



JRC SCIENCE FOR POLICY REPORT

Blockchain for digital government

An assessment of pioneering implementations in public services

Authors:

David Alessie

Maciej Sobolewski

Lorenzino Vaccari

Editor:

Francesco Pignatelli

2019



Joint
Research
Centre

EUR 29677 EN

This publication is a Science for Policy report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

Contact information

Name: European Commission, Joint Research Centre, Digital Economy Unit (JRC/B6)
Address: Edificio Expo, c/ Inca Garcilaso 3, 41092 Seville (Spain)
Email: JRC-LIST-B6-SECRETARIAT@ec.europa.eu

EU Science Hub

<https://ec.europa.eu/jrc>

JRC115049

EUR 29677 EN

PDF	ISBN 978-92-76-00581-0	ISSN 1831-9424	doi:10.2760/942739
Print	ISBN 978-92-76-00582-7	ISSN 1018-5593	doi:10.2760/93808

Seville: European Commission, 2019

© European Union

The reuse policy of the European Commission is implemented by Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Reuse is authorised, provided the source of the document is acknowledged and its original meaning or message is not distorted. The European Commission shall not be liable for any consequence stemming from the reuse. For any use or reproduction of photos or other material that is not owned by the EU, permission must be sought directly from the copyright holders.

All content © European Union, 2019, except: Figure 17 on *page 80*, used under *CC0 licence*. Source: *Wikipedia.org*

How to cite: ALLESSIE D, SOBOLEWSKI M, VACCARI L, PIGNATELLI F (Editor), Blockchain for digital government, EUR 29677 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-00581-0, doi:10.2760/942739, JRC115049

Contents

- Foreword 1
- Acknowledgements 2
- Abstract..... 3
- Executive summary 4
- 1 Introduction..... 8
 - 1.1 Key benefits of Blockchain and Distributed Ledger Technologies 8
 - 1.2 Blockchain and digital governments..... 10
 - 1.3 Value added and composition of this report 12
- 2 Empirical analysis of blockchain projects..... 13
 - 2.1 Methodology 13
 - 2.1.1 Selection of projects 13
 - 2.1.2 Assessment framework..... 13
 - 2.2 Individual case studies 18
 - 2.2.1 Exonum land title registry – Georgia 18
 - 2.2.2 Blockcerts academic credentials – Malta 22
 - 2.2.3 Chromaway property transactions – Sweden 26
 - 2.2.4 uPort decentralised identity - Zug, Switzerland 31
 - 2.2.5 Infrachain governance framework - Luxemburg 35
 - 2.2.6 Pension infrastructure - the Netherlands 38
 - 2.2.7 Stadjerspas smart vouchers - Groningen, the Netherlands 42
 - 2.3 Horizontal comparison of case studies 46
 - 2.4 Insights from case studies 53
- 3 Exploration of potential for scale-up of blockchain services..... 57
 - 3.1 Assumptions 57
 - 3.2 Evaluation of individual services 59
 - 3.3 Insights from scale-up exploration 63
- 4 Conclusions and policy recommendations 65
 - 4.1. Main conclusions from the study 65
 - 4.2. Recommended policy agenda 68
- References 71
- List of abbreviations and definitions 74
- List of figures..... 76
- List of tables..... 77
- Annex: Blockchain against VAT fraud 78

Foreword

This report presents the main findings from the research project entitled "Digital Government Benchmark" undertaken by the Joint Research Centre of the European Commission in collaboration with Gartner Consulting, and financed by the "European Location Interoperability Solutions for e-Government" (ELISE) Action of the ISA² Programme.

For more details on the scope of ELISE and ISA², please visit:

https://ec.europa.eu/isa2/actions/elise_en

https://ec.europa.eu/isa2/home_en

Acknowledgements

Several people contributed to the project. We would like to thank Benoit Abeloos, Paula Galnares, Ken van Gansen, Ioannis Kounelis, Georges Lobo, Susana Nascimento, Daniel Nepelski, Fidel Santiago, Robin Smith, Nikolaus Thumm, Theodoros Vassiliadis, Mark Williams and Clementine Valayer for their valuable comments and support during field work, preparation and revision of the report. All errors remain the sole responsibility of the authors.

Authors

David Alessie (MSc) is a consultant at Gartner Consulting, specializing in blockchain and other emerging technologies.

Maciej Sobolewski (PhD) is an economist at the Digital Economy Unit of the Joint Research Centre of the European Commission, specializing in research on the economic impact of digital technologies and digital transformation.

Lorenzino Vaccari (PhD) is a computer scientist at the Digital Economy Unit of the Joint Research Centre of the European Commission, specializing in digital technologies and infrastructures for public sector.

Editor

Francesco Pignatelli (PhD) is a senior scientist at the Digital Economy Unit of the Joint Research Centre of the European Commission, responsible for the Digital Government institutional research.

Abstract

In less than ten years from its advent in 2008, the concept of distributed ledgers has entered into mainstream research and policy agendas. Enthusiastic reception, fuelled by the success of Bitcoin and the explosion of potential use cases created high, if not hyped, expectations with respect to the transformative role of blockchain for the industry and the public sector. Growing experimentation with distributed ledgers and the emergence of the first operational implementations provide an opportunity to go beyond hype and speculation based on theoretical use cases.

This report looks at the ongoing exploration of blockchain technology by governments. The analysis of a group of pioneering developments of public services shows that blockchain technology can reduce bureaucracy, increase the efficiency of administrative processes and increase the level of trust in public recordkeeping. Based on the state-of-art developments, blockchain has not yet demonstrated to be either transformative or even disruptive innovation for governments as it is sometimes portrayed. Ongoing projects bring incremental rather than fundamental changes to the operational capacities of governments. Nevertheless some of them propose clear value for citizens.

Technological and ecosystem maturity of distributed ledgers have to increase in order to unlock the transformative power of blockchain. Policy agenda should focus on non-technological barriers, such as incompatibility between blockchain-based solutions and existing legal and organizational frameworks. This principal policy goal cannot be achieved by adapting technology to legacy systems. It requires using the transformative power of blockchain to be used to create new processes, organizations, structures and standards. Hence, policy support should stimulate more experimentation with both the technology and new administrative processes that can be re-engineered for blockchain.

Executive summary

The origins of blockchain technology date back to 2008 when it was proposed as a computer science design to enable the secure direct trading of assets among peers who may not have sufficient confidence in each other. The core innovation that blockchain introduces is essentially a distributed append-only ledger on which messages can be irrevocably recorded. This new concept eliminates a need to maintain central intermediaries, which has potentially large economic and political implications. As electronic ledgers became a universal way of record-keeping, blockchain technology started to expand rapidly beyond an original payment system application. Today it is being explored by a growing developer community and a vibrant start-up ecosystem, being seen as a general purpose technology (Brynjolfsson & Hitt, 2000; Jovanovic & Rousseau, 2005) that will disrupt, if not transform, both industry and the public sector (Freeman & Perez, 1988; Smith, Stirling, & Berkhout, 2005).

Governments can be seen to increasingly focus their attention on potential applications of blockchain technology in the public sector. In general terms, distributed ledgers may become a new information infrastructure supporting the exchange of information between public administrations, citizens and businesses. Specific groups of use cases that leverage decentralised information infrastructures have been identified in the public sector context, as identified by Kounelis et al. (2017) and Grech & Camilleri (2017). In particular, blockchain technology is expected to revolutionise or, at least, facilitate various government services and functions. These include, for example, the provision of citizen records, running state registries and support to electronic voting, the facilitation of economic transactions, providing a regulatory oversight of markets, fighting tax fraud/evasion and the redistribution of public money, including grants, social transfers and pensions.

Digital government is the state-of-art concept from public administration science, a successor of e-government paradigm. The former model simply indicated the digitalisation of the public administration. Digital government refers to the creation of new public services and service delivery models that leverage digital technologies and governmental and citizen information assets. The new paradigm focuses on the provision of user-centric, agile and innovative public services. Blockchain absolutely is the one of the most innovative digital technologies that has to be considered under the new paradigm of governmental policy making and service delivery.

The goal of the study is to identify the relevance of distributed ledger technologies (DLT) for digital governments. The analysis is based on empirical evidence from a group of seven ongoing projects in Europe, which have utilised blockchain technology for developing end-user services relevant for public sector.

The study focuses on answering the following four research questions:

- What activities blockchain can serve from the public sector perspective and what are governments currently doing with this technology?
- What benefits does blockchain bring for digital government and, in particular, for citizens?
- Which blockchain services developed within ongoing projects can be scaled-up beyond their current scope?
- What policy actions are needed to fully utilise these technologies for the benefit of society and citizens?

The study begins with providing a brief definition and contextualisation of blockchain and distributed ledger technologies from a governmental perspective (Chapter 1). Then it analyses seven pilot deployments in the public sector with respect to functionalities, governance, usage, technical architecture, costs and benefits (Chapter 2). Based on the horizontal analysis of the pilot deployments and the exploration of the potential for the services to be scaled-up (Chapter 3), policy actions that are required to support

development of this technology are discussed alongside the conclusions of the study (Chapter 4).

Highlights from individual projects

- The Exonum land title registry project in Georgia was able to move quickly into a production phase as blockchain technology is used as a separate, additional technology layer that provides safety and security for digital certificates stored in the National Agency of Public Registry's (NAPR) land title database.
- The Blockerts academic credential verification project in Malta highlighted the importance of the exploration of blockchain technology for capturing first-mover advantages by adopting platform agnostic open source standards. Verification of academic credentials is the only end-user service in the sample that can be recommended for top-down implementation in the form of an EU-wide multi-sided platform. The service generates network benefits across universities, citizens and employers and responds to policy priorities of the Digital Single Market. The technical design is mature and relies on existing open source standards and public blockchain infrastructure.
- The Chromaway property transactions project in Sweden demonstrates the potential of blockchain-based automation in achieving huge efficiency gains in the settlement of multiparty transactions and reducing uncertainties between agents. This project points to a number of hurdles that inhibit the use of blockchain technology for complex and high value transactions, such as real estate transfers. These hurdles include the legality of digital signatures.
- The uPort decentralised identity project of Zug Municipality in Switzerland allows citizens to create blockchain-based identity that is independent from the government and only once attested by the authorities. The project design utilises smart contracts for the management and controlled sharing of personal data, providing a prime example of how blockchain can be used to empower citizens. The decentralised identity system, however, still requires a centralised, government-owned attestation system to exist in parallel.
- The Infrachain project, which had its origins in Luxembourg, enables more rapid blockchain pilot deployment in the public and private sector through a governance framework for private nodes, a key element of blockchain technology, and compliance of the chain they produce. This project provides a foundational building block for blockchain systems running end-user services that have access control for registered users. The framework also establishes reference requirements for the physical infrastructure needed, including a separation of hardware resources from the software layer.
- The Pension Infrastructure project in the Netherlands aims to create a pension administration system for all ecosystem partners based on blockchain. A shared database and workflow automation blockchain functionalities are leveraged to generate significant efficiencies in the administration and the regulation of pension system. Yet the scale and complexity of the system go beyond current technological frontiers. In particular, the large volume of transactions to be processed with smart contracts can be seen to constitute a major challenge.
- The Stadgerspas smart vouchers system in Groningen in the Netherlands introduces a blockchain-based redistribution system of benefits for low-income citizens. This service is operational and highlights the potential of programmable money for targeting and allocating social benefits and grants, enabled by blockchain technology. Programmable money allows defining the rules that govern authorisation, payment and settlement of transaction, making it impossible to hack.
- As well as the above examples, the study also explores the speculative use case of blockchain technology for countering value added tax (VAT) fraud. By design,

blockchain-based collection of VAT eliminates intra-EU vat carousels, effectively closing a large part of the VAT gap in Europe, estimated to be €147.1 Billion annually. This use case presents a number of technological challenges, such as the EU-wide scale of the system, an extremely large volume of transactions and a backward correction of accounts, which are likely to preclude operational deployment of such systems in the near future (see Annex).

Specific findings

- All three main blockchain functionalities: *notarization, shared database and workflow automation* can be useful for different operational capacities of governments and beneficial for interactions with the citizens and business.
- Services leveraging blockchain notarization are relatively more mature, while more disruptive solutions face challenges in implementation, mainly related to incompatibility with the current administrative processes and regulatory noncompliance.
- Projects with a higher level of maturity tend to have less stakeholder complexity and more centralised governance.
- Blockchain-based services that are already in operation respond to clear business needs. They also have an active public sector actor and a strong technological partner.
- Blockchain implementations are predominantly based on open source software. Some governments are pushing towards the publication of platform-agnostic open standards to minimise the risk of lock-in and to incentivise the adoption of the service by third parties.
- Blockchain is always just one layer of a more developed service. It usually depends on a non-DLT layer which runs on top of a legacy-type of centralised database.
- Private data is always stored off-chain. When a private permissioned blockchain is used, private data in principle could be stored on-chain in an encrypted form. On-chain storage creates, however, inefficiencies related to sending large portions of data over the networks, which make this design option, arguably, impractical.
- Transaction throughput does not appear to be a major bottleneck. The throughput in permission-less blockchain protocols is significantly less than those involving permissions to read, write and validate transactions. Those projects that anchor transaction on public permissionless blockchains have designed ways to mitigate throughput constraints.
- Blockchain technology currently does not threaten public institutions role as intermediaries, i.e. disintermediation. Blockchain-based solutions are either complementary or are only partially substituting existing online public services.
- Analysed blockchain-based designs generate specific cost items, yet their overall deployment costs should not be higher than the implementation costs of centralised designs.
- Blockchain-based services promise a range of benefits to the ecosystem. The main benefit drivers of blockchain technology in the public sector are process efficiency and the increased reliability of record-keeping which contributes to an increased trust in public institutions. Blockchain technology may also enhance citizens' and businesses' experience when interacting with public authorities. For example, personal certificates and land titles issuance and legally binding confirmations can be provided to the citizen automatically via mobile app, without a need to visit a town hall.

General conclusions

The study proposes the following conclusions and recommendations:

1. Contrary to how it is often portrayed, blockchain, so far, is neither transformative nor even disruptive for the public sector. We have not observed the creation of new business models, the emergence of a new generation of services nor direct disintermediation of any the public institutions involved in the provision of governmental functions.
2. Significant incremental benefits can be realised in some areas through the utilisation of blockchain technologies for the provision of public services. The two main groups of benefits related to blockchain are increased security (enhancement of data integrity, immutability and data consistency between organisations) and efficiency gains (such as reduced processing time and lower costs).
3. Blockchain technology can increase reliability of public institutions that use it for record-keeping. Consensus mechanism validates and registers transaction in a consistent way, spotting for any possible errors or counterfeiting attempts. Constantly updated ledger is stored in multiple copies by independent nodes in a peer-to-peer network. Decentralisation is argued to provide higher security and integrity of the records than most of the centralised systems offer.
4. Blockchain technology permits both new public service delivery and interaction models, as it can create data consistency within an ecosystem of organisations and actors, beyond the traditional public organisational boundaries. Blockchain provides a way to comply with the Once-Only Principle (OOP). By removing the need for the endless copying of data and artificially connecting different back office systems, it can help span organisational IT silos in the public sector.
5. Incompatibility between blockchain-based solutions and existing legal and organisational frameworks is a major barrier to unlocking the transformative potential of blockchain. Hence, the major policy objective should be to increase technological and ecosystem maturity of distributed ledgers. Reducing incompatibility requires not only the adaptation of technology to legacy systems, but also, to a greater extent, a transformation of existing processes, organisations and structures by using the disruptive power of blockchain.
6. Finally, the study proposes a framework for potential policy steps to exploit the full potential of blockchain technology across a spectrum of growing technology maturity. The policy agenda should focus on supporting: (i) knowledge sharing between the Member States; (ii) a focused development of new pilot projects; (iii) defining security, privacy, governance and interoperability standards; (iv) the creation of blockchain foundational components; and (v) the creation of dedicated infrastructures for specific use cases of high importance for the EU, for example taxation, customs or diploma sharing.

1 Introduction

1.1 Key benefits of Blockchain and Distributed Ledger Technologies

Distributed Ledger Technology

A distributed ledger technology (DLT) is a technology that facilitates an expanding, chronologically ordered list of cryptographically signed, irrevocable transactional records shared by all participants in a network. Any participant with the right access rights can trace back a transactional event, at any point in its history, belonging to any actor in the network. The technology stores transactions in a decentralized way. Value-exchange transactions are executed directly between connected peers and verified consensually using algorithms over the network.

DLTs address the 'double spending' problem. The double spending problem refers to the fact that digital information can be copied using the internet. If, for example, somebody would send a digital asset like a digital paper of ownership of a car to someone else, then there is a risk that the sender sends a copy over the internet and still keeps the original paper of ownership (EVRY, 2016). Traditionally, this risk has been mitigated by having trusted third parties or administrators, like banks, to act as a centralized authority keeping track of all transactions (Swan, 2015). DLT's shift this responsibility of validating the actual transfer of the asset to the whole network using carefully designed algorithms. This eliminates the need for a centralised database. Every actor in the network has a copy of the record of transactions, and any change of ownership of the digital assets in the system requires validation from its users.

There is no clear consensus on the definition of distributed ledger technologies and blockchain technology. In this study, a distributed ledger is defined as:

"Distributed ledger technology refers to the protocols and supporting infrastructure that allow computers in different locations to propose and validate transactions and update records in a synchronised way across a network."

Blockchain Technology

Blockchain is the most well-known and used distributed ledger technology. Blockchain is the type of a ledger in which value-exchange transactions (in the form of cryptocurrencies, tokens or information) are sequentially grouped into blocks. Each block contains a signature that is based on the exact content (string of data) of that block. The next block contains this signature as well, linking all previous blocks to each other up until the first block. Blocks are immutably recorded across a peer-to-peer network, using cryptographic trust and assurance mechanisms. Cryptocurrencies are a decentralized subset of digital currencies, based on a set of algorithms and protocols that enable a peer-to-peer, cryptographically based payment mechanism, a medium of exchange and a store of value, the best-known example being bitcoin (Gartner, 2018a). A token is a digital item which represents either the right to perform some operation or a physical object of value.

Blockchain finds its origin in a paper published by an anonymous (group of) author(s) called Satoshi Nakamoto. In this paper, the idea of a Bitcoin was introduced as a purely peer-to-peer (P2P) electronic transaction network.¹ This network allows for direct financial transactions instead of via a financial institution (Nakamoto, 2008). To simplify, blockchain technology allows two actors in the system (called nodes) to transact in a peer-to-peer (P2P) network and stores these transactions in a distributed way across the

¹ According to the widely accepted convention, the name of the blockchain network running Satoshi's protocols is written with capital 'B' (Bitcoin) to distinguish it from the coin generated inside the system (bitcoin).

network (Back et al., 2014). It registers the owners of the assets that are transacted and the transaction itself.

A transaction is verified by the network by a 'consensus mechanism', which allows users in the P2P network to validate the transactions and update the registry in the entire network (Warburg, 2016). The consensus mechanism is used to establish trust in the accuracy of the data in the system which is traditionally established by an intermediary or an administrator in a centralized system. A consensus mechanism is a process by which nodes in a distributed network agree on proposed transactions. This mechanism provides a way to record information in the ledger in a manner that ensures data integrity, immutability and consistency. Consensus mechanisms are distributed network governance rules and protocols that enable the recording, completion and execution of transactions under certain conditions. Therefore, a consensus can be built upon the previous transaction, forming a sequence of transactions, similar to a ledger. In blockchains, multiple transactions are clustered into a block which mathematically refers to the previous block. In the case of Bitcoin, after a set time, a new block is created with the occurred transactions included in the block and validated across the network. This forms a chain of blocks: hence the name 'blockchain'.

The Bitcoin blockchain was the first mechanism that implemented this decentralized, distributed ledger of cryptocurrency transactions — yet many alternatives have been introduced since. While the term "blockchain" refers to a specific technology stack, it is also increasingly used to refer to a loosely combined set of technologies and processes that span middleware, database, security, analytics/artificial intelligence (AI), and monetary and identity management concepts. Blockchain is becoming the common shorthand for a diverse collection of distributed ledger products (Gartner, 2018c) .

Another key feature leveraged by multiple blockchains are smart contracts. Smart contracts are pieces of software that execute a specified action based on the state of the system or a transaction that occurs. A smart contract is a computer program or protocol that facilitates, verifies or executes the terms of a contract (Gartner, 2018b). Smart contracts operate on a decentralized ledger. They are independent from human intervention and execute automatically. Smart contracts can be seen as private regulatory frameworks – a system of rules that govern transactions between interested parties. Once established, smart contracts are irrevocable and binding, triggering, yet unresolved, problem of handling damages caused by improper operation or errors in code.

As stated earlier, blockchain technology is the most commonly known distributed ledger technology. Although the two concepts are often used in an interchangeable manner, there is a clear difference in the two concepts. Blockchain is a distributed ledger technology that stores the transaction details in blocks that are sequentially linked, whereas in other distributed ledger technologies this does not necessarily have to be the case. The following definition of blockchain technology is used in this report:

“Blockchain is a type of distributed ledger in which value exchange transactions (in bitcoin or other token) are sequentially grouped into blocks. Each block is chained to the previous block and immutably recorded across a peer-to-peer network, using cryptographic trust and assurance mechanisms. Depending on the implementation, transactions can include programmable behaviour.”

Key benefits of blockchain technology

Blockchain technologies offer new algorithm-based mechanisms to establish and manage trust across entities. As the cost of providing algorithmic trust is likely to be much lower, these technologies can be impactful for interactions between citizens, businesses, and governments. Real life transactions typically suffer from a huge trust deficit and in most cases require costly monitoring, reputation checks or third party intermediation. The technical characteristics of blockchain present a number of key generic benefits that are widely regarded to occur in most of domains.

1. A distributed ledger shares content across multiple parties. This shared nature makes transactions easily trackable and full disclosable even in large and complex ecosystems.
2. The physical decentralisation of the storage of transaction details is argued to provide security integrated into the design of the technology stack. This feature eliminates the risk of a single point of failure, where one node is critical for the operation of the network and vulnerable for cyber-attacks.
3. New entries are recorded in an append-only manner and linked to the previous transactions. The entries cannot be changed, which safeguards data integrity on the ledger.
4. Transactions are verified via a peer-to-peer consensus mechanism ensuring a common truthful ledger. Centralized parties are no longer needed to assure transaction validity. As a consequence, blockchain shifts power from an intermediary towards the ecosystem. This decentralisation of control and power establishes ownership of the nodes and introduces checks and balances ingrained in the technology stack.
5. The combination of a distributed, append-only ledger and a consensus mechanism is argued to present disintermediation: the elimination of middle-men or brokers and remove any middle-men or broker-related transaction costs.

1.2 Blockchain and digital governments

Digital government is the state-of-art paradigm in public administration science. The former, much narrower, concept of e-government acknowledged the role of digitalisation as an input or enabler of modernisation of the public administration. Digital government takes a step ahead and focuses on the provision of user-centric, agile and innovative public services. These services and service delivery models should leverage digital technologies and governmental and citizen information assets. Blockchain definitely is the one of the most innovative digital technologies that has to be considered under the new paradigm of governmental policy making and service delivery. The main benefits of applying blockchain technology in governments are claimed to be:

- Reduced economic costs, time and complexity in inter-governmental and public-private information exchanges that enhance the administrative function of governments.
- Reduction of bureaucracy, discretionary power and corruption, induced by the use of distributed ledgers and programmable smart contracts.
- Increased automation, transparency, auditability and accountability of information in governmental registries for the benefit of citizens.
- Increased trust of citizens and companies in governmental processes and recordkeeping driven by the use of algorithms which are no longer under the sole control of government.

In the context of digital government, blockchain technology has a potential of facilitating direct interactions between public institutions, citizens and economic agents. At the most basic level, this implies improved public services in information registration and exchange processes. Blockchain technology is a combination of several existing, but distant, technologies that form a new decentralised information infrastructure. Decentralisation of blockchains is the core feature that can reshape the way governments interact with citizens and with each other (Atzori, 2015). Blockchain technology could take away a large part of the administrative tasks that governments fulfil in society nowadays. Governments possibly do not have to provide, on their own, information storage and information exchange processes in order to facilitate economic activities in societies, as

this could be provided by blockchain protocol. Instead, they should maintain a supervisory role with regards to the transactions taking place in this infrastructure.

Blockchain technologies can potentially be used as an information infrastructure for exchanging information between public administrations. For example timely and reliable exchange of criminality information, the distribution of grants and the exchange of information regarding academic degrees or taxes could be facilitated by blockchain (Davidson, De Filippi, & Potts, 2016). Distributed registration of documents and assets, instead of solely registering in a centralized way, is argued to bring several technical and economic advantages. Greater transparency, reliability and improved performance are in particular important when applications require data from multiple sites, organizations or countries. On the contrary, the distributed nature of blockchain systems is expected to create uncertainties regarding the stability in the network, as it removes one point of control. For example, whereas in the banking system banks act as centralized intermediaries in control of the system, in a blockchain-based system the power in the network is distributed among all the participants. Decentralisation is, to a certain extent, challenging, as it is incompatible with institutional structures of governments, corporations and marketplaces, as we know them today. Therefore, especially governments should consider the governance and organizational impacts of blockchain implementations, given their fundamental differences with traditional information infrastructures. It is argued that in order to fully harness the potential of blockchain in the public sector, administrative processes and governmental structures will have to be re-engineered to adapt to the technology and not the other way round.

Blockchain technology is also promising from the citizen-centric perspective. In particular, citizens can experience economic benefits and efficiency gains from services that leverage smart contract automation or notarization, such as personal certificates or land titles issuance (Atzori, 2015; Norta, 2015; Swan, 2015; Van Zuidam, 2017). Moreover, services drawing on decentralised nature of blockchain, such as identity or voting, change a balance of power, increasing the ownership and control of citizens over democratic processes.

