since it will cover all the aspects of decision making in Cardano: from funding and initial ideation to the very last stage where changes are activated on the mainet. This holistic approach to decentralized governance is often missing in existing projects in the cryptocurrency space and we strongly believe that will be appreciated greatly by the Cardano community.

2.9.5 Report on Economic Impact

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

Beyond individual partners' exploitation plans described in the previous section, 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 collaborating on efficient constructions of non-interactive zero-knowledge argument systems that rely on non-programmable random oracles and superpolynomial-time simulation.

SCCEIV and University of Salerno are working on definitions, constructions and proof-of-concept implementations of an e-voting protocol with everlasting privacy.

Eindhoven University of Technology and University of Salerno are working on connecting MPyC (`https://www.win.tue.nl/~berry/mpyc/`) to the toolkit on ledger-oriented secure two/multi party computation.This toolkit is developed by University of Salerno allows the add to traditional software for two-party and multi-party computation (MPC) the benefits of the public verifiability given by blockchains. Indeed the toolkit allows to redirect[18] the communication that traditionally is point-to-point to blockchains, so that everyone can verify the state of the computation. This can be in particular useful when many players would like to join a computation and when a player for privacy reasons prefers to avoid direct network connections with other players of the joint computation. The toolkit can be useful also to transparently allow the use of blockchains since it includes a generic API and a proof-of-concept implementation. The development of the toolkit is in collaboration with Eindhoven University of Technology so that their library MPyC for verifiable multi-party computation can also exploit the features of the toolkit. 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. In particular, the two research teams have recently worked on the problem of secure activation protocols. A secure activation protocol is one that achieves a secure transition

[18]This step requires the MPC software to satisfy some requirements.

from the current version of the consensus protocol to a new one. They have formally defined what is a *secure activation* and have proposed two distinct protocols that provably achieve this. In a nutshell, *secure activation* means, the secure transition from the old ledger (L1) whic henjoys liveness to the new ledger (L2) which enjoys consistency, while L2 has L1 as a prefix.

The first activation protocol requires the structure of the current and the updated blockchain to be very similar (only the structure of the blocks can be different) but it allows for an update process more simple and efficient. The second activation protocol that the joint team proposes is very generic (i.e., makes few assumptions on the similarities between the structure of the current blockchain and the updated blockchain). The drawback of this protocol is that it requires the new blockchain to be resilient against a specific adversarial behavior and requires all the honest parties to be online during the update process. However, they show how to get rid of the latest requirement (the honest parties being online during the update) in the case of proof-of-work and proof-of-stake ledgers. The interested reader can find more details on this topic in their published paper [**?**].

Beyond this direct collaboration, PRIViLEDGE toolkits, which we initially described in Deliverable D5.3 serve as a basis for future collaboration among partners and exploitation beyond PRIViLEDGE timeframes.

4 Conclusion

PRIViLEDGE generated important and impactful 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. One of the main impact of PRIViLEDGE is availability of toolkits in leading open-source DLTs such as Cardano and Hyperledger Fabric.

Academic partners benefit from PRIViLEDGE in several ways. The research results obtained during PRIViLEDGE are published at high-level academic venues, improving reputation of academic partners. Results developed and experiences gained during PRIViLEDGE help advance existing or developing new courses, and 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.