Alma Mater Studiorum – Università di Bologna
in cotutela con LAST-JD consortium:
Università degli studi di Torino
Universitat Autonoma de Barcelona
Mykolas Romeris University
Tilburg University

DOTTORATO DI RICERCA IN

Erasmus Mundus Joint International Doctoral Degree in
Law, Science and Technology

Ciclo XXXII - A.A. 2016/2017

Settore Concorsuale: 12/H3

Settore Scientifico Disciplinare: IUS/20

TOKENIZATION OF REAL ESTATE ON BLOCKCHAIN

Presentata da: Oleksii Konashevych

Coordinatore Dottorato

Prof.ssa Monica Palmirani

Supervisore

Prof.ssa Marta Poblet

Supervisore

Prof. Pompeu Casanovas

Esame finale anno 2020

Alma Mater Studiorum – Università di Bologna
in partnership with LAST-JD consortium:
Università degli studi di Torino
Universitat Autonoma de Barcelona
Mykolas Romeris University
Tilburg University

PhD Programme in

Erasmus Mundus Joint International Doctoral Degree in
Law, Science and Technology

Cycle XXXII - 2016/2017

Settore Concorsuale: 12/H3

Settore Scientifico Disciplinare: IUS/20

TOKENIZATION OF REAL ESTATE ON BLOCKCHAIN

Submitted by: Oleksii Konashevych

The PhD Programme Coordinator

Prof. Monica Palmirani

Supervisor

Prof. Marta Poblet

Co-supervisor

Prof. Pompeu Casanovas

Year 2020

THESIS BY PUBLICATION

CONTENT

I. Thesis introduction.

II. Paper 1. General Concept of Real Estate Tokenization on Blockchain.

III. Paper 2. Cross-Blockchain Protocol for Public Registries.

IV. Paper 3. Constraints and Benefits of the Blockchain Use for Real Estate and Property Rights.

V. Paper 4. Data Insertion in Blockchain For Legal Purposes. How to Sign Contracts Using Blockchain.

VI. Paper 5. Blockchain Anchoring of Public Registries: Options and Challenges.

VII. Thesis conclusions.

Abstract

This thesis presents research at the junction of law, governance, blockchain technology and real estate. The concept of real estate tokenization includes legal, technological, and organizational aspects. The research introduces a theory of a Title Token - a digital record of ownership on the blockchain. It is discussed the principle of technological neutrality, where the traditional land (property) registry is not necessarily abandoned in favor of blockchains, but instead, people gain the right to choose. The key output of this research is an architecture of the system presented as a cross-blockchain protocol designed to support free choice and transferability of assets across blockchains. Another important feature of the protocol is enforceability to address the constraint of the blockchain technology, i.e., the intolerance to retroactive transactions. To resolve disputes and other legal issues, the protocol provides a framework for smart laws and digital authorities. Among objects of interest were questions on the effectiveness of governance and bureaucracy, corruption, automation, fraud on the market, and the role of the government and other intermediaries in the protection of property rights and interests. The multilevel analysis undertaken in this thesis is a preliminary step towards making any policymaking suggestion. It also aims at delivering a solid ground for further research and experimentation. Such analysis aims to address the thorny issue of effectively applying emergent technologies to law and governance. The outcome is a set of reflections and conclusions for policymakers and researchers regarding the capabilities and limits of blockchain technology, wrapped into a consistent concept of improving the current system.

ACKNOWLEDGEMENTS

I express my sincere gratitude to my supervisors Prof. Marta Poblet from RMIT University and Prof. Pompeu Casanovas from La Trobe University. These four years of research your support and wisdom guided me through all challenges in academia. It was a great privilege to have your advice.

I am grateful to Prof. Monica Palmirani at the University of Bologna, who is a coordinator of the LAST-JD program and made possible this international doctoral consortium. Thanks to Dr Dina Ferrari from the University of Bologna who helped a lot in administrative issues.

I am also thankful to Prof. Ugo Pagallo and Prof. Massimo Durante from the University of Turin, Prof. Antoni Roig from the Autonomous University of Barcelona and Prof. Ronald Leenes from the University of Tilburg, who made my research productive during six months in their universities.

Special thanks to Prof. Jason Potts and Dr Cris Berg, co-directors at RMIT Blockchain Innovation Hub who kindly accepted me in their wonderful team and supported me throughout the last two years in Melbourne.

And of course, great thanks to my wife Halyna, who gave me her love and shared with me all the stresses of moving all around the world during this four-year journey, and my parents who were always a pillar of support. Thank you all so much!

THESIS INTRODUCTION

Tokenization of Real Estate on Blockchain

Oleksii Konashevych
Erasmus Mundus Joint International Doctoral Fellow in Law, Science and Technology

Supervisors:
Associate Professor Marta Poblet, RMIT University
Research Professor Pompeu Casanovas, Autonomous University of Barcelona and La Trobe University

2020

Contents

1. Background 3
2. Research questions and methodology 3
2.1. Research questions and context 3
2.2. Methodology and Theoretical Framework 4
2.3. Research limits 7
3. What is blockchain and what does (De)centralization mean 7
3.1. Blockchain origin 8
3.2. How do blockchain, permissioned and private DTLs work? 8
3.3. What is (De)Centralization and why does it matter? 10
3.4. Definition 12
4. Why blockchain is impossible to use in public service in its present form 13
4.1. Hardforks 13
4.2. Immutability 13
4.3. Anonymity (pseudonymity) 13
4.4. Data integrity, off-chain data and issues of personal data 14
4.5. Scalability 14
4.6. Price volatility 14
4.7. What is opposed to blockchains and why it is still a good idea to use them 14
5. Thesis publications 15
5.1. General Concept of Real Estate Tokenization on Blockchain 15
5.2. Cross-Blockchain Protocol for Public Registries 15
5.3. Constraints and Benefits of the Blockchain Use for Real Estate and Property Rights 16
5.4. Data Insertion in Blockchain For Legal Purposes. How to Sign Contracts Using Blockchain 16
5.5. Blockchain Anchoring of Public Registries: Options and Challenges 17
6. Literature review 17
6.1. Technical documentation and academic research in blockchain and cryptography 17
6.2. Academic papers regarding the use of blockchain for real estate and industry reports 19
6.3. Academic papers regarding the use of blockchain and public sector (public services) 20
6.4. Public policy papers and government reports on the use of blockchain 22
References 23

1. Background

This thesis presents research at the junction of law, governance, blockchain technology and real estate. For the purposes of this thesis, I define blockchain as an irrevocable public repository that keeps records of ownership and manages property rights through peer-to-peer transactions with fewer intermediaries and minimum involvement of public servants.

The purpose of the thesis is to improve public services and make real estate relationships more efficient. In parallel to the research on blockchain technology, it includes the exploration of issues in land registration and the role of governments in maintaining public registries and other protective functions of the state towards property rights.

The outcome of this research is presented as a concept for the tokenization of real estate on blockchain, including aspects of public policy and regulation, technology architecture and implementation aspects. The concept includes a proposal to redesign the existing paradigm of centralized databases in favor of distributed ledgers with the objective of enhancing real estate innovations and investments. This research includes conclusions on the applicability of the existing ledger technologies, limits and constraints of blockchain compared to the existing centralized technologies and permissioned distributed ledger technologies. Conclusions are drawn from analysis on fallacies around the technology, questionable concepts, results in pilots and startups.

The thesis also presents an architecture of the system for a property registry: a cross-blockchain protocol. It supports the idea of a free choice of citizens of the technology, i.e., technological neutrality, which implies the right to choose a traditional land registry or blockchain, and a blockchain agnostic principle aligned with the idea of neutrality. To make blockchain land (property) registry sustainable, the protocol accommodates the concept of smart laws and digital authorities, which are also novel concepts of this research.

Ultimately, this research introduces a theory of a title token that can contribute to developing the technology of shared ledgers. A title token is a record of ownership in the ledger supported by a technology of smart laws, which makes unnecessary keeping the record in any other traditional electronic or paper-based cadastre (hereinafter, cadastre, land registry, real estate registry, etc., are used in the same meaning).

The concept of tokenization raises questions about the role of the government. First, how to introduce a new concept. Secondly, what needs to be done with regard to technology, standards, security, regulations and land authorities. As a part of this discussion, the thesis addresses the issues of (i) digital identity and electronic signature to make transactions; and (ii) smart contracts to make them legally binding and compliant. Two of the papers (Paper 1 and Paper 2) draw a vision on how to make digital identities and e-signature native on blockchain, rather than trying to integrate it with off-chain traditional Public Key Infrastructure models. Inevitably, this vision triggers the question of personal data and privacy, which is also further discussed. The concept is designed to accommodate models and methods of Decentralized Identities (DIDs) and Self-Sovereign Identity. Further objects of interest were questions on the effectiveness of governance and bureaucracy, corruption, automation, fraud on the market, and the role of the government and other intermediaries in the protection of property rights and interests.

2. Research questions and methodology

2.1. Research questions and context

The cornerstone hypothesis of this thesis is whether the blockchain is an efficient alternative to present systems for real estate management. The existing model of estate conveyance and transactions involving property rights heavily rely on multiple intermediaries: land authorities that keep registries, authorize and register transactions, public notaries, brokers, and banks, among others. Some intermediaries and their functions can become obsolete with the introduction of blockchain and smart contracts.

The core question of the thesis is how to improve legal relationships in the real estate domain. Real state is a highly regulated field, and the government's role is crucial both in everyday tasks and when introducing innovations.

In most countries, public policy is based on registration and acknowledgment of transactions in real estate in one or another manner. This involves land authority and other government bodies, land surveyors,

evaluators, notaries and brokerage. Broadly, all these are third parties and constitute an "intermediary" as a general notion. It also involves a land registry, also known as cadastre, real estate registry, registry of immovable rights and so on, and some other auxiliary registries, which may exist separately in various countries: notary registry, mortgage, etc. Taking into account well-known problems with the effectiveness of government agencies and issues with corruption, high transaction costs, constraints in the free flow of capital in the world, my hypothesis explores the advantages of blockchain and the need to upgrade the existing system of property relations. To answer the question of how blockchain can improve real state, it is important to take into account issues such as bureaucracy bottlenecks, high transaction costs, and risks related to having multiple intermediaries.

Governments keep their land registries and establish rules under which transactions are considered legal. Governments delegate public servants the authority to record transactions in the registry when landlords and interested parties apply. This process establishes a public order in the society by answering the question of who owns what. Undoubtedly, the process has great societal value since it prevents or mitigates legal conflicts.

The figure of the intermediary is a reasonable solution to the imperfect nature of human relationships, but it also introduces several issues related to trust, efficiency and accountability. Therefore, the thesis explores the question of (de)centralization and explicitly postulates that everything capable of becoming decentralized should be decentralized, and everything else (if not decentralized) should be made accountable and, generally, more effective. Therefore, it becomes essential to distill which functions of the middleman can be automated and replaced by technology, and what interposal is inevitable. The starting point is whether "registration" equals to "centralized land registry" and to a "public servant who registers each transaction." Can a registration be called so, if all purposes assigned to the act of registration are achieved, even without a centralized database and a public registrar? As stated above, my core hypothesis is that the blockchain has the potential to be the decentralized database that stores all transactions without the need of a third party and without the risk of loss and or counterfeit.

Registration is not just about keeping records securely. A registration may enclose various purposes other than just the storage. For example, in some countries, registration is the result of government or community approval of the transaction[1]. Besides, there is another mandatory procedure in many countries - a deed acknowledgment, i.e., a process that requires legal expertise of the transaction. The acknowledgment is typically performed by a notary[2]. Therefore, the question is, why we need registration, acknowledgment of a deed, and the need to atomize this process, and what path towards the use of blockchain would look like? What features of blockchain technology makes it a unique solution for the issue? What are its limitations? Exploring these questions requires to start from a more basic set of questions: what is the blockchain? What is distributed ledger technology? What is "permissioned" or "private" DLT?

Finally, the "problem" of the immutability of the blockchain is also crucial to this research. Blockchain is an append-only database; hence retroactivity or erasure is impossible. While this is an advantage, for it creates certainty in the archive records, it also makes the technology intolerant to mistakes. As the thesis shows, immutability solves important issues, but it will also trigger the need to resolve legal disputes and enforce new forms of distributed justice.

2.2. Methodology and Theoretical Framework

Any multidisciplinary field requires a combination of different research methods. The results are presented as a concept of tokenization of real estate on blockchain and consist of five published peer-reviewed papers. The concept of tokenization includes legal aspects of digitization of property rights and transactions, a discussion on public policy, and a system architecture, i.e., a cross-blockchain protocol for public registries and a framework of smart laws.

My research has applied two basic methods: analysis of policy studies and design science research. The analysis work included an in-depth examination of regulatory frameworks, policy papers, technical

[1] As per [67], municipal or regional pre-emption rights exist all over Europe. Beyond that, there are frequent limitations on special kinds of transactions: tender for public land (Poland), restrictions for deeds with farming land, forests (Germany and Sweden), or land and buildings with cultural, historical interest (Italy) or high ecological value (Spain).
[2] Acknowledgment by a notary is mandatory for real estate transactions in most civil law countries (Italy, France, The Netherlands, Ukraine, Russia, etc.). Also, it is observed in other forms in Common Law countries (the thesis presents the analysis of Vermont state in the U.S.).

documentation, industry cases and a systematic literature review. Each of the papers included in this thesis describes the details of the chosen methodology therein.

The theoretical framework contains various concepts that have been developed in previous literature in the area of e-governance. In "The Evolution and Continuing Challenges of E-Governance" [1], the author defines this field of knowledge as "the use of information and communication technologies (ICTs) to support public services, government administration, democratic processes, and relationships among citizens, civil society, the private sector, and the state."

The methodology that I apply in this research draws from the one used in both "Conceptual Framework for Context-Based E-Government Interoperability Development" [2] and "The understanding of ICTs in public sector and its impact on governance" [3]. In the first paper [2], the author provides an analysis and generalization method to define the concept of e-government interoperability. In his analysis of ICT capabilities and methods, the author recommends that policymakers, public managers and related private sector organizations should assess the technical and evolutionary fitness of dynamic organizational capabilities for interoperability before starting any cross-organizational e-government initiative. This process should be done through the analysis of related processes, asset position and path-dependency factors of all participating parties. The author also suggests incorporating these principles of context analysis in the research of e-government.

In the second paper, the author [3] raises the question of whether managers in the government are fully aware and understand the many functions and roles that ICTs have, and how they should be governed. The author researches the phenomenon of mismatch of the functions implicit in the objectives that are stated for e-government and the way ICTs are governed. Jansen argues that this discrepancy can be attributed to an inadequate understanding of ICTs and its many functions. Jansen's conclusions are a methodological basis and a leitmotiv for this thesis.

The multilevel analysis undertaken in this thesis is a preliminary step towards making any policymaking suggestion. It also aims at delivering a solid ground for further research and experimentation. Such analysis aims to address the thorny issue of effectively applying emergent technologies to law and governance. The outcome is a set of reflections and conclusions for policymakers and researchers with regard to the capabilities and limits of blockchain technology, wrapped into a consistent concept of how to improve the current system.

Design science research (DSR) frames the part of the thesis that presents the system architecture concept [4]. From this perspective, I present an "artifact" that is defined as a set of "constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), and instantiations (implemented and prototype systems)" using the terminology of DSR introduced by Hevner et al. [4]. This research deals mostly with *models* and *methods*. In particular, the cross-blockchain database is a model, and cross-blockchain protocol can be considered as a set of methods providing suggestions on how this model can be designed. The research grants a broad discussion and evaluation of the applicability of the proposed invention and constructs various models for its use in the governance domain. The research is also compliant with the 7-step research guidelines provided by Hevner et al. [4], and corresponds with Design Science Research Publication Schema [5] by Gregor and Hevner:

(1) The *Introduction Section* of Paper 2 discusses the purpose and scope of the artifact to be developed (what the system is for). Namely, the design concept of a cross-blockchain protocol to enable the creation of end-to-end public databases across multiple blockchains. The paper also introduces practical issues on the use of blockchain by governments – these are research questions, which are to be addressed by this DSR. How to eliminate the use of centralized (permissioned and private) DLTs, learn how to deal with immutability (enforceability of smart contracts), address anonymity and privacy issues, price volatility and scalability of a blockchain.

(2) The *Literature Review* is not formalized in Paper 2 as a separate section, but this paper provides extended references throughout the text to the relevant academic research in ICT and blockchain to support the integral elements of the protocol and proposed methods. A literature review for this thesis is summarized in Section 6 below.

(3) Methods Section. The primary method for this DSR is *exaptation*, i.e., adoption of solutions from other fields. The research is looking into existing technologies which are applied here as elements of the protocol: Name-Value Storage, Berkley DB, RAID protocol, among others.

(4) Artifact Description Section. This section includes a design concept of a cross-blockchain protocol for creating of end-to-end public databases across a bundle of blockchains.

(5) The *Evaluation Sections* are based on *analytical* and *descriptive* methods (according to Hevner et al., 2004), which includes a technical evaluation of the architecture and a general evaluation of the technology applicability with legal and political aspects. The evaluation consists of:

- **Architecture Analysis:** Paper 2 studies the ability of the cross-blockchain protocol to work with different DLTs to ensure consistency of a key-value database built across a bundle of ledgers, and eventually, the use of a standard solution as an end-to-end database.
- **Optimization**: Optimization of the network by excluding fault networks and adding new ledgers on the run; issues with relations of a local network database and a cross-blockchain database; issues of network and astronomical time discrepancy and optimization of confirmation pending to prevent forking. The paper presents design concepts to prevent name squatting.
- **Static and Dynamic Analysis**: The research examines the artifact in use for static and dynamic qualities (performance, vulnerabilities, time synchronization, transferability of assets, bundle management, blocks confirmation, among others.). Paper 2 evaluates methods of adding and dropping off blockchains on the run to avoid hardforks of cross-blockchain database and evaluates fault tolerance in case of a compromise of a blockchain in the bundle; one of the RAID methods is evaluated as a solution. Assets squatting issues are evaluated in comparison of two main protocols which are Proof-of-Work and Proof-of-Stake, and experience of addressing these issues in two networks Namecoin and Emercoin, which provides for decentralized TL DNS (Top-Level Domain Name Service).
- **Informed Argument**: The research is based on information from the knowledge base (e.g., relevant research) to build a convincing argument for the artifact's utility. The paper refers to the accumulated experience in the use of conventional technologies: Emercoin's Name-Value Storage, RAID protocols and Berkley DB may become an integral part of the cross-blockchain database architecture.
- **Scenarios**: The evaluation of the applicability of the invention is analyzed through various use cases and scenarios: the use of cross-blockchain databases to manage digital IDs and more general as a new approach for Public Key Infrastructure; the research could not omit methods for personal data protection and anonymity. Another broad discussion reflects the issues of managing the cross-blockchain protocol. The method of protocol "patching" is presented as an act of justice to resolve disputes over assets and provide for smart contract enforceability. The paper discusses the framework for "smart laws," proposing to look at jurisdictions as a set of filters in the protocol ("code is law" [6]), which help to distinguish legal and illegal transactions, rather than fighting against ledgers' immutability.
  Similarly, this method addresses hardforks. The evaluation presents arguments for the use of bundles of blockchain instead of using a mono ledger. This approach does not address the bandwidth of any blockchain but instead proposes a market-driven solution of free competition of blockchains under the umbrella of the cross-blockchain protocol. This may reduce the negative consequences of price volatility on business by letting end-user flexibly transfer their assets from blockchain to blockchain to fit their needs in price and quality.

The reason for not using experimental and testing methods for evaluation in this thesis is two-fold. First, the thesis does not establish quantitative objectives (for example, it does not deal with improving latency performance, bandwidth or size transaction optimization, among other quantitative indicators). Second, the creation of an artifact presented in Paper 2, i.e., a key-value database across a bundle of public repositories, is feasible to argue its implementation possibility.

The theoretical value of this research consists of presenting viable models and scenarios for the use of decentralized blockchains, rather than permissioned DLTs, in the public sector. The absence of any real solution in this space makes the application of the blockchain, rather uncertain for property registries, due to known legal issues. Therefore, this research focuses on designing the concept of a new protocol and, more generally, a concept for managing public registries across multiple blockchains. Both hypothetical concepts are crucial in opening a new discussion in the field of real state, and I expect this thesis to be a significant and path-breaking contribution to that field. I am fully aware that the development of the proposed systems may require substantial resources, but I also expect that broader independent evaluation

and contribution from researchers in this space may create more knowledge and debate about how to develop prototypes in the future. This thesis aims at significantly contributing to this emerging debate.

2.3. Research limits

The goal of the thesis is to develop a larger picture for improving relationships in real estate by applying blockchain technologies. Countries that lack an effective land system and property protection, suffer from high levels of corruption and bureaucratic legacies may benefit from this model. My proposal does not intend to provide any ready-to-use solution for any given country or resolve those issues at once and forever. Corruption issues and bureaucracy legacies typically stem from political issues that are out of the scope of this research. Rather than scrutinizing any particular economic problem in real estate, the thesis refers to the existing knowledge on this subject [7]. The typical issues include:

- risks of "single point of failure" in central server systems, and the need to maintain a cumbersome and expensive infrastructure to manage risks, which lead bureaucracy and high transaction costs;
- restricted access to vital information in registries that constraint entrepreneurship and causes problems of fraud;
- corruption and abuse of power, this limits economic growth because investors do not opt into jurisdictions where private property is not protected.

Governments generally benefit from the free flow of investments in their economies by introducing innovations. Quantitative evaluation of the proposed concept requires piloting at a state level. Therefore, this work can be considered as providing a theoretical basis rather than a practical implementation and evaluation. Likewise, the concept of smart laws outlines existing possibilities to develop a system that can be governed in different ways: from digital dictatorship to direct e-democracy with online voting on blockchain, where plebiscite results do not even require any intermediate public body (e.g., an election commission) since the "governing code" executes itself right after the voting.

The architecture proposed in this thesis accommodates a wide range of political systems and models of governance. I discuss the boundaries of the range of models that I identify based on the current state of the art in science and technology. For example, I argue that that digitized property rights require digital identity and electronic signatures with a legally binding effect. This triggers issues of privacy and personal data and cybersecurity. Future property management systems must be developed within the principles of privacy-by-design [8]. The thesis does not propose any particular recipe, but it can accommodate best practices in this area and defines general requirements that property management systems must be compliant with.

While the thesis does not cover the field of regulatory compliance systems, my research proposes to address the problem of enforceability of smart contracts. Contracts have an imperfect nature because it is materially impossible to predict everything in legal relationships and set all possible rules for the parties in the agreement. To resolve disputes, courts apply relevant laws even if the contract does not contain references to these legislative norms. Digitization of a transaction refers to encoding the relationships into machine algorithms. From a computer programming point of view, it is relatively easy to develop a contract in algorithms, but the complete digitization of laws seems to be unfeasible at this point in time. Therefore, the digital transaction is a piece of code in a closed system that does not refer to any high-level rules or has very limited interaction with them.

The closed system design problem is one of the major difficulties in this research because transactions in the distributed ledger are immutable. Users cannot change the transaction if something goes wrong in their legal relationships. To address this problem, I propose a new operational layer above - an overlaid database that does not challenge immutability but introduces a level of smart laws and digital authorities (to enforce law) and a level of "model smart contracts," which may be optionally used to improve a contractual process. The concept does not explore the compliance methods, but the proposed system does not limit the introduction of the existing knowledge in this field.

3. What is blockchain and what does (De)centralization mean

There is an ever-growing body literature providing definitions of "blockchain" and describing its underpinning technologies. The literature includes a great variety of academic papers, government reports and industry materials (reports, white papers, blog series, guidelines, etc.). Therefore, there are several

varieties of definitions and discussions of what should be called blockchain and what we should understand and include in the "Distributed Ledger Technology" category, which usually refers to "permissioned," "private," "federated," and "enterprise" ledgers.

This thesis considers the blockchain as a decentralized public technology of a shared ledger. The immutability of the ledger is, from this point of view, one of its key advantages. DLTs may establish different portions of centralization and censorship and have much in common with the blockchain, but they are different from Nakamoto's innovation. This research shows that there is no convincing evidence that permissioned technologies are somehow better in terms of decentralization compared with traditional databases, as they can provide immutability at the discretion of a governing body. In contrast, the blockchain is a self-organized and self-governed infrastructure, an ecosystem operating without a trusted party or a defined group of trusted parties. My further research develops this vein for the real state domain.

3.1. Blockchain origin

Satoshi Nakamoto invented blockchain [9] with a set of distinguishing features. The paper "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008) introduces "a purely peer-to-peer version of electronic cash" for online payments to be sent directly from one party to another without going through a financial institution." The blockchain ensures that transactions are done in a decentralized, public, immutable, and censorship-resistant manner. Even though distributed systems existed for decades, this invention was the first to find an optimal combination to become a large-scale global network, giving birth to a constellation of distributed ledger technologies (DLT).

The system can be either decentralized or centralized. These are mutually exclusive concepts that beg the question of whether "permissioned" distributed ledger technology constitutes a blockchain or not. Permissioned systems require someone to create trust and certainty in the state of the ledger. This "someone" can be one single actor or a group, but it is always a limited number of actors. In Nakamoto's blockchain, the ledger has no master. In my perspective, the phrase "permissioned blockchain" should be considered an oxymoron.

Chain of blocks vs. blockchain—The original Nakamoto's paper [9] does not contain the exact word "blockchain" but the "chain of blocks" instead and similar phrases: "blocks are chained," "blocks in the chain," etc. Nevertheless, there is no room for an argument here because "chain of blocks" and "block chain" are noun modifiers that constitute a semantic equivalent in English. Further research of Nakamoto's writings and communications with developers shows that they used both phrases "block chain" and "blockchain" on the forum and emails understanding the same thing. Examples can be found on the website "Satoshi Nakamoto Institute," which collected available Nakamoto's online appearances [10].

The subsequent transformation of "chain of blocks" and "block chain" to monolith word "blockchain" makes practical sense because the first two are not necessarily unique phrases for search systems (for instance, for Google), as the "blockchain" is. Being a searchable keyword, "blockchain" creates a better user experience. Therefore, "blockchain" is just a result of the evolution of the notion.

Neither in the 2008 paper nor emails and posts did Satoshi Nakamoto come up with a short and straightforward definition of the blockchain. One may even argue that Nakamoto's invention is "Bitcoin," since they never explicitly defined the blockchain as a technology. This argument could hardly be accepted because the proposed technology can be replicated as a standalone cryptocurrency system. Bitcoin is a proper name, a manifestation of the blockchain technology embodied in the concrete system.

3.2. How do blockchain, permissioned and private DTLs work?

To understand why terminology accuracy is relevant, let us first outline how these technologies work. Nakamoto's invention is based on public-key cryptography, Merkle trees, chain of hashes and Back's "proof-of-work."

The idea of chaining data for time-stamping by including a hash sum of the current set of data to the next was first proposed by Stuart Haber and W. Scott Stornetta in 1991 [11]. The authors proposed computationally practical procedures for digital timestamping of electronic documents so that it is not feasible for a user to back-date or to forward-date his document, even with the collusion of a timestamping

service. Their procedures maintain complete privacy of the documents themselves and require no record-keeping by the time-stamping service.

First, Nakamoto's innovation lies in chaining blocks of transaction records that are interconnected through a Merkle tree and designed in such a way that transactions cannot spend already spent coins ("double speeding" problem). Some other distributed ledger technologies developed afterward inherit this principle. The second crucial element of this system is how blocks are being created and validated. Nakamoto's paper describes the "Proof-of-Work" method, regarding its originator Adam Back [12], which ensures the decentralized mechanism of blocks mining. The fundamental principle is that nodes freely compete with each other doing mathematical calculations. The protocol ensures the unpredictability of who gains the right to introduce a new block in the network.

The node who finds the solution to the mathematical problem presents a new block to the network. All the other nodes use the same protocol. Therefore, nodes validate the solution with the initial task, and if it matches, they add the block to their ledgers. No one is capable of producing a block without doing the work, even though the work itself is just a check of all possible solutions for the challenge with some linear probability to find the key during a specified period. The randomness of creators ensures that no corruption is possible. No authorities decide who can participate in the competition, no one authorizes blocks, neither create computational tasks. All participants in the network are equal and independent. All these rules are defined in the code (protocol) of the system. This is a part of a social agreement, no one is forced to accept blocks, but when the node downloads the wallet, they accept this protocol and accept blocks when they are valid. This is a peer-to-peer network where honest and malicious nodes compete in the mathematically proven fair computational challenge. And the credibility of this system is based on the assumption that the majority of participants are honest. The only thing that stands between nodes is the blockchain protocol, i.e., the program that embodied all these rules in the code.

The common feature of DLT, starting from Nakamoto's blockchain is that transactions are performed by owners of cryptocurrency through a native mechanism of public key cryptography. Traditional databases require an administrator and an access management system. For security reasons, they usually do not allow users performing transactions themselves. There are no countries in the world that allow landlords to perform transactions directly in the land registry; it is performed by registrars. With the blockchain and any other DLT, users need a private key to sign a transaction. The user's relevant public key becomes the address where assets (records) are stored. The difference in permissioned DLT is that they can establish censorship: to filter users and transactions under some conditions. To ensure compliance in some DLT protocols exist, so-called "validators" accept transactions and digitally sign them to certify the compliance.

Thus, in permissioned systems not all users are equal (e.g., someone in the system may create blocks, and someone may not). There are different protocols designed since 2008 that can support centralized mining (minting, staking, forging, etc.), for example, Proof-of-Stake (PoS) [13]. PoS does not require PoW calculations but defines the right to create a block based on a lottery, where tickets are coins. The user who owns more coins has more chances of creating new blocks. Having a whole or a substantial stake, this protocol makes it possible to hold the system in one hand or share the control within a closed group of stakeholders. Some other protocols support centralized governance, for example, Delegated PoS [14] and Proof-of-Authority [15]. In PoA, the right to create blocks is gained by those whose public key is authorized; they are called "validators." This system is similar to Public Key Infrastructure, which is based on a trusted third party that identifies and validates owners of public keys. If a key is revoked, it loses authorization.

Centralization not only allows restriction of the right to create blocks but also enables retroactivity. The PoS authority may target any block in the past and begin the creation of blocks from this moment. In PoA, the master-node may revoke access to all but one validator who will rewrite the ledger. After the targeted block, the original chain will be dropped when the new version of the chain will overtake the dropped one. Other nodes (wallets) on the network will accept a new version as this rule is designed by the protocol; only the longest chain is valid. Thus, one of the most fundamental features of the technology – to be immutable and irrevocable – disappears with the centralization.

"Private" means that this group is not open for the outer circle, which is not necessarily the case in other permissioned systems. Open permissioned systems may potentially welcome other block creators, and may even create some formal rules for newcomers, but still will be centralized.

Blockchain is resistant to censorship. The purpose of the technology is to ensure that any transactions and scripts defined in the protocol can be performed without any authorization. Users may also insert some arbitrary information in the allowed amount of data, for example, up to 100 kB in Bitcoin [16].

In permissioned systems, transaction validation will be under someone's control. Moreover, the authorities may filter the transactions or validator nodes at their discretion.

To become "permissioned" and/or "private," the system must be pre-designed with these properties. However, public systems may fall into someone's control because decentralization in blockchains is not static. This is a *dynamic process* of competition of nodes which independently or collectively in a pool try to create new blocks and gain the right to write down a defined amount of cryptocurrency in these blocks as their reward. Therefore, "permissioned" and "private" are the worst evolution scenarios towards the up and running blockchain system.

3.3. What is (De)Centralization and why does it matter?

Various disciplines propose different definitions and explanations of decentralization. Surveys such as the ones conducted by Schneider [17] have shown that there is no unique definition of decentralization, and usually, decentralization is context-specific. Benkler [18] wrote that decentralization occurs when coordination can happen without hierarchy—when "many agents cohere and are effective, even though they do not rely on reducing the number of people who counts to direct effective action."

Interestingly, Nakamoto did not use the word "decentralization" in their paper. Instead, the reader finds a "trusted third party" and "a trusted central authority." As a matter of fact, in cryptography, "a trusted third party" is more preferred to describe the presence or absence of a third party between users. For instance, "centralized" is never used in NIST's Digital Signature Standard [19], where instead "Trusted third party" (TTP) is defined (Section 2.1) as "an entity other than the owner and verifier that is trusted by the owner or the verifier or both. Sometimes shortened to "trusted party."

Vitalik Buterin, Ethereum's founder, has proposed three levels of understanding (de)centralization [20]:

"Architectural (de)centralization — how many physical computers is a system made up of? How many of those computers can it tolerate breaking down at any single time?

Political (de)centralization — how many individuals or organizations ultimately control the computers that the system is made up of?

Logical (de)centralization— does the interface and data structures that the system presents and maintains, look more like a single monolithic object, or an amorphous swarm? One simple heuristic is: if you cut the system into half, including both providers and users, will both halves continue to fully operate as independent units?"

The issue of political and architectural (de)centralization can be illustrated with the following example. There is a peer-to-peer community that votes to make their collective decisions using an electronic system. If they have a central-server architecture, their organizational (political) structure is still decentralized, non-hierarchical. Yet, their electronic system is controlled by someone, which means that their "decentralization" relies on the will and honesty of the central authority. Hence, decentralization is *illusive*. See Fig. 1.

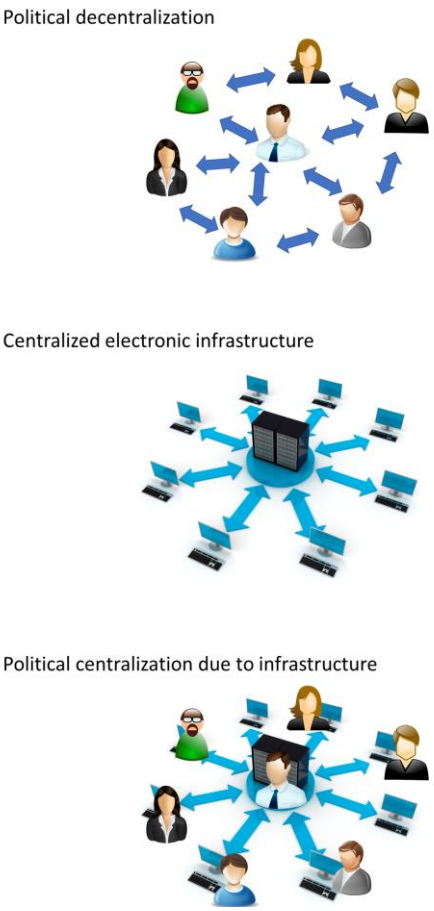


Fig 1. Influence of a centralized infrastructure on a political system.

Central authorities are a single point of failure surrounded by risks of violation of rules, abuse of authority, and usurpation of power. Inevitably, from time to time, centralization generates conflicts of a different scale.

Misrepresentation of truth about specifics of "permissioned blockchains" may lead to false expectations. Politicians may announce state-level projects, claiming their interest in the use of blockchain, but instead, they may be thinking of permissioned and private DLTs, that is, centralized solutions. This may lead to disappointment, but worse to no progress in governance and democracy.

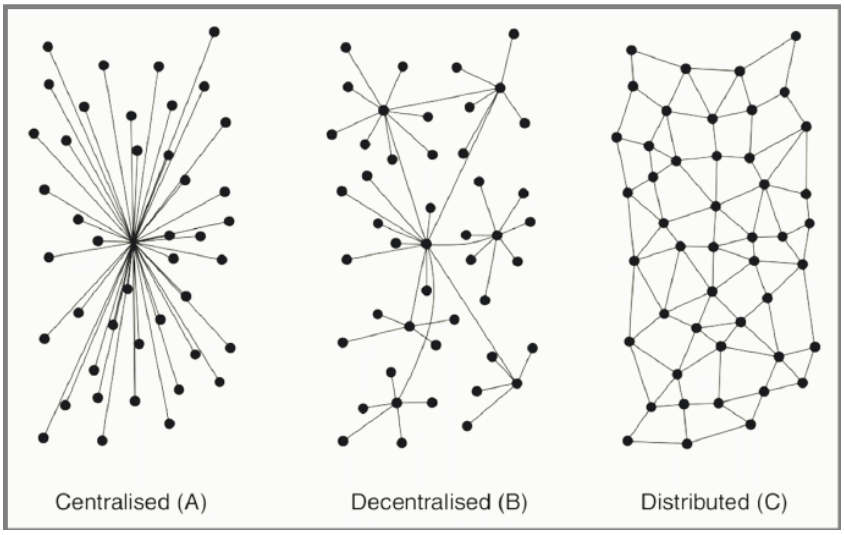


Fig. 2. Baran's network topology: Centralized, Decentralized and Distributed Networks

Decentralized vs. Distributed—Paul Baran proposed in his paper [21] a vision of decentralized and distributed systems during the Cold War. The research aimed to address the issue of resistance of the network in the event of an attack and the ability to ensure communication between nodes.

The famous Baran's figure (See Fig. 2) presents a centralized radial system and two alternative schemes:

- "Decentralized" still has a star topology but peripherals, at the same time, play a role of data exchange point for peripherals nodes of a group. In case of an attack on the central server, the group loses communication with other groups, but still maintains its group interaction.
- According to the distributed scheme, there are no central servers, and each has a protocol of interaction, which helps to find a path through other nodes to any nodes of the network.

"For example, type (b) in Fig. 2 shows the hierarchical structure of a set of stars connected in the form of a larger star with an additional link forming a loop. Such a network is sometimes called a "decentralized" network because complete reliance upon a single point is not always required."

It should be noted that Baran was addressing the issue of communication of nodes in a distributed network topology (in case of an attack during the Cold War), which is not the same as the task of a decision-making ("political" level as per Buterin). The communication can be distributed, but the protocol of consensus (decision making) centralized, i.e., decentralized architecture but centralized organization. The task of keeping the registry is the level of political decentralization. So, does "distributed" mean "non-hierarchical" and is "decentralized" a hierarchical? According to Baran, the answers is yes.

Nevertheless, this discussion can be considered as a historical retrospective. According to some conclusions [22], Baran's idea was not implemented in his initial concept. Therefore, it is reasonable to use a binary state approach where "centralized" is hierarchical, and "decentralized" is non-hierarchical. "Distributed" is a subset of decentralized in the meaning of the topology where the geographical position of nodes is distanced.

Altcoins and Modifications—There is no doubt that Nakamoto invented blockchain, but can we extend this notion to other, not bitcoin-like technologies? How do we define what is legitimately referred to as "blockchain"? Recapping the previous sections, we can distinguish two principal elements that matter in the comparison of distributed ledger platforms. The first is the "chain of blocks," where each next block includes the hash sum of the previous one (blocks contain transactions, and there are also many details, of course here, but are not crucial for this level of abstraction). And the second is the consensus mechanism - how these blocks are created. In Nakamoto's scenario, it is Proof-of-Work. It is reasonable to abstract away from PoW because it is just a method of achieving decentralization. The main here what it does, but not how. This method is meant to provide a decentralized consensus. As long as any other method can do it without involving a *certain* trusted third party to conduct the creation of blocks, it can be considered as blockchain.

3.4. Definition

Blockchain has become a popular word in media, and it is not always used in the original Nakamoto's meaning. It is hard to say who was the first to generalize "blockchain" to all variations of shared ledgers, and which arguments supported this generalization. But the use of "permissioned blockchain" by scholars and government agencies creates dangerous precedents, which open possibilities of misleading the society in introducing public projects by calling them "blockchain" but without any decentralization effect (transparency, accountability, etc.). However, some public institutions articulate a more balanced vision. For example, the European Union Agency for Network and Information Security (ENISA) uses "permissioned ledger" –instead of "permissioned blockchain"— in one of their reports [23].

Blockchain is an emerging technology. It is non-proprietary, and its inventor remains unknown. No one legally uses their intellectual rights, and therefore, there is no one to protect the title of technology and the integrity of the initial concept. Openness is good for this technology, and it probably became the key point of its success. But openness creates a confusion in terminology, opinions and approaches.

As a result of following this discussion over the last few years, this thesis proposes to define the blockchain as a distributed ledger technology. In a blockchain, a block contains records of transactions and the hash sum of the previous block. In this way, blocks are chained to avoid changes in transaction or block order. Transactions reflect transfers of units of account, which are also known as cryptocurrency. The

ownership of the cryptocurrency is based on public-key cryptography, where a user's private key is used to authorize transactions and public key to generate the address where cryptocurrency is attached. To work together in one network, nodes use the same protocol initially designed as per Satoshi Nakamoto's concept. Blocks are created based on a free public decentralized competition of network nodes. The protocol ensures the fortuity in creation of blocks. The node that is lucky to find a new block presents this block, including the reward record, i.e., the amount of cryptocurrency that the node has the right to assign to any address as per the protocol. If the new block complies with the protocol, other nodes will accept it, adding the new block to their versions of the chain and share on the network.

4. Why blockchain is impossible to use in public service in its present form

This research started interrogating whether the blockchain could ensure the decentralization of the infrastructure for public services. The next step was to explore the constraints of the technology; therefore, what was required to address obstacles and achieve such a goal. The major conclusion in this section is that due to hardforks, the immutability of the ledger, pseudonymity of transactions, exposure of personal data and scalability of the technology and price volatility, blockchain is unlikely to be of use for electronic governance. This section outlines these impediments and the conceptualization presented in this thesis.

4.1. Hardforks

The hardfork is the major concern for systems with open competition since there are no authorities that impose and enforce one exclusive status quo. The system can split into two or more branches or so-called "forks," after which each branch becomes independent but has a spare history of transactions till the moment of fork. As a result of the split, tokens are duplicated. For example, if the system is used to manage rights on movable or immovable property (often mentioned as "asset-backed tokens"), as a result of a hardfork, the user will still have one plot of land but two title records in parallel systems. These records can be managed independently (for example, in one system, the user sells the plot, but in the other, the user still owns it), thereby creating legal collisions.

4.2. Immutability

The immutable feature of the ledger can cause a lot of undesirable use cases. For example, the loss of private keys will make a cryptocurrency, a token, or a smart contract uncontrolled, with negligible possibilities ever to restore it. Even if the blockchain can prevent many ownership disputes, the imperfect nature of people's relationships will always cause issues with ownership and the need to settle when they arise. In its pure design, the blockchain does not leave practical possibilities for enforcing any legitimate judicial decisions or legal actions by authorities.

4.3. Anonymity (pseudonymity)

The authorization and authentication for a transaction are provided only with the relevant private key within the asymmetric pair owned by the user.

The public key of the pair is taken to generate the address. The concept of addresses is the cornerstone of the blockchain. In a completed transaction, a coin is spent from one address and added to another address, but to enable such transfer, the owner of the coin must use the relevant private key. Thus, the address is the only public record in the ledger that identifies the user. However, some research has shown that addresses could be deanonymized by different digital fingerprints found in the network (IPs, behavior patterns, among others.) [24], [25]. The pure blockchain protocol is not suitable for keeping records on property and securities from the perspective of governments — blockchain anonymity veils money laundering, financing terrorism, and other unlawful activity.

Beyond that, the censorless nature of the blockchain creates confusion in identifying records at the practical level. Anyone may perform any transaction and publish any data in the blockchain. If a government must authorize a land title deed, how do you define if any transaction on the blockchain belongs to the town's clerk if they are all pseudonymous? Without overlaid solutions for digital identities and trust services, it is almost impossible to create any scalable model for governance.

4.4. Data integrity, off-chain data and issues of personal data

In the blockchain, any published data is exposed, and removal is not an option. Alternatively, users can insert into the blockchain cryptographic hashes of the data. The blockchain that stores hash sums will provide for two things: the user can verify the authenticity of the data (whether it is still the same or not) and timestamping since blocks are chronologically stored. However, hashing does not ensure the protection of the data itself. Once it is tampered with and/or deleted, the hash sum is useless for restoring. This leads to two possible solutions: data will be stored either by the third-party (for instance, a government agency) or by users themselves.

At present, all personal data and property records (title records) are stored in closed databases controlled by governments, and publishing hashes whether into the centralized DLT or open blockchain does not add much security. To verify this data, the user needs access to that closed database or just blindly trusts the entity which stores it. Even if a public blockchain is used to store hashes, there is still in this scheme a trusted party as the source of "truth," and therefore, one single source concentrating many risks for leaks and corruption of data becomes a single point of failure.

4.5. Scalability

One exclusively chosen blockchain for governance will necessarily create issues. Again, because of the open and free nature, the blockchain protocol does not prevent anyone from publishing junk data in the ledger.

The potential bandwidth of Bitcoin per year, for example, is roughly 220 million transactions [26]. For instance, 300 public registries in Ukraine generate as much as Bitcoin's bandwidth [27], which leaves no space for other cryptocurrency transfers. Overload with the transactions creates the problem of high transaction fees and price volatility. Although Bitcoin is not the best in terms of bandwidth, it is still the most attractive in terms of security [28]. This is not a workable solution on a scale, even for one country with a 40-mln population, randomly chosen as an example.

For blockchains using other consensus protocols or other data structure, scalability is not the main issue. For example, Ethereum, IOTA, NXT, NEM, and many other systems ensure better bandwidth and performance. The choice of one network or another is a discussion about technological neutrality – a principle that is often discussed in the context of public policy. The reader may find discussions comparing one specific blockchain network with some specific centralized system, where usually blockchain performance worsens. Having in mind the principle of technological neutrality, the problem of scalability has to be considered from another perspective. One blockchain network does not necessarily provide enough scalability, while a bundle of blockchains may become much more effective.

4.6. Price volatility

Due to speculation, the price of bitcoin and other cryptocurrencies can dramatically fluctuate, creating a bad user experience for those who need cryptocurrency to pay fees for transactions, for publishing and managing data, running smart contracts, etc. Together with the mentioned scalability issues, it makes it hard for governments to use or even to announce their intention to use any specific blockchain. It will inevitably incentivize high speculative interest on the market, exacerbating the problem of scalability even more.

4.7. What is opposed to blockchains and why it is still a good idea to use them

Eventually, it could be argued that permissioned DLTs are much better than the blockchain, as they address all these issues. Yet, as previously discussed, permissioned systems are centralized, and hence they imply manual control and restriction of unwanted practices and fixing of troubles, including retroactive actions. Compared to existing centralized closed government systems, such DLTs may have some advantages. However, from a conceptual point of view, they are very similar.

Another reason why the choice of a permissioned DLT leads to centralization is that the choice of one exclusive network/technology prevents competition. By choosing one permissioned DLT, the government takes responsibility for developing and maintaining infrastructure. On the contrary, open blockchain systems do not have central authorities that build the network. Any user is free to add their

computational resources for public needs and therefore, compete for rewards for finding blocks, without the reward being distributed by someone centrally, but automatically obtained as per the protocol. The infrastructure is self-organized and incentivized by cryptocurrency with free competition for mining, i.e., creating and storing blocks.

The principle of decentralization is the basis of this research. Therefore, we neither argue nor compare blockchain to other centralized solutions. Centralized databases have already been in use for quite a long time by governments and both their advantages and disadvantages are well-known. In this perspective, permissioned systems cannot be considered a significant evolutionary step in government systems.

In contrast, Blockchain is novel for governance, but the problems, as mentioned above, restrain its implementation at the state level if not properly addressed. Among various properties of the blockchain technology for a new generation of public property registries, we can distinguish the following:

- Blockchain provides an append-only type of database, an immutable ledger. It prevents data corruption and unauthorized changes.
- Blockchain has a native mechanism for managing ownership through public-key cryptography; thus, it is not only an immutable storage but a system for peer-to-peer transactions. Unlike traditional real estate registries, for example, it does not require a trusted third party to record a deed in the database.
- Blockchain is self-organized and does not require central authorities to govern and maintain the infrastructure.

The proposal in this research is to leverage the immutability aspect of the blockchain with the help of "smart law." The core idea is to reduce centralization when possible and, at the same time, make the system accountable when centralization is inevitable.

5. Thesis publications

This thesis is presented in five different papers (Subsections 5.1 – 5.5).

5.1. General Concept of Real Estate Tokenization on Blockchain

European Property Law Journal, De Gruyter. 2020, Volume 9, Issue 1, Pages 21–66, Oleksii Konashevych, https://doi.org/10.1515/eplj-2020-0003

The paper presents a concept of real estate tokenization, which includes legal, technological, and organizational aspects. The research introduces a theory of a Title Token - a digital record of ownership on the blockchain. It is discussed the principle of technological neutrality, where the traditional land registry is not necessarily abandoned in favor of blockchains, but instead, people gain the right to choose. Nowadays, public administrations use central-server databases, giving no alternatives for citizens. Recognition of the right of citizens to choose which technology to apply for managing their property rights creates a basis for free competition and the development of new technologies for better public services. Decentralized distributed ledgers are the key to decentralization. They enable more secure automation of legal procedures. On the contrary, centralization is a source of many issues in governance: abuse of power, corruption, inefficient governance, and high costs, slowness and complexity of bureaucratic procedures. With automation and reduction of intermediaries, the role of the government does not decrease but changes significantly, i.e., land cadaster bodies should not be monopolistic providers on the market. The paper introduces a theoretical basis for developing a new type of property registries.

5.2. Cross-Blockchain Protocol for Public Registries

International Journal of Web Information Systems, Emerald Publishing (accepted for publication, DOI: 10.1108/IJWIS-07-2020-0045), 2020, Oleksii Konashevych,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3537258

This paper presents a concept of the protocol for public registries based on blockchain. The proposed mechanism allows creating a standard database over a bundle of distributed ledgers. It ensures a

blockchain agnostic approach and utilizes the benefits of various blockchain technologies in one ecosystem. In this scheme, blockchains play the role of journal storages (immutable log), while the overlaid database is the indexed storage. The distinctive feature of such a system is that in blockchain, users can perform peer-to-peer transactions directly in the ledger using blockchain native mechanism of user access management with public-key cryptography (blockchain does not require to administrate its database). The protocol is designed for public property registries, i.e., land titles, cars, boats, corporate rights, etc. Users can create and manage their rights using the full power of blockchain technologies and smart contracts. The governance component in this protocol is introduced as Smart Laws and Digital Authorities, the algorithms to manage the overlaid system and address legal issues with property rights and law enforcement.

5.3. Constraints and Benefits of the Blockchain Use for Real Estate and Property Rights

Journal of Property, Planning and Environmental Law, Emerald Publishing, 2020, Vol. 12 No. 2, pp. 109-127, Oleksii Konashevych, https://doi.org/10.1108/JPPEL-12-2019-0061

Many recent social media posts and news may create a perception of big success in the use of blockchain for the real estate industry, land registration and protection of titles and property rights. A sobering outlook is crucial because misleading concepts may bury the whole idea of blockchain use. The paper aims to research the possibilities of blockchain and other distributed ledger technologies (DLT) and the applicability of these technologies for different purposes in real estate, property rights and public registries. This research is framed with policy studies and focuses on property rights, land registration regulatory framework and ICT innovations. The context of this paper is decentralization, which has been developed in political science studies and the role of blockchain and DLT in it. Therefore, the provided analysis of blockchain and DLT is interdisciplinary research to interpret the facets of DLT technologies in the context of real estate and land title registration. Permissioned and private DLT systems cannot be considered a significant evolutionary step in government systems. Blockchain, which is distinguished from permissioned systems as the technology of the immutable ledger that does not require authorities, is a new word in governance. However, this technology has some principal features that can restrain its implementation at the state level, and so require further research and development. The application of blockchain requires a proper architecture of overlaid technologies to support changes of outdated and mistaken data, address issues of digital identity and privacy, legal compliance and enforceability of smart contracts, hardforks and scalability of the ledger. This paper shows the constraints of the technology's properties which were not explained before in the context of title rights and land registration, even though technological limits are known in more specific technical sources. Along with the known benefits, this meant to help to avoid misinterpretation of some DLT features by non-technical people. A multidisciplinary approach in analyzing the technology and laws helped to understand better what can and cannot be beneficial for public registries and the protection of property rights. The presented outcomes can be laid down as requirements for the technical protocols aimed at addressing the issues of DLT and public policies to put blockchain at the service of society.

5.4. Data Insertion in Blockchain For Legal Purposes. How to Sign Contracts Using Blockchain

Electronic Modeling, 2019, №5 (19), Oleksii Konashevych, https://doi.org/10.15407/emodel.41.05.103

This article explores the use of blockchain technology, in particular, data insertion (anchoring, hashing) in the blockchain as a way of signing documents or imparting legal properties to facts. There is a comparing analysis of known methods of digital signature application towards the method of data insertion in the blockchain. During the research, we addressed the following issues. What is the data insertion in the blockchain, and what properties do the data acquire? What is the difference between insertion, anchoring, and hashing on the blockchain? What is the difference between blockchain hashing and a digital signature on a document? Will the document be legally binding if it is anchored in the blockchain? What conditions must be met to give legal force? How can anchoring be used to sign contracts, certify evidence that has legal value, denote time stamps, confirm authorship and copyrights, as well as transfer them, issue, and transfer power of attorney and delegate other rights, issue and transfer bearer instruments, etc.?

5.5. Blockchain Anchoring of Public Registries: Options and Challenges

International Conference on Theory and Practice of Electronic Governance (ICEGOV 2019) ACM Proceedings, 2019, Oleksii Konashevych and Marta Poblet, https://doi.org/10.1145/3326365.3326406

Governments across the world are testing different uses of the blockchain for the delivery of their public services. Blockchain hashing–or the insertion of data in the blockchain (anchoring)–is one of the potential applications of the blockchain in this space. With this method, users can apply special scripts to add their data to blockchain transactions, ensuring both immutability and publicity. Blockchain hashing also secures the integrity of the original data stored on central governmental databases. The objective of this paper is to analyze the use of data hashing (anchoring) on the blockchain for public state-owned registries. This paper starts by analyzing possible scenarios of hashing on the blockchain and assesses in which cases it may work and in which it is less likely to add value to a public administration. Second, the paper compares this method with traditional digital signatures using PKI (Public Key Infrastructure) and discusses standardization in each domain. Third, it addresses issues related to concepts such as "distributed ledger technology" and "permissioned blockchains." Finally, it raises the question of whether blockchain hashing is an effective solution for electronic governance, and concludes that its value is controversial, even if it is improved by PKI and other security measures. In this regard, we claim that governments need to identify pain points in governance in the first place, and then consider the trade-offs of the blockchain as a potential solution versus other alternatives.

6. Literature review

The study of relevant literature covered these basic directions: (i) technical documentation and academic research in blockchain and cryptography; (ii) academic papers covering the use of blockchain for real estate and industry reports and news; (iii) academic papers covering the use of blockchain and public sector (public services); (iv) public policy papers and government reports on the use of blockchain; (v) regulations in real estate and public registries.

The sources for the literature review included databases from the following publishers: Elsevier, Springer, IEEE, Ledger Journal, government agencies and public organizations. The analysis included exploring different industry platforms, such as Github, Bitcointalk, and online technical documentation of different blockchain projects and their wiki. These constitute a primary source of information about emerging technologies. Due to the lack of academic literature at the very begging of this research (four years ago), it became a crucial task to collect and analyze credible sources in the industry and media. For the purpose of this review, a final set of 53 items are considered and clustered into the five mentioned topics.