Given all these benefits and challenges, blockchain technology can disrupt the status quo in the public sector. Blockchain can bring efficiency by spanning siloes, flattening tiers and inspiring new service delivery models for governments. The architectural set-up of blockchain can also reduce operational risk and transactional costs, increase compliance and increase trust in government institutions. However, the lack of mature, stable, commercial platforms, some gaps in essential functionality (e.g., smart contracts) and the lack of actual implementations within government indicate that this technology has yet to mature. Challenges often recognized are scalability, governance, flexibility and implementation styles.

Policy context

The relevance for the EU has been publicly recognized over the last two years by the European Commission (EC) and the European Parliament (EP). In order to “highlight key developments of the blockchain technology, promote European actors and reinforce European engagement with multiple stakeholders involved in blockchain activities” (European Commission, 2018c), the European Commission has launched the EU Blockchain Observatory & Forum. In addition, the EC has been funding blockchain projects through research programmes FP7 and Horizon 2020 since 2013, and projects can be funded up to 2020 with funds accumulating to €340 million. For governments, the EC has identified the following use cases (European Commission, 2018d):

- Citizens’ ID management;
- Taxation reporting;
- Development aid management;
- eVoting;

- Regulatory compliance.

Recognizing that blockchain technology may bring great improvements for Europe, not only for the private sector but also for the public sector, the EC and the EP believe that blockchain enables the provision of more efficient and new services by:

- The improvement of business processes for governmental actors at any level of government;
- Enabling new distributed business and interaction models for citizens without centralized platforms, intermediaries or institutions (European Commission, 2018b);
- The creation of fast, cheap and especially secure public records (Boucher, 2017).

In addition, blockchain systems could also facilitate the Once Only Principle (OOP) announced by the European Commission in eGovernment Action Plan for 2016-2020 (European Commission, 2016). The OOP mandates that citizens, public administrations and companies must only enter information once to access public services across the EU. Shared, decentralised database of credentials presumably could provide a technical solution for the OOP and hence contribute towards increasing the efficiency of the Digital Single Market.

As stated in the European Council conclusions of 19 October 2017, blockchain is a key emerging trend that the European Union should foster, while “ensuring a high level of data protection, digital rights and ethical standards” (European Council, 2017) The European Union agrees about the potential of blockchain technology to enhance the effectivity of digital governments and regards blockchain technology to have the potential to be a key backbone component of a world-class trusted data economy infrastructure. To foster innovation in this area, the EU should focus on setting the right conditions and boundaries for developing blockchain technology that digital governments can use to provide, open, trustworthy, transparent and compliant public services. In order to define the right approach for identifying those conditions and boundaries, a deep dive into the current state of play is needed. The current report attempts to fill this knowledge gap.

1.3 Value added and composition of this report

The vast majority of studies focus on potential applications in particular domains, like logistics, education or payments by analysing use cases. Speculative approach is valid as an initial step in exploration of emerging technology. It has however very limited value for assessing actual take-up of the technology, identification of the most beneficial implementations and formulation of policy agenda.

Growing experimentation and piloting with distributed ledgers and the emergence of first projects that already reached the production phase provide an opportunity to analyse the potential of blockchain based on the first pieces of empirical evidence. Our study adopts such an empirical approach to analyse the potential of blockchain in the public sector. We have collected data on seven projects that are being deployed in Europe. They all relate to public services and have public authorities participating in the project consortia. This study is among the first ones that take a focus on the public sector. Existing research mostly looks at applications of blockchain in business and financial sectors.

In the current study a new analytical framework is adopted that focuses on institutional, functional, technical and economic aspects of each project and enables comparative analysis. With this approach we can gain insights into the adoption of blockchain technology in the public sector with regards to the composition of blockchain functionalities, consortium governance, network architecture or a ledger protocol.

The report is structured in three chapters. In chapter 2 an analytical framework is proposed and seven blockchain deployments are individually presented and then compared, highlighting the key similarities and differences between projects and technical designs. Chapter 3 explores the potential of each service to be scaled up. Chapter 4 presents main conclusions and discusses recommended policy agenda.

2 Empirical analysis of blockchain projects

2.1 Methodology

The analysis is based on data collected from structured interviews with the representatives of the project teams. The interviews are complemented with the information from a desk research. Given the specificity of the data sources used for this study, our methodological choice is a case study analysis. A customized assessment framework was developed to facilitate a collection of field data and a comparative analysis of case studies.

2.1.1 Selection of projects

The initial list of candidate projects was created based on several publicly available sources: enterprise reports, expert blogs, news articles, academic papers and highlights from conferences and events on blockchain in the public sector. After restricting the list to projects that are implemented in Europe and last for at least six months, the number of available projects already fell down to twelve. This number was already close to the limit of maximum ten case studies for detailed investigation in the study. We wanted to ensure sufficient variety in the sample not only along geographical dimension, but more importantly also with respect to the type of public service and the level of government involved. The selection of ten projects was done according to three criteria:

- Field of implementation;
- Country of implementation (restricted to European countries, both the EU and non-EU);
- Level of government involved in the project (local vs national).

It is important to note, that some of the projects have been implemented by the international consortia in which technological partners do not necessarily have European origins. Therefore we classify projects by the country of implementation. The composition of consortium served also as a basis for the application of a third criterion. We allowed only those projects in which an agency representing local or the national government was officially listed among partners.

After checking for the availability of team representatives to participate in the interviews within the time frame foreseen in the study, we had to restrict the sample to seven projects, listed in Table 1 below. Our final sample contains the projects representing:

- Three broad service groups: public aid and social transfers; citizen's records and public registries; foundational components (identity and regulatory compliance);
- Six countries: Georgia, Luxembourg, Malta, Netherlands, Sweden and Switzerland;
- Two government levels: national and local.

The selection of projects does not exhaust all potential implementation fields in the public sector which are associated with blockchain technology. For example, voting and taxation are not covered in the analysis due to the lack of ongoing projects. The fact that blockchain is immature for large scale implementations seemed to affect experimentation choices of the project consortia.²

2.1.2 Assessment framework

Every project consists of a particular blockchain-based service and an institutional structure which develops it. To ensure comparability of collected data among projects and also generalizability of results, a customized case study assessment framework has

² An example of a large-scale use case is discussed in the Annex. We provide an overview of the VAT anti-fraud use case, discussing potential benefits and technological hurdles related to its implementation.

been developed, as presented in Figure 1. In the framework we have accounted for several elements covering institutional, functional, technical and economic aspects of each case study. These aspects can be grouped into four layers. We elaborate upon each layer below. During data collection phase, this framework has been transferred into a structured interview format. Prior to an interview with a representative of the particular developing team, a desk research has been conducted on the project. For the sake of completeness and correctness of information, in most cases interviews have been complimented with an additional file providing detailed figures on economic data. In this chapter we first present a more detailed overview of each project (Section 2.2) and then turn to the horizontal comparison of case studies (Section 2.3).

Table 1. List of blockchain projects

Project No	Project Name	Country of implementation	Field of implementation	Level of government involved
1	Exonum land title registry	Georgia	Land title registry; property transactions	National
2	Blockcerts academic credentials	Malta	Academic certificates verification; personal documents storage and sharing	National
3	Chromaway property transactions	Sweden	Property transactions; transfer of land titles	National
4	uPort decentralised identity	Switzerland	Digital identity for proof of residency, eVoting, payments for bike rental and parking	Local (Municipality of Zug)
5	Infrachain governance framework	Luxemburg	Blockchain governance	National
6	Pension infrastructure	The Netherlands	Pension system management	National
7	Stadjerspasm smart vouchers	The Netherlands	Benefit management for low-income residents	Local (Municipality of Groningen)

Source: Own elaboration.

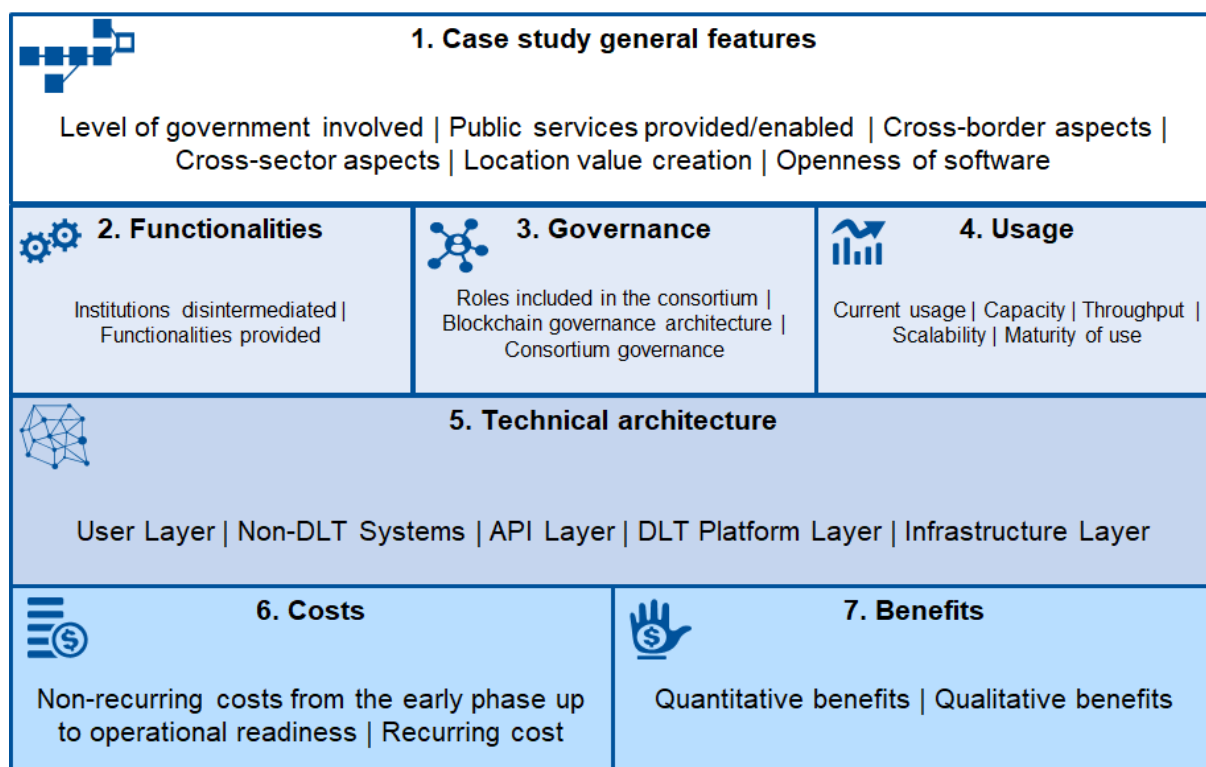
Project characteristics

This includes the country or countries a project caters to and the level of government that is involved. Also, the services provided or enabled by the blockchain pilot are described. This element of the assessment framework also investigates if the pilot deployment applies to multiple sectors and multiple countries. The way location creates value in the blockchain service is also described. Location can bring value in form of personalization, creation of a location-based community or intelligence. Lastly, this element of the assessment framework describes the openness of software developed for the implementation of blockchain in the public service. The openness of software can range from completely open source to completely proprietary.

Functionalities, governance and usage

The second layer of the assessment framework identifies the functionalities provided by the blockchain-based service, the governance structures of both project consortium and blockchain protocol, and the current usage of the blockchain service. For the functionalities, the functions executed by the blockchain platform, like for example a proof of provenance, an automatic execution of transactions or an identity check are listed. We also investigate the extent to which the blockchain solution can disintermediate existing public services and institutions.

Figure 1. Case study assessment framework



Source: Own elaboration.

Regarding the governance model adopted by a given blockchain architecture, we distinguish four archetypes which differ with respect to the openness of transaction validation (validate/commit) and the openness of participation (read/write) in the transactions:

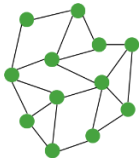

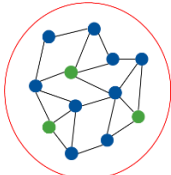
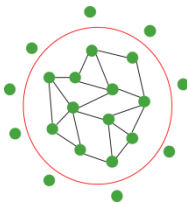
- A blockchain architecture where anyone with the right hardware is able to validate or commit transactions is called *permissionless*.
- A blockchain architecture where only a number of selected nodes can validate or commit transactions is called *permissioned*.
- A blockchain architecture where anyone can participate in transacting using the protocol is called *public*.
- A blockchain architecture where only selected participants can participate in transacting using the protocol is called *private*.

In general, four major blockchain types can be distinguished: public permissionless blockchains, public permissioned blockchains, private permissioned blockchains and private permissionless blockchains of which Table 2 provides an overview. The green dots are the validating nodes, meaning that they are able to validate the transactions in the system and participate in the consensus mechanism.³ The blue dots represent participants in the network in the sense that they are able to transact, but they are not able to participate in the validation mechanism. The blue dots denote users that are not participating in the consensus mechanism. A red ring indicates that only the nodes within the ring can see the transaction history. The visualizations without a ring mean that

³ In distributed networks, consensus mechanism is needed to maintain a unique version of a ledger shared between all nodes. In blockchain systems a validator of the next block of transactions is either a single node or the decision is taken by voting. Consensus algorithms differ in ways this single node is selected for a period of time. Public blockchains use some form of a random assignment, while private blockchains (with known nodes) may appoint validators in a systematic manner, for example cyclically or apply voting.

everyone with a connection to the internet is able to see the transaction history of the blockchain.

Table 2. Blockchain archetypes

Blockchain type	Explanation	Example	Visualization
<i>Public permissionless blockchains</i>	In these blockchain systems, everybody can participate in the consensus mechanism of the blockchain. Also, everyone in the world with a connection to the internet is able to transact and see the full transaction log.	Bitcoin, LiteCoin, Ethereum	
<i>Public permissioned blockchains</i>	These blockchain systems allow everyone with a connection to the internet to transact and see the transaction log of the blockchain, but only a restricted amount of nodes can participate in the consensus mechanism.	Ripple, private versions of Ethereum	
<i>Private permissioned blockchains</i>	These blockchain systems restrict both the ability to transact and view the transaction log to only the participating nodes in the system, and the architect or owner of the blockchain system is able to determine who can participate in the blockchain system and which node can participate in the consensus mechanism.	Rubix, Hyperledger	
<i>Private permissionless blockchains</i>	These blockchain systems are restricted in who can transact and see the transaction log, but the consensus mechanism is open to anyone.	(Partially) Exonum	

Source: Own elaboration.

The consortium governance is defined based on the high-level set-up, ranging from a centralized to a decentralized governance structure. The governance structure refers to the way the project is controlled and directed. Decentralized governance means that all consortium stakeholders have an equal say in the decision-making and centralized governance means that a central party has the ability to take decisions on the direction and implementation of the service deployment.

Usage aspect examines the total amount of users currently transacting in the project. The assumed throughput and the actual number of transactions per second in the pilot are also collected. The teams were also asked to provide information on the system capacity, understood as a number of users that the blockchain system can comfortably facilitate. Capacity has to be taken into account for service scale-up considerations.

Technical architecture

For the description of the blockchain technical architecture we use a layered model. This hierarchical framework differentiates between DLT and non-DLT systems involved and for the DLT part recognizes four vertical blocks, starting from infrastructures and protocols and finishing on APIs and user applications.

Costs and benefits

The fourth element of the assessment framework analyses the costs and benefits involved in the development and operation of a blockchain service. The total cost is separated into non-recurring and recurring categories. Non-recurring costs include research and development (R&D), project management, acquisition of hardware, acquisition of software, installation, integration, test and validation cost. The recurring costs include staff and operation and maintenance cost.

For the benefits, a distinction between quantitative and qualitative benefits is made. Quantitative benefits include:

- Cost savings, for example a reduction in a cost of registering a single transaction compared to the current system;
- Capacity gains, such as an increased volume of registered transactions per unit of time;
- Efficiency gains, such as a reduced time of completing a transaction compared the current system.

Qualitative benefits include:

- Reliability gains, for example a decreased risk of cyber-attacks, system breakdowns or leakage of sensitive data;
- Environmental benefits, such as reduced energy needed to keep the system running;
- Improved accountability and incorruptibility, such as an increased transparency and traceability of transactions and the current state of the system.








The relatively early stage of experimentation and the nature of data we have collected make it impossible to conduct a systematic analysis of business and project risks. In particular we could not provide quantitative assessment of the reduced risks. Such analysis can be carried out in future, when data from more projects becomes available.

2.2 Individual case studies

In this section we present a detailed overview of each of the seven projects investigated in this study.

2.2.1 Exonum land title registry – Georgia

Figure 2. Resume of Exonum case study

 Land title registry in Georgia									
1. General features									
Level of government involved	Public services provided/enabled	Cross-border aspect	Cross-sector aspects		Location value creation	Openness of software			
National	Land title registration and verification	None	None		Location is the product	Open source			
 2. Functionalities		 3. Governance			 4. Usage				
Institutions disintermediated	Functionalities provided	Roles included	Blockchain governance architecture	Consortium governance	Current Usage	Capacity	Throughput	Scalability	Maturity
None	Provenance (notarization)	Government; OS community; tech provider	Public permission-less; private permissioned	Centralized (NAPR)	Over 100k titles	Unknown	Unknown	5000 tps for private blockchain	Production
 5. Technical architecture									
User Layer	Non-DLT Systems	API Layer		DLT Platform Layer		Infrastructure layer			
Admin NAPR application	NAPR Land Title Registry system	Admin API to Land Title Registry		Private consensus for private blockchain and PoW		Known nodes & Bitcoin blockchain			
 6. Costs					 7. Benefits				
Non-recurring costs		Recurring costs			Quantitative benefits			Qualitative benefits	
Organizational capacity cost; developments cost		Bitcoin transaction fees; operation cost			400 times faster registration of extract; 90% reduction of operational costs			Improved transparency; fault-tolerance and intelligibility	

Source: Own elaboration, based on data reported by the project team and desk research.

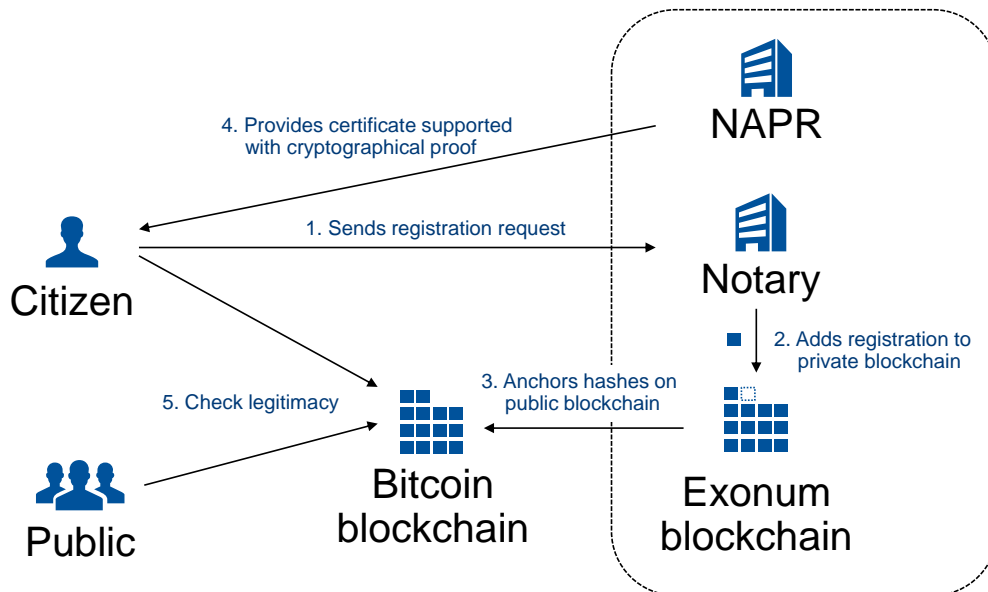
The National Agency of Public Registry (NAPR) of the Republic of Georgia uses blockchain technology to provide its citizens with a digital certificate of their land title. It does so by adding the cryptographical proof that the transaction is published on the Bitcoin blockchain. NAPR partnered-up with Bitfury Group, who provides solutions based on the Bitcoin protocol, and the project started in April 2016 (Bitfury Group, 2017). It helps Georgia fight corruption and resolve disputes over property claims (Eurasianet, 2017). The aim of using blockchain is to increase public confidence in the property-related record-keeping.

The process of adding or changing a land title can be characterised by the following steps, displayed in the figure below.

1. A citizen can initiate a request to the service-hall or a notary for the registration or verification of a land title extract, just as in the traditional system.
2. The notary registers the land title on the private Exonum blockchain.
3. Hashes of the private Exonum blockchain are anchored on the public Bitcoin blockchain. This guarantees the integrity of all transactions in the Exonum blockchain, up to the latest anchored block in the Bitcoin blockchain.
4. NAPR provides the citizen a digital certificate of their asset, supported with the cryptographical proof of the originality of the extract, published on the Bitcoin blockchain.

- The only difference from a citizens' perspective is that they can now check if a land title is legitimate. This can be done by any Georgian citizen.

Figure 3. Land tile registration process by NAPR



Source: Own elaboration, based on data collected from project teams and desk research.

Functionalities

Blockchain technology is used by citizens to validate property-related certificates and by notaries to make new registrations. At the moment of writing (Q2 2018) the service allows for the registration of purchases and sales of existing land titles and a registration of new land titles. In the future, the system will be extended to a registration of property demolitions, mortgages and rentals and notary services (Shin, 2017).

Governance

Only NAPR, notaries and Georgian citizens can participate in transacting, so it is a permissioned blockchain. The blockchain system is private with regards to who can validate the transactions. The actual transaction validation occurs by a group of known servers or nodes. The transaction data is then hashed and recorded on the public Bitcoin blockchain, which creates transparency of the existence of the land title for all citizens. Therefore the system is a mix between a public permissioned and private permissioned blockchain. This hash is a cryptographic proof that transaction details match with the data recorded on the private blockchain, without actually seeing it. The consortium governance is centralized, as NAPR can decide on the direction of the consortium and Bitfury is the technology provider.

Usage

The blockchain-based land title registry implementation is mature, meaning that the verification of the transaction occurs via the public blockchain network. Since April 2016, over 100,000 land titles have been registered using the technology. The Exonum protocol can handle up to 5000 transactions per second (tps) between the private nodes. Hence, the adopted blockchain solution does not have bottlenecks related to registration.

Technical architecture

The Exonum Framework is used to facilitate the project, which allows organisations to build a permissioned private or public blockchain while still maintaining the security and

auditability that the Bitcoin blockchain provides. This framework allows actors, in this case notaries across the country, to validate the information on the client-side using light clients. It also stores the hashes on the Bitcoin network, making it impossible to change. The software is fully an open source. The Exonum framework is connected with the Admin NAPR application using Exonum's user API.

Private data is not stored on the public Bitcoin blockchain itself. What is stored on the public Bitcoin blockchain is a hash of the state of the system. Every full node of the private Exonum blockchain (NAPR and the notaries) has an exhaustive and actual copy of data. The private Exonum blockchain uses an authenticated consensus mechanism similar to the Practical Byzantine Fault Tolerance (PBFT). Only one node is needed to restore a blockchain in case of corruption of the nodes. This blockchain system is fully integrated with the digital land title record system of NAPR. The land titles are stored in a centralized database only. A private blockchain stores registration details sent by the notary nodes and location details of the titles in NAPR. On the roadmap of the project there is an implementation of smart contract functionality, in order to execute, amongst others, escrow services.

Costs and benefits

This blockchain deployment offers a mixture of quantitative and qualitative benefits:

- A significant reduction of the land title registration and verification time. Whereas in the past these actions took around 1 to 3 days to process, the transaction time using blockchain has been reduced to a matter of minutes;
- Increased transparency in the registration process of land titles;
- Increased reliability for citizens driven by the accuracy of the data stored at NAPR;
- Efficiency gains realised in the ecosystem, as the time to verify a certificate has been reduced from a matter of days to a matter of seconds;
- Operational costs were reduced up to 90% for the land title registering service.

The costs involved in the implementation of the new system are mainly non-recurring, related to the customization of Exonum protocol and the integration with NAPR and the notaries. These costs, borne by NAPR, include:

- The development cost of a custom-built protocol based on the Exonum framework. There was no hardware cost, as NAPR did not need to buy additional infrastructure;
- The maintenance and operation costs of Exonum blockchain;
- The organisational capacity cost to prepare NAPR to understand and utilize blockchain technology;
- Transaction cost related to anchoring transactions on the Bitcoin blockchain. As transactions are anchored in groups, fees are paid not on per transaction basis but periodically.

The actual levels of these cost items were not disclosed. Citizens are not charged any extra fees. It is noteworthy, that several cost items that existed in the old system are still present, as the blockchain system does not substitute the legacy solution. These items are related to the maintenance of a central digital record system. Also the check-up of a request initiated by citizens is still manually done by a notary.

Key takeaways

- As stated by the project representative, the main value added of using a blockchain technology in this particular implementation is the increased security and reliability of digital certificates.
- The blockchain system does not provide any disintermediation of organisations nor replaces any existing system. It merely provides a new functionality on top, in the

form of an additional assurance to citizens. For this reason the integration with legacy systems was relatively easy.

- Verification of certificates is made on a public blockchain, which is beyond control of any participant or a group of participants. This independent and incorruptible layer helps to combat frauds and cease land title disputes.
- The ease of implementation and the success of the blockchain-based system have been facilitated caused by the organizational and political autonomy of NAPR in the Republic of Georgia.
- Under the Georgian law, the land title data is by definition public. This legal provision considerably helped the implementation the blockchain technology.
- Another success factor is user agnosticism. Citizens interact via a convenient web interface and do not need to know anything about blockchain to use the service.
- Currently the Exonum framework is used, but to avoid lock-in to the Bitcoin blockchain, NAPR is exploring alternative public blockchain platforms.

