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.

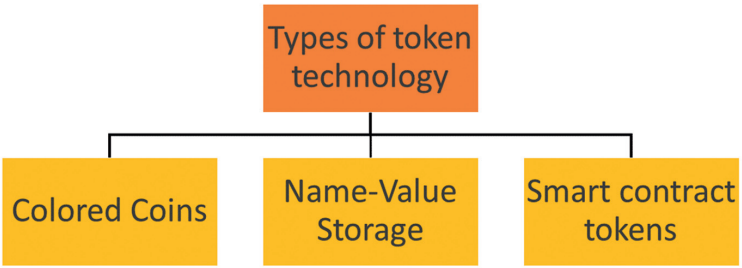


Fig. 2: Types of token technology: Colored Coins, Name-Value Storage, Smart contract tokens

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.

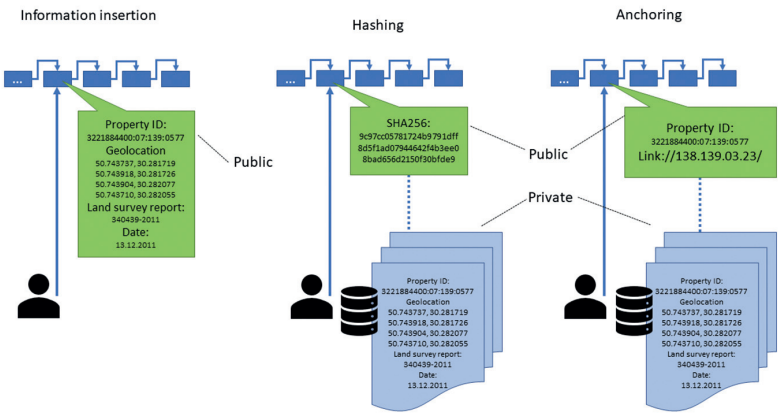


Fig 3: How to store data on blockchain. "Information insertion" – store a record in the blockchain, "Hashing" – store hash sum of a record, "Anchoring" – store some metadata of a record

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.

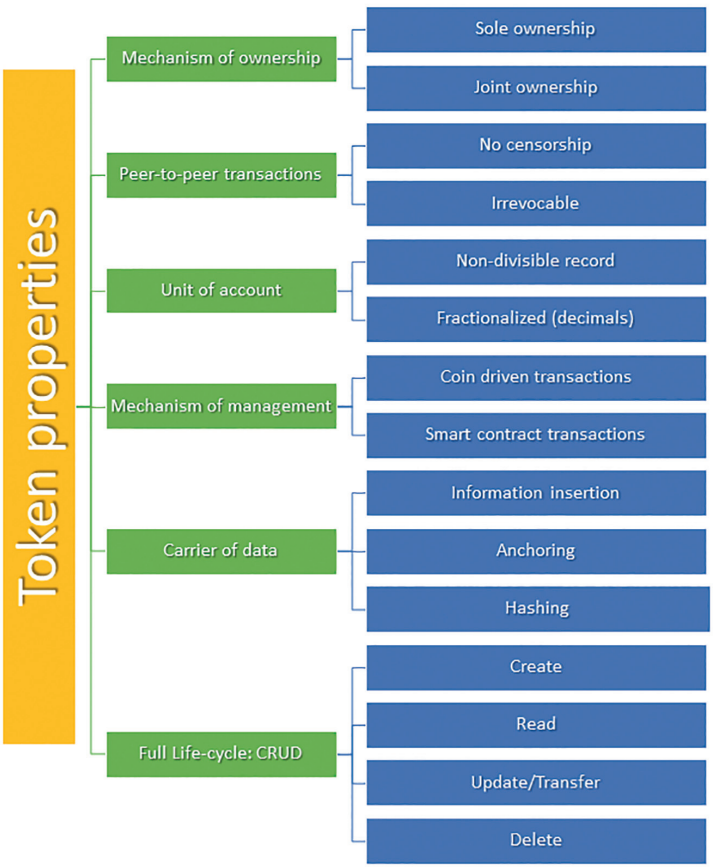


Fig. 4: Token properties

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).