6.1. Technical documentation and academic research in blockchain and cryptography

The exploration of primary sources is a crucial element of this research because most of inventions and startups were born out of academic environments. This research was meant to select resources from the industry and the media, which are not just promotional but also materials supported with some level of research. Also, this section includes some academic papers exploring knowledge and experience in the industry.

The initial paper is the one authored by the elusive Satoshi Nakamoto, who introduced Bitcoin in 2008, later famously known as “cryptocurrency” [9]. This is the first design concept of blockchain technology. The 10-page “white paper” mostly discussed aspects of the future system design. Even though the paper was written in an academic style, there is no evidence that it was peer-reviewed. As of today, Github [29] and two notable community ‘wiki’ platforms [30], [31] provide information on blockchain technology and Bitcoin, i.e., Proof-of-Work, mining difficulty, block confirmations, bitcoin address generation, transaction structure and scripts (OP_RETURN, OP_DROP, etc.), block structure, signatures and multisignature schema, Colored Coins (on Bitcoin), etc.

Ethereum became a game-changer in the emerging technology by introducing the second-generation of ledger technologies. First launched by Vitalik Buterin in 2014, Ethereum gathered a team of innovators and investors through one of the first successful ICO (Initial Coin Offer) [32]. The innovators presented a second generation blockchain system with smart contracts and a Turing-complete programming language. Ethereum blockchain is not [only] a cryptocurrency but a decentralized multipurpose platform for developing applications on its blockchain. The community documentation can be found on Github [33], and eth.wiki [34]. Besides, Buterin's blogs provide a broad understanding of the project objectives, principles, and plans, and his discussions on decentralization are often cited in both media and academia. Notably, "The Meaning of Decentralization" [20] discusses three levels decentralization (the paper is analyzed in Section 3.3 above), and "Hard Problems in Cryptocurrency: Five Years Later" [35] discusses measures which are meant to support decentralization in a public blockchain.

Emercoin project is the third project in this list of sources because their Name-Value Storage (NVS) became the reference technology for the cross-blockchain protocol presented in my thesis. NVS is an overlaid public database for the Emercoin blockchain. The technology itself is partially inherited from Namecoin blockchain [36], academic research of which is provided by Loibl (2014) [37]. The Emercoin community documentation thoroughly presents the NVS technology [38].

Another group of papers that became a basis for this research comes from various fields in social sciences: economics and finances, legal studies, governance and politics. One key paper is the article "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" [39] by Wright and De Filippi (2015) that explores the benefits and drawbacks of this emerging decentralized technology and argues that its widespread deployment will lead to the expansion of a new subset of law, known as Lex Cryptographia: rules administered through self-executing smart contracts and decentralized (autonomous) organizations. As blockchain technology becomes widely adopted, centralized authorities, such as governmental agencies and large multinational corporations, could lose the ability to control and shape the activities of disparate people through existing means. As a result, there will be an increasing need to focus on how to regulate blockchain technology and how to shape the creation and deployment of these emerging decentralized organizations in ways that have yet to be explored under current legal theory.

The paper "Bitcoin: Economics, Technology, and Governance" [40] by Böhme et al. (2015) presents the technology in the language of economics. Researchers share empirical data on capitalization and economic impact. Another key paper in this field is "BlockChain Technology: Beyond Bitcoin" by Nachiappan (2016) [41] – describing blockchain technology and some compelling specific applications in both financial and non-financial sectors. Its authors define challenges and business opportunities "in this fundamental technology that is all set to revolutionize the digital world."

The third paper in economics outlining the place of the emerging technology in the world economy and history appears in the book "Understanding the blockchain economy: an introduction to institutional Cryptoeconomics" by Berg, Davidson and Potts (2019) [42]. This book explores the future of global capitalism by offering the first scholarly analysis of the economic nature of blockchains and the formation of the blockchain economy. Applying the institutional economics of Ronald Coase and Oliver Williamson, the authors highlight how blockchains are poised to reshape the nature of firms, governments, markets, and civil society. Chapters apply basic economic principles to explore blockchains and distributed ledger technologies through the framework of institutional economics. The book suggests ways in which cryptocurrencies such as Bitcoin may develop further in the future, bringing us back to a barter economy that removes the need for a third person in economic transactions. Outlining a ledger-centric view of the economy, the authors explore how blockchains and dehierarchalization will reduce the demand for government regulation.

As opposed to multiple industry publications on the benefits and advantages of blockchain, which sometimes are not supported by rigorous research, an important point is taken by academic explorations. Thus, "Data Insertion in Bitcoin's Blockchain" Sward, Vecna and Stonedahl (2018) [16] scrutinize scripts and methods of inserting arbitrary data in Bitcoin ledger. Data insertion became the major fundamental

feature of the technology leading to all known applications of blockchain beyond cryptocurrency: colored coins subsequently known as tokens, smart contracts, public databases on a ledger (e.g., NVS), decentralized applications (dApps) and decentralized autonomous organizations (DAO). The paper analyzes the ability of the ledger to store and operate data securely.

6.2. Academic papers regarding the use of blockchain for real estate and industry reports

This section introduces a wide range of issues regarding the use of blockchain for real estate: how to improve a land registry, how to facilitate transactions in real estate using DLT, how to introduce fractional ownership in those jurisdictions where co-owners cannot own titles, how to use blockchain for investments in real estate, and other problems in the industry. A number of papers discuss high-level ideas of the blockchain implication for real estate. It is also important to notice that some papers present their conclusions on cases that were subsequently less successful than expected. The major conclusion here is that the industry requires more pilots and observation to conclude which practices are viable.

For example, in "Blockchain and Property in 2018: At the End of the Beginning," [43] Graglia and Mellon (2018) discuss the advantages of the blockchain and attribute its features to centralized distributed ledger systems. Among examples, the authors identified Dubai and the Republic of Georgia. Neither example can be considered as a success in the field. In Dubai, there are still no details of the project to conclude any progress. In Georgia, even though there is a working project, the design of the system and benefits are questionable, something that is discussed in this thesis in Paper 5.

In "Implications of block chain in real estate industry" [44], Mehendale, Masurekar and Patil (2019) discuss the technology of a distributed ledger and identify "public blockchain" and "permissioned blockchain," attributing the same features and advantages to both types. The authors discuss various aspects of contractual relations (payments, sharing data, etc.) in real estate and conclude that blockchain could be helpful. The paper does not provide any particular system design.

The advantages of blockchain are also considered in "Challenges and opportunities using multichain for real estate" [45] by Avantaggiato and Gallo (2019). The authors propose some ideas in the system design and discuss the system's applicability in the contractual process. The concept is drawn out of the context of a title right, a land registry, registration and acknowledgment procedures.

A discussion on opportunities for investments in real estate is presented in the overview "Disruptive potential of real estate crowdfunding in the real estate project finance industry: A literature review" [46] by Montgomery, Squires and Syed (2018). The paper discusses the advantages of DLT tools for investments in real estate. The paper guides through potentially successful examples of the blockchain application. In the working paper "Tokenization – The Future of Real Estate Investment?" [47] Baum (2020) continues the discussion on new ways of investments and funding, exploring various examples. The author extends the discussion to the problem of fractional ownership, which is inevitably related to crowdfunding. This is a larger discussion on the absence of a basic legal concept of fractional title ownership in some jurisdictions (UK, USA, Australia, etc.). In "Blockchain technology in commercial real estate transactions," [48] Wouda and Opdenakker (2019) propose a blockchain-based infrastructure to enhance the current transaction process of an office building. As per the authors, "Blockchain technology relies on DLT." The paper proposes a limited discussion on the system architecture design and does not touch on a land registry, registration and acknowledgment of deeds.

Four additional papers focus their attention on national/regional land registries and blockchain. Two of them are academic papers, and the remaining two are reports from land authorities and their partners introducing pilot projects. In "Can blockchain spark off the reincarnation of India's living dead?" [49] Pandey (2018) discusses the problem of corruption in the land registry of India and the advantages of blockchain to address it. The author proposes to use "permissioned blockchain" and high-level architecture design. The paper leaves space for further research. For example, the reader will not find answers to why a centralized "permissioned' system is better than the existing electronic registry and how without changes in bureaucracy (which led to the existing problems), the government may improve the land registry and

protect citizens' property rights. In the other academic paper, "Blockchain technology and land registry" [7] Themistocleous (2018) identifies some problems in the land registries. This paper articulates the idea of improving the quality of land registries by using blockchain technology to overcome the limitations of centralization. The author proposes piloting a project in the Republic of Cyprus, though the paper does not specifically address how to apply the blockchain. In "The Land Registry in the blockchain - testbed. A development project with Lantmäteriet" [50] under collective authorship of representatives from six organizations – Lantmäteriet (Swedish land authority), Landshypotek Bank, SBAB, Telia company, ChromaWay and Kairos – it is presented a pilot project testing DLT for land transactions. The prototype system was based on a centralized (permissioned) system. Since 2017 (when the testing took place) until 2020, the project did not see any further application or implementation in Sweden or elsewhere. A similar situation is observed with the pilot in Cook County (Illinois, US). The county's land office issued its report [51] but did not continue. The pilot presented the transaction on a blockchain that contains a hash sum taken from the land registry. This basic idea is repeated in the pilot in the Republic of Georgia, the analysis of which is presented in Paper 5.

6.3. Academic papers regarding the use of blockchain and public sector (public services)

A large portion of papers operate on a higher level when it comes to land registry, i.e., public services and e-government, seeking answers on how blockchain can improve this field. Among the first to discuss governance and blockchain was a journal paper "Beyond Bitcoin enabling smart government using blockchain technology" [52] by Ølnes (2016). The author refers to the example of publishing hashes on Bitcoin - a small project at the University of Nicosia, where students were given electronic certificates after finishing a course, and a hash sum of the certificate was inserted in Bitcoin's blockchain. Hashing on blockchain is much discussed in Paper 5 and also a part of a larger discussion on data insertion in blockchain for legal purposes or "How to Sign Contracts Using Blockchain" in Paper 4 of this thesis.

In "Disrupting governance with blockchains and smart contracts," [53] Shermin (2017) discusses the major constraints of the use of blockchain. There is a gap between the initial conceptualizations of blockchains and their first instantiations. First use cases show that as circumstances change, protocols can become inappropriate for the new environment and require modification. Modification of blockchain code happens through majority consensus, but reaching consensus in a distributed multi-stakeholder network with sometimes unaligned interests is complex, potentially introducing new agency issues.

In "Blockchain technology as a support infrastructure in e-Government," [54] Ølnes and Jansen (2017) continued the exploration of blockchain for governance. The authors are among the first to caution unreasonable optimism in the use of "permissioned" and "private" systems in public services: "Closed blockchains [...] must rely on traditional security mechanisms in order to prevent unwanted access and modification to the blockchain." The paper mainly discusses open blockchains [networks], because as authors emphasize, "closed systems are never able to build an infrastructure."

In "Blockchain in Government: Benefits and implications of distributed ledger technology for information sharing," [55] Ølnes, Ubacht and Janssen (2017) ask whether blockchain technology will lead to innovation and the transformation of governmental processes. To address this question, the authors presented a critical assessment of the often- "exaggerated benefits of blockchain technology" found in the literature and discussed their implications for governmental organizations and processes. The paper summarizes directions for further research into the potential benefits of blockchain applications in e-government and the role of governance of blockchain architectures and applications to comply with societal needs and public values.

In "A framework of blockchain-based secure and privacy-preserving E-government system," [56] Elisa et al. (2018) argue that most of the existing e-government systems, such as websites and electronic identity management systems (eIDs) are centralized at duplicated servers and databases. A centralized management and validation system may suffer from a single point of failure and make the system a target to cyberattacks such as malware, denial of service attacks (DoS), and distributed denial of service attacks

(DDoS). The blockchain technology enables the implementation of highly secure and privacy-preserving decentralized systems where transactions are not under the control of third-party organizations. They propose a framework of a decentralized e-government peer-to-peer (p2p) system using blockchain technology to ensure information security and privacy while simultaneously increasing the trust of the public sectors. In addition, a prototype of the proposed system is presented with the support of a theoretical and qualitative analysis of the security and privacy implications of such a system. It is important to note that the authors share the idea that a "permissioned" (centralized) system can be called "blockchain." They attribute this system features of blockchain: "The permissioned blockchain system ensures that the stored records are trustworthy, auditable and transparent." In the proposed architecture, it is clear that infrastructure is introduced and maintained by the government. The question of how the proposed centralized system is better than the existing one remains open.

A more political tone is observed in "Blockchain Regulation and Governance in Europe, Blockchain Regulation and Governance in Europe" [57] by Finck (2018). The author examines the relationship between blockchain technology and EU law and introduces the theme of blockchain governance. The book provides a general introduction to blockchains as both a "regulatable and regulatory technology." It outlines the interaction between distributed ledger technology and specific areas of EU law, such as the General Data Protection Regulation.

Batubara, Ubacht and Janssen published their "Challenges of blockchain technology adoption for e-government: A systematic literature review" [58] in 2018. The paper guides through a number of studies and pilots in the use of blockchain in governance available by 2018. Several countries such as the USA, the United Kingdom, the Netherlands, the United Arab Emirates, Estonia, Sweden and China announced blockchain initiatives to explore its uses in the public sector actively. Their findings have shown that academic research in this area had only just started and issues discussed in the selected literature were still significantly limited. Consequently, more intensive research in this area was still necessary to advance this field's maturity. As per the authors, the major challenges from the organizational perspective are the need for new governance models and the acceptability of this technology. The research into blockchain technology standards and a reference architecture for e-Government applications was proposed to resolve the technological challenges.

Further directions are found in Franciscon et al. (2019) "A systematic literature review of blockchain architectures applied to public services" [59]. This work provides a systematic review of blockchain-based applications across multiple domains: supply chain, business, healthcare, IoT, privacy, and data management. Authors point to the shortcomings identified in the relevant literature, particularly limitations the blockchain technology presents and how these limitations spawn across different sectors and industries. Building on these findings, authors identify various research gaps and future exploratory directions that are anticipated to be of significant value both for academics and practitioners. To add, the authors include in their research the review of permissioned and hybrid (federated) systems. The latter two are characterized as prune to "collusion attacks," while immutability corruption is almost impossible in public consensus systems immutability corruption is "almost impossible."

Brinkmann and Heine (2019) in "Can blockchain leverage for new public governance? A conceptual analysis on process level" [60] presents the preliminary results of ongoing research, which aims to shed light on the more concrete benefits of Blockchain for the purpose of New Public Governance (NPG). The preliminary results show that Blockchain offers valuable support for governments seeking methods to coordinate co-producing networks effectively. It becomes evident that there is a need for off-chain processes. Therefore, it is argued in favor of intensifying research on off-chain governance processes better to understand the implications for and influences on on-chain governance.

More recently, the paper "Smart Contracts for Government Processes: Case Study and Prototype Implementation" [61] by Krogsbøll et al. (2020) contains a description of the pilot with the Danish Municipality. The government partner concluded that the risk of losing access to the system (due to loss of private keys) outweighed any benefits. The researchers on the other side think that smart contract

implementations of government processes need to be immutable and outside of the government's control when running; however, they also need to be updatable when laws change and provide an "out" for the rare case when errors in the contract implementation result in unlawful behavior and consider these problems as the "foundational research challenge for blockchain to be applicable to governmental processes."

6.4. Public policy papers and government reports on the use of blockchain

The government of the UK was among the first to publish their report on blockchain "Distributed ledger technology: Beyond blockchain [41] (2015). This report explains the use of blockchain technology and outlines significant application directions in the public sector. This report was drawn to explain the society a general idea of advantages of the emerging technology, rather than introducing exact projects.

A similar report is presented in the European Parliament by their Research Service (2017), "How Blockchain Technology Could Change Our Lives" [62]. The report is "an explanatory guide to the technology, challenges, and possibilities that bring emerging technology to EU society." Another European organization - European Union Agency for Network Information Security - issued "Distributed Ledger Technology & Cybersecurity: Improving information security in the financial sector" [23]. This report contains valuable technical information and guides readers through distributed ledger technology. One of the sections is devoted to risk analysis.

The Australian research unit Data61 at CSIRO introduced their report in 2017 "Distributed Ledger" [63]. This study contains analysis, interpretation, and foresight in consultation with subject-matter experts, in order to inform government, industry, and the broader Australian community of the plausible implications of Distributed Ledger Technology (DLT). The intended outcome was to provide warning of potential challenges, risks aand opportunities so that leaders and innovators can make better-informed decisions, including high impact policies, for today, which will impact our future.

In 2019 governments at different levels – national in Cyprus and the EU - published their reports to cover strategy issues with regard to the emerging technology. In "Distributed Ledger Technologies (Blockchain). A National Strategy for Cyprus" [64] the government of Cyprus expresses its interest in applying blockchain in different spheres, including land registry. A blockchain network will validate ownership, property details and encumbrances with the DLS. Integration with external oracles and smart contracts will help to integrate various stakeholders: involve multiple departments (TAX) at both governmental and private sector (law firms, Financial Institutions such as Banks). In "Blockchain for Digital Government, Publications Office of the European Union," [65] a group of researchers (Allessie et al.) under the umbrella of the Joint Research Centre of the European Commission studied various use cases. It concluded that contrary to how it is often portrayed, blockchain, so far, is "neither transformative nor even disruptive for the public sector." They have not observed the creation of new business models, the emergence of a new generation of services, nor direct disintermediation of any public institutions involved in the provision of governmental functions. Incompatibility between blockchain-based solutions and existing legal and organizational frameworks is a significant barrier to unlocking the transformative potential of blockchain.

In 2019 International Organization for Standardization (ISO) – "ISO/TC 307 Blockchain and distributed ledger technologies" [66]. This document presents the basic terminology and concepts of DLT.

References

1. Dawes, S.S.: The Evolution and Continuing Challenges of E-Governance. Public Adm. Rev. 68, S86–S102 (2008). https://doi.org/10.1111/j.1540-6210.2008.00981.x.
2. Malinauskienė, E.: Conceptual Framework for Context-Based E-Government Interoperability Development. Soc. Technol. 3, 68–84 (2013). https://doi.org/10.13165/st-13-3-1-05.
3. Jansen, A.: The understanding of ICTs in public sector and its impact on governance. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 174–186 (2012). https://doi.org/10.1007/978-3-642-33489-4_15.
4. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design Science in Information Systems Research. MIS Q. Manag. Inf. Syst. 28, 75–105 (2004). https://doi.org/10.2307/25148625.
5. Gregor, S., Hevner, A.R.: Positioning and presenting design science research for maximum impact, https://openresearch-repository.anu.edu.au/handle/1885/35868, (2013). https://doi.org/10.25300/MISQ/2013/37.2.01.
6. Lessig, L.: Code 2.0. (2002).
7. Themistocleous, M.: Blockchain technology and land registry. Cyprus Rev. 30, 195–202 (2018).
8. Cavoukian, A.: Privacy by design [leading edge]. IEEE Technol. Soc. Mag. 31, 18–19 (2012). https://doi.org/10.1109/MTS.2012.2225459.
9. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, last accessed 2016/12/27. https://doi.org/10.1007/s10838-008-9062-0.
10. BitcoinTalk: overflow bug SERIOUS, https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/185/, last accessed 2019/11/10.
11. Haber, S., Scott Stornetta, W.: How to time-stamp a digital document. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 437–455. Springer Verlag (1991). https://doi.org/10.1007/BF00196791.
12. Back, A.: Hashcash - A Denial of Service Counter-Measure. Hashcash.Org. (2002).
13. King, S., Nadal, S.: PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. (2012).
14. Daniel Larimer: Delegated Proof-of-Stake Consensus | BitShares Blockchain, https://bitshares.org/technology/delegated-proof-of-stake-consensus/, last accessed 2019/11/10.
15. Wood, G.: guide/poa.md at master · ethereum/guide · GitHub, https://github.com/ethereum/guide/blob/master/poa.md, last accessed 2019/11/10.
16. Sward, A., Vecna, I., Stonedahl, F.: Data Insertion in Bitcoin's Blockchain. Ledger. 3, 1–23 (2018). https://doi.org/10.5195/LEDGER.2018.101.
17. Schneider, N.: Decentralization: an incomplete ambition. J. Cult. Econ. 12, 265–285 (2019). https://doi.org/10.1080/17530350.2019.1589553.
18. Benkler, Y.: Degrees of freedom, dimensions of power. Daedalus. (2016). https://doi.org/10.1162/DAED_a_00362.
19. Digital Signature Standard (DSS), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf, (2013). https://doi.org/10.6028/NIST.FIPS.186-4.
20. Buterin, V.: The Meaning of Decentralization, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274, last accessed 2019/09/14.
21. On Distributed Communications Series,

https://www.rand.org/pubs/research_memoranda/RM3420/RM3420-chapter2.html, last accessed 2019/10/26.

22. Yoo, C.S.: Paul Baran, Network Theory, and the Past, Present, and Future of Internet. SSRN Electron. J. (2019). https://doi.org/10.2139/ssrn.3317642.

23. Distributed Ledger Technology & Cybersecurity: Improving information security in the financial sector. (2016). https://doi.org/10.2824/80997.

24. Ober, M., Katzenbeisser, S., Hamacher, K.: Structure and Anonymity of the Bitcoin Transaction Graph. Futur. Internet. 5, 237–250 (2013). https://doi.org/10.3390/fi5020237.

25. Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S.: Evaluating user privacy in Bitcoin. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). p. 596 (2013). https://doi.org/10.1007/978-3-642-39884-1_4.

26. Roio, D.J.: Bitcoin, the end of the Taboo on Money. Dyne.org Digit. Press. 1–17 (2013).

27. Data.gov.ua, https://data.gov.ua/, last accessed 2019/09/16.

28. Cost of a 51% Attack | Crypto51.app, https://www.crypto51.app/about.html, last accessed 2019/08/13.

29. Bitcoin Core, https://github.com/bitcoin/bitcoin, last accessed 2017/01/04.

30. Bitcoin Wiki, https://en.bitcoin.it/wiki/Bitcoin_Wiki:About, last accessed 2020/06/02.

31. BitcoinWikipedia, https://en.bitcoinwiki.org/wiki/BitcoinWiki:About, last accessed 2020/06/02.

32. [ANN] Ethereum: Welcome to the Beginning, https://bitcointalk.org/index.php?topic=428589.0, last accessed 2020/06/02.

33. Ethereum Wiki, https://github.com/ethereum/wiki/wiki/Glossary, last accessed 2017/07/04.

34. Ethereum Wiki, https://eth.wiki/, last accessed 2020/06/02.

35. Hard Problems in Cryptocurrency: Five Years Later, https://vitalik.ca/general/2019/11/22/progress.html, last accessed 2019/12/02.

36. Namecoin.org, https://namecoin.org/, last accessed 2018/09/05.

37. Loibl, A.: Namecoin. (2014). https://doi.org/10.2313/NET-2014-08-1_14.

38. Emercoin NVS, https://wiki.emercoin.com/en/Emercoin_NVS, last accessed 2018/01/31.

39. Wright, A., De Filippi, P.: Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Soc. Sci. Res. Netw. 62, 4–22 (2015). https://doi.org/10.2139/ssrn.2580664.

40. Böhme, R., Christin, N., Edelman, B., Moore, T.: Bitcoin: Economics, Technology, and Governance. Source J. Econ. Perspect. J. Econ. Perspect. 29, 213–238 (2015). https://doi.org/10.1257/jep.29.2.213.

41. Nachiappan, Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V.: BlockChain Technology: Beyond Bitcoin. Appl. Innov. Rev. (2016).

42. Berg, C. (Research fellow), Davidson, S., Potts, J.: Understanding the blockchain economy: an introduction to institutional cryptoecnomics. Edward Elgar (2019).

43. Graglia, J.M., Mellon, C.: Blockchain and Property in 2018: At the End of the Beginning. Innov. Technol. Governance, Glob. 12, 90–116 (2018). https://doi.org/10.1162/inov_a_00270.

44. Mehendale, D.K., Masurekar, R.S., Patil, H. V.: Implications of block chain in real estate industry. Int. J. Recent Technol. Eng. 8, (2019).

45. Avantaggiato, M., Gallo, P.: Challenges and opportunities using multichain for real estate. In:

2019 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom 2019 (2019). https://doi.org/10.1109/BlackSeaCom.2019.8812780.

46. Montgomery, N., Squires, G., Syed, I.: Disruptive potential of real estate crowdfunding in the real estate project finance industry: A literature review, (2018). https://doi.org/10.1108/PM-04-2018-0032.

47. Baum, A.: Tokenisation – The Future of Real Estate Investment? , Oxford (2020).

48. Wouda, H.P., Opdenakker, R.: Blockchain technology in commercial real estate transactions. J. Prop. Invest. Financ. 37, 570–579 (2019). https://doi.org/10.1108/JPIF-06-2019-0085.

49. Pandey, P.: Can blockchain spark off the reincarnation of India's living dead? In: 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies, 3ICT 2018. Institute of Electrical and Electronics Engineers Inc. (2018). https://doi.org/10.1109/3ICT.2018.8855731.

50. The Land Registry in the blockchain - testbed. (2017).

51. Mirkovic, J.: Blockchain Pilot Program. Final Report. (2017).

52. Ølnes, S.: Beyond Bitcoin enabling smart government using blockchain technology. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 253–264. Springer Verlag (2016). https://doi.org/10.1007/978-3-319-44421-5_20.

53. Shermin, V.: Disrupting governance with blockchains and smart contracts. Strateg. Chang. 26, (2017). https://doi.org/10.1002/jsc.2150.

54. Ølnes, S., Jansen, A.: Blockchain technology as s support infrastructure in e-Government. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (2017). https://doi.org/10.1007/978-3-319-64677-0_18.

55. Ølnes, S., Ubacht, J., Janssen, M.: Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Gov. Inf. Q. 34, 355–364 (2017). https://doi.org/10.1016/J.GIQ.2017.09.007.

56. Elisa, N., Yang, L., Chao, F., Cao, Y.: A framework of blockchain-based secure and privacy-preserving E-government system. Wirel. Networks. (2018). https://doi.org/10.1007/s11276-018-1883-0.

57. Finck, M.: Blockchain Regulation and Governance in Europe. Cambridge University Press (2018). https://doi.org/10.1017/9781108609708.

58. Batubara, F.R., Ubacht, J., Janssen, M.: Challenges of blockchain technology adoption for e-government: A systematic literature review. In: ACM International Conference Proceeding Series. Association for Computing Machinery (2018). https://doi.org/10.1145/3209281.3209317.

59. Franciscon, E.A., Nascimento, M.P., Granatyr, J., Weffort, M.R., Lessing, O.R., Scalabrin, E.E.: A systematic literature review of blockchain architectures applied to public services. In: Proceedings of the 2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design, CSCWD 2019. pp. 33–38. Institute of Electrical and Electronics Engineers Inc. (2019). https://doi.org/10.1109/CSCWD.2019.8791888.

60. Brinkmann, M., Heine, M.: Can blockchain leverage for new public governance? A conceptual analysis on process level. In: ACM International Conference Proceeding Series (2019). https://doi.org/10.1145/3326365.3326409.

61. Krogsbøll, M., Borre, L.H., Slaats, T., Debois, S.: Smart Contracts for Government Processes: Case Study and Prototype Implementation. In: Financial Cryptography and Data Security 2020. pp. 1–8. International Financial Cryptography Association (2020).

62. Boucher, P.: How Blockchain Technology Could Change Our Lives. In-Depth Analysis. European

Parliamentary Research Service. (2017).

63. Distributed Ledger, https://www.data61.csiro.au/en/our-work/safety-and-security/secure-systems-and-platforms/blockchain, (2017).

64. Distributed Ledger Technologies (Blockchain). A National Strategy For Cyprus. (2019).

65. Allessie, D., Sobolewski, M., Vaccari, L., Pignatelli, F.: Blockchain for Digital Government., Luxembourg (2019). https://doi.org/10.2760/93808.

66. ISO/TC 307 Blockchain and distributed ledger technologies. (2019).

67. Schmid, C., Hertel, C.: Real Property Law and Procedure in the European Union General Report Final Version scientific co-ordinators. (2005).

PAPER 1

Oleksii Konashevych*

General Concept of Real Estate Tokenization on Blockchain

The Right to Choose

https://doi.org/10.1515/eplj-2020-0003

Abstract: This paper presents a concept of real estate tokenization, which includes legal, technological, and organizational aspects. The research introduces a theory of a Title Token – a digital record of ownership on the blockchain. It is discussed the principle of technological neutrality, where the traditional land registry is not necessarily abandoned in favor of blockchains, but instead, people gain the right to choose. Nowadays, public administrations use central-server databases, giving no alternatives for citizens. Recognition of the right of citizens to choose which technology to apply for managing their property rights creates a basis for free competition and the development of new technologies for better public services. Decentralized distributed ledgers are the key to decentralization. They enable more secure automation of legal procedures. On the contrary, centralization is a source of many issues in governance: abuse of power, corruption, inefficient governance, and high costs, slowness and complexity of bureaucratic procedures. With automation and reduction of intermediaries, the role of the government does not decrease but significantly changes, i.e. land cadaster bodies should not be monopolistic providers on the market. The paper introduces a theoretical basis for developing a new type of property registries.

Keywords: blockchain, distributed ledger technologies, real estate, property rights, land registry, cadastre, tokens, title tokens

I. Intro

Since the invention of the blockchain technology by Satoshi Nakamoto (Nakamoto, 2008), the media has proliferated a ton of news with ambitious statements of projects which were to disrupt various fields, including governance, bureaucracy, and public registries. One of the promising directions in exploration is the field of peer-to-peer deeds with land titles and other property rights.

***Corresponding author: Oleksii Konashevych,** Erasmus Mundus Joint International Doctoral Fellow in Law, Science and Technology (EU), E-Mail: oleksii.konashevych2@unibo.it

There are several attempts by governments around the world to try distributed ledger technologies (DLT) and blockchain applications, but there are no examples of revolutionary transformations in the public sector, though. Many researchers (Ølnes and Jansen, 2017), (Allessie *et al.*, 2019), (Alketbi, Nasir and Talib, 2018), (Konashevych, 2020a) emphasize that projects are at early stages to conclude any success; there is a need for further observation and collecting empirical data. Many pilots have never progressed far beyond the initial stages. As recent research showed (see in the literature review section), many initiatives either lack a systematic approach or bump up against old fashioned legislation and government inertia. Even if good ideas appear, they have fewer chances of being effectively introduced because one change may trigger the other, which eventually creates the need for a high-level concept and an elaborate action plan. Recent review shows (Batubara, Ubacht and Janssen, 2018) that the field also lacks proactive concept development, which will involve a multidisciplinary approach.

It is assumed that the systematic approach requires a combination of:

- Design Science Research, which is a direction of Information System (IS) science purposed to develop new technologies and improve existing software; and
- Social Sciences, including Policy Studies, aimed to improve and modernize governance and economics.

This paper accumulates knowledge of previous research. It introduces a comprehensive vision in managing property rights in the 21st century, which inevitably involves discussions on technology design, legislation, and public administration.

Among examples, where a pilot has been developed, but no consistent plan was introduced is a project in the UK within the initiative "Digital Street" (*HM Land Registry is making it easier to remortgage – GOV.UK*, no date), Chromaway in Sweden (*The Land Registry in the blockchain – testbed*, 2017), Bitfury in Georgia (*Republic of Georgia to Develop Blockchain Land Registry – CoinDesk*, no date). Various previous research showed that mentioned projects are in early practical attempts to probe the technology rather than revolutionize the domain.

As a result, we have a vicious circle: enthusiasts generate ideas of the blockchain use but cannot support them with a consistent concept which fit into the overall picture of governance, legislation, and transformation of public services, on the other side governments holding in their hands old fashioned bureaucratic system and but restrain initiatives because they lack systematic approach and theoretical background.

Let us consider which recent academic research creates a background for developing a new public policy in protecting the property rights of citizens and transforming the red tape.

1.1 Literature review

Wright and De Philippi turned a new page in academia research in the use of blockchain for governance by introducing their concept of "Lex Cryptographia" (Wright and De Filippi, 2015). "Lex Cryptographia" are rules administered through self-executing smart contracts and decentralized (autonomous) organizations. The researchers emphasized that *"Blockchain technology has the potential to reduce the role of one of the most important economic and regulatory actors in our society—the middleman."* The research outlined important directions of further development: automated contractual negotiation, execution, and enforcement, growth of the peer-to-peer economy, smart property and machine-to-machine communications, distributed real-time governance, algorithmic governance, the regulation of decentralized architectures.

Another paper that became a basis for this research was "Constraints and Benefits of the Blockchain Use for Real Estate and Property Rights" (Konashevych, 2020a) introduced an analysis of existing technical problems of the blockchain use in public registries and land registration: multiplication of assets due to hardforks, the enforceability of transactions and smart contracts; anonymity and digital identity, personal data exposure, scalability and price volatility. The paper argues that to address these issues, so-called "permissioned blockchains" are considered, but they appear neither decentralized nor immutable. The paper raises the question of the responsibility of politicians, public servants, the media, and leaders of public opinion in presenting projects based on permissioned DLTs titling them "blockchain" but without an intention and potential of decentralization. The paper discussed conceptual and practical issues of the blockchain implementation by the governments and enthusiasts. The research addresses various misconceptions in the use of blockchain. A multidisciplinary approach in analyzing the technology and laws helped to understand better what can and cannot be beneficial for public registries and the protection of property rights.

The presented concept "Cross-Blockchain Databases for Governments: The Technology for Public Registries and Smart Laws" (Konashevych, 2020b) laid down as a backbone of the system design that addresses the issues with public blockchains discussed in the previous paper. The protocol accommodates a framework of smart law, which is a set of digitized rules to manage users' records and govern the information system.

Other papers appear less relevant to this research work; however, they became a source of knowledge in the domain. "Challenges of blockchain technology adoption for e-government: A systematic literature review" (Batubara, Ubacht and Janssen, 2018) provides a valuable overview of the research directions in the field of use of blockchain in the public sector. Their findings showed that aca-

demic research in this area has only just started, and issues discussed in the selected literature were still very limited. Consequently, more intensive research in this area is still necessary to advance the maturity of this field of research. Researchers emphasize the need for new governance models and acceptability of this technology are the major challenges from the organizational perspective. To resolve the technological challenges, they propose research into blockchain technology standards and a reference architecture for e-Government applications.

We can consider the research of cross-blockchain infrastructure (Konashevych, 2020b) as the initiative in building standards and this paper as an architectural concept and a model of the blockchain use in estate and other public registries.

1.2 Theoretical Framework and Methodology

This is a multidisciplinary research framed with Policy and Legal Studies, Information Science, and Legal informatics. This paper draws conclusions from different sources: (1) technical reports and white papers of projects, such as Bitcoin, Ethereum and Emercoin; (2) academic papers; (3) technical analysis from forums and open industry platforms, mainly GitHub. Last but not least, the paper is based on the author's empirical experience acquired throughout four years of research on the topic, which included attending conferences, workshops, and meetings in different countries within the blockchain industry and academia.

The experience of developing e-governance in different countries is considered a valuable source of knowledge for this research. In "The Evolution and Continuing Challenges of E-Governance" (Dawes, 2008) the author defines this field of knowledge as "the use of information and communication technologies (ICTs) to support public services, government administration, democratic processes, and relationships among citizens, civil society, the private sector, and the state." The author emphasized that given the nature and pace of technological change, ICT strategies, tools, and innovations will continue to shape the information environment of governance.

Though this paper is distinguished from observational and descriptive research with its pro-active research outcomes by proposing a systematic concept for implementation, further research, and improvement. The paper bridges the complex matter of technologies to social science: law, governance, and economics. The research can be used by policymakers and ICT developers to design a useful application.

1.3 Research structure

The research consists of an Introduction, the main section, and the conclusion. The main section starts with a brief outlining of the concept. The next subsection explains the incentives and prerequisites to the concept application. The following section consists of seven subsections that scrutinize the details. The last part concludes the research.

1.4 Glossary

The paper is aimed to present the concept for a wide range of readers from different domains: academic researchers, IS developers, policy developers, and the general public. The multidisciplinary nature of the discussion may create difficulties in understanding details. The following thesaurus presents the terminology and concepts which are used in this paper and aims to fill the gap in technical knowledge, at least in extent, which is enough to read this paper. Instead, to address academic disputes in the field, this terminology is designed to clarify the author's point of view and approach for further reading:

- Distributed ledger technology (DLT) –
  A technology of a network with a shared ledger.
- Blockchain –
  DLT which stores transactions in cryptographically interconnected blocks with a decentralized consensus. Blockchain is distinguished from "permissioned," "private," "federated," enterprise," and other centralized types of DLTs, as the immutability of the ledger depends not on someone's will but a public peer-to-peer interaction where an administrator or administrators are not distinguishable.
- Token –
  A record on DLT attached to a user's blockchain address (public key) and managed by a user's private key through blockchain transactions.
- Hash function (cryptographic hash function) –
  A one-way cryptographic function that represents the original data in a short string – a hash sum (digest, checksum). Hash is a "digital fingerprint" of data; it represents but does not disclose the original data. It is used to verify the authenticity of data.
- Public-Key Cryptography (asymmetric cryptography) –
  - Private key
    Is a secret string used to encrypt data to obtain a digital signature and to decrypt data that is encrypted with the relevant public key.

- Public key
  Is a string used to decrypt data that is signed with the relevant private key. The public key is exclusively interconnected with the private key. If any data can be decrypted with a public key, it means it was encrypted with the relevant private key. Public key can be used as digital identity, i.e., the one who knows who owns the private key can be sure the data is encrypted by relevant private key. The public key is also used to encrypt data and send secret messages to the private key's owner because only that key can decrypt it.
- Digital signature
  The result of private key encryption is the digital signature. One of the major schemes is that data (message) is first hashed, and the hash sum is encrypted. A digital signature is attached to the original message and sent to the receiver that uses the relevant public key to decrypt the digital signature and compare hash sums: the decrypted one with the hash, which is retrieved from the original message. If they match, the verifier concludes the digital signature is valid.
- Cryptocurrency address (or blockchain address)
  An address that is exclusively generated from a user's public key. It is an address where cryptocurrency, tokens, and smart contracts are attached to but also is a user's digital identity.

II. The concept

The first subsection briefly outlines the concept. The next subsections provide detailed explanations and arguments to support the concept.

2.1 Outline

In accordance with the proposing concept, the blockchain serves as a decentralized, immutable public repository of records for land titles and other property rights. It is not only a secure database but a system for managing ownership because this is an inherent feature of the technology. With the DLT, users may directly manage their property performing peer-to-peer (P2P) transactions.

Tokens are blockchain-based records that represent the title and other property rights. A token is a unit of account, and it is connected with the user's address. Exclusive control over the address is enabled by the user's private key.

The token is technologically connected with the cadastral data (geo-data) and property rights, including leases, mortgages, superficies, and other encumbrances and liens. The connection of title records with real estate and property rights is ensured by relevant blockchain records done by trusted third parties who have the authority to certify ownership, deeds, and other transactions with property rights.

Smart contracts are the driving mechanism for managing ownership. Smart contracts[1] are an integral part of blockchain transactions. The blockchain transaction can be considered as the equivalent of a legal deed. The token record is always a result of a blockchain transaction: starting from the creation of the token to its various transfers (title deeds, smart contracts with property rights, etc.) and eventually deactivating the token in case if it ceases to represent any value.

Tokens are distinguished from cryptocurrency. The latter does not represent any particular property, and it is a value itself, as it is a drive gear for transactions because users pay coins as fees for transactions. More generally, cryptocurrency is a motivation for miners who create and maintain a blockchain network infrastructure and ensure the security of the system.

Tokens, in accordance with this concept, are titles in a digital form. Though title tokens themselves create a basis for various derivative tokens, which are not titles but are connected with them and create different property relationships of economic entities, including new forms of economic activities, i.e., ICOs[2], IEO[3], DAO[4], etc.

When the land title and property rights are tokenized, there is no need to keep this kind of records elsewhere, for example, in a traditional land (cadaster) registry, because blockchain is a registry itself. The procedure of tokenization will require initial interaction with land authorities, but once the title is on the blockchain, there is no need to perform registration each time a transaction is completed – the blockchain serves as a secure repository, where none transaction can be revoked or altered.

To address legal problems of the immutability of records on DLT, a specific technology – Cross-Blockchain Protocol – is applied. The protocol accommodates a framework for "smart laws." Smart laws are designed to address issues of inheritance, dispute resolution, restore access to tokens when keys are lost, and all

1 "Smart contract" is understood here in a broad sense as per the author of this concept, not as Ethereum smart contracts, i.e. "A smart contract is a computerized transaction protocol that executes the terms of a contract" (Szabo, 1994).

2 Initial Coin Offering

3 Initial Exchange Offering

4 Decentralized Autonomous Organization

other possible issues with enforcement that also involves various trusted third parties, i.e. "Digital Authorities."

Citizens gain the right to choose between the existing technologies. The government provides for procedures to transfer title records from paper-based or electronic databases to blockchains and vice versa.

The cross-blockchain protocol enables the use of multiple blockchains in the bundle. Users freely choose which blockchain to use for managing their property rights, which incentivize technologies to compete for users, improving their quality.

The role of a government is to provide for smart laws, technical standards. Rather than providing services of land registration and keeping registries, the public administration establishes regulations and digitizes them in the form of smart laws. The work of a cross-blockchain database (registry) is ensured by security standards, defined by the government. Those blockchains which ensure immutable and decentralized public ledger may work in the property registry bundle.

2.2 Why change the system?

Before addressing details of the concept, let us consider the prerequisites for this discussion. Why may stakeholders be interested in considering the shift from the old-fashioned centralized database to public ledgers?

Many countries use electronic cadastral systems for years, but at the same time, they still heavily rely on paper transactions. As a matter of fact, none of the countries enabled electronic peer-to-peer transactions with title rights yet.

Even though in such registries title rights and property rights are recorded in electronic form, these records are secondary and subsequent towards the transactions that happen in the paper form. Parties perform the typical deal as a [paper] title deed, which the land authorities acknowledge and record in the electronic database, i.e., land, cadastral, or real estate registry (or whatever it is called in different countries).

Nevertheless, it is important to admit that a few countries, for example, the United Kingdom, Australia, Canada, and New Zealand, are closer to electronic transactions (Christensen, 2004). They have systems of so-called electronic lodgment. An authorized person, i.e., a lawyer, a law firm, or a title company, may submit online an e-deed to the land authority. Thus, the parties of the contract are still detached from peer-to-peer interaction and may perform an electronic deed only through these intermediaries.

Acknowledgment and registration of deed and/or transactions with property rights (lease, superficies, emphyteusis, mortgage, lien, and other rights and en-

cumbrances) is an important role of the government and law in the protection of property rights. The involvement of the third party, be it a government agency directly, or those whom the government authorizes (a notary public, a title agent, etc.) is a "necessary evil." The transaction without intermediaries would look like scenes from gangster movies. Parties meet in person; the buyer shows the money, the seller shows the "product." Moreover, the intermediary performs an archive function, that is, keeps the record of the legal fact that happened with the estate and the bundle of rights, providing independent evidence if a legal dispute arises.

Two categories of land registration systems exist: registration of deeds and registration of title (Hanstad, 1998). As the earlier research (Konashevych, 2020a) defines, different countries have their specifics of the registration of deeds and titles, and two bureaucratic procedures – acknowledgment and registration – are usually present, in one or other form, with one or another intermediary.

For example, in the U.S. is widespread *registration of deeds* (27 V.S.A. § 342, The Vermont Statutes, n.d.[5]). Therefore, to check who is the lawful owner of the title, there must be a valid chain of registered deeds (27 V.S.A. § 601, The Vermont Statutes, n.d.).

Torrens[6] system, Australia and some other countries (Hepburn, 2018), and the majority of civil law countries use the system of *registration of titles* (*European Land Registry Association: Description of land registration systems*, no date), and some of the states in the U.S. (Rood, 1914). The cadastral[7] land identifier (cadastral number) is connected to the record of the current owner of the title. As to the form of the electronic database, this difference can be illustrated in Fig. 1:

5 Vermont state is arbitrary chosen as an example, though some states have registration of titles, not deeds.

6 This system was first introduced in Australia, in 1858, by Sir Robert Torrens.

7 As Hanstad defines, a "cadastre" is a systematically organized database of property data within a certain jurisdiction (Hanstad, 1998).

Electronic table of the title registry

Title ID* (cadastral number)	Owner
000489:9090:23	Alice (Inheritance)
000489:9090:23	Bob (Title Deed)
000489:9090:23	Charlie (Title Deed)

Electronic table of the deed registry

Deed ID*	Subject of the transaction
898-09	Alice inherits from... (Will)
778-0-09-2001	Alice (the landlord based on 898-09) conveys to Bob (Title Deed)
89334-0001	Bob (based on 778-0-09-2001) coveys to Charlie (Title Deed)

Fig. 1: Comparison of a title centric registry and deed centric. The title registry keeps Title IDs as the keys of the registry, while the registry of deeds traces the legal acts (deeds) as the registry keys.

In many countries, a notary public must acknowledge a contract with immovable property. The requirement of acknowledgment may exist in other forms and roles. For example, the town clerk or master in Vermont state (U.S.) performs this job (27 V.S.A. § 341, The Vermont Statutes, n.d.).

Apparently, there is a great role of the government and intermediaries who are either authorized by the government or licensed to conduct professional services for landlords and interested parties. All this infrastructure of regulations, authorities, and intermediaries is called to establish certainty in "who owns what."

However, centralization is a source of risks of data loss, corruption, and abuse of power. Inevitably, from time to time, it leads to conflicts of a different scale. Specifically, for information systems, centralization means control over the database, which is a single point of failure. The maintenance of such a system is costly and difficult. This is one of the reasons why citizens do not interact online, performing peer-to-peer transactions with the government database. When there is a chance of losing or corrupting critical data, the government chooses to be on the safe side by restricting any direct interaction.

It is important to define that the blockchain is a decentralized technology that ensures the ledger to remain immutable. "Permissioned" and "private" DLTs are centralized and the state of their ledgers rely on the will of a trusted third party that runs and controls the network. Thus, such systems are not discussed and considered applicable in this concept, as they are not different in principle from those databases of public registries which government runs for decades around the world.

Let us summarize the possible *benefits* of introducing blockchain technology:

1. It addresses the problem of a single point of failure for a public registry (Krogsbøll et al., 2020). Corruption of data is practically impossible.
2. It provides for infrastructure for peer-to-peer legal relationships of landlords and interested parties with no or minimum involvement of third parties, including public servants (Konashevych, 2018). Algorithms, not people, serve to manage property rights. Inevitably it cuts spent time and transaction costs for business and expenses on public administration. Eventually, it makes transactions with property rights transboundary and inevitably activates the economy.

As it then will be shown, even those governments that are not willing at the moment to make a shift to peer-to-peer transactions (*benefit 2*), they may also choose to introduce a cross-blockchain infrastructure with smart laws. They will obtain a peer-to-peer ready infrastructure, which they may use to gradually step-by-step decentralize the domain. While staying with the centralized infrastructure, any project each time will bump against its constraints.

Keeping this in mind, let us discuss how this can happen.

2.3 In-depth of technology, law and governance

In this subsection, it is discussed the technological, legal, and economic nature of a token.

2.3.1 A Token Technology

In Distributed Ledger Technology, a token is a record in the ledger owned by the user via the mechanism of public-key cryptography.

The token is distinguished from cryptocurrency. Usually, it is based on cryptocurrency. To create the token, the user must spend ("burn") some coins and apply scripts depending on technology. Cryptocurrency is spent as well to make further transactions with tokens. For instance, in Ethereum, Ether coins needed to pay for "gas" to run a transaction with a smart contract (*Ethereum Wiki*, 2017). Hence, in such systems, tokens do not exist without cryptocurrency.

In the industry and theory, users may find another interpretation of the token. Sometimes cryptocurrency is also called tokens. At least there is one DLT, i.e., EOS, which initially does not have any native cryptocurrency, and tokens are created without spending coins (*EOS.WIKI*, no date).

In this variety of technologies, it is necessary to define major features which are common and may be useful for title rights.

Creation. — Even though tokens and cryptocurrency have a mechanism of ownership via the user's private key, they distinguished based on the way they are created:

- *coins* are created in the result of the competition of independent nodes in the network which use a mathematical protocol that insures an extent of the unpredictability (Konashevych, 2020a) of which node gains the right in the creation of the next block[8], and not the user, but the protocol defines the number of coins the node can get for the block when wins the mining race, while
- *tokens* can be arbitrarily created by any user, and the fact of the creation does not depend on the network's consensus. Nevertheless, the consensus plays here a crucial role in maintaining the ledger, where such tokens are stored.

Value. — Cryptocurrency and Tokens have different economic nature that creates their values:

- Cryptocurrency does not represent any property rights, and it is value itself as it reflects the result of a collective work and material expenses that miners spend in competition to create cryptocurrency. It is a value because such interaction results in the creation of the network infrastructure. While in centralized systems, the owner is responsible for maintaining IT infrastructure, blockchain is a decentralized, self-organized, and self-governed infrastructure (Allessie *et al.*, 2019), and while it is so, the ledger is immutable, all data including transactions and inserted user's arbitrary data remains safe. Thus, the immutability of the ledger is the *value* of cryptocurrency. This is the first building block of the tokenization – the use of a decentralized system.
- Having the same advantage of being protected by an immutable ledger, the user defines the value of a token. The token as technology is a carrier for data (information) that can represent some property rights, which is discussed in the next subsection. Thus, the token value in its economic values (property rights) that stand behind the token.

In legislations and academic literature, there are a few definitions that may be helpful for a better understanding of the nature of this technology.

Malta was among the first countries to define in their legislation the notion of a token. As per the island's law (*Malta Virtual Financial Assets Act*, 2018), "virtual

8 Often it is called "mining," however, it is also known in different systems as "staking," "minting," "forging," etc.

token" means *"a form of digital medium recordation that has no utility, value or application outside of the DLT platform on which it was issued and may only be redeemed for funds on such platform directly by the issuer of such DLT asset."* The legislative act distinguished tokens from electronic money.

Lichtenstein introduced their vision on what is token (*Liechtenstein Blockchain Act*, 2019), which is *"a piece of information on a TT System [DLT] which can represent claims or rights of memberships against a person, rights to property or other absolute or relative rights; and is assigned to one or more TT Identifiers (addresses)."*

In academic legal literature, tokens are defined as "cryptographically-secured coupons which embody a bundle of rights and obligations" (Hacker and Thomale, 2018).

In Economics, Potts et al. emphasize the distinction of ownership and possession, using the following example. Possession of a banknote *token* indicates ownership. In the nineteenth century, the possessor — 'bearer' — of a banknote had a right to draw on the issuing bank the value of the note. These banknotes were direct liabilities for the issuing bank and were recorded on the banks' ledger (Berg, Davidson and Potts, 2019).

Three types of tokens. — It is defined at least three groups of tokens from the perspective of the technology:

- **Colored Coins** (Mizrahi, no date), which are the earliest way to utilize Bitcoin and similar systems. To create tokens, users must apply some standard features of the protocol, i.e. "burn" some coins and publish a transaction by applying some variety of built-in protocol scripts. In the transaction the user inserts some data that defines a new instance of coins that are marked and distinguished from the cryptocurrency. The embedded data being immutable allows creating some economic logic around it using transactions and the mechanism of ownership in blockchain. Such tokens are an *overlaid technology* because initially, the blockchain protocol did not have dedicated elements of the token technology. The software that has a mechanism to insert and interpret data is built as a complementary part of a core wallet. For instance, the user may create "Redcoins" on Bitcoin, which represents some property rights, while users of Bitcoin standard wallet will not know what these records mean. The community which gathered around the relationships around Redcoins will have their custom software which they use based on their *social consensus* (agreement) and build economic relations around it.
- **Name-Value Storage** is another type of *overlaid technology*, designed by Namecoin (2014) (Loibl, 2014) and improved by Emercoin (2015) (*Emercoin NVS – Emercoin Community Documentation*, no date); the insertion of data in the blockchain is provided in a structured form as a key-value record. Such an

entry becomes a container where the user inserts an arbitrary data of two elements: a "key," that is a short string that must be unique within the database; and a "value" which is the user's data (message) which is attached to such key. The technology provides for the functionality of a standard database, i.e., CRUD[9]. Inserted data in the blockchain, of course, cannot be altered, instead, to update an entry, the user publishes the same key using the same cryptocurrency address but with an updated "value," or a command to delete or transfer this entry to another address (owner). The NVS protocol hooks such commands and performs changes of the token status in the overlaid database. Because blockchain has a native mechanism of timestamps, the last record can be considered as the one which reflects the current state of affairs, that is why this database is decentralized – no one keeps the current state, only the user may manage entries through the mechanism of private keys and data insertion into the blockchain. The NVS protocol was initially designed to make possible independent maintenance of the same copy of the key-value database across all nodes in the network. This method allows one to have an irrevocable history of changes but dynamically manage the current status. NVS can be considered as a token, which is not necessarily a unit of account. One user may create many NVS records that all have unique keys. If someone owns the record "MyPropertyID," no one may own it within the blockchain NVS. Both, the variety of colored coin technologies and the NVS technology complement each other in terms of creating units of account and data insertion to develop economic and legal relationships around these technologies.

– **Tokens based on smart contracts**, at first, this notion was attributed to Ethereum (*Ethereum Wiki*, 2017). This technology introduced the blockchain protocol that contains a native mechanism for creating so-called "smart contracts." Smart contract is an executable software code that the user inserts in the blockchain via a cryptocurrency transaction. Tokens are created by deploying a smart contract. Number of tokens, conditions, and features are defined in the smart contract and cannot be arbitrarily changed on the run due to the immutability of the ledger. Smart contract-based tokens have the same mechanism of ownership via public-key cryptography, and therefore, can be an object of economic relationships.

9 CRUD, an acronym that means create, read, update and delete, i.e., four standard features of a full database.

Fig. 2 presents a summary of the types of token technologies.

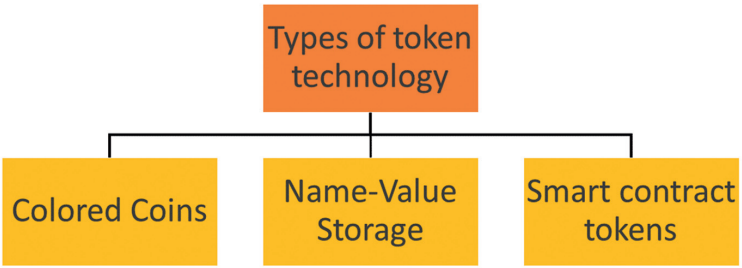


Fig. 2: Types of token technology: Colored Coins, Name-Value Storage, Smart contract tokens

Tokens, which are designed as units of account, can represent fractional property rights. An integer or a key-value token will usually represent a full title right, i.e., one unique token equals full title right, while decimals may represent fractionalized ownership, i.e., Alice and Bob own 0.5 of tokens each. Alternatively, a mechanism of multi-signature, where a transaction requires more than one private key, may be used to manage joint ownership. Though in some protocols (usually Bitcoin-similar), the number of parties that can participate in a token transaction is limited to the limit of the block size (the transaction which does not fit the block limit will not be accepted).