2.2.2 Blockcerts academic credentials – Malta

Figure 4. Resume of Blockcerts case study

Academic credentials in Malta									
1. General features									
Level of government involved	Public services provided/enabled	Cross-border aspects	Cross-sector aspects	Location value creation	Openness of software				
National	Certificate verification	Yes	Business – Education	Location is static	Open source				
2. Functionalities		3. Governance			4. Usage				
Institutions disintermediated	Functionalities provided	Roles included	Blockchain governance architecture	Consortium governance	Current Usage	Capacity	Throughput	Scalability	Maturity
Certificate verification office at university	Provenance (notarization)	Government; OS community; tech provider	Public permissionless	Hybrid – various consortium partners	Hundreds	Unknown	3 tps (Bitcoin)	3 tps (Bitcoin)	Early stage pilot
5. Technical architecture									
User Layer	Non-DLT Systems	API Layer		DLT Platform Layer		Infrastructure layer			
Wallet (mobile app) and issuer software	Certification database of institutions	Blockchain APIs for confirmation and searching		Proof-of-Work		Bitcoin blockchain			
6. Costs					7. Benefits				
Non-recurring costs		Recurring costs			Quantitative benefits			Qualitative benefits	
Integration cost; development cost		Transaction costs on blockchain; maintenance costs			Lower administration costs			Citizens' ownership; convenient storage and selective sharing	

Source: Own elaboration, based on data collected from project teams and desk research.

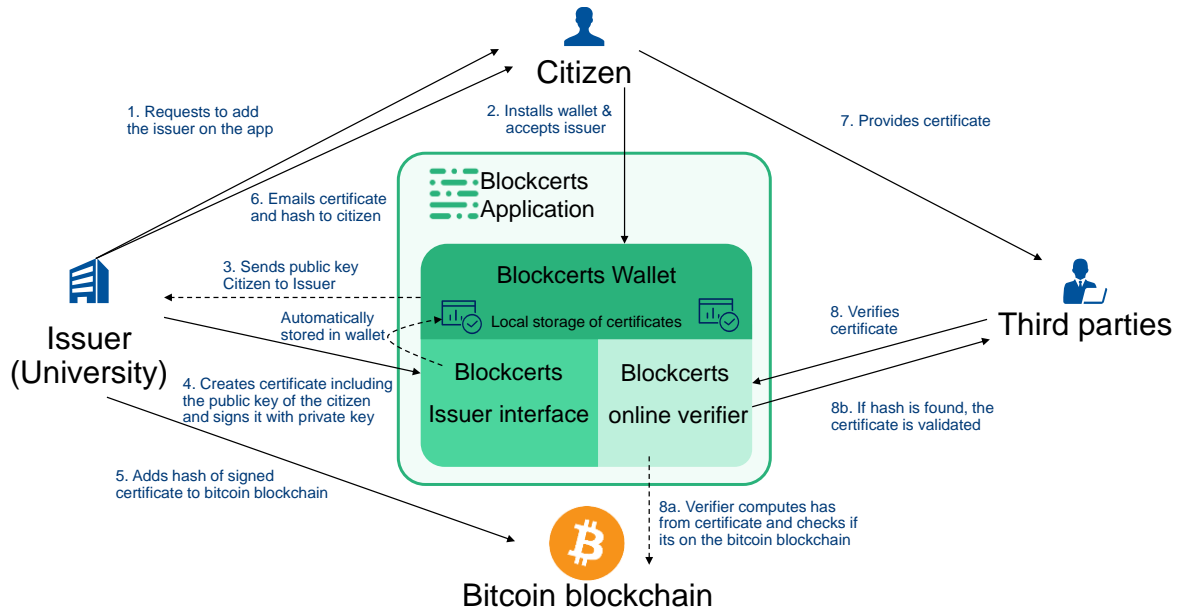
In October 2017, the Maltese government has launched a project that develops academic credentials verification using blockchain technology. The Ministry for Education and Employment (MEDE) of Malta decided to use the Blockcerts open standard for management of academic records. Blockcerts provides all aspects of the value chain: creation, issuing, viewing, and verification of the certificates, and uses blockchain technology as the infrastructure. The pilot was initiated to create a verifiable proof of education for citizens (Commission, 2017).

The Blockcerts open standard was developed in 2015 by Massachusetts Institute of Technology (MIT) and Learning Machine – a startup focussed on blockchain-based credentialing systems. The issuance and verification process of an academic certificate, using the Blockcerts system, consists of the following steps (Grech & Camilleri, 2017):

1. Academic institution sends a request to its alumni to download the Blockcerts app and add them as an issuer
2. A citizen (graduated person) installs a wallet and accepts the issuer. While doing this, the wallet generates a private and public key.
3. Because the citizen has approved the issuer as a provider of certificates, the Blockcerts app sends her public key to the issuer
4. The issuer creates a digital certificate including the public key of the citizen in the Blockcerts issuer interface application. This certificate is signed with the private key of the issuer. Once the certificate includes the public key of the citizen, it is automatically saved in his Blockcerts wallet.
5. The issuer hashes the certificate in the Blockcerts issuer environment and saves the hash on the Bitcoin blockchain.

6. The issuer emails the certificate to the person, including the Blockcerts URL which refers to the hash stored on blockchain.
7. The person can provide third parties with the electronic certificate and the URL.
8. A third party (ex. potential employer) enters the certificate and the URL in the Blockcerts online verifier, which checks if the hash of the provided certificate matches with the hash on the Bitcoin blockchain, specified in the URL. If the hash is found, the certificate is validated. The third party now has proof of originality of the document.

Figure 5. Blockcerts certificate verification process



Source: Own elaboration, based on data collected from project teams and desk research.

Functionalities

The functionalities provided in the project include the issuance of academic credentials, the verification of certificates, and the storage of personal credentials in the user app. The Blockcerts app provides a wallet where the citizen has a full ownership of his records. System allows a citizen to control which third parties can see his academic records and verify their originality. Verification can be done via the Blockcerts universal verifier⁴, which is a webpage accessible for all. By providing the URL of the certificate, one can verify the validity of the certificate, the owner of credentials, the issuing date, the issuing institution and the transaction ID.

Governance

From a governance perspective, the consortium involved is hybrid. The MEDE is the instigator and sponsor of the pilot, but many several other parties are involved in the project. The consortium includes the Malta College of Arts, Science and Technology (MCAST), and the Institute of Tourism Studies (ITS). Learning Machine is a technological partner that implements the Blockcerts code. The Maltese project develops an application layer on top of the public permissionless Bitcoin blockchain. Anyone that has credentials of one of the consortia partners can use the service. The verification of the certificates is

⁴ Accessible via <https://www.blockcerts.org/>

done by the Blockcerts universal verifier and hash verification is done on the public Bitcoin network.

Usage

The Blockcerts open standard is still being developed and because of that the pilot project launched by the Maltese government has a small scale. It only includes two educational institutes and their students. The verification software is implemented in both institutions and the Blockcerts wallet gives control over the certificates to the students. Over a hundred credentials have been issued at the moment of writing (Q2 2018). The number of verifications performed by third parties is unknown. Scalability is dependent on the chosen blockchain platform. The Blockcerts standard issues hashes on the blockchain in batches, which allows for scalability even on the Bitcoin platform. The throughput of Bitcoin is currently seven transactions per second, but batching allows a greater amount of throughput.

Technical architecture

Blockcerts consists of open source libraries, tools, and mobile apps for creating, storing, sharing and verifying personal certificates. The private blockchain network will be composed solely of the certified institutions that participate in registering academic certificates using Blockcerts solution. The standard leverages public blockchain, as it anchors hashes of the certificates on the Bitcoin blockchain. The DLT layer of the solution currently uses the classical Proof-Of-Work consensus mechanism among anonymous nodes. Learning Machine attempts to develop the integration of their standard with multiple blockchain platforms, yet currently only the Bitcoin blockchain is used. This is largely caused by the fact that when Blockcerts started up in 2015, Bitcoin was the only stable blockchain platform. Currently, however, much of the community effort goes into creating Ethereum interoperability as well based on the open components for creating, issuing, viewing, and verifying certificates.

Cost and benefits

The benefits of the blockchain pilot for end users include:

- Citizen's ownership of credentials as the Blockcerts application allows for a greater control over his educational achievements and certificates.
- Self-sovereignty. The permission to share is placed at the citizens instead of the issuing institution.
- Identity and privacy protection. The citizens can choose to share certain certificates with specific institutions.
- Convenient storage and sharing, quick verification of certificates. Hard copies are not needed anymore and the risk of using a fake certificate is eliminated.

The benefits for the educational institutions include:

- An easy integration with the existing academic record-keeping systems, using the Blockcerts APIs. APIs integrate the back-end of existing systems with the Blockcerts application. As a result digital certificates can be automatically created without any additional administrative tasks for the issuer. Also third parties may use APIs to automatize credential verification process.
- The main benefit of having an open standard is that other organisations or countries can build their own verifier or credential issuing systems based on the standard, and be interoperable. A verifier system could, for example, perform automatic credential checks in a recruitment process for companies. A credential issuing system could automatically create verifiable credentials as is done in this pilot deployment
- The administration costs for educational institutions are lower as an institution does not need to be involved in future queries related to certificate copies or transcripts.

The costs involved in the project include:

- The cost of standard development. The Maltese government is willing to finance the development of the Blockcerts open standard, as it will benefit the society. The government intends to roll out this pilot for all academic issuing institutions, as well as expand to other types of credentials. A high priority use case currently investigated is the one where the Blockcerts system can help to store and verify certificates of refugees, such as their identity and interactions with authorities.
- The cost of service implementation and integration. The technology developer bears huge costs of building an automated credential process for various consortium partners. This is the main cost driver in the Maltese project.

Key takeaways

- For the Maltese government, setting up the pilot had a strategic dimension. The government wanted to be a frontrunner in developing and experimenting with the blockchain technology.
- The Maltese government was also driven by an ideologist element. A number of the key stakeholders believe in the notion of self-sovereignty and shifting the power into the hands of the learners instead of the institutions.
- The current use case is limited to academic credentials, yet the system itself could be extended to include multiple types of citizen records, such as birth certificates, marriage certificates, etc.
- The case is limitedly driven by the economic incentives to the issuers. Academic institutions have a little economic reason to change from the working centralized solutions. However, the benefits for citizens and third parties, such as an increased convenience and time savings are evident.
- The Maltese government is currently exploring the expansion of the current project to also include credentials for refugees. In this project, the Blockcerts open standards could be used for verification of identity and recording social aid obtained by refugees in the European countries.
- The legality of the blockchain-based issuance and verification of certificates is the main barrier to deploy this solution on an international scale.

2.2.3 Chromaway property transactions – Sweden

Figure 6. Resume of Chromaway case study

Property transactions in Sweden									
1. General features									
Level of government involved	Public services provided/enabled	Cross-border aspects	Cross-sector aspects	Location value creation	Openness of software				
National	Transfer of land title; facilitation of transaction	None	None	Location is the product	Proprietary				
2. Functionalities		3. Governance			4. Usage				
Institutions disintermediated	Functionalities provided	Roles included	Blockchain governance architecture	Consortium governance	Current Usage	Capacity	Throughput	Scalability	Maturity
Notaries	Smart contract automation;; shared database	Government; tech provider; banks	Private permissioned	Hybrid – various consortium partners	Unknown	Unknown	Unknown	160 tps	Proof of concept
5. Technical architecture									
User Layer	Non-DLT Systems	API Layer		DLT Platform Layer		Infrastructure layer			
Smart contract interface	Swedish Land Registry	Internode API; Client API and Legacy API		Proof-of-authority consensus		Storage is in PostgreSQL or another RDBMS			
6. Costs				7. Benefits					
Non-recurring costs		Recurring costs		Quantitative benefits			Qualitative benefits		
Integration effort; development costs		Transaction costs		Est. €100M. Reduced transaction time (over 95%) and cost (90%)			Increased transparency and security of trans; improved mortgage handling		

Source: Own elaboration, based on data collected from project teams and desk research.

In real estate the value at stake is high, highlighting the importance of security and transparency of property transactions. Currently, transaction settlement in real estate is slow, costly and exposed to various business risks, including contested property deeds. This project attempts to tackle both the distrust between parties in real estate transfers and the speed of transactions. The project was initiated in September 2016 by the Swedish Mapping, Cadaster and Land Registration Authority, Landshypotek Bank, SBAB, Telia, Chromaway and Kairos Future (Chromaway, 2017a). The project was set-up to redefine real estate transactions and mortgage deeds. It aims to address the main pain points of the current transacting system, which are:

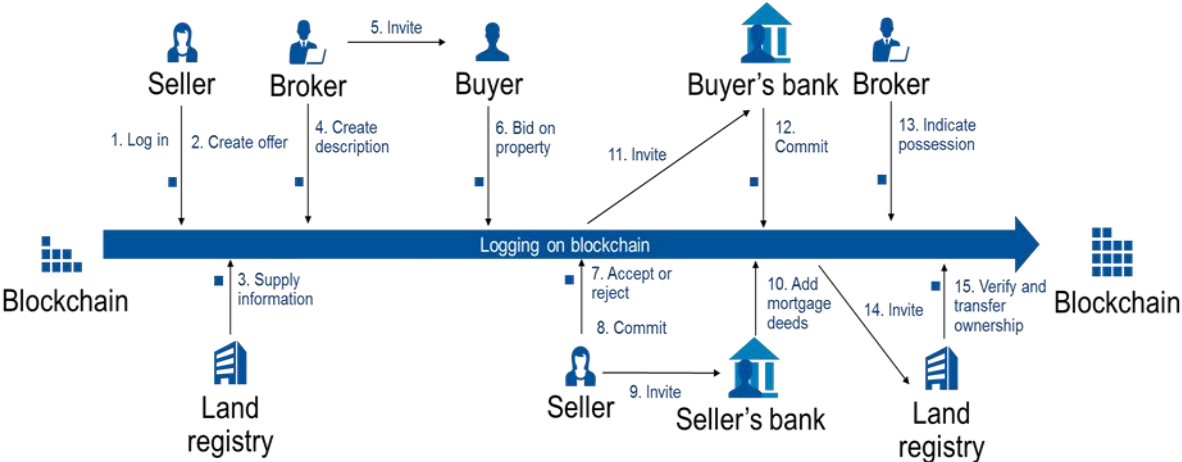
- The lack of transparency. The Land Authority is not involved in the transaction from the beginning, but enters only in the very end. A large body of documentation has to be reviewed in the final stage of the process, causing delays in the transfer of land title and uncertainties about the outcome of the transaction.
- A slow registration system. The approval of the title by the Land Authority may take up to six month.
- The complex process for agreements between buyers and sellers. Lack of trust in the system and the high value at stake increase transaction costs. Insurance safeguarding a transfer of the title is a typical example of transaction costs on the real estate market.

The underlying technology in this project consists of two main components: the blockchain platform and the smart contract workflow. The smart contract workflow enables an automatic processing of transaction by the participants. The blockchain system combines the capabilities of centralized, relational databases with private blockchains.

From a user perspective, the citizen logs into the Chromaway web browser, which allows for access to Esplix - the smart contract mechanism. Five types of actors are involved in the workflow: the buyer, the seller, the real estate agent, the banks and the land registry. The whole transaction process underlying a transfer of the property is described below and depicted in Figure 7:

1. A seller logs in to Esplix.
2. The seller wants to sell his property and does so by launching a smart contract and selecting the property he wants to offer.
3. Information about the property belonging to the seller, including its mortgage register, is supplied by the land registry.
4. A broker (real-estate agent) is invited into the workflow. He describes the property.
5. The broker then invites a buyer using the buyer’s public key.
6. The buyer bids for the property by providing the amount he wishes to pay.
7. The seller then accepts (or rejects) the price offered for the property.
8. Once the seller has accepted the price, the buyer has to commit to the transaction and proceeds to the agreement.
9. The seller then invites the seller’s bank into the workflow.
10. The bank can add the ordered collection of mortgage deeds.
11. The seller can now invite the buyer’s bank into the workflow, as the collection of mortgage deeds is received.
12. The buyer’s bank commits to transfer a payment of the agreed amount.
13. The broker now needs to indicate that the buyer has the physical possession of the property.
14. Then the land registry is invited to the workflow by the broker.
15. The land registry then checks whether all steps have been done properly and transfers the title.

Figure 7. Chromaway real estate transfer workflow



Source: Own elaboration, based on data collected from project teams and desk research.

Functionalities

The solution introduces a completely new blockchain-based workflow that streamlines and secures the process of transferring a property title. The system interfaces to the Swedish Land Registry which is responsible for storing land titles. The blockchain only stores the state of the system after the execution of each step in the workflow. In this way, the synchronization among participants involved in the transaction is ensured. There is one private element that is stored on blockchain: the seller's price. All data that is stored in a land title, such as the information on physical extent of the property and on the owner is public under the Swedish law.

Governance

The blockchain pilot is defined as a private permissioned blockchain. Transactions are validated by known nodes and the rights to transact and see the data are assigned only to the known users. The project uses the centralized ID system (Telia ID) to authenticate different users.

Usage

The blockchain pilot is, although the project has been around for two years, in a proof-of-concept phase. The consortium has the technology that works, but the technical solution it is not integrated into the environment of the real estate agents yet. Also, retrieving from blockchain is not automatic yet. These technical hurdles need to be overcome before the project moves to the experimentation phase. The blockchain system is based on a private blockchain set-up. Scalability is not an issue, as if the transaction volume goes up, the nodes can increase capacity by adding extra servers.

Technical architecture

This pilot uses a private blockchain system, which is a distributed database within the consortium (a cluster of nodes belonging to the Swedish Land Title Registry). The blockchain system is called Postchain. Postchain uses a relational database natively, which means that it can be directly integrated into a legacy system, removing any redundancy issues. Postchain uses PostgreSQL, and the capacity of this database is large enough to store all data on the blockchain. In order to meet laws and regulations, the identifying (personal) data is stored off-chain and is represented on the blockchain by a hash. The hash refers to the document containing the full information. The architecture includes smart contract functionality which splits a property transaction into a sequence of actions executed by different actors. A new action undertaken by a user triggers a new state of the smart contract, according to the predefined transition function. The message about each updated state of the system is added to the blockchain and shared among all transaction participants.

The user application layer currently contains web interfaces, yet there is also an API for users who want to move contracts forward in an algorithmic way (like banks). There is no admin application, yet monitoring applications can be deployed to view the activity in the system. There are three types of APIs provided in the system:

- The inter-node API for reaching consensus between the nodes;
- The client API that receives client-signed statements in a correct format readable by Postchain;
- The API for legacy systems that do not work with signed statements but with logins. For these systems Chromaway has defined an API server that is customized by partners in the project to interface between the legacy systems and a signed-statements system such as blockchain. These interfaces can be used by banks that want to automatically execute the loan granting process and update this into their legacy systems.

The consensus mechanism is Proof-Of-Authority (PoA) with the Practical Byzantine Fault Tolerance. Proof-Of-Authority is a mechanism that allows specific nodes to validate transactions, as they have the authority in the system. This consensus mechanism is only suitable for private blockchains, because it requires that the validators are known. Byzantine fault tolerance refers to a system that allows for a certain amount of nodes to fail. Chromaway uses PFBT, which ensures that even if one third of the nodes in the network are not functioning correctly, consensus will be achieved. Currently all nodes are located within the participating actors. Potentially banks/brokers will also become nodes, but citizens will not host nodes.

Costs and benefits

The benefits of the blockchain pilot include:

- Reduced transaction costs. Property transaction time drops from weeks to minutes or hours, depending on the speed at which parties execute their actions in the workflow. In particular, involvement of the Land Title Registry in the workflow drastically reduces title registration time and generates huge savings on title insurance cost. Currently, the cost of insurance safeguarding a real estate transfer can go up to 10% of the purchasing value. In the Chromaway system, this could be reduced to 1%. Other positive effects, such as elimination of paperwork and reduced risk of fraud also translate to economic gains.
- Improved market operation and increased liquidity of assets. Quicker and reliable workflow restores trust among participants of high value transaction. In the current setup, the risk of one party pulling out from transaction is significant throughout several weeks. In the smart contract workflow, once both parties agree to start a negotiation, they enter into an automatic commitment which rules out possible intervention of a third party.
- An improved resilience to any modifications to the storage system from external actors given the distributed nature of the blockchain platform.

The costs involved in the project include:

- Integration costs. To implement the system for all the stakeholders, a lot of effort goes into integration with legacy systems and making the system interoperable with the banking systems.
- Operation costs. Interestingly, from the perspective of the Land Title Registry, this cost item is expected to be higher comparing to the centralized database solution (Chromaway, 2017b). The increased cost is caused by the continuous replication of the consortium database that is a part of the blockchain protocol, whereas a centralized system would not need such duplication.

Key takeaways

- This project leverages more advanced functionalities of blockchain technology to automate execution of the real estate transactions. By providing a common workflow for various actors, several efficiency and economic gains occur. For citizens, there is no need for a physical presence in the bank or at notary. On a more systemic level, the new solution reduces paper work, risk of fraud and significantly reduces transaction costs.
- Automated workflow is enabled by using a private blockchain as a distributed database which stores anonymously transaction data submitted by different actors. Transaction data is shared among actors and stored securely in multiple nodes. The service however still relies on inputs from the centralized systems, such as the provision of property details and electronic authentication of users. In particular, electronic identity system must be attested by the government and linked to the specific natural or legal persons who want to enter into a property transaction.

- The smart contract workflow partially disintermediates traditional notaries. In the current system a notary verifies identities of the transacting parties, checks for authenticity of documents and signatures. A notary also verifies if the statements of the transacting parties are consistent with the real-world facts and expressed with a free will. In the new system these elements will be provided automatically in the electronic form. There are some doubts however about how the external consistency of electronically-submitted statements could be ensured, without an outside arbiter.
- At present, legal noncompliance constitutes a main hurdle for further roll-out of the system. Electronic signatures and user commitments are not yet recognized as legally binding in the real estate transactions. A new legislation is required in this respect.

2.2.4 uPort decentralised identity - Zug, Switzerland

Figure 8. Resume of uPort case study

Government-attested decentralised identity in Switzerland									
1. General features									
Level of government involved	Public services provided/enabled	Cross-border aspects	Cross-sector aspects	Location value creation	Openness of software				
Local	Proof of residency	None	Yes	Location is static	Open source				
2. Functionalities		3. Governance			4. Usage				
Institutions disintermediated	Functionalities provided	Roles included	Blockchain governance architecture	Consortium governance	Current Usage	Capacity	Throughput	Scalability	Maturity
None	Provenance (notarization)	Government; OS community; tech provider	Public permissionless	Hybrid – various consortium partners	About 300 people	30k	Unknown	7 tps	Early stage pilot
5. Technical architecture									
User Layer	Non-DLT Systems	API Layer		DLT Platform Layer		Infrastructure layer			
uPort (mobile app)	Front-end portal	uPort Connect API		Proof-of-Stake consensus		Ethereum blockchain. User data stored locally.			
6. Costs				7. Benefits					
Non-recurring costs		Recurring costs		Quantitative benefits			Qualitative benefits		
Integration and installation cost		Transaction costs; operation cost		Lower administration cost; lower storage cost			E-identity without a central administrator; citizen's control over data		

Source: Own elaboration, based on data collected from project teams and desk research.

The City of Zug has launched a government-issued identity on the Ethereum blockchain, called uPort. The aim of the project is to provide a trusted and self-reliant blockchain-based identity to authenticate for e-government services and share personal data with third parties. The project itself does not focus on developing public services that would use the blockchain-based identity. From the citizen's perspective the Uport service allows for a selective disclosure of specific information to particular companies or governmental institutions giving citizens a full control and de facto ownership over their personal data.

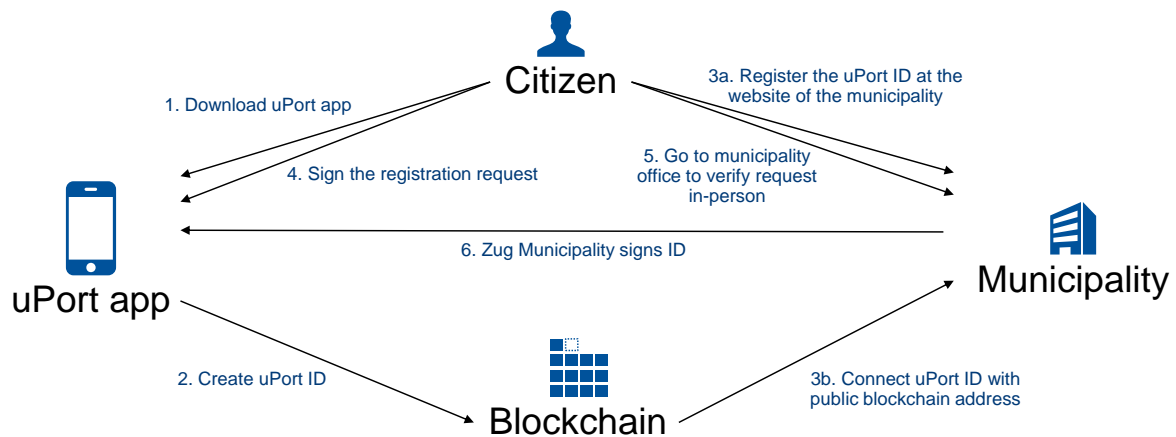
In the first stage of the project, only proof of residency is provided as a test service accompanying the Uport identity. The registration of digital blockchain-based identity on Ethereum, certified by the City of Zug, has commenced on 15 November 2017. The pilot phase will take at least six months. The uPort app creates a unique and unchangeable crypto address on the blockchain and links it to the local user wallet, located on the smartphone. The process of registering for the uPort identity is depicted in Figure 9.