Data insertion. — Data insertion is the fundamental feature of blockchain technology beyond the cryptocurrency. Many methods and protocols support this service. Mainly the insertion of data is related to the transactions, which requires spending of some coins. Publishing a smart contract is also a kind of data insertion. The amount of data is usually limited by the protocol or economically by fees, which increases with the size of the message which the user wants to publish. There are two methods of utilizing this feature.

The research in blockchain data insertion (Konashevych, 2019) argues two ways of publishing data: publish some information, which has some explicit meaning for the user – a message, a file, etc. or to anchor data. The latter does not protect the data itself but, for example, anchor a hash sum of data, and some metadata helps to verify the authenticity of the data. Hence, an end-user must decide, whether they want to make data public but secure, or keep it private on a personal device or a third-party server and use blockchain to detect the corruption of this data. But it is important to notice, in the case of data forgery or loss, the blockchain does not anyhow help to recover it, because the hash sum is a one-way function.

In Fig 3, it is proposed two basic schemes for storing public data and private.

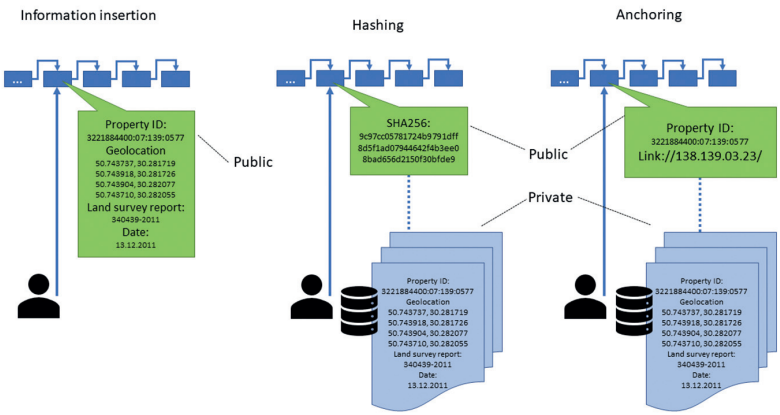


Fig 3: How to store data on blockchain. "Information insertion" – store a record in the blockchain, "Hashing" – store hash sum of a record, "Anchoring" – store some metadata of a record

Ownership. — The token is distinguished from a record, say, in spreadsheet or any other database entry, by having an independent mechanism of ownership, where users can exclusively possess the record and transfer it using their private key. In multi-access databases, there can be an individual mechanism for users to manage their records, but it will always depend on the administrator, who grants and manages accesses. Public-key cryptography is the fundamental element of any DLT. The public key is used to generate a blockchain address ('Bitcoin address · Programming The Blockchain in C#', no date). The user applies his/her relevant private key to digitally sign a transaction. Nodes, to include the transaction in the blockchain, verify digital signature whether it corresponds with the address (public key) from which the user is trying to spend coins.

Thus, the public and private keys are a mechanism of digital identity and authentication, respectively. Randpay technology (Konashevych and Khovayko, 2020) can also be used here to perform mutual authentication of the transaction. This technology was designed for microtransactions; however, within the set of tools, the technology introduced at the level of the blockchain protocol a mechanism which also requires a digital signature of the receiver to accept the incoming transaction[10]. This feature is important to address legal issues. For example, some jurisdictions may require explicit consent to receive a gift.

10 To note, Randpay does not require the recipient to spend any coin.

Let us summarize what makes a token applicable for property relationships, and specifically for land titles.

A token is an object of ownership and a carrier for information on property rights. Users create, update, delete tokens and transfer them within the blockchain via mechanism of public-key cryptography. A token is attached to a user's address, where the address is a representation of a user's public key, and only the relevant private key can be applied to sign a transaction—tokens altered (transferred, updated, deleted, etc.) via blockchain transactions. Tokens are distinguished from cryptocurrency. The latter is used as fees for transactions and "gas" for smart contracts.

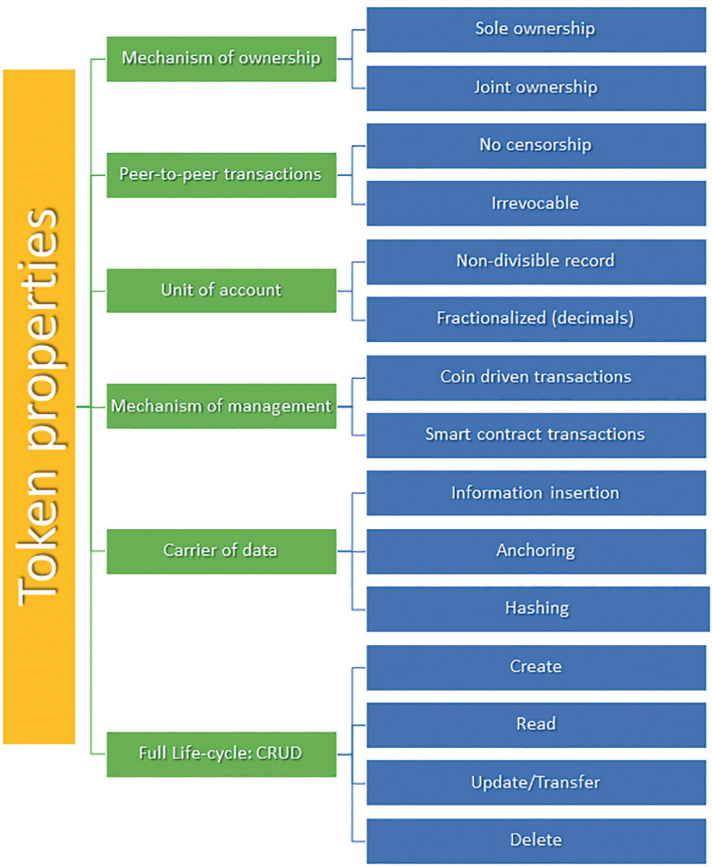


Fig. 4: Token properties

Tokens in blockchain represent two types of information: who owns it, that is to which address it is recorded, and the chain of transactions. Because blockchain is public, immutable, and chronological, the history of transactions is natively available in the ledger, creating a traceable sequence of transactions. Fractional ownership is possible via decimal units of account and/or multi-signature schemes.

2.3.2 Legal Side of a Token

As seen in the previous subsection, tokens on DLT fit the purposes of ownership having a native mechanism for managing property rights via P2P transactions.

Blockchain carries both types of information:

- the token (i.e., title) is attached to the address (owner) that corresponds with the *title registration* procedure; but
- the token is always the result of a transaction, a subsequent transaction refers and inherits the previous. Thus, the *chain of deeds* is also available as a way of representing the land registry database.

We infer that the blockchain technology has a dichotomous nature that corresponds with both *title*- and *deed*-centric ways of registration (presented in Subsection 2.2 and Fig 1). Hence, it fits both conventional systems of keeping records in a public registry as a chain of deeds (U.S.) and maintaining the registry of title records (Torrens system, civil law countries), where the latest entry reflects the title and its current owner (see Fig. 5).

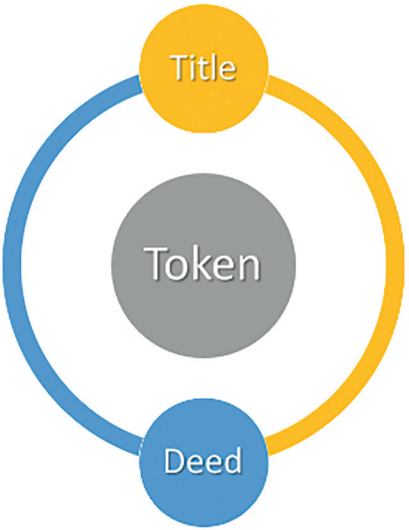


Fig. 5: Dichotomous nature of a token. Token is evidence of a property right, which is an equivalent of the concept of a title. A token is a result of a transaction, which is an equivalent of the concept of a deed.

2.3.3 How does a token become a title?

A short definition of a title – it is evidence of ownership (Cushman, 1937), (*Systems Of Ownership And Registration*, no date). It is commonly known as a theoretical legal concept. The title does not always exist as a single legal act but rather a combination of different legal documents: certificate of ownership, a title deed, or even a court decision. Together various legal acts may constitute a title (evidence of ownership). As it was earlier specified in the Torrens system and civil law countries, governments maintain *land title* registries. Typically, the title's identifying element is a cadastral number. The U.S. and many other countries keep registries of deeds, so by identifying the chain of deeds, it is possible to define who is the current title owner.

The title represents the property. It points to the object of ownership – a plot of land, and everything which is attached to it, i.e., buildings, constructions, etc. The title is attributed to the cadastral (geographical) information of a land plot, i.e., geolocation, distances, and other measures, which is usually collected in one document – a survey report (Hanstad, 1998).

In the previous subsection, we described a mechanism of data insertion; in this way, a token becomes a record that has legal meaning and hence an econom-

ic value. To add to a token some legal properties, such data should answer the question of what property rights does this token represent.

There are two ways to legitimize any immovable property, and attributed rights and obligations: (1) by declaration and agreement of private parties, and (2) by public acknowledgment.

This is also relevant to any movable property title, especially that is subject to registration: cars, boats, aircraft, and also to corporate rights. However, it is not always relevant to securities, though, as you will see the security tokens as which are connected with title rights can also work together.

The user creates 10.000 tokens and writes that this token represents their flock of sheep of that amount. When such an owner sells any number of tokens, they transfer the ownership to the relevant number of sheep. The buyer of tokens in this transfer accepts the owner's declaration (that tokens are equal to sheep), believing that such a farmer did not create other tokens that represent the same flock. Thus, such tokens have a contractual nature and do not involve any trusted third party.

If the buyer does want to rely on the seller's honesty and wants more certainty, especially if the purchase is remote, the buyer may ask a trusted third party to certify the fact that these tokens represent the property. In real estate, the government plays the role of that third party, i.e., land and other authorities. The scheme of certification of records is presented in Fig 6.

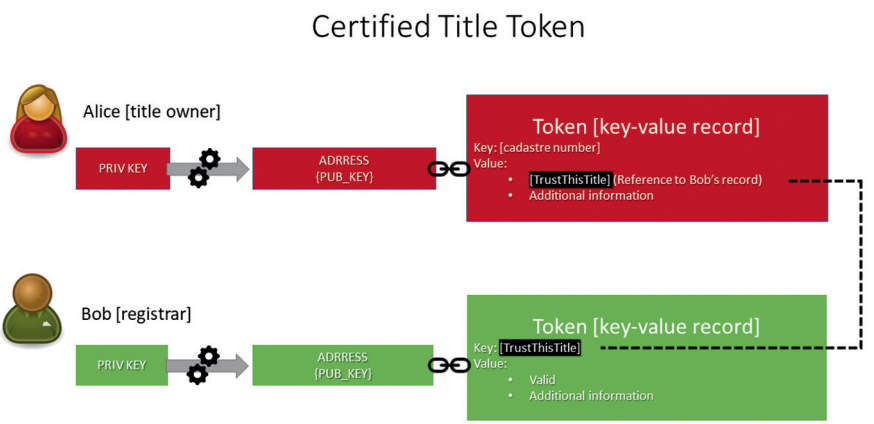
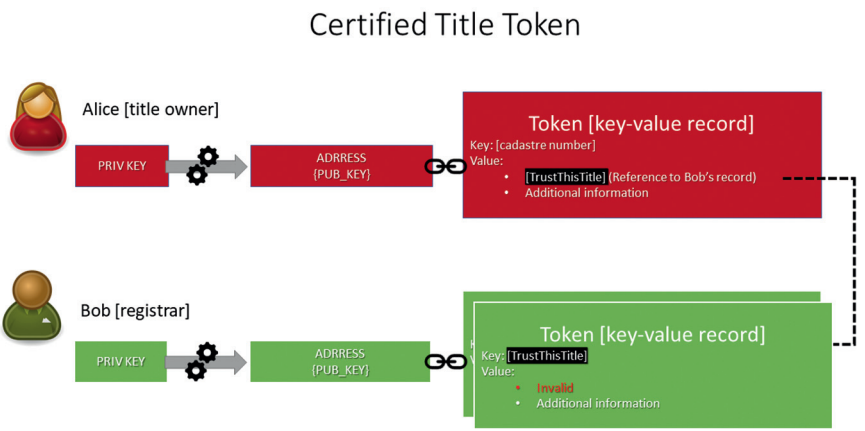


Fig. 6: Title Token certified by Registrar's Token. Alice creates a token where the key is the title cadastral number (unique key), and value is a reference to Bob's token. Bob creates a token with the key, which Alice included in her token as the reference. Bob adds in the field "Value" the record of status of Alice's token ("valid").

The owner creates a record where they declare a title. The land authority creates another record where they certify the owner's rights. The reference in the owner's record links to the certifying record, providing an exclusive connection between these records (See technical details of the protocol in Annex).

The one who searches in the blockchain the information about the title retrieves the link to the land authority's record and follows it to get the information of its validity. If the owner lost the private key, hence cannot dispose of the property, they may ask the authority to update their record, so the one who enquires the status will see that the token became invalid at some point in time (See Fig. 7). Such an update will include certification and link to a new title record re-issued to reinstate the ownership.



See Fig. 7: Invalidated Title Token. Bob updates his token by adding a new status ("invalid") in the field "Value." Bob's record certifies Alice's token.

Both the owner and the authority independently manage their records. The title owner controls his/her token, having full control over it and ability to perform peer-to-peer transactions. The government, on the other hand, having their token under control, has an obligation to govern relationships as per the law. The link to the authority's record ensures enforceability. If the parties have a dispute, the land authority will be able to execute a court's decision. Transactions that the government commits are recorded in the blockchain; hence they are irrevocable and accountable.

The above level of the system protocol is smart laws that enable governance. If any government agency loses its access to the system, another government branch/body patches the cross-blockchain protocol or reset it or reinstate the access, which is further discussed.

Due to such interaction with the government, the owner may split the title into two and more land plots, or merge plots into one land title. And therefore, new title records will be created instead. If the property ceases to exist, the owner or the authority performs the transaction that marks the token liquidated.

2.3.4 Acknowledgment, registration and authorization

The owner has freedom of action with the token. Only the private key is necessary to perform a transaction. Once the token is certified, there is no need to perform a registration as it happens with the centralized land registry each time the transaction is performed (See Fig. 8).

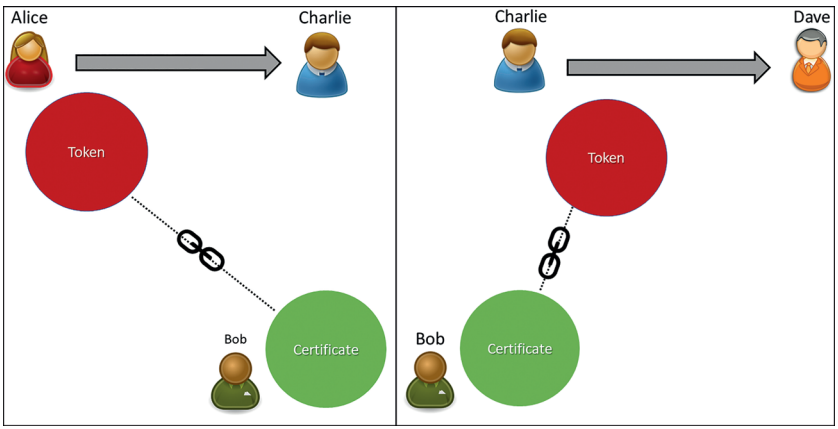


Fig. 8: Title Token transfer. Alice transfers her token to Charlie. Then Charlie transfers Dave. In both cases, Bob initially certified the token; this connection remains in all subsequent transactions. There is no need to register a deed because blockchain is the registry.

Though some jurisdictions may require an authorization from the government for title conveyance and other property disposition, for example, consent of the local community for land sale, architecture and planning permit for (re)constructing a building, mandatory valuation in various cases, or acknowledgment by a notary public.

All these cases are also covered by the proposed schema of linked records on blockchain. The authorizing body, be it a building inspector, or a notary public, create their token and insert/anchor data of their legal act. The owner to perform a compliant deed obtains the permission and includes it in the title token record. The basic scheme is presented in Fig. 9, some other methods are shown in Annex.

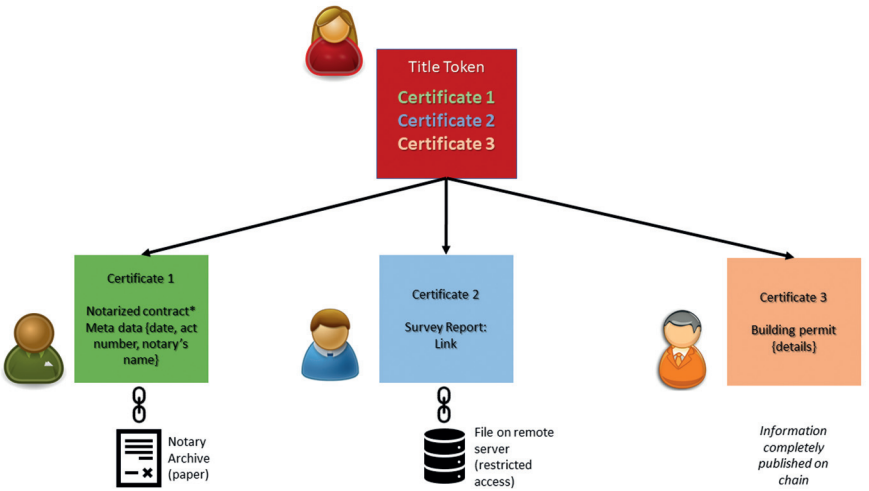


Fig. 9: Title token transaction authorized by multiple bodies. Notary acts may be performed in a rudimentary form (paper); thus, the notary publishes the token that declared that the act had been performed, token contains metadata of the act. The survey report may be published on the blockchain or included as the link to the file (by anchoring and/or hashing) on a remote server with public or restricted access. Building permits similar to the survey may be published on the blockchain or stored on a third-party server.

2.3.5 Bundle of rights and mathematical model

There is no uniform and generally accepted classification of real property rights in the world. For example, the big study "Real Property Law and Procedure in the European Union" (Schmid and Hertel, 2005) showed there is no unity neither at theoretical level nor legislative. Nevertheless, the report distinguished common grounds. The report specifies *"full ownership rights and limited (subordinate) rights on the land of another person such as rights to use (e.g., usufruct, servitudes, habitation rights, trust life rents in England and Scotland, and different kinds of easements or, synonymously, servitudes) security rights interests (i.e., mortgages, liens, charges and rent charges), and pre-emption rights established by contract or statute (such as pre-emption rights in favor of local governments)."*

Immovable property, that is, buildings and constructions, is attached to the title. The title gives ground to a bundle of property rights, which includes landlord's rights, encumbrances, and rights of other interested parties, i.e., mortgage, lease, easement, etc. Various concepts of collective rights define sharing rights

with different owners, for example, an apartment in a multi-dwelling unit in some jurisdictions is known under the legal concept of "condominium," there are also such concepts as joint ownership, fractional property, marital property, etc.

Computer programs do not operate with theoretical concepts, so-called "dummy variables." Computers require numbers. There has never been a public request for a mathematical model of property rights yet. If such a model is to be created, it should be universal to fit different theoretical legal concepts.

However, for this level of discussion, it is defined three most common elements: the right to dispose of, the right to possess, and the right to use (enjoy), see Fig. 10. The ownership is defined as a bundle of these rights.

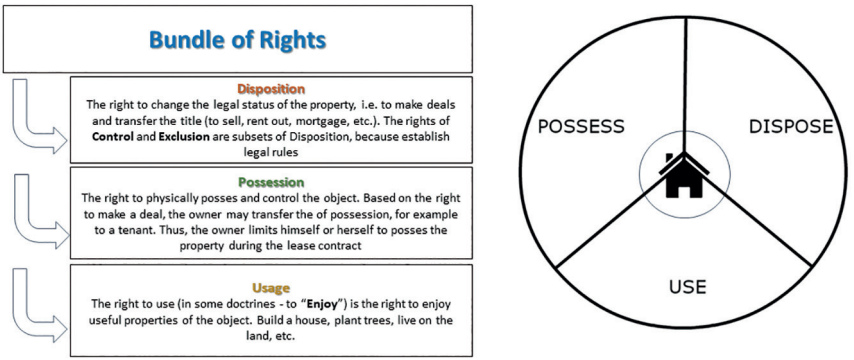


Fig. 10: Bundle of rights: to dispose of, to possess, to use (enjoy)

For instance, the title owner, based on the right to dispose of, may convey the title to another owner or perform a transaction with other rights. The owner may limit herself/himself to the rights. For example, during the lease contract, the landlord may not use the rented premises. The right to *use* and *possess* are temporarily transferred to the tenant. Moreover, the law may even restrict a new owner, i.e., this limit is transferred with the title while the lease contract is valid.

Information Science independently from legal issues of property rights developed a robust technology for managing rights on digital objects (files and folders), which may appear relevant to the bundle of rights.

Change mode or CHMOD developed in in AT&T Unix version 1 (Introduction to the Linux chmod command | Opensource.com, no date) and can be represented using this table (Fig. 11):

CHMOD

	Read	Write	Execute
Owner	4	2	1
Group	4	2	1
Public	4	2	1

Fig. 11: Change mode (CHMOD) scheme

File or folder properties consist of three elements of rights (read "4", execute "2", write "1") and actors who may possess these rights: owner, group, and public (all). For example, if the file is being attributed to code 777, it means each of the actors (owner, group, public) has full access (4+2+1 = 7).

In legal parlance, these elements might mean the following; Owner means title owner or landlord, and a group is anyone who is included in a legal act (contract, law, or court decision) as the beneficiary of any of the rights. A group may consist of one actor or multiple. There can be multiple groups towards one title. Public means all or anyone.

Any legal transaction can be represented as a mathematical code, where "read" will mean "possess," "execute" – "use," "write" – "dispose" (See Fig. 12).

CHMOD - Bundle of Rights

	Possess (Read)	Dispose (Write)	Use (Execute)
Owner	4	2	1
Third parties	4	2	1
Public	4	2	1

Fig. 12: CHMOD for a bundle of rights

If an agent is entitled to sell the land plot, in the Power of Attorney will be recorded the right of a group (the group includes only one actor, i.e. the "Agent") to write/dispose of. The agent is not granted the right to use the land, hence cannot live there or plant trees (read/possess, execute/use).

The tenant will be granted the right to (read/possess, execute/use). In a mortgage, the owner will be limited with the right to dispose of the land plot without a bank's permission while paying the loan. Therefore, the landlord is limited in the "write/dispose" having "0". See Fig. 13.

CHMOD - Bundle of Rights

	Possess (Read)	Dispose (Write)	Use (Execute)	CHMOD
Landlord	0	2	0	=2
Tenant	4	0	1	=5
Public	0	0	0	=0

Example
Lease: The right use and possess is granted to the tenant. The landlord is limited to use and possess during their lease contract, though may sell the land, because has the right to dispose of. A new title owner will inherit this limitation while the contract is valid.

Fig. 13: CHMOD record for lease. CHMOD 250. The right to use and possess is granted to the tenant (4+1=5). The landlord is limited to use and possess during their lease contract, though they may sell the land because they have the right to dispose of (2). A new title owner will inherit this limitation while the contract is valid.

The road will have records for the Public (All) to possess (read), which means to physically be present on the road and use (execute) to drive or walk. Paid tolls instead will ban Public (All) and require paying fees, so be included in the Group of customers of the paid toll.

The difference between "use" and "possess" is better illustrated on movable properties. The passenger may leave a bag in the luggage room. The stuff that stores luggage is temporarily granted with the right to possess the bag (physically control it). However, they do not have the right to use it.

When the house is temporarily transferred to the bank in a case of mortgage debt, the bank acquires the right to possess (read) the object, i.e., physically control it, but not to live use (execute) there.

The neighbors (Group) ask the court for the right to pass through someone's land, for example, to access the river, so-called "easement." The court will grant them the right to possess and use the road without consequences of trespass, while the Public (All) will not have this right.

CHMOD was initially designed in the Linux system and subsequently improved in Windows by introducing more specifics and usability: full control, modify, special permissions, granting to each element "allow" or "deny" property, see Fig. 14.

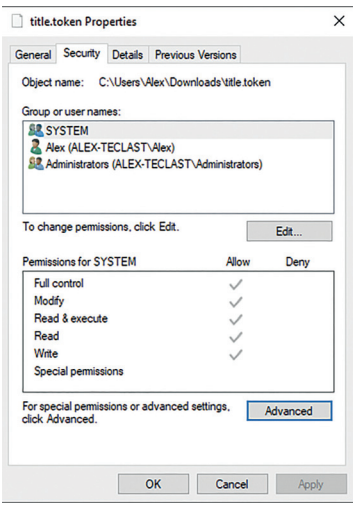


Fig. 14: Windows CHMOD

CHMOD and its variations are valuable experiences of managing property rights in the digital world, which should be considered in the tokenization of property rights.

2.3.6 Model Smart Contracts and Smart Laws

To better understand the role of smart contracts in token management, it is worth determining what smart contracts are not. The word "contract" may confuse readers, because in this case, it does not mean any verbal form. This is a machine code that exists in the form of algorithms that are written in a programming language. There is no human language; everything that is said in words and/or written has a secondary nature with respect to smart contracts. The smart contract described in words does not create any legal consequences; only algorithms create legal action and meaning.

The second difference is that the smart contract is not just a file. Sometimes electronic contracts include agreements in the form of a text file, and sometimes even its scanned hardcopy. The second distinguishing feature of a smart contract

in the blockchain is the mandatory presence of a transaction. A smart contract in the blockchain *is* always a transaction. Moreover, it always involves a crypto asset (coin, token, etc.).

Although transactions are not called smart contracts in Bitcoin, they are a kind of, at least, as per the one who invented this concept (Szabo, 1994). In Bitcoin, it is a scripting language that does not have Turing completeness, that is, significantly limited in possible actions compared to the Solidity language in Ethereum (Jansen *et al.*, 2020).

The logic of the transaction in the blockchain is always approximately the same: the user compiles the transaction code[11] using the allowed commands for the given blockchain protocol in which the user describes the "tasks" for the system, for instance, spend five coins from this address and transfer it to another address. And when the code is prepared, the user presents it to the network – the mempool – where the miners check and include it in their list of transactions for the future block. If a miner has acquired the right to publish the block, miner's system adds it to its chain and reports this to the other nodes in the network. Nodes verify the block and also include it in their copy of the chain. If in the previous transaction, it was written that the coin could not be alienated until block number 350, all nodes, when the user tries to spend this coin, will refuse to publish it. And if the transaction contained a multi-signature script, then a node will accept it after verifying the digital signatures of all participants in the transaction. These are all different smart contracts and their conditions.

There is a good practice of standardization of documents for legal transactions instead of creating new documents each time. For example, in 1990–2010, many European countries introduced a company's model charter and abolished mandatory notarization for registration of a company. A similar practice is observed in the U.S. and many other countries. Governments adopted the model charter, and instead of visiting a notary/lawyer, a businessperson applies a standard application form (nowadays, mostly online), where the person chooses such a charter. Surely, it does not cover 100 % needs; therefore, the option of developing a custom company charter is also available.

A model smart contract can be implemented in the following way. The government adopts a technical standard for different smart contracts: purchase, lease, mortgage, gift, emphyteusis, etc. The user may choose one of these, or develop themselves, or order professional services to create a custom smart con-

11 Of course, an ordinary user does compile code manually, but uses wallet interfaces with predefined functions

tract. Of course, some governments may introduce limits in custom development by licensing or prohibit it at all.

To perform a deed, that is a transfer of token from one address to another; there can be two scenarios:

- *lenient*, when the user choses to follow the standardized rules, if the user performs a non-compliant transaction, it will be automatically filtered out; hence, any transaction is possible, but not all will be recognized valid (legal); or
- *strict*, when the transaction will not be accepted by the system when it is incompliant.

Strict rules is a common practice in online services. For instance, registration on a forum: the field of a telephone number can be mandatory and checked against the standard country code. Unless the user addresses the requirement, they will not move forward. Similarly, the "smart laws" are digitized mandatory rules. Paper rules encoded into algorithms that assist users in staying in the legal field when they perform a transaction and do not allow turning in the wrong direction.

Even though model smart contracts may satisfy the vast majority of needs, it is almost impossible to address 100 % market demand in the variety of legal relationships. Therefore, the system should still offer traditional legal transactions. For those jurisdictions where acknowledgment of the contract is mandatory, they may involve a notary public (a town clerk, a title agent, etc.) that will acknowledge a paper deed and publish the record on the blockchain (See Fig. 9), which certifies the acknowledgment is duly performed. The landlord will include in the transaction the reference to the notary's token.

The next element of smart laws is enforceability. To examine this protocol at a more abstract level, let us assume all transactions which happen in the country, be they paper-based or electronic. The legislation is a set of rules. When we apply these rules to any transaction, it will either be compliant with the law or not. The proposed technology of a cross-blockchain protocol and a framework of smart laws we can imagine a set of filters. The government designs these requirements in algorithms to apply to blockchains. Transactions are filtered out if they do not comply. Those that are compliant will be collected in one public database. The database is a file, which any user can retrieve by installing and running a blockchain node complemented with the filter. The user's local wallet runs a full node, each new block is checked against these rules, and those transactions which satisfy algorithms are copied in the local database. This algorithm is proposed in the cross-blockchain protocol (Konashevych, 2020b).

Thus, not only the government but everyone keeps the same version of the public registry. The role of the government is to introduce smart laws with model transactions and filters.

It is essential to notice that public blockchains have no censorship. Even though the government applies a strict model, there is still a possibility for those who can code a blockchain transaction to design a non-compliant transaction and omit the smart law framework pushing such transactions directly into the blockchain. Here the filter plays a crucial role. It scans each new block, the non-compliant transaction will be published in the blockchain, but it will not be added to the overlaid database because of such filters. See the scheme of a three-layer system in Fig. 15.

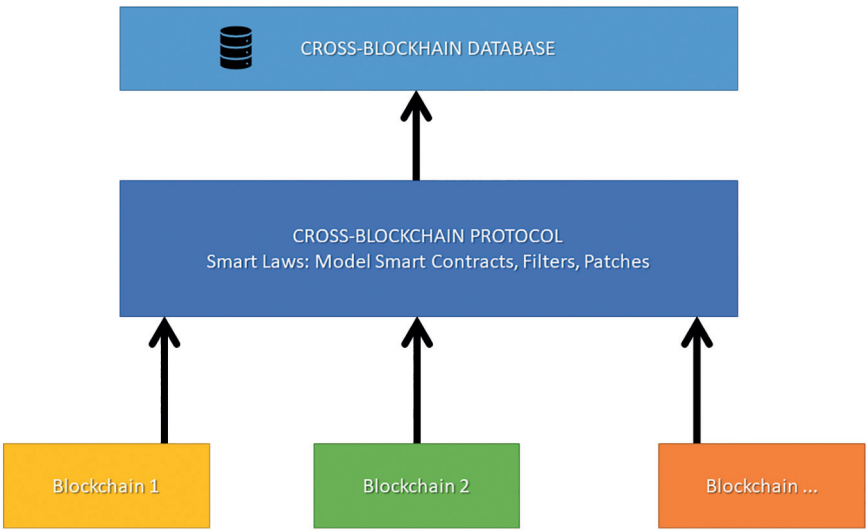


Fig. 15: Three layers of a smart law system. 1. Blockchains are public repositories with mechanisms of ownership and P2P transactions. 2. The Cross-blockchain protocol unites blockchains in the bundle and contains "filters," i.e., the rules which are applied to transactions when they are published, model smart contracts and patches. 3. The public registry is a database where resulting records are stored.

This filter makes possible reinstating power. As we mentioned, regular enforcement can be performed by updating those records (tokens) on the blockchain, which the government owns and controls using their private keys. They will provide the society knowledge which token is valid, and which is not. But if the private key is compromised, the government loses control. To address this, they patch the protocol, providing new filtering rules, new addresses that belong to the government agencies, or filter out the transactions which are not compliant.

The reader may argue. This technology is centralized: government, court, land authority, public notary, etc. First of all, we need to admit there can be no

fully decentralized system. There are many moments in our lives that we cannot resolve on our own. A person, for example, cannot certify his or her death to initiate inheritance transfer. The two parties need a third person to resolve their dispute. People need trusted third parties, be it a public servant, a notary public, or a judge.

However, this system is different because:

- retroactivity is impossible; neither the government nor the user may alter a transaction. Transactions serve society as evidence of everything that happens in the real world, be it legal or illegal. We do not rewrite transactions as it may occur in the centralized database, to fix any legal issue.
- the government bodies publish their decisions on the blockchain, so ledgers keep all transactions, including those which enforce and fix legal issues. When the government reinstates the access, they also do it in the form of a blockchain transaction.

Eventually, it is a matter of each citizen if they trust their government. And at this moment, it cannot be addressed by any mathematical consensus.

This is a social consensus, a social contract (Friend, 2004), in more conventional terms. Citizens delegate authority, and the government has the mandate of power. Of course, this is a political level of discussion. The paper has no aim to address the political structure of any state.

Instead, the protocol proposes a range of options, including voting on blockchain, collective (multisig) transactions, and other forms of governing the system. So, any system can be designed with regard to existing political traditions and forms of governance.

One remains stable, with highly reliable public blockchains, the society will be protected from corruption. The stability of the system is determined not just by the ability to withstand the threat, but to return to the correct state in the event of an attack. Even if the government abuses power and violates civil rights, the system can be reset by reindexing the blockchain from the very beginning and applying proper filters.

It is essential to note the reliability of blockchains. It is defined by the physical security of nodes and their owners and the right to free fair competition in producing blocks. Therefore, the police, antitrust bodies, and the judicial system is another crucial role of the government: not to allow cartels and any threatening activity against nodes and miners. Otherwise, in the worse scenario, miners will need to hire armies to protect their lives and interests.

2.3.6 Digital identity and Privacy

Being decentralized blockchain does not allow the deletion of data. Once anything is published, a transaction, and a user's data, it cannot be altered. It raises concerns about privacy. On the other hand, anonymous transactions veil unlawful activities, for instance, money laundering and financing terrorism.

If a transaction is anonymous, it creates uncertainty for the public in the case when the token owner seeks acknowledgment from the authority. How will the counterparty understand if the certifying record belongs to the land registry office or any other authorized person?

The concept of Public-Key Infrastructure (PKI) during decades has been equipped with various protocols and standards which are applicable to address these issues.

Conceptually PKI works as follows. Alice generates her private and public key. A private key is used to encrypt a message. As a result of this function, Alice receives a digital signature, which is a cryptographic representation of the message, and adds it to her message. The recipient of the message, Charlie, uses Alice's public key to decrypt the digital signature. If the message matches the original one, Charlie knows that it was Alice who signed it. The question is that how Charlie and any other counterparty knows if Alice's key was valid, i.e., was not stolen. For that reason, they involve a trusted third party, which is called Certificate Authority ('Digital Signature Standard (DSS)', 2013), and more specifically, in the EU – Trust Service Provider (TSP) (Council of the European Union, 2014).

The main role of Bob, who will be a CA/TSP in our hypothetical example, is to verify if the private key belongs to Alice. For that reason, more likely, Alice will initially visit Bob's office and show her ID. Bob will issue a certificate where he will include Alice's public key and write that her key is valid. Alice may want to add also personal or business details, i.e. her contact number, etc. Bob will sign this certificate (x.509 standard) using his private key and will publish it on his server.

Now, if anyone inquires about the validity of Alice's digital identity, they will find this certificate in Bob's server and check if it is valid or not. If Alice loses her key, she will ask Bob to update his certificate. So, if anyone inquires about its status, they will see that it is invalid from the specified date. If anyone stole the private key and signed the document, everybody will know that it happened after Alice's public key was announced invalid, and so will ignore the illegal transaction.

Conventional PKI scheme completely corresponds with the proposed model of certification of property rights on the blockchain. To create a digital identity, Alice will publish a token using her private key. In the token, she will specify who

is her CA/TSP, including the reference to Bob's certifying record on the blockchain. If Alice's key is compromised, Bob will update his token, where he will specify the reason for changes in Alice's digital identity.

The use of two independent tokens where one token certifies another has an advantage. Alice controls her token. This is her record, her digital identity. She may include whatever she wants: contact details, her picture, education records, recommendations, etc. If she initially included her telephone number and then changed it, she would perform an update transaction. But if she loses control over her identity, she will ask Bob to invalidate *his* record.

As a result of this scheme, Alice has one private key which she uses to sign transactions on the blockchain, including title tokens and other property rights. The key (by fact, her blockchain address) will be identified and verified by someone whom economic actors trust.

Who do we trust CA/TSP and know that Bob is Bob? This is the role of the government or self-organized community, to define the first trustable record(s). In PKI, the initial key that grants trust CA/TSP's is usually called the "root." This key is highly protected and used to reset trust in the system. Eventually, the government has the authority to reissue the root if it is also compromised. This model is relevant to digital identities and trust services on the blockchain. Some more details are provided in Annex.

The difference and the advantage of the blockchain towards the conventional PKI is that certificates are stored not on CA/TSPs' servers but on blockchain. The CA/TSP's server may also be in some sense public, but it will always be vulnerable to multiple risks, i.e., external attacks, like DDOS and MITM (Spies, 2013), or internal threats because Bob may corrupt any record on his server, or even disconnect the server at his discretion at any time from responding to inquiries.

On the contrary, the blockchain provides for 100 % uptime for public access; certificates are secured from unauthorized changes from anyone. If Bob acts maliciously, for example, marks Alice's certificate invalid, this action will also be stored on the blockchain. While in PKI, such forgery is almost impossible to detect (Spies, 2013). The previously described algorithms of smart laws will help to reinstate the trust in the system using patches, or even to reset the whole system.

Another advantage of the blockchain is that, on the contrary, the traditional PKI, it does not require a Time-Stamp Authority. This is another trust third party whose role is to provide a timestamp at the moment when the user signs the file. User's local machine time is not trustable as it can be manipulated. The blockchain addresses this issue without a dedicated third party because blockchain is a so-called "timestamping machine," transactions are chronologically stored in blocks and cannot be altered (Konashevych, 2020b).

To address the issues of privacy, there are various cryptographic methods and techniques. Instead of publishing names and other personal details, certificates contain hashes and other cryptographically protected data. Personal data itself should be stored off-chain under the user's control on the personal device or trusted third party server.

W3C in December 2019 introduced the first version of Decentralized Identifiers (DIDs) (Reed *et al.*, 2019). The framework and its best practices should be used in future title token systems to enhance privacy and usability.

2.3.7 Tokens Derivatives, ICOs and property rights

The ICO boom in 2016–18 raised many talks on the legal nature of tokens. First of all, many issued tokens had no mechanisms for inheritance transfer and even resolution of disputes. Why would investors trust any technology, which may jeopardize their interests? Once the owner loses control over the token, it becomes useless. To address these issues, some projects left backdoors in their smart contracts and dApps to manually resolve disputes. Why would anyone call such a project decentralized? These are just a few practical questions of the applicability of emerging technology.

However, more confusion arose during discussions on the legal nature of the token. Readers may find some discussions that tokens have a completely new legal nature in terms of property rights. This is something new that has never existed before.

Since there are no academic or any other grounded explanations of what new legal nature brings tokens, it is reasonable to support the conventional understanding of property rights.

Token is just a record on the blockchain; it has a native mechanism of user access and peer-to-peer transactions. Unless economic actors entitle a token with any legal property, it remains just an electronic record. That is why it is crucial to distinguish fraud. If during ICO the tokens are not supported with legally binding promises, that is, the issuer declares no obligation, and therefore the acquirer does not get any rights or interests now, or in the future, more likely people deal with fraud.

On the other hand, a token that is legally and technologically connected with property rights, be it a contractual based relationship or a law based to become a legitimate market tool.

The title token can become a basic record. It corresponds with the idea of F. De Soto (Soto, 2000), which argued the fundamental importance of land rights for economic growth and prosperity. Based on title tokens, the beneficiary may create derivative tokens and so tokenize various property rights and interests,

even those who probably were not even in the focus of economic interest before the invention of blockchain.

The farmer may tokenize his land, and grow fruits, which he also tokenizes. Tokens become a tradable asset giving the farmer direct access to the global market, which guarantees him a fair, competitive revenue. The relation with the title token provides buyer certainty in the origin of goods and their quality. Fruit tokens become a logistic instrument that provides for all members of the supply chain to the end customer a traceable history of transactions. Having a jar of jam bought in a local store, the customer will know this was initially grown by the farmer somewhere on the other part of the planet and came across the supply chain to the food producer.

2.3.8 The right to choose. How to reform

There are at least two options to implement the concept of land tokenization. First, is to abolish the existing model of public registries and introduce the proposed one. This way will require significant efforts to reform the existing and unlikely will be welcomed.

The alternative, even though it requires a reform, still may be adopted with less efforts. It is based on the idea of a free choice of how and where rights are registered. The right to choose means that a landlord decides where he or she wants to manage their property rights, that is, in the conventional public registry or transfer the title to the blockchain and use smart contracts. The landlord may transfer it back for any reason.

To make this happen, the government must ensure at least two things: recognize the legal right to choose and adopt regulations.

Of course, these are added to the previously mentioned obligation of the government to develop cross-blockchain infrastructure, ensure high-security standards, smart laws, and model smart contracts.

The advantage of this approach is that it allows gradual implementation.

The government may not enable free development of custom smart contracts. But introduce only a few model smart contracts. For example, purchase, smart will, mortgage, and the lease will cover a vast majority of market needs.

The government may not abolish mandatory notarization or other forms of deed acknowledgment. Moreover, the notary may use paper notarization and reflect only the fact of an accomplished notarial act in the token, the same as in many countries of Latin notary they acknowledge paper deeds but register them in a public electronic notary database. Blockchain, in this case, will be that electronic database.

The process of tokenization may look as follows. The landlord creates their digital identity as per the officially recognized procedure, which involves CA/TSP. Then the landlord will create a token and apply their intention to the land authority. The land authority will issue a record, where they specify the token ID as a valid representation of the title and mark in their registry that this title is not maintained by the centralized database anymore, including the link to the title record on the blockchain. From this moment, the landlord may perform peer-to-peer deeds using model smart contracts or other deeds involving third parties that are authorized to acknowledge the deed. The landlord may deploy the smart will; however, it will require beneficiaries to create their digital identities. The landlord may borrow money and mortgage the house using the specific smart contract. The smart contact ensures that if the landlord does not return the money, the creditor will acquire the title token to initiate the auction. The proceeds will be spent to close the debt.

III. Conclusion

Blockchain is an immutable public repository. The immutability of the ledger is achieved by the decentralized interaction of peers based on their social contract and mathematical protocol. Blockchain is distinguished from other DLTs with centralized governance, where the state of the ledger relies on the will of a defined actor.

Users can apply blockchain public repositories to create tokens and insert arbitrary data. Blockchain provides for a mechanism of ownership over tokens, inserted data, and smart contracts through public-key cryptography, where user's private key is used to sign (authenticate) transactions.

A token is a unit of account and a container for user's information. Tokens are managed through coin transactions and smart contracts, i.e., read, update, transfer, or delete data. This functionality is achieved through the chronological nature of transactions stored in the chain of blocks. Users cannot change or delete data in the blockchain but can agree to consider that the latest record represents the current state of affairs. Therefore, immutability does not create legal problems with enforceability; it is the most important advantage: all records, if they are legal or not, valid or not, are stored in the ledger. Blockchain is a repository of evidence; that is, everything that happens with property rights in the real world is recorded and then interpreted by the technology of the cross-blockchain protocol and the framework of smart laws.

All this gives ground for the tokenization of land rights and other property rights. Users create tokens that represent their title rights. Trusted third parties are

needed to certify legal facts, which normally, users cannot do themselves, i.e., birth, death, notary acts, etc. A trusted party here is a broad notion. It can be a land authority, a certificate authority or a trusted service provider (for digital identity), a notary public, a court, a surveyor, etc.

The trusted third party creates their token that specifies some legal facts about the user's token. Therefore, the user's token is linked to the token of the trusted third party. This ensures enforceability. If the user lost control over the token, they ask the trusted party to update their token, where they specify that the user's token is not valid anymore. Similarly, they resolve disputes and address any other legal issues.

The system of referenced tokens is governed by smart laws that consist of model smart contracts, filters, and a mechanism of patching. The property registry is a superstructure over a bundle of blockchains. While the level of blockchains as public repositories contains all possible transactions (valid and invalid, legal and illegal), the overlaid database reflects the current state of the registry based on filters. Invalid transactions are filtered out. Therefore, filters are something that is called laws and jurisdiction.

Thus, smart laws are digitized rules, which in the form of algorithms allows users to define which transaction is legal (valid) or illegal (invalid). Model smart contracts provide for better usability. The transaction which is performed as per the model smart contract is considered valid by default.

If a registrar or any other a trusted third-party loses control over their private key, another public body issues a patch in the protocol to reinstate their authority. These patches are also performed as blockchain transactions; therefore, governance is public, and public administration is accountable.

The tokenization can happen step by step by introducing it as a parallel alternative to the existing system. The government should take a leading role in such reform. First, the citizens must be guaranteed with the right to a free choice, whether a person wants to protect his or her property rights in the traditional way or transfer the title record from the centralized land cadastre to blockchain. Once the record is in the ledger, there is no need to duplicate it in the centralized database; the blockchain is the registry itself. All transactions that happen with the token are registered in the ledger.

There is no reason to believe that there will be one exclusive blockchain or the blockchain of the blockchain. Therefore, the role of the government is to establish a cross-blockchain infrastructure and security standards. This will ensure users the ability to choose themselves, which blockchain they wish to use to manage their property rights. On the other hand, it will enhance the fair competition of technologies for the user. It will inevitably lead to better quality, security, and further development of technologies.

This research is the first to attempt to grub a whole domain of property rights and public registries on blockchain; it leaves a lot of room for further research and development. Nevertheless, further development is impossible without the first steps.

Annex

Guidelines for Protocols of Smart law

1. Digital Identity Creation

1.1 User and Trust Service Provider/Certificate Authority (hereinafter – TSP) establish a trusted channel of communication, for instance, meet in person.
1.2 TSP gives the User a `secret` phrase through the trusted channel.
1.3 User publishes from addressA a token, where Key is arbitrary chosen unique string, and Value is reference consist of hash sum retrieved from addressA and a secret phrase:
`Key: [UserID]`[12]
`Value: [reference=hash(addressA:secret)]`[13]; other data[14].

12 The field "key" must be unique throughout the overlaid database. Name-Value Storage is an example of the technology which ensures the uniqueness of key-value records. If the user published a key-value record, the key would be exclusive; nobody can create the record with the same key. The chronological nature of blockchain transactions ensures it. When any user is trying to publish a record, the key-value protocol will check if anyone before published the record with the same key. The same way the protocol ensures the ownership in a transfer of the key-value token or update. The protocol verifies if the transfer/update transaction is received from the same address where it has been created.
In Ethereum, token(s) is created by publishing a smart contract. The Ethereum protocol ensures that the smart contract's ID is unique. It is a contract's hash sum, which is automatically generated at the moment of publishing the contract. This can be another example of how the protocol maintains uniqueness of keys in the database. The record's "key" plays a crucial role in having exclusive records that represent property rights. It is unacceptable that two users claim the same right over the same property.
13 The user publishes hash sum of the string [addressA:secret] because this string must be used by TSP as the key of his token record. Hash allows hiding this string. Otherwise, when the User's token becomes publicly available on the blockchain, anyone may see the string and create the token with this string. Because a key is unique in the database, TSP will not be able to use this string as his key.
14 Other data mean the data which may require (name, date of birth, etc.) and/or the user may wish to include. Personal data (name, etc.) may be cryptographically protected to ensure privacy. For details, see DID framework and the concept of SSI.

1.4 TSP publishes from `addressB` a token using string(addressA:secret) as key and specifies the status of the User's ID as value (for example, valid):
`Key: [addressA:secret]`[12, 15]
`Value: [status:UserID=someStatus]`[16]

2. Identity Verification

2.1 Any user may enquire[17] `addressA`.
2.2 The system searches tokens that begin with the key `addressA`.
2.3 Every found token is verified whether it belongs to the root of trust third parities' addresses, i.e., `addressB`. Those records which do not belong to a list of trusted third parties are ignored.
2.4 The system checks the presence of the status record and parses this in all remained tokens. The system searches to which token the status points out and searches tokens with such keys. If it is found that the token `UserID` belongs to `addressA`, the system reads its status and returns as a message to the user (for example: `UserID` is valid).

3. Title Certification

3.1 User creates a token from address A:
`Key: [uniqueString]`[12]
`Value: [reference=referenceString], other data.`
3.2 Registrar from creates a token address B:
`Key [referenceString]`[18]
`Value: [any standardized record]`[16]

15 TSP's key [addressA:secret] must be identical to the string[addressA:secret], which the User used to generate hash sum, so automatic inquiry for verification is possible.
16 Value must contain a record designed in a machine-readable standard. The value contains information that specifies the legal status of the user's token. For example, value:UserID=valid.
17 All inquiries should be made to the user's local full blockchain node (wallet). Inquiries to remote third parties' servers will be surrounded with all corresponding risks which are present in any centralized (client-server) system.
18 User's referenceString and Registrar's referenceString must be identical, so automatic inquiry for verification is possible.

4. Token Verification

4.1 To verify the certification, any user searches[17] the user's token *uniqueString*. When it is found:
4.2 The system verifies if the token belongs to a verified digital identity (See 2). The system searches in its field Value for a reference; and then
4.3 Enquires token with the key referenceString.
4.4 If such token is found, the system *verifies the identity of the address* (See 7) where this token is recorded, whether it is a trusted third party, i.e., the authority (See 8); and
4.5 Searches for a standard machine-readable record in the field Value to check its validity.
4.6 Archive inquiry includes the history of all token updates (status changes, other value updates, and transfers).

5. Multiple Certification and Verification

To perform certification by more than one trusted third party, the user inserts in the token references to different certifying records (a notary, a surveyor, valuer, building inspector, etc.). The system performs verification[17] against every reference.

6. Token Update and Transfer

6.1 The user and a trusted third party may perform update or transfer of token. In case of an update, the user specifies in a new Value. In the case of a token transfer, the user specifies. Transfer of a digital identity token, makes such identity invalid (see 2.4) because the address and the certifying token will not match. Therefore, on the contrary to Title Token transfer, the transfer of identity is impossible.

7. Trusted Third Party Identity

The identity of a trusted third party (registrar, notary public, surveyor, etc.) is verified by TSP/CA as per Protocol scheme 1 "Digital Identity Creation."

8. Trusted Third Party Authorization

The authority of a trusted third party (hereinafter – Government) creates a certificate, and the trusted third party includes the reference to the Government's certificate as per Protocol scheme 3 "Title Certification."

9. Root Record. Patches

9.1 Both the Government and TSP/CA may be the root records. Government records may have branch roots, as per branches of power. They all may have one root record, rather than separate.
9.2 The authority generates a private key and public key (+blockchain address) as per a secure protocol.
9.3 The authority creates a token using a multisig scheme[19] with the *List* of Trusted Third Parties (branches, bodies, departments, government agencies, etc.).
9.4 The Government creates as many levels down of Trusted Third parties/lists, where the superior level of the government branch/body certificates the level below, as per the established hierarchy of the public administration.
9.5 If any trusted third party loses authorization (resigned, dead, etc.) or their private key is compromised, the level above updates the certificate token as per Protocol 6 "Token Update and Transfer."
9.6 The root record may create records which defines the validity of other records. For example, the root address authority may create a token which invalidates any third-party token.

10. Recognition of the Authority. Reset of power

11. The government notifies the user which root(s) is a trustable using official off-chain public channels: (official newspaper "Gazette," etc.).
12. User includes the root(s) in his/her local node (wallet). Alternatively, the user downloads software through government resources with set up roots.
13. The verification of a digital identity and certificate is performed through the chain of certificates from the low to the highest level and ends with checking the presence of the root address in the user's list of trusted roots.

---

19 Multi-signature scheme may be used to have collective control over the root token, so to make Collegial decisions over its updates.

14. User may add other addresses in the list of trusted. For example, to create a private Web-of-Trust.
15. If the root record is compromised, the Government notifies the user using off-chain official channels. To reinstate the power, the user excludes the old root and includes a new one.[20]

Acknowledgments: This paper is an outcome of the PhD research performed inside of the Joint International Doctoral (Ph.D.) Degree in Law, Science and Technology, coordinated by the University of Bologna (CIRSFID) incooperation with the University of Turin, Universitat Autònoma de Barcelona, Tilburg University, Mykolas Romeris University, The University of Luxembourg. The author is grateful to RMIT University and the team of Blockchain Innovation Hub for the seminal collaboration. Thanks to supervisors Associate Professor Marta Poblet Balcell, RMIT University (Melbourne, Australia) and Professor Pompeu Casanovas Romeu, La Trobe University (Melbourne, Australia).

References

Alketbi, A., Nasir, Q. and Talib, M.A. (2018) 'Blockchain for government services-Use cases, security benefits and challenges', in *2018 15th Learning and Technology Conference, L and T 2018*. IEEE Xplore. doi: 10.1109/LT.2018.8368494.

Allessie, D. *et al.* (2019) *Blockchain for Digital Government, Publications Office of the European Union*. Luxembourg. doi: 10.2760/93808.

Batubara, F. R., Ubacht, J. and Janssen, M. (2018) 'Challenges of blockchain technology adoption for e-government: A systematic literature review', in *ACM International Conference Proceeding Series*. Association for Computing Machinery. doi: 10.1145/3209281.3209317.

Berg, C. (Research fellow), Davidson, S. and Potts, J. (2019) *Understanding the blockchain economy: an introduction to institutional cryptoecnomics*. Edward Elgar. Available at: https://www.e-elgar.com/shop/gbp/understanding-the-blockchain-economy-9781788974998.html (Accessed: 16 September 2019).

'Bitcoin address Programming The Blockchain in C#' (no date) in. Available at: https://programmingblockchain.gitbook.io/programmingblockchain/bitcoin_transfer/bitcoin_address (Accessed: 1 July 2018).

Christensen, S. (2004) 'Electronic Land Dealings in Canada, New Zealand and the United Kingdom: Lessons for Australia – [2004] MurUEJL 37', *eLaw Journal: Murdoch University Electronic Journal of Law*, 11(4). Available at: http://www5.austlii.edu.au/au/journals/MurUEJL/2004/37.html (Accessed: 27 March 2020).