Functionalities

uPort provides a new solution for identity confirmation and personal data management. It introduces a decentralised model of ownership, management, representation and attestation of the identity of a person. So far, the only public service working with the new digital identity is a proof of residency. The project however aims to expand to other public services run by the local authorities, like: surveys, e-voting, bike renting, book borrowing, tax declarations or parking payments. Citizens have to register the uPort identity, which is a public address of a smart contract on Ethereum, with the Municipality of Zug. The city registration office has admin rights in the uPort application. After the verification, which has to be done in person in the town hall, the municipality issues an attestation signed with its private key, as a server-side credential. This means that the

uPort identity is recognized as an official government-issued identity. This coupling process has to be done only once.

Figure 9. uPort process overview



Source: Own elaboration, based on data collected from project teams and desk research.

1. A citizen of Zug downloads the uPort app on his mobile phone.
2. Upon installation, a uPort ID, that is a public address of a smart contract on the Ethereum blockchain, is automatically created.
3. The citizen registers the uPort ID on the website of the Municipality of Zug, adding his current Zug ID number and the date of birth as the verifiable personal information. By doing this, the uPort ID automatically connects to a personal ID in the digital citizen registry of Zug.
4. The citizen uses the app to cryptographically sign the registration request, which is then sent to the municipality.
5. The citizen visits municipality in person in order to verify the request.
6. The Zug Municipality cryptographically signs the ID and automatically sends the verification to the uPort application.

Governance

The consortium governing the uPort application has a public-private hybrid structure, including ConsenSys, TI&M AG, Institute of Financial Services Zug (IFZ) at the Lucerne University of Economics and the City of Zug. The Municipality of Zug is responsible for pairing Zug residency number with the uPort address and approves services to be used with this identity. Ultimately, the development of particular end-user services should be ecosystem-driven with an engagement of public organisations, businesses and the open source community of uPort and Ethereum.

Usage

The service went live on the 15th of November, 2017. In the initial phase of the pilot the Testnet of Ethereum Rinkeby is used and not the main Ethereum network. Eventually, the service will move away from the Testnet because it provides only a limited amount of nodes with a loose governance structure. Of the 30.000 citizens of Zug, around 300 have registered so far. This amount of identities can be facilitated on the Testnet, which can register up to 15 transactions per second. However, with the current architecture, scaling to other municipalities could be an issue.

Technical architecture

From a user's perspective, the main interaction point with the system is the uPort application. It is used for storing all personal data locally on the user's device. Upon installation, the uPort application creates a unique private key, stored on a mobile device and two smart contracts running on Ethereum virtual machine. This is a runtime environment for smart contracts based on Ethereum. Specifically, there are two types of smart contracts that act as the users' identity hub: a controller contract and an identity (proxy) contract. The identity contract stores permanent identifiers of a person. It can interact with other smart contracts and uPort identities. The self-sovereignty property means that only the identity smart contract can make statements about a person's identity when interacting with other smart contracts or uPort users. These statements are neither backed nor confirmed by any centralized certification providers. The identity contract is monitored by a controller contract. The controller contract grants or withdraws an authorisation to sign statements. It also allows a citizen to recover identity access if a phone with the private key is lost. This is done by substitution of his public key in the identity contract and placing a corresponding new private key on a new mobile device.

The uPort registry is a shared contract which allows for a verification of private statements made to specific parties. It is in fact the on-chain reference point for off-chain data. It contains only a public profile of the user with his permanent Ethereum address and the hash of all private data stored locally. For attestation purposes, a citizen can reveal part of his identity information linked with the Ethereum public address to a specific party of his choice. The data is encrypted with that party's public key and signed with a private key of the sender. A recipient receives these credentials via uPort app installed on his device. Using the uPort registry he verifies integrity of the data and the source of it. In this particular implementation, the recipient can also check whether the sender has an attestation from the Zug Municipality.

The exchange of personal details is done in the uPort application, but all information is anonymized before sending via network. The only elements shared via the uPort registry are statements and messages related to attestation. Once created, the Ethereum public address, which corresponds to the user identity, cannot be erased. However, the user can choose to delete all personal data from his device, removing the ability to share it.

To create login functionality from an identity smart contract, the uPort connect API can be used by third-party applications. Integration of this API allows for communication with the uPort wallet, ultimately allowing uPort users to sign into third party applications. The transactions are processed through the Ethereum claims registry where the uPort identities can send messages for a permanent public record.

The uPort application can be considered as a non-DLT external data source, which stores personal data locally on the mobile device. The Zug residency register is not the part of DLT either, but rather an official government pool to which uPort identities can be attached. Outside of the DLT system there is a front-end web portal to register the uPort addresses and link them to the Zug resident numbers using a QR code. The outside personal data includes the name, date of birth, ID number and citizenship.

The consensus mechanism of this blockchain is Proof-Of-Stake, in which participants commit money to the system. The data stored on the blockchain has only a form of a hash, while the user personal data is always stored locally. Organization of identity storage and sharing among uPort users is facilitated by the distributed, content-addressing file system.

Costs and benefits

The benefits of the blockchain pilot include:

- Lower operational costs. The Zug Municipality can move away from storing personal data, to just having a single check of the identity of a person, for all services it provides. This could lead to operational cost savings.

- A reduced risk of cyberattacks and lower infrastructure costs. A self-sovereign identity solution reduces the need to maintain centralized repositories of identifying information. Once the ownership and attestation of identities is shifted to citizens there is no need to host servers and databases with personal data. Moreover, in the distributed architecture, the risk of large personal data leak is eliminated.
- Efficiency gains for citizens. The new form of attestation generates time savings for citizens in terms of accessing services. If a large number of businesses and public administrations would allow single identity solution for authentication and accessing their services, efficiency gains could be realized. Services could be integrated and different passwords would not be needed.

The costs involved in the project include:

- Development costs. Whilst the cost of development and management of the project remain undisclosed, about ten full-time equivalents have been spent on system integration over the first 8 months.
- Operating costs. In the future, only a single clerk at the town hall is required for the operation of the system. However, transactions cost could become an important factor. Adding each new user is estimated to cost US\$10 if the pilot is moved to the main Ethereum net.⁵ With 300.000 citizens of Zug, each requiring a transaction for registration, the cost could amount to US\$3.000.000. Since statements sent by smart contracts are also costly on the main Ethereum, using the uPort identity may generate even higher transaction costs.

Key takeaways

- The uPort identity allows for an authentication without the commonly used user/password or the private-public key infrastructure. The uPort identity is a smart contract address, which can interact with other smart contracts and users. There are ways to recover keys that give access to the identity, which is not the case in other blockchains.
- Users of the uPort identity can selectively release personal information to other parties, gaining control over their identity. They can choose how much data, to whom and when to disclose. As a consequence companies and apps could effectively get only a minimal set of personal data from users, as postulated by the General Data Protection Regulation (GDPR).
- Personal data is stored in a secure, encrypted form on a mobile device. Personal attestations are always sent off-chain. They can be verified on a blockchain and serve as user authentication for service providers or public institutions, generating efficiency and security gains.
- Since the launch of the pilot service by the Swiss Municipality of Zug, about 300 out of the 30.000 Zug citizens have registered the uPort identity. Currently, only the proof of residency is provided as public service accompanying the uPort identity. However, in the future several other services, like: surveys, e-voting, bike renting, book borrowing, tax declarations and parking payments could be developed by the ecosystem actors.

⁵ At the time of writing (April, 2018).

2.2.5 Infrachain governance framework - Luxembourg

Figure 10. Resume of Infrachain case study

Blockchain governance framework									
1. General features									
Level of government involved	Public services provided/enabled	Cross-border aspects	Cross-sector aspects	Location value creation	Openness of software				
National	Enabler for public services (voting)	Yes; within Europe	Yes	Location is static	Open source				
2. Functionalities		3. Governance			4. Usage				
Institutions disintermediated	Functionalities provided	Roles included	Blockchain governance architecture	Consortium governance	Current Usage	Capacity	Throughput	Scalability	Maturity
None	Notarization; shared database; smart contract automation	Government; Businesses, Tech provider	Private and public permissioned	Decentralized	Unknown	Depending on blockchain	Depending on blockchain	Depending on blockchain	Early stage pilot
5. Technical architecture									
User Layer	Non-DLT Systems			API Layer		DLT Platform Layer			
Not applicable	Not applicable			Not applicable		Private consensus (PoW)			
6. Costs				7. Benefits					
Non-recurring costs		Recurring costs		Quantitative benefits			Qualitative benefits		
Undisclosed hardware cost		Membership fee (€1K-€6K per year); management cost; transaction fees		Not applicable			Increased security and privacy protection		

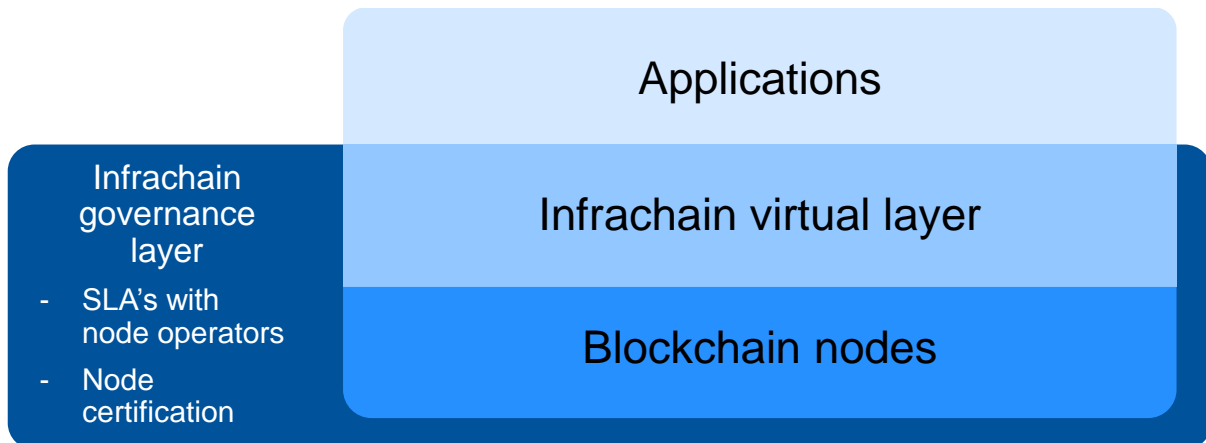
Source: Own elaboration, based on data collected from project teams and desk research.

Infrachain is a non-profit organisation, launched in November 2016 in Luxembourg. The aim of the organisation is to support the creation of independent and incorruptible nodes involved in the operation of blockchain instances. Infrachain develops a governance layer placed 'on top' of existing and future permissioned blockchains. The Infrachain governance framework gives attention to privacy protection, cyber-security, law enforcement and business continuity to the same degree as centralized systems. The framework postulates a separation of service and network layers and the establishment of a reference blockchain infrastructure, composed of independent nodes, hosting different public and private services.

Currently, individual private blockchain infrastructures comply with some security and confidentiality requirements, but there is no comprehensive set of shared rules followed by different implementations. This could be achieved via a virtual layer that serves as a host network operator with participating nodes operating under common service-level agreement (SLA). Because physical nodes are owned by different organisations, the host network would have a federated structure with a common governance framework. The host operator network is expected to offer high network stability and performance, typical for public blockchains, while hosting numerous private blockchain instances.

The project is backed by the Luxembourgian national government. Actors involved in the initiative have committed to provide and run certified nodes that comply with SLA-enforced governance. The certification will be based on the ISO27001 standard on the information security. The geographical outreach of the host operator network is regarded to be pan-European.

Figure 11. Infrachain governance framework overview



Source: Own elaboration, based on data collected from project teams and desk research.

Functionalities

The project does not provide any specific functionality for citizens, yet the initiative acts as an orchestration platform between blockchain applications and a European network of independent certified nodes. As such, no public institution is disintermediated. The initiative could be argued to disintermediate cloud providers or permissioned blockchain providers, as the certified node operators will provide similar functionalities. The initiative allows only for private permissioned or permissionless blockchains to be hosted.

Governance

Infrachain is set-up as a not for-profit-organisation and is a private sector initiative. The government of Luxemburg is just one of the members. Other business members are KPMG, KYC3, Scorechain, SnapSwap, Bitbank, Abax Consulting, Allen & Overy and more. The governance structure of the project overall is decentralized, as it is a community project and decisions within the projects are made in deliberation with the members of the initiative. Currently, Ethereum protocol is used most but the aim is to be blockchain agnostic. Recently, Infrachain has joined the Hyperledger consortium.

Usage

The project is currently in an initial pilot phase, but some use cases have already been tested on certified nodes of the Infrachain founding members.⁶ However, many features are still under development, such as the positioning towards the GDPR, SLA framework and elements of the architecture.

The current number of active projects using Infrachain is unknown, though a number of projects have been identified. One example is LuxTrust start-up, which is owned for two-third by the Luxemburg government. LuxTrust combines authentication, signature and document management services on top of the private blockchain developed by another start-up, Cambridge Blockchain. The project uses the Infrachain framework as part of the blockchain governance and for the orchestration of resources.

Technical architecture

Infrachain uses certification and SLA's for operating nodes to create a governance layer that adds trust and accountability in the nodes, ensures a sustainable operational

⁶ One of the developed use cases is the so called 'know your customer'. KYC is related to the identity verification of a transacting party to prevent fraud.

environment for blockchain projects and regulatory compliance. The governance layer is blockchain agnostic meaning that it does not focus on any specific protocol. The operators of certified nodes provide SLAs to Infrachain, and Infrachain provides SLAs to the application providers.

One of the drivers of this project is that private data can be stored on-chain. The SLA defines the proper governance structure to ensure that certified nodes meet security and privacy requirements. Currently, a testbed for this use case has been set up, running on five nodes, of which one is operated by the government of Luxemburg and is based on the Ethereum protocol.

Costs and benefits

The benefits of the blockchain pilot include:

- Increased reliability and resilience. The Infrachain organisation allows projects to reap the reliability benefits that blockchains in general provide, such as the mitigation of a single-point-of-failure, distributed data storage, incorruptibility of data, while being compliant with legislation on data security, privacy and public services regulations.
- Lighter (less costly) consensus mechanisms. The Infrachain orchestration platform allows projects to realize a high degree of resilience to crash and byzantine attacks that is usually only reached by public permissionless blockchains with a computational-heavy consensus mechanism. Certified nodes are environmentally friendly as they do not run heavy consensus mechanisms, such as Proof-of-Work.
- Transparency and flexibility. The governance layer of Infrachain enables the same level of transparency that is typical for public blockchains, while ensuring the flexibility and robust legal framework of private chains. Even though the nodes are private, the record-keeping is still distributed, making it almost impossible for one actor to tamper with the ledger. Furthermore, the SLAs of Infrachain ensure a degree of independence of the different nodes.

At this stage of the project no direct efficiency gains or economic savings could be identified.

The costs of the blockchain pilot include:








- Membership cost. The Infrachain is a non-profit organisation, set-up as a public-private partnership with funding coming from its members, including the Luxembourg government. The amounts are undisclosed. Membership fees for the Infrachain organisation range between €1-6 thousand per year.
- Management and hardware cost. Project management is the main cost driver. Infrachain intends to become the main blockchain federation in Europe. This requires reaching out to the stakeholders and working out alignment on the governance framework and the governance of the initiative. The exact amount for the management cost has not been disclosed. Likewise, the hardware cost related to the establishment of a certified node is unknown.

Key takeaways

- The Infrachain project aims to create a governance framework and a host network operator composed of independent federated nodes. The nodes will be compliant with regulations on data storage, security, privacy and operate based on SLAs.
- The Infrachain framework is a virtual layer placed 'on top' of existing private blockchain infrastructures. It removes the need for computationally intensive mining operations for data incorruptibility, as only certified nodes are accepted.
- Public services may benefit from a project of this type by getting faster time to market. They could adopt the governance framework instead of creating own complex solutions and use a common pool of certified nodes.

2.2.6 Pension infrastructure - the Netherlands

Figure 12. Resume of pension infrastructure case study

 Pension administration infrastructure in the Netherlands									
1. General features									
Level of government involved	Public services provided/enabled	Cross-border aspects	Cross-sector aspects	Location value creation	Openness of software				
National	Improved pension administration	None	Yes	Location is static	Open source and closed custom code				
 2. Functionalities		 3. Governance			 4. Usage				
Institutions disintermediated	Functionalities provided	Roles included	Blockchain governance architecture	Consortium governance	Current Usage	Capacity	Throughput	Scalability	Maturity
None	Notarization; shared database; smart contract automation	Government; Businesses; Tech provider; OS community	Private permissioned	Hybrid – various consortium partners	5000 users	Unknown	Unknown	Limited	Proof of concept
 5. Technical Architecture									
User Layer	Non-DLT Systems	API Layer	DLT Platform Layer	Infrastructure layer					
User group specific application	Existing salary and pension databases	Currently unknown	Proof-of-stake	Only hash stored in blockchain; storage of transaction details unknown.					
 6. Costs				 7. Benefits					
Non-recurring costs		Recurring costs		Quantitative benefits			Qualitative benefits		
Undisclosed		Undisclosed		Est. €500M. Lower administration cost; lower transaction costs			Increased transparency; security of data; improved regulatory oversight		

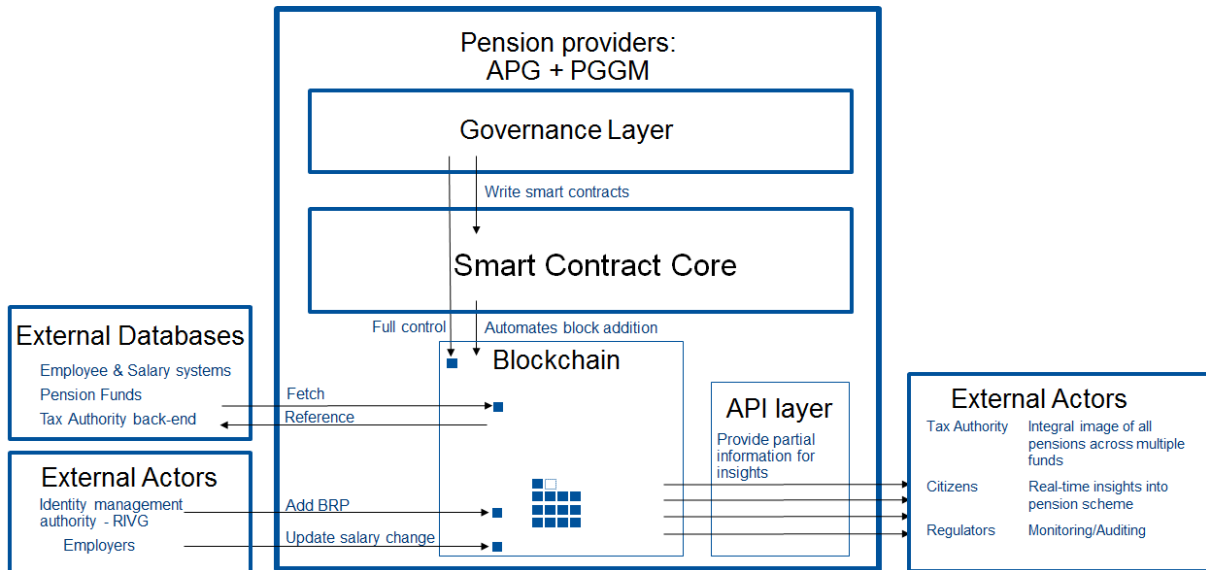
Source: Own elaboration, based on data collected from project teams and desk research.

The Pension Infrastructure (PI) is a complete community-based pension administration blockchain back-office. The aim of the project is to realize a more flexible and transparent pension administration system for citizens, while reducing significantly pension management costs. The project was initiated on the notion of the large similarities between blockchain payments and pension administration. In both systems actors have a personal balance and transactions between the balances occur.

The pilot was started in response to the identified trend of increasingly individualising workforce relations. Contemporary employees have multiple employers and job types over their lifespan. This has an impact on pension administration as future pensioners often sign-up to multiple personal pension schemes with various pension fund providers. In addition, people increasingly have entrepreneurial episodes in their careers. This creates a need for more customized pension solutions for self-employed workforce. Building the prototype started in 2018 in collaboration between the two largest pension providers in the Netherlands. The project has a variety of stakeholders, including employers, the national identity service, the tax authority, payroll providers, pension funds, technology providers and citizens.

The Dutch pension provider APG is exploring multiple use cases for blockchain technology, yet the PI project is the most advanced in terms of thinking through the application design and advancing solution. The Dutch National Government is involved in the project through the Dutch Authority for the Financial Markets (AFM) and the Dutch National Tax Office (Belastingdienst). An overview of the PI project is provided in the figure below.

Figure 13. Pension Infrastructure project overview



Source: Own elaboration, based on data collected from project teams and desk research.

Functionalities

The system provides different functionalities based on the role of the actor. For the tax authority, for example, it provides an integral image of the contributions collected by a specific individual across many pension funds. For a citizen, it provides real-time insights into the evolution of their pension scheme and pension balance. Employers can directly introduce a salary change. Regulators do not have an active role, yet they can see part of the data.

The project requires a combination of several blockchain functionalities: distributed registration, membership management, information exchange, automatic execution and digital fingerprints (hashing). Currently, no institution has a ready-to-use technical infrastructure which provides all these functionalities. The system is developed organically and internally by setting up connections between the back-end systems of all the involved parties.

Governance

The PI is a collaborative project between APG and PGGM – the two largest pension providers in the Netherlands. The infrastructure is co-developed with Accenture. The project has the following stakeholders:

- Government actors: Tax authority, AFM and identity management authority (RIVG);
- OSS community: Ethereum developers;
- Technology provider: Accenture;
- Citizens: Pension fund members and pensioners;
- Businesses: Employers and payment solution providers.

The pilot uses private blockchain architecture with a tweaked version of the Ethereum protocol. The nodes in the network have known identity and represent the stakeholders involved in the development of the infrastructure. Thus, the blockchain archetype used is private permissioned. The consortium has a hybrid-federated governance set-up. Decentralized governance facilitates co-creation of distributed database and integration with 'silos' systems of various ecosystem stakeholders. A centralized governance element is also present, as APG and PGGM steer the project into a certain technical direction.

Usage

Currently the project is in a proof of concept phase. All basic elements of the infrastructure, the business model and compliance with the regulator (involved in the project) are already elaborated. The project cannot yet be marked as a pilot, because certain functionalities are incomplete. For example, calculation of pension balance is doable only for the domestic employees, but not for someone who lived abroad for multiple times. A fully functional system is expected in 2 to 3 years. The current test case is based on the pension data of APG's own personnel (PPF APG) with about 5000 users currently participating.

The project uses a permissioned instance of the Ethereum protocol. The current number of transactions, as well as the maximum number of transactions, which can be processed, is unknown. Scalability may be a challenge in this project, due to a large number of smart contracts used, which send multiple statements. Additional users are being added to see at which point the test infrastructure starts to display capacity problems.

Technical architecture

Smart contracts are at the core of the DLT layer. Smart contracts are used to determine the rules for building up a pension balance for a citizen. They will also prescribe rules of who can view, change, and use the data. The runtime environment used is the Ethereum virtual machine, with Proof-Of-Work consensus mechanism. It executes scripts in Ethereum blockchain network and automates transactions between users and smart contracts. The ledger in the Pension Infrastructure contains an overview of transactions that occur in the whole lifecycle of building up a pension. This includes for example a transfer of funds between the employer and the pension fund as well as a change in salary.

Pension funds are likely to have admin applications in order to maintain a certain oversight over the system. A certain degree of admin rights in the system is deemed important as smart contracts in the infrastructure need to be adaptable to changes in the real world and regulatory environment. The system relies on external data supply coming from different databases of the pension funds, employers' systems and the tax authority back-end systems. It is likely that these data will be stored outside the DLT layer, with a hash referencing to it on the blockchain. The details of data handling are not public at the moment of writing. In any case, databases will have to be shared among partners to some extent and blockchain facilitates trusted sharing environment.

User applications for different stakeholders are still to be created. Each stakeholder receives different outputs from the infrastructure. For example, citizens would have an application that provides a real-time insight into their pension scheme. An application for employers would provide an integration of their salary systems with pension funds. All applications provided in Pension Infrastructure will use authentication based on the identities from centralized identity registry in the Netherlands (BRP). Integration of national citizen registry in the system requires careful handling of user ID data. While users ID need to be anonymized on the blockchain to ensure privacy, the tax authority, for example, needs to have non-anonymized IDs to use the functionalities ascribed to its role. For example tax offices could integrate payroll and pension scheme data back to its own infrastructure to generate automatic tax declarations for citizens.

Costs and benefits

The benefits of the blockchain pilot include:

- Cost savings on pension administration. Pension administration requires a great deal of labour-intensive tasks, such as administrative checks and document copying. Currently, the system is based on a large number of bilateral connections between the pension funds, governmental and private sector systems, which are mandated by law. This implies a continuous copying of data between the databases. The total costs

of pension administration in the Netherlands are estimated at €1 billion. The pension funds, who initiated the project, expect that blockchain-based pension infrastructure could generate €500 million of cost savings.

- Efficiencies related to creation of a distributed database. Distributed database, serving as a single source of truth for all participants, creates efficiencies in the administration of pensions. The current situation is characterized by many different systems connected by a large number of artificially created and organically grown connections. Efficiencies are created by allowing all parties to use the same infrastructure and have real-time access to the same data: information is entered only once and does not need to be copied or replicated.
- Lower transaction costs for citizens. One of the objectives of the project is to lower economic costs for pension funds members. From a citizen perspective, transaction costs are lowered as the information, although distributed, is accessible via one single interface. Currently, average participation cost for citizens in pension fund is estimated at €80 per year. The aim is to lower this cost to €15.⁷
- Increased security and transparency of information. Distributed systems are regarded to be more secure than centralised databases. In case of an attack or a failure of a node, the confirmed pension balance of a citizen is stored by other nodes. Furthermore, the information is recorded on the shared infrastructure and cannot be changed or erased by one actor. Greater transparency and accountability of information allows regulator to oversight the whole system without information asymmetry and immediately detect hazards or irregularities.
- Development and implementation costs were not disclosed. Their total level is not known yet, as these costs depend on many unknown factors.

Key takeaways

- The project focusses on all aspects of the pension system administration: from citizens having an access to a historical and current balance of (all) their pension schemes to automatic tax declarations, based on payroll data from employers. Even though all types of actors are represented in the project, the complexity of distributed pension infrastructure causes this implementation to be at a very early stage of a lifecycle.
- The project aims to create a new shared database which will provide customized and actual data for all actors involved in the pension system. New blockchain-based implementation is expected to generate multimillion savings by boosting the efficiency of pension administration, increasing regulatory oversight of the system and lowering transaction costs for citizens.

⁷ Figures provided in the interview with the project team.

2.2.7 Stadjerspas smart vouchers - Groningen, the Netherlands

Figure 14. Resume of Stadjerspas case study

Smart voucher system in the Netherlands									
1. General features									
Level of government involved	Public services provided/enabled	Cross-border aspects	Cross-sector aspects	Location value creation	Openness of software				
Local	Providing benefits to low-income residents	None	Yes	Location is static	Proprietary				
2. Functionalities		3. Governance			4. Usage				
Institutions disintermediated	Functionalities provided	Roles included	Blockchain governance architecture	Consortium governance	Current Usage	Capacity	Throughput	Scalability	Maturity
None	Notarization; shared database; smart contract automation	Government; service providers; tech provider	Public permissioned	Centralized	20k users	Unknown	7 tps	7 tps	Production
5. Technical architecture									
User Layer	Non-DLT Systems	API Layer	DLT Platform Layer	Infrastructure layer					
QR code; browser (mobile app)	Municipal registries	Admin API	Proof-of-authority consensus	Zcash protocol					
6. Costs				7. Benefits					
Non-recurring costs	Recurring costs			Quantitative benefits			Qualitative benefits		
Undisclosed	Undisclosed			Lower administration cost; lower transaction costs			Improved public accountability and auditability; effective redistribution		

Source: Own elaboration, based on data collected from project teams and desk research.

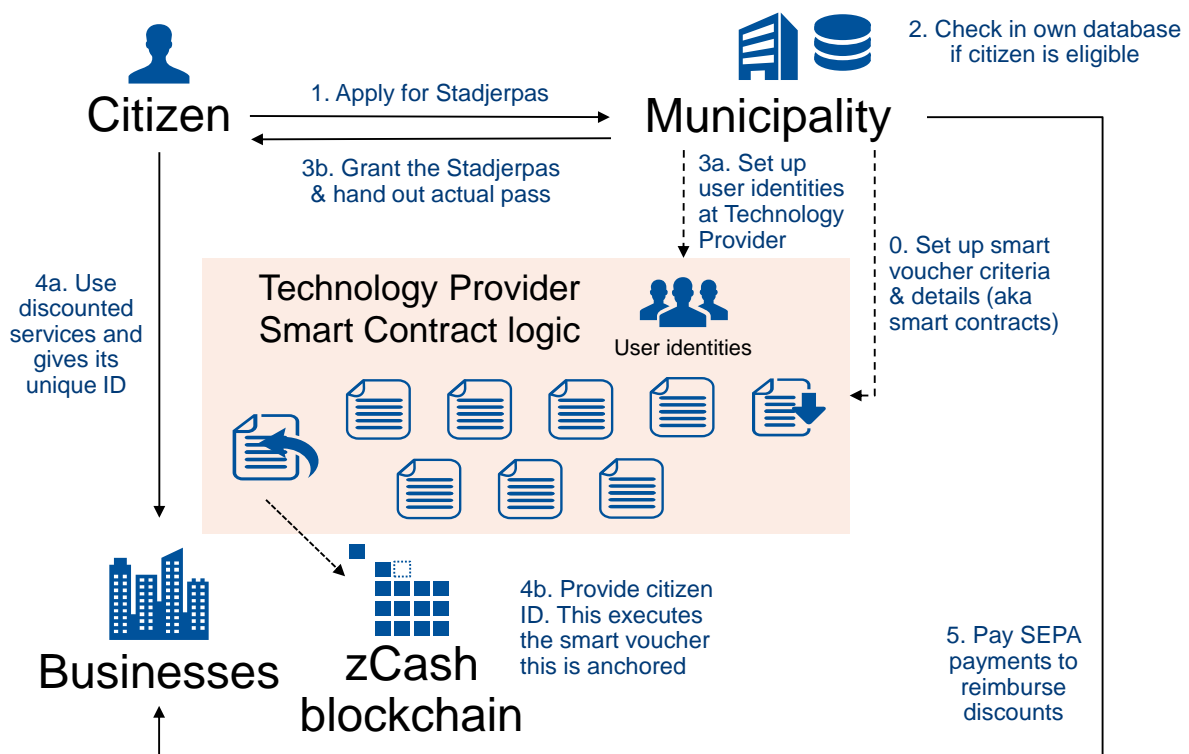
Stadjerspas is a fully operable service which uses blockchain infrastructure to provide discounted services to low-income citizens of the Municipality of Groningen. Promotion of inclusivity in the city via a voucher system started in 1994. Up until 2013 vouchers were completely paper-based. In 2016 the voucher system in Groningen was moved to a blockchain, developed by DutchChain, a technology provider company. The core value-added of the blockchain-based system is the enhanced targeting of public money thanks to programmable money flows. Detailed spending conditions and eligibility criteria are programmed in the smart contract. Possible criteria include: detailed profiles of the beneficiaries and authorized providers, financial thresholds or usage limits. Smart vouchers can be used, for example, in sport clubs, cinemas or for subsidization of solar panels for home owners. From the municipality perspective Stadjerspas ensures that public money reserved for a specified purpose is spent exclusively on that purpose and targeted at a desired group of beneficiaries.

The system works as follows:

1. A citizen applies for the Stadjerspas at the municipality, providing their name, address and citizen's number.
2. The municipality checks whether the registered citizen is eligible for any smart voucher. If so, the municipality sets up an anonymised user identity on the blockchain, linked with personal details stored off-chain.
3. The municipality grants the citizen a Stadjerspas, accompanied with a personal QR code referencing to his ID in the blockchain-based smart voucher system. The municipality also manually assigns smart vouchers to the citizen in its own system.

4. The citizen uses a service of the authorised provider. Each provider has an application that scans the QR code on the pass to activate the smart voucher and calculates discount. Every time a smart voucher is invoked smart contract checks whether this user is eligible for the criteria and how many times he has used this smart voucher already.
5. There is also an application for the beneficiaries, for browsing offers from authorised providers and making reservations. It is however not a mandatory part of the system.
6. After a certain period, SEPA payments are done from the municipality to the providers.

Figure 15. Stadjerspas process flow



Source: Own elaboration, based on data collected from project teams and desk research.

The system subsidizes private services that low-income citizens would otherwise not be able to access, thereby promoting inclusivity. The municipality or a voucher issuing partner can provide eligibility criteria for users of smart vouchers, for example based on the neighbourhood of their residence, their income, number of children or any data linked to the resident number. Users of the system can see the vouchers they are eligible for in the mobile app or in the web portal, upon providing a QR code. The QR code is specific to a citizen. Each instance of a voucher use is recorded in the system by the provider of the discounted service who scans user's QR code. Citizens using the application or pass are not aware that they are interacting with a blockchain system. The same applies for the organisations that provide subsidized services.

Functionalities

This blockchain implementation uses smart voucher functionality and automatic payments. The SEPA payments are not instant, but are done at the end of certain period based on the transactions that have occurred in the system. The blockchain system allows for transparency and programmability of public funding, specifically by adding

functionalities of distributed registration, membership management, information exchange and automatic execution. However, it does not replace any existing system.

Governance

The blockchain system is a part of the official service provided by the Municipality of Groningen. The governance structure is central, as the Municipality of Groningen and DutchChain are in a client-service provider relationship. The stakeholders of the project include:

- Government actor: Municipality of Groningen;
- Technology provider: DutchChain Systems;
- Citizens of Groningen and Ten Boer;
- Businesses: Providers of services subsidized via smart vouchers.

The validation of transactions is performed on a public blockchain, yet the users that can transact are permissioned. The system is therefore of a public permissioned blockchain type. Initially the Bitcoin protocol was used, but the system has transferred to Zcash, which has significantly lower transaction costs. Stadjerspas has its own smart contract logic on top of the blockchain protocol. Every transaction is recorded in form of a hash, but the details of the transaction are not stored on blockchain.

Usage

The system is fully operational since 2016 and is used on a daily basis. Over 20.000 citizens and service providers are registered in the program and around 4000 smart voucher transactions occur per month. The system can process 7 transactions per second. Scalability issues are not foreseen, because the capacity of the system depends on the number of smart contracts and not the number of users or use instances.

Technical architecture

On the end-user side there is the Stadjerspas application for citizens, which allows citizens to browse and access smart vouchers for which they are eligible. Service providers use the Stadjerspas application for business, which allows for scanning of a citizen's pass and granting an access to a discounted service.

The users are authenticated by the municipality. A low-income citizen can apply for the Stadjerspas by providing personal details including their name, address and citizen number with which they are registered at the municipality. The municipality then can grant the citizen a Stadjerspas, which is accompanied with a unique ID for the blockchain-based smart voucher system. The database of the Municipality of Groningen is used to check whether the registered citizen is eligible for any smart vouchers. Each voucher corresponds to a particular service, such as a swimming pool or a cinema. An admin application operated by the municipality then assigns the smart vouchers to the eligible citizens. Additionally, there is an admin API which allows the municipality to add new smart vouchers, increase the total amount of times a voucher can be used and add new users.

Vouchers are set up as smart contract addresses on Zcash. The runtime environment for the smart contract logic is hosted at DutchChain. User identities for the smart contract environment are set-up by the municipality administrator and stored in an anonymised form on the Zcash permissionless protocol (with Proof-Of-Authority). The ledger stores data on the usage of the vouchers: by whom and how many times a voucher is used. The ledger does not disclose the origin, destination, or amount of any transaction. The technology provider hosts the voucher criteria, voucher details and user details.

Costs and benefits

In this case study, precise benefits from introducing a blockchain-based system cannot be specified, as there is no previous (centralised) digital system to compare the benefits with. In more general terms, this blockchain deployment can be expected to bring a number of positive effects:

- Improved allocative efficiency of public spending. Programmable smart vouchers are a new redistribution mechanism that assures that every euro dedicated to a specific purpose and beneficiary is spent accordingly. Smart vouchers reduce possibility of economic arbitrage by recording each instance of use and setting usage limits. There is no space for somebody trying to tamper with the voucher for their own benefit because transactions are stored on the Zcash blockchain.
- Operational efficiency gains for a municipality. Blockchain-based vouchers offer an efficient way of programming and monitoring the use of subsidized service, including automatic payments to providers. The use data recorded on the ledger serves for audit purposes which increases an accountability of public spending. Smart contract automation eliminated paper-based processes and reduced the amount of human labour required by the municipality.

Unfortunately, none of the project costs have been disclosed. The current system has been selected in a public tender that was competitive on price. Hence, it can be presumed that the development, implementation and operation cost were not higher than for a centralized, non-blockchain system. The only novel cost item is the cost of validating transaction in the public blockchain, borne by municipality. Validation cost may become significant as it grows with the number of services offered. To mitigate the impact of this item, the service has been migrated from Bitcoin to Zcash. From a citizen's perspective, the use of Stadjerspas system is free of charge and has clear advantages over the paper-based system. The citizen manages his use via a mobile application and is not confronted with any back-end systems.

Key takeaways

- The Stadjerspas allows for precisely targeted allocation of subsidies for consumption of private or public services for low-income citizens, promoting inclusivity.
- Blockchain technology facilitates better targeting and management of redistribution programs. The benefits of a smart contract solution include efficiency gains in the operation and design of redistribution programs and increased public accountability and auditability of spending.
- Smart vouchers have programmable rules that specify service providers, set of eligible beneficiaries, use thresholds, subsidy limits and conditions of use. They cannot be transferred, changed or sold. The user of the Stadjerspas voucher system does not notice that he is using a blockchain-based solution.
- Costs of the system are not disclosed. However, the project won a competitive tender and scored well on overall costs compared to the other tender projects which included centralized voucher systems.

2.3 Horizontal comparison of case studies

Our sample of projects exhibits large heterogeneity. This section focuses on uncovering common patterns and main differences between ongoing blockchain implementations in the public sector. This is done by comparing projects along the dimensions set out in the case study assessment framework. The results are presented in Table 3 to 9.

Project characteristics

Table 3. Case study characteristics overview

Project	Level of government involved	Public services implemented / foreseen	Cross-border aspects	Cross-sector aspects	Location value creation	Openness of software
1. Exonum land title registry	National	Land title registration and verification / Property transactions	None	None	Location is the product	Open source
2. Blockcerts academic credentials	National	Certificate verification / Storage and sharing of personal documents	Yes	Business, Education	Location is static	Open source
3. Chromaway property transactions	National	Property transactions and transfer of land title	None	None	Location is the product	Proprietary
4. uPort decentralised identity	Local	Proof of residency / eVoting, bike renting, parking payment	None	Yes, many	Location is static	Open source
5. Infrachain governance framework	National	None	Yes	Yes, many	Location is static	Open source
6. Pension infrastructure	National	Improved pension administration	None	Yes, many	Location is static	Hybrid: os standards, proprietary software
7. Stadjerspas smart vouchers	Local	Providing benefits to low-income residents	None	Yes, many	Location is static	Hybrid: os blockchain protocol, proprietary smart contract layer

Source: Own elaboration, based on data collected from project teams and desk research.

In all case studies we observe a direct involvement of public governments in project consortia. Local and national governments (central agencies and municipalities) experiment with a number of specific services like registration, verification and transfer of land titles, verification of personal certificates and attestation of identity or allocation of benefits. These concrete services support the three main functions of governments: (i) management of public registries (ii) management of social transfers / benefits and (iii) provision of verified information for facilitation of economic transactions and setting regulatory frameworks. Most of these services are targeted at citizens as end-users, but there are also projects which focus on foundational elements of blockchains. These building blocks of decentralised architecture, such as government-attested decentralised identity or governance framework will serve as enablers for the new generation of public services such as electronic voting or provision of access to public infrastructure.

The level of government involved varies across case studies, yet dominantly the national government is involved. Projects where local governments are included in the consortia are relatively advanced in the lifecycle and have narrower scope.

Cross-border aspects are explicitly present only in the Infrachain project. Infrachain has an aim to create European high reference network, composed of independent nodes, which could host different blockchains. Remaining projects have a local or national focus,

but in some cases a clear value added could be realized if the solution is expanded across borders, as in the case of academic credentials verification.⁸ The majority of the case studies display cross-sector aspects, meaning that the services can affect multiple industries or markets. For example, the decentralised identity developed in Zug, could be expanded beyond public sector. The set-up allows for private services, like payments and rentals, to be authenticated using the uPort identity solution. Projects that develop sector specific services are Chromaway property transactions and Exonum land title registry.

Location information creates value in many different ways in digital services, including adding a community element or personalizing the service that is provided. In blockchain-based systems, location is often a static element, as can be seen in Table 43. For the two projects related to land title and property transactions, location can be considered as a product, but it is restricted to static data. Although there are some initiatives that give a more prominent role for location information in blockchain systems⁹, none of the case studies directly processes user location data.

Four out of seven projects are fully open source. Only the Postchain system in Chromaway property transactions is proprietary. The remaining projects utilize open source blockchain protocols but develop also proprietary software implementing smart contracts.

Functionalities

Table 4. Functionalities overview

Project	Institutions disintermediated: Full / Partial	Blockchain functionalities leveraged: Notarization / Shared database / Smart contract automation
1. Exonum land title registry	None / None	Notarization
2. Blockcerts academic credentials	None / Yes: reduced tasks for admin office at university	Notarization
3. Chromaway property transactions	Yes: Notaries / Yes: reduced tasks for banks and land registry back offices	Smart contract automation / shared database
4. uPort decentralised identity	None: / Yes: reduced tasks for municipality	Notarization
5. Infrachain governance framework	None	Notarization / shared database / smart contract automation
6. Pension infrastructure	None / Yes: reduced tasks for pension funds back offices	Notarization / shared database / smart contract automation
7. Stadjespas smart vouchers	None / Yes: reduced tasks for municipality	Notarization / smart contract automation

Source: Own elaboration, based on data collected from project teams and desk research.

For each project, it was investigated if the blockchain platform made any public organisation redundant and/or took over one or more tasks from such an organisation. In none of the projects we observed a full disintermediation of any public institution. In the Chromaway project a private notary is disintermediated. The notary would not need to be involved in registration and attestation of property transaction documents as this is done directly in a smart contract workflow. Nevertheless most projects assume handling tasks, such as for example attestation of identity, verification of documents, or eligibility check-up to blockchain protocol. These changes reduce paper work and generate time savings.

⁸ For details, see section 4 on scaling-up.

⁹ The FOAM protocol uses a consensus mechanism to determine whether an event or agent is verifiably at a certain point in time and space – more via <https://foam.space/>

Analysed projects differ with respect to the scope of blockchain functionalities which are implemented. Two projects (Exonum and Blockcerts) use blockchain for recording hashes, which are cryptographic, time-stamped extracts of documents. Blockchain-based notarization allows verifying the originality of a document, together with a date of its creation and owner. This elementary functionality provides only limited gains for citizens. However it brings value added if combined with other elements, such as ownership of personal certificates and credentials. The majority of projects implement more advanced features of blockchains, namely programmable smart contracts. Smart contracts enable shared database and information exchange between different actors (Pension Infrastructure), decentralised identity management (uPort decentralised identity), automatic execution of transactions (Chromaway property transactions) or usage monitoring and eligibility check-up (Stadjerspas voucher system). The type of functionality partially impacts the maturity of the service. Those projects which utilize smart contracts for shared databases or automated workflows are relatively less advanced. This is however expected as these implementations have to reconcile different needs in the ecosystem and integrate legacy systems of various actors.

Governance

Table 5. Governance overview

Governance	Roles included	Blockchain governance architecture	Consortium governance
1. Exonum land title registry	Government; Open source community; Tech provider	Private permissioned and public permissionless	Centralized (NAPR)
2. Blockcerts academic credentials	Government; Open source community; Tech provider	Private permissionless	Hybrid – various consortium partners
3. Chromaway property transactions	Government; Tech provider; Banks	Private permissioned	Hybrid – various consortium partners
4. uPort decentralised identity	Government; Open source community, Tech provider	Private permissionless	Hybrid
5. Infrachain governance framework	Government; Businesses, Tech provider	Private and public permissioned	Decentralized
6. Pension infrastructure	Government; Open source community; Pension funds; Tech provider	Private permissioned	Hybrid
7. Stadjerspas smart vouchers	Government; Businesses, Tech provider	Private permissionless	Centralized (City of Groningen)

Source: Own elaboration, based on data collected from project teams and desk research.

The composition of roles in consortium greatly varies among the projects. In around half of the case studies, an open source software community contributes to the solution, whereas in the other half a technology provider does the major development work. The governance of the project consortia are mostly centralized or hybrid. In the centralized model, usually government has a vast amount of decision-making power. In the hybrid model, few large players can steer the consortium in certain directions, often with a strong influence of the technology provider.

The choices of blockchain governance architectures are not clear-cut. What is interesting to note is that none of the projects are based solely on a public permissionless blockchain archetype. There is always some type of restriction: either on who can transact in the system or on who can validate transactions. Four cases display elements of a private permissioned design, with limited number of known nodes participating in the validation.

Usage

Table 6. Usage overview

Project	Current Usage	Current Throughput	Scalability (per May 2018)	Maturity
1. Exonum land title registry	Over 100.000 titles	Unknown	5.000 tps (private permissioned part)	Production
2. Blockcerts academic credentials	Hundreds of users	7 tps (Bitcoin)	7 tps (Bitcoin)	Early stage pilot
3. Chromaway property transactions	Unknown	Unknown	160 tps	Proof-of-concept
4. uPort decentralised identity	300 users	Unknown	7 tps	Early stage pilot
5. Infrachain governance framework	Unknown	Depending on blockchain	Depending on blockchain	Early stage pilot
6. Pension infrastructure	5.000 users	Unknown	Unknown	Proof-of-concept
7. Stadjerspas smart vouchers	20.000 users, 4.000 transactions monthly	7 tps	7 tps	Production

Source: Own elaboration, based on data collected from project teams and desk research.

At the time of writing, the majority of projects were in a conceptual or pilot phase. Only two services were already operational. The current usage differs greatly per project and is logically largely dependent on the lifecycle phase. Usually pools of test users do not exceed few hundreds, but for operational services they reach several thousands. Georgian authorities have registered over 100 thousand land titles hashed on the Exonum blockchain. Voucher system of the Municipality of Groningen already has over 20 thousand users.

As can be seen from Table 6, early stage projects have a limited account of the current throughput parameter of their blockchain systems. This is not surprising as at this stage the main objective is to develop a functional service in a test environment. Stability and scalability of the system are considered at later stages of experimentation when the main goal is optimization of prototype for operation. Although impossible to verify, the declared scalability in current environments (understood as a maximal number of transactions in a given time interval) ranges from 7 transactions to 5000 transactions per second. As a general rule, projects which utilize permissioned blockchains do not report scalability constraints. Scalability is often considered to be a hurdle for permissionless blockchain implementations, but it does not seem to be a major obstacle in reality. Analysed projects with permissionless design have developed ways to overcome throughput bottleneck. For example Blockcerts records transactions in batches and Exonum hashes the whole state of the system, instead of individual land titles. In the case of Stadjerspas current throughput is not a bottleneck for the foreseen amount of subsidized services and corresponding smart contracts.

Technical architecture

The technical architectures of blockchain-based services differ greatly among projects. An overview of the architecture layers of each project is displayed in Table 7.

In the user layer wallets, web portals and specifically developed applications are found. Mobile applications are dominant and usually they enhance the experience of end-users from a service. Looking at the non-DLT systems, a separate registry or database is

always found. All deployments have a connection to existing databases. This ranges from salary or credential databases to municipal or state registries.

Table 7. Technical Architecture overview

Project	User Layer	Non-DLT Systems	API Layer	DLT Platform Layer	Infrastructure layer
1. Exonum land title registry	Admin NAPR application	NAPR Land Title Registry system	Admin API to Land Title Registry	Private consensus (private blockchain) and Proof-Of-Work (Bitcoin)	Known nodes & Bitcoin blockchain
2. Blockcerts academic credentials	Wallet (mobile app) and issuer software	Certification database of institutions	Blockchain APIs for confirmation and searching	Proof-Of-Work consensus	Bitcoin blockchain
3. Chromaway property transactions	Smart contract interface (mobile app)	Swedish Land Registry	Internode API, Client API and Legacy API	Proof-Of-Authority with PBFT (Private) consensus	Storage is in PostgreSQL or another RDBMS with known nodes
4. uPort decentralised identity	uPort (mobile app)	Front-end portal (municipal webpage)	uPort Connect API	Proof-Of-Stake consensus	Hash is stored in Ethereum (test net) blockchain, user data stored locally
5. Infrachain governance framework	Not applicable	Not applicable	Not applicable	Private consensus (currently Proof-Of-Work)	Nodes based on Ethereum protocol
6. Pension infrastructure	User group specific application	Exiting salary and pension databases	Currently unknown	Private consensus (currently Proof-Of-Work)	Hash stored in Ethereum blockchain with known nodes, storage of transaction unknown
7. Stadjerspas smart vouchers	QR code, browser (mobile app)	Municipal registries	Admin API	Proof-Of-Authority consensus	Nodes using the Zcash protocol

Source: Own elaboration, based on data collected from project teams and desk research.

Blockchain pilots dominantly use APIs to connect the blockchain layer to the existing databases or to existing systems of project participants. The most complex blockchain pilots display a range of different APIs with varying functions.

The physical storage of the transaction data heavily depends on the architecture. Private blockchain infrastructures often allow participants to host blockchain nodes and participate in the consensus. In public blockchain architectures, the physical location of transaction data is usually unknown.

Varying consensus mechanisms occur in the pilot deployments. Blockchain architecture (private/public and permissionless/permissioned) only determines to a certain extent how computational heavy the used consensus mechanism is. Proof-Of-Work requires a lot of energy and hardware to validate, but also Proof-Of-Stake or Proof-Of-Authority consensus mechanisms are seen in permissionless blockchain deployments, like Stadjerspas using Zcash. Fully private permissioned blockchain deployments, like Chromaway, also use this consensus mechanism. Among the nodes that are known, a more efficient consensus model can be deployed, such as PBFT. Generally, there is an increasing research towards creating more computational "light" consensus mechanisms like Proof-Of-Stake for permissionless blockchain deployments.

The infrastructure layer on which the consensus mechanism is running varies depending on the deployment. In permissioned blockchains, the nodes are often owned by consortium participants, including government institutions. In permissionless deployments, anyone can theoretically establish a node. If a service anchors hashes in the Bitcoin blockchain, these would be stored in all full Bitcoin nodes, which are spread out all over the globe.

Costs

Gathering quantitative insights into the costs of the blockchain pilots proved to be impossible for most of the case studies. This deficit of quantitative economic evidence presumably has two reasons. First, as multiple public organisations are investigating similar pilots, there is limited willingness to share the cost figures given the strategic importance of being the first mover. Secondly, the lack of focus on costs could also be explained by the nature and goals of pilot projects. Contrary to production implementations, experimentation projects focus mainly on the development of functional mock-ups. Economic and technical efficiency is not considered at this stage. Given the above factors, we could only identify various categories of costs that occur during the development of services, as displayed in Table 8.