20 In further versions, there should be developed e-voting methods for delegation of power and direct decision making. Though the possibility to include and exclude the root is the ultimate protection from a digital dictatorship.

Council of the European Union (2014) *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 (eIDAS), Official Journal of the European Union*. EU. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910.

Cushman, E. (1937) 'Torrens Titles And Title Insurance', *University of Pennsylvania Law Review*, 85 (6), p. 589. Available at: https://scholarship.law.upenn.edu/penn_law_review/vol85/iss6/3 (Accessed: 6 April 2020).

Dawes, S. S. (2008) 'The Evolution and Continuing Challenges of E-Governance', *Public Administration Review*, 68, pp. S86–S102. doi: 10.1111/j.1540–6210.2008.00981.x.

'Digital Signature Standard (DSS)' (2013). Gaithersburg, MD. doi: 10.6028/NIST.FIPS.186–4.

Emercoin NVS – Emercoin Community Documentation (no date). Available at: https://emercoin.com/en/documentation/blockchain-services/emernvs (Accessed: 28 June 2018).

EOS.WIKI (no date). Available at: https://eos.wiki/ (Accessed: 27 December 2019).

Ethereum Wiki (2017). Available at: https://github.com/ethereum/wiki/wiki/Glossary (Accessed: 4 July 2017).

European Land Registry Association: Description of land registration systems (no date) *ELRA*. Available at: https://www.elra.eu/facts-sheets/description-of-land-registration-systems/why-register/ (Accessed: 30 December 2019).

Friend, C. (2004) 'Social Contract Theory', *Internet Encyclopedia of Philosophy*, pp. 139–155. doi: 10.1086/292887.

Hacker, P. and Thomale, C. (2018) 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law', *Degruyter European Company and Financial Law Review*, 15(4). Available at: https://www.degruyter.com/view/journals/ecfr/15/4/article-p645.xml (Accessed: 30 March 2020).

Hanstad, T. (1998) 'Designing Land Registration Systems for Developing Countries', *American University International Law Review*, 13(3), pp. 647–703. Available at: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1358&context=auilr (Accessed: 30 March 2020).

HM Land Registry is making it easier to remortgage – GOV.UK (no date). Available at: https://www.gov.uk/government/news/hm-land-registry-is-making-it-easier-to-remortgage (Accessed: 27 March 2020).

Introduction to the Linux chmod command | Opensource.com (no date). Available at: https://opensource.com/article/19/8/linux-chmod-command (Accessed: 27 March 2020).

Jansen, M. *et al.* (2020) 'Do Smart Contract Languages Need to Be Turing Complete?', in, pp. 19–26. doi: 10.1007/978-3-030-23813-1_3.

Konashevych, O. (2019a) 'Comparative Analysis of the Legal Concept of Title Rights in Real Estate and the Technology of Tokens: How Can Titles Become Tokens?', in *Lecture Notes in Computer Science* (*including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*). Springer Verlag, pp. 339–351. doi: 10.1007/978-3-662-58820-8_23.

Konashevych, O. (2019) 'Data Insertion in Blockchain For Legal Purposes. How to Sign Contracts Using Blockchain', *Electronic Modeling*. Ukrinformnauka Co. Ltd., 41(5), pp. 103–120. doi: 10.15407/emodel.41.05.103.

Konashevych, O. (2020a) 'Constraints and Benefits of the Blockchain Use for Real Estate and Property Rights', *Journal of Property, Planning and Environmental Law*. Emerald Publishing Limited, ahead-of-p(ahead-of-print). doi: 10.1108/JPPEL-12-2019-0061.

Konashevych, O. (2020b) 'Cross-Blockchain Protocol for Public Registries', *SSRN Electronic Journal*. doi: 10.2139/ssrn.3537258.

Konashevych, O. and Khovayko, O. (2020) 'Randpay: The technology for blockchain micropayments and transactions which require recipient's consent', *Computers and Security*. Elsevier Ltd, 96, p. 101892. doi: 10.1016/j.cose.2020.101892.

Krogsbøll, M. *et al.* (2020) 'Smart Contracts for Government Processes: Case Study and Prototype Implementation', in *Financial Cryptography and Data Security 2020*. International Financial Cryptography Association, pp. 1–8. Available at: https://fc20.ifca.ai/preproceedings/163.pdf.

Liechtenstein Blockchain Act (2019). Liechtenstein. Available at: https://perma.cc/H2GT-88CN (Accessed: 30 March 2020).

Loibl, A. (2014) 'Namecoin'. doi: 10.2313/NET-2014-08-1_14.

Malta Virtual Financial Assets Act (2018). Malta. Available at: http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29079&l=1 (Accessed: 30 March 2020).

Mizrahi, A. (no date) *Colored Coins Protocol*. Available at: https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/ (Accessed: 23 September 2019).

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*. doi: 10.1007/s10838-008-9062–0.

Ølnes, S. and Jansen, A. (2017) 'Blockchain technology as s support infrastructure in e-Government', in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. doi: 10.1007/978-3-319-64677-0_18.

Reed, D. *et al.* (2019) *Decentralized Identifiers (DIDs)*. Available at: https://w3c-ccg.github.io/did-spec/ (Accessed: 1 January 2020).

Republic of Georgia to Develop Blockchain Land Registry – CoinDesk (no date). Available at: https://www.coindesk.com/bitfury-working-with-georgian-government-on-blockchain-land-registry (Accessed: 12 July 2019).

Rood, J. (1914) 'The Registration of Land Titles', *Articles*, 12, pp. 379–93. Available at: https://repository.law.umich.edu/articles/1133 (Accessed: 30 March 2020).

Schmid, C. and Hertel, C. (2005) *Real Property Law and Procedure in the European Union General Report Final Version scientific co-ordinators*. Available at: https://www.eui.eu/Documents/DepartmentsCentres/Law/ResearchTeaching/ResearchThemes/EuropeanPrivateLaw/RealPropertyProject/GeneralReport.pdf (Accessed: 31 March 2020).

Soto, H. de (2000) *The mystery of capital: why capitalism triumphs in the West and fails everywhere else*. Basic Books.

Spies, T. (2013) 'Public Key Infrastructure', in *Cyber Security and IT Infrastructure Protection*. Elsevier Inc., pp. 75–107. doi: 10.1016/B978-0-12-416681–3.00003–3.

Systems Of Ownership And Registration (no date). Available at: https://www.icsm.gov.au/education/fundamentals-land-ownership-land-boundaries-and-surveying/land-and-land-ownership/systems (Accessed: 6 April 2020).

Szabo, N. (1994) *Smart Contracts*. Available at: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (Accessed: 31 March 2020).

The Land Registry in the blockchain – testbed (2017). Available at: https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf.

Wright, A. and De Filippi, P. (2015) 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia', *Social Science Research Network*, 62, pp. 4–22. doi: 10.2139/ssrn.2580664.

PAPER 2

The paper is accepted for publication in the International Journal of Web Information Systems, Emerald Publishing. This is a pre-print version under Creative Commons Attribution Non-commercial International Licence 4.0 (CC BY-NC 4.0). DOI: 10.1108/IJWIS-07-2020-0045

Cross-Blockchain Protocol for Public Registries

Oleksii Konashevych [0000-0003-0068-5962]

Erasmus Mundus Joint International Doctoral Fellow in
Law, Science and Technology, oleksii.konashevych2@unibo.it

Abstract. This paper presents a concept of the protocol for public registries based on blockchain. The proposed mechanism allows creating a standard database over a bundle of distributed ledgers. It ensures a blockchain agnostic approach and utilizes the benefits of various blockchain technologies in one ecosystem. In this scheme, blockchains play the role of journal storages (immutable log), while the overlaid database is the indexed storage. The distinctive feature of such a system is that in blockchain, users can perform peer-to-peer transactions directly in the ledger using blockchain native mechanism of user access management with public-key cryptography (blockchain does not require to administrate its database). The protocol is designed for public property registries, i.e., land titles, cars, boats, corporate rights, etc. Users can create and manage their rights using the full power of blockchain technologies and smart contracts. The governance component in this protocol is introduced as Smart Laws and Digital Authorities, the algorithms to manage the overlaid system and address legal issues with property rights and law enforcement.

Keywords: blockchain, electronic government, public registry, land registry, smart law, digital authority

1 Intro

Governments play a crucial role in keeping public registries to prevent legal disputes about “who owns what.” Thus, the government acts as a trusted third party in private relations. However, if the government as a mediator loses the ability to be a source of law and order, it becomes a cause of conflicts.

Therefore, for instance, centralization in state-owned land registry is a solution, but a source of risks. Risks are addressed by a system of hierarchically organized public administration, separation of powers, multiple checks, and balances. It all becomes a burden for citizens that pay taxes and deal with red tape.

For quite some time, it prevails Weber's doctrine of the inevitability of bureaucracy (Weber, 1922). He believed that at this point of development, society should accept bureaucracy as inevitable and necessary.

The idea of the blockchain[1] use for state-level governance and public registries is an open space for discussion in academia and blockchain industry because it may reduce centralization.

A conceptualization in this field so far was limited to general ideas of "disrupting governance" (regulations, bureaucracy, middlemen, among others); superficial in their essence, and unable answer how to design the system where law and technology will not collide, exposing existing problems: enforceability in an immutable ledger of the blockchain technology, scalability, sustainable governance and many more discussed below.

Cross-Blockchain Protocol (CBP) is the technology of an overlaid database across a bundle of ledgers that enables smart laws and enforceability. The protocol is fundamental for using blockchains for property registries (for example, land cadastre) and other public databases run by governments. It may also have applications in the private and commercial sphere.

Alternatively, an open and decentralized blockchain technology, tech consortia propose governments so-called "permissioned" (also known as private, federated, enterprise, etc.) Distributed Ledger Technologies (DLT), which are centralized, have similar vulnerabilities and limitations which other centralized technologies have. The advantages of such systems DLTs are questionable. There is no convincing evidence why this kind of technology is better than those centralized systems that governments have used for decades. It ensures immutability for records at the discretion of the authorities, i.e., retroactivity, censorship, corruption, and even full-stop services depending on a specific design of a system.

Moreover, DLTs have some unique features and some trade-offs, which may address one problem but ignores another. There is no reason to believe that any particular DLT is better than others, and there will be one ultimate ledger. Hence, why would the government choose one DLT in favor of others?

But the major question in any technological shift is the cost of a mistake. Will governments have an opportunity to shift back or choose alternative technology with reasonable costs if anything goes wrong?

While one government agency runs one permissioned DLT solely, there is no decentralization. If instead, a private network is in use, why would the government allow one private infrastructure provider (or a consortium) to monopolize public services?

Other questions may also arise. For example, is this constitutional to share government sovereignty with a closed group of providers (nodes) that run a private network to provide public services?

---

[1] The word "blockchain" is used here in the original meaning, i.e., a decentralized, uncensored public system. Hence, "permissioned" and "private" DLTs due to their centralized nature are not blockchains. Therefore, governments that use centralized technologies cannot claim the application of blockchain.

And finally, if many decent, competitive, and secure networks can provide reasonable infrastructure for public services, why not choose all?

Public blockchains, even though they are decentralized, are not static. Decentralization is ensured by constant fair competition. Bitcoin, Ethereum, and some other public networks show that they remain sustainable. If some troubles happen in their ways, they can tackle them without any central authority. Decentralization is the guarantee of the records to be safe and immutable. Centralized databases cannot provide such a level of immutability.

Therefore, this research is based on a hypothesis that public blockchains can be used as storage for records of land rights and other property rights (which are normally stored in government databases) and various government services, which also involves the need to store data in public databases.

Though immutability is not the only advantage, the traditional database cannot provide direct access for end-users; transactions are performed through registrars. Blockchains have a native mechanism to manage ownership with public-key cryptography, and the user can perform peer-to-peer transactions (title deeds). Thus, the user needs neither registrars nor registry keepers.

Once a token representing the owner's land title is created on the blockchain, there is no need to keep track of its transactions elsewhere. There is no need in any land registry because blockchain is the registry itself.

Nevertheless, people still need legal procedures, which now exists in paper form and applied by those registrars and other public bodies. Hence, the combination of blockchain and automation of procedures may significantly improve governance.

Such ideas remain hypothetical for now, but this research is the first attempt to introduce a systematic approach of a system architecture for public services.

The proposed protocol aims to ensure that within the created bundle of existing blockchains, it is the citizens that decide where to keep their ownership records and manage property rights not the government. The bundle may unite not only public ledgers, but also permissioned, private, etc., and also interact with closed, centralized databases, which makes possible a shift from mono-database run by the government agency to multiple ledgers and cross-chain transfers.

This ensures fair competition among technologies, because users not only may choose any ledger within the bundle but transfer their assets from one chain to another if any technology does not suit their interests. On the other side, there is no need for the government to decide for citizens which technology to use, which corresponds with the principle of technological neutrality.

The protocol is a standard that transforms the “wild west” of incompatible and non-interactive networks into a unified ecosystem. Notably, it does not require upgrades or permissions of these networks for the protocol to be applied.

A straightforward use of blockchain for running public registries is impossible. There are legal issues with enforceability and immutability, hardforks, digital identity, privacy, scalability, and price volatility. The protocol is designed to address them.

It introduces the concept of “smart laws.” This is a framework for smart contracts and enforcement. Smart laws consist of algorithms that enable digital authorities to address legal issues: disputes, inheritance, loss of private keys, etc.

2. Theoretical Framework, Methodology and Literature Review

a. Methodology and Theoretical Framework

This paper is framed with design science research (DSR) provided by Hevner et al. (Hevner et al., 2004). As per DSR, the research is meant to present an "artifact" which is defined as "constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), and instantiations (implemented and prototype systems)." This research deals mostly with *models* and *methods*.

In particular, the cross-blockchain database is a model, and cross-blockchain protocol is a set of methods of how this model can be designed. The research provides a broad discussion and evaluation of the applicability of the proposed invention and constructs various models of its use in governance.

This research is complaint with 7-step research guidelines provided by Hevner et al., and corresponds with Design Science Research Publication Schema (Gregor and Hevner, 2013) by Gregor and Hevner. The following table outlines steps of the performed SDR:

The following table outlines steps of the performed SDR:

#	Step	Comment
1	Introduction	Section 1 - the purpose and scope of the artifact – present a public registry model for property rights based on a bundle of existing public blockchains with enforcement and interoperability. Section 3 presents issues of the blockchain use by governments, which forms a corpus of research questions, which are to be addressed by this DSR.
2	Literature review	Subsection 2b provides context to the relevant academic research in blockchain and governance to support the protocol's integral elements and proposed methods.
3	Method	Subsection 2a (this subsection)
4	Artifact description	Section 3 - a design concept of a cross-blockchain protocol to create end-to-end public databases across a bundle of blockchains.
5	Evaluation	Subsection 4.3 is a technical evaluation of the architecture, its limitations, and strategies to manage risks and constraints.
6	Discussion	Section 5 is a general evaluation of the technology applicability with legal and political aspects.
7	Conclusion	Section 6 is a summary of the research outcomes and discussion of further directions of the research.

Method. The primary method for this DSR is *exaptation*, i.e., adoption of solutions from other fields. The research is looking into existing technologies applied here as elements of the protocol: Name-Value Storage, Berkley DB, RAID protocol, among others. The choice of Name-Value Storage as a reference technology for creating a database over blockchain is based on the analysis and comparison with two other similar technologies: Bigchain and Amazon QLDB, presented in Section 4.1.a.

The evaluation does not use experimental and testing methods for a few reasons. Firstly, there are no quantitative objectives (for example, there are no purposes to improve latency performance, bandwidth, or size transaction optimization, among others); hence, there is nothing to measure for evaluation.

Secondly, creating a key-value DB across a bundle of public repositories is feasible enough to argue its implementation possibility.

This research's theoretical value is vital since it is meant to present viable models and scenarios of the use of decentralized blockchains, instead of permissioned DLTs in the public sector. The absence of any solution in this space practically makes the application of the public blockchain impossible. For instance, for property registries, due to known legal issues. Therefore, the hypothetical concept is valuable as it opens a discussion in the field.

Lastly, the development of the running system may require substantial resources. Therefore, broader independent evaluation and contribution among researchers may create more knowledge to consider developing prototypes in the future.

Therefore, this research focused on designing the protocol's concept and, generally, public registries across multiple blockchains. All elements of this architecture exist and are tested in other applications.

b. Literature review

Recent academic literature creates a valuable context on blockchain use, its benefits, applications, characteristics, classification, and constraints.

The paper “Constraints and benefits of the blockchain use for real estate and property rights” (Konashevych, 2020) became a basis for this research because it identified major constraints of the emerging technology for a public property registry, which laid down as the purpose to address in this research, i.e., to find the way to utilize blockchain for public property (real estate, land, etc.) registry and overcome major constraints (see Section 3).

Many papers operate on a higher level when it comes to land registry, i.e., public services and e-government, seeking answers on how blockchain can improve this field. Among the first to discuss governance and blockchain was a journal paper “Beyond Bitcoin: enabling smart government using blockchain technology” (Ølnes, 2016) by Ølnes (2016). The author refers to the example of publishing hashes on Bitcoin - a small project at the University of Nicosia, where students were given electronic certificates after finishing a course, and a hash sum of the certificate was inserted in Bitcoin’s blockchain. Hashing on blockchain is much discussed in “Blockchain Anchoring of Public Registries: Options and Challenges” (Konashevych

and Poblet, 2019). The authors discussed requirements for better system architecture for centralized public registry and DLT over it to hash DB entries.

In “Disrupting governance with blockchains and smart contracts,” (Shermin, 2017) Shermin (2017) discusses the major constraints of the use of blockchain. There is a gap between the initial conceptualizations of blockchains and their first instantiations. First use cases show that as circumstances change, protocols can become inappropriate for the new environment and require modification. Modification of blockchain code happens through majority consensus, but reaching consensus in a distributed multi-stakeholder network with sometimes unaligned interests is complex, potentially introducing new agency issues.

In “Blockchain technology as a support infrastructure in e-Government,” (Ølnes and Jansen, 2017) Ølnes and Jansen (2017) continued the exploration of blockchain for governance. The authors are among the first to caution unreasonable optimism in the use of “permissioned” and “private” systems in public services: “Closed blockchains [...] must rely on traditional security mechanisms in order to prevent unwanted access and modification to the blockchain.” The paper mainly discusses open blockchains [networks], because as authors emphasize, “closed systems are never able to build an infrastructure.”

In “Blockchain in Government: Benefits and implications of distributed ledger technology for information sharing,” (Ølnes et al., 2017) Ølnes, Ubacht and Janssen (2017) ask whether blockchain technology will lead to innovation and the transformation of governmental processes. To address this question, the authors presented a critical assessment of the “often exaggerated benefits of blockchain technology” found in the literature and discussed their implications for governmental organizations and processes. The paper summarizes directions for further research into the potential benefits of blockchain applications in e-government and the role of governance of blockchain architectures and applications to comply with societal needs and public values.

In “A framework of blockchain-based secure and privacy-preserving E-government system,” (Elisa et al., 2018) Elisa et al. (2018) argue that most of the existing e-government systems, such as websites and electronic identity management systems (eIDs) are centralized at duplicated servers and databases. A centralized management and validation system may suffer from a single point of failure and make the system a target to cyberattacks such as malware, denial of service attacks (DoS), and distributed denial of service attacks (DDoS). The blockchain technology enables the implementation of highly secure and privacy-preserving decentralized systems where transactions are not controlled by third-party organizations. They propose a framework of a decentralized e-government peer-to-peer system using blockchain technology to ensure information security and privacy while simultaneously increasing the public sectors' trust. Also, a prototype of the proposed system is presented with the support of a theoretical and qualitative analysis of the security and

privacy implications of such a system. It is important to note that the authors share the idea that a "permissioned" (centralized) system can be called "blockchain." They attribute this system features of blockchain: "The permissioned blockchain system ensures that the stored records are trustworthy, auditable and transparent." In the proposed architecture, it is clear that infrastructure is introduced and maintained by the government. The question of how the proposed centralized system is better than the existing one remains open.

Batubara, Ubacht and Janssen published their "Challenges of blockchain technology adoption for e-government: A systematic literature review" (Batubara et al., 2018) in 2018. The paper guides through several studies and pilots in blockchain in governance available by 2018. Several countries such as the USA, the United Kingdom, the Netherlands, the United Arab Emirates, Estonia, Sweden and China announced blockchain initiatives to explore its uses in the public sector actively. Their findings have shown that academic research in this area had only just started, and issues discussed in the selected literature were still significantly limited. Consequently, more intensive research in this area was still necessary to advance this field's maturity. As per the authors, the organizational perspective's major challenges are the need for new governance models and the acceptability of this technology. The research into blockchain technology standards and a reference architecture for e-Government applications was proposed to resolve the technological challenges.

Further directions are found in Franciscon et al. (2019) "A systematic literature review of blockchain architectures applied to public services" (Franciscon et al., 2019). This work provides a systematic review of blockchain-based applications across multiple domains: supply chain, business, healthcare, IoT, privacy, and data management. Authors point to the shortcomings identified in the relevant literature, particularly the limitations the blockchain technology presents and how these limitations spawn across different sectors and industries. Building on these findings, authors identify various research gaps and future exploratory directions anticipated to be of significant value both for academics and practitioners.

Brinkmann and Heine (2019) in "Can blockchain leverage for new public governance? A conceptual analysis on process level" (Brinkmann and Heine, 2019) presented the preliminary results of ongoing research, which aimed to shed light on the more concrete benefits of blockchain for New Public Governance (NPG). The preliminary results show that blockchain offers valuable support for governments seeking methods to coordinate co-producing networks effectively. It becomes evident that there is a need for off-chain processes. Therefore, it is argued in favor of intensifying research on off-chain governance processes better to understand the implications for and influences on on-chain governance.

More recently, the paper "Smart Contracts for Government Processes: Case Study and Prototype Implementation" (Krogsbøll et al., 2020) by Krogsbøll et al. (2020) contains a description of the pilot with the Danish Municipality. The government

partner concluded that the risk of losing access to the system (due to loss of private keys) outweighed any benefits. The researchers, on the other side, think that smart contract implementations of government processes need to be immutable and outside of the government's control when running; however, they also need to be updatable when laws change and provide an "out" for the rare case when errors in the contract implementation result in unlawful behavior and consider these problems as the "foundational research challenge for blockchain to apply to governmental processes."

The proposed protocol for blockchain-based public registry inevitably deals with digital identities and triggers issues of privacy. The collision of blockchains and GDPR in the EU is the most indicative discussion in this context. The paper by Pagallo et al. "Chronicle of a clash foretold: Blockchains and the GDPR's right to erasure" (Pagallo et al., 2018) is worth a mention as it not only formulates the problem but discusses possible solutions.

The governance in the cross-blockchain protocol relevant to issues of governance in blockchain. The paper by M. Crepaldi "Why blockchains need the law: Secondary rules as the missing piece of blockchain Governance" [16] drew attention to the concept of secondary rules of law and its problem governance in blockchains. The issues of secondary, or meta-rules, was introduced by the legal philosopher, Hart in the '60 (Noonan, 1962); these are the rules which define how primary rules (laws) are introduced and changed. In the last section of this paper, the problem of secondary rules will be discussed as they appear to be the cornerstone of the cross-blockchain protocol.

To sum up, the recent research introduced a variety of opinions about the blockchain technology, its features, benefits, and limits. This creates grounds for further research and development, especially in various economic activity spheres beyond cryptocurrency. There are lots of perspective ideas that remain in theoretical phases that are yet to be noticed or in early piloting stages. Therefore, the future challenge is to observe, collect, and analyze more empirical data to define better practices and pitfalls across multiple fields and disciplines.

3. Public blockchains issues

This section defines problems on the way of the blockchain use for public registries: risks of multiplication of assets due to hardforks, enforceability, anonymity, digital identity, privacy, data integrity, scalability and price volatility. In the end, it is summarized what is opposed to blockchains and why blockchain is still a good choice for infrastructure.

3.1. Why blockchain is impossible to use in public service as it is

a. Hardforks

The hardfork is the major concern for open competition systems because there are no authorities that impose and enforce one exclusive status quo.

The system can be split into two or more branches or so-called “forks,” after which each branch becomes independent but has a spare history of transactions till the moment of fork.

Tokens are duplicated as a result of the split. For example, suppose the system is used to manage rights on movable or immovable property (often mentioned as “asset-backed tokens”) due to a hardfork, the user will still have one plot of land but two title records in parallel systems. As a result of the fork, they can be managed independently, thereby creating legal collisions. For example, in one system, the user sells the plot, but in the other, the user still owns it.

b. Immutability

Being an advantage of blockchain technology, the ledger's immutability can cause a lot of untoward use cases. For example, the loss of private keys will make cryptocurrency, a token, or a smart contract uncontrolled with negligible possibilities to restore it. Even if the blockchain can prevent many ownership disputes, the imperfect nature of people’s relationships will always cause issues with ownership and the need to settle when they arise. In its pure design, the blockchain itself does not leave practical possibilities for enforcing any legitimate judicial decisions or any legal actions by authorities.

c. Anonymity (pseudonymity)

The authorization and authentication for a transaction are provided only with the relevant private key within the user’s asymmetric pair. The public key of the pair is taken to generate the address. The concept of addresses is the cornerstone of the blockchain. In the result of a transaction, a coin is spent from one address and added to another address, but to enable such transfer, the coin owner must use the relevant private key. Thus, the address is the only public record in the ledger that identifies the user.

However, some research showed that addresses could be deanonymized by different digital fingerprints found in the network (IPs, behavior patterns, among others.) (Ober et al., 2013), (Androulaki et al., 2013). The pure blockchain protocol is not suitable for keeping records on property and securities from governments' perspective — blockchain anonymity veils money laundering, financing terrorism, and other unlawful activity.

Beyond that, at the practical level, the blockchain's censorless nature creates confusion in identifying records. Anyone may perform any transaction and publish any data in the blockchain. If the government must authorize a land title deed, how do

you define if any transaction on the blockchain belongs to the town clerk if they are all pseudonymous? Without overlaid solutions for digital identities and trust services, it is almost impossible to create any scalable governance model.

d. Data integrity, off-chain data and issues of personal data

In blockchain, any published data is exposed, and removal is not an option. Alternatively, users can insert into the blockchain cryptographic hashes of the data. The blockchain that stores hash sums will provide two things: the user can verify the authenticity of the data (whether it is still the same or not) and timestamping because blocks are chronologically stored.

However, hashing does not ensure the protection of the data itself. Once it is tampered with or deleted, the hash sum is useless for restoring. This leads to two possible solutions: data will be stored by a trusted third party (for instance, a government agency) or users themselves.

Today all personal data and property records (title records) are stored in closed databases controlled by governments, and publishing hashes, whether into the centralized DLT or open blockchain does not add much security. To verify this data, the user needs access to that closed database or trusts the entity that stores it.

Even if public blockchain is used to store hashes, there is still in this scheme a trusted party as the source of truth, and so concentrating many risks for leaks and corruption of data as a single point of failure.

e. Scalability

One exclusively chosen blockchain for governance will necessarily create issues. To verify this data, the user needs access to that closed database or blindly trusts the entity that stores it.

The potential bandwidth of Bitcoin per year, for example, is roughly 220 million transactions (Roio, 2013). For instance, 300 public registries in Ukraine generate even more data than Bitcoin's bandwidth ("Data.gov.ua," n.d.), which leaves no space for other cryptocurrency transfers.

Overload with the transactions creates the problem of high transaction fees and price volatility. Although Bitcoin is not the best in bandwidth, it is still the most attractive in terms of security ("Cost of a 51% Attack | Crypto51.app," n.d.). This is not a workable solution on a scale, even for one country with a 40-mln population, randomly chosen as an example.

For blockchain using other consensus protocols or other data structure, scalability is not the main issue. For example, Ethereum, IOTA, NXT, NEM, and many other systems ensure better bandwidth and performance.

The choice of one network in favor of others is a discussion about technological neutrality – a principle that is often discussed in public policy. The reader may find discussions that compare one specific blockchain network with some specific centralized system, where usually blockchain performance is fewer. Having in mind the principle of technological neutrality, it is proposed to consider the problem of

scalability from another perspective. One blockchain network does not necessarily provide enough scalability, while a bundle of blockchains may become much more effective.

f. Price volatility

Due to speculations, the price can dramatically fluctuate; therefore, creating a bad user experience for those who need cryptocurrency to pay fees for publishing and managing data and running smart contracts. The mentioned scalability issues make it infeasible for the government to use or even announce their intention to use any specific blockchain. It will inevitably incentivize agiotage on the market, exacerbating the problem of scalability even more.

3.2. What is opposed to blockchains and why it is still a good idea to use them?

Is the permissioned DLT better than the blockchain, as it addresses all these issues due to its centralized nature, purposed to control and restrict unwanted practices, and manually fix troubles?

There is no one specific consensus for permissioned systems. This is instead a title of various design concepts aimed to leave the leverage of control over the network in the hands of an authority, which can be by one actor or a closed group of actors.

Some protocols were not initially developed for permissioned design. For example, the Proof-of-Stake protocol (PoS) (King and Nadal, 2012) is designed as a cheaper alternative of Proof-of-Work. In PoS network, if a node (or a group of nodes who mutually agreed) has enough stake at their control, they may perform retroactive actions by rolling back blocks (Higgins, 2014) and can censor transactions.

Proof-of-Authority (Wood, 2015), and a family of Hyperledger consensuses (*Hyperledger Architecture, Volume 1*, 2017) protocols are dedicated to architecture with controlling features.

It is possible to design different schemas with privileged (master) nodes authorized to create blocks, write transactions, and some other specific rights providing those other participants of the network will not have them. Such systems can also be closed; therefore, users will need the authorization to read the information from blocks, whereas some protocol provides anonymous interaction (see, for example, DLT Quorum (“Blockchain and Distributed Ledger | J.P. Morgan,” n.d.)). Compared to existing centralized closed government systems, such DLTs may have some advantages; however, they are the same conceptually. They are centralized and censorable and are not necessarily immutable for those who control it.

Another reason why the choice of one DLT leads to centralization is that the choice of one exclusive network prevents competition. By choosing a permissioned DLT, the government takes responsibility for developing and maintaining infrastructure.

On the contrary, open blockchain systems do not have central authorities that build the network. Any user is free to add their computational resources for public needs and, therefore compete for having rewards for finding blocks, and this reward is not

distributed by someone centrally but automatically obtained as per the protocol. The infrastructure is self-organized, incentivized by a cryptocurrency with free competition for mining, i.e., creating and storing blocks.

The principle of decentralization is the basis of this research; therefore, we neither argue nor compare blockchain to centralized solutions. Centralized databases have already been in use for quite a long time by governments; therefore, we already know their advantages and disadvantages. Therefore, permissioned systems cannot be considered a significant evolutionary step in government systems.

Blockchain is a new word in governance, but this technology has some principal features that can restrain its implementation at the state level, and the following research conceptualizes ideas to address them.

Among various properties of the blockchain technology, we distinguish the following highly considerable for a new generation of public property registries:

- Blockchain provides an append-only type of database, which is called an immutable ledger. It prevents data corruption and unauthorized changes.
- Blockchain has a native mechanism for managing ownership through public-key cryptography; thus, it is not only an immutable storage, but also, it is a system for peer-to-peer transactions. Unlike traditional method, for example, real estate registry, it does not require a trusted third party to record a deed in the database.
- Blockchain is self-organized and does not require central authorities to govern and maintain the infrastructure.
- The proposal in this research concept utilizes the blockchain's immutability with the help of “smart laws”. It reduces centralization when possible and makes it accountable when centralization is inevitable.

4. Building a database across blockchains

The first subsection introduces an idealistic design model of a database across a bundle of blockchains (Subsection 4.1). Subsections 4.2 and 4.3 analyze the model's constraints and evaluate possible design solutions to get the system working.

4.1. General idea and basic elements

a. General idea

A cross-blockchain database is a logic superstructure over a bundle of blockchains, see Fig 1. To create a mutual interaction, users should agree which blockchains they include in the bundle and according to which rules and filters - the cross-blockchain protocol - they create the database.

The designed system collects users’ records from the bundle's blockchains into a consistent end-to-end public database. The “record” is an entry the user inserts into any blockchain in the bundle, it can be a token (or a “colored coin”) or a key-value record.

An entry must be compliant with the format so the algorithm will automatically select and send it into the cross-blockchain database from heterogeneous data flow in blockchains. Note that blockchain is uncensored; therefore, a lot of chunk data is also published there. This is the role of the protocol. It scans upcoming blocks in every ledger of the bundle and searches for records of a specific standard.

It verifies each record as per the protocol's rules and filters out if a record is non-compliant. Eventually, the system inserts the complaint record into the database, which is a local file on the user's computer.

When a user applies the same protocol on any computer, he or she will receive the same copy of the database that every other user has on their local computers. Thus, there is no mathematical consensus for the database itself. The database relies on existing consensus protocols of those ledgers, which are included in the bundle.

The consensus of the overlaid structure is a sort of a social contract because users must agree on the initial architecture of any particular database: which ledgers to scan and starting from which blocks, the format of the entry, and filtering rules, how to add new ledgers and drop a ledger from the bundle, how to transfer entries from ledger to ledger, how to upgrade and create patches in the protocol by collective decisions or by a central authority, etc. Thus, by applying the protocol and scanning blocks, users independently build a copy of the database. The protocol also includes so-called secondary rules or meta-rules for governance, i.e., a protocol change mechanism.

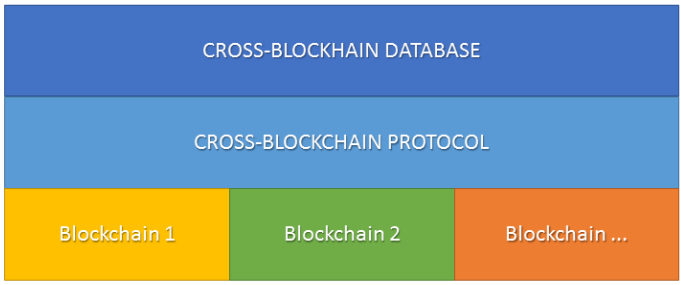


Fig. 1. Basic scheme of a bundle of blockchains with overlaid database The bundle can contain any number of ledgers, but the list must be definite at any point in time. The protocol provides for format rules and filters for entries and rules for scanning, adding new and deleting included ledgers intro the bundle. The system scans block across ledger of the bundle and hooks records compliant with the rules and adds them to the database.

The blockchain provides for a native mechanism of ownership through public-key cryptography: the user publishes a record, and the protocol considers the address from which he or she created this transaction as the owner of the record. Thus, to perform any update, the user must create a new record using the same private key because the private key is the authorizing mechanism for the address.

Several blockchain projects developed this mechanism. To better explain this protocol, let us refer to Emercoin's Name-Value Storage (NVS) technology, which started in 2014 as one of the successful designs for storing arbitrary users' data in the

structured form in the database. Emercoin's itself became a successor of a Namecoin's non-ICANN TLD service (Top-Level Domain ".bit").

It should be noted that other types of databases and technologies may be applied, and therefore, it will require a compatible format of a DB entry.

Emercoin's NVS protocol details are specified in Annex. We can extract a set of useful elements of both Emercoin's and Namecoin's NVSs. The following subsection presents which elements should be taken as a basis for a cross-blockchain protocol.

To address the legitimate question of why other types of blockchain-enabled databases, for instance, Bigchain and Amazon QLBD, were not chosen as a reference technology, it considers the following. Bigchain is a framework that connects DLT framework Tendermint and MongoDB ("About BigchainDB," n.d.). The first version of the technology appeared in 2015, a year later then Namecoin and Emercoin. Amazon QLDB is a similar concept that connects the Hyperledger and PartiQL database ("Overview of Amazon Quantum Ledger Database (Amazon QLDB)," n.d.), created in 2019. Both projects have one common feature, i.e. they took one of the existing DLT frameworks (Tendermint and Hyperledger Fabric) and use them as log systems for databases (MongoDB and PartiQL). DB entries are inserted in ledger transactions, then hooked and pushed through to the connected database. Here, something similar happens with Namecoin and Emercoin. The difference is that public blockchain due to having native tokens (cryptocurrency) has embed user access mechanism through public key-cryptography, where a user's address is a representation of a public key, and a private key is used to authorize transactions by digital signatures. The database entry to get through the blockchain is wrapped in a coin-spending transaction; therefore, they use their native access management mechanism and authentication mechanism. Each DB entry is natively attached to the address to which it has been published.

In stacks like Bigchain[2] and Amazon QLDB[3], the transaction carries only an instruction (create, update, delete) for DB entry, while the authentication for the transaction is performed in the level of interaction with "validators" (also through public-key cryptography). We can conclude that authorization for pushing DB entries through the ledger to the DB is performed as a mechanism of coin ownership, which is not natively present in the mentioned frameworks. Without this mechanism, it is impossible to transfer the ownership of the DB entry from one address to another. Of course, it can be developed; however, the purpose was not to choose one particular technology but to analyze various technologies' benefits and extract their useful features to develop the database across a bundle of ledgers. Therefore, we refer to

[2] Note, that is coin-less DLTs "transaction" is an arbitrary byte array, see for reference Tendermint specification https://github.com/tendermint/spec/blob/953523c3cb99fdb8c8f7a2d21e3a99094279e9de/spec/blockchain/blockchain.md

[3] In the block example the transaction does not contain user's digital signature, as per the specification the authentication is performed through Amazon ID protocol out of the transaction itself, https://docs.aws.amazon.com/qldb/latest/developerguide/journal-contents.html?fbclid=IwAR2L563qjoUlH72yWM-9-HT39PvSntO9FggMDNtcBfLYmg4AjBPXcbuyRwU#journal.block-example

such technologies which natively include required elements. Also, Fabric and Tendermint also can be used in a bundle of ledgers, though in both cases, the transaction must contain the user's signature of the data, while the user's public key will be used as the address.

b. Key-value format and transaction processing

According to the proposed concept, users insert key-value records into any bundle blockchain using a native mechanism of data insertion of the chosen blockchain. These are not just records, but tokens, because users can own them through their private keys.

Here are basic rules for any cross-blockchain protocol design:

- data published in the blockchain must be compliant with the format, so the scanner knows what to hook into the database upon the bundle of blockchains;
- keys of this database must be unique. The hook collects a new entry if the key has never been published before.
- the protocol connects the entry and the address from which it has been published. This address is considered the owner.
- the owner may publish updates to this entry. The protocol ensures the mechanism of a full-featured CRUD[4] database (Martin, 1983).

The database itself is a standard technology. In this research, we refer to BerkleyDB. The principal difference in using such a database is that the user performs updates not directly in the .db file but through blockchain transactions. First, the user inserts the data in blockchain, and then the protocol if this data is compliant with the initially designed rules, inserts, or updates this record into .db file.

Because it is a standard technology, the database file can play the role of a building block for developing end user-applications.

A simplified scheme of the relation of blockchain and database and entry structure is presented in Fig. 2.

[4] Create, read, update, and delete (CRUD) are the four basic functions of persistent storage.

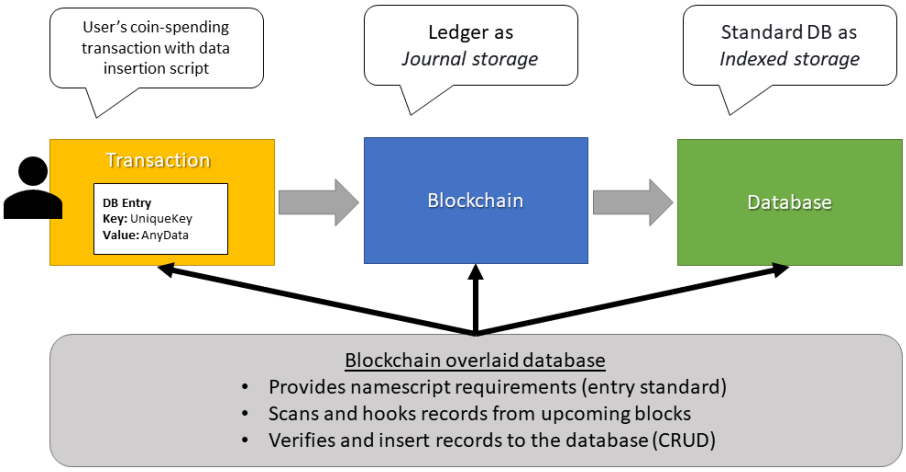


Fig. 2. Relation of blockchain data to key-value database
The system scans upcoming blocks according to the provided format standard and adds records to the database table. The entry may also contain the field which specifies how long this data is valid.

In the first generation of DLTs (Bitcoin and similar), users apply specific scripts and methods to add arbitrary data in a coin transaction (from a few bytes up to around 100 kB per transaction, including the transaction itself, i.e., in Bitcoin (Sward et al., 2018)). As a result of such transaction, the coin itself is "burnt."

In the second generation of DLTs, data insertion may have larger limits or no theoretical limits and are constrained by fees the user must pay for the message size. For example, in Ethereum, data insertion is performed by deploying a smart contract, which is designed as an application to store user's arbitrary data. Combining different types of ledgers in one bundle may require distinguishing common features and approaches, which will be reflected in the data format requirements.

Data format. To insert data compliant with the cross-blockchain protocol, it must be structured in the following elements:

- "*Key*" is a short string that identifies the user's data; it must be unique across the bundle of blockchains. It is a searchable key in the overlaid database. In some systems, it is also called "Name."
- "*Value*" is any arbitrary data related to Key (Name).
- "*Lease time*" is a record which points out the length of time, while the user's key-value record will be valid. The outdated record will be erased from the overlaid database after this block. The initial record itself will be irrevocably stored in the blockchain where it has been published. The lease time element is optional but preferable as it helps to limit the bloat of the overlaid database. But the developer

should consider the constantly growing size of the database and can set up some defaults.

A key-value entry, or particularly an NVS record (as it is referred to Name-Value Storage technology), is attached to a user's address resulting from a blockchain transaction, so this ensures the ownership of a record. Only the holder of the address's private key may update or transfer the record; nobody else can publish the record with the same name while it is valid (while Lease time is valid, or until the user performs a "Name delete" transaction).

Basic transactions. There are three types of transactions:

- **name new** – the creation of a new key-value record; before publishing, the record is checked with the database against its uniqueness; if the key already exists, the user may not publish it; though if the user did previously create it (the owner of the record), it can be updated;
- **name update**, which includes
  - **value update -** the owner of the key can publish the same key and add a new data in the field "Value;"
  - **change Lease time** (reduce or extend); and
  - **transfer** a key-value record to another address, and so transfer the ownership over this record; all these types of updates may be performed in the same transaction;
- **name delete** – the owner publishes the name record with the instruction for deletion; from the block where it has been published, the record becomes invalid. The protocol passes the command to the database to erase the record. Any user may publish the same key from the following block (because nobody owns it anymore).

The concept of a database across a bundle of blockchains is presented in Fig. 3. The example of NVS in action is the following. The user publishes the key "Alice" and Value "+61414739692" to store the record of her public contact unless "Alice" already belongs to someone in the database. Anyone who enquires in their cross-blockchain node "Alice" will see the telephone number which belongs to a specific cryptocurrency address.

Timestamps provide the exclusiveness of keys in the database. Blockchain is a "timestamp machine," which ensures certainty in the chronology of facts (transactions).

The concept of blockchain timestamping is a matter of academic interest presented in several publications (Buldas and Saarepera, 2004), (Gao and Nobuhara, 2017), (Gipp et al., 2015), (Breitinger and Gipp, n.d.) and (Crespo and Luis García Cuende, 2016).

Thus, the Name (key) which is published first in the bundle of blockchains appears in the cross-blockchain database; any other entries with the same keys are rejected; therefore, name squatting is impossible.

Key-value storage is a “raw material” for any sort of monetary and non-monetary tokens, overlaid digital currencies, smart contracts and decentralized applications.

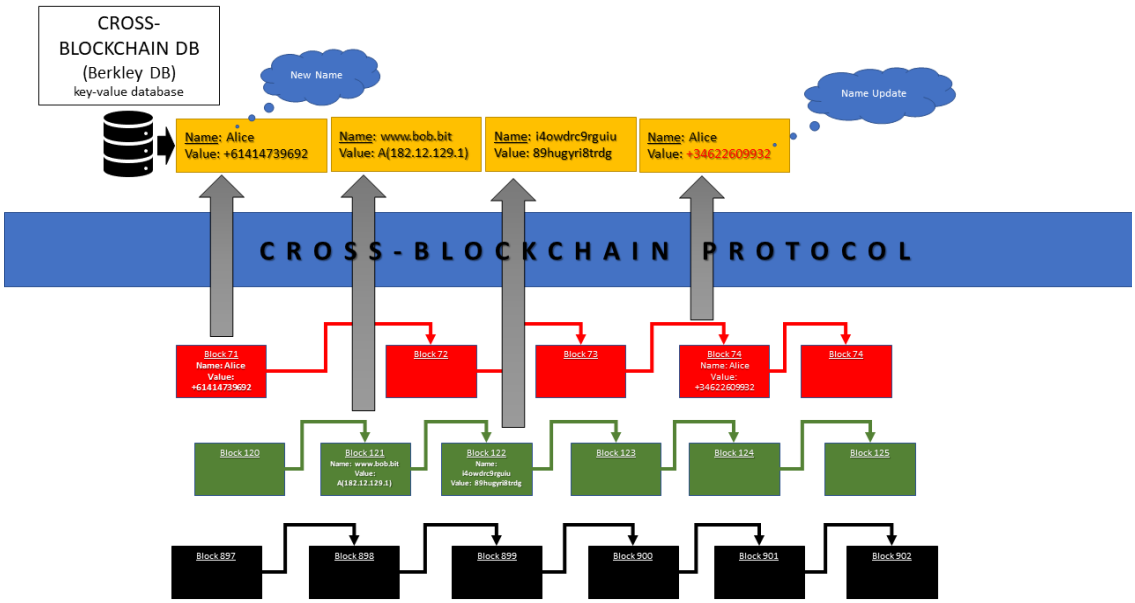


Fig. 3. Cross-blockchain “key-value” database

The scheme presents the bundle in dynamics. The system scans three ledgers: Redcoin (R), Greencoin (G), and Blackcoin (B). When it detects a compliant record, it hooks it up and adds to the overlaid database. The format is simplified; only Key and Value are traced. The hook detected blocks R-71, G-121, G-122, and R-74. Because R-74 contains the key from R-71, it updates the field Value in the relevant database record.

From the perspective of any user, a cross-blockchain database is public storage. Every user who installed the cross-blockchain protocol and full nodes (wallets) of every blockchain of the bundle will obtain a public database copy.

When the user installs the nodes, the cross-blockchain protocol hooks key-value entries from downloading blocks.

When the user requests a key (name), the system retrieves the information from the user’s local storage, i.e., the overlaid database built across the blockchains' bundle. Besides the database's decentralized nature, another advantage is the high speed of interaction because a copy of the database is on the local machine.

We say that the cross-blockchain protocol performs two main functions, i.e., input and output.

The “**Input**” mechanism is aimed to create a key-value compliant transaction, meaning that it must contain all required fields of a new database entry. The key itself

must be unique in the database and must belong to one address, and the protocol accepts it only under this condition.

The "**Output**" tool scans downloading blocks and adds hooked records to the database file, and responds to users' queries to read entries from the database.

Any updates to database records are performed through blockchain transactions. It ensures that the user will not publish a key that already exists, will not capture someone's key (name), and only the owner may publish updates and transfer it.

A standard wallet with integrated key-value storage should have UI and API, which provides the user's necessary assistance to create a correct key-value transaction for the cross-blockchain database.

Nevertheless, as far as public blockchain is an uncensored system, anyone may manually write the transaction code, which will not be necessarily compliant, and send it directly to a blockchain mempool omitting the protocol. Therefore, a non-compliant entry will not appear as the record in the database. This is the major role of the output tool – to build a database as per the rules.

4.2. Setting and Operation of the System

a. How and which blockchain is to include in the bundle?

The cross-blockchain protocol is based on a social consensus, the same as any blockchain protocol at a higher level, is a social consensus: the one who agrees with rules provided by the blockchain protocol installs the node and run it.

In the architecture of a future cross-blockchain database, the first step is to define which blockchains are scanned, in other words, added in the bundle, and how to add and exclude blockchains. Typically, the user will download and install the same software, assuming that the user expresses consent. Once it is installed, the user's node scans through the blockchains applying the protocol, and in the result, creates the database, which will be the copy of the database which every other user has.

Also, another protocol may create an entirely different database using other lists of blockchains or the same blockchains but with other rules and filters.

It is also assumed that the provider of a rightful version of the national cross-blockchain protocol may be the government, and therefore, it can be centralized to some extent. Furthermore, every user may decide to use multiple versions of protocols, including those provided by the government or any other community.

The development of a bundle is limited in the available disk space. This limitation has a significant practical meaning, as many blockchains tend to bloat and reach hundreds of Gigabytes. A bundle of blockchains to work property must constantly be running in one node. Storing large data is a barrier for ordinary users. Therefore, the number of blockchains for the bundle will be limited with the current limitation of the disk space with the projected growth margin.

b. Initialization of a bundle

There are different types of blockchain protocols, and each may have different data insertion mechanisms, which are discussed above. If the blockchain supports the Data Format and Basic Transactions described in the previous subsection, such blockchain can become part of the bundle.

For better user experience, the blockchain wallet (node) should provide user-interface and API for data insertion complaints with the format and ensure that the user will not publish a key published by someone.

The criterion for choosing a blockchain for a bundle is reliability. A PoW network with three nodes is less resistant to an attack compared to the network with three thousand nodes. Today, there is no golden standard of blockchain security. Therefore, any decision must be empirically and expertly motivated.

The issue of network reliability is the subject of a separate study beyond this paper's scope. However, we show which approach should be taken to automatically and independently diagnose this work's reliability.

c. Exclusion of ledgers and rescue of names

The cross-blockchain protocol must be able to smoothly exclude on the run any blockchain that becomes unreliable from the bundle. The same action must be performed by all nodes of the system; otherwise, nodes will have different versions of their databases. The algorithms of exclusion and security criteria are defined during the initial set-up of the protocol.

The system should not receive metrics that trigger the exclusion from any third-party source, except the blockchains themselves, since we strive for decentralization as the fundamental criterion of reliability.

However, in the following section, certain centralized scenarios are also explained.

A decentralized system works as follows. Each cross-blockchain node collects data from included blockchains for analysis. A blockchain network is indexed in the bundle while it meets the security threshold. Eventually, any running node will locally calculate these parameters and automatically exclude the network from indexing. Hence, every cross-blockchain node will apply the same algorithm, and it will end up with the same copy of the database across the bundle.

For PoW, this parameter can be difficulty/hash rate, number of nodes. For PoS, such a parameter is PoS difficulty, among others. However, the security level is never enough, and there is plenty of room for further research and development.

When the cross-blockchain node detects a threat, it stops indexing jeopardized blockchain from the relevant block.

It is important to note that this exclusion happens not in the case of a hardfork and a roll-back attack (hardfork with rewriting the history deeper than the typical wait of confirmations); these issues are discussed in the next subsection.

After excluding a blockchain, all records till the block of exclusion remain valid in the database and are available for reading. However, they are not admitted to normal transactions, i.e., name update and name delete become impossible. The dropped

blockchain user can transfer the name from this blockchain to any other blockchain of the bundle.

The proposed concept of security leaves space for designing systems with different parameters. Here is one example. The bundle includes a few blockchains which have PoW and PoW+PoS consensus. The criteria for reliability for PoS and PoW are their dynamics of difficulty. If average difficulty decreases say twice, nodes drop such blockchain. The difficulty is calculated periodically for each bundle blockchain, taking the longest period of difficult recalculation among blockchains in the bundle. For example, in Bitcoin, the difficulty is recalculated every 2016 blocks (approximately two weeks); in Ethereum, it is dynamically recalculated so that on average, one block is produced by the entire network every 12 seconds ("Mining - ethereum/wiki Wiki," n.d.).

d. Adding on the run

Once chosen and built, the cross-blockchain system may require adding blockchains in the future. The main issue here is choosing the block to begin indexing from. This question is also relevant to initiating any new cross-blockchain protocol: from which block to start scanning if the blockchain is not new.

When a blockchain (which is running a while) is added in the bundle, rebuilding a database from the very first block may lead to a logic conflict with ownership. If one of the records already exists in the added blockchain but was created earlier than the one in the current cross-blockchain database, a new re-indexed version of the database will re-assign it. Thus, the owner of the record will lose control over it in the new database.

A better approach is to index a blockchain from the current block when it is being added. Hence, the reallocation of ownership is excluded.

e. How to transfer a name between blockchains

The name record can be transferred from the dropped blockchain. For better user experience and competition between existing blockchains, the user should also have this transferability in running blockchains.

A user of a blockchain may transfer the record to any blockchain in the bundle. The user signs the string [record key + challenge] with their private key from the dropped network and then publishes this key in another blockchain. The system will see that someone is trying to capture the record, which already exists in the database. It will verify the digital signature, and if it belongs to the original owner of the record in the dropped blockchain, it will update the entry in the database.

The "challenge" is needed to exclude attempts of non-authorized capture of records. The owner could sign the key in the past for various reasons. Thus, the attacker could obtain the signature to reuse it. To exclude this, the owner signs the key with the ID of the latest block:

```
priv_key (record_key, latest block ID)
```

Transferability of assets between blockchains is one of the most fundamental ideas of the cross-blockchain protocol because it supports competition between blockchains, leading to a better quality of technology and services.

f. Local Name-Value Storage vs. Cross-blockchain

Another issue of better design is the relation of a local and cross-blockchain key-value storage.

Any blockchain may have its key-value storage even before it becomes a part of a cross-blockchain protocol. For example, Namecoin has NVS database to run TLD (Top-Level Domain) *.bit, Emercoin runs NVS as a public database for general purposes and maintains four TLDs (.coin, .emc, .lib, .bazar).

It is possible that names in one blockchain, when added to a global bundle, may conflict with other blockchains. Therefore, it is better for the system's design that the local NVS running in parallel with the cross-blockchain database will prevent (or at least notify users) from publishing conflicting records.

g. Name squatting protection

Namecoin designed the squatting protection for their system. When the user publishes a Name (key), it becomes available publicly in the mempool before publishing in the blockchain. In PoW, users can compete for the priority of a transaction by proposing miners a higher fee. The attackers can try to push the same name first after they have seen the name in the mempool by proposing a higher fee to capture it.

For that reason, Namecoin designed a two-step publishing protocol (Loibl, 2014): (1) publish the hash of the name; then (2) publish the name itself.

In Emercoin, the queue is ordered chronologically, and fees, although proposed, are burned instead. The miner/minter gets no fee from the user.

Cross-blockchain must be designed in the way to accommodate both models. For blockchains, where easy squatting is possible, there should be two steps.