Table 8. Costs overview

Project	Non-recurring costs	Recurring costs
1. Exonum land title registry	Development cost (customization of Exonum protocol); integration cost (with NAPR systems); organizational capacity cost to adopt technology.	Maintenance and operation cost; Transaction fees for anchoring hashes.
2. Blockcerts academic credentials	Development cost (standard development; service implementation); integration cost (with the legacy credential-issuing systems).	Transaction costs on blockchain, software maintenance costs (academic institutions).
3. Chromaway property transactions	Development cost; Integration cost (with banks and land title systems).	Maintenance and operation cost (replication of the consortium database).
4. uPort decentralised identity	Development cost (so far 80 person-months of full-time equivalents).	Ethereum transaction fees; operation cost.
5. Infrachain governance framework	Undisclosed hardware cost.	Membership fee (€1.000-€6.000 per year); management cost, transaction fees.
6. Pension infrastructure	Undisclosed.	Undisclosed.
7. Stadjespas smart vouchers	Undisclosed, but not higher than for centralized design.	Undisclosed. Transaction fees on blockchain.

Source: Own elaboration, based on data collected from project teams and desk research.

Development and integration cost are the two main types of non-recurring costs observed. Apart from development, blockchain-based services require an extensive integration with the existing systems. Providing a secure and automatized link (API) to the external data repositories will likely be a significant cost item. Development costs include either writing blockchain protocol or customizing an existing open source solution. Customization of open source components is usually cheaper, therefore this option is predominantly adopted. Apart from creation of DLT layer, each project develops dedicated user interfaces and applications. Analysed projects do not report large infrastructure costs, because in test environments the numbers of participating users and blockchain nodes are limited. Operational services require heavier and more robust infrastructures, but at this point related cost data is not available. Infrastructure costs related to the use of blockchain are a function of a number of nodes which take part in consensus mechanisms and capacities for storage of transaction data. Different models of provision of infrastructure will be in place. Services which utilize mainly notarization

functionality in the public permissionless blockchains in principle do not need to invest in a dedicated infrastructure. Services implementing functionalities specific for permissioned blockchains, such as for example a shared database, will likely require dedicated infrastructures. But even in this case there will be a choice between deploying own infrastructure and using a reference infrastructure provided as a service, for example developed by the Infrachain project. In the cases of both operational services in our sample, public institutions do not host dedicated blockchain infrastructures in-house, but rather enter into service agreements with technology partners.

Transaction fees are inherent to permissionless blockchains and are observed in all four instances of this archetype. In some projects, blockchain validation cost has to be paid for every new user, while other implementations send for validation only one transaction with a total state of the system. Services that require verification of multiple transactions in public permissionless blockchain and rely on computationally heavy consensus mechanisms add up substantially to the environmental cost.

Benefits

Table 9. Benefits overview

Project	Quantitative benefits	Qualitative benefits
1. Exonum land title registry	400 times faster registration of extract; reduction of operational costs (over 90%).	Improved transparency; higher fault-tolerance; increased reliability of data
2. Blockcerts academic credentials	Lower operation cost; efficiency gains; lower integration cost.	Citizens' ownership of data, convenient storage; quick and selective sharing; identity and privacy protected; no hard copies; elimination of fake certificates.
3. Chromaway property transactions	Est. €100M/annum; reduced transaction time (over 95%); reduced transaction cost (90%); faster registration and transfer of land title.	Increased trust; higher liquidity of assets; improved market operation; improved resilience to record modification and fraud.
4. uPort decentralised identity	Lower administration cost; lower storage cost; lower infrastructure cost; efficiency gains for administration; efficiency gains for citizens.	Citizens' ownership of data; reduced risk of cyberattacks.
5. Infrachain governance framework	Not applicable.	Increased reliability and resilience; increased transparency and flexibility.
6. Pension infrastructure	Est. €500M/annum; lower storage cost; efficiency gains for pension funds; efficiency gains for administration; lower transaction costs for citizens.	Increased transparency; increased security of data; improved regulatory oversight.
7. Stadjspas smart vouchers	Lower administration cost; efficiency gains for administration; lower transaction costs for citizens.	Effective redistribution; improved auditability of public funds.

Source: Own elaboration, based on data collected from project teams and desk research.

For similar reasons as above, it proved difficult to obtain quantitative insights into the benefits generated by the blockchain-based implementations. Nevertheless, a stock of different positive impacts could be taken from project teams.

Process efficiency is the most frequently declared benefit of blockchain-based services. Elimination of human-based registration and verification of documents and reduction of hard copies generate savings in operation and administration costs. Much quicker but more reliable settlement of transaction reduces transaction costs. This can be seen particularly well in case of the Chromaway project. Reduction in end-to-end property transaction time from weeks to hours results in huge savings on insurance for safeguarding mortgage deed. Projects that establish shared databases, like Chromaway or Pension Infrastructure avoid endless copying of the same data between different IT

systems. Smart contract enable to streamline various business processes and hence create efficiency by reducing the uncertainty and automating transactions.

Two projects reported monetary estimates for efficiency gains. The blockchain-based pension administration system in the Netherlands is expected to bring €500 million annually of savings on pension system administration. This corresponds to 50% decrease in costs from the actual level. The Chromaway project estimates the net gain from implementation of smart contracts for property transactions to be €100 million annually. These gains are attributable in part to public and private institutions and in part to the citizens. In case of the Stadjerspas project, the benefits can be attributed to society as a whole, for example when the technology improves targeting of public funds and lower costs of redistributive policies.

Blockchain technology brings also a number of qualitative benefits. The fact that the transactions are shared on the distributed ledger by multiple nodes increases security and resistance to crashes and malicious behaviour. The append-only way of updating the blocks ensures the irrevocability of a ledger and increases the integrity and auditability of data. All these features are directly provided by the technology itself and are likely to increase reliability of governmental record-keeping. The lack of a central intermediary to assure the validity of transactions has another beneficial impact. It shifts the control over processes towards ecosystem. For example in the uPort project users gain full control over their personal data and may selectively disclose it to any third party. Encryption techniques ensure compliance of sharing and storing of personal data with the GDPR.

Last but not least, blockchain-based digital services have a potential to improve user experience from interacting with the public authorities. For example land title or personal documents can be issued and transferred within mobile app, without hard copies and visits to the town hall or state registry.

2.4 Insights from case studies

In what follows we present the key findings regarding the current use of blockchain technology for provision of public services.

1. Ongoing projects experiment with a full spectrum of blockchain functionalities

The three main blockchain functionalities: notarization, shared database and workflow automation all can be useful for different operational capacities of governments and beneficial for the citizens. Blockchain notarization enables verification of originality of a document and confirmation of the date of its creation and the owner. Decentralised notarization represents only incremental innovation and hence if added on top of existing centralised services it brings only incremental value. However, in combination with other innovations such as peer-to-peer file system and data sharing, notarization has a clear cut-value for citizens (Blockcerts, uPort). More advanced blockchain functionalities are based on programmable smart contracts. Smart contracts are implemented for different purposes such as shared database, information exchange (Pension Infrastructure, Stadjerspas) or automation of multiparty transactions (Chromaway). Advanced functionalities have high stand-alone value because they are themselves disruptive innovations. They will be relevant for all functions that digital governments have to perform efficiently: data management, facilitation of economic transactions, redistribution of public funds and creating regulation. Citizens using smart contract-based services also benefit from higher process efficiency, reduced uncertainty or reduced settlement times.

2. Services leveraging blockchain notarization are relatively more mature, while more disruptive services still face challenges.

The type of implemented functionality impacts the maturity of projects. Projects which utilize smart contracts to facilitate shared database or automated workflows are less advanced in their lifecycle. This is expected as these implementations have to reconcile different needs in the ecosystem and integrate legacy systems of various actors. In some cases, advanced functionalities already work well technically, but are not compliant with legal frameworks. Lack of regulation and governance standards hinders the development of more disruptive services beyond a proof-of-concept or early pilot phase. Projects that utilize solely proof of existence via verification of hash have quicker implementation times. They require less integration effort and may use existing software components.

3. Projects with a higher level of maturity tend to have less stakeholder complexity and more centralized governance.

The Pension Infrastructure project, which is in proof-of-concept stage, is the most complex in the sample. It has several types of stakeholders involved with varying business objectives and different legacy databases. On the other hand, Stadgerspas voucher system, Exonum land title registry or Blockcerts academic credentials have fewer stakeholder types. In addition, projects with more centralized governance structure are more advanced. This is likely caused by more hierarchical decision-making processes in consortia that have a strong leader.

4. Blockchain-based services that are already in operation respond to the clear business needs. They also have active public actors and strong technological partners.

Two projects in our sample already deliver operational services. In both cases there is a strong technological partner, providing required integration with the legacy systems. Both projects also fit within the current technological limits. They utilize basic blockchain functionality, essentially time-stamped proof of existence. Stadgerspas utilizes also a programmable layer that allows for setting requirements for the usage of specific smart vouchers. In addition, both projects have clearly defined business needs: registration and verification of land titles and allocation of vouchers according to specific criteria of beneficiaries.

5. Blockchain implementations are predominantly based on open source software.

Most of the projects rely on the open source components because they already proven to some extent and have strong supporting communities of developers and users built round them. Open source elements include blockchain protocols, for example Zcash or Bitcoin, and software layer on top of the protocol, like Exonum or Blockcerts frameworks. Open source is a predominant choice for the project teams because it speeds up development of a service. In some projects open source solutions are combined with proprietary development of user applications and APIs for legacy systems integration. These elements are provided by a technology partner in the consortium. Some governments involved in blockchain projects push towards opening of proprietary elements created within the project. In this way the governments support expansion of created solutions to multiple platforms and creation of third party applications. This strategy aims to speed-up the adoption of the service by minimizing the risk of a lock-in.

6. Blockchain is just one layer of developed service. It usually depends on a non-DLT layer which runs on top of a legacy type of centralised database.

Blockchain is always one of several layers in the system, and in all projects a centralized database is found that either stores user data or that feeds transaction data into the distributed system. Exonum and Stadgerspas projects are the examples where a centralized database is used to store transaction data. Blockchain protocol is used only to

anchor hashes yet all the transaction details are stored in the databases of NAPR or DutchChain. The Uport project is an example of implementation where a centralized database is used to feed into the distributed system. Municipality checks the validity of the citizen's request and links own records with the Uport address, referred to as the blockchain identity.

7. Private data is always stored off-chain.

The storage of private data is carefully designed in all pilot deployments. When permissionless or public blockchains are leveraged, private data is stored off-chain, either in centralised repositories, like in the Exonum project or locally by the users, like in the Blockerts or uPort projects. When a private permissioned blockchain is used, private data in principle could be stored on-chain in an encrypted form. However sending large portions of data in the network is usually inefficient due to bandwidth restrictions. In the Chromaway project for example, a smart contract platform is used to connect centralised databases of participants and record statements about the new states of the workflow.

8. Transaction throughput does not appear to be a major bottleneck.

A clear difference between permissioned and permissionless blockchains is observed with respect to the number of transactions that can be validated in a period of time. The throughput in permissionless blockchain protocols is significantly less than the permissioned blockchain protocols (up to 7 tps compared to 160-5.000 tps). Projects that anchor transaction on public permissionless blockchains have designed ways to mitigate throughput constraints. For example, they batch transactions or hash the total state of the system. Projects that use permissioned blockchains usually do not report any problems with a throughput however the most transaction-intensive projects, such as Pension Infrastructure, expect some scalability problems related to transaction processing by smart contracts.

9. Blockchain technology does not pose a threat of disintermediation of existing public institutions.

The vast majority of analysed blockchain-based solutions are either complementary or partially substitute to the existing public services. Complementary solutions build on top of existing processes, like in the Exonum project. Partially substitute solutions propose new ways of providing a service or organizing an administrative function. In the latter case, blockchain technology takes over some tasks from public institutions, such as for example attestation of identity, or eligibility check-up. These changes reduce paper work and generate time savings for administration. In none of the cases does blockchain disintermediate public institution. Chromaway is the only project that assumes a disintermediation of the notary.

10. Blockchain-based designs generate specific cost items, yet overall deployment costs should not be higher than for centralised designs.

Based on the evidence from Stadterspass project, where blockchain-based solution was chosen in a public tender, the overall level of implementation costs is competitive. Blockchain-based services also have similar structure of non-recurring costs as centralised services. On the other hand designs which leverage permissionless blockchains involve new cost item: fees for validating transactions, denominated in volatile cryptocurrencies. Using computationally heavy and hence energy intensive consensus mechanisms to validate multiple transactions may generate substantial operating costs to the administration or citizens. It also generates an external environmental cost.

11. Blockchain-based services promise a range of benefits to the ecosystem.

The main benefit drivers of blockchain technology in public sector are process efficiency and transparency of transaction data. Reduced registration and verification times, quicker

and more reliable settlement of transactions and elimination of hard copies could potentially generate huge savings in operation and administration costs. Blockchain technology promises also a number of qualitative gains, which increase trust in record-keeping: higher security and resistance of a ledger and increased integrity and auditability of data. Elimination of a centralised validation function brings also strategic benefits to the non-governmental actors in the ecosystem. For example users can gain full control over their personal data and become largely independent from central repositories. Last but not least, blockchain-based services combined with digital user interfaces can improve the experience of interacting with the public authorities. Elimination of hard copies and visits to the town hall to validate documents or receive certified copies are the examples changes that can be expected, and would be endorsed, by the citizens.

3 Exploration of potential for scale-up of blockchain services

The case studies presented in chapter 2 represent the state-of-art developments of blockchain technology in the public sector within Europe. All analysed services, including operational implementations, are currently limited in scope to a single local or national administration. This chapter examines the potential of the services to be scaled up. Scaling up is understood here as expanding the outreach of a service to another local or national administration and not simply as an increase in a number of users within a single implementation.¹⁰ It is important to note that we assess a scaling potential of the service by looking solely at generic design principles. In particular we do not assess specific technical solutions provided within the projects or the organizational capacities of a particular project consortium or technology provider to engage in multiple implementations.¹¹ We also put aside restrictions related to the reuse of proprietary software components that may be present in few cases.

3.1 Assumptions

Adoption of the same service across different administrations can be advocated on technical and economic grounds. For example, different administrations could use the same software protocols based on open standards or create a shared infrastructure of validating nodes. Most importantly however certain blockchain-based services have the potential to release huge positive externalities on the demand-side, when scaled-up. For example, the creation of a common system for the verification of academic credentials on the European level could bring more value than separate country-level systems. The additional value, in this case, lies in support for cross-border education and recognition of diplomas and an increase of cross-border labour mobility. In order to release these benefits, a coordinated implementation of a credentialing service would be needed with interoperability between country-level systems and common governance. This scenario assumes coordination either on the EU level or at least at the level of a group of countries. Some services may not generate significant demand-side externalities from extending the scope across administrations. Still it might be worthwhile to replicate the same design in different countries and gain from using a proven protocol or a shared infrastructure. Hence, depending on the nature of cross-administration and cross-border externalities, two scaling options can be logically differentiated: replication and coordinated implementation. They are further described in Table 10 below.

Several technical, legal and economic aspects need to be considered in the assessment of scaling potential, for example:

- Whether additional benefits or positive network externalities can be realized when a solution is scaled;
- Whether economies of scope are likely to occur, for example by avoiding duplication of infrastructure;
- To what extent the developed service contributes to an important policy domain of the European Union;

¹⁰ It is well known that digital systems, including also decentralised or peer-to-peer systems are in general easily scalable. This is caused by the two supply side factors: economies of scale and decreasing capacity costs. Economies of scale relate to the fact that adding an extra user or transaction within a current capacity of the system generates zero marginal costs. Capacity can be increased by adding fixed-cost hardware elements. Over time the unit fixed-cost of expanding capacity has been sharply decreasing due to continuous innovation in microelectronics. Public permissionless blockchains represent an exception to this rule as they use a computational heavy mechanism to validate transactions which restricts capacity expansion. However other types of DLT systems are easily scalable.

¹¹ The conclusions from the scaling analysis must not be, in any event, interpreted as a recommendation for or against any particular technology provider or any particular technical solution implemented in the analysed services.

- If the underlying blockchain architecture and functionalities have sufficient technical maturity for production, including legal compliance;
- If specific adjustments to non-harmonized legal and institutional frameworks will be required.







Table 10. Scaling options for blockchain-based services

Aspect	Replication	Coordinated implementation
Description	The solution is offered as a service to another Member State or a local administration.	The solution is deployed across different Member States in a coordinated way with joint governance.
Implications	Software and protocols: The same user apps, APIs and blockchain protocols are utilized.	Software and protocols: The same user apps, APIs and blockchain protocols are utilized.
	Governance and interoperability: Blockchains are logically and institutionally separated. There is a separate governance body in each Member State. Legal harmonization is not required. Technical and semantic interoperability are not required (although exist by definition).	Governance and interoperability: Blockchains are logically interconnected. There is a common governance body formed by public actors from each Member State. Legal harmonization is required. Technical and semantic interoperability and are in place.
	Infrastructure: Either a separate or a common infrastructure is used by another Member State.	Infrastructure: Common infrastructure is used by the Member States.
Example	Ex1. Sweden productizes its property transaction solution and offers an 'instance' to France as a service. France thereby uses Swedish infrastructure or extends it by adding a number of own servers. Ex2. Italy replicates academic credential verification solution from Malta, using available open source libraries and own infrastructure.	Common frameworks for property transactions or credential verification are established in the EU. All interested Member States deploy this framework based on the European guidelines and standards. Dedicated European infrastructure is established to run the service. Each country hosts a number of servers. The same protocols and standards are utilized in each Member State.
Potential domains of application	Areas under exclusive or shared competence of the Member States: taxation, social policy, industrial policy, health protection, education.	Areas under exclusive or shared competences of the EU: customs, internal market, consumer protection, education, innovation policy.

Source: Own elaboration.

Building on the above considerations, five different technical, economic and institutional factors that affect scaling potential are explored: benefits, costs, technological maturity, priorities of the EU policies, institutional and legal compliance. Given a qualitative nature of the empirical evidence that is available, the contribution of each factor to the scaling potential is evaluated on a simplest 3-level ordinal scale, with levels represented by Harvey balls. Once these factors are evaluated, the two scaling options are assessed on another 3-level scale. Figure 16 provides a reference for the interpretation of both scales.

Figure 16. Evaluation scales for scale-up

Contribution of a given factor to the scaling potential	Low	Medium	High
			
Recommendation for each scaling option	Option not recommended	Option can be considered	Option recommended
			

Source: Own elaboration.

In what follows we evaluate the scaling potential of each service individually.








3.2 Evaluation of individual services

Land title registry

The land title registry service provides a digital certificate of a land title and uses blockchain to provide an additional layer of verifiable proof of the existence of the transaction. Also, the service speeds up registration of titles by using a private blockchain. The benefits to be realized when implementing a land title registry across borders with a similar set of functionalities are limited. Most property transactions occur within countries and a common title registration service would need to be fully aligned with legal systems of all countries in order to work. Each Member State has its own institutions that have own roles in the registration and verification of the transactions. These roles would need to be harmonised. The costs involved in this harmonisation would likely outweigh the benefits. Also the advantage of a blockchain-based registration system vis-a-vis efficient, centralised registry is debatable.

Transaction throughput is sufficient for production implementation. The blockchain layer already allows for 5.000 transactions per second between the private nodes and the hashes of the registered titles can be placed on a public blockchain in batches. However, in order to scale a system to another country, the institutions responsible for registering the real estate transactions would need to function as host nodes. The implied architectural consequences would likely reduce the economies of scope. In addition, harmonization of land title registration is not a key policy area for the EU. Hence, coordinated implementation of the service is not recommended. Replication would be a more practical option, as the infrastructure could more easily adapt to the legal environment in this way.

Table 11. Land title registry scaling exploration

Factors					Scaling option	
Benefits	Costs	Tech maturity	Policy priority	Institutional and legal compliance	Replication	Coordinated implementation
						

Source: Own elaboration.

Academic credentials verification

The service allows users and businesses to verify their academic credentials. When deployed cross-border, the potential outreach of a credential issued in the system rises. The cross-border dimension provides a clear business case for distributed ledger which is not addressed by any legacy system. Scaling to different countries would increase the value of the system. The service is as valuable as the number of businesses and institutions that accept and use the common solution. Scaling would require additional integration into the systems of the educational institutions in order to issue the credentials. The technical architecture allows batches of certification hashes to be stored

on the blockchain. If scaled across various countries, the same blockchain platform must be used. In addition, recognition of academic credentials supports important policy areas of the EU. It would complement standardisation of education profiles across universities based on ECTS and support cross-border exchange programmes. The EU-wide recognition of certificates of accomplishment and academic diplomas would improve operation of labour markets and increase labour mobility. As a result, coordinated scaling of the service to other countries would potentially result in more benefits than costs and contribute to the key policy areas. The technology used is mature enough for this specific use case, however when different types of credentials will be added, more effort will be required in order to ensure semantic interoperability. A solution backed by open source software has more chances to diffuse and cover different types of citizen records, such as birthday or marriage certificates. Both replication and scaling could occur. Replication would represent a more incremental approach that is likely needed given the required integration with the educational institutions. However, this could also be leveraged by the coordinated approach that would implement the EU-wide recognition of academic diplomas that can be verified in a distributed manner. The main current inhibitor to deployment of the service relates to potential non-legality of using electronic credentials and their validation on blockchain.

Table 12. Academic credentials scaling exploration

Factors					Scaling option	
Benefits	Costs	Tech maturity	Policy priority	Institutional and legal compliance	Replication	Coordinated implementation

Source: Own elaboration.

Property transactions

The service developed goes beyond mere registration of land titles. It looks to facilitate the end-to-end transaction of real estate for all actors, while increasing security and transparency of the process. The service covers also real estate transactions involving mortgage deeds and promissory notes. Similarly to the land title registry service, there are limited benefits to be realized when implementing property transactions across borders. In addition, in the current system there are already concerns about the legality of the transactions. Scaling to other countries would only add to this uncertainty. Although difficult to assess, the private permissioned blockchain architectural set-up is likely to facilitate scaling comfortably. However other countries involve specific institutions in the real estate transactions, so that smart contracts steering the cross-border workflow would need to be redesigned and extended. As a result, this service is at this stage of technological maturity and legal harmonisation too complex to scale to other countries in Europe. Replication could possibly occur, given that the same actor types would be present and that the regulatory environment would be relatively similar.

Table 13. Property transactions scaling exploration

Factors					Scaling option	
Benefits	Costs	Tech maturity	Policy priority	Institutional and legal compliance	Replication	Coordinated implementation

Source: Own elaboration.

Decentralised identity

The blockchain-based identity solution uses DLT in order to attest the residence, authenticate for e-government services and share government-attested personal data. It

provides a foundational component for other decentralised or centralised services that require user identity management. The issuer of traditional identity keeps a centralized record of the identities, and will continue to do so in order to attest that the person is who he or she says she is. However this only needs to happen once, after which the citizen could start providing a verifiable proof of his identity, using blockchain technology, without engaging the authorities. The service can be used to provide authenticated access to multiple public or private services, hence complying with the Once-Only Principle (European Commission, 2017a). The Once-Only Principle requires that individuals and businesses should not have to provide the same information more than once to public administrations. Already potential scaling of decentralised ID is explored at Swiss Kanton and federal level. The benefits of scaling this service to other regions or countries include a single user management system for public/private organisations and a common interoperable identity solution that can be used for several public and private services in different countries or regions. Some technical hurdles need to be overcome before realizing this, such as the choice of blockchain platform and the run-time environment for smart contracts. Electronic authentication of citizens is a key policy area of the EU, as can be seen in the creation of the eIDAS regulation (European Parliament & European Council, 2014). Leveraging this solution for various countries could benefit other blockchain pilot deployments, such as voting, as user management systems are often referred to as challenges in the other case studies. A single solution could be replicated, but in principle several different identity management systems could co-exist as long as interoperability between them is ensured. Hence the benefits from the top-down coordinated implementation of exactly the same solution across all Member States are not evident. Lighter coordination, ensuring adherence to common standards seems to be the optimal scenario.

Table 14. Decentralised identity management scaling exploration

Factors					Scaling option	
Benefits	Costs	Tech maturity	Policy priority	Institutional and legal compliance	Replication	Coordinated implementation

Source: Own elaboration.

Blockchain governance framework and hosting infrastructure

Common blockchain governance framework does not provide any service for end-users. It sets a number of compliance conditions for validating nodes in permissioned blockchains and separates infrastructure and application layers. Establishment of reference blockchain infrastructure composed of certified, independent nodes to host public services has already become a policy priority for the EU. It is recognized that on such infrastructure blockchain-based services could be faster, safer and more securely deployed. Because of the inherent cross-border application, positive effects driving scaling potential are obvious. The more businesses and institutions would adopt the common framework and participate in the hosting infrastructure the safer and more secure it would become. Hence, on the benefits side there are positive network externalities. The governance framework would contribute to the increasing use of permissioned blockchain networks for the public sector, which in general enable more advanced functionalities and can process more transactions. The costs and technical consequences would be limited. The framework could be used to eliminate legal barriers and move towards production those blockchain use cases that involve citizen data. Both the replication, where different countries support the initiative, and coordinated scaling, where the network is expanded to cover all European countries, could apply.

Table 15. Blockchain governance framework scaling exploration

Factors					Scaling option	
Benefits	Costs	Tech maturity	Policy priority	Institutional and legal compliance	Replication	Coordinated implementation

Source: Own elaboration.