When the squatter is a miner, there is no simple solution because the miner may shuffle the queue. However, if the system design does not allow cheating, squatting is just a free-market competition for who registers the name first. It is recommended to use a two-step protocol in all cases, propose higher fees and publish a new name simultaneously in all blockchains of the bundle; it reduces the chances for a squatter to capture the name. Once a new name is published, it is impossible to capture it in future transactions.

h. Database

The choice of appropriate technology for the database is an essential step in designing the cross-blockchain system. It may be unreasonable to create a new technology for the database; the market proposes an extensive choice of reliable solutions.

Under the hood of Emercoin’s Name-Value Storage is Berkeley DB (“Oracle Berkeley DB,” n.d.), an Oracle’s key-value database. Initially, many elements of the

Bitcoin system relied heavily on Berkeley DB. Subsequently, in version 0.8.1, developers migrated to LevelDB (“GitHub - google/leveldb: LevelDB,” n.d.) to store transactions and block indices but left “wallet.dat” on Berkley DB (“Bitcoin-Qt version 0.8.1 released,” n.d.).

There might be reasons to choose one or another solution (LevelDB, Redis, among others) or a database from SQL family, depending on the specific project's needs. It is noteworthy that the database is the fundamental part of the software.

Furthermore, since we create the cross-blockchain database for applications, the database's choice should match the needs of further development.

A high-level design concept is presented in Fig 4.

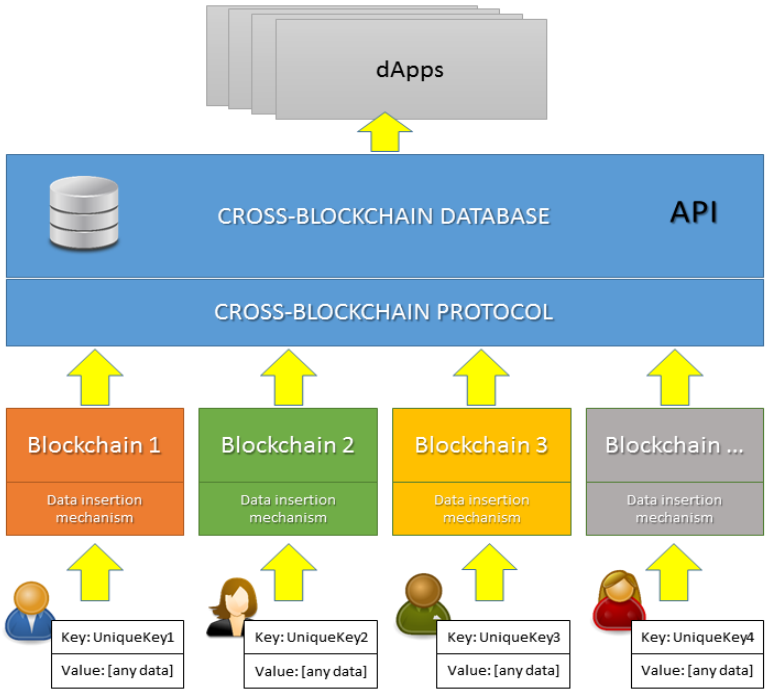


Fig. 4. Cross-blockchain protocol scheme

The scheme presents a more general view of the bundle interaction. Users may choose any ledger in the bundle to publish records. The protocol creates a database of user’s entries across these ledgers. The database is used to develop decentralized applications.

Blockchains towards the database play the role of the channel through which users insert and manage data.

Cross-blockchain database has CRUD features, but removing and updating blockchains is impossible because they are performed through blockchains. They are immutable logs through which CRUD commands are passed and performed in the database.

The second important role of the blockchain is a mechanism of ownership because records are attached to their users' addresses. Through the native blockchain mechanism of addresses and private keys, database records are managed and transferred between users as tokens.

The cross-blockchain protocol ensures the connection of blockchains in the bundle with the database.

To make sure the record gets into the database, data insertion accompanied by protocol format, for instance, key-value record entries, will require the user to fill in the relevant fields and other designed format requirements.

The system checks against the database's uniqueness; if the key exists in the database, the system ensures that only the address's owner may publish an update. The entry is packed in the blockchain transaction and published in the chosen blockchain if the rules are followed.

In the result of data insertion in the blockchain, the entry gets into the database It makes no sense for the user to change or somehow omit the protocol's algorithms in their local machine, trying to publish the name that someone already owns. Even the user does this trick by pushing the name up to the database. This version of the database will exist only on the user's machine, while all other cross-blockchain nodes will have the normal version. This is a social consensus mechanism, i.e., users install the protocol, resulting in the same local copy of the database.

The database may be used for developing various user applications. Since DB is local, the interaction is instant, which makes the development of heavily loaded applications possible.

4.3. How to chronologize the index

This section discusses the inaccuracy of time in blockchains compared to each other and astronomical time, the possible consequences of hardforks, and roll-back attacks and variants of the system design to address these issues.

a. Inherent issues of blockchain to be dealt with in the bundle architecture

Let us define and evaluate issues to be dealt with in a cross-blockchain architecture.

Mistiming. Timestamps in each blockchain are not necessarily accurate to astronomical time. It happens because a node that closes a block includes a timestamp based on its current time, which might be inaccurate Usually, two protocol limits are applied here: a block cannot be earlier than the last block and 2 hours ahead from network peers' median time. This rule is relevant to Bitcoin and many other similar systems, though these parameters are specific to a blockchain platform ("Block timestamp - Bitcoin Wiki," n.d.).

Orphan blocks. The longest chain of blocks is accepted, and shorter is dropped out. Nodes compete for finding new blocks, and this kind of fork happens each time whenever any node presents a correct longer chain to the network. If not addressed in

the system's design, it will create the problem of a forked database because the cross-blockchain protocol does not re-index the whole ledger when a new block arrives.

Hardfork. Let us separate a retroactive “roll-back” attack in another category. Here we consider a hardfork that is not a result of the attack, but a conscious and willing decision to change the blockchain protocol. The nodes that did not switch to a newer protocol will see incompatible blocks that will not accept. The minority may create their network by forking. Two versions of the blockchain will have the same history of blocks till the block of the split. After that, users will have the same amount of cryptocurrency, the same tokens, and smart contracts in both networks. The protocol will not know about the parallel network. That is a solution itself, however.

Nevertheless, it is assumed that the community may wish to include the fork to the bundle. Is an automatic inclusion of a forked network for indexing possible? The solution must address logic collisions when two records in different blockchains represent the same asset.

Retroactivity (roll-back). Even though some DLT systems may be designed to allow retroactivity as a legitimate feature, we assume that the immutability must be preserved as the major advantage. Therefore, we consider a roll-back as a form of attack, causing a hardfork of the database in the cross-blockchain bundle. The running node will not notice a history change because it does not re-index from the beginning of the database each time a new block arrives. Suppose the record belonged to address A in the original blockchain, and in the result of retroactivity, it was re-assigned to address B. In that case, the database will still contain the record of the entry attached to address A. At the same time, when a new node is installed, or the old node starts re-indexing, it will create a new database file with the key attached to address B. Therefore, new and re-indexed nodes will have a forked version of the database, while old nodes will have the original one.

Let us discuss possible solutions and evaluate their applicability.

b. Assumption of time inaccuracy

Inaccuracy may create some negative user experience. For instance, in green blockchain (see Fig. 5), the miner finalizes the block with the timestamp that is 02:12 ahead of the current astronomical time. In red blockchain, the block is closed 19 seconds earlier than the astronomical time. If the same records are published there, they will be accepted only from the red blockchain, though they are published at the same astronomical time. Technically, even though they happened simultaneously according to the astronomical time, the red one comes first, which is compliant with the protocol.

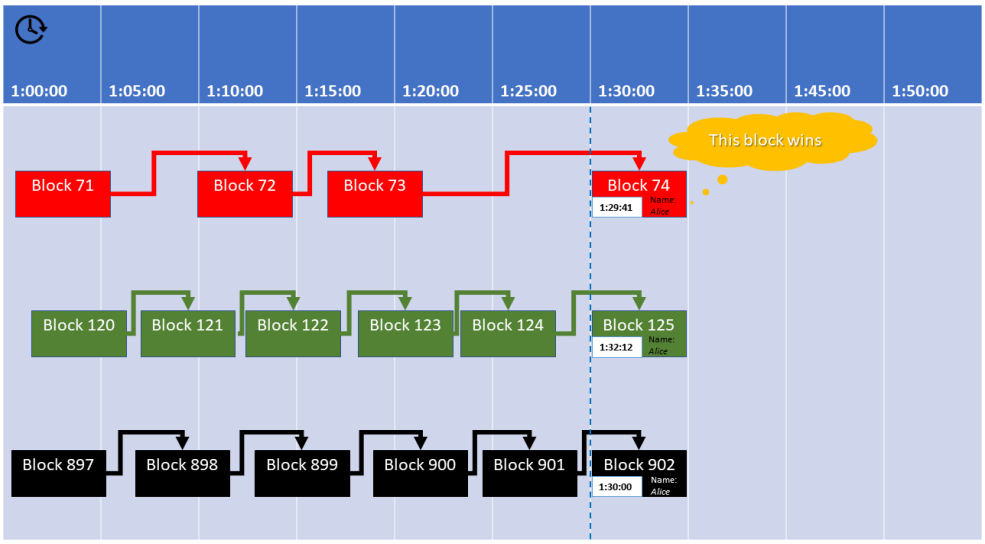


Fig. 5. Mistiming of key publication

Three transactions happened simultaneously as per the astronomical time, at 1:30, but each network has time discrepancy; therefore, the red chain is taken first (19 seconds earlier).

Publication of the key at the same time can also be an issue. However, even if it happens, the node will compare timestamps of transactions in blocks and will select the one which is earlier among the blocks. However, there will always be a possibility that the node will obtain two or more competitive records with equal timestamps among blocks of different blockchains. The system must have an algorithm to resolve this collision. One of the possible scenarios is to refer to the same logic of a choice of blockchains in the bundle. As we already discussed, the security can become such a criterion based on each blockchain's difficulty/hash rate and coefficients that will be make these figures comparable. Inevitably, we will need to introduce and justify a rating of blockchains in the bundle as per their credibility. This rating can address the collision of timestamps, choosing the record in the higher blockchain.

Time inaccuracy is a natural limit that cannot be resolved in a cross-blockchain index without either centralization or changing each blockchain's protocol to provide for cross-blockchain time synchronization. Because such changes require hardforks in existing blockchains, they may become infeasible due to their decentralized nature.

Therefore, it is proposed that time inaccuracy will be the assumption users must accept. Free market competition will demand blockchain communities to provide for better services and user experience. If the record is valuable, the user may wish to send the same key simultaneously for the registration in all blockchains of the bundle, thus competing with themselves. Once one transaction arrives first in the blockchains, the user may wish to transfer it to that blockchain where they want to manage it.

c. Orphan blocks

The cross-blockchain protocol solves the orphan blocks' problem by pending a few blocks after the record was published. This period is called “confirmations,” and it is specific for different consensus; for example, in Bitcoin, 6-blocks are the reasonable time that reduces the probability of the fork (“Confirmation - Bitcoin Wiki,” n.d.).

Therefore, in the cross-blockchain system, each blockchain will have its pending time, and the protocol is tasked to add records to the cross-blockchain database after this quarantine.

d. Hardforks

Hardforks are different from just orphan blocks due to how they create two sustainable independent networks. One will be the majority, and users will typically see this branch of the network. If the minority is organized enough, they may establish a new network. Till the block of the hardfork, two networks have the same blockchain history. However, from the next block after the fork, all assets can be independently moved within the new blockchain, thereby creating double-spending.

To address this issue, let us define the scenarios of a hardfork.

(1) The majority of nodes do not change the current protocol, only the minority buds off with a new protocol incompatible with the current. In this case, it is not necessary to do anything. The fork will exist as Elusive Joe; unless the mainstream community wishes to include it in the bundle.

(2) Inclusion of a minor fork may happen in the following way. Beforehand the hardfork miners will put flags in blocks for the future fork, announcing to the community the number of the block from which the fork will happen. The protocol detecting the threshold of flags (say, 10% of nodes) will require the user to explicitly include this blockchain as a new one in the bundle.

(3) To resolve the issue of duplicating keys, the protocol will apply the following rule. Until the user stops making any transaction in the bundle, doubled keys do not constitute a problem itself; they can exist in parallel at any time. The user may decide to transfer the record or update it in any of the blockchains. The transaction which happens first among two blockchains will be accepted in the protocol, and from that moment, any other transaction in the parallel blockchain will never be approved by the protocol.

(4) If the majority is going to move to another protocol, the community will also use flags. When the system detects that the majority will adapt to an incompatible protocol, the protocol will stop indexing the blockchain, and then ask the user for explicit consent for the new version of the blockchain in the bundle. This scenario can be combined with both blockchains' accommodation described in (2) and (3).

In both cases with flags, the system requires the user’s consent; otherwise, the protocol stops running the bundle in the user’s machine, thereby preventing the cross-blockchain database forking.

e. Retroactivity

Retroactivity can cause the reallocation of ownership of records in the blockchain locally, and capture records from other blockchains of the bundle.

There are two specific issues to address:

(1) the node does not know on the run of a deep reorganization of blocks in the blockchain. Technically, this is still a legitimate behavior. Here, it applies the rule of the longest chain of blocks. When it is presented to the network, nodes automatically pick it up, replacing the current chain. Because the cross-blockchain system does not re-index database, changes in ownership that happened due to this attack will not be reflected. That might be a solution itself; but

(2) When a new bundle is installed, or the same bundle is re-indexed from the very beginning, the resulting database will reflect changes resulting from the attack.

Therefore, in the result of retroactivity, some community users will have one version, some users another.

Before discussing the possible solutions, let us define the probability of this attack.

The fault tolerance of the bundle is defined by multiplication of probabilities of the attack of all blockchains of the bundle, because the failure of at least one blockchain in the group may lead to the failure of the whole bundle:

$$P = (1- (1-p_1) (1-p_2) (1-p_n)) \quad (1)$$

However, the mathematical expectation of the attack for a bundle can be 0. Therefore, statistical methods may not be helpful.

Thus, we keep this in mind as a theory. To implement any system based on this concept, it will be a good practice to remember that there are no perfect systems, and all reasonable measures must be considered.

More important than the level of resistance to attacks is the ability of the system to restore after the fault. Thus, let us define some measures that can be designed to address possible retroactivity issues.

Retroactivity in one blockchain may compromise the overlaid database because it relies on the immutability and the chronological order of blocks. For example, an attacker deletes someone's transaction in one blockchain and publishes a new transaction in any other blockchain of the bundle with the same key-value entry. In this way, the attacker can capture this asset. Furthermore, such an attack will lead to a hardfork of the bundle, i.e. one part of the nodes will stay with the old version of the database, another part (those who just have installed the bundle or reindexed it) will have the attacker's version of the DB. The general strategy here is to localize the attack and not to let it harm the other segments of the system. In principle, four actions must be taken:

1. Any node in the network must independently detect an attack.
2. The node must detach the fault blockchain from the bundle.
3. A new or re-indexed node, must define that there was an attack and be able to build an uncorrupted database across the bundle.
4. The node must support the transferability of records from the fault blockchain to any blockchains in the bundle.

Here is the solution.

(a) The running node will define retroactivity as a legitimate feature because it applies the longest chain rule. It is proposed to add heuristic analyzes at the level of the cross-blockchain protocol. It will keep blockchain headers' state and compare them to detect changes that happen deeper than a normal reorganization of blocks (see “Orphan forks”).

For instance, for Bitcoin, the norm will be the change up six blocks in depth. For each blockchain, this figure will vary. When the system detects an abnormal fork, it defines the fork's depth by comparing two states of headers and marks the blockchain excluded from this block and continues indexing other ledgers of the bundle. When the attack is detected, it is also recommended to backup the database. An automatic backup must happen when a new version with the chain of blocks deeper then *n*-blocks appears in the node. As a result of this step, the running system will preserve the original state of the database and detach the faulty blockchain from further indexing and continue working.

(b) To detect corruption when installing a new node/re-indexing, an approach of redundant copies can be used, similar to RAID massive, see Fig 6. Existing methods for data storage among multiple drives are relevant to the name-value storage. RAID has different methods. For example, in the cross-blockchain protocol with RAID 1 (Jones and Dawkins, 2009), the user will store the name in two or more blockchains. If one blockchain is attacked, when re-indexing the system, the node will detect the collision at some block using analysis of RAID collisions.

(c) The publication of a RAID record must contain the signatures of the [record_key+challenge] from the parallel blockchain. The pointer to the highest block will help to detect the exact height of the blockchain attack. From this moment, the system will detach the blockchain from indexing, allowing the possibility to retrieve records from the faulty blockchain by a transfer to the rest in the bundle.

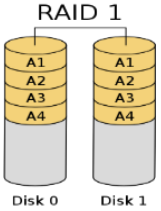


Fig. 6. RAID 1
Basic RAID 1 scheme with two storages where data is duplicated.

Because the probability of a successful attack of two blockchains at the same time is significantly lower, RAID methods may create enough protection. The more redundancy, the lower are chances of the fault of the cross-blockchain database.

5. Evaluation of the invention or why does the cross-blockchain protocol suit governments?

This section evaluates how the cross-blockchain protocol addresses the issues defined in Section 3 and corresponds with the initial goal of developing a system that suits government purposes, i.e., to run, for example, property registry using various public blockchains. It consists of two subsections: brief evaluation (5.1) and extended discussion with scenarios (5.2).

5.1. Brief evaluation

Hardforks are addressed by filtering duplicate assets after a hardfork. The protocol must contain rules to define which record the user updates first after the hardfork. Hence, the duplicated record in the parallel system is not traced anymore.

Two complementary solutions address immutability and the ability to enforce lawful actions: cross-references validate records, and trusted addresses could patch the protocol.

Each of this element inside has various scenarios which are further discussed. Here are basic examples: Alice creates a record that represents her property rights (token). In the token, she writes who validated it, literarily, who says that this token represents her property right, say, land title. Let it be Bob. Bob creates his key-value record, which says, “Alice’s token is valid.” While Alice controls her private key, she can perform transactions with her asset. If Alice lost her key, she would ask Bob to update his record, that her token is not valid anymore, and re-issue a new token.

Bob may also update the record in case of her death, or based on a court decision, etc. One asset may have multiple references to such trusted third parties: land registry, notary, court, land surveyor, local government, building inspector, etc. Invalidation provided by any of these authorities may trigger some logic in the system. The logic itself must reflect legislative norms and government structure of the jurisdiction where this system is implemented. That is why this system is called “smart laws.”

The second level is an “emergency brake.” It is obvious that Bob is part of the public body. Bob’s authority is validated hierarchically by someone higher, using the same method of cross-references. This system reflects a real-life public office, which has an appointment and dismissal procedure.

We eventually come to the root record, or multiple roots (because of separation of powers). If Bob [the authority] abuses his power, the court, another authority that has no interconnection with Bob’s root, may *patch* the protocol.

Root address(es) must be pre-installed in the user’s bundle. Each root record may have its specific role and power, i.e., an authorization of what it can do and what cannot.

Therefore, the court publishes the record, which says the system “Bob’s authority is invalid.” The court may also publish a new rule for Alice’s token. Because the user’s node trusts the court’s address (as we mentioned, it was pre-installed), it hooks this patch and applies new rules. Hence, if Alice’s is stolen, it will be invalidated. Bob

will lose its authority. Of course, this is a simple example; the system may contain collectively managed addresses (multi signatures). The system may have e-voting (e-referendum) mechanisms directly on blockchain. There is still a possible solution when the government announces off-chain (for example, by publishing in the Gazette), which address (root) is valid/invalid. And finally, each person reserves the right to exclude the "root" if he or she does not trust the government anymore although it does not influence other nodes, as they all act independently.

The advantage of such a system is that all records, including patches, remain irrevocable at the level of blockchains. Any digital dictatorship can eventually be thrown. All blocks are rescanned from the beginning with new fair rules and filters that rebuild the database.

To address the issue of digital identity, a similar way of cross-referencing is proposed. Alice creates her token that says she is Alice, Dave (trust service provider) creates his token where he says Alice's digital identity is valid. To address the issue of privacy, it is advisable to not publish any personal data on-chain. Various methods and frameworks may be applied (see the next subsection) to publish only cryptographic fingerprints and store personal data off-chain.

The cross-blockchain protocol addresses the problem of scalability and price volatility. The bundle of blockchains together can have a good performance if the government does not decide which blockchain to use but the user. The user can also transfer the asset from one ledger to another within the bundle. These mechanisms leverage fair market competition of technologies and services. If at some point in time one ledger is overloaded with transactions, fees will rise in this blockchain. Unsatisfied users will choose other ledgers in the bundle, with better performance and suitable fees.

5.2. Why does the cross-blockchain protocol suit governments?

a. Hardforks

Nowadays, the land authority exclusively maintains one legitimate version of the registry. In different countries, they may have different names and specializations (cadastre, land title registry, real estate registry, among others). Still, the purpose is the same: to provide certainty in property rights by tracking records of transactions (title deeds). Besides land titles, there are registries for movable properties (cars, boats, aircraft, etc.), shares, other securities, and corporate rights.

The use of any decentralized system, including the blockchain, was limited because it could create registry forking issues. A case where the government points out which blockchain is legitimate, for example, Bitcoin or Bitcoin Cash, Ethereum or Ethereum Classic, is unlikely to be accepted. Why would anyone use a decentralized system but end-up with the central authority? It disables competition between blockchains.

The cross-blockchain protocol addresses it with a free choice for users. The proposed protocol may support both blockchains after their fork. The same as

Schrödinger's cat, the record has a dual nature until the user chooses. Having two records is not a legal collision; it becomes so when the user performs two different transactions with the same record in different blockchains of the bundle. Therefore, the protocol ensures that a user's choice is irrevocable. Once it is done, they will not perform a conflicting transaction in the second blockchain. Hence, with the properly designed protocol of the bundle, the hardfork is not a problem anymore.

b. Immutability, trusted third parties, and governance

Blockchain immutability is considered as one of the major advantages of blockchain technology. The transaction records and inserted data are irrevocable and immutable. Since the blockchain was invented, the discussion of its use for state governance is open, especially towards property registries.

In the previous subsections, we discussed the example when the key-value record represents someone's property rights; for instance, the land title.

The record is worth nothing unless there is a certainty that it has a legal connection with the real-world asset. With the cross-blockchain database, it is possible to create an ecosystem of trust, where records refer to other records certifying them.

For example, Alice publishes her land title record. Bob, a town clerk, creates his record to certify that Alice's record duly represents her land title (see Fig. 7).

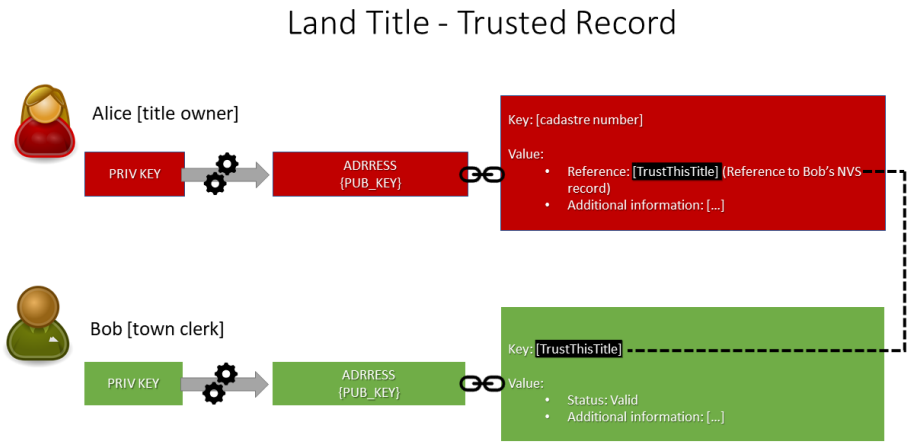


Fig. 7. Scheme of trust services

Alice included in Value the reference to Bob's record with the key "TrustThisTitle" (read, any valid key). Bob's record says that Alice's record is valid. Alice used Redcoin, Bob - Greencoin. Because they are in the bundle, the system may resolve an inquiry on Alice's token's validity. It searches the database for the key [cadastral number], and parses it to find a reference. When the reference [TrustThisTitle] is found, the system searches it as the key to the database entry. When [TrustThisTitle] entry is found, it parses its value to find the status "valid." Because we trust Bob, he is our town clerk, we trust Alice's record representing her property right. Land title is used here as an example. Any property rights and facts can be certified.

To buy Alice's land, Charles needs to acquire her record. Charles will search Alice's record in the cross-blockchain database and will find in this record the reference to Bob's record. The system will check Bob's statement, which certifies Alice's asset. Charles trusts Bob; hence, Charles can trust Alice's record and make a title deed even without meeting her in person. The parties can do an atomic swap: Alice will send him the title record, and Charles will pay cryptocurrency in return, so they do not need any intermediaries. It is just a brief illustration of the possibilities. Having titles on a blockchain, parties can use smart contracts' full power to design transactions of any complexity.

The proposed scheme of cross-reference certification suits any real-world facts: immovable and movable property, digital identity, facts of life (birth, death, missing, etc.), contracts, for instance, acknowledgment by a notary public (for civil law countries), facts of some events (force majeure, etc.). See Fig. 8.

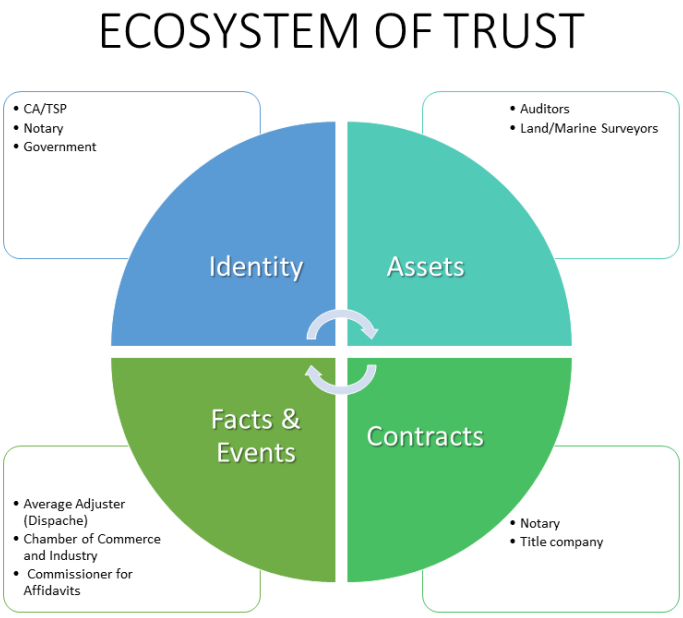


Fig 8. Map of trust records and trust providers

The map shows examples of how third parties in real-world cases certify identity, assets, contracts, facts and events: Identity by Certificate Authorities or Trust Service Providers (EU), by a notary public and different government agencies. Auditors, land and marine surveyors verify assets. Contracts can be certified by notaries, land title deeds by title companies. Facts and events by Dispache (a person who certifies claims, especially for marine insurance), by Chamber of Commerce and Industry the origin of products and force majeure events, Commissioner for Affidavits certifies witnesses' declarations and statements.

It is impossible to completely get rid of trusted third parties, at least at this level of science and technology. Trust records address the problem of credibility. An intermediary is a "necessary evil," especially in growing digitalization and remote relationships.

Without commercial intermediaries and governments, relations would have looked like scenes from gangster movies where the seller and the buyer need to meet personally and show each other the money and product to make the deal. The progress required more effective economic forms. According to Potts et al. (MacDonald et al., 2016), the current U.S. GPD consists of 33% of services produced by intermediaries.

If Alice lost her private key in the proposed scheme, she cannot sell her property anymore. She may ask Bob to update his record specifying that Alice's record is not valid anymore.

Digital identity. Likewise, a conventional Public Key Infrastructure (PKI), the cross-blockchain database can store certificates of digital identity. There can be a root record at the government level, which will enable multilevel hierarchical trust interaction. For example, if Alice's and Bob's keys are compromised simultaneously, Bob's upper validator will mark his record invalid, and so on, going up to the root record if needed.

The scheme also accommodates two/multi-factor authorization (2FA/MFA) and hardware devices for signing transactions, for instance, hardware crypto wallets.

For 2FA/MFA, Alice will ask a trusted third party to send a "challenge" (secret phrase) using a closed trusted channel established during initial identification, which she will sign and include in the transaction as proof. At the same time, the trust provider will publish the hash of the secret in the cross-blockchain database[5].

To protect the private key from a theft, Alice will use a hardware wallet. For example, in the EU, such a protection level is necessary to have a non-reputable[6] Qualified Electronic Signature, as per eIDAS regulation (Council of the European Union, 2014).

The government may keep the "root" of trust, the record which is used to sign certificates of trusted third parties, also known as "Certificate Authorities" and more specifically for eIDAS "Trust Service Providers."

Such identity and trust services, even though they require third parties, are not necessarily highly centralized. Opposite to a single root record, there can be multiple roots and self-signed certificates of numerous third parties. Alice, as an end-user, decides whom she trusts, creating her white list of credible entities, including government root, commercial providers, or even her circle, similar to the concept of "web-of-trust" (Heinrich, 2005): Alice trusts Bob, but does not know Charles, Bob trusts Charles, therefore, Alice trusts Charles. See Fig. 9.

[5] This is one of many possible 2FA/MFA protocols as an example.

[6] A signature for which the signatory cannot deny that they are the originator of such a signature (as per eIDAS regulation in the EU).

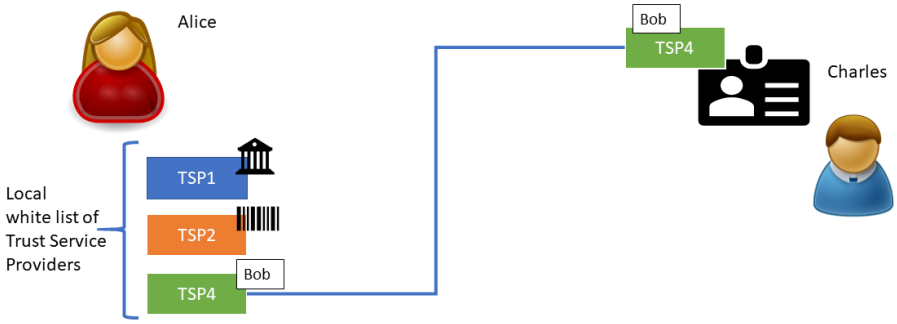


Fig. 9. Multiple TSP providers

Alice can create her list of trusted addresses in a decentralized trust scheme that belongs to the government, a commercial trust service provider, and Bob (web-of-trust scheme). Because she trusts Bob and Bob certified Charles' digital identity, Alice can trust Charles, even without knowing and meeting him personally.

The truth source is in the sequence of published key-value records where the latest record represents the current state of affairs (valid, invalid, revoked, compromised, stolen, etc.). This is the first level of overcoming the immutability where the blockchain plays an important role because no record can be voluntarily altered or erased, and all the history of transactions is preserved.

Jurisdiction as a filter. However, what if the root is compromised? To address this issue, the system will use patches.

The bundle's output mechanism can be considered as a filter. In the discussion above, we proposed "timestamp" as the main rule for filtering records. The bundle ignores repeating entries, adding to the database only first found unique assets and then tracks updates to these records.

If we look at any jurisdiction as a kind of filter, the laws will be these filtering rules. We normally call "legal" (as per the law) not filtered in the system and shown in the database. In this way, legal norms and procedures can be digitized and applied to transactions.

The smart laws in the cross-blockchain protocol are the rules which have at least two elements:

(1) Cross-references, when one record (authority) validates another record (asset, digital identity, fact, or contract), this level does not influence the database records; it is a logic how to resolve queries to records based on their references in the database; and

(2) At least one trusted root address initiated in the bundle as a "digital authority," which may publish records in a ledger considered in the system as *protocol patches*. The patch will contain a command (a new rule) for the database; the system will apply the patch to update the database by deleting existing records,

including the record which exists at the level of a ledger but not included in the database or ignores some address.

Both elements can be much more complicated based on the existing intricacies of political systems and regulations.

If the root record is compromised, the cross-blockchain authority must reset the trust using one of the proposed scenarios:

- Distributed (unstructured social consensus) – users will arbitrarily install root address(es) and accept patches; though it may lead to multiple hardforks of the cross-blockchain database, different communities which stick to different roots will see a different state of affairs in their databases.
- Centralized – patches are published from the trusted address (or addresses), initially provided in the system. The patch is automatically recognized as authorized instructions and installed by the system, but if the root is compromised, the authority announces it invalid off-chain. Users to have a legitimate version of the database will have to install a new root address and reindex the bundle. Normally, users will download a new version of the cross-blockchain software from the official website.
- De-centralized (collective control over the root address) – The patch is initially created in the system, with a blank Value, and controlled by a multi-signature scheme. A user's system accepts updates of the field Value where patches are published based on a collective decision in the multi-signature scheme.

It is considered that in the future, direct e-voting on the blockchain with automatic implementation may also be designed to address the issue of decentralized governance in large-scaled online systems. The combination of these methods can make the system more sustainable.

Also, many other cases are possible in a "smart law." For instance, Alice died, and Charles has the right to inherit her record. When Alice designed her "smart will," she could not know which notary would fulfill her will, even if she specifies all licensed notaries in the country, by the time of her death, it might appear no notary can execute the smart will because the list is not valid anymore, for example, because of the root reset.

In traditional "paper" bureaucracy, Charles will apply to any notary to issue a record of inheritance that grants him Alice's title right; the only thing that matters here is that he has to choose one by the time of application of the existing authorized notaries. Even if Alice designed her will to perform execution automatically without any notary, this similar issue would still arise. Who will certify her death to trigger self-execution of the will?

Even if Alice assigns a redundant[7] list of trusted third parties with such authorization, they may still have legal issues that will lead to the impossibility of running successfully without violating someone's rights. For example, if Alice leaves everything to Bob, Charles may claim that his rights are violated. If the parties do not

[7] Redundancy is not the best option. If too many people have access to her assets, it may decrease security.

agree in the dispute, Charles has the right to take it to court. How and who will enforce justice in such a system?

Finally, if Alice did not leave any will, someone must apply the general norms of inheritance law.

Hence, the system needs authorities, i.e., lists of authorized addresses (notaries, registrars, judges, etc.) and the relevant procedures. The blockchain can be used to improve and automate bureaucracy. Procedures can be designed in a more transparent and accountable way. Such automation can be done using closed centralized systems that are widely used by governments nowadays; the difference is that blockchain provides a decentralized infrastructure.

In a centralized system, there will be someone who controls it, this is a sticking point. In blockchain, even if some applications are designed in a centralized fashion, it can be decentralized step-by-step in the future; this is impossible in a centralized system.

The governance system has two elements: the “authority,” which is the list of addresses of public bodies, and “smart laws,” which are algorithms that define how the government may act.

Government addresses, according to their authorization, may perform some actions in the protocol. For example, the judicial system addresses are in charge of issuing individual patches for records in disputes. If Bob illegally seized Alice’s record, the court will issue and disseminate a patch in the system according to which this transaction is ignored. Therefore, Alice re-issues her token again.

Patches themselves are disseminated among nodes through key-value transactions; the authority publishes specific records, providing rules for nodes for reallocation of records. Therefore, all actions of authorities are recorded and hence, are accountable.

Each node in the network hooks such records, verifies if they arrived from any authorized address, and applies to the cross-blockchain database's current state.

This allows addressing all possible issues of the blockchain immutability: lost keys, deaths, hardfork doublings, contract breaches, and misappropriations.

This kind of scenario requires a certain level of trusted third parties’ involvement. Nevertheless, we can consider the cross-blockchain protocol a sort of public consensus, a social agreement since each user voluntarily decides to use this system on their own and also agrees with this. If they trust the government, they apply these algorithms.

A purely voluntary model may not be scalable though; it will probably work in small communities. Therefore, to extend the system but not to jeopardize it by centralization, it is essential to adopt more structured forms of governance, including electronic voting on the blockchain. Let us leave this issue for further research and development since this was not the purpose of this research. It is also important to notice that forms of governance should be developed according to the political system where the cross-blockchain protocol is applied.

c. Secondary rules and dynamic governance

As the last subsection let us discuss meta rules of this system. This research presented details of creating a public database across several blockchains. We discussed how the database can be used to maintain records of property rights and digital identities. It inevitably led the discussion to the legal governance, which is required to maintain the legal validity of property records and resolve legal issues and actors in the system that are authorized to certify, validate, and update records' status. These two elements are referred to as smart laws and digital authorities.

The difficulty of such a system must remain decentralized because otherwise, it makes no sense compared to any other centralized registry. Therefore, the meta-rules, or as per Hart the “secondary rules,” must be designed in the extent to satisfy the need to govern legal relationships in property rights and govern the protocol of the bundle itself.The purpose of this research was to find the range of options for each problem so to form a theoretical framework for the subsequent work in this space.

Particularly, the protocol consists of rules for the inclusion and exclusion of blockchains in the bundle. It is driven not only by ideas of a fair blockchain competition but a consistency of the registry which is built upon such blockchains. To have a decentralized system, these rules must be formalized and hardcoded in the protocol to ensure the nodes do not need an authority to exclude a ledger from the bundle in the case of a fault. However, the need to conduct this orchestra lies beyond the exclusion of blockchains from the bundle. The chain of reasoning leads the discussion to limit the number of blockchains in the bundle due to the limits of disk space. The choice must be based on blockchains' merits, though the fundamental criterion is security. Even if the blockchain's exclusion can be formalized and automated, the inclusion of new blockchains remains an open question and requires further research. One of the options, as discussed, is the use of flags (the messages which miners include in blocks to announce their intention/decision on any issue).

Similarly, the cross-blockchain nodes can translate their decisions towards the protocol of the bundle. However, it is hard to call it a structured meta rule. Hence, the system requires a segment of the off-chain governance, when the decision is made using traditional governance methods and then translated into the protocol through the pre-designed meta rules.

The problem of the governance in this protocol implies that these rules may also require changes. The solution appears in “root” addresses that must be implanted in the system. In the range of options, they are not necessarily centralized but can be governed through collective decision-making mechanisms. For example, to publish a record that will introduce a new rule in the system, the transaction from such an address will require multiple signatures. How such decisions will be made is not a subject of this research because there are different political systems and ways to design it. Root addresses and their specialization, or using more common legal rhetoric the “separation of powers”, play a vital role in balancing the system. Some roots may be responsible for everyday tasks, e.g. validation of legal facts; some will translate judicial acts, some will provide smart laws, etc.

The root addresses are those elements that govern the primary rules by publishing "patches" to the protocol, but constitute the basis for the secondary rules. Eventually, if something goes wrong with the protocol and the bundle cannot provide a consistent public registry, blockchains themselves ensure that the records will not disappear. Through the off-chain governance mechanism or better to say through traditional legal governance, it is possible to reset the registry, the protocol itself, reintroduce new governance, and reinstate lost and violated rights. The use of blockchains makes it all possible because all transactions are irrevocable, valid or not, legal or illegal, correct or mistaken. From the perspective of this system, it is just a matter of their interpretation at the bundle's level of the overlaid database. None of the centralized systems proposes such a privilege, as the loss of records in the centralized system is irreversible, which no government can afford, hence requiring a strong hand of bureaucracy that limits innovations.

d. Market mechanism of free competition

The issue of scalability and price volatility are addressed by one mechanism. The cross-blockchain protocol is a mechanism that supports free-market competition, and this is the key answer.

Frequently, the issue of bandwidth is considered as the problem of a standalone blockchain. One blockchain is compared to one centralized system, such as, Bitcoin (Ethereum, Tron, etc.) vs. Visa (MasterCard, American Express, etc.). Readers may find figures that any of the named centralized systems can process up to 100 times more transactions per minute.

There are at least two typical fallacies found in discussions on scalability. First, centralized payment systems can accept up 20,000 payments per minute, but they do not settle that amount of transactions. It can take up to 3 days to handle the queue. This system is centralized, and transactions are reversible; any mistakes and balance deviation can be manually fixed (*Payment, clearing and settlement systems in the CPSS countries ("The Red Book"), Volume 1 - CPSS - August 2011*, 2011).

The blockchain instead provides immutable certainty in some reasonable time and does not require intermediary, i.e., transactions are peer-to-peer. These systems provide for different user experiences and can hardly be compared. Moreover, some third-party solutions can provide instant transactions as an added layer on a blockchain, for example, based on the Lighting Network (Poon and Dryja, 2016) or Randpay (Konashevych and Khovayko, 2020).

The second inaccuracy is the comparison "one versus one." The bandwidth of blockchain can and should be evaluated in the bundle.

A cryptocurrency is used in speculative purposes and payments. Blockchain limits user experience in two ways: (1) the speed of the transactions, from a few seconds to 10 minutes (average) to wait for the finalization of a transaction, plus blocks of confirmations (for example, in Bitcoin 6 blocks); and (2) the bandwidth. For example, Bitcoin has 2 Mb per block, and therefore, when too many transactions are coming in one moment, they are queued, which then extends the waiting period. Users may jump up into the queue since many blockchains support the priority of higher fees.

The real power of competition is that the user may choose another blockchain for payments and speculations. The buyer who sells products for only one cryptocurrency does not gain an advantage on the market. Between two similar products of different sellers on the market, the seller who offers the product for various cryptocurrencies has more chances of being chosen. What is the principle difference for the seller to get 1 BTC for the product, which she will immediately convert into 10.000 USD or 50 ETH, which are convertible to the same amount of money[8]?

For speculations, investors will be choosing those cryptocurrencies that are more in use, driving these coins' price. Thus, all these market levers create an effective crypto-economics. Even the first dozen of the blockchain list on Coinmarketcap.com in total gives an incomparable bandwidth to any centralized technology.

Therefore, the answer to which blockchain the government should choose is "none." Instead, the government should support the cross-blockchain protocol that enables the unified ecosystem of blockchain technologies, and each user decides which technology to choose.

e. Privacy issues: where to store personal data?

The use of public blockchains raises questions about privacy. It is impossible to fully convert the cadastral register into an open database because it contains personal data. The blockchain cannot be used to publish any personal data in an open format.

The first approach is now generally accepted: public bodies store personal data in closed, centralized systems. This model can be used in the proposed protocol: having the title record in the cross-blockchain database and personal data outside this database.

However, it is important to mention that the blockchain's use means the transactions themselves are public. Some blockchains support zero-knowledge protocols, but their use for the cross-blockchain protocol needs further research. Even if some transaction elements are hidden through the hashing, the proposed scheme with transparent pseudonymous transactions on blockchain, requires its legitimization regarding the existing rules of data protection and privacy.

It might be an issue, for example, in the EU due to the GDPR rules. Pagallo et al. (Pagallo et al., 2018) explain that the right to be forgotten clashes with the blockchain's immutability. The authors discuss hashing and other methods of cryptographic protection of data, but as they emphasize, these methods are unlikely to be considered the proper response to the regulation. Hence, the blockchain's use might be initially questioned as a rightful technology for a public registry. For this level of the discussion, we consider that this precondition is met, and blockchains themselves are legal.

Alternatively, the personal data can be stored on local users' devices (instead of a centralized government database). So, neither the blockchain nor any third party stores any personal information at all, but only digital fingerprints (hash sums,

[8] As of September 2019, https://coinmarketcap.com

encrypted data, etc.). The keeper of personal data is the owner of this data with their devices as carriers.

The research community is actively developing such protocols. For example, the W3C offers the concept of Decentralized Identifiers (DID) (Reed et al., 2019).

It would be appropriate as an example to consider the project proposed by the developer M. Tiutin, who in 2018 at the EOS hackathon presented a model for storing personal data by a user with Selective Disclosure Protocol using the Merkle tree, where the leaves are hashes of personal data, and the root is certified by an authorized person (state agencies, organizations, etc.) (Konashevych, 2019). Such a model may address the problem of personal data disclosure.

Incorrect design of the system leads to redundant disclosure of personal data. In many cases, both from a practical point of view and the law's point of view, not all personal data of a person is required. Having personal data under control on the local user's device, and cryptographic identifiers on-chain, the personal data is not disclosed. Still, only cryptographic evidence of the correctness/existence of the fact is presented. We leave this issue for further research and development.

The largest companies and government agencies lose personal data from time to time. Storing data on centralized servers inevitably leads to leaks. For example, in September 2019, a database with the names, phone numbers, and other information of about half a million Facebook accounts appeared on the internet ("A huge database of Facebook users' phone numbers found online | TechCrunch," 2019). Assuming that the data of active users ("Facebook's grew its monthly average users in Q1 - Business Insider," 2019) is stolen (who needs to steal outdated accounts?), the leak could touch 17% accounts of the social network.

The model in which users store their data locally, without transferring it to centralized databases, has the advantage that it is challenging to hack half a million devices than one server with half a million accounts.

f. Miscellaneous Scenarios

The cross-blockchain protocol is a flexible technology. There can be designed one single cross-blockchain protocol for general purposes. It is also possible to create various customized databases for different applications: decentralized DNS system, property registry, Public Key Infrastructure, etc. There can be localized databases that are dedicated to a territory or community of its application.

The government's cross-blockchain database as a more centralized option may have in the bundle also permissioned DLTs or even provide for an API for closed government databases to develop a hybrid system. For example, a government agency may have its permissioned DLT for the registrar office. The user's record will refer to the clerk's record in the permissioned DLT.

6. Conclusions

The cross-blockchain protocol is a set of tools to build an indexed database across multiple blockchains. The technology makes it possible to set up an initial bundle of blockchains and hook “key-value” entries from upcoming blocks.

It proposes to add new blockchains in the bundle where newly added blockchain is indexed from the current block.

The core of the system is the name-value storage indexed through the bundle of blockchains. The uniqueness of keys (“names”) in the database is ruled by chronology. A name record that is published first among blockchains is added to the database. Subsequent entries with the same names are not passed.

The protocol supports detaching a blockchain in case of an attack or decrease of reliability, and such algorithms must be designed the protocol set up. Reliability and attacks are self-diagnosed by nodes independently based on heuristic analysis of hash rate, difficulty, and abnormal orphan length. When threats are detected, indexing of this blockchain is stopped, and users may transfer the record to the rest in the bundle. Also, the transferability of records among blockchains in the bundle works as a regular feature, supporting competition between technologies, ensuring a free choice of a repository for end-users.

Key-value records are raw materials for building applications. They are assigned to addresses and controlled by users through private keys. Users may change records inserting in the blockchain updated information and command with transactions, i.e., change Value, Lease Time, Delete record from the database or transfer the record to another address.

The protocol's advantage is that it normally does not require changing blockchains; it is set up as an overlaid technology.

The inserted data is recognized and hooked from blocks if it corresponds with the standard format.

The proposed technology addresses issues of the scalability, price volatility, hardforks, and immutability, which discourage governments from using the blockchain, giving preferences to centralized frameworks, so-called “permissioned DLTs.”

Governments can use the protocol to maintain public registries, for example, property (cadastre) databases. Users may own records representing property rights (titles), providing references to trusted third parties that certified these rights. Similarly, the traditional Public Key Infrastructure can be improved, where Certificate Authorities (Trust Service Providers) issue certificates to digital identities. The protocol can also accommodate more strict rules of IDs and electronic signatures, for example, as per eIDAS regulation in the EU, providing users to manage their private keys on secure devices (hardware crypto devices) and 2F/MF authentication protocols.

Such an ecosystem addresses trust issues at the first level: each record has its trust provider, which ensures its validity. If the access to the record is lost, the trusted provider marks the referenced record invalid. It is proposed to initiate patches to the protocol to reset the provider’s record and reset the root record.

The patch in the cross-blockchain protocol aims to provide nodes with a command that a key record must become invalid and which record is the correct one. Such patches being published by authorized addresses are hooked by nodes in the network and applied to provide that every node has the same state of the database.

Such filters, authorized addresses, algorithms, how they are introduced, run and updated, constitute the "smart law" of a cross-blockchain database. The smart law can work in a democratic and decentralized way by electronic voting on the blockchain, which is a matter of the political system where it is introduced.

The protocol can be used to build a comprehensive database for any records, for customized and localized databases for specific communities, countries, and so on.

Annex

Name-Value Storage (NVS) is invented by Namecoin for a decentralized Domain Name System (DNS) and then improved by Emercoin for publishing "key-value" entries in the database supported by API for developing of applications. The data is published in the blockchain using OP_DROP command.

NVS service consists of two basic I/O elements:

(1) Publishing data. Tools for publishing data that are aimed to create transactions based on the standard. The moment the data is inserted into the blockchain, the wallet adds a record in "nameindex" file, which is a database table; and

(2) Retrieving data. Tools for retrieving data from "nameindex" (BarkeleyDB).

The service works as follows. By using the command "NAME_NEW" and further mentioned parameters, the user creates a blockchain transaction. In the transaction, the user adds arbitrary data filing fields Name and Value. The transaction can be created using the standard user wallet interface or via API.

The record includes the following elements:

- NAME is the field to store 512 Bytes of the user's data. When a transaction is published, the protocol verifies if the NAME is unique in NVS; NAME is a search key.
- VALUE is 20 Kilobytes limited field to store any user's data connected with the relevant NAME.
- LEASE_TIME is the period when the NVS record is valid and maintained under the control of the user's address; records are permanently stored in the database of the blockchain, even beyond a lease time. When the period is over, anyone can create the record with the same NAME.
- PREFIX/SUFFIX are service abbreviations added before and after NAME, i.e., "prefix:name:suffix." Abbreviations extend the usability of records of the same type: EmerDNS, EmerDPO, EmerSSH, EmerSSL, among others.
- NEW ADDRESS, if blank, the system puts the user's address by default. The user may specify any address, including one that does not belong to them, to grant the NVS record to someone else.

In Emercoin, fees in cryptocurrency for the transaction are calculated depending on the volume of attached data, lease time, and difficulty level in the network, as per the formula, for details see Emercoin documentation ("Emercoin NVS - Emercoin Community Documentation," n.d.). The fee is "burnt," i.e., becomes unrecoverable.

When fields are completed and submitted by the user, the system calculates the fee, and after the user's confirmation, sends it to the blockchain with the OP_DROP script.

The owner can update the record by publishing a new record with the same NAME with changed VALUE, LEASE_TIME (extend or reduce) and ADDRESS (transfer the record to a new address) using the command NAME_UPDATE. In this case, the system creates a new blockchain transaction as described above, but with new details. Therefore, nothing happens with the previous record.

There is also a command that terminates LEASE TIME of the NVS record, which is called "NAME_DELETE." When this is used, it is not shown in the list of valid records anymore, and it is not controlled by the users' address either.

NVS technology is used to develop applications that require permanent repositories. For example, decentralized SSL, SSH, DNS, among others. In DNS, the user publishes a record in the following format: Name = DNS:domainname.coin, Value = NS record (A, CNAME, AAA, TXT and). The user may include in Value a list of authorized subdomains (|Subdomain1|Subdomain2|…). Therefore, the squatting of subdomains is impossible. If any user publishes a subdomain that is not included in the higher-level domain records list, the system ignores this record. This is an example of how algorithms working as filters make it possible to have decentralized governance of the system.

Acknowledgment

This paper is an outcome of the Ph.D. research performed inside of the Joint International Doctoral (Ph.D.) Degree in Law, Science and Technology, coordinated by the University of Bologna, CIRSFID in cooperation with the University of Turin, Universitat Autònoma de Barcelona, Tilburg University, Mykolas Romeris University, The University of Luxembourg. Thanks to supervisors Professor Marta Poblet Balcell, RMIT University (Melbourne, Australia), and Professor Pompeu Casanovas Romeu, La Trobe University (Melbourne, Australia).

Thanks to Oleg Khovayko (CTO Emercoin, U.S.) and Denis Dmitriev (CTO Emertech, Hong Kong), who took an active part in the discussion of the cross-blockchain protocol, provided their valuable advice. Oleg Khovayko shared his ideas of redundancy (RAID) for cross-blockchain records, Denis Dmitriev suggested cross-references for records and helped with the analysis of a fault probability of the cross-blockchain system.

Compliance with Ethical Standards

Funding: This study is not funded.

Conflict of Interest: Author declares that he has no conflict of interest.

Ethical approval: This article does not contain any studies with human participants or animals performed by the author.

Informed consent: No individual participants included in the study.

References

A huge database of Facebook users' phone numbers found online | TechCrunch [WWW Document], 2019. . TechCrunch. URL https://techcrunch.com/2019/09/04/facebook-phone-numbers-exposed/ (accessed 9.25.19).

About BigchainDB [WWW Document], n.d. URL https://www.bigchaindb.com/about/ (accessed 7.10.20).

Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S., 2013. Evaluating user privacy in Bitcoin, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). p. 596. https://doi.org/10.1007/978-3-642-39884-1_4

Batubara, F.R., Ubacht, J., Janssen, M., 2018. Challenges of blockchain technology adoption for e-government: A systematic literature review, in: ACM International Conference Proceeding Series. Association for Computing Machinery. https://doi.org/10.1145/3209281.3209317

Bitcoin-Qt version 0.8.1 released [WWW Document], n.d. URL https://bitcoin.org/en/release/v0.8.1#how-to-upgrade (accessed 2.19.20).

Block timestamp - Bitcoin Wiki [WWW Document], n.d. URL https://en.bitcoin.it/wiki/Block_timestamp (accessed 4.21.20).

Blockchain and Distributed Ledger | J.P. Morgan [WWW Document], n.d. URL https://www.jpmorgan.com/global/blockchain (accessed 8.21.19).

Breitinger, C., Gipp, B., n.d. VirtualPatent -Enabling the Traceability of Ideas Shared Online using Decentralized Trusted Timestamping.

Brinkmann, M., Heine, M., 2019. Can blockchain leverage for new public governance? A conceptual analysis on process level, in: ACM International Conference Proceeding Series. https://doi.org/10.1145/3326365.3326409

Buldas, A., Saarepera, M., 2004. On Provably Secure Time-Stamping Schemes. Adv. Cryptol. - ASIACRYPT 2004 3329, 500–514. https://doi.org/10.1007/978-3-540-30539-2_35

Confirmation - Bitcoin Wiki [WWW Document], n.d. URL https://en.bitcoin.it/wiki/Confirmation (accessed 2.25.20).

Cost of a 51% Attack | Crypto51.app [WWW Document], n.d. URL https://www.crypto51.app/about.html (accessed 8.13.19).

Council of the European Union, 2014. 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 (eIDAS), Official Journal of the European Union. EU.

Crespo, S.D.P.A., Luis García Cuende, I., 2016. Stampery Blockchain Timestamping Architecture (BTA). https://doi.org/10.13140/RG.2.2.34164.76168

Data.gov.ua [WWW Document], n.d. URL https://data.gov.ua/ (accessed 9.16.19).

Elisa, N., Yang, L., Chao, F., Cao, Y., 2018. A framework of blockchain-based secure and privacy-preserving E-government system. Wirel. Networks. https://doi.org/10.1007/s11276-018-1883-0

Emercoin NVS - Emercoin Community Documentation [WWW Document], n.d. URL https://emercoin.com/en/documentation/blockchain-services/emernvs (accessed 6.28.18).

Facebook's grew its monthly average users in Q1 - Business Insider [WWW Document], 2019. . Bus. Insid. URL https://www.businessinsider.com/facebook-grew-monthly-average-users-in-q1-2019-4/?r=AU&IR=T (accessed 9.25.19).

Franciscon, E.A., Nascimento, M.P., Granatyr, J., Weffort, M.R., Lessing, O.R., Scalabrin, E.E., 2019. A systematic literature review of blockchain architectures applied to public services, in: Proceedings of the 2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design, CSCWD 2019. Institute of Electrical and Electronics Engineers Inc., pp. 33–38. https://doi.org/10.1109/CSCWD.2019.8791888

Gao, Y., Nobuhara, H., 2017. A Decentralized Trusted Timestamping Based on Blockchains. IEEJ J. Ind. Appl. 6, 252–257. https://doi.org/10.1541/ieejjia.6.252

Gipp, B., Meuschke, N., Gernandt, A., 2015. Decentralized Trusted Timestamping using the Crypto Currency Bitcoin, in: IConference 2015 Proceedings. iSchools.

GitHub - google/leveldb: LevelDB [WWW Document], n.d. URL https://github.com/google/leveldb (accessed 2.25.20).

Gregor, S., Hevner, A.R., 2013. Positioning and presenting design science research for maximum impact. MIS Q. Manag. Inf. Syst. https://doi.org/10.25300/MISQ/2013/37.2.01

Heinrich, C., 2005. Pretty Good Privacy (PGP), in: Encyclopedia of Cryptography and Security. Springer US, pp. 466–470. https://doi.org/10.1007/0-387-23483-7_310

Hevner, A.R., March, S.T., Park, J., Ram, S., 2004. Design Science in Information Systems Research. MIS Q. Manag. Inf. Syst. 28, 75–105. https://doi.org/10.2307/25148625

Higgins, S. (CoinDesk), 2014. 8 Million Vericoin Hack Prompts Hard Fork to Recover Funds [WWW Document]. URL http://www.coindesk.com/bitcoin-protected-vericoin-stolen-mintpal-wallet-breach/ (accessed 12.31.16).

Hyperledger Architecture, Volume 1, 2017.

Jones, A., Dawkins, B., 2009. Common RAID Disk Data Format Specification.

King, S., Nadal, S., 2012. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake.

Konashevych, O., 2020. Constraints and Benefits of the Blockchain Use for Real Estate and Property Rights. J. Prop. Plan. Environ. Law ahead-of-p. https://doi.org/10.1108/JPPEL-12-2019-0061

Konashevych, O., 2019. Will Blockchain Stop Personal Data Leaks? | Cointelegraph [WWW Document]. Cointelegraph. URL https://cointelegraph.com/news/will-blockchain-stop-personal-data-leaks (accessed 9.17.19).

Konashevych, O., Khovayko, O., 2020. Randpay: The technology for blockchain micropayments and transactions which require recipient's consent. Comput. Secur. 96, 101892. https://doi.org/10.1016/j.cose.2020.101892

Konashevych, O., Poblet, M., 2019. Blockchain anchoring of public registries: Options and challenges, in: ACM International Conference Proceeding Series. Association for Computing Machinery, Melbourne, Australia, pp. 317–323. https://doi.org/10.1145/3326365.3326406

Krogsbøll, M., Borre, L.H., Slaats, T., Debois, S., 2020. Smart Contracts for Government Processes: Case Study and Prototype Implementation, in: Financial Cryptography and Data Security 2020. International Financial Cryptography Association, pp. 1–8.

Loibl, A., 2014. Namecoin. https://doi.org/10.2313/NET-2014-08-1_14

MacDonald, T.J., Allen, D.W.E., Potts, J., 2016. Blockchains and the boundaries of self-organized economies: Predictions for the future of banking. New Econ. Wind. https://doi.org/10.1007/978-3-319-42448-4_14

Martin, J., 1983. Managing the Data Base Environment, 1st ed. Prentice Hall PTR, USA.

Mining - ethereum/wiki Wiki [WWW Document], n.d. URL https://github.com/ethereum/wiki/wiki/Mining (accessed 9.2.19).

Noonan, J.T., 1962. THE CONCEPT OF LAW. By H. L. A. Hart. Oxford: Oxford University Press, 1961. Pp. viii, 263. 21s. Am. J. Jurisprud. 7, 169–177. https://doi.org/10.1093/ajj/7.1.169

Ober, M., Katzenbeisser, S., Hamacher, K., 2013. Structure and Anonymity of the Bitcoin Transaction Graph. Futur. Internet 5, 237–250. https://doi.org/10.3390/fi5020237

Ølnes, S., 2016. Beyond Bitcoin enabling smart government using blockchain technology, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer Verlag, pp. 253–264. https://doi.org/10.1007/978-3-319-44421-5_20

Ølnes, S., Jansen, A., 2017. Blockchain technology as s support infrastructure in e-Government, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). https://doi.org/10.1007/978-3-319-64677-0_18

Ølnes, S., Ubacht, J., Janssen, M., 2017. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Gov. Inf. Q. 34, 355–364. https://doi.org/10.1016/J.GIQ.2017.09.007

Oracle Berkeley DB [WWW Document], n.d. URL https://www.oracle.com/database/technologies/related/berkeleydb.html (accessed 2.19.20).

Overview of Amazon Quantum Ledger Database (Amazon QLDB) [WWW Document], n.d. URL https://docs.aws.amazon.com/qldb/latest/developerguide/what-is.overview.html (accessed 7.10.20).

Pagallo, U., Bassi, E., Crepaldia, M., Durante, M., 2018. Chronicle of a clash foretold: Blockchains and the GDPR's right to erasure, in: Frontiers in Artificial Intelligence and Applications. IOS Press, pp. 81–90. https://doi.org/10.3233/978-1-61499-935-5-81

Payment, clearing and settlement systems in the CPSS countries ("The Red Book"), Volume 1 - CPSS - August 2011, 2011.

Poon, J., Dryja, T., 2016. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments.

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., Sabadello, M., 2019. Decentralized Identifiers (DIDs) [WWW Document]. URL https://w3c-ccg.github.io/did-spec/

(accessed 1.1.20).
Roio, D.J., 2013. Bitcoin, the end of the Taboo on Money. Dyne.org Digit. Press 1–17.
Shermin, V., 2017. Disrupting governance with blockchains and smart contracts. Strateg. Chang. 26. https://doi.org/10.1002/jsc.2150
Sward, A., Vecna, I., Stonedahl, F., 2018. Data Insertion in Bitcoin's Blockchain. Ledger 3, 1–23. https://doi.org/10.5195/LEDGER.2018.101
Weber, M., 1922. Bureaucracy, in: Waters, T., Waters, D. (Eds.), Weber's Rationalism and Modern Society: New Translations on Politics, Bureaucracy, and Social Stratification. Palgrave MacMillan, pp. 73–128.
Wood, G., 2015. PoA Private Chains · GitHub [WWW Document]. GitHub. URL https://github.com/ethereum/guide/blob/master/poa.md (accessed 12.30.19).

PAPER 3

Constraints and benefits of the blockchain use for real estate and property rights

Oleksii Konashevych
Erasmus Mundus Joint International Doctoral Fellow in Law, Science and Technology, Research Centre of History of Law, Philosophy and Sociology of Law, Computer Science and Law, University of Bologna

Received 31 December 2019
Revised 11 February 2020
Accepted 1 April 2020

Abstract

Purpose – Many recent social media posts and news may create a perception of big success in the use of blockchain for the real estate industry, land registration and protection of titles and property rights. A sobering outlook is crucial because misleading concepts may bury the whole idea of blockchain use. This paper aims to research the possibilities of blockchain and other distributed ledger technologies (DLT) and applicability of these technologies for different purposes in real estate, property rights and public registries.

Design/methodology/approach – This research is framed with policy studies and focuses on property rights, land registration regulatory framework and information and communication technologies innovations. The context of this paper is decentralization which has been developed in political science studies and the role of blockchain and DLT in it. Therefore, the provided analysis of blockchain and DLT is interdisciplinary research to interpret the facets of DLT technologies in the context of real estate and land title registration.

Findings – Permissioned and private DLT systems cannot be considered a significant evolutionary step in government systems. Blockchain, which is distinguished from permissioned systems as the technology of the immutable ledger that does not require authorities, is a new word in governance. However, this technology has some principal features that can restrain its implementation at the state level and thus require further research and development. The application of blockchain requires a proper architecture of overlaid technologies to support changes of outdated and mistaken data, address issues of digital identity and privacy, legal compliance and enforceability of smart contracts and scalability of the ledger.

Originality/value – This paper shows the constraints of the technology's properties which were not explained before in the context of title rights and land registration even though technological limits are known in more specific technical sources. Along with the known benefits this meant to help to avoid misinterpretation of some DLT features by non-technical people. A multidisciplinary approach in analyzing the technology and laws helped to better understand what can and cannot be beneficial for public registries and the protection of property rights. The presented outcomes can be laid down as requirements for the technical protocols aimed at addressing the issues of DLT and public policies to put blockchain at the service of society.

Keywords Real estate, Blockchain, Property rights, Smart contracts, Distributed ledger technology, Land registry

Paper type Research paper

This paper is an outcome of the PhD research performed inside of the Joint International Doctoral (PhD) Degree in Law, Science and Technology, coordinated by the University of Bologna (CIRSFID) in cooperation with the University of Turin, Universitat Autònoma de Barcelona, Tilburg University, Mykolas Romeris University, The University of Luxembourg. The author is grateful to RMIT University and the team of Blockchain Innovation Hub for the seminal collaboration. Thanks to supervisors Professor Marta Poblet Balcell, RMIT University (Melbourne, Australia) and Professor Pompeu Casanovas Romeu, La Trobe University (Melbourne, Australia).

Journal of Property, Planning and Environmental Law
Vol. 12 No. 2, 2020
pp. 109-127

2514-9407
DOI 10.1108/JPPEL-12-2019-0061

1. Introduction

Blockchain and other distributed ledger technologies (DLT) drew the attention of the real estate industry and governments. This research shows that there are no outstanding examples of success in the utilization of this technology in real estate and property registries. Therefore, this paper provides analysis and discusses the use of blockchain in addressing misconceptions and myths in this space.

The common feature of most of the projects is the idea of disrupting and decentralizing the real estate industry, developing, or improving land registries on blockchain, applying smart contracts and so on. None of the discussed examples however use public blockchains. This analysis shows there are no benefits in using centralized ("permissioned") DLTs for the public sector. At least, there is no justification found among such projects as to why certain centralized solutions are better than those which government agencies have already used for decades to run public registries. Inconsistency of ideas of decentralization and their implementation is a result of a lack of research and understanding of the technology's capabilities.

Even more alarming is a tendency for politicians and some startups to mislead society in their intentions to introduce any decentralized solution titling their technologies "permissioned" or "private" blockchains. The word "blockchain" is expected to correspond with inherent features of Nakamoto's invention – uncensored and public technology with an immutable ledger, with no dedicated trusted third party to conduct the system and provide a single source of truth for the state of transactions.

Sections 2 and 3 explore the constraints of the technology and its applicability to property rights and land registration issues.

Section 2 discusses the general ideas of blockchain use and decentralization, specifically, public ledger versus private/permissioned. The next section provides the analysis of issues in using public and private DLTs and some misconceptions. The fourth section shows some projects in the Republic of Georgia, Sweden, Ghana, The Netherlands, the USA and some other places and discusses practical issues that they encounter. The analysis shows that it is too early to make conclusions about these projects or at least they are not as enthusiastic as the perception media may have created. The cases should be further observed and scrutinized for an unambiguous assessment.

The conclusion summarizes ideas on the applicability and benefits of the technology in public services, particularly land cadasters and other property registries.

The value of this research is that it presents a systematic approach in the analysis of the use of blockchain for property rights and public services, considering that there is a lot of speculative and misleading information in media.

This paper contains a lot of technical discussions interpreted and summarized for a wide range of readers to fill a gap in the understanding of DLT and blockchain.

1.1 Theoretical framework and methodology

This research is framed with policy studies and focuses on property rights, regulatory framework of land registration and information and communication technologies (ICT) innovations. The context of this paper is decentralization which has been developed in political science studies and the role of blockchain and DLT in it. The provided analysis of blockchain and DLT is an interdisciplinary research.

This paper is draws conclusions from different sources:

- technical reports and white papers of projects, such as Bitcoin, Ethereum and Emercoin;
- academic papers; and
- technical analysis from forums and open industry platforms, mainly Bitcointalk and GitHub.

Media posts and social networks also provided some news on progress in the industry.

Questions found in subsection 3.2 are sourced from empirical data gathered by the author through participating in conferences, workshops and meetings around the world within industry and academia. This subsection is focused on addressing probable fallacies that may appear in the field.

The theoretical framework is not new and contains multiple developed concepts. In "The Evolution and Continuing Challenges of E-Governance" (Dawes, 2008), the author defines this field of knowledge as "the use of information and communication technologies (ICTs) to support public services, government administration, democratic processes, and relationships among citizens, civil society, the private sector, and the state."

The methodology which is used in this research is similar to such works as "The understanding of ICTs in public sector and its impact on governance" (Malinauskienė, 2013) and "Conceptual Framework for Context-Based E-Government Interoperability Development" (Jansen, 2012).

In the first paper (Malinauskienė, 2013), the author provides the analysis and generalization to define the concept of e-government interoperability. The researcher in the result of analysis of ICT capabilities and methods concludes that policymakers, public managers and related private sector organizations should assess the technical and evolutionary fitness of dynamic organizational capabilities for interoperability before starting any cross-organizational e-government initiative. It should be done through the analysis of related processes, asset position and path-dependency factors of all participating parties. The author recommends incorporating these principles of context analysis in the research of e-government.

In the second paper, the author (Jansen, 2012) asks if managers in the government really understand the many functions and roles ICTs have and how they should be governed. The author researches the phenomenon of mismatch of the functions implicit in the objectives that are stated for e-government and the way ICTs are governed. Jansen argues that this discrepancy can be attributed to an inadequate understanding of ICTs and its many functions. Jansen's conclusions became a methodological basis and leitmotiv for this paper.

The analysis provided by this paper is a typical preparation step before any policymaking while it also delivers grounds for further research and experimenting. Such analysis aims to bridge the complex matter of technologies to social science: law, management and economics. The outcome is a set of inferences for policymakers and researchers of the capabilities and limits of the technology.

2. Use of blockchain for real estate

A variety of ideas for using DLT for property rights recently appeared in the blockchain industry. However, speculation can make a reader think that blockchain has extraordinary features. Therefore, before designing any application it is important to understand what the technology can and cannot do.

Any abstract ideas in blockchain can be materialized in the existing features and services, which the technology can provide:

- *Cryptocurrency* is a unit of account in the blockchain network with no ways to double spend it. Cryptocurrency is an asset in the ledger, which is produced by users of the network as a result of some decentralized consensus mechanism, and then used as a transfer of value. Therefore, the user may own their "coins" in a wallet and transfer it as a digital cash. Technically cryptocurrency is a record attached to the address (public key) which can be managed by a private key. Public and private keys are elements of asymmetric cryptography (Schneier, 1996). Cryptocurrency can be used as payment in a property deed, i.e. a title in exchange for cryptocurrency. Cryptocurrency is also spent in

blockchains to run smart contracts, for example, to pay "gas" in Ethereum (Ethereum Wiki, 2017). Users also usually spend some coins as fees to miners during the transfer of cryptocurrency from one address to another.

- *Data insertion* into blockchain as the immutable storage became the subsequent useful property of the technology which the inventor (Nakamoto, 2008) has never explicitly mentioned as the fundamental benefit, but was always present as the essential feature of the technology. With a transaction, the user can insert some arbitrary data into blockchain. To insert data, the user must apply some specific scripts and methods in the transaction (Sward *et al.*, 2018). Data insertion may be useful for real estate to store data, which, in this case, becomes public and irrevocable. It is usually not used, as it is because the insertion of data became the fundamental feature beyond cryptocurrency, which made possible all further useful technologies, such as the colored coins (Colored Coins – Bitcoin Wiki, 2020), tokens (Ethereum Wiki, 2017), smart contracts [1] (Ethereum Wiki, 2017), name-value storage (Emercoin NVS – Emercoin Community Documentation, 2020) and decentralized applications (Raval, 2016). One the most known critical comments in the real estate industry of this feature is that inserted data cannot be altered; therefore, wrong and outdated information may mislead users. This issue is addressed by some methods which are further discussed.
- *Tokens* are records that first appeared as an overlaid technology on top of cryptocurrency or a part of a smart contract. However, a token can be a standalone record in the system, not related to any cryptocurrencies (EOS.WIKI, 2020). Also, cryptocurrency can be deemed as tokens themselves. A coin (for example, the smallest fraction – Satoshi coin) in the first generation of blockchains are used as a carrier of a token because all transactions are kept in the ledger, and each coin can be identified and traced, users may pull some external logic on it. For instance, some records of property rights which the coin can represent. Thus, a token is the record in the ledger that can be distinguished as a unique unit of account and attached to the address and therefore, owned by the user. Someone who has the relevant private key can use it to authenticate a transaction. The token is the technology around which users may establish legal relations by connecting the token to some property rights. Therefore, tokens for real estate play one of the most crucial roles.
- *Smart contracts* is a technology for automated transactions in a digital form [2] with some crypto assets (coins and tokens), in a broader sense in the second generation of DLT platforms smart contracts are programs that allow managing of crypto assets and automate transactions. For real estate, tokens and smart contracts are cornerstones since they allow digitizing of property rights and provide for online contracts.
- *dApps* (decentralized applications) is a broader understanding (than smart contracts) of a class of applications built on blockchain; dApps may consist of smart contracts but aim to provide a full range of end-user online services (Raval, 2016).

All speculations about the use of blockchain are limited to this list of services. It either can be used as cryptocurrency for payments, or as a storage for applications and records, including property rights and titles which can be managed by tokens and smart contracts.

Nevertheless, these things can be done with more traditional centralized electronic systems. The distinguishing feature that unites all this – a decentralized consensus. The consensus protocol is a logic of how these services are created and legitimized in the system.

2.1 Consensus and (De)centralization

The invention of blockchain aimed to provide the technology to maintain a ledger without authorities, i.e. a dedicated third party which provides the legitimate version of the database for other nodes in the network.

All nodes keep a copy of the ledger, while the consensus allows them to choose which copy is correct. The first designed consensus – Proof-of-work (Proof-of-work (PoW) – BitcoinWiki, 2020) – at a higher level of understanding is the mechanism of randomness. Nodes perform some calculations to find a new block and present it to the network as a legitimate piece of the ledger, and they do not know who is next to present a block.

In different consensus protocols, there are methods of how to increase the probability of getting this right, but they are still relative, and randomness is the key thing, and if this balance is broken, then the network becomes centralized – meaning there is someone who can dictate the right version of the protocol and database.

Centralization means the ability to change the protocol and effect the history of transactions, or even rewrite the blocks (especially in Proof-of-stake [PoS], which will be discussed later) and to censor incoming transactions.

In some discussions, especially among non-engineers, the consensus protocol is considered to be something which solves issues of the real estate industry. It should be emphasized that there is nothing else in the protocol besides the mechanism of randomness, aimed to provide decentralization in keeping records of cryptocurrency transactions, and the logic which is attached to it, i.e. tokens and smart contracts.

"Permissioned" and "private" shared ledgers are different from the idea of blockchain. Initially, they are designed as a centralized system where one node or a group of nodes can control the process of the creation of blocks and their validation.

Decentralization in public blockchains is not static. This is a dynamic process of competition of nodes which independently or collectively in a pool try to create new blocks and gain the right to write down a defined amount of cryptocurrency in these blocks as their reward. Therefore, "permissioned" is the worst scenario toward the running blockchain system.

Another essential feature of blockchain is a censorship resistance. The purpose of the technology is to ensure that any transactions and scripts defined in the protocol can be performed without any authorization. Users may also insert some arbitrary information in the allowed amount of data, for example, up to 50 kB in Bitcoin (Sward *et al.*, 2018).

To explain some misconceptions about the use of the permissioned DLT, let us provide some more technical details of the most typical consensus protocols.

In PoS (King and Nadal, 2012), the right to create a block is gained randomly as a lottery. Nodes can put their coins as the "stake" for the lottery against other nodes, the one who has a mathematically proven win, presents a new block, the node does not lose their staked coins, and may continue their play. The more coins a user has, the more chances to win. This protocol can be designed initially as centralized, at least, more than 50% of coins must be allocated ("pre-mined") in this case to one address in the genesis block, therefore, providing at least a 1 in 2 chance to create a new block or more if more coins are owned.

PoS can be used to develop a private DLT, so only a group of actors will maintain and use the network, for example to maintain the ledger that keeps records of property rights and transactions with them. Because no one has coins outside of this group, no one else beyond can perform transactions as well. However, this "peace" will be fragile, which means coin owners will not be limited by the technology from sharing their coins with someone outside of such a consortium. Thus, at any moment, such a group can fall apart, and the network becomes more decentralized and open for other users. So, how the private DLT

consortium keeps the ledger closed and private lies beyond the mathematics of the PoS. These are contractual relations of partners.

Another essential property of PoS is rewriting history. The actor can present the network with a new version of the chain beginning from any block in the past when the actor had enough stake to create a block. For example, history rewriting happened with Vericoin (Higgins, 2014). Here a general rule applies nodes accept the longest chain as legitimate. Therefore, when the controlling stake presents the longest chain, other nodes with minor stakes drop down the old version of the chain and consider the new one as the right one. This scenario is called "rollback" (Figure 1).

Therefore, the ledger is not immutable, and transactions are not irrevocable. The controlling stake owner will not necessary capture someone's coin, because they still will need the private key for any particular address, but they may drop off transactions from blocks, which means the attacked address will lose ownership over the coins (tokens, smart contracts).

Another centralized protocol for permissioned and private ledgers is *Proof-of-Authority* (PoA) (Wood, 2015). One actor in the system will provide the list of authorized addresses, which are allowed to create (validate) blocks. The supernode can arbitrarily grant and withdraw authorization to validators. Therefore, rewriting history is still possible when the supernode withdraws all access except one, which will rewrite the ledger and present it to the network.

Both protocols allow the pre-authorization of transactions. The validators will check and censor transactions before sending them to a new block. Therefore, rewriting history is considered the last measure.

PoS and PoA may be mixed with other consensus protocols, for example, with PoW or cast the snapshot (a hash sum) of the ledger from time to time to a more decentralized ledger

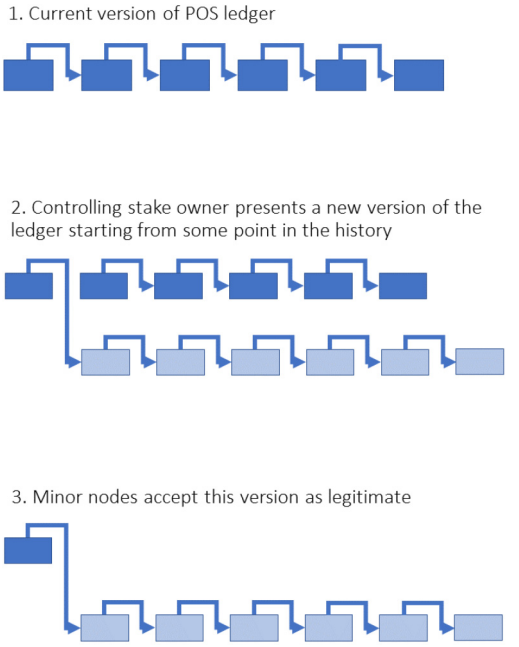


Figure 1.
Rewriting the ledger in "roll back" scenario in PoS consensus

(for example, Bitcoin). These measures can be used to add more credibility to the system. However, centralized remains as such, and these measures are considered as the goodwill of the owner, which can change their mind at any moment.

Interestingly, the Digital Transformation Agency of Australia in their report (*Blockchain Overview: Australian Government Guide*, 2018) noted:

> There are additional risks [besides those which are mentioned in NIST report] and considerations when using permissioned consortium blockchains, where leading users often in effect control blockchain. This usually removes the perceived benefits of decentralization.

The main conclusion of this analysis is that permissioned and private DLTs have no advantages against other centralized databases in terms of decentralization or at least, those who advocate these technologies did not provide reasonable arguments to support this technology against other centralized registries. It does not mean that the permissioned DLT is not applicable. It is a good technology for the private sector; however, for public administration and public services, this is questionable. Permissioned has a single point of failure, and users must delegate authority to the owner of the network and rely on their goodwill. This is relevant to other centralized technologies, more traditional databases, which have already been in use by governments for decades.

However, this discussion is not over, and more empirical research and analysis may provide a deeper understanding. Nevertheless, the very first question which must be addressed in using any DLT is the purpose. If the aim is decentralization, then blockchain is the answer. There is no other scalable technology for this objective that has been created before or after 2008 so far.

3. Issues with blockchain

Although the idea of decentralized governance is attractive, practical implementation is not viable at the moment. Some additional development at the technical level and, of course, at the political and legislative level is needed, which is discussed in this section.

3.1 Seven major issues

3.1.1 Immutability. There are two different conceptually designed DLT systems in terms of the consensus:

- initially decentralized and public (blockchain); and
- initially centralized are often referred to as "permissioned" and "private" (as a subset of permissioned).

However, as it is noted, decentralization is not a state, it is a process which also may end-up with centralization.

One of the essential advantages of using blockchain beyond the mentioned high-level ideas of decentralization, at the practical level, is *immutability*. In the ledger, users can store cryptocurrency transactions, and useful information not related to crypto at all. For example, records of property rights, title rights, etc.

Why an immutable ledger is better can be shown in the example of the loss of data by the Ukrainian government. The Ukrainian tax office lost a cluster of 3 terabytes of electronic records of tax returns and correspondence, more than half a million documents disappeared (*UNIAN Information Agency*, 2016), (The State Fiscal Service of Ukraine, 2016).

Public registries, which are controlled by centralized authorities, are an act of trust, where citizens usually have only one option; to decide during the elections whether they believe the government or not. But this will not return vital information when it is lost.

If we are talking about the record of a property right, especially if it is the only source of evidence, this is something that no owner wants to lose. Therefore, this risk shows how much the system with a single point of failure is vulnerable. Assuming no perfect organizational and technical structures, to be on the safe side, we should refer to Murphy's law [3], "Anything that can go wrong will go wrong," and act accordingly.

The bold promise of the government to serve the society fairly may be nothing if the technology does not limit embezzlement and corruption.

Blockchain as the technology, which excludes and minimizes human faults and corruption in providing an irrevocable and immutable ledger, is more competitive than the social contract based on pure political promise and trust.

Despite this fundamental conclusion and obvious benefits of the use of blockchain technology for keeping records of property rights, immutability creates obstacles that make this technology inapplicable unless a proper solution is found.

For example, the loss of private keys will make a cryptocurrency, a token, or a smart contract uncontrolled with negligible possibilities to ever restore it. Even if blockchain can prevent many ownership disputes, the imperfect nature of people's relationships will always cause issues with ownership, and the need to settle when they arise.

Blockchain itself, in its pure design, does not leave practical possibilities for enforcing any legitimate judicial decisions or any rightful actions by authorities because normally retroactivity is impossible and no one except the owner of the private key of the asset can perform a transaction.

Therefore, permissioned DLTs may be justified as the only possible solution, losing its initial properties of being immutable and censorless inherited from blockchain.

3.1.2 Permissioned VS public in terms of infrastructure. Public blockchain systems do not require authorities to create infrastructure. Their drive gear is cryptocurrency. Independent participants are incentivized to share their computing resources to the network and compete for the reward. The node, which presents a valid block to the network, has the right to include a record of new cryptocurrency. The protocol provides the amount of the reward which the node may assign; therefore, there are no authorities, which manage and maintain the system, it is self-organized and self-governed.

On the contrary, the permissioned system may require a central authority that is responsible for developing infrastructure, i.e. data centers, nodes, gateways, API, cybersecurity measures, etc. Therefore, with the ability to control and vary the ledger, comes the burden of infrastructure expenses and its centralization as well.

3.1.3 Hardforks. The government plays the role of a keeper of a traditional property registry. In different countries, they may have different names and specializations (cadastre, land title registry, real estate registry, etc.) but the purpose is the same: to provide certainty in property rights by tracking records of transactions (title deeds). It is similar to registries for movable properties (cars, boats, aircraft, etc.), shares and other securities and corporate rights.

The use of any decentralized system, including the blockchain is limited, because it may create issues with registry forking. The system can split into two or more branches or "forks" after which each branch becomes independent. In the result of the split, tokens are duplicated. For example, if the system is used to manage rights on movable property (often mentioned as "asset-backed tokens"), in the result of a hardfork, the user will still have one plot of land but two title records in parallel systems, which they can be managed

independently, thereby creating legal collisions. For example, in one system, the user sells the plot, but in the other, the user still owns it.

One possible solution is that the government will point out which blockchain is legitimate in the case of a hardfork. For example, Bitcoin or Bitcoin Cash, Ethereum or Ethereum Classic. Buy why would anyone use a decentralized system but end-up with the central authority? It also restraints competition between blockchains.

3.1.4 Anonymity (pseudonymity). The authorization and authentication for a transaction are provided only with the relevant private key, which belongs to the asymmetric pair. The public key of the pair is taken to generate the address of the transaction, and the address (to which coins are recorded) is the only public record in the system that identifies the user.

Some research showed that addresses could be deanonymized by different digital fingerprints, i.e. IPs, behaviour patterns, etc. (Ober *et al.*, 2013), (Androulaki *et al.*, 2013). The original blockchain protocol is not suitable for keeping records on property and securities from the perspective of governments and users themselves. Blockchain anonymity may veil money laundering, financing terrorism, and other unlawful activity.

Beyond that, at the practical level, the censorless nature of blockchain creates confusion in identifying records. Anyone may perform any transaction and publish any data in blockchain. If the government must authorize a land title deed, how do you define if any transaction on blockchain belongs to the town's clerk if they are all pseudonymous? Without overlaid solutions for digital identities and trust services [or more specifically, Public Key Infrastructure (Trček, 2006)], it is almost impossible to create any scalable model for governance.

3.1.5 Personal data. In blockchain and other DLTs which are open for reading, any published data is exposed, and removal is not an option. Therefore, ledgers are not suitable for storing personal data; users must at least have the right not to disclose their details. Otherwise, the right to be forgotten (GDPR) is not applicable. The use of DLT requires some technologies and methods for privacy preservation. For example, a cryptographic hash, published as immutable evidence in a DLT, will provide a one-way link to the personal data, but the data itself will be stored on the user's device or a closed third party's server.

3.1.6 Scalability. One exclusively chosen blockchain for governance will necessarily create issues. Again, because of the open nature, blockchain protocol does not restrain publishing junk data in the ledger. The potential bandwidth of Bitcoin per year, for example, is roughly 220 million transactions (Roio, 2013). For instance, more than three hundred public registries in Ukraine generate as much as Bitcoin's bandwidth (Data.gov.ua, 2020), which leaves no space for other cryptocurrency transfers. Overload with the transactions creates the problem of high transaction fees and price volatility. Although Bitcoin is not the best in terms of bandwidth, it is still the most attractive in terms of security (Cost of a 51per cent Attack for Different Cryptocurrencies | Crypto51, 2020). This is not a workable solution on a scale, even for one country with a 40-mln population, randomly chosen as an example.

3.1.7 Price volatility. Owing to speculations, the price can dramatically fluctuate, therefore creating a bad user experience for those who need cryptocurrency to pay fees for publishing and managing data, running smart contracts, etc. Together with the mentioned scalability issues, it makes it infeasible for the government to use, or even to announce their intention to use any specific blockchain. It will inevitably incentivize agiotage on the market, exacerbating the above-mentioned problem of scalability even more.

Eventually, as might be thought, the permissioned DLT is much better than blockchain as it addresses all these issues because of its centralized nature, purposed to control and restrict unwanted practices, and manually fix troubles.

This creates two basic misconceptions: centralized DLT is presented as an improved version of blockchain, able to address known limits. As we can see, it does, but this is not a blockchain (not decentralized, not censorless, etc.). The second is that one DLT is opposed to one blockchain.

It is proposed to create solidarity of reliable blockchains working in a bundle. The government should not choose one blockchain, but instead, provide an infrastructure solution based on common technical standards to support free competition of blockchain technologies. A market-driven approach is aimed at addressing the problem of scalability. The citizen, not the government, should decide which blockchain to use. The role of the government is to provide standards of security requirements (hash rate, etc.) for blockchain to exclude unreliable networks.

3.2 Misconceptions

There are a few major misconceptions in the use of blockchain technology. This subsection aims to address them.

"Immutability does not tolerate mistakes."

In the previous section, a general discussion is presented on the benefits and constraints of immutability. It is possible to suggest that immutably is something that prevents fixing mistakes. Let us clarify this position.

The mistaken transaction is irrevocable. Wrongly transferred coin matters. This is something that the sender cannot handle without the will of the receiver to refund back.

For example, one user mixed up the field which specifies the amount of coins to send with the filed he specifies the fee for this transaction. The user accidentally sent 2,100 ETH (US$300,000) as fee and would not get them back, unless the miner who received such a jackpot willingly returned (Insanity: Ethereum Wallet Pays Nearly $575,000 in Fees to Transfer $25 in ETH, 2020).

If we are talking about data insertion, immutability is not an issue. The mistakenly published information cannot be changed, but a proper architecture of the service can address it.

The solution is straightforward because timestamping is an essential feature of the system, all transactions are chronologically stored. The latest data inserted must be deemed as the correct one. Thus, even the user publishes inaccurate information initially, at any moment, they can update it by publishing corrected data. In the case where the user lost the private key and cannot publish an update from the initial address, then the architecture will require the involvement of a trusted third party. The user initially refers to the record of the validator. The validators will publish into blockchain a record (message) with the information about the validity of the target message (Figure 2).

Therefore, if the user lost the key, they will contact the validator and enquire to publish a message of invalidity of the target message. Of course, the validation must be performed in a machine-readable format to provide automation and better UIX. This technology and method are already in space, at least, since 2014, examples can be found in Namecoin (Namecoin.org, 2020), and Emercoin projects, pioneers in decentralized DNS systems (Loibl, 2014) and Name-Value Storage technologies (Emercoin NVS – Emercoin Community Documentation, 2020).

"How to include all title records of the country in the Genesis block?"

The issue is irrelevant in the case of developing the application of property rights on existing blockchains, for example, strongholds of public blockchains - Bitcoin, Ethereum,

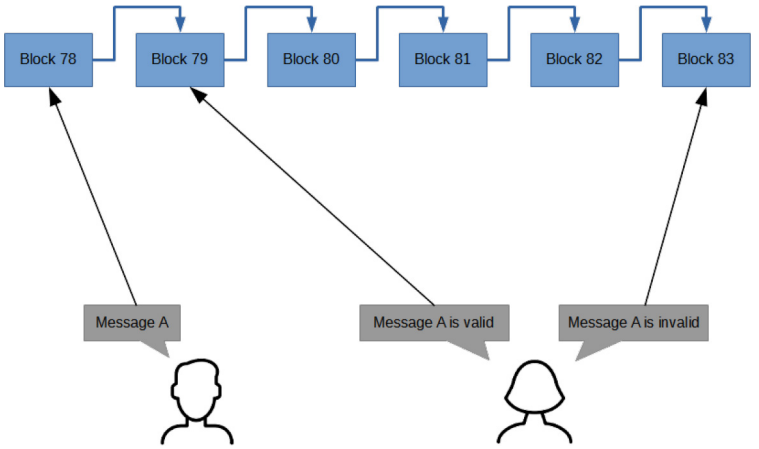


Figure 2.
Scheme for maintaining validity of records in blockchain

etc. However, these ideas may be discussed in the context of private and permissioned systems, which can be developed specifically to manage property rights and public registries.

The issue is as follows. If we build a new DLT where we initially would like to include all titles and other property rights records, which are currently in paper form or in the electronic land registry database, how do we deal with ongoing disputes and inheritance? There is no point in time when all deeds and disputes are settled.

The idea of moving all records to any DLT has some objections. There is a principle of *technological neutrality*, which means any technology may be applied, and the government should not prevent competition between technologies. Therefore, voluntary movement from one technology to another is a fallacy, the same as a fallacy as staying with the existing centralized technologies.

A better scenario is a free choice of every citizen in determining which technology to use to manage their property rights. And when this principle is ensured, citizens will be able to move their title records from papers and centralized DBs to blockchain. Therefore, there will be no starting Genesis block. This is a continuous process.

Ongoing disputes and uncertainty of some records can be addressed by the proper design of the technology, which must support algorithms for updating inaccurate or outdated records. Some of the existing methods are mentioned already in the previous question.

"Do we need a land registry?"

Free choice of technology requires returning to a higher level of understanding of what the "land registry" and "registration" themselves are. The purpose of the registry is to provide certainty in "who owns what." Therefore, the registry must ensure secure storage for records that are managed as per law. If the citizen has chosen to store the record in blockchain, there is no need to duplicate this record in the existing centralized land registry. Blockchain is the registry itself. Moreover, we cannot have two sources of truth for one title, otherwise such duplication will require protection from double spending and avoiding collisions of records in both systems.

Hence, the title record should be stored exclusively in one of the available ledgers.

"Title registration vs registration of deeds"

Different countries have their specifics of the registration of deeds and titles. For example, in the USA, there is a registration of deeds (*27 V.S.A. § 342, The Vermont Statutes*, 2020) [4]. Therefore, to check who is the lawful owner of the title, there must be a valid chain of registered deeds (*27 V.S.A. § 601, The Vermont Statutes*, 2020).

Torrens system [Australia and some other countries (Hepburn, 2018)] and most civil law countries use the system of registration of titles (European Land Registry Association: Description of land registration systems, 2020). The cadastral land identifier is connected to the record of the current owner of the title.

Blockchain includes *both* types of information: the token (i.e. title) is attached to the address (owner) that corresponds with the title registration, but the token is always the result of a transaction. Thus, the chain of deeds is also viable as a way of representing the land registry database. Therefore, blockchain technology has a dichotomous nature that corresponds with both title- and deed-centric ways of registration.

"Will the government be detached from providing registration?"

The government agency provides for the authenticity of the database. If the record of property rights and titles are tokenized, then there is no need for a public body to keep this registry. Once the record is in the database, there is no need for one specific authority to prevent the database from corruption. Nevertheless, the registration itself must be lawful, which is a job of public bodies and other intermediaries. The future development may include deep automation of procedures that will eliminate public servants and middlemen in real estate transactions.

"Will a notary public be excluded?"

In many countries, notaries public must acknowledge the contract with immovable property. Blockchain ensures only one of the functions of notarization, inter alia, the timestamp. Other aspects of notarization are not automated; therefore, it can be a matter of future research and development. Otherwise, the notary must authorize blockchain transactions. Hence, the architecture of the system must include this third party in the process of real estate deeds.

The requirement of acknowledgment may exist in other forms and roles. For example, town's clerk or master in Vermont state do a similar job (USA) (*27 V.S.A. § 341, The Vermont Statutes*, 2020).

"How to enforce smart contracts?"

Smart contracts are limited with the code, while normal contractual relations, even though they have some autonomy, are still interlinked with the existing laws. When parties interpret clauses of the contract, they first look at what the contract says, but if the issue is not regulated directly by the contract, law, precedents, and general business practice are applied. This is beyond the current possibilities of the technology of smart contracts. There is no framework for "smart law," and this is something which probably will be developed in the future.

However, at a practical level, the real headache of the smart contract is enforceability. If no third party is initially involved in the role of the arbitrator in the algorithm of the smart contract, the smart contract can get stuck in a dispute. This should be addressed by the component of the "authority" (judicial power, notary, etc.) in the system. At least one solution is conceptualized already. The cross-blockchain protocol (Konashevych, 2019) provides for a systematic approach in governing legal relations in the bundle of blockchains.

The protocol accommodates the concept of "smart law" as the framework for smart contracts.

"Who will become nodes-validators?"

This is a question in the context of applying permissioned DLT. Despite that, the issue of "permissioned" and "permissionless" systems is addressed in the previous sections and the use of permissioned DLTs when the government solely introduces it will be a game of one team on the ground. We must note that the question becomes more interesting if the government shares control with some other nodes.

How are those nodes chosen, and why must the government compromise their sovereignty with someone? Whomever they choose from the long list of credible companies and NGOs, there will be the questions why others who also deserve to share the control over the system are left behind, and why some entities, which are not a public body, are raised to the level of governance. This is a constitutional level of discussion, and there is no systematic approach found in addressing this issue.

At the same time, when public blockchains are used, there is no issue of nodes-validators. Anyone can have a node and freely compete in "mining." Blockchains, in this case, play the role of secure public repositories where information cannot be erased, and government agencies are validators not of the blocks, but validators of records (see Figure 2) which citizens insert in the ledger provided the insertion itself is not censored, but any user is free to apply for the government validation to provide for credibility of their records.

For example, the registry office of land titles will ensure that the user's token represents the property rights. So, the user can interact with a counterparty remotely. Even without knowing each other, the counterparty will know that this is a title record on blockchain, because they will see the assuring record from the government agency.

This structure seems to be more acceptable because two things are distinguished:

(1) blockchain as a decentralized infrastructure for reliable and immutable storage; and

(2) the role of the government in relationships that are built upon this infrastructure.

"Hashing records of the land registry"

Previous research (Konashevych and Poblet, 2018a) showed that this application is limited in terms of its benefits. Moreover, improper design may create even more trouble for security. The use of the centralized and decentralized system (blockchain) makes no sense because there will be an issue with this source of truth in the case of a discrepancy.

There are some other issues with hashing. There is a need to provide identification, authorization, and authentication because blockchain provides only for pseudonymous authentication.

Also, publishing hashes does not provide for a secure store of the initial data itself. The user must protect the record, wherever they store it off-chain. The centralized storage for such entries will always be a target.

Also hash publishing does not provide knowledge of the validity of the record. Usually, land registries' databases are closed systems, and an outside observer who sees only DLT, does not know if any public hash is authorized or not. The insider may illegally change the record in the database and reveal the hash as if it was retrieved from the valid record. To address this issue, the government requires more transparency and better design of the hashing method.

However, the main concern about this method is probably that it does not provide any basis for tokenization on blockchain; the property rights records are still exclusively stored in the centralized government database.

"What is a token: Title, Property right, Security, or a New Legal Concept?"

The token is just a record in the ledger. It does not necessarily have any legal side, the same as not every record on a piece of paper creates any legal relationship.

To make any sense, it must be based on the law and the contract. Therefore, to answer this question, the user must look inside the token (literally inside because some methods allow including legal text with the record) or behind the token. For example, many early projects like Colored Coins (Colored Coins – Bitcoin Wiki, 2020) were based on bitcoins, and the legal logic was developed beyond blockchain protocol as an overlaid technology.

The applicable law must also be a part of this analysis because when the jurisdiction provides for a certain way and form of performing some legal relationships, the creation of the token out of the existing legal framework makes it legally invalid or void.

Therefore, a title right or property rights will be valid in the form of a token, which is performed lawfully with regards to the jurisdiction where it is created, as far is it known, no jurisdiction has dedicated any legal framework for that.

It may also be found in some discussions that the token has a completely new legal nature. During the boom of Initial Coin Offerings (ICOs), 2016–2018, tokens were not company shares or traditional assets.

This is nonsense, and if the token does not represent any property right or obligation, it does not have any legal essence at all. This kind of ICO can be considered as fraud. However, in some cases, the token had a derivative nature (even if not called so), and so had a nature of a property right. For example, the token as a "square meter" in the future real estate appeared to be a right to convert this token to the actual record of ownership in the future.

4. Practical issues with implementation

This section provides a few examples of issues which arise at the junction of blockchain, governance and real estate industry. Media news may create a perception of a large disruption. This research shows no revolution is on the way. Nevertheless, it is not time to put an end to it.

4.1 Political will and corruption

Implementation of a game-changing project may not start unless the government has the will to start it. One of the earliest pieces of news in the field of the use of blockchain for land registry proliferated in media in 2015 from Honduras with the help of Epigraph and Factom Inc. Being referred to by many enthusiasts for a long time, the project itself was never kicked off (Jun, 2018). No evidence is found that the government has ever supported this initiative.

Here we find not a technological constraint but a political one. Countries that have issues with transparency of their public administrations, corruption and protection of property rights can significantly benefit from blockchain — a tamper-proof, transparent, public and decentralized database; but the introduction of such technology depends on their political will. Thus, we a vicious circle.

4.2 Does any prosperous society want changes?

Chromaway was founded in Sweden in 2014, giving the hope of disrupting the old-fashioned centralized and bureaucratized land cadaster. Two papers revealed details of the pilot (*The Land*

Registry in the Blockchain – Testbed, 2017) with the Swedish land registry authorities (and other partners) and "Chromia," former name is "Chromapolis" (Chromapolis Platform. White Paper, 2018).

Both documents advocate the use of the centralized "private" DLT assigning this technology attributes and features of blockchain which are irrelevant.

In 2019 the team showed their centralized DLT platform and revealed a lab prototype app for title deeds (Walk through – Swedish Land Registry Smart Contract – YouTube, 2019). The app requires a government agency and participating intermediaries to acknowledge a transaction between counterparties.

Here is unveiled the second significant misconception. In general, the problem of the architecture of such systems is that records have legal force when they are stored in the closed governmental database; all peer-to-peer transactions on blockchain between parties make no sense, as far the last word is on the side of the one who controls the central registry. Therefore, they need legislative changes.

Without shifting from centralized to a distributed architecture, any attempts of disruption turn into mimicking the existing system. Nothing more happens than digitizing bureaucracy and middlemen.

However, Chromaway teaches us another lesson. Over five years, the project did not succeed in introducing a working system at the state level. Prosperous and highly developed societies are often discouraged in changing their existing system. What for, if it works, though imperfect? It must make extraordinary sense for changes, especially at the scale of a whole country. And the Swedish government has no incentive to let go of its monopoly on political power over the centralized cadastral registry.

It is early to put an end and draw conclusions from the Chromaway initiative, therefore, further observation and study of the case will be required in the future.

4.3 Do the plans match the state of affairs?

None of the above-mentioned examples stated that they had failed. However, it is found in media some mismatch of public expectations and reality. White papers and projects' websites are used as sources for analysis of plans and intentions.

Bitland has been in Ghana since 2014 on a project to "register land and real property ownership and use rights" using blockchain (Bitland. Land Title Protection Ghana, 2020). The available updates on the website do not specify the stage of development of the blockchain infrastructure and achievement of objectives. Propy Inc., during its ICO in 2017, stated that their far-reaching plans were to disrupt the industry by eliminating third parties with a global real estate supermarket on blockchain, driven by smart contracts (Propy: The Global Property Store With Decentralized Title Registry (White Paper), 2017). However, their system at this stage has no connection to any land registry, and their demo is closed for public use; only private access is available upon requests. Both projects are claimed to be ongoing and further observations and case studies may provide more knowledge in the future.

REX, founded in the USA in 2016, promised a new multiple listing system (MLS) standard for real estate brokers. Eventually, they introduced IMBREX – online ad listing protocol for brokers and landlords (IMBREX White Paper. A Decentralized Real Estate Data Exchange and Real Estate Transaction Application, 2020). This example shows that blockchain may be useful for intermediaries and may not trigger the public sector. There is no information of mass adoption of this protocol, therefore, it is too early to say if the protocol found its wide applicability.

Velox.re demonstrated in Cook County, IL (USA) how hashing on a blockchain can be applied for land registry but ceased its activities in this direction (Velox.re, 2018). No

intentions to continue were found, and neither the land registry office nor Velox.re articulated reasons for that.

Bitfury, in 2018, launched their centralized DLT based on the Exonum DLT framework in the Republic of Georgia (Republic of Georgia to Develop Blockchain Land Registry – CoinDesk, 2020).

In Ukraine, they also had intentions to introduce a similar project but abandoned it [5].

As the case study explains (Shang and Price, 2019), the project did not set out to build a brand new blockchain-based land title registry system for the Republic of Georgia.

The project purposed to hash records of the real estate database on the centralized DLT, based on Bitfury's framework "Exonum." The benefits of the use of centralized technology are not justified, and the wider discussion on this issue was previously published (Konashevych and Poblet, 2018b).

However, another conclusion besides the concerns on a centralized nature of architecture is that hashing does not lead to tokenization of real estate titles and/or digitization of property rights, nor any changes in the traditional bureaucratic way of land registration.

The discussed in this section examples are often referred to in the industry and academia. Stated ambitions of the projects and optimistic opinions in social networks may create a perception of much success in the implementation. However, this analysis shows, the cases should be further observed and scrutinized for an unambiguous assessment.

5. Conclusions

This paper provided a broad overview of the use of blockchain and other DLTs in real estate, with the focus on title rights and property registration in public databases.

Speculation about the use of blockchain is limited to the list of services blockchain can provide. It can either be used as cryptocurrency for payments, or as a storage for applications and records, including property rights and titles which can be managed by tokens and smart contracts.

Nevertheless, these things can be done with more traditional centralized electronic systems. The distinguishing feature that unites all this – a decentralized consensus. The consensus protocol is a logic of how these services are created and legitimized in the system. The major element in blockchain that supports decentralization is the mechanism of randomness, where nodes compete for the right to create new blocks and to offer them to the network, known as mining, minting, staking, forging, etc. In different consensus protocols, there are methods of how to increase the probability of getting the right to create a new block, but they are still relative and randomness is the key thing; if this balance is broken, then the network becomes centralized – meaning there is someone who can dictate the right version of the protocol and database.

Centralization means the ability to change the protocol and effect the history of transactions, or even to rewrite the blocks and to censor incoming transactions.

Permissioned and private DLT systems cannot be considered a significant evolutionary step in government systems. Blockchain, which is distinguished from permissioned systems as the technology of the immutable ledger that does not require authorities, is a new word in governance.

However, this technology has some principal features that can restrain its implementation at the state level, and thus require further research and development. In particular, the application of blockchain requires proper architecture of the overlaid technologies to support changes for outdated and mistaken data (to overcome the problem of immutability), address issues of digital identity and privacy, legal compliance and enforceability of smart contracts, hardforks and scalability of the ledger.

The applicability of blockchain for real estate relationships, i.e. land registration, deed acknowledgement, and managing of property rights (titles) requires a systematic rethinking of the constraints and benefits of DLT technologies along with the purposes.

Tokens can represent land titles and other property rights. It makes no sense to distinguish tokens as title records from the transactions because they are technologically inextricable. Therefore, the land registry cannot co-exist with the blockchain as a standalone system. Blockchain is a registry itself. It indicates both: records of property rights (titles) and records of transactions (deeds). Therefore, blockchain fits both legal traditions of property registries, i.e. keeping title records (Torrens system and civil law) and keeping chains of deeds (common law system). It is clear that it is not possible to transfer the whole cadastral system to the blockchain in one night for various reasons (technological, political, organizational, legal). Instead, the traditional public registry and blockchain systems can work in parallel, and therefore, citizens will have the right to choose where they want to manage their property rights. This approach will ensure technological neutrality and competition of technologies. The role of the government in this case is to ensure high security standards and legislative support, because normally there is no such choice for citizens and the land registry is a monolithic centralized system. Future blockchain development and implementation may include deep automation of bureaucratic procedures that will eliminate public servants and middlemen in real estate transactions.

More empirical research and technical analysis is to be done to develop a substantial knowledge in this field.

Notes

1. Nick Szabo developed the idea of a smart contract in pre-blockchain period (Szabo, 1997).
2. The term "smart contract" is proposed by Szabo (1997).
3. Murphy's law is an adage or epigram.
4. Vermont state is chosen as an example.
5. According Viktor Vyshnov's report, General Director of the State Ukrainian Enterprise "SETAM", at Industry 4.0 & Blockchain Conference, www.blockchaingeorgia.org, September 28, 2019, The University of Georgia, Tbilisi, Republic of Georgia.

References

27 V.S.A. § 341, The Vermont Statutes (2020), *VT*, available at: https://legislature.vermont.gov/statutes/section/27/005/00341 (accessed 31 December 2019).

27 V.S.A. § 342, The Vermont Statutes (2020), "The Vermont statutes online", *VT*, available at: https://legislature.vermont.gov/statutes/section/27/005/00342 (accessed 30 December 2019).

27 V.S.A. § 601, The Vermont Statutes (2020), "The Vermont statutes online", *VT*, available at: https://legislature.vermont.gov/statutes/section/27/005/00601 (accessed 30 December 2019).

Androulaki, E. Karame, G.O. Roeschlin, M. Scherer, T. and Capkun, S. (2013), "Evaluating user privacy in bitcoin", *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Vol. 7859 LNCS, p. 596.

Bitland. Land Title Protection Ghana (2020), available at: www.bitland.world/about/ (accessed 5 January 2018).

Blockchain Overview: Australian Government Guide (2018), available at: www.dta.gov.au/help-and-advice/technology/blockchain/blockchain-overview-australian-government-guide (accessed 18 December 2019).

Chromapolis Platform. White Paper (2018), Chromaway, available at: https://chromapolis.com/papers/chromapolis-platformwhitepaper.pdf

Colored Coins – Bitcoin Wiki (2020), available at: https://en.bitcoin.it/wiki/Colored_Coins (accessed 30 December 2019).

Cost of a 51% Attack for Different Cryptocurrencies | Crypto51 (2020), available at: www.crypto51.app/?fbclid=IwAR15KMMvqM6SydcPJ7c3XfZjMatogrp584ZfkswH8jD2xyAgtFgulPeuC0I (accessed 16 September 2019).

Data.gov.ua (2020), available at: https://data.gov.ua/ (accessed 16 September 2019).

Dawes, S.S. (2008), "The evolution and continuing challenges of e-governance", *Public Administration Review*, Vol. 68, pp. S86-S102.

Emercoin NVS – Emercoin Community Documentation (2020), available at: https://emercoin.com/en/documentation/blockchain-services/emernvs (accessed 28 June 2018).

EOS.WIKI (2020), available at: https://eos.wiki/ (accessed 27 December 2019).

Ethereum Wiki (2017), available at: https://github.com/ethereum/wiki/wiki/Glossary (accessed 4 July 2017).

European Land Registry Association: Description of land registration systems (2020), *ELRA* available at: www.elra.eu/facts-sheets/description-of-land-registration-systems/why-register/ (accessed 30 December 2019).

Hepburn, S. (2018), *Australian Property Law: Cases Materials and Analysis*, 4th ed.

Higgins, S. (CoinDesk). (2014), "8 million vericoin hack prompts hard fork to recover funds", available at: www.coindesk.com/bitcoin-protected-vericoin-stolen-mintpal-wallet-breach/ (accessed 31 December 2016).

IMBREX White Paper. A Decentralized Real Estate Data Exchange and Real Estate Transaction Application (2020), available at: https://about.imbrex.io/white-paper.html (accessed 14 June 2019).