Pension administration

This service aims to provide blockchain back office for pension system management. Potential benefits from having a decentralised but integrated information system with interfaces for employers, employees, tax authorities and pension funds are huge. The benefits are realized by having access to the same transaction data by various actors in the ecosystem. Yet the administration system tailored to a pension system in one country is not easily scalable to other Member States, due to large differences in institutional settings. Coordinated scaling is likely to have huge technical consequences and related costs. It would require incorporating more actors that act under different legal conditions and pension regulations. It is also questionable whether blockchain infrastructure would be able to facilitate the required throughput of one complex system. Yet the benefits from such a solution would accrue mainly to those citizens that have been working in various countries throughout their career, but not for domestic workers. The political adherence of this use case is also limited although it might grow in the coming years in case of the success of Pan-European pension plans. Recently the European Commission has proposed the Pan-European Personal Pension Product (PEPP) with an objective to bring transparent, flexible and easily portable pension plan to the market. This initiative clearly aims to target the needs of increasingly mobile workforce with a standardised pension product, but yet does not introduce any changes to the pension administration side. Given the current immature state of technology, the service seems too complex with an ecosystem that is too large to benefit from a larger scale than a single country. If the technology reaches a mature enough stage for production, replication of the service in a different country could be implemented after significant customization.

Table 16. Pension administration system scaling exploration

Factors					Scaling option	
Benefits	Costs	Tech maturity	Policy priority	Institutional and legal compliance	Replication	Coordinated implementation

Source: Own elaboration.

Smart vouchers

Smart vouchers aim to promote social inclusivity by allocating subsidized services to low-income citizens. The service does so by prescribing customized digital rights. The use of vouchers is monitored via a blockchain-based system. By implementing the concept of programmable money the service improves allocative efficiency and accountability for spending public funds. This functionality could be scaled and leveraged on a larger scale, with other institutions dedicating money for specific purposes and a larger community of citizens to reach. Scalability is not foreseen as an issue, especially with the development of the Lightning network.¹² The scope of the system could also be expanded to grant management. For a larger scale implementation, a solid proof-of-identification

¹² The Lightning network is an additional layer on top of the Bitcoin protocol to facilitate instant payments while ensuring scalability, currently under development: <https://lightning.network>

mechanism needs to be built in. From a security point of view, the service would still be reliant on external security measures (for example showing an ID with picture for accessing the discount/grants). Social inclusion is also a key priority for the European Union. Replication where different municipalities or regions could leverage a common infrastructure would be best suited. Scaling the current system to the national or the EU-wide level brings challenges in terms of having a solid user management system that fits with the specific legal environment. Also the economic justification of a top-down implementation is problematic because positive externalities are not immediately apparent.

Table 17. Voucher system scaling exploration

Factors					Scaling option	
Benefits	Costs	Tech maturity	Policy priority	Institutional and legal compliance	Replication	Coordinated implementation

Source: Own elaboration.

3.3 Insights from scale-up exploration

The exploration of the scaling potential of the services results in the following overview and insights:

Table 18. Scaling potential of blockchain-based services

Blockchain-based service	Factors					Scaling option	
	Benefits	Costs	Tech maturity	Policy priority	Institutional and legal compliance	Replication	Coordinated implementation
Land title registry							
Academic credentials verification							
Property transactions							
Decentralised identity							
Governance framework and infrastr.							
Pension administration							
Smart vouchers							

Source: Own elaboration.

Out of seven considered solutions, two can be recommended for coordinated implementation: (i) blockchain governance framework with hosting infrastructure and (ii) academic credentials verification. Both services generate positive externalities driven by interoperability and fit into policy priorities of the EU. The governance framework and hosting infrastructure present a possible basis to smoothen any legal hurdles in terms of where data is stored, and could be a catalyser for moving blockchain use cases that involve citizen data into production. The credential verification service provides a possibility of creating an EU-wide multisided platform bringing together issuers (universities), certificate holders and third parties (employers, universities). The credentials are recorded electronically in a standardised form and stored at the holder's

level. The benefits, including strong positive externalities, for all three groups of participants are evident.

Two other services, smart vouchers and decentralised identity, are border-line cases for the top-down scenario. Optimally both services require interoperability but not necessarily the same technical specification. Redistribution policies remain in the domain of the Member States. Hence, scalability of the smart voucher system can be justified up to the national level but makes little sense above. On the other hand government-attested decentralised identity is the key foundational building block for transformative digital services based on blockchain technology. Most probably, citizens would prefer to use only one self-sovereign personal data management system for all digital services that require identification. In principle, however, there is no reason for everybody to use exactly the same solution as long as different identity management systems provided on a competitive basis are standardised. An important step in ensuring this has been made in the eIDAS Regulation, which mandates mutual recognition of eID schemes across Europe by 29 September 2018.

All four services discussed above, and in particular the two border-line solutions, could be also replicated in different administrations. This approach would be recommended at the current stage to allow for more experimentation and technical checks. Nevertheless the full range of benefits can only be maximized under interoperability, which requires either full top-down implementation or at least light coordination.

Out of the remaining three services, pension administration and property transactions are the two which score low in technical maturity or legal compliance and hence are not ready for scaling-up at the current stage. The amount of customization required and technical limitations, like throughput, are the main barriers for replication. In fact, both services are still in the proof-of-concept phase. Once they advance in the development life-cycle, the scale-up assessment can be revisited towards bottom-up model. The land title registration service has already reached technological maturity and demonstrated legal compliance, but does not generate sufficient positive externalities. Hence, this service could only be replicated in another country.

4 Conclusions and policy recommendations

This study investigated a the number of ongoing blockchain developments in the public sector in Europe in order to assess how blockchain technology starts influencing operation of governments and the life of citizens. This section draws the final conclusions from the study and recommends policy actions in order to utilize the full potential of blockchain technology for digital governments. Conclusions and recommendations are structured along the four research questions of the study:

- Scope: What activities blockchain can serve from the public sector perspective and what are governments currently doing with this technology?
- Benefits: What benefits does blockchain bring for digital government and, in particular, for citizens?
- Scale-up: Which blockchain services developed within ongoing projects can be scaled-up beyond their current scope?
- Policy agenda: What policy actions are needed to fully utilise these technologies for the benefit of society and citizens?

4.1. Main conclusions from the study

The scope: Contrary to how it is often portrayed, blockchain, so far, is neither transformative nor even disruptive for the public sector. We have not observed the creation of new business models, the emergence of a new generation of services nor direct disintermediation of any the public institutions involved in the provision of governmental functions. Truly transformative services which enable decentralised voting or civic governance without direct involvement of governments are missing from the current landscape.

From the perspective of ongoing projects which develop public services, blockchain technology principally offers efficiency improvements in record keeping. By recording extracts of documents on a public distributed ledger, which is opened to everyone, governments can increase reliability of the record keeping of their own centralised registries. Blockchain ledger can be updated in an append-only manner and link current entries with previous transactions. This implies that the history documenting transitions between different states of the ledger is integral, accurate and fully auditable. The fact that blockchain ledger is distributed, implies that every node runs the same shared copy of the ledger, which makes it resistant to crashes or malicious behaviour. Some blockchain-based implementations simply utilize these technological features to establish an additional layer of trust on top of existing centrally provided registry services. Services that build on these trust-by-design and security-by-design features of blockchain currently constitute the main area of experimentation and are closest to market maturity.

But the experimentation with blockchain in the public sector goes beyond rudimentary applications that focus on notarisisation via distributed consensus. Some projects use blockchain as a shared database technology. Such database is a single source of truth that enables automation of business processes involving multiple agents, including both private parties, public parties and citizens. Smart contracts are programmable executables, anchored in the blockchain, that interact with other smart contracts and real users based on a specific system state. This allows for controlling and executing more advanced workflows based on various possible contingencies that can be shaped by users or external factors. Another side of the coin is that the content of the smart contract has to be carefully designed and properly coded to evoke an exact behaviour at exact conditions. In real life implementations reconciliation mechanisms must be in place to correct for instances of improper operation or errors in code.

Smart contracts are an advanced and powerful functionality of blockchain technology that increases the efficiency and reduces the uncertainty of transactions. In the context of the

analysed projects smart contracts are applied to targeting social benefits, facilitate economic transactions on property markets and support regulatory foresight and administration of pension system. Advanced workflow-based applications have a longer way to the market, due to their complexity and compliance issues. Narrower applications, which use smart contracts for a specific task, such as eligibility check or store of personal identifiers are already operable.

Blockchain also holds a promise to shift the power from a central intermediary towards an ecosystem. The fact that centralised parties are no longer needed to assure transaction validity may have various implications for governance and political processes, starting from the expansion of self-governed and self-sustainable forms of direct democracy. Blockchain offers ways to increase the transparency of governmental institutions in areas like public finance or expand citizen's control over election procedures. These examples of potentially transformative applications of blockchain as a new governance mechanism are not currently explored in ongoing experimentation. This trend will likely continue in the coming years for two reasons. First, at this stage technology does not seem to guarantee reliability to be entrusted a role of sole intermediary. Currently multiple centralized technologies like central registries are still needed to support it. Second, bureaucratic institutions may not be interested in limitation of their power in favour of a consensus mechanism established directly between citizens.

The benefits: Significant incremental benefits can be realised in some areas through the utilisation of blockchain technologies for the provision of public services. The two main groups of benefits related to blockchain are increased security (enhancement of data integrity, immutability and data consistency between organisations) and efficiency gains (such as reduced processing time and lower costs).

Ongoing experimentation is still on a relatively early stage with only few operational implementations. The analysed projects demonstrate however that blockchain technology can indeed be expected to increase efficiency and reliability and reduce transactions costs and uncertainty. These potential benefits will be allocated to administration, citizens and society as a whole. Services utilizing blockchain-based notarization increase the auditability of data and the transparency of administrative processes. Immutability of records on the ledger can possibly enlarge trust of citizens and companies in the governmental record-keeping. Blockchain can also increase reliability of markets on which governmental institutions participate as providers of information and facilitators of transactions. Besides trust and reliability, blockchain generates efficiency gains measurable in monetary terms. For example, streamlining mortgage handling and transfer of land titles in a smart contract workflow, shortens property transaction times from weeks to hours. Quicker settlement reduces property transaction costs and improves liquidity on the market, providing possibilities for more economic activity. Given the high value of traded properties these savings may account for hundreds of millions of Euro annually. Blockchain based pension management system is another example of potentially high gains induced by smart contract workflow. Smart contracts allow for high level of process automation, which translates to lower administration costs, elimination of paper work and storage costs. At this point impressive monetary gains expected by some projects are just promises which need to be proven as these services become operational.

Shared ledger offers also new opportunities for governmental institutions in policy design and regulatory oversight. For example, an immediate access to the actual information about the state of the pension system or business transactions among business would greatly enhance ways, in which governments can counteract fraud or tax evasion. The smart voucher program for promoting social inclusion is another successful. Besides administration savings due to automation of management process, smart contracts improve the allocative efficiency of public funds and their targeting to beneficiaries.

From the citizen's perspective blockchain in combination with other digital decentralised technologies can eliminate excessive bureaucracy, hard copies or visits in the town hall in

favour of remotely operating mobile apps. Part of the improved user experience from interacting with the public authorities relates to gaining independence, also known as self-sovereignty. Having full control over their personal data, citizens become largely independent from central repositories which can only be endorsed. It is important to note that as the blockchain based services are mostly in a pilot phase or operate in a small scale, these gains are not accessible yet. It is also worthwhile to recall that blockchain technology constitutes always just one of several layers in the technical design of the service. Hence the value from a service derived by the users has to be accrued to a bundle of different technologies and functionalities.

Scale-up: Verification of academic credentials is the only end-user service in the sample that can be recommended for top-down implementation in form of EU-wide multi-sided platform. The service generates network benefits across universities, citizens and employers and responds to policy priorities. The technical design is mature and relies on existing open source standards and public blockchain infrastructure. While few other services already have relatively mature technical designs that could be launched in different administrations, such replication should first of all serve testing purposes. At this stage of the technology life cycle, the continuation of experimentation with different technical designs is vital. Prior to the scale-up, technical and governance standards need to be developed, in order ensure interoperability of different designs and facilitate operative services.

The majority of the analysed services are not ready for scaling-up in their current form. This is caused by insufficient technical maturity or noncompliance with legal environment, for example with regards to legality of digital signatures and notarization via cryptographic proofs. In case of complex designs, extensive customization to local institutional setting is another barrier to scaling. For example solutions using blockchain as a shared database, require the integration of diversified legacy databases in the ecosystem. Several projects are currently working on solving these various technical challenges. Hence even the most complex solutions that are currently in the proof-of-concept phase could at some point be replicated in different administrations after the necessary customization. However, even if technical and legal obstacles are overcome, there is still no good reason to stick to a single technical solution instead of having a choice between several competing but standardised designs for example for identity management. Prior standardisation is particularly important for foundational services: governance framework and decentralised identity management as these elements constitute building blocks for end-user services.

Out of seven analysed services, two can be recommended for top-down implementation. To release full benefits of these services, closer coordination between institutions from different Member States is required during implementation and operation. Top-down implementations must be streamlined with common guidelines to ensure compliance with security or privacy requirements and technical interoperability. The academic credentials verification service is based on open source libraries and documentation, which constitute an open source standard. Moreover it uses tested environment of public blockchains, while being platform agnostic and implements well known notarization functionality. Given clear-cut value for citizens and no risk of lock-in for the issuers, the academic credentials verification service could be scaled-up to the EU level.

Policy agenda: Incompatibility between blockchain-based solutions and existing legal and organizational frameworks is a major barrier to unlock the transformative potential of blockchain. Hence, the major policy objective should be to increase the technological and ecosystem maturity of distributed ledgers. Unlocking transformative potential of blockchain requires several actions, elaborated in great detail in the next section. Policy actions should aim not only at adaption of the technology to existing ecosystems but also at transformation of existing processes, organizations and structures using the disruptive potential of blockchain.

4.2. Recommended policy agenda

In order to unlock the transformative power of blockchain, technological and ecosystem maturity of distributed ledgers have to increase. This principal policy objective can be translated to a set of specific goals and policy actions that spur exploitation of the full potential of blockchain technology:

1. **Guidance & knowledge sharing** – Create programs for sharing best practices on blockchain deployments between the Member States and providing guidelines and recommendations to develop knowledge on the technology.
2. **Focused pilot development** - Identify key use cases and ongoing implementations in line with the EU policy priorities. Co-finance pilot projects which experiment with blockchain technology and new re-engineered administrative processes in the areas of relevance.
3. **Standards definition** – Support the development of international standards on security, privacy and governance. Create certification process to ensure compliance of blockchain architectures with these standards.
4. **EU blockchain foundational components** - Provide foundational components to support the utilization of blockchains, such as data model for certificates credentials and distributed identity management.
5. **Use case-based dedicated infrastructures** - Define reference conditions and create shared infrastructures most suitable for specific use case types, such as land title registries or tax systems.

All recommended actions already are to different extents part of the policy agendas of the Member States and the EU. Support to knowledge sharing, capacity building and framing conditions can be provided in parallel and without any preconditions (see Table 19). The last two steps: development of blockchain building blocks and dedicated infrastructures, are conditional on the emergence of security, privacy and governance standards. Specifically, technical and interoperability standards are necessary for large-scale, cross-border use cases.¹³

Guidance and Knowledge Sharing

An approach that is argued to benefit all blockchain-based pilot deployments is ensuring guidance and knowledge sharing on this immature yet developing technology. Better knowledge on the topic for all ecosystem actors will result in easier adoption and increased effectivity. The European Commission and Parliament have already recognized the relevance of expertise building over the last two years. In order to “highlight key developments of the blockchain technology, promote European actors and reinforce European engagement with multiple stakeholders involved in blockchain activities”, the European Commission has launched the EU Blockchain Observatory & Forum (European Commission, 2018c). In addition, the EC has been funding blockchain projects through research programmes FP7 and Horizon 2020 since 2013, and projects can be funded up to 2020 with funds accumulating to €340 million. This potential policy action builds upon these existing actions and focusses on creating a program for sharing best practices on blockchain deployments between the Member States and providing teaching programs to develop knowledge on the technology. This could still result in the various blockchain protocols used for similar use case types and allows the market to develop standards and requirements for the infrastructures.

¹³ In the Annex to this report we elaborate in greater detail on the use of blockchain against VAT fraud. This is an example of a complex use case, which under current state of technology life cycle is premature.

Table 19. Recommended policy actions

	1. Guidance and Knowledge Sharing	2. Focused Pilot Development	3. Standards Definition	4. EU Blockchain Connection Building Blocks	5. Use Case-Based Dedicated Infrastructures
Goal	Expertise building	Development of high value pilots	Framing guidelines	Creation of building blocks that connect services using blockchain technologies across the Member States	Creating dedicated infrastructures for use case type
Exemplary activities	Sharing best practices on blockchain deployments between the Member States. Providing teaching programs to develop knowledge on the technology	Identify use cases and implementations in line with the EU policy priorities. Co-finance pilot projects using blockchain for digital government.	Development of international standards. Certification process to ensure compliance with security and privacy.	Providing building blocks supporting the utilization of blockchains: certificates and identity management system.	Defining or creating infrastructures most suitable for use case types, such as property transactions, pension administration or tax systems.
Technology maturity dependency	Low maturity	Low maturity	Maturing	Mature	Mature
technology standardisation dependency	Low – Infrastructures are created or used based on best practices	Low – Infrastructures are created or used based on best practices	Medium – deployments compliant with security, privacy and governance standards	High – Interoperability standards on technology and services level	High – standardised, interoperable dedicated infrastructures
Interoperability focus	Best practices	Best practices	Legal, Organisational, Semantic and Technological standards	Technological and service interoperability	Technological and service interoperability
Adoption Approach	Bottom-up	Bottom-up	Top-down	Bottom-up	Top-down
Government level for funding	Local/National and European	Local/National/ and European	European	Local/National and European	Local/National and European
Effect on current initiatives	Increased effectivity and easier adoption	Faster time to production	Increased cross-border and cross-pilot interoperability	Increased effectivity and potential to be incorporated with other services	Increased focus on services and applications

Source: Own elaboration.

Focused Pilot Development

Another recommended policy action should support development of blockchain pilots for digital government that are of high priority for the EU. In order to make this policy action effective, use cases which are in line with the EU priorities and experimentation gaps need to be identified. To cover high-priority gaps, the EU could co-finance pilot projects using funding mechanisms and research programs. For example explored pilots could contribute to key policy initiatives, such as creating a digital single market and supporting a democratic change (European Commission, 2015). This policy action would enable pilots to move faster to a production phase. It could still result in the various blockchain protocols being used in similar use cases while allowing for the development of common requirements for standards and infrastructures. Pilots focused on most

transformative use cases would also demonstrate to what extent administrative process must be re-engineered.

Standards Definition

The EU needs to focus on defining common standards for blockchain infrastructures. The proven model relies on the European and international standard setting organisations (ETSI, CEN/CENELC and ISO). The European Commission and several Member States have already recognized the importance of defining standards and participate in various working and study groups of ISO Technical Committee 307 on blockchain and distributed ledgers. The standardisation should conform with the European Interoperability Framework (EIF) (European Commission, 2017b), with a focus on legal, organisational, semantic and technological interoperability. This is particularly important for the EU-level use cases, which by definition have cross-border and cross-domain dimensions. In addition to engagement in standards setting, the EC may provide guidelines on which technological standards to use for specific use cases or even set up a certification body for blockchain infrastructures. Standards compliance will mark a critical point on the maturity scale of distributed ledger technologies. Still, the choice of a particular platform or infrastructure will have to be made by the Member States according to their needs.

EU Blockchain Connection Foundational Components

A more elaborated policy action is the creation of a number of foundational components that link and connect services using blockchain technologies across. These foundational components of infrastructures could be similar to the Connecting Europe Facility (CEF) building blocks, where a number of generic and reusable Digital Service Infrastructures (DSI) are created to establish cross-border interoperability and intercommunication (European Commission, 2018a). For blockchain infrastructures, these foundational components could support identity management systems, and include certificate issuance systems and hosting certification. This policy action could be implemented in a similar way as the CEF building blocks: by providing the EU foundational components service platforms and providing grants to support the implementation of these foundational components in the Member States. This policy action would require a lot of research and market consultation, yet it could enable a high degree of interoperability on a service level, allowing the Member States to use blockchain technology for their public services.¹⁴

Use Case-Based Dedicated Infrastructures

The most involved policy action to be taken by the EU is creating dedicated blockchain infrastructures for specific use cases. These are horizontal components, with for example one type of blockchain infrastructure for the registration of land titles or the verification of credentials. The top-down approach towards determination of the protocols used across the Member States for one specific use case, enhances interoperability and coordination yet potentially creates political and policy challenges. Importantly, this action would shift a focus from operational issues to services and applications as use case-based infrastructure could be leveraged. In 2017 European Commission has initiated an important first step towards the creation of dedicated infrastructures by launching the study on opportunity and feasibility of the EU blockchain infrastructure (European Commission, 2017c). In 2019 the EC has launched a call under CEF Programme to deliver a generic and reusable blockchain building block. This block, expected to come in 2020, will serve as a core service platform with identification and authorisation protocols running on permissioned blockchain with national nodes and the EU master node.

¹⁴ Actually, the recently approved CEF work programme 2019 will deliver a blockchain building block named European Blockchain Infrastructure Services. It will include an initial set of 4 use cases to be deployed on the new blockchain infrastructure: cross-border identity, diploma sharing, taxation and customs, and notarization. For details see <https://ec.europa.eu/digital-single-market/en/connecting-europe-facility>

References

- Ainsworth, R. T., & Shact, A. (2016). *Blockchain (Distributed Ledger Technology) Solves VAT Fraud* (SSRN Scholarly Paper No. ID 2853428). Rochester, NY: Social Science Research Network. Retrieved from <https://papers.ssrn.com/abstract=2853428>
- Atzori, M. (2015). *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* (SSRN Scholarly Paper No. ID 2709713). Rochester, NY: Social Science Research Network. <https://doi.org/10.2139>
- Back, S. A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., ... Timón, J. (2014). Enabling Blockchain Innovations with Pegged. *OpenScienceReview*.
- Boucher, P. (2017). *How blockchain technology could change our lives*. European Parliament Research Service. Retrieved from [http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA\(2017\)581948_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf)
- Brynjolfsson, E., & Hitt, L. M. (2000). Beyond Computation: Information Technology, Organizational Transformation and Business Performance. *Journal of Economic Perspectives*, 14(4), 23–48. <https://doi.org/10.1257/jep.14.4.23>
- Chromaway. (2017a). Blockchain and Future House Purchases Third phase to be completed in April 2018. Retrieved January 21, 2019, from <https://chromaway.com/landregistry/#oc-slider>
- Chromaway. (2017b). Blockchain Land Registry Report 2017. Retrieved from https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf
- Davidson, S., De Filippi, P., & Potts, J. (2016). Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2811995>
- Eurasianet. (2017). Georgia: Authorities Use Blockchain Technology for Developing Land Registry. Retrieved January 21, 2019, from <https://eurasianet.org/georgia-authorities-use-blockchain-technology-developing-land-registry>
- European Commission. (2015). The 10 priorities of the European Commission for 2014-19 [Text]. Retrieved January 21, 2019, from https://ec.europa.eu/commission/priorities_en
- European Commission. (2016). European eGovernment Action Plan 2016-2020. Retrieved January 18, 2019, from <https://ec.europa.eu/digital-single-market/en/european-egovernment-action-plan-2016-2020>
- European Commission. (2017a, February 1). EU-wide digital Once-Only Principle for citizens and businesses - Policy options and their impacts [Text]. Retrieved January 21, 2019, from <https://ec.europa.eu/digital-single-market/en/news/eu-wide-digital-once-only-principle-citizens-and-businesses-policy-options-and-their-impacts>
- European Commission. (2017b, February 16). The New European Interoperability Framework [Text]. Retrieved January 21, 2019, from https://ec.europa.eu/isa2/eif_en
- European Commission. (2017c, November 9). Study on opportunity and feasibility of a EU blockchain infrastructure [Text]. Retrieved January 21, 2019, from <https://ec.europa.eu/digital-single-market/en/news/study-opportunity-and-feasibility-eu-blockchain-infrastructure>
- European Commission. (2018a). About CEF building blocks. Retrieved January 21, 2019, from <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/About+CEF+building+blocks>

- European Commission. (2018b). Blockchain Technologies. Retrieved January 18, 2019, from <https://ec.europa.eu/digital-single-market/en/blockchain-technologies>
- European Commission. (2018c). EU Blockchain Observatory and Forum. Retrieved January 18, 2019, from <https://ec.europa.eu/digital-single-market/en/eu-blockchain-observatory-and-forum>
- European Commission. (2018d). How can Europe benefit from blockchain technologies? Retrieved January 18, 2019, from <https://ec.europa.eu/digital-single-market/en/news/how-can-europe-benefit-blockchain-technologies>
- European Council. (2017, October 19). European Council meeting (19 October 2017). Retrieved from <http://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/en/pdf>
- European Parliament, & European Council. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Pub. L. No. 32014R0910, 257 OJ L (2014). Retrieved from <http://data.europa.eu/eli/reg/2014/910/oj/eng>
- EVRY. (2016). Blockchain - Powering the Internet of Value. Retrieved from <https://www.evry.com/globalassets/insight/bank2020/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf>
- Freeman, C., & Perez, C. (1988). Structural crises of adjustment, business cycles and investment behaviour. In *Technology, Organizations and Innovation: Theories, concepts and paradigms* (Dosi G., Freeman C., Nelson R., Silverberg G. and Soete L., pp. 38–66). London, N.Y.: Pinter Publishers. Retrieved from <http://www.carlotaperez.org/downloads/pubs/StructuralCrisesOfAdjustment.pdf>
- Gartner. (2018a). Hype Cycle for Blockchain Business. Retrieved from <https://www.gartner.com/doc/3884146/hype-cycle-blockchain-business->
- Gartner. (2018b). Preparing for Smart Contract Adoption. Retrieved February 7, 2019, from <https://www.gartner.com/doc/3894102/preparing-smart-contract-adoption>
- Gartner. (2018c). Top 10 Strategic Technology Trends for 2019. Retrieved February 7, 2019, from <https://www.gartner.com/doc/3891569/top--strategic-technology-trends>
- Grech, A., & Camilleri, A. F. (2017). *Blockchain in Education*. Luxembourg: Inamorato dos Santos (ed.). Retrieved from <http://nbn-resolving.de/urn:nbn:de:0111-pedocs-150132>
- Jovanovic, B., & Rousseau, P. (2005). *General Purpose Technologies* (NBER Working Papers No. 11093). National Bureau of Economic Research, Inc. Retrieved from <https://EconPapers.repec.org/RePEc:nbr:nberwo:11093>
- Kounelis, I., Di Gioia, R., Geneiatakis, D., Steri, G., Neisse, R., Karopoulos, G., ... Giuliani, R. (2017). *Blockchain in Energy Communities* (Technical report). Luxembourg: European Commission, Joint Research Centre (JRC). Retrieved from <https://ec.europa.eu/jrc/en/publication/blockchain-energy-communities-proof-concept>
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
- Norta, A. (2015). Creation of Smart-Contracting Collaborations for Decentralized Autonomous Organizations. In R. Matulevičius & M. Dumas (Eds.), *Perspectives in Business Informatics Research* (pp. 3–17). Springer International Publishing.
- Poniatowski, G., Bonch-Osmolovskiy, M., Durán-Cabré, J. M., Esteller-Moré, A., & Śmietanka, A. (2018). Study and Reports on the VAT Gap in the EU-28 Member States: 2018 Final Report TAXUD/2015/CC/131. Retrieved January 21, 2019, from

https://ec.europa.eu/taxation_customs/sites/taxation/files/2018_vat_gap_report_en.pdf