Insanity: Ethereum Wallet Pays Nearly $575,000 in Fees to Transfer $25 in ETH (2020), available at: www.newsbtc.com/2019/02/21/ethereum-wallet-fees-eth/ (accessed 4 February 2020).

Jansen, A. (2012), "The understanding of ICTs in public sector and its impact on governance", *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *LNCS*, Vol. 7443, pp. 174-186.

Jun, M. (2018), "Blockchain government-a next form of infrastructure for the twenty-first century", *Journal of Open Innovation: Technology, Market, and Complexity*, Vol. 4 No. 1, p. 7.

King, S. and Nadal, S. (2012), "PPCoin: peer-to-peer crypto-currency with proof-of-stake", available at: https://peercoin.net/whitepaper

Konashevych, O. and Poblet, M. (2018a), "Blockchain government-a next form of infrastructure for the twenty-first century", *Frontiers in Artificial Intelligence and Applications*, Vol. 313 No. 1, pp. 195-199.

Konashevych, O. and Poblet, M. (2018b), "Is blockchain hashing an effective method for electronic governance?", *Frontiers in Artificial Intelligence and Applications*, Vol. 313, IOS Press, pp. 195-199.

Konashevych, O. (2019), "Cross-blockchain databases for governments: the technology for public registries and smart laws", ArXiv.Org, available at: http://arxiv.org/abs/1912.01713 (accessed 30 December 2019).

Loibl, A. (2014), "Namecoin", 10.2313/NET-2014-08-1_14.

Malinauskienė, E. (2013), "Conceptual framework for context-based e-government interoperability development", *Social Technologies*, Vol. 3 No. 1, pp. 68-84.

Nakamoto, S. (2008), "Bitcoin: a peer-to-Peer electronic cash system".

Namecoin.org (2020), available at: https://namecoin.org/ (accessed 5 September 2018).

Ober, M., Katzenbeisser, S. and Hamacher, K. (2013), "Structure and anonymity of the bitcoin transaction graph", *Future Internet*, Vol. 5 No. 2, pp. 237-250.

Proof-of-work (PoW) – BitcoinWiki. (2020), available at https://en.bitcoinwiki.org/wiki/Proof-of-work (accessed 27 December 2019),

Propy: The Global Property Store With Decentralized Title Registry (White Paper) (2017), Propy, available at: https://whitepaper.io/document/288/propy-whitepaper

Raval, S. (2016), *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*, 1st ed., O'Reilly Media, available at: https://dl.acm.org/citation.cfm?id=3074145 (accessed 27 December 2019).

Republic of Georgia to Develop Blockchain Land Registry – CoinDesk (2020), available at: www.coindesk.com/bitfury-working-with-georgian-government-on-blockchain-land-registry (accessed 12 July 2019).

Roio, D.J. (2013), *Bitcoin, the end of the Taboo on Money*, Dyne.Org Digital Press, pp. 1-17.

Schneier, B. (1996), *Applied Cryptography: Protocols, Algorithm, and Source Code in C, Second Edi*, John Wiley and Sons, Inc., doi:10.1016/S0740-624X(96)90083-0.

Shang, Q. and Price, A. (2019), "A blockchain-based land titling project in the republic of Georgia: Rebuilding public trust and lessons for future pilot projects", *Innovations: Technology, Governance, Globalization*, Vol. 12 Nos 3/4, pp. 72-78.

Sward, A., Vecna, I. and Stonedahl, F. (2018), "Data insertion in bitcoin's", *Ledger*, , Vol. 3, pp. 1-23.

Szabo, N. (1997), "Formalizing and securing relationships on public networks", *First Monday*, Vol. 2 No. 9, doi: 10.5210/fm.v2i9.548.

The Land Registry in the Blockchain – Testbed (2017), available at: https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

The State Fiscal Service of Ukraine (2016), available at: http://sfs.gov.ua/media-tsentr/novini/245619.html (accessed 30 December 2019).

Trček, D. (2006), "Managing information systems security and privacy", *Managing Information Systems Security and Privacy*, doi: 10.1007/3-540-28104-5.

UNIAN Information Agency (2016), "The fiscal service lost more than 500,000 documents", Kyiv, 18 April, available at: www.unian.ua/economics/finance/1322681-fiskalna-slujba-vtratila-ponad-500-tisyach-dokumentiv-zmi.html

Velox.re. (2018)

Walk through – Swedish Land Registry Smart Contract – YouTube (2019), Chromaway, available at: www.youtube.com/watch?v=nkMm8PBozjI (accessed 30 December 2019).

Wood, G. (2015), "PoA private chains · GitHub", *GitHub*, available at: https://github.com/ethereum/guide/blob/master/poa.md (accessed 30 December 2019).

Corresponding author
Oleksii Konashevych can be contacted at: oleksii.konashevych2@unibo.it

PAPER 4

doi:https://doi.org/10.15407/emodel.41.05.103

UDC 004.056.55, 347.441.142.52

O.I. Konashevych
Erasmus Mundus Joint International Doctoral Fellow in Law, Science and Technology
(Via Galliera, 3, 40121, Bologna, Italia;
e-mail: oleksii.konashevych2@unibo.it)

Data Insertion in Blockchain For Legal Purposes. How to Sign Contracts Using Blockchain

The use of blockchain technology, in particular, data insertion (anchoring, hashing) in the blockchain as a way of signing documents or imparting legal properties to facts is researched. A comparative analysis of the known methods of using electronic digital signature with the method of inserting data into the blockchain is carried out. The following issues were addressed. What is the data insertion in the blockchain and what properties do the data acquire? What is the difference between insertion, anchoring, and hashing on the blockchain? What is the difference between blockchain hashing and a digital signature on a document? Will the document be legally binding if it is anchored in the blockchain? What conditions must be met to give legal force for the document? How can anchoring be used to sign contracts, certify evidence that has legal value, denote time stamps, confirm authorship and copyrights, as well as transfer them, issue, and transfer power of attorney and delegate other rights, issue and transfer bearer instruments?

K e y w o r d s: Blockchain, OP_DROP, OR_RETURN, electronic signature, eIDAS, PKI, proof-of-existence.

Introduction. The blockchain has been designed to securely store transaction data [1]. However, starting from the first block, non-payment information was inserted into the database, also as «ledger» [2]. Since then, not only different methods of inserting data into Bitcoin have been invented, but a variety of blockchains appeared specifically designed for such and similar purposes. Although the technical side of the question of inserting data into the blockchain is already well studied, not much is said about the use of data insertion for legal purposes. In publications [2, 3], the accumulated experience of data insertion on Bitcoin is revealed.

Therefore, we decided to explore this area and answer the following questions. What is data insertion in the blockchain and what properties do the data acquire? What is the difference between insertion, anchoring, and hashing on the blockchain? What is the difference between blockchain hashing and a digital signature on a document? Will the document be legally binding if it is anchored in the blockchain? What conditions must be met in order to give legal force for document?

How can anchoring be used to sign contracts, certify evidence that has legal value, denote time stamps, confirm authorship and copyrights, as well as transfer them, issue, and transfer power of attorney and a general concept of delegation of rights, issue, and transfer bearer instruments and others? To understand blockchain technology and how a distributed ledger and infrastructure work, the reader must understand the basics of cryptography: asymmetric pair, cryptographic hash function. Therefore, it is recommended that you first expand your knowledge in this area.

Data insertion for legal purposes. 1. *What is data insertion in the blockchain?* There are a few methods of data insertion in the blockchain. The analysis of known methods in Bitcoin can be found in this paper [2]. However, this can be irrelevant in some aspects for other blockchain protocols. Accordingly, to summarize the existing experience of data insertion in the blockchain, we will emphasize the following. The arbitrary data is inserted into the blockchain as the result of a transaction. By the transaction, it is understood that the individual has spent some cryptocurrency. However, this is not a normal sending of «coins» to someone but a transaction when some cryptocurrency is permanently immobilized («burned») in the result of the application of some scripts (OP_RETURN, OP_DROP, etc.).

Such transaction as any other on the blockchain is signed by the sender using their asymmetric cryptographic private key. The user attaches arbitrary data which is signed within the body of the transaction.

The use of the blockchain provides a set of advantages, which are inherent to the blockchain itself:

I m m u t a b i l i t y. Once published on the blockchain the data cannot be altered or deleted; therefore, it is tamper-proof.

P u b l i c. User's data is stored on each node of the network; therefore, it is public.

U n c e n s o r e d. Using the blockchain is permissionless. The only condition of the transaction being accepted by the network is that it must be performed as per the blockchain protocol. Because each node is a carrier of the copy of the protocol, each block of transactions is verified by mining nodes. When the node propagates a new block to the network, other nodes using the same set of rules verify the validity of this block before to add it to their copies of the ledger.

P e r m a n e n t a c c e s s. The published data in the blockchain database can be retrieved from any remote node in the network, and the system will work while at least one node exists, including a local node as well.

T i m e s t a m p. The blocks of the transactions are sequentially «chained», and because of immutability, the chronology is preserved as well. Therefore, the time and date of any transaction are available with the accuracy of the average time of block creation (for example, in Bitcoin it is 10 minutes in average).

P s e u d o n y m o u s (anonymous[1]). Each transaction belongs to a specific blockchain address[2]. To spend the balance from the address, the user must have only the private key to this address. The address itself is retrieved from the public key. Therefore, users are authenticated only by their private keys.

There are some negative aspects of data insertion. One of the main concerns is about ledger overfilling. This is because the blockchain is a distributed database on which copies are kept by every node of the network. During ten years of operation Bitcoin database grew up to 197 Gb [7], and after four years Ethereum grew to 720 Gb [8].

Such redundancy is emphasized, for instance, in Bitcoin wiki in a discussion of one of the existing methods of insertion: «Many members of the Bitcoin community believe that use of OP_RETURN is irresponsible in part because Bitcoin was intended to provide a record for financial transactions, not a record for arbitrary data» [9].

2. *What does it mean to insert the data?* The user may wish to insert in the blockchain the data itself or anchor it by publishing a hash. The method of publishing itself is constrained by the maximum size of data, which can be inserted in one transaction. The maximum size depends on a chosen method and script and can be from 8 kB to ≈50 kB, which is not much from the perspective of usability[3]. For the reason of data redundancy but not as the main one, it proposed to store checksums (hashes) of data. Those hash functions are based on «strong cryptography»[4] [10] and provide for some advantages against keeping data itself [5]:

---

[1] In paper [1] of Satoshi Nakamoto offers to ensure privacy by keeping keys anonymous. However, some researchers [4, 5] claim that it does not guarantee complete privacy because other digital fingerprints (IP addresses, behavioral patterns and others) can disclose the user; instead of this, it is proposed to use the term «pseudonymity» instead.

[2] The blockchain address is retrieved from public key, see [6].

[3] It should be noted that, some blockchain similar technologies (distributed ledger technologies, DLT) are purposely developed to store unlimited amount of data. In other cases nodes do not store the data in the ledger as well or at least not all of the nodes, therefore, the information is not copied to every node of the network, instead some approaches to reduce data redundancy are applied (Maidsafe, Storj etc.).

[4] According to PCI DSS and PA-PSS (2016), as of the publication day of these standards, industry-tested and accepted standards and algorithms include AES (128 bits and higher), TDES/TDEA (triple-length keys), RSA (2048 bits and higher), ECC (224 bits and higher), and DSA/D-H (2048/224 bits and higher). See the current version of NIST Special Publication 800-57 Part 1 (http://csrc.nist.gov/publications/) for more guidance on cryptographic key strengths and algorithms.

[5] There can be different types of hashes. Here we are talking about cryptographic hashes. Other hash functions may not necessarily provide for mentioned advantages.

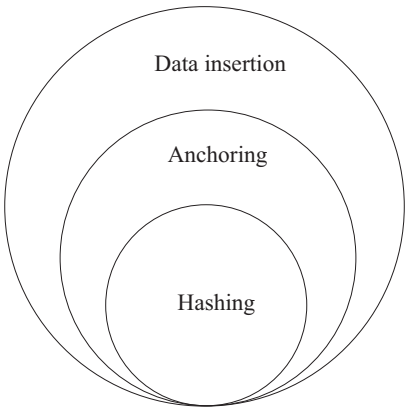


Fig 1. Relationship diagram: data insertion, data anchoring and data hashing in the blockchain

P r i v a c y. User's data does not become public. Hash is the result of a one-way function. It is not feasible to generate a message from its hash value (often also called a «digest» or a «checksum») except by trying all possible messages [11], which in practice is extremely difficult when strong cryptography is used.

A u t h e n t i c i t y v e r i f i c a t i o n. When the file is not inserted, the blockchain cannot protect an integrity of it itself, but it can provide for an auditability of integrity. When a hash function is applied, the same message results in the same hash with the negligible probability of a collision [12] if the strong cryptography is in use. Therefore, to verify the integrity of data, the user can compare the output hash with the hash which was earlier published in the blockchain.

The existing experience of data insertion in the blockchain is showed in the following relationship diagram (Fig. 1), from which the relationship diagram is: data insertion, data anchoring and data hashing in the blockchain. We can see that data insertion is a general concept attributed to any insertion which includes the subset of anchoring and hashing. When not the message itself but something which represents this data is inserted, it is referred to as a notion of «anchoring». Hashing is a subset of anchoring, referred to publishing hashes (usually understood as cryptographic hashes) in the blockchain. Anchoring in general might be referred to publishing of non-cryptographic hashes and some other data which may represent the original file (date, time, index number, author etc.).

The second column of Table 1 shows the properties that the original data source acquires when it is directly inserted into the blockchain and in the third column, the properties that acquire the data, if not the data itself is published in the blockchain, but only their hash sum.

3. *What is the difference between digital signing and blockchain hashing*? This question can be raised considering that a blockchain transaction is signed using an asymmetric cryptography. As it known, asymmetric cryptography is widely used beyond blockchain transactions. For example, to sign legal documents (transactions).

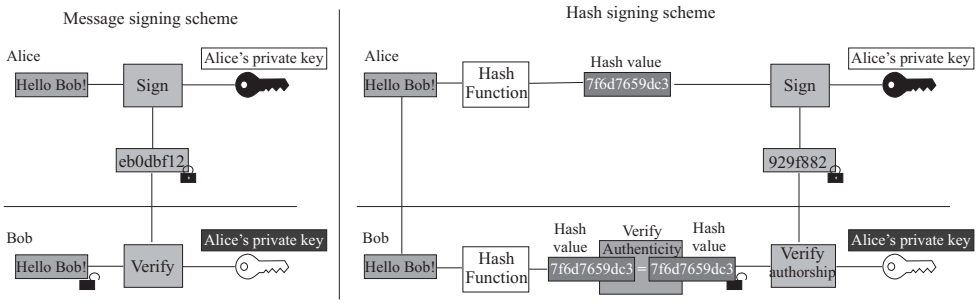


Fig. 2. Comparison of signing schemas: «message recovery» vs. «signature with appendix» (hash signing)

Table 1

Source	Data insertion	Hashing insertion
User's data become	Public	Private
	Limited (up to 50 kB)	Unlimited
	Tamper-proof	Verifiable

There are two basic approaches in terms of what to sign: the data (the message) or the hash (the message hash)[6] [13]. It means that the user may decide to apply a digital signature to the legal document itself or to sign the cryptographic hash of the document, which is presented on Fig. 2.

In the first scheme the message is encrypted by Alice's private key, and then Bob decrypts it using Alice's public key. In the process of decryption Bob recovers Alice's initial message. The difference in the second scheme is that Alice encrypts not a message, but a hash of the message, and Bob recovers this hash. The hash without the message is useless for Bob, that is until Alice also sends him the original message. Therefore, Bob calculates the hash from the message and compares the two hashes. If they are equal, then Bob understands that this is the original message which belongs to Alice. The hash signing scheme is widespread; however, some other schemas exist, but this is not crucial for the level of our discussion.

[6] To sign a digest message (hash value) is a scheme also known as "signature scheme with appendix" developed in Public Key Cryptography Standards # 1 (PKCS#1, based on RSA-PSS standard). The implementation can be found in RFC 8017 https://tools.ietf.org/html/rfc8017, and a similar approach is found in DSS-DSA standard (US Federal Information Processing Standard) and ENISA Standards (EU); this method is opposed to the initial concept of message signing, which however is also standardized. For example, ISO/IEC 9796-2:2010 — Information technology — Security techniques — Digital signature schemes giving message recovery.

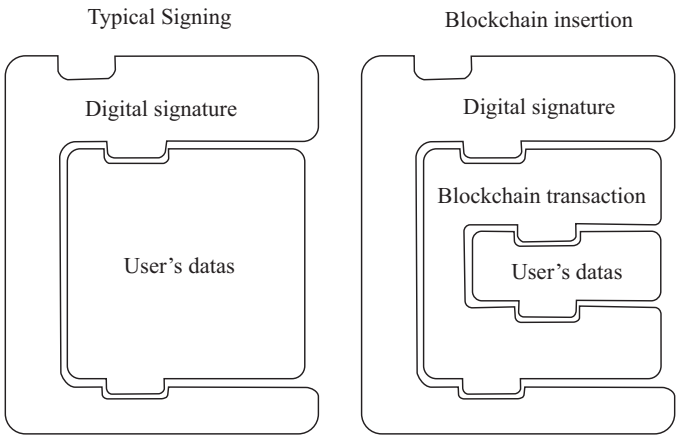


Fig. 3. Typical document e-signing vs. insertion in the blockchain

In typical digital signing, as an input is taken, only user's data (a document or a hash value) is to be signed, but in the blockchain, both the transaction data and user's data are signed (Fig. 3). In blockchain scheme it can be seen that the user's data can be a document itself or a hash of the document. Therefore, the practice of asymmetric cryptography is still in place in such case when the blockchain is applied: either document inserted itself, or a hash of it. In both situations this data is signed within the blockchain transaction with the user's private key. Some principal differences are found in comparison with the use of a Public Key Infrastructure.

4. *Public Key Infrastructure and Blockchain.* More substantial differences are apparent in a comparison of document e-signing with the use of Public Key Infrastructure (PKI). PKI is a set of technologies and procedures that enable the deployment of public-key cryptography-based security services [14].

In practice, to use digital cryptography for signing legal documents, many countries introduced regulations that mainly provide for:

trust services – which are performed by Certificate Authorities[7] (CA) or Trust Service Providers[8] (TSP) to identify signatories, so they can interact with each other remotely.

Timestamp – To guarantee that during signing, the trusted third party provides for a timestamp, known as a Time Stamping Authority [9] (TSA) or a Trusted Timestamp Authority[10].

---

[7] More common name in the USA.

[8] An official name as per eIDAS regulation in the EU.

[9] Typically in EU [15, 16].

[10] Terminology commonly used in the US [17].

Obviously, there are a lot of other aspects of PKI relationships. The regulations are supplemented with a set of technical standards and best practices.

A distinguishing feature in a blockchain is that it does not require TSA as a standalone service. As mentioned, the timestamping is an inherent feature of the technology that does not require any trust to a certain provider but depends on a distributed consensus scheme, in some academic literature this is called «decentralized trusted timestamping» [3].

As to identity, the blockchain is the technology that provides for pseudonymity. The blockchain address works as an authentication and authorization mechanism meaning that only the holder of the private key to this address can perform a transaction. Therefore, the blockchain itself can be called a decentralized pseudonymous PKI. At the same time, PKI-based identity services are standards that allow trusted parties (usually authorized/licensed by the government) to provide IDs. Similar services can also be applied as an overlay service of a blockchain infrastructure.

One of the most developed PKI schemes is in the EU and was introduced by eIDAS regulation [18]. Typically, the scheme is the following: TSP identifies a user in person and generates an asymmetric pair using one of the recognized standards. The public key is signed by such TSP and included in a certificate (using x.509 standard), which then is uploaded to a public repository. When the user computes a signature for a document using their private key, the software enquires a timestamp from the TSA server and includes it in the signing package. When the timestamp is retrieved and the signature of the document is computed, the system will form a data package in a container (see for details standards XAdES, CAdES, PAdES, and ASiC [19]). An addressee of the signed document will check the certificate (valid or not at the time of signing) and will verify the file and the digital signature. The successful verification means that an addressee holds a copy of the document, which is signed by the person who is specified in the certificate.

To ensure the sustainability of this system, there are some mechanisms to revoke certificates when the key is outdated, lost or compromised. To enable an Advanced electronic signature (AES), the TSP provides a scheme for multifactor authentication of the user and some other technical and organizational measures, which add more reliability that the transaction is signed exactly by the claimed person.

To enable a Qualified Electronic Signature (QES), the TSP provides for the highest standards of the security, including hardware devices for signing. The user will use only a certified device that computes the signature on a secure cryptoprocessor [20] (smart cards, USB devices, etc.). QES signature guarantees the authenticity from the point of view of the technology and the law.

The European Union Agency for Network Information Security (ENISA) issued a guidance brochure where they explained «non-repudiation of a signature» as a signature for which the signatory cannot deny that they are the originator of such a signature. For that reason, signature is archived with a set of technologies and standards described as follows: «Such electronic signatures thanks to the obligations set by the eIDAS Regulation on both the TSP managing them (in particular the CAs) and on the underlying technologies: warrant data integrity, identify the signatory with a high level of certainty, and ensure the non-repudiation of signing» [21].

This system is also typical in many other countries and based on the high attention of the government in this domain and thorough regulation and standardization. However, eIDAS also guarantees for technological neutrality and does not deprive any electronic signature of its legal force only based on the premise that it does go along with existing standards or accepted schemas [18]. Nevertheless, the use of other e-sign schemas may require proof of the evidentiary value in any concrete case. For that reason, there may be applied a methodology introduced by UNCITRAL.

5. *UNCITRAL and Legal Validity.* An electronic signature is considered to be reliable as per the requirements provided in [9]:

«(a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) any alteration to the electronic signature, made after the time of signing, is detectable;

(d) where the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable» [22].

An analysis of the blockchain insertion. Requirement (a) is ensured by the strong relationship between the signatory and the document by the use of asymmetric cryptography, where the blockchain address (public key) is an identifier. Requirement (b) is also ensured by the nature of asymmetric cryptography: the right to sign the transaction exclusively belongs to the holder of the private key, meaning that technically there is no any other way except by this key.

Of course, any fact of unauthorized seizure and use of the private key ends the legal validity of the e-signature. In [9] of the mentioned article discusses the level of reliability: «Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was

generated or communicated, in the light of all the circumstances, including any relevant agreement».

For that reason, to ensure requirement (b) of being «under the control of the signatory and of no other person», the use of the blockchain may require overlaid services of identification and authentication, which depend on a combination of certified hardware, standardized software, and participation of an authorized trust service provider (CA/TSP).

The compliance with the requirements (c) and (d) – the integrity of the signature and data itself is also based on asymmetric cryptography. The usage of asymmetric cryptography itself can provide for a certain level of reliability to the transaction notwithstanding the use of the blockchain.

The analysis is correct for the blockchain, which is based on a standard asymmetric signature among the existing; otherwise, it may require additional expertise of the applied cryptography itself. For example, Bitcoin is based on ECDSA cryptography, which is a standard in the USA, EU, and many other countries. The compliance of the used technology to any certain standard is ensured by the fact that blockchain is open source, and thus, verifiable.

6. *Applicability.* The usage of any blockchain requires an understanding of whether the network itself it reliable or not. As of the day of publication, there are no technical standards that allow for formally defining the security of the network, but it is clear that the network with 3 nodes is less reliable than the one having three thousand. Therefore, an empirical analysis of number of nodes, hash rate, consensus mechanism, and existing experience of the use will help to find a proper blockchain for concrete legal tasks.

As it was found, data insertion inherits both features of the asymmetric cryptography and the blockchain. In practice, blockchain provides for a reliable decentralized timestamping and a secure immutable public repository.

Being decentralized, timestamping becomes more effective: disappears so called «single point of failure», meaning that the risk of corruption, multiple sorts of denial-of-service attacks is much lower especially if we are talking about scaled blockchain networks. At the same time, the transactional costs as to the achieved level of data protection and timestamping are affordable if not say, low. For example, the cost per publication in Emercoin is around 0,1 cents of US dollars (at the time of this publication). The average cost per transaction in Bitcoin is 2 US dollars, and at the highest historical point of exchange rate, it was around 25 dollars, which still can be affordable, for example, if the alternative to timestamping of copyrights is a visit to a notary public in person, which can be costly and time-consuming.

Timestamping is important for contracts, protection of copyrights and authorship and other evidence where proof-of-existence is required. But before the

blockchain, timestamping itself was not an open issue, the blockchain just raises the reliability of timestamping when compared to previous technologies. The real advantage of the blockchain is that it can extend the use of electronic communication, make it more «smart».

When data insertion is applied with some sort of blockchain-based technologies as tokens (Ethereum, NXT, NEM and others), smart contracts[11] (Ethereum, EOS and others), name-value storage (NVS) (Emercoin, Namecoin and others), it can make legal relationships more «intelligent» and interactive. The electronic document, while it is a file, is still a paper analogy – «flat» and non-interactive. With blockchain, the user can issue bearer instruments, power of attorneys, transfer and manage rights online.

For example, an artist can create a copyright and use www.emernotar.io to protect it in the blockchain. The artist will publish via this web-service in Emercoin a hash sum of the file adding a hash of his/her identity with the help of PayPal payment. In the result, the artist will have a NVS record[12] in Emercoin blockchain [24], where «Name» field is a hash record of the created picture and the field «Value» which contains the hash of email of a PayPal account which was retrieved as a result payment (therefore, the payer is the owner of the record). The user may also wish to add to this record a license data or any other public message. Then such NVS record can be transferred (i.e. sold) to any other user, and copyrights are transferred as well.

Another example can be a power of attorney. The hash of the file that contains the text of a power of attorney can be inserted in a NVS record or a smart contract. This then carries this data and has an expiration date and can be terminated by the issuer. To check the authorization of the attorney, the counterparty will check the integrity of the file by comparing hashes, and the status of NVS record or smart contract will tell the user if delegated rights are still valid or not. In «flat» paper PoA or even in an electronic file digitally signed, that would not

[11] Usually the term «smart contracts» is attributed to [23], however, Ethereum introduces their smart contracts as a tool for creating applications, which by fact are not necessarily contracts.

[12] Name-Value Storage is similar to the concept of tokens but non-monetary. In this record, data is stored in the form of «key & value» pair. «Name» is a searchable indexed key, and is always exclusive in the database; therefore, no one can create the record with the same Name while it is valid. «Value» is the second field, where the user adds any arbitrary information related to this Name (for example, user's name and telephone number). The NVS record is valid during the period defined by the user. The NVS record can be transferred to any other user of the blockchain, terminated or updated. In all these cases the initial record is not changed (the data is immutable in the blockchain) but new records with the same Name are inserted in following blocks with the updated information. See more details in Namecoin https://namecoin.org / and Emercoin https:// emercoin.com/

be possible, the principal cannot remotely revoke PoA at any moment, or vice versa to issue a new document or extend the existing PoA in minutes.

Another important feature of that as any closed system it can provide for proof of non-existence. It should be noted that «evidence of absence» is a fundamental gnoseological issue [25]. To assert the absence, one needs to check all the existing places, after which it can be argued there is nothing found. Due to the fact that the blockchain is a closed database, it can serve as a solution for a reliable local proof of non-existence.

This is important for jurisprudence since the parties can agree that a certain fact should be reflected in the blockchain to trigger the legal consequences for them or some rights and obligations to appear. The absence of the expected data in the specified blockchain will be considered as reliable evidence for private relations.

To mention here that the original blockchain protocol does not have a native lookup tool for inserted data. But for practical use, especially for legal purposes, it is important to have a reliable data retrieval system. To provide for the exclusiveness of records, there must also be developed algorithms that deny repetitive insertion, if the same data has ever been published thereof. There is no known implementation in the blockchain as a part of protocol core by the moment of this publication, but it can be be developed as an overlaid technology using the Name-Value Storage technology and custom developed decentralized applications (DApps) using smart contracts.

The main idea of this solution is that algorithms trace the ledger and select the inserted data to the custom database, which is by the fact an interpreter (the filter). When the user tries to publish the same data (for example, in «key-value» pair where the field «key» must always be exclusive through the whole database), the algorithms will then deny the publication. By fact, such «watchdog» can be omitted by publishing directly to the ledger the same record because as we mentioned above, the blockchain has no native censorship mechanisms to filter data (except the double spending denial), which is already published. Anyway, double publishing does not make much sense, because there is still timestamping, and strict chronology is in place. So, the first record is always the first, and the evidence of absence thereof is achieved by the whole scan of the ledger. Therefore, the role of a data retrieval mechanism is very important here, as it must present the reliable result of the search in the ledger.

Also, the blockchain database can be used for public purposes. For example, the government can keep cadastral records of ownership of real estate. The difference is that the blockchain is a distributed database that does not require a high level of trust in the central holder of such a database. However, this is a topic for another research, as there are a lot of other legal issues as well.

Table 2

#	Issue	Comment
1	Is the blockchain reliable?	Consensus mechanism, number of nodes, hash rate, history of successful use helps assess the reliability of concrete technology.
2	Which asymmetric cryptography is in use?	Is it a standard cryptography? Which standard? Is there any expertise of the compliance with the standard? If the cryptography is not standardized, is there any expertise? Does it comply with Art.6 of UNICITRAL Model Law on Electronic Signatures?
3	Which method is chosen: data insertion, anchoring or hashing?	Anchoring is useful if other metadata must be published. Data insertion for public purposes, and to protect the data integrity itself. Data integrity and privacy are also provided if data is ciphered. Hashing is for privacy and for verification of data authenticity, but the user must securely keep the data itself beyond the blockchain.
4	What method of data insertion is chosen? How much data can be inserted per one transaction?	Different scripts and methods provide for different file capacity limits. There may be some constraints, and theoretical flaws that must be taken into account depending on the purpose and required reliability.
5	Is there a reliable data retrieving mechanism from the ledger?	The blockchain wallet may not necessarily have native lookup tools or they may not have a user [friendly] interface.
6	Are there tools for the search of proof-of-existence or proof-of-non-existence?	Typically, the blockchain will not have native censorship mechanism. Therefore, the applied filters must be reliable and correspond with the use case. If the task is proof-of-existence and exclusiveness, only the first record must be considered as valid. If local proof-of-non-existence, then the absence through the whole ledger must be ensured.
7	Is exclusiveness of entry necessary?	If so, then take into account that a blockchain is designed as free of censorship. Therefore, there needs to be some sort of «watchdog» solutions developed on top to ensure that the same data will not be inserted, otherwise, the lookup instrument need to know how to filter irrelevant data when finding the first ever entry. Such overlaid solutions are available in Name-Value Storage technology (Emercoin, Namecoin and others) or if designed through a smart contract/DApp (Ethereum, EOS, TRON and others).
8	Is there an applicable law or an agreement between the parties to use the blockchain for a contract signing?	Any specific jurisdiction may or may not provide a framework for electronic signing. And thus, do parties need to have a prior-agreement where they mutually recognize blockchain signing/insertion as legally binding for themselves (if the law does not provide this by default)?
9	Are identity and authenticity reliable?	Typically, trusted third parties (CA/TSP) may provide for identification and authentication services. As many standards and best practices are applied as better, as they all are imperfect. However, any use case may require a different level of identification/authentication.

Ending of Table 2

#	Issue	Comment
10	If data insertion is used for copyrights	The non-third-party scheme may include a prior "handshake" when signatories identify each other and exchange with each other their public keys (blockchain addresses) by meeting in person, for example. Signatories may publish their public keys through their public social accounts or perform a penny bank transition or use other services which are not purposed to provide ID services howbeit can be relevant evidence as well. A good practice is if an author will: insert in the blockchain the hash prior to sharing the file anywhere include license terms in the publication include the author's name (pseudonym) or hashes of their contact details (if privacy is preferred) publish blockchain transaction ID in their public social account or use third-party services to connect transaction ID and their identity (for example, using a banking payment).

The user may wish to sign the data or a hash it is depending on the purposes. Some facts that require publicity can be inserted in the blockchain in its initial state and vice versa hashed or cyphered data provides for privacy.

A buzz question that recently appeared in the blockchain-oriented community is whether the smart contract is a contract? It is important to admit here that there is no general answer. As it comes from this research any concrete blockchain and any concrete case must be considered in the context of law and practice. This is the same as if someone were to ask if a napkin constitutes a contract or not. If one wrote a contract on the napkin (meaning that it has all elements of a contract), then yes, this is a contract.

The result of this study is Table 2, which allows you to analyze the applicability of the data insert for legal purposes.

Conclusion

In the result of this research we saw that the blockchain is useful for legal relations. The blockchain transaction is signed using asymmetric cryptography. That is why it inherits all properties of the modern cryptography and can be applied to sign legal documents and certify facts. This is also confirmed by the analysis of UNCITRAL Model Law on Electronic Signatures.

The real use of the blockchain comes from the nature of this technology. Towards the legal counter-parties (signatories) the blockchain plays the role of a re-

liable channel of the communication and a timestamp machine ensuring that the message will be public, immutable, irrevocable and accessible at any time.

The comparison of the blockchain in regard to the public key infrastructure shows that trusted third parties are required to play the role of certificate authorities; otherwise blockchain addresses are pseudonymous.

Users may wish to establish their own private channels of communication by peer exchange of their public keys (actually, blockchain addresses). They can also use open channels of communication, such as social accounts, where they share their public keys (blockchain addresses) upon the so-called scheme of «web of trust» or they can use conventional public key infrastructures with Certificate Authorities/Trust Service Providers.

The blockchain itself does not have any layer of «trusted services» and, therefore, cannot compete with such highly developed systems as European eIDAS. But it does not mean that the blockchain cannot be endowed with relevant layers of ID services, multi factor authentication, hardware signing devices and other properties. For that reason, the blockchain and blockchain-related technologies must be standardized.

The practical advantage over PKI is that the blockchain has one inherent feature out-of-box, which is timestamping. It does not require any centralized third party such as TSA, as in the traditional PKI scheme.

The blockchain which uses standardized asymmetric cryptography can be applied to legal relationships without obstacles. Otherwise, non-standard cryptography may require painful expertise to prove its reliability. Many known blockchain projects (Bitcoin, Ethereum, EOS, Emercoin, Litecoin and others) are based on standard cryptography.

Data insertion in the blockchain is a method of use of the blockchain beyond cryptocurrency. To make it happen, the user must publish a transaction, applying special scripts to add arbitrary data and «burn» coins.

Blockchain anchoring and blockchain hashing are subsets of the concept of data insertion. Instead of the initial data, the user publishes some metadata and(or) a hash value of this data. Anchoring and hashing are useful when privacy is required. Also, it reduces the bloat of the ledger.

Why might one wish to use the blockchain for legal purposes?

Reliable timestamping is useful for protecting copyrights. The author can publish in the blockchain the data (hash) before to share it with anyone. Any claims in the future can be resolved easier because of the timestamp which provides evidence of having this data earlier than anyone else.

The blockchain can make electronic contracts more interactive. For example, the Power of Attorney can be revoked or extended remotely by the principal at any moment by publishing updated information of the status of the document. For example, using Name-Value Storage or a relevant smart contract app.

Such publishing of legal documents can be useful for any sort of bearer documents. To make them more interactive, beyond revoking, the parties may wish to transfer NVS records or tokens. The bearer will show the electronic file of the warehouse receipt to certify their rights. The hash sum of the file will be published in NVS record or a token data. Therefore, it can be transferred to a new owner or filed for receipt of goods at the warehouse.

To sign a contract remotely, the first signatory can hash their legal document in the blockchain and send it to the counterparty. The counterparty will answer by publishing it again. Therefore, signatories, having each other's blockchain addresses known, will understand that they remotely came to the agreement.

This paper is an outcome of the PhD research performed inside of the Joint International Doctoral (Ph.D.) Degree in Law, Science and Technology, coordinated by the University of Bologna, CIRSFID in cooperation with University of Turin, Universitat Autonoma de Barcelona, Tilburg University, Mykolas Romeris University, The University of Luxembourg. Thanks to supervisors of Oleksii Konashevych Professor Marta Poblet Balcell, RMIT University (Melbourne, Australia) and Professor Pompeu Casanovas Romeu, La Trobe University (Melbourne, Australia). Special thanks to Oleg Khovayko, who is a developer of Name Value Storage in Emercoin for the consultation during this research.

REFERENCES

1. Nakamoto, S. «Bitcoin: A Peer-to-Peer Electronic Cash System», available at: ttps://bitcoin.org/bitcoin.pdf (accessed August 28, 2019).
2. Sward, A., Vecna, I. and Stonedahl, F. (2018), «Data Insertion in Bitcoin's Blockchain. Ledger. 3», pp. 1-23.
3. Gipp, B., Meuschke, N. and Gernandt, A. (2015), «Decentralized Trusted Timestamping using the Crypto Currency Bitcoin», the Proceeding of iConference 2015, iSchools, 2015.
4. Ober, M., Katzenbeisser, S. and Hamacher, K. (2013), «Structure and Anonymity of the Bitcoin Transaction Graph», Futur. Internet, Vol. 5, pp. 237-250.
5. Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T. and Capkun, S. (2013), Evaluating user privacy in Bitcoin, In: Lecture Notes in Computer Science, p.596.
6. «Bitcoin address · Programming The Blockchain in C#», available at: https://programmingblockchain.gitbook.io/programmingblockchain/bitcoin_transfer/bitcoin_address (accessed August 28, 2019).
7. «Bitcoin blockchain size 2010-2019 | Statistic», available at: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/ (accessed August 28, 2019).
8. «Ethereum Chain Data Size Growth», available at: https://etherscan.io/chart2/chaindatasizefast (accessed August 28, 2019).
9. «OP_RETURN», available at: https://en.bitcoin.it/wiki/OP_RETURN (accessed August 28, 2019).

10. «Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS)», Glossary of Terms, Abbreviations, and Acronyms, available at: https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf?agreement=true&time=1548119951687 (accessed August 28, 2019).
11. Schneier, B. (1996), Applied cryptography: Protocols, algorithm, and source code in C. John, Wiley & Sons.
12. «Announcing the first SHA1 collision», available at: https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html (accessed August 28, 2019).
13. Menezes, A.J. (1997), Handbook of applied cryptography, CRC Press.
14. Trcek, D. (2006), Managing information systems security and privacy.
15. (2011), Electronic Signatures and Infrastructures (ESI), Time stamping profile (ETSI TS 101 861).
16. (2008), Electronic Signatures and Infrastructures (ESI), Policy requirements for time-stamping authorities ETSI TS 102 023 , ETSI-TS102.
17. Barker, E.B. (2006), Recommendation for Obtaining Assurances for Digital Signature Applications, NIST.
18. «Trust Services and eID» (eIDAS), available at: https://ec.europa.eu/digital-single- market/en/policies/trust-services-and-eidentification (accessed August 28, 2019).
19. «KSI Blockchain», available at: https://e-estonia.com/component/keyless-signature-infrastructure/ (accessed August 28, 2019).
20. Anderson, R., Bond, M., Clulow, J. and Skorobogatov, S. (2005), Cryptographic processors-a survey Cryptographic processors-a survey, Technical Report Number 641.
21. (2016), «ENISA: Security Guidelines on the Appropriate Use of Qualified Electronic Signatures. Guidance for Users», European Union Agency for Network Information Security.
22. (2001), UNCITRAL Model Law on Electronic Signatures with Guide to Enactment.
23. Szabo, N. (1997), «Formalizing and Securing Relationships on Public Networks», First Monday, Vol. 2.
24. «Emercoin NVS», available at: https://wiki.emercoin.com/en/Emercoin_NVS (accessed August 28, 2019).
25. Turvey, B.E. (2008), Criminal Profiling: an Introduction to Behavioral Evidence Analysis, Elsevier Science.

Received 07.08.19

А.И. Конашевич

ВСТАВКА ДАННЫХ В БЛОКЧЕЙН ДЛЯ ЮРИДИЧЕСКИХ ЦЕЛЕЙ.
КАК ПОДПИСАТЬ КОНТРАКТ С ПОМОЩЬЮ БЛОКЧЕЙНА

Исследована технология блокчейн, в частности, вставка данных (привязка, хеширование) в блокчейн как способ подписи документов и придания юридических свойств фактам. Проведен сравнительный анализ известных способов применения электронной цифровой подписи с методом вставки данных в блокчейн. Рассмотрены следующие вопросы. Что такое вставка данных в блокчейн и какие свойства они получают? В чем разница между вставкой, привязкой и хешированием в блокчейне? В чем разница между хешированием в блокчейне и цифровой подписью на документе? Будет ли документ юридически обязательным, если он будет закреплен в блокчейне? Какие условия надо выполнить, чтобы придать законную силу документу? Как можно использовать привязку для подписания контрактов, сертификации доказательств, имеющих юридическую ценность, обозначения временных отметок, подтверждения авторства и авторских прав, а также их

передачи, выдачи и передачи доверенностей и делегирования других прав, выдачи и передачи инструментов на предъявителя?

К л ю ч е в ы е с л о в а: блокчейн, OP_DROP, OR_RETURN, электронная подпись, eIDAS, PKI, доказательство существования.

О.І. Конашевич

ВСТАВКА ДАНИХ У БЛОКЧЕЙН ДЛЯ ЮРИДИЧНИХ ЦІЛЕЙ.
ЯК ПІДПИСАТИ КОНТРАКТ ЗА ДОПОМОГОЮ БЛОКЧЕЙНА

Досліджено технологію блокчейн, зокрема вставку даних (прив'язку, хешування) в блокчейн як спосіб підпису документів і надання юридичних властивостей фактам. Проведено порівняльний аналіз відомих способів застосування електронного цифрового підпису із методом вставки даних у блокчейн. Розглянуто такі питання. Що таке вставка даних в блокчейн і які властивості вони отримують? У чому різниця між вставкою, прив'язкою і хешем у блокчейні? У чому різниця між хешуванням у блокчейні і цифровим підписом на документі? Чи буде документ юридично обов'язковим, якщо він буде закріплений у блокчейні? Які умови треба виконати, щоб надати законну силу документу? Як можна використовувати прив'язку для підписання контрактів, сертифікації доказів, що мають юридичну цінність, позначення тимчасових відміток, підтвердження авторства та авторських прав, а також їх передачі, видачі та передачі доручень і делегування інших прав, видачі та передачі інструментів на пред'явника?

К л ю ч о в і с л о в а: блокчейн, OP_DROP, OR_RETURN, електронний підпис, eIDAS, PKI, доказ існування.

KONASHEVYCH Oleksii Ihorovych, Erasmus Mundus Joint International Doctoral Fellow in Law, Science and Technology, European Union. Graduated from National Aviation University in 2005. Field of research — use of blockchain for electronic governance and electronic democracy.

PAPER 5

ICEGOV2019: Proceedings of the 12th International Conference on Theory and Practice of Electronic GovernanceApril 2019 Pages 317–323 https://doi.org/10.1145/3326365.3326406

Blockchain Anchoring of Public Registries: Options and Challenges

Oleksii Konashevych
Erasmus Mundus Joint International Doctoral Fellow in Law, Science, and Technology
LAST-JD.eu
European Union
a.konashevich@gmail.com

Marta Poblet
RMIT University,
Graduate School of Business and Law
124 La Trobe Street, Melbourne VIC 3000
Australia
marta.pobletbalcell@rmit.edu.au

ABSTRACT

Governments across the world are testing different uses of the blockchain for the delivery of their public services. Blockchain hashing—or the insertion of data in the blockchain (anchoring)—is one of the potential applications of the blockchain in this space. With this method, users can apply special scripts to add their data to blockchain transactions, ensuring both immutability and publicity. Blockchain hashing also secures the integrity of the original data stored on central governmental databases. The objective of this paper is to analyse the use of data hashing (anchoring) on the blockchain for public state-owned registries. This paper starts by analysing possible scenarios of hashing on the blockchain and assesses in which cases it may work and in which it is less likely to add value to a public administration. Second, the paper also compares this method with traditional digital signatures using PKI (Public Key Infrastructure) and discusses standardisation in each domain. Third, it also addresses issues related with concepts such as "distributed ledger technology" and "permissioned blockchains." Finally, it raises the question of whether blockchain hashing is an effective solution for electronic governance, and concludes that its value is controversial, even if it is improved by PKI and other security measures. In this regard, we claim that governments need to identify pain points in governance in the first place, and then consider the trade-offs of the blockchain as a potential solution versus other alternatives.

CCS CONCEPTS

• **Applied computing** → **Computers in other domains** → Computing in government → *E-government*

KEYWORDS

Blockchain, hashing, e-governance, digital signatures, PKI

ACM Reference format:

O. Konashevych, M. Poblet. 2019. Blockchain Anchoring of Public Registries: Options and Challenges. In *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance (ICEGOV2019), Melbourne, VIC, Australia, April 3-5, 2019*, 7 pages. https://doi.org/10.1145/3326365.3326406

1. INTRODUCTION

In recent years, governments across the world have started to test the use of the blockchain in different areas of their public sector. Estonia was among the first countries expressing interest in blockchain technology and launching several initiatives in that direction. First, by embedding blockchain technology within the data transfer platform X-Road. Second, by testing a "notarisation on the blockchain" in a project with BitNation [11]. Third, by piloting keyless authentication [6] supported by distributed ledger technology [16]. Yet, the outcomes of these different initiatives are still elusive: the integration of the blockchain within X-Road has not been achieved [28]; the lack of regulatory background has deprived "blockchain notarised" acts of any legal force [11]2; details of the pilot on keyless authentication have not yet been released. Some other countries have launched pilots [15]: Honduras announced a blockchain-based real estate registry, but the project was eventually discontinued [15] [7]; Chromaway—a Swedish start-up—announced in 2016 promising plans to upgrade the Swedish real estate registry by conducting deeds on the blockchain [4]. Yet, two years later the third phase of the pilot has been concluded but no results are yet available [22]. In the USA,

ICEGOV2019, April 3–5, 2019, Melbourne, VIC, Australia

ACM 978-1-4503-6644-1/19/04…$15.00
https://doi.org/10.1145/3326365.3326406

2 The link to the joint project of the Estonian government and Bitnation was active during 2016-2017 and it eventually became unavailable. The "notarisation" on the blockchain service contained the disclaimer that such legal acts had no legal force as a notary act and users had still to apply to the public notary.

the project Velox.re in Cook County (Chicago) tested a transaction outside of the real registry to imitate the use of the blockchain for deeds with real estate [5]. The clerk's office of the county issued a report [17] but the project never went beyond the testing phase. Ubitquity.io announced the project Bitland to implement a blockchain-based real estate registry in Ghana with no further continuity either [18], [3].

Other pilots are currently work in progress. Ukraine and the Republic of Georgia announced their cooperation with Bitfury [26] to apply distributed ledger technology and blockchain to their cadastral registries.

Different organisations in the EU and UK have recently released reports on the use of the blockchain [5] [10] [27]. These reports generally express positive views about the impact of the technology and its value in the development of the informational society. Yet, they are much less specific about the design of blockchain-based e-government systems and how to implement blockchains in particular areas.

Blockchains and other distributed ledger technologies (DLTs) can be applied to a vast range of domains, but no technology comes as a panacea. In this paper we signal some caveats about the use of the blockchain for public—state-owned—registries. Our objective is to assess the potential use of data hashing (anchoring) on the blockchain for public state-owned registries. To do so, we compare blockchain hashing—the process of securely storing hash sums (checksums) of data—with the existing infrastructure of digital signatures using standardised PKIs (Public Key Infrastructures) such as eIDAS in the European Union [24]. We contend that the present lack of regulatory frameworks and standards makes the adoption of blockchain hashing contentious, as in some cases it could undermine e-government services and public interest in general. We conclude that governments should identify and address pain points in the administrative processes before making decisions that involve blockchain adoption.

2. HOW DOES HASHING ON THE BLOCKCHAIN WORK?

A cryptographic hash function is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash) and is designed to be a one-way function, that is, a function which is infeasible to invert. The function takes an input (or 'message') and returns a fixed-size alphanumeric string. The string is called the "hash sum", "hash value", "message digest", "digital fingerprint", "digest" or "checksum". The ideal hash function has three main properties: (i) it is easy to calculate a hash for any given data; (ii) it is extremely difficult (computationally) to calculate an alphanumeric text that has a given hash; (iii) it is extremely unlikely that two slightly different messages will have the same hash [20].

In addition, if the same hash function is applied to the same data, it always gives any user acting independently the same hash sum as the result at any time. In terms of public registries, if the hash sum of an entry is securely stored, then it allows to reveal any further changes in the original entry. Thus, it is useful in exposing forgery, although it does not protect the data itself.

Data insertion is one of the first useful applications of the blockchain beyond the hype of cryptocurrencies. Broadly, hashing on the blockchain refers to inserting a hash sum in a blockchain transaction. Insertion implies that data is "published in the ledger and cannot be censored or retracted and will be permanently available to the world" [21]. Sward, Vecna, and Stonedahl offer a comprehensive analysis of different methods of data insertion in Bitcoin [21]. Fig. 1 below shows the principal data insertion scheme in the blockchain.

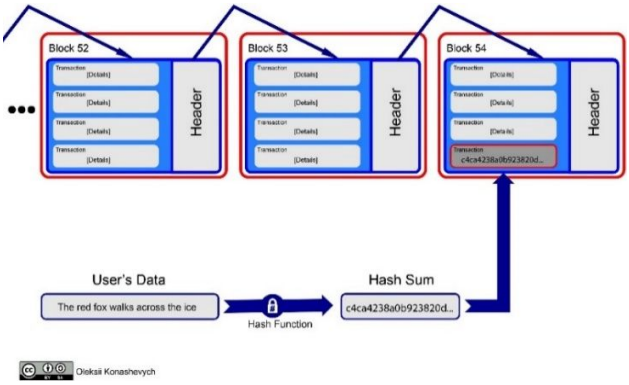


Figure 1: Blockchain data insertion

The method of hashing is recognised as a way of securing public data on the blockchain. Each entry of the central database of the public registry is hashed and casted to the blockchain. Some governments, as the example below shows, are considering this method to secure their cadastral data.

2.1. Hashing Cadastral Data in Ukraine

An example of blockchain hashing is the project by Bitfury in Ukraine, developed in partnership with Transparency International (TI) and the Ukrainian government. The project, launched in 2017, applies Bitfury's distributed ledger technology "Exonum" [13] for hashing records of the geocadastral registry [26].

Authorised nodes that are controlled by the government cast hashes to the Exonum-based ledger. The hash of the current state of the ledger is periodically anchored on the public blockchain. Initially, this public blockchain was Bitcoin, but it was later moved to Emercoin [8]. TI keeps another node, which plays the role of the observer and has permission to read the ledger only. The scheme is explained in Fig. 2 below:

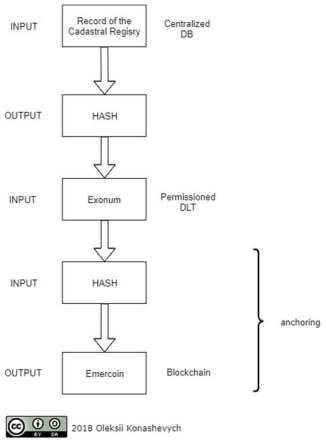


Figure 2: Hashing on DLT Exonum

Exonum is just an example of a private permissioned distributed ledger technology. Nodes in Exonum must be authorised to access the network and create blocks. The administrator keeps the private key and grants permissions to nodes. Exonum uses a Byzantine Fault Tolerant consensus algorithm—resistant to malicious behavior or failure of one or several nodes—that requires the approval of 2/3 of authorised nodes to accept new blocks. If the nodes reach such consensus, the new block is added to the chain. Technical details are described on the site of the project [13], [8] and [12].

3. DIGITAL SIGNATURES

The idea of an asymmetric public-private key cryptosystem is attributed to Whitfield Diffie and Martin Hellman, who published this concept in 1976 [9]. This idea was developed and laid down in the patent by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977 [19] and has been further improved by other cryptographers over the last decades.

In public key cryptography—also known as asymmetric cryptography—digital signatures consist of a pair of keys: public and private. The public key is a code string that uniquely identifies a certain individual or company. The private key must be kept absolutely secure and not shared, whereas the public key can be shared with anyone [1].

To illustrate this, let us present two scenarios involving Alice and Bob—the two most famous characters in the cryptographic world. In the first scenario, Bob wants to send Alice a message, and Alice needs to be sure that the message came from Bob. So, Bob uses his private key to encrypt the message. Alice can then validate that the message came from Bob by decrypting it using Bob's public key. In the second scenario, Alice wants to send Bob a message that only he can read, so she encrypts it with Bob's public key. Then the only person who can decrypt it is Bob, using his very well-protected private key [1].

3.1. Digital signature vs hashing on the blockchain

The signing of a blockchain transaction is based on asymmetric cryptography as well [2]. In that respect, cryptographic signing of data is not different from signing blockchain transactions.

The main difference between the two methods is that hashing on the blockchain adds another layer of data. With digital signatures, users insert their data as an input to the cryptographic function; with hashing on the blockchain, users insert payment data along with the required data, as it is schematically shown in Fig. 3.

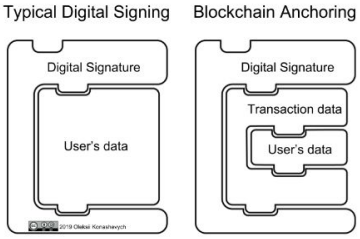


Figure 3. Typical digital signing vs DLT based digital signing

Digital signatures have not been used for public purposes in this basic form. For this to happen, the system needs to be supported by a Public Key Infrastructure (PKI) and a set of standards. PKI consists of technologies, procedures and actors that enable deployment of public-key cryptography-based security services [25]. Within PKI, one provider—known as Certificate Authority (CA) or Trust Service Provider (TSP)—is responsible for the provision of identity services, while other providers—Timestamp Authorities (TSA)—authenticate time and date information. Blockchain hashing, in contrast, does not require a centralised TSA since all blocks are chronologically stored. Timestamps are embedded in the blocks, and it is not possible to alter them due to the inherent immutability of the blockchain.

At present, PKI benefits from a complete infrastructure with regulations, standards, and procedures. For example, a roadmap of standards in the EU is described in the ETSI publication TR 119 000 [30]. The paper contains the list of all standards relating to trust services and signatures and grouped together by a numbering scheme, as shown in Fig. 4.

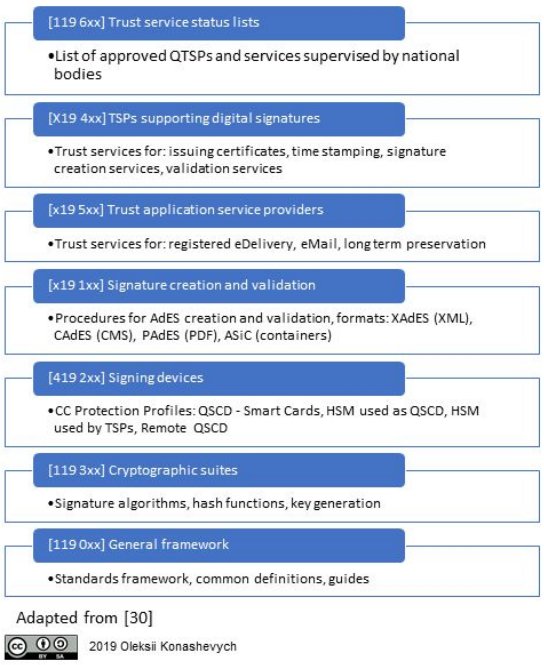


Figure 4: Framework of eIDAS trust service related standards

Each clerk imposing a signature can be identified because they use qualified electronic signatures with certificated hardware devices for digital signing (or signatures with the similar level of security and identification). This is the case in the European Union, Switzerland, Ukraine, and many other counties.

As compared with typical PKI, there is no standardised protocol establishing the procedures of authentication to the permissioned blockchains. There are no procedures for authorising nodes and operators (clerks) either. Clerks use private keys, but there is no standardised protocol if these keys are compromised. More generally, there is no standard for a permissioned distributed ledger technology (DLT).

As it obvious from this analysis, blockchain/DLTs can be augmented either by typical PKI standards or PKI-similar to achieve required identification, authentication and authorization procedures.

DLT and the blockchain, in summary, are not fully equipped yet. The only feature "out of the box" is a timestamp. Timestamps are an integral property of the blockchain, because transactions are chronologically saved in an strong chain of blocks of records and secured by cryptography [2] [29]. Thus, any transaction has its immutable place in this chronology.

While other infrastructural solutions are not in place by default, hashing on the blockchain without regulations, standards, procedures, and certifications can only work in limited environments, under supervision and, presumably, for research purposes. This is definitely not a scalable approach for e-government at this moment in time.

3.2. How hashing on the blockchain should work?

There are at least three issues that must be addressed to leverage hashing for improving the security of centralised public registries, for example, of properties, real estate, finances, etc. These are (i) identification, authentication and authorization; (ii) bi-directional relations of entries in the database and hashes on the blockchain; and (iii) standardisation.

3.2.1. Identification, authentication and authorization

The blockchain was designed in a way to provide for pseudonymity 3 of both nodes owners ("miners") and owners of blockchain addresses ("users"). Therefore, authentication requires here only a user's private key.

For public use to add trust to blockchain records, the original blockchain or other DLTs must be supplemented with overlaid solutions for identification, authorisation and authentication with the component of trust services where necessary.

DLT means that the administrator of the system is on top of the system hierarchy. The administrator keeps the key to the system and grants permissions. Therefore, standards and procedures for managing keys and accesses must be applied here as a part of a standard protocol.

In the case of hashing on the original blockchain a public ledger is used instead. This raises two issues: free access by anyone and anonymity of addresses. Therefore, when any data is published, no one knows who did that: an authorised officer or an attacker. Thus, before that happens, the address must be either identified or the inserted data must contain an identifiable digital signature. Moreover, if the private key to the blockchain address is stolen or compromised in another way, there is a need to have a procedure for a stop list where such an address is added to the special database and any further action from the address is considered invalid. So, as we see again, this takes us back to the need for the PKI based on known and proven principles.

3.2.2. Bi-directional relations between databases

The probable attack scenario we are facing here is that the record on the central database is changed or replaced with a new one, and if there is no reverse relation with the hash stored on the ledger, a new hash can be created for the corrupted record and published in the distributed ledger, and so presented as a correct one. Apparently, such use of the blockchain does not add any value in terms of the security.

The problem is that hashing does not protect the data itself from being deleted and changed, it just helps to reveal the forgery if the user still keeps in their hands the original record. If the database is closed and centrally controlled (that's how it basically works in the public administration), such manipulation inside the database is still possible.

3 Originally in Section "Privacy" [2] Nakamoto uses word "anonymous". However, as anonymity can hardly be achieved due to various specific reasons, the term "pseudonymous" is preferable.

The issue is illustrated in the Fig. 5. Here the observer did not have access to the original record and the hash which is published on the blockchain has no pointer itself to the original record. Whoever sees the hash sum on the ledger, even if it matches the record in the central DB, still cannot know if the record itself is authorised or not.

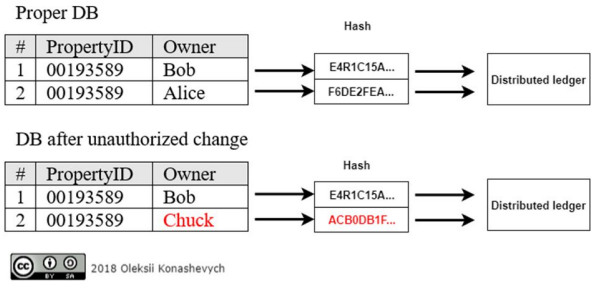


Figure: 5. The issue of unauthorised change of DB

Traditionally, in government registries changes are addressed by a multilayered system of security measures, logs, and management of access.

One of the possible ways to use the blockchain is to build a central registry in the style of "chain of blocks" (chain of records, actually) similar to the blockchain, either public or private, or just to move the registry on the blockchain. Thus, the complex use of the blockchain for public administration implies both the transfer of the central database to the blockchain (and not just hashing) and the use of PKI for identification.

As an example, this could be implemented using the Name Value Storage (NVS) technology. NVS is a complex technology for managing data. First developed by Namecoin and then significantly improved by Emercoin, NVS works as a build-in protocol in the blockchain. NVS records are designed to store arbitrary data of users in the blockchain, but this is not just data insertion. The user publishes the data in a form of pairs [name -> value], where "name" is a key (unique searchable index field) and "value" is data that specifies the key or simply, any data that the user wants to add. After publishing the NVS record, the use can update it using their private key to the blockchain address.

As a result of such an update, a new record is created where "name" remains the same, but "value" is changed. Because this is made on the blockchain, the whole chronology, i.e. "chain of records," is stored on the blockchain. Nobody else can create the record with the same "name." Therefore, NVS ensures an unbreakable chain of records where the next record is connected to the previous NVS record with the same name. Fig. 6 shows the basic NVS scheme, where "Name" remains the same interconnected through the blocks and can play the role of any pointer (for example, a cadastral number) and "Value" is updated when necessary (Bob to Alice).

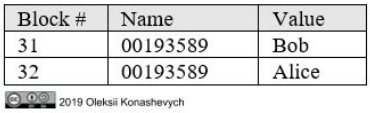


Figure: 6. NVS in Emercoin/Namecoin

Of course, both PKI and some additional measures of security are still required in the architecture of such registry. This is just one example, but the emerging variety of blockchains and overlaid technologies gives a wide scope for solutions.

3.2.3. "Permissioned blockchain," standardisation and state policy

The recent hype about the blockchain may lead to some confusion when it comes to adoption by governments. The alleged achievements in blockchainisation of e-government services tend to refer to "permissioned blockchains". However, these "permissioned blockchains" may lack some of the key features of the blockchain. To illustrate this point, we need to distinguish between the blockchain and other distributed ledger technologies (DLTs).

The blockchain, famously introduced as "Bitcoin" by Satoshi Nakamoto in 2008 [2], is a decentralised peer-to-peer system underpinned by cryptographic functions. All nodes in the blockchain network are hierarchically equal and have the same rights in creating (mining) blocks of data with transaction records (ledger).

DLTs are often used as a general term referring to a subset of technologies that use some elements of the blockchain. As opposed to the original blockchain, DLTs can be architecturally centralised with a hierarchical system of nodes. This is the case of the so called "permissioned blockchains." In our view, nevertheless, the use of the notion "blockchain" or "permissioned blockchain" to refer to a centralised system can be misleading. Arguably, what system can qualify as a blockchain is still under discussion: What are the main properties that give us the right to call any specific network the blockchain? Original Bitcoin-like networks only? Decentralised systems based on other types of consensus mechanisms? A mix of them? Ultimately, governments need to rely on shared conceptual frameworks and standards to make the appropriate technology choices. Otherwise, we may end up with scenarios where different departments use different types of conflicting blockchains, or use blockchain protocols with only a few nodes (that are unable to maintain the required level of security of the network), or use DLTs that are not blockchains at all.

Another risk associated with the lack of standardisation is that governments must keep the list of public blockchains whose technologies are proven trustworthy. Yet, such lists of "trusted" blockchains can lead to discrimination, arbitrarily excluding potentially appropriate networks and technologies. Standardisation is a better way to ensure fair competition and stable development.

Public policy and clear roadmap are the most preferable scenario, otherwise, we are at risk to see voluntarism and mistakes which are unacceptable for public data.

Finally, the consistent state policy regarding the use of the blockchain must contain the recognition and legitimisation of cryptocurrency. Cryptocurrency is the blood of the system, the main mechanism and incentive that allows the creation of a large sustainable network. Nodes can claim some amount of crypto when creating blocks. Likewise, nodes can also receive cryptocurrency as a fee from the user when performing transactions. The alternative to cryptocurrency is that the government must create an infrastructure that, ultimately, it is a way to centralisation.

4. Conclusion

Since 2017, ISO is considering the first blockchain standard [14]. However, standardisation of the blockchain domain is still in the early stages. For this reason, we consider that hashing on the blockchain may be premature for public registries. Rather, the alternative option of PKI supported with standards, regulation and complex measures of security seems more plausible solution at the present stage.

In summary, the discussion is still open. Why, and what for, should we use the blockchain in e-government? To improve security? As we have outlined, the security of traditional centralised databases has worked reasonably well so far.

Arguably, governments will need to rethink the nature of relations around public databases and look in the direction of decentralised applications (DApps). Technically, a registry is a database. In developed countries registries are usually digitised or, at least, have both actual realisations, i.e. exist in paper and in electronic form. However, in the spatial sense, registries reflect large domains of specific regulated relations.

For example, a land registry is framed by laws and regulations of property rights and procedural acts. The infrastructure includes bodies of acknowledgement of deeds (notaries public, attorneys, title agents, etc.), recording offices and clerks and mediators, which are professionals in the market (brokers, escrows, insurance companies, etc.). Markets of professionals are usually regulated by statutory laws, licensing, and include the system of regulatory and control bodies, professional unions and associations.

Each land deed triggers some certain mechanism of this large infrastructure. Each element of this infrastructure has its own purpose to add some sustainability in the domain, i.e. most regulations and institutions exist to prevent misunderstandings in legal issues, or prevent fraud and corruption.

Such state-level "paper" registry or centralised electronic system is based on understanding that the centralised form of governing is the only way to organise large relations in the scale of a country.

The use of DApps is not about “securing data.” Rather, it is about changes in public administration, in governance, and in regulations. There many examples where the clerk is no longer needed. Why does the government need clerks for registering a business? Businessmen could file the company automatically by online submission of an entry controlled and guided by the “smart” system where fields of the online application form would be algorithmically verified, and errors excluded. Such systems could work even better and exclude human errors, which typically occur on both sides of the process: citizens and governments.

We can even think in terms of the necessity of a traditional registration of the business and securities. The registration is aimed to record the fact, but the blockchain is the register itself. So why would we need to record twice the issue of shares in the Securities and Exchange Commission and ICO on the blockchain? All these questions remain open for further research.

If we think in the direction of the second generation of the blockchain technologies, smart contracts [23] and DApps, we can leverage much more useful functionalities than data insertion (blockchain hashing) which is primitive and does not unleash the full potential of the blockchain. Thinking in the direction of automation of manual work of clerks using “smart” algorithms we can define the following goals:

- reducing fraud and corruption;
- raise in the level of data security;
- reducing costs for public administration (work of people costs more than work of machines);
- reducing human-generated mistakes;
- reducing bureaucracy and so incentivisation of economic activity.

ACKNOWLEDGMENTS

This paper is an outcome of the PhD research performed inside of the Joint International Doctoral (Ph.D.) Degree in Law, Science and Technology, coordinated by the University of Bologna, CIRSFID in cooperation with University of Turin, Universitat Autònoma de Barcelona, Tilburg University, Mykolas Romeris University, The University of Luxembourg.

REFERENCES

[1] Allin, J. et al. 2017. The eIDAS Regulation. John Wiley & Sons, Ltd.
[2] Bitcoin: A Peer-to-Peer Electronic Cash System: 2008. https://bitcoin.org/bitcoin.pdf. Accessed: 2016-12-27.
[3] Bitland. Land Title Protection Ghana: http://www.bitland.world/about/. Accessed: 2018-01-05.
[4] Blockchain and Future House Purchases: https://chromaway.com/landregistry/. Accessed: 2017-07-09.
[5] Boucher, P. (Scientific F.U.E.P. 2017. How Blockchain Technology Could Change Our Lives.
[6] Buldas, A. et al. 2013. Keyless Signatures’ Infrastructure: How to Build Global Distributed Hash-Trees. (2013), 1–9.
[7] Chavas, J. and Cox, T.L. 2018. BLOCKCHAIN AND PROPERTY IN 2018: AT THE END OF THE BEGINNING. (Washington DC, 2018), 1–58.
[8] Consensus Algorithm Speci cation: https://exonum.com/doc/advanced/consensus/specification/. Accessed: 2018-01-08.
[9] Diffie, W. et al. 1976. New Directions in Cryptography. IEEE Transactions on Information Theory. 22, 6 (1976), 644–654. DOI:https://doi.org/10.1109/TIT.1976.1055638.
[10] ENISA 2016. Security Guidelines on the Appropriate Use of Qualified Electronic Signatures. Guidance for Users. European Union Agency for Network Information Security.
[11] Estonian Government and Bitnation Begin Cooperation - e-Estonia: https://goo.gl/88pBui. Accessed: 2016-04-29.
[12] Exonum: Networking Specification: https://exonum.com/doc/advanced/network/. Accessed: 2018-01-19.
[13] Exonum — A framework for blockchain solutions: https://exonum.com/. Accessed: 2018-09-07.
[14] ISO/TC 307 - Blockchain and distributed ledger technologies: 2017. https://www.iso.org/committee/6266604.html. Accessed: 2017-11-10.

[15] Jun, M. 2018. Blockchain government-a next form of infrastructure for the twenty-first century. Journal of Open Innovation: Technology, Market, and Complexity. 4, (2018), 7. DOI:https://doi.org/10.1186/s40852-018-0086-3.
[16] KSI ® blockchain in Estonia: https://e-estonia.com/wp-content/uploads/faq-ksi-blockchain-1.pdf. Accessed: 2018-09-19.
[17] Mirkovic, J. 2017. Blockchain Pilot Program. Final Report.
[18] Real Estate Land Title Registration in Ghana Bitland: http://bitlandglobal.com/. Accessed: 2017-07-09.
[19] Ronald L. Rivest et al. 1977. CRYPTOGRAPHIC COMMUNICATIONS SYSTEM AND METHOD. 4,405,829. 1977.
[20] Schneier, B. 1995. Applied cryptography: Protocols, algorithm, and source code in C.
[21] Sward, A. et al. 2018. Data Insertion in Bitcoin's Blockchain. Ledger. 3, 0 (Apr. 2018), 1–23. DOI:https://doi.org/10.5195/LEDGER.2018.101.
[22] Sweden's Land Registry Demos Live Transaction on a Blockchain: 2018. https://www.coindesk.com/sweden-demos-live-land-registry-transaction-on-a-blockchain/. Accessed: 2018-09-19.
[23] Szabo, N. 1997. Formalizing and Securing Relationships on Public Networks. First Monday. 2, 9 (1997). DOI:https://doi.org/10.5210/fm.v2i9.548.
[24] Thomas Fillis 2016. Electronic Registered Delivery Service (ERDS) and the eIDAS Regulation. European Commission.
[25] Trček, D. 2006. Managing information systems security and privacy.
[26] Ukraine launches big blockchain deal with tech firm Bitfury: 2017. http://www.reuters.com/article/us-ukraine-bitfury-blockchain-idUSKBN17F0N2.
[27] Walport, M. 2015. Distributed ledger technology: Beyond block chain. A report by the UK Government Chief Scientific Adviser.
[28] X-Road not to be confused with blockchain: 2018. https://e-estonia.com/why-x-road-is-not-blockchain/. Accessed: 2018-09-19.
[29] Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS). Glossary of Terms, Abbreviations, and Acronyms. Payment Card Industry. Security Standards Council, LLC.
[30] 2015. Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview.

THESIS CONCLUSIONS

Tokenization of Real Estate on Blockchain

Oleksii Konashevych
Erasmus Mundus Joint International Doctoral Fellow in Law, Science and Technology

Supervisors:
Associate Professor Marta Poblet, RMIT University
Research Professor Pompeu Casanovas, Autonomous University of Barcelona and La Trobe University

2020

Contents

1. Brief 3
2. Concept outline 3
3. Cross-blockchain protocol basics 4
4. High-level findings 7
4.1. Technological neutrality and the right to choose 7
4.2. The advantages of the system architecture 8
4.3. Blockchain instead of land registry 8
4.4. No application at blockchain consensus 9
4.5. Is a trusted third person required? 10
4.6. How not to allow a digital dictatorship? 11
5. References 13

1. Brief

"You never change things by fighting the existing reality.
To change something, build a new model that
makes the existing model obsolete."
— R. Buckminster Fuller

The thesis consists of five published academic papers that present a concept of tokenization of real estate on blockchain land registry.

As per the concept. tokens represent title rights that users manage through smart contracts performing peer-to-peer transactions on blockchain.

The key output of this research is an architecture of the system presented as a cross-blockchain protocol designed to support free choice and transferability of assets across blockchains. Another important feature of the protocol is enforceability to address the constraint of the blockchain technology, i.e., the intolerance to retroactive transactions. To resolve disputes and other legal issues, the protocol provides a framework for smart laws and digital authorities, which are further discussed.

There are following major statements supported by the thesis:

- Blockchain, as a decentralized public shared ledger technology might be used for a variety of property relationships, including land title rights.
- There are six major constraints in the technology which are to be addressed for digitalization of ownership: hardforks, immutability & enforcement, privacy, digital identity, scalability and price volatility.
- The proposed system architecture based on the cross-blockchain protocol is designed to address major constraints of the blockchain technology.
- Title token is proposed as a new model for digitized ownership on blockchain-driven by smart contracts. Its novelty in a combination of smart contracts and smart laws.
- To address the problem of enforcement and inheritance, a framework of smart laws and digital authorities is proposed.
- Trusted third parties might be eliminated in some cases, but it is an unenviable component of system sustainability. Blockchain increases transparency and accountability of third parties.
- There are privacy concerns on blockchain. Therefore, personal data must be managed off-chain. There are various protocols and frameworks that may support it: DID, SSI, etc.
- The cross-blockchain protocol supports competition of ledgers, where the user decides which ledger to apply.
- Tokenized property does not require other forms of registries, i.e., the centralized land registry.
- The traditional land registry may co-exist with blockchains giving every user a choice on where to manage their ownership, which aligns with concepts of technological pluralism and neutrality.
- The concept addresses basic aspects and requires further research and design specifically to any chosen jurisdiction. Technical standardization and elaboration of models of good governance are also crucial.
- Implementation of this concept requires regulative innovations for procedures of the registration and deed acknowledgment. Further development and piloting, i.e., from small to a larger scale is a viable, practical option that arises from this thesis.

2. Concept outline

The blockchain serves as a decentralized, immutable public repository of records for land titles and other property rights. It is not only a secure database but a system for managing ownership because this is an inherent feature of the technology. With distributed ledger technologies, users can directly manage their property performing peer-to-peer (P2P) transactions.

Tokens are blockchain-based records that represent title and other property rights. A token is a unit of account, and it relates to the user's address. The user's private key enables exclusive control over the address. The token is technologically connected with the cadastral data (geo-data) and records on property rights, including leases, mortgages, superficies, and other encumbrances and liens. The connection of title

records with real estate and property rights is ensured by relevant blockchain records done by trusted third parties who have the authority to certify ownership, deeds, and other transactions with property rights, for example, land authorities, notaries, etc.

Smart contracts are the driving mechanism for managing ownership. Smart contracts are an integral part of blockchain transactions. The blockchain transaction can be considered as the equivalent of the legal deed. The token record is always a result of a blockchain transaction: starting when the user creates the token to its various transfers (title deeds, smart contracts with property rights, etc.) and eventually deactivating the token in case if it ceases to represent any value.

Tokens can be distinguished from cryptocurrency. The latter does not represent any particular property, and it is a value itself, as it is a drive gear for transactions because users pay cryptocurrency as fees for transactions. More generally, cryptocurrency is a motivation for miners who create and maintain a blockchain network infrastructure and ensure the security of the system.

Tokens, in accordance with this concept, are titles in a digital form. Though title tokens themselves create a basis for various derivative tokens, that is various other tokens, which are not titles but are connected with them and create different property relationships between parties, including new forms of economic activities, i.e., ICOs, IEO, etc.

3. Cross-blockchain protocol basics

To address legal problems of the immutability of records (intolerance to retroactivity) on a distributed ledger (Distributed Ledger Technologies, or DLT), a specific technology - Cross-Blockchain Protocol - is applied. The protocol accommodates the framework for smart laws and digital authorities. Smart laws are designed to address issues of inheritance, dispute resolution, reinstate title tokens when private keys are lost, and other possible enforcement issues.

The core of the system is the key-value storage indexed through the bundle of blockchains. The uniqueness of keys (tokens) in the database is ordered chronologically. A record (token) that is published first among blockchains is added to the database. Subsequent entries with the same keys are not passed. It is important to create a consistent non-conflicting database upon the blockchain which stores record on property rights. For instance, a cadastral number of a land plot is a unique identifier. Once it has been created in the database, the blockchain and the proposed protocol will not let creating unauthorized copies of it (double spending).

The protocol supports adding new blockchains in the buddle and detaching a blockchain in case of an attack or decrease of reliability. Reliability and attacks are self-diagnosed by nodes independently based on heuristic analysis of hash rate, difficulty and abnormal orphan length. When a node detects a threat using the proposed protocol for heuristic analysis (Paper 2), indexing of this blockchain is stopped, and users may transfer the record (token) to the rest in the bundle. The transferability of records among blockchains in the bundle works as a regular feature, which supports competition between technologies, ensuring a free choice of a repository for end users. This principle is known as blockchain agnostic; it is relevant to a high-level concept of technological neutrality.

Key-value records (tokens) are the raw material for building applications. They are assigned to addresses and controlled by users through the native mechanism of private keys. Users may change records inserting in the blockchain updated information and transferring records to other addresses, i.e., in this way, changing ownership. The advantage of the protocol is that normally it does not require changing existing blockchains; it is set up as an overlaid technology.

The inserted data in blockchains is recognized and hooked from blocks if it corresponds with the standard format of the protocol. The protocol can be used by governments to maintain public registries, for example, property (cadastre) databases but not only. Users can own records that represent property rights (titles), providing references to trusted third parties that certified these rights. In the same way can be improved the traditional Public Key Infrastructure, where Certificate Authorities (Trust Service Providers) issue certificates to digital identities (public keys). The protocol can also accommodate stricter rules of IDs and electronic signatures, such as per eIDAS regulation in the EU, providing users options to manage their private keys on secure devices (hardware crypto devices) and 2F/MF authentication protocols.

Such an ecosystem addresses issues of trust at the first level: each record has its trust provider that ensures its validity (see Fig. 1). Being "valid" as the property of a transaction is a specific term that means "legally binding due to having been executed in compliance with the law."[1] As per Poblet, Casanovas and Rodríguez-Doncel in their book "Linked Democracy" (2019), validity is a characteristic feature of such a continuum, a property pertaining and emerging from the whole regulatory system which is essentially dynamic and related to the interactive behavior of agents [1]. Usually, a "valid" norm is deemed to be a "legal norm." And, to acquire this quality of law, a rule or norm is expected to be (or become) valid [1].

With regard to the proposed protocol, a valid transaction consists of two elements: the off-chain act of the "validator" whose role is to verify the object (a property, for example), and the on-chain act which is the certification that the object is verified. The criteria of the validity are norms that applied for this particular transaction. The role of the validator may arise from a contract (parties mutually agreed) and from regulations. For example, the auditor of the property will be assigned by the landlord based on the contract. The authority of the land registrar arises from public law. The transaction may also include an evaluator, a surveyor, a notary, etc. The validators will do their job based on either public or private law. Even more, there are situations when both are applied. For example, the land survey may be mandatory for the transaction based on the statutory law, but a surveyor will be at the discretion of the landlord among available professionals on the market, and so parties are free to choose any (private law). The flexibility of the protocol allows for supporting all types of scenarios.

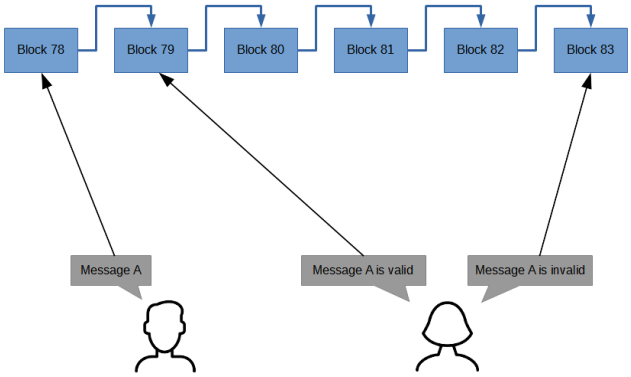


Fig 1. Scheme for maintaining validity of records (messages) in blockchain
Bob inserts Message A, Alice inserts her message that says: "Messages A is valid" if Bob lost his private key, there is no way in blockchain how he can gain the access back of over his record. Therefore, he asks Alice to update her record publishing the update: "Message A is invalid."

The blockchain as I presented in the introduction and discussed in Paper 2 and 3 has some constraints, for instance, the loss of private keys as an exclusive access to the property record (title token as evidence of property rights), will mean the loss of the control over the record. If the access is lost, the trusted provider – the authorized validator - marks the referenced record invalid. But the trust provider can also lose control over their records. To reset the provider's record and to reset the root record, it is proposed to initiate a mechanism of *patches* to the protocol. The patch in the cross-blockchain protocol aims to provide for nodes a command which key record must be considered invalid and which record is the correct one. Such patches being published on-chain by authorized addresses are hooked by nodes in the network and applied to provide that every node has the same state of the overlaid database. The public administration maintains the list of authorized addresses or precisely keeps private keys to these addresses. This model, as I discussed in Paper 2, is not new. As per eIDAS in the EU, the system of state governments manages their national trust "roots," i.e., private keys for public key infrastructure (PKI), which they use to sign keys of Trust Service Providers (TSP). TSPs are those players on the market which provide digital identities and electronic signature for citizens. Usually, the task of the "root" keeper is delegated to the government body responsible for data security of the state.

Such filters, authorized addresses and private keys for these addresses, algorithms, how they are introduced, run and updated, constitute the "smart law" of a cross-blockchain database. The issue of the

[1] Merriam Webster Online

validity of transactions and authorization to perform some public duty links to the discussion about legal governance. In “Linked Democracy” [1], the authors propose in their Regulatory Quadrant for the Rule of Law to consider 4 types of legal governance: hard law, soft law, policy and ethics, where hard law refers to legally binding obligations; soft law, on the contrary, is usually not mandatory (best practices, and principles that facilitate the governance of networks). Policy is usually defined as “a set of ideas, or a plan of what to do in particular situations, that has been agreed officially by a group of people, a business organization, a government, or a political party.” Ethics primarily refers to morals, social mores, practical knowledge and principles that should be implemented into legal regulations, policies, and governance structures. To integrate and cope with the different notions of norms stemming from social, cognitive and computer science scholars incepted the field of Normative Multi-Agent Systems (NorMAS). It can be defined “as the intersection of normative systems and multiagent systems (MAS)” [2].

Likewise, as for smart contracts, among other proposals, Governatori et al. [3] have contended that understanding a smart contract, and assessing its legal validity and effects, requires determining what legal transitions the contract is meant to implement. Legality is deemed to affect the whole context and the contract itself. Thus, the set of legal transactions and the executable instructions would need to be kept aligned.

Depending on the level of digitization of procedures and overall governance paradigm, the level of on-chain / off-chain governance changes. “Off-chain” entails more traditional forms of legal governance. The combination of the off-chain procedures, as it is shown in the validity scheme, can be combined with on-chain transactions. But this is as a transitional model where conventional forms co-exist with digital governance through NorMAS, but as agents subsequently find new ways of how to reduce the transaction costs, they try to improve or abolish obsolete forms of governance and transform norms.

A simpler way (for a pilot) is to design a centralized electronic system where authorized addresses will be under the control of a dedicated public office, and governance is performed through traditional procedures, for instance, through “off-chain” elected representatives. The authority in charge of running the system and maintaining the mentioned addresses implements on-chain decisions that are made off-chain.

The smart law, which I showed as a combination of private and public law, can work in a democratic and decentralized way through smart contracts and electronic voting on blockchain, which is a matter of the political system where it is introduced. Other methods of collective decision-making can also be applied, for example controlling addresses in various multisignature schemas that support collective decision making, for instance, by a public commission of representatives. The protocol can be used to build a comprehensive database for any records, also for customized and localized databases for specific communities and nations.

The implementation of such a public property registry system will also require applying a viable model for information technology management and IT governance. Legal governance and IT governance are different fields, even if the latter serves as an infrastructure of the first one. Various mature models, developed through decades, are applicable. For instance, COBIT (Control Objectives for Information and Related Technologies). The COBIT framework ties in with COSO[2], ITIL[3], BiSL[4], ISO 27000[5], CMMI[6], TOGAF[7] and PMBOK[8] [4].

---

[2] The 'Committee of Sponsoring Organizations of the Treadway Commission' ('COSO') is a joint initiative to combat corporate fraud.

[3] ITIL, formerly an acronym for Information Technology Infrastructure Library, is a set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.

[4] Business Information Services Library (BiSL), previously known as Business Information Service Management Library, is a framework used for information management.

[5] ISO/IEC 27000 is part of a growing family of ISO/IEC Information Security Management Systems (ISMS) standards, the 'ISO/IEC 27000 series'. ISO/IEC 27000 is an international standard entitled: Information technology — Security techniques — Information security management systems — Overview and vocabulary.

[6] Capability Maturity Model Integration (CMMI) is a process level improvement training and appraisal program.

[7] The Open Group Architecture Framework (TOGAF) is a framework for enterprise architecture that provides an approach for designing, planning, implementing, and governing an enterprise information technology architecture.

[8] The Project Management Body of Knowledge is a set of standard terminology and guidelines (a body of knowledge) for project management.

4. High-level findings

4.1. Technological neutrality and the right to choose

The cross-blockchain protocol is designed to enable the use of multiple blockchains and other types of ledgers (private and permissioned) and traditional centralized databases on the par. And it is a matter of good governance to balance the system and provide people the choice.

Having the principle of technological neutrality as the cornerstone, implemented in legalized right of every citizen to decide themselves which technology to choose, it ensures free-market competition. Of course, this right is supported not only with hard law. It is a complex matter of all types: hard law, soft law, policy and ethics.

Why is this idea novel concerning the land registry system? As we observed in Paper 1, the traditional system is preserved for more than a century, and with all arsenal of modern technologies, citizens use the old-fashioned infrastructure. The state, through its executive public bodies, plays the role of a monopolistic service provider of this infrastructure. As I showed, none of the land registries support peer-to-peer electronic transactions, which interested parties can perform directly on the registry. The answer to the research question is yes, distributed ledger technologies can support these new types of relationships, but some conditions must be met with regard to regulation and technology.

At a more conceptual level, it is important to adhere to the principles of neutrality and pluralism in technologies. Pluralism in Latin means "multiple." Principles of technological pluralism and neutrality contribute to each other. The latter practically means none of the technologies is pre-defined and constant. The world of technologies constantly changes, and the exclusive position of one of the technologies (among others competing) will be irrational and ineffective. The principle pluralism creates the component of competition of technologies supported by free market and mechanism "demand and supply." With free choice and the open market comes accountability. Here we refer again to the principle defined in the introduction – to decentralize everything that is possible to decentralize; all the rest make accountable. Though in practice, pluralism and neutrality may encounter barriers. Historically, various land registries were developed in the nineteenth century, at least in basic modern forms as we know it now. Through decades of progress in technologies, the paper registry became a central-server electronic database, but the paradigm did not change. The centralized model of governance remained dominant. It should be noted that no alternative concepts were developed that could challenge this paradigm. The electronic form of the database just made governance more effective but not decentralized.

Blockchain became a game-changer (important to notice, distributed technologies existed before the blockchain, but they were not scalable). The implementation of blockchain technologies require new viable model of governance. The government's role shifts from being a single national provider of the land registry and registration services to a regulator on a free market of different technologies and registration services. In this system, the "registration" is not equal to the "centralized land registry." Registration is the act of *being registered*, not necessarily in one closed database owned by the government and not necessarily by a human agent. Though the government preserves the role of maintaining the traditional land registry as one of the options always available for citizens. And the government ensures enforceability in blockchains by providing a proper infrastructure based on the cross-blockchain protocol.

The validation of transactions intersects with the notion of compliance. According to the concept, registration and acknowledgment under a new public policy will mean to perform a land title deed compliant with the law with respect to private and public interests, in the way to preserve certainty in property rights based on a free choice of credible technologies. Compliance from the regulatory perspective can be understood broadly as "the act and process of ensuring adherence to the law" [1]. In the proposed scenario, the cross-blockchain protocol allows starting from semi off/on-chain compliance but subsequently adopts Compliance-by design (CbD) and Compliance-through design (CtD), which are distinguished according to the structure, components, and the nature of their effects [5]. The government adopts procedures for transferring title records from paper-based or traditional electronic databases to blockchains and vice versa. The role of the government is to provide for smart laws, model smart contracts and technical standards. Rather than providing services of land registration and keeping registries, the public administration establishes regulations and digitizes them in the form of smart laws. This is a distinctive

feature of the proposed model. Through the years, electronic governance has been presented as a way to provide seamless public services online, where the public administration is "not seen" by the citizen who uses the web-application. But the public servant is always present on the other side of this interaction. Citizens still interact through human agents, which verify the validity of the transaction that citizens submit online; therefore, e-governance is a digitized form of bureaucracy. The land registry on blockchain is the infrastructure that supports a significant reduction of bureaucratic procedures through automation. The cross-blockchain database (registry) is protected by security standards, defined by the government. Those blockchains which ensure immutable and decentralized public ledger may work in the property registry bundle.

4.2. The advantages of the system architecture

The research shows that since 2015 there were many attempts to test and trial DLTs in real estate, and currently, there is no iconic successful project which can be presented as a good practice.

At a higher level of abstraction, failed innovations have common features:

- Startups tend to address the problem using some specific technology, while the problem itself is not at the technological level. For example, the project Moneycatcha aims to reduce 14-steps of bureaucracy in the mortgage process and shrink it from an average of 42 to 5 days [6]. Both centralized and distributed ledger technologies can accommodate the solution, with almost no doubt that it will work successfully in both systems. There are many examples when blockchain is presented as a solution, while there is no problem with the technology.
- Some of the proposed solutions in the researched cases trigger the question of a proper level of solution. Instead of digitizing bureaucracy, it worth looking into the origin of the problem and address its roots (and in most cases, it requires changes in public policy – see the next problem). For example, one of the significant functions of land authorities is to maintain the electronic registry providing the infrastructure, including data centers. It becomes unnecessary with public blockchains because they are self-organized and self-sustainable.
- Most of the projects are constrained with the legislation and government inertia. And there is a reason for that. Blockchain projects mostly offer one solution for one problem, in ad hoc fashion. For example, one may propose cutting mortgage bureaucracy, another thinks about a global real estate supermarket, someone offers a multi-platform advertising standard, someone offers fractionalization of ownership. But none of these propose a bigger picture of a long-term strategy. All these projects neither have a common basis for creating a synergy of proptech innovations to contribute to each other nor the architecture design, which can accommodate various innovations working together.

The advantage of the proposed concept of tokenization of real estate and system architecture that supports it is that it is not a solution for all problems at once, but an infrastructure where all these projects will be possible to elaborate. And the public administration plays here a crucial role as a "bridge builder" to support proper solutions at the proper level.

4.3. Blockchain instead of land registry

Many of the projects and ideas around improving registration and legal relationships in real estate are based on the idea of preserving the traditional centralized electronic database and the registration act. In explored use cases, for example, Bitfury [7], and testbed with Chromaway in Sweden [8], tried to develop a blockchain solution upon their existing land registries, neither changing the land registry nor the existing regulations.

First, there is no evidence that such a structure developed over the centralized system is viable. If in the end, there is a strong role of the traditional "off-chain" land authority with discrete powers, the system remains centralized, whatever attempts are taken to build on top of that.

Secondly, as shown in this research, the registration (acknowledgment) should not be considered as a sacral act. When it is atomized on basic functions, it becomes clear which functions must be replaced by the technology:

- **archive**, which is to securely store transaction data, aimed to create certainty in "who owns what;"

- **public interest**, which means that the government leaves the right of the "last word" in a transaction by granting or not the consent for the transaction. Sometimes this is a general rule for all transactions; sometimes it is limited to certain situations, depending on the role of the government in different political systems. For example, local communities may have the right to approve a deed. They may decide not to allow an unwanted person to become a new landowner in their neighborhood (community). This tradition is preserved in many countries.
- **legal assistance or acknowledgment**, usually observed in civil law countries as a mandatory step in a transaction, known as deed acknowledgment, and widespread in most countries on volunteer basis. Depending on legal traditions and the level of government paternalism (supportive intervention of the government into a private sphere of life), such third parties help to draw a proper legal document; verify the legal capacity of parties, verify easements and other interests of third parties; and many other things so to exclude legal disputes in the future.

Neither public interest nor legal assistance (acknowledgment) can be addressed by blockchain. Blockchain for land registration can address *archive function*, and as this research shows better than traditional systems as the data cannot be erased or altered.

Though, it is incorrect to say that archive function is the dominant advantage. This feature inextricably linked to the chronological order of transactions (blockchain as a "timestamp machine"), and even more important, the transaction does not happen elsewhere and then stored on blockchain. The ledger is actually the environment where transactions happen in a peer-to-peer manner. None of the land registries provides direct access for landlords to manage their property rights on the database, but blockchain does. It works through a native mechanism of public-key cryptography, where public key is an address where a token (a record of ownership) is attached and controlled through the user's private key.

While many researchers and enthusiasts expressed the idea of peer-to-peer transactions with land titles, there was no clear vision on how to address legal intricacies. Especially when the discussion dips to the level of the architecture design. The novelty of this thesis is that it presented in a consistent concept that addresses them.

Therefore, there is no need to keep tokenized land rights elsewhere, for example, in a traditional land (cadaster) registry, because blockchain is a registry itself. The procedure of tokenization will require initial interaction with land authorities, but once the title is on the blockchain, there is no need to perform registration each time a transaction is completed - the blockchain serves as a secure repository for peer-to-peer transactions where none transaction can be revoked or altered.

The concepts of web-of-data and semantic web play crucial support to this type of electronic system. The Semantic Web is an extension of the World Wide Web through standards set by the World Wide Web Consortium (W3C) [9]. Semantic Web is to make Internet data machine-readable. Encoding semantics with the data is enabled through such as frameworks as Resource Description Framework (RDF) and Web Ontology Language (OWL) that are used to represent metadata. Ontology describes concepts, relationships between entities, and categories of things, which goes along with the NorMAS framework when we are talking about legal governance. Properly designed blockchain property registry is not just a storage of transaction with the mechanism of enforcement. The embedded semantics creates ground for reasoning over data and operating with heterogeneous data sources. That is why the future design of the land registry must include best practices of governance and ICT. This piece of the research is left for further elaboration.

4.4. No application at blockchain consensus

Based on the previous conclusion, it is important to debunk the myth of using permissioned DLT to address all aspects of land registration. The research shows that permissioned cannot ensure immutability due to its centralized nature, and it is unlikely to solve all problems of governance on the consensus level.

In permissioned ledgers, it is hypothesized that a transaction must happen only if the public interest is preserved and an act of acknowledgment is performed. The consensus protocol of the permissioned system is supposed to include the whole spectrum of legal governance withing the NorMAS framework. In other words, only compliant with law transactions are passed to the ledger. Usually, it is performed in such DLTs through so-called validators. Public "permissionless" blockchain, on the contrary, does not deal with

legal compliance and governance, its consensus protocol is focused on maintaining an irrevocable repository of transactions with particularly one public rule – no double spending is allowed, which is algorithmically hardcoded in the protocol. Permissioned protocol is imagined as an algorithm that gives or does not give consent to a transaction, gives someone access or not, etc., it heavily relies on validators and the authorization mechanism. Moreover, such technology may support retroactivity by design, where the authority can perform a retroactive action toward transactions/blocks. Of course, retroactivity can be limited in some way, but it will never become that extremely hard as in Bitcoin for example.

With such architecture, the system loses its major advantage, i.e., to remain immutable. In permissioned DLTs, the state of the database is not a result of an open, decentralized competition of unnamed nodes but belongs one actor or to a limited number of defined actors. Hence, it is a centralized system.

Compared to the approach of including addressing all the tasks of public registration in the consensus protocol, public open blockchains address the problem of transaction archiving and leave other tasks to be resolved on the level above, i.e., on the social consensus level. The cross-blockchain protocol represents the solution where the social consensus can be achieved. In the proposed concept, all other government functions, i.e., identification, authentication, enforcement, are performed at the level above. Figure 2 presents a diagram that compares the flow of transactions through consensus protocol and cross-blockchain protocol.

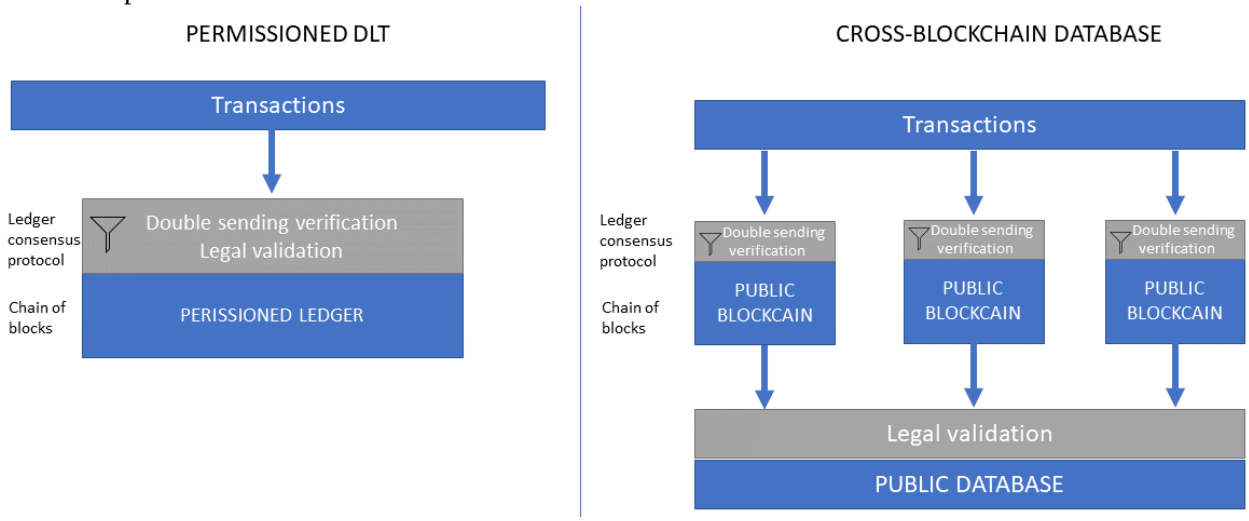


Fig. 2. Comparison of workflows of transactions between permissioned DLT consensus protocol and cross-blockchain protocol

Therefore, blockchain serves as a reliable repository of all facts that happened in the real world, be they legal or not. There is nothing to develop at the level of ledger consensus, except the protocol that ensures decentralized transaction storage and double-spending preventing, which are native functions of the blockchain invention.

4.5. Is a trusted third person required?

There are a lot of discussions mainly in the industry that the blockchain eliminates intermediaries. This statement is true but must be accurately explained. As previously discussed, the blockchain provides for:

- peer-to-peer transactions between counterparties, none of the traditional land registries support this user experience. The transactions in the electronic database are performed by registration.
- immutable storage. Blockchain is an append-only database and deleting and altering archived data is not an option. A centralized system can be changed at the discretion of administrators.
- Timestamps are one of the important functions of title registration and acknowledgment of deeds. Blockchain makes it obsolete because the chain of block ensures unchangeable chronology of transactions – blockchain is a timestamping machine.

Though it is incorrect to say that blockchain eliminates the need for trusted third parties, there are many moments in our lives that we cannot resolve on our own. A person, for example, cannot certify her or his death to initiate inheritance transfer. The two parties need a third person to resolve their dispute. People need trusted third parties, be it a public servant, a notary public, or a judge. Obviously, it is impossible to completely get rid of intermediaries, at least at this level of science and technology.

Trust records address the problem of credibility. An intermediary is a necessary trade-off, especially in the world of growing digitalization and remote relationships. Without commercial intermediaries and governments, relations would have looked like scenes from gangster movies where the seller and the buyer need to meet personally and show each other the money and the product to make the deal. The progress required more effective economic forms of intermediary to scale up the business. According to Potts et al. [10], the current U.S. GPD consists of 33% of services produced by intermediaries. It means that one-third of a transaction value between two parties belongs to the third party, the middleman.

In the proposed protocol, those whom people trust in the real world, play the same role on-chain, i.e., they certify and witness facts. In this way, any real-world facts can be certified: immovable and movable property, digital identity, facts of life (birth, death, missing, etc.), contracts, for instance, acknowledgment by a notary public (for civil law countries), facts of some events (force majeure, etc.). See Fig. 3.

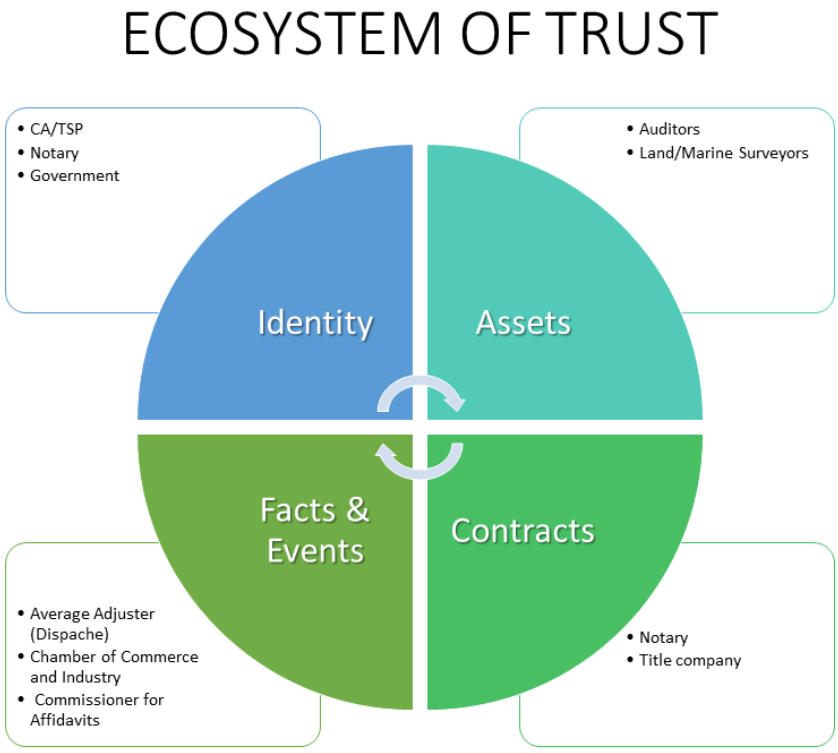


Fig 3. Map of trust records and trust providers

The map shows examples of how third parties in real-world cases certify identity, assets, contracts, and facts & events: Identity by Certificate Authorities or Trust Service Providers (EU), by a notary public and different government agencies. Assets are verified by auditors, land and marine surveyors. Contracts can be certified by notaries, land title deeds by title companies. Facts and events by Dispache (a person who certifies claims, especially for marine insurance), by Chamber of Commerce and Industry the origin of products and force majore events, Commissioner for Affidavits certifies witnesses' declarations and statements.

4.6. How not to allow a digital dictatorship?

The cross-blockchain protocol can be considered as a filter. Theoretically, any jurisdiction can also be presented as a filter, where the laws will be those filtering algorithms. What we normally call "legal" (as

per the law) is not filtered in the system and shown in the database. In this way, legal norms and procedures can be digitized and applied to transactions.

The **smart laws** in the cross-blockchain protocol are the rules which have at least two elements:

(1) *Cross-references*, when one record that belongs to the authority validates another record of an asset, a digital identity, a legal fact or a contract.

(2) At least one trusted *root address* initiated in the bundle as the "*digital authority*," which may publish records in a ledger that are considered in the system as protocol *patches*. Patches provide new filters that are accepted by all nodes in the bundle.

Both elements can be much more complicated based on the existing intricacies of politics and regulations. And some mature technologies and frameworks can support this model, i.e., semantic web. The first essential step to apply the framework of the semantic web to blockchain was made English, Auer and Domingue in "Block Chain Technologies & The Semantic Web: A Framework for Symbiotic Development" [11]. The authors: (i) have presented innovative forms of governance; (ii) advanced a set of minimal conditions for the rule of law on the web; (iii) introduced some of the requirements for legal interoperability; (iv) and proposed a conceptual scheme to frame socio-legal ecosystems.

The operational level of legal governance is to maintain trust in the ecosystem by keeping the root record (the private key). If the root record is compromised, the cross-blockchain authority must reset the trust using one of the proposed scenarios:

- Distributed (social consensus) – users will arbitrarily install and re-install root address(es) and accept patches. However, it may lead to multiple hardforks of the cross-blockchain database, different communities which stick to different roots will see a different state of affairs in the database.
- Centralized – patches are published from the trusted address (or addresses), initially provided in the system, the patch is automatically recognized as authorized instructions and installed by the system, but if the root is compromised the authority announces it invalid. The announcement will happen off-chain, for example, through the public agency website or the official publication in "Gazette." Users will have the legitimate version of the database if they install a new root address and reindex the bundle. Normally, users will download a new version of the cross-blockchain software from the official website.
- De-centralized (collective control over the root address) – The patch is initially created in the system and controlled by a multi-signature scheme. A user's system accepts patches which are published based on a collective decision.

It is considered that in the future, direct e-voting on the blockchain with automatic implementation might also be designed to address the issue of decentralized governance in large-scaled online systems. The combination of these methods can make the system more sustainable.

The blockchain can be used to improve and automate bureaucracy. Procedures can be designed in a more transparent and accountable way. Such automation can be done using closed, centralized systems that are widely used by governments nowadays; the difference is that blockchain provides a decentralized infrastructure. In a centralized system, there will be someone who controls it being a single point of failure. In blockchain, even if some applications are designed in a centralized fashion, it can be decentralized step-by-step in the future what is impossible to achieve in initially centralized infrastructure.

The system of governance has two elements: the "government," which is the list of addresses of public bodies, and "smart laws," which are algorithms that define how the government may act. Government addresses, according to their authorization, may perform some actions in the protocol. For example, addresses of the judicial system are in charge of issuing individual patches for records in disputes. If Bob illegally seized Alice's record, the court will issue and disseminate the patch in the system according to which this transaction is ignored. Therefore, Alice re-issues her token again.

Patches are disseminated among nodes through key-value (token) transactions; the authority publishes specific records, providing rules for nodes for reallocation of records. Therefore, all actions of authorities are recorded and hence, public servants are accountable.

Each node in the network hooks such records verifies if they arrived from an authorized address and apply to the current state of the cross-blockchain database. This allows addressing all possible issues of the blockchain immutability: lost keys, deaths & inheritance, hardfork doublings, contract breaches and misappropriations. This kind of scenario requires a certain level of trusted third parties' involvement.

Nevertheless, we can consider the cross-blockchain protocol a sort of public consensus, a social agreement. Since each user voluntarily decides to use this system on their own and also agree with this. If they trust the government, they apply these algorithms.

A purely voluntary model may not be scalable though; it will probably work in small communities. Therefore, to extend the system but not to jeopardize it by centralization, it is essential to adopt more structured forms of governance, including electronic voting on blockchain. Let us leave this issue for further research and development. Also, it is important to notice that forms of governance should be developed according to the political system where the cross-blockchain protocol is applied.

And eventually, to address anti-utopian concerns, it is worth mentioning that this system is resistant to a digital dictatorship. Even if corruption and violation of power happen, the citizens leave technical possibilities to overthrown authorities and "reset" the system. Here comes the major advantage of the blockchain; it remembers everything. If Alice's property is captured by the corrupted government, by applying unlawful patches, these will be recorded in the blockchain. To reset such system, the bundle must be reindexed across blockchains of the bundle from the initial block to apply new fair rules and patches. Thus, unlawful acts will be filtered out and justice restored.

5. References

1. Poblet, M., Casanovas, P., Rodríguez-Doncel, V.: Linked Democracy. Springer International Publishing (2019). https://doi.org/10.1007/978-3-030-13363-4.
2. Boella, G., Van Der Torre, L., Verhagen, H.: Introduction to the special issue on normative multiagent systems. Auton. Agent. Multi. Agent. Syst. 17, 1–10 (2008). https://doi.org/10.1007/s10458-008-9047-8.
3. Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., Xu, X.: On legal contracts, imperative and declarative smart contracts, and blockchain systems. Artif. Intell. Law. 26, 377–409 (2018). https://doi.org/10.1007/s10506-018-9223-3.
4. De Haes, S., Van Grembergen, W.: Enterprise Governance of IT, Alignment and Value. Presented at the (2015). https://doi.org/10.1007/978-3-319-14547-1_1.
5. Hashmi, M., Casanovas, P., De Koker, L.: Legal Compliance Through Design: Preliminary Results of a Literature Survey. In: Proceedings of the 2nd Workshop on Technologies for Regulatory Compliance (TERECOM 2018) co-located with the 31st International Conference on Legal Knowledge and Information Systems (JURIX 2018). pp. 59–72 (2018).
6. Homechain – Moneycatcha Pty Ltd, https://mcatcha.com/homechain/, last accessed 2020/05/22.
7. Weiss, M., Corsi, E.: Bitfury: Blockchain for Government, https://www.hbs.edu/faculty/Pages/item.aspx?num=53445, (2017).
8. The Land Registry in the blockchain - testbed. (2017).
9. W3C Data Activity - Building the Web of Data, https://www.w3.org/2013/data/, last accessed 2020/06/12.
10. MacDonald, T.J., Allen, D.W.E., Potts, J.: Blockchains and the boundaries of self-organized economies: Predictions for the future of banking. New Econ. Wind. (2016). https://doi.org/10.1007/978-3-319-42448-4_14.
11. English, M., Auer, S., Domingue, J.: Block Chain Technologies & The Semantic Web: A Framework for Symbiotic Development. Comput. Sci. Conf. Univ. Bonn Students. (2016). https://doi.org/10.1111/j.1364-3703.2010.00667.x.