- Shin, L. (2017). The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project. Retrieved January 21, 2019, from <https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#5a9b2694dcdc>
- Smith, A., Stirling, A., & Berkhout, F. (2005). The governance of sustainable socio-technical transitions. *Research Policy*, 34(10), 1491–1510.
- Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc.
- The Bitfury Group. (2017, February 7). The Bitfury Group and Government of Republic of Georgia Expand Historic Blockchain Land-Titling.... Retrieved January 21, 2019, from <https://medium.com/@BitfuryGroup/the-bitfury-group-and-government-of-republic-of-georgia-expand-historic-blockchain-land-titling-4c507a073f6b>
- van Engelenburg, S. H., Janssen, M. F. W. H. A., & Klievink, A. J. (2017). Design of a software architecture supporting business-to-government information sharing to improve public safety and security: Combining business rules, Events and blockchain technology. *Journal of Intelligent Information Systems*. <https://doi.org/10.1007/s10844-017-0478-z>
- Van Zuidam, R. (2017). Blockchain for dummies - 5 questions to Blockchain expert Rutger van Zuidam. Retrieved January 18, 2019, from <https://www.cityoftalent.nl/en/news/blockchain-for-dummies---5-questions-to-blockchain-expert-rutger-van-zuidam>
- Warburg, B. (2016). *How the blockchain will radically transform the economy [TED talk]*. Retrieved from <https://www.youtube.com/watch?v=RplnSVTzvnU>

List of abbreviations and definitions

AFM	Authority for the Financial Markets
API	Application Programming Interface
BCT	Blockchain Technology
BRP	Basisregistratie Personen (Centralized identity registry in the Netherlands)
CEF	Connecting Europe Facility
CEN	European Committee for Standardization
CENELEC	Comité Européen de Normalisation en Electronique et en Electrotechnique
DAO	Decentralized Autonomous Organization
DG	Digital Government
DLT	Distributed Ledger Technology
DSI	Digital Service Infrastructure
ELISE	European Location Interoperability Solutions for e-Government
EC	European Commission
ECTS	European Credit Transfer System
EIF	European Interoperability Framework
EP	European Parliament
ETSI	European Telecommunications Standards Institute
EU	European Union
FP7	Framework Program 7
ID	Identifier
IFZ	Institute of Financial Services Zug
ISA	Interoperability Solutions for public Administrations
ISO	International Organization for Standardization
ITS	Institute of Tourism Studies
JSON	JavaScript Object Notation
KPMG	Klynveld Peat Marwick Goerdeler
KYC3	Know Your Customer, Counterparty and Competition
MCAST	Malta College of Arts, Science and Technology
MEDE	Ministry for Education and Employment (in Malta)
MIT	Massachusetts Institute of Technology
MTIC	Missing Trader Intra-Community
NAPR	National Agency of Public Registry (in Georgia)
OOP	Once Only Principle
OSS	Open Source Software
PoA	Proof-Of-Authority
P2P	Peer to Peer
PEPP	Pan-European Personal Pension Product

PI	Pension Infrastructure
PBFT	Practical Byzantine Fault Tolerance
PPF APG	Personeels Pensioen Fonds APG (Pension fund for APG's own personnel)
QR	Quick Response
R&D	Research and Development
RIVG	National Identity Service/Identity management authority (the Netherlands)
SBAB	SBAB Bank AB
SEPA	Single Euro Payments Area
SLA	Service-Level Agreement
TOOP	The Once Only Principle
Tps	Transactions per second
URL	Uniform Resource Locator
VAT	Value Added Tax
VIES	VAT Information Exchange System

List of figures

Figure 1. Case study assessment framework 15

Figure 2. Resume of Exonum case study 18

Figure 3. Land tile registration process by NAPR 19

Figure 4. Resume of Blockcerts case study..... 22

Figure 5. Blockcerts certificate verification process 23

Figure 6. Resume of Chromaway case study 26

Figure 7. Chromaway real estate transfer workflow 27

Figure 8. Resume of uPort case study 31

Figure 10. Resume of Infrachain case study..... 35

Figure 11. Infrachain governance framework overview 36

Figure 12. Resume of pension infrastructure case study 38

Figure 13. Pension Infrastructure project overview..... 39

Figure 14. Resume of Stadjerspas case study..... 42

Figure 15. Stadjerspas process flow 43

Figure 16. Evaluation scales for scale-up..... 59

Figure 17. Missing trader intra-community fraud 79

Figure 18. Smart contract workflow for VAT payments 80

Figure 19. Blockchain against VAT fraud..... 83

List of tables

Table 1. List of blockchain projects 14

Table 2. Blockchain archetypes 16

Table 3. Case study characteristics overview 46

Table 4. Functionalities overview 47

Table 5. Governance overview 48

Table 6. Usage overview 49

Table 7. Technical Architecture overview 50

Table 8. Costs overview 51

Table 9. Benefits overview 52

Table 10. Scaling options for blockchain-based services 58

Table 11. Land title registry scaling exploration 59

Table 12. Academic credentials scaling exploration 60

Table 13. Property transactions scaling exploration 60

Table 14. Decentralised identity management scaling exploration 61

Table 15. Blockchain governance framework scaling exploration 62

Table 16. Pension administration system scaling exploration 62

Table 17. Voucher system scaling exploration 63

Table 18. Scaling potential of blockchain-based services 63

Table 19. Recommended policy actions 69

Annex: Blockchain against VAT fraud

Another area where blockchain and distributed ledger technologies may bring substantial benefits is taxation and specifically value added tax (VAT) frauds. The VAT on final goods and services within the European Union (EU) is charged by a business and paid by its customers. In business-to-business domestic sales, a business receiving supplies must pay "input VAT" (that is, VAT on its input supplies), yet it is able to recover this input tax once the output is sold and taxable. This recovery is generally done by offsetting the input VAT against the output VAT, or if there is an excess by claiming a repayment from the government. These VAT returns occur by submitting VAT returns or declarations on a periodical basis to the tax authority of the EU country where the business is registered in. Vat accounting in cross-border intra-EU trade works similarly with the one important exception. Like in a domestic trade, VAT is collected by the tax authorities at each stage of the supply chain within a single Member State, yet the export of goods is free of tax. By means of the destination principle, VAT accrued in the exporting state is fully reclaimed by the company that sales it to another Member State. While intracommunity delivery is exempted from VAT, an importer charges the output VAT according to the local VAT regime of the importing country, passing on VAT credit to a subsequent company along the chain in importing Member State. Each Member State has its own VAT legislation and collection system that must comply with the provisions of the EU VAT law. There is an ambition to move towards a single EU VAT area, as can be seen in the Action Plan on VAT adopted in April 2016 by the European Commission. A single EU VAT area would contribute to the EU-wide single market that is deeper and fairer, and is argued to create additional jobs, growth, investment and competitiveness.

The current set-up of this system, where different legislations (with their own VAT rates) and collection systems exist across the EU, gave rise to a number of fraud mechanisms that are fought against in different administrative ways. These fraud mechanisms result in VAT not being paid to one of the countries in the supply chain, and the resulting VAT gap varies from less than 5% to more than 40% of the expected VAT revenues between the Member States. The most recent report published in September 2018 calculates the current VAT gap across the EU to be approximately €147.1 billion in 2016 (Poniatowski et.al 2018). The two principal fraud mechanisms are the missing trader intra-community (MTIC) and the missing trader extra-community (MTEC) frauds which account for €50 Billion due tax loss in goods and similar amount in services or intangible rights. In the domestic trade, fake invoices are the most common mechanism for committing VAT frauds.

Current measures to fight cross-border frauds in business-to-business transactions are based on the centralised VAT Information Exchange System (VIES), which is ineffective. Cross-border business-to-consumers transactions are more effectively protected via an electronic mini one-stop shop. In the domestic trade, anti-fraud measures rely on rapid controls and verifications of VAT claims. The current tracking measures are costly as they require operation of specialised investigation units inside tax authorities. Recently, thanks to the digitization of tax returns and electronic collection of invoice level data, tax authorities are able to perform a targeted risk analysis and selective cross-checks of individual transactions between taxable persons. Still, even under the data-intensive approach, a time between the moment of committing a fraud and its discovery is way too long in order to counteract frauds.

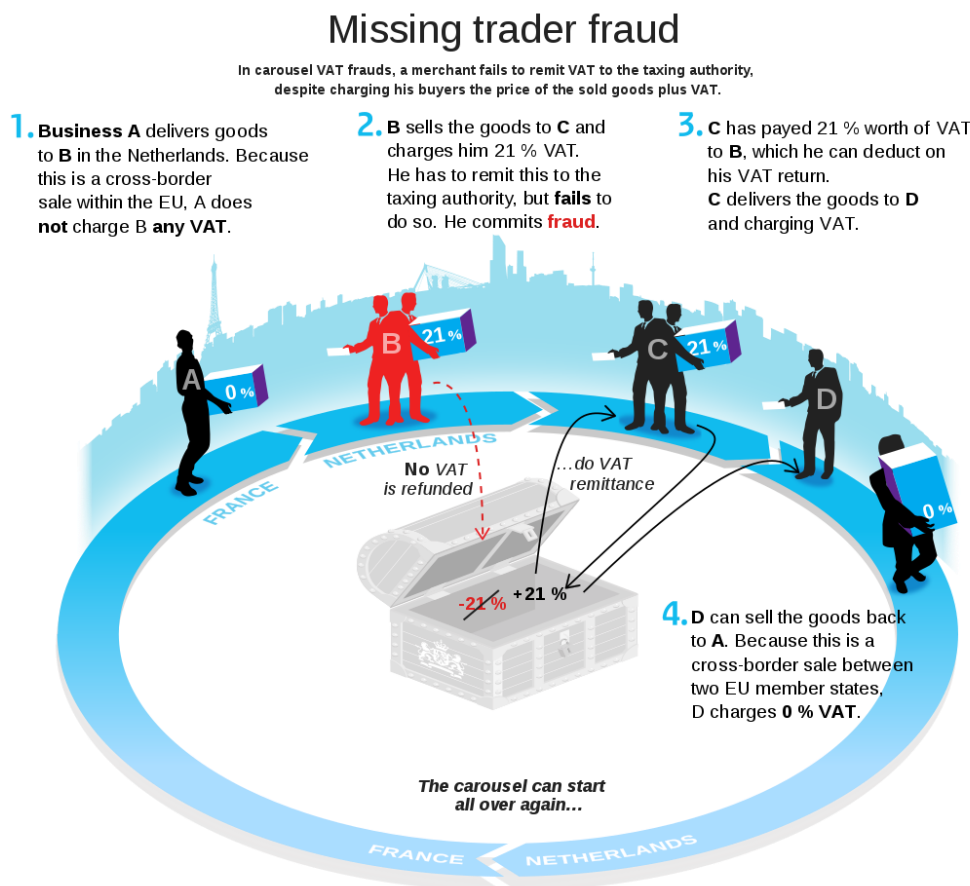
The state-of-art literature makes a strong point that the blockchain technology presumably may become a real game changer in fighting major forms of tax frauds. It is argued, that by coupling a real-time transaction registration on blockchain with an off-chain real-time tax payments, MTIC and fake invoice frauds could be eliminated. This would immediately cut the multibillion losses of tax revenue in the EU. Moreover,

contrary to the other debated alternatives¹⁵, recording business-to-business transactions on a distributed ledger, would not introduce distortions to the current vat regime.

Missing trader intra-community fraud

The MTIC fraud is a mechanism that abuses the way VAT is treated in the cross-border trading, where the movement of goods between jurisdictions is VAT-free. A fraudulent business imports goods from a company registered in another EU Member State. This transaction is exempted from VAT. Then, the fraudulent business sells the goods to another trader in his country for the price including a positive VAT. Instead of remitting this VAT to the government, the fraudulent trader disappears with money, hence becoming a missing trader. If the buyer further resells the goods to another company, he is entitled to reclaim paid VAT from the tax authority. At some point, the goods are exported to another country. This transaction is again exempted from VAT which causes a net damage to the public budget, because the tax authority has not retrieved any of the VAT that should have been paid. This fraud mechanism is often referred to as VAT carousel fraud, as fraudulent transactions often appear multiple times in a circular supply chain. An overview of the missing trader intra-community fraud can be found in the figure below.

Figure 17. Missing trader intra-community fraud



Source: Wikipedia.¹⁶

¹⁵ Such as generalized reverse charge mechanism or reversion to the origin-based VAT system.

The potential of blockchain technology against missing trader intra-community fraud

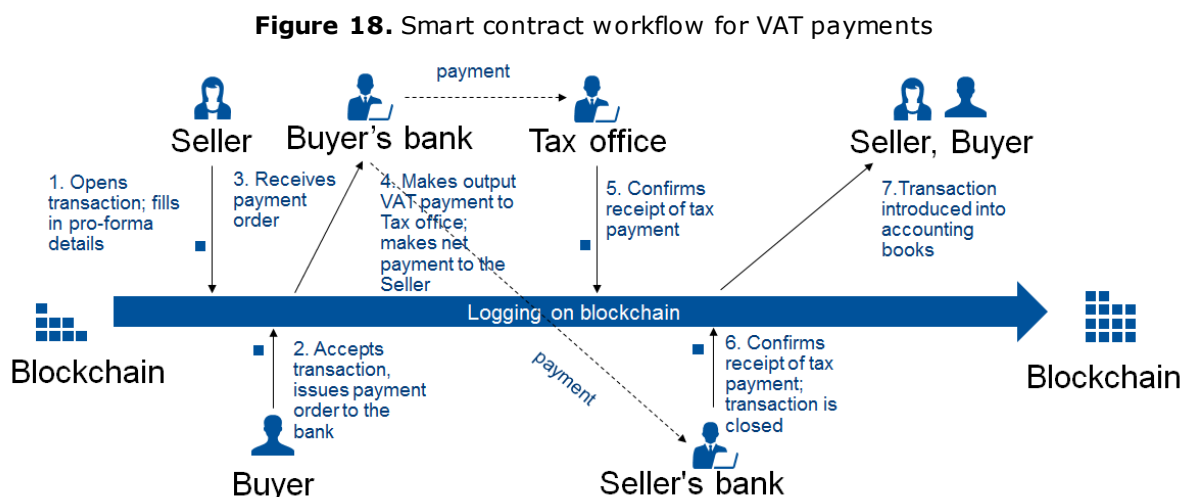
A number of researchers and institutions have argued for blockchain-based remedies to the missing trader intra-community fraud. According to Ainsworth & Shact (2016), the technology is able to bring efficiencies in the collection of VAT, reduce verification costs and improve relationships between governments. Ainsworth and Shact argue that these positive effects could generate a potential reduction of the VAT fraud of €50 to €60 billion per year. So far, the details of the blockchain design for the VAT anti-fraud have not been discussed in greater detail. This case study speculates on the potential architecture of an EU-wide blockchain system to collect VAT. We restrict the analysis to the three components of the blockchain assessment framework introduced in Chapter 2: functionalities, technical architecture and governance.

Functionalities

So far, two set-ups of a blockchain-based EU-wide VAT system have been explored. Ainsworth and Shact explore a Digital Invoice Customs Exchange using blockchain technology. A software architecture for business-to-government information sharing that leverages blockchain technology is proposed by van Engelenburg, Janssen, & Klievink (2017).

A blockchain-based system that would be used to register all transactions and support collection of VAT charges would, in principle, have to be based on a multi-directional smart contract between a buyer, a seller, the tax authority, a buyer's bank and a seller's bank. This system would register transaction details and govern transaction workflow between all involved parties (see Figure 18). The blockchain system would produce digitalized, invoice level data and introduce an automatic taxation by splitting the payment made via banking system. Another crucial change is a shared nature and a quick circulation of information in the system. The tax office would learn about the tax duty arising from a new transaction prior to the payment, in the moment of invoice issuance.

The blockchain-based system would require a distributed registration of all transactions that include VAT-eligible goods or services. It would also require a (near) real-time recording of the movement of payments when they occur as is shown in Figure 18.



Source: Own elaboration.

¹⁶ Source: https://en.wikipedia.org/wiki/Missing_trader_fraud#/media/File:Carrouselfraude.svg

Payments would still be done via banking system and not on blockchain – provided that:

- The seller's and buyer's banks become parts of the smart contract;
- Electronic payments are obligatory (cash payments in B2B transaction ruled out);
- A bank transfer is marked with a hash of transaction recorded on blockchain;
- The buyer's bank automatically splits payment, deducting payable VAT and transferring it to the respective tax office. A seller receives only the net payment.
- The smart contract receives signatures from the banks and tax office and completes the transaction, changing the status of an invoice from pro-forma (pending) to final (verified).

One major implication of the new system of transaction registration and supporting VAT payments is that the input-output VAT clearing would have to be done by the tax office and not by the firms submitting VAT declarations, as is the case at present. This could however be easily and reliably implemented based on the transaction data recorded on the immutable blockchain ledger. For each firm, the tax office would run its input-output VAT balance, continuously updated with new transactions recorded on blockchain. The tax office would remit to the seller part of the output VAT transferred by the buyer's bank. The upper limit for the repayment is the current amount of input VAT paid by the seller in up-stream transactions. The VAT clearing can be automatized, provided that the seller's bank has an access to the actual state of his VAT balance with the tax office.

Technically, the new system of transaction registration requires that businesses need to have a connection to register transactions and the blockchain protocol would need to be able to facilitate a high amount of throughput. This poses a potential threat: the total amount of transactions that are VAT eligible is extremely high, much higher than what the protocols of for example Bitcoin and Ethereum can comfortably facilitate.

Smart contracts are crucial in a system as such, as there needs to be some programmable logic that occurs based on the transactions. This poses two additional threats: the potential of smart contracts for exploitation and the lack of a superior arbiter. Smart contracts could be potentially exploited, as most of them are written in the Ethereum-based Solidity language, which is a Java-script extension. Solidity is a procedural language and not a functional language, and it therefore does not allow for the identification of unintended side-effects of a contract. A functional language uses mathematical functions, so the analysis of the outcomes can be done with an absolute certainty. A procedural language performs a series of sequential steps, and the analysis of a complex structure written in the procedural language can only be done with a limited certainty. Exploitation can occur as it is important to note that smart contracts are a general-purpose code that executes on every computer in the network. They are activated by transactions that occur. If smart contracts are written in a procedural language, actors with malicious intents can exploit possible vulnerabilities in the smart contract code, which are difficult to check a priori. Exploitation as such occurred during the DAO hack, when an attacker managed to move Ether 3.6 million to another organizational structure by exploiting a bug in the code.

Governance and architecture

A smart contract is in legal terms a formal intent. In a centralized system, a formal intent can be judged by an arbiter in case of a dispute. However, in a permissionless blockchain-based system, there is no superior arbiter and the human intent cannot be checked by computer coding.

Although it might not completely solve the problem of having the need for a superior arbiter, a permissioned private blockchain-system would be able to provide rights to the tax authority to check and potentially correct or reject certain transactions. A permissioned architecture is also needed, as user management is the key challenge in the system with the large number of registered addresses in the system: transacting

businesses, the 28 tax offices and banks of the buyers and sellers. The tax offices would act as the full nodes and the banks would act as external oracles which certify that a split of payment has been executed. The businesses would interact with the infrastructure as light clients (storing parts of the ledger yet not validating the transactions) or using a portal connecting to the tax office system. A rigorous user management system is potentially also a challenge, as it would need to be compliant with all Member States registries and integrated with the existing ID solutions. To become operational, this system would need to be eIDAS compliant (European Parliament & European Council, 2014). In addition, the network of computers storing the full ledger will potentially store confidential taxpayer information, so a permissioned architecture would be required. For security reasons and for practicality, businesses should store fragments of a ledger which is necessary for verification of the momentary state of an own VAT balance (for example using a light client set-up). To have a complete overview, tax offices should store at least all domestic transactions and international ones where local companies are involved as importers or exporters. This poses the requirements of having a highly secure blockchain infrastructure.

Many architectural types are currently being examined, but a private permissionless architecture would enable the highest throughput and would enable the supervisory role of tax authorities in a distributed system. The blockchain nodes that store the full ledger would, in that architecture, be under the control of the tax authorities of the various Member States. Web portals or APIs could be leveraged to register the transactions of the businesses. Each verified transaction would constitute as a new block added to the ledger structure. The architecture would need to enable a real-time encryption of data, as each Member State would need to have their own data host with data shared through encryption and exchange of access keys with other countries.

The permissioned, private blockchain architecture could have an appeal instance built in. The ledger could correct backwards taking advantage of the fact that transactions are always bilateral and separable (changes in transactions between A and B do not have an impact on A and C nor B and C). Any changes to the ledger would need to be authorized by the tax authorities and validated before becoming effective.

Another challenge that this use case presents is that the blockchain protocol allows for automatic validation of transactions on a technical level, but assessing the transactions that are VAT eligible requires a semantic validation as well. Semantic questions on each transaction could include questions on the legitimacy of the transactions and the goods or services that are part of it. Semantic validation would also perform checks related to the application of reduced or preferential VAT rates. Artificial intelligence could be leveraged as there are billions of transactions to be check annually. This makes the system largely depended on the development of other technologies as well.





The blockchain platform for registering transactions and supporting collection of VAT charges should leverage open source software in order to build trust, enable verification of the protocol and ease integration via third party solutions.

Key takeaways

- Using blockchain to fight VAT frauds could in theory save billions of euros of tax revenues in the EU. The value at stake provides sufficient incentive for governments to start small scale experimentation with this use case.
- A fully fledged system would combine registration of transactions on the blockchain leveraged by smart contract functionality with automatic split payments. This would require input-output VAT clearing to be done by the tax office and not by the firms submitting VAT declarations, as is the case at present.
- Blockchain-based VAT system can be restricted to recording new transactions. Registering invoices upon issuance would provide a close to real-time notification to the tax authorities, which could then run AI-based algorithms for detecting a risk of fraud by the buyer soon becoming a missing trader.

- A more advanced blockchain-based VAT system could be also integrated with automated split payments. In this case VAT reclaims would be done automatically and successively by the tax office to the firms as they settle transactions along the value chain. Split payments are supported by the escrow functionality in smart contracts.
- A permissioned, private blockchain architecture in which the tax authority also acts as a blockchain node operators would present the required legal oversight while enhancing scalability.
- At present, technology is immature for the size and scale of this use case to have an operational deployment in the near future. Current protocols would have severe difficulties in handling the required volume of transactions.
- The system would likely rely on smart contracts, yet there are a number of challenges regarding smart contracts in this use case, including legality (lack of authority) and completeness (non-functional languages, only procedural languages).
- Permissioned, private blockchain architecture allows for backwards corrections of transactions between two parties.
- The system will have to be bullet-proof and work seamlessly. There is a large impact on the commerce across the EU if anything goes wrong in the operation of the ledger.
- In order to provide the required (legal) oversight, the system would potentially be dependent on the development paths of other technologies like artificial intelligence.

Figure 19. Blockchain against VAT fraud

 Blockchain against VAT fraud					
1. General features					
Level of government involved	Public services provided/enabled	Cross-border aspects	Cross-sector aspects	Location value creation	Openness of software
EU	VAT eligible transaction registration	Yes	Yes	Location is static	Open source / closed source
 2. Functionalities			 3. Governance		
Institutions disintermediated	Functionalities provided		Roles included	Blockchain governance architecture	Consortium governance
None	3-way contract between buyer, seller and tax authority Direct tax (pre)payments on the transactions		Government; OS community; Businesses	Private permissioned blockchain architecture with tax authorities as nodes	Centralized
 4. Technical Architecture					
User Layer	Non-DLT Systems	API Layer	DLT Platform Layer	Infrastructure layer	
Web portals; transaction declaration applications	User management system; transaction database	Government-to-business APIs; G2G APIs	Light consensus protocol including semantic validation	Tax authorities as blockchain nodes	

Source: Own elaboration.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696, or
- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from EU Bookshop at: <https://publications.europa.eu/en/publications>. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.



EU Science Hub

ec.europa.eu/jrc



@EU_ScienceHub



EU Science Hub - Joint Research Centre



Joint Research Centre



EU Science Hub



Publications Office

doi:10.2760/942739

ISBN 978-92-76-00581-0