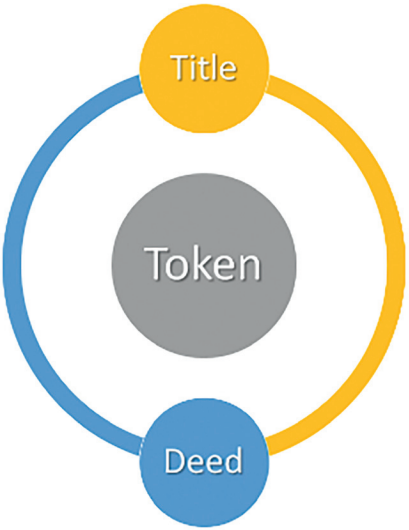


Fig. 5: Dichotomous nature of a token. Token is evidence of a property right, which is an equivalent of the concept of a title. A token is a result of a transaction, which is an equivalent of the concept of a deed.

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.

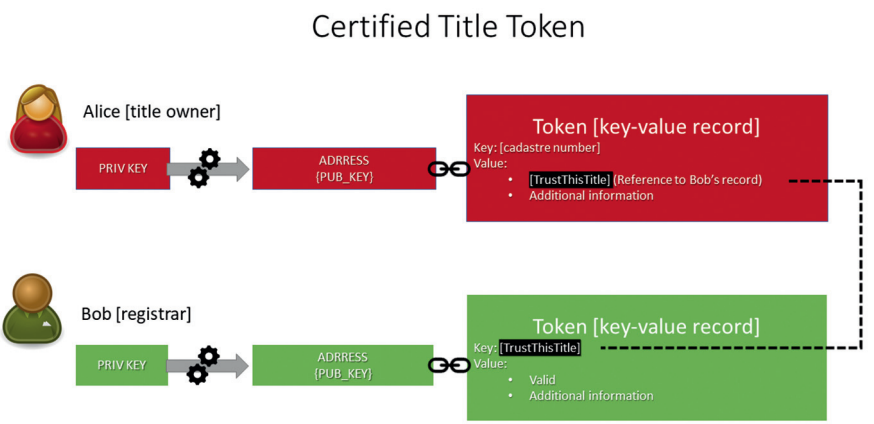
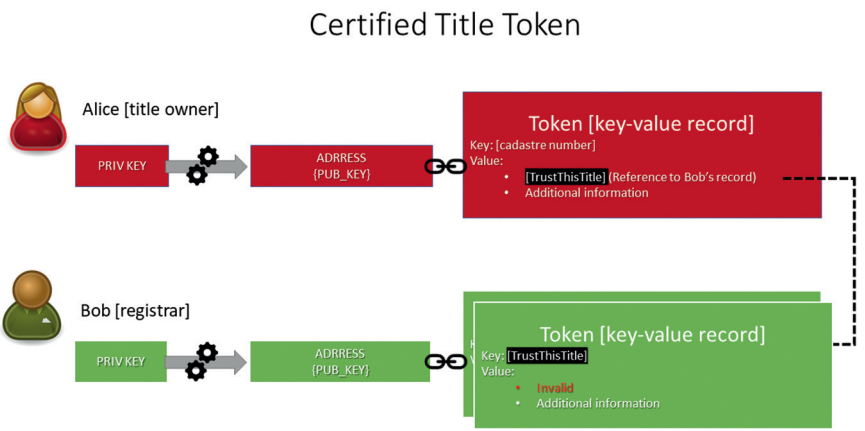


Fig. 6: Title Token certified by Registrar's Token. Alice creates a token where the key is the title cadastral number (unique key), and value is a reference to Bob's token. Bob creates a token with the key, which Alice included in her token as the reference. Bob adds in the field "Value" the record of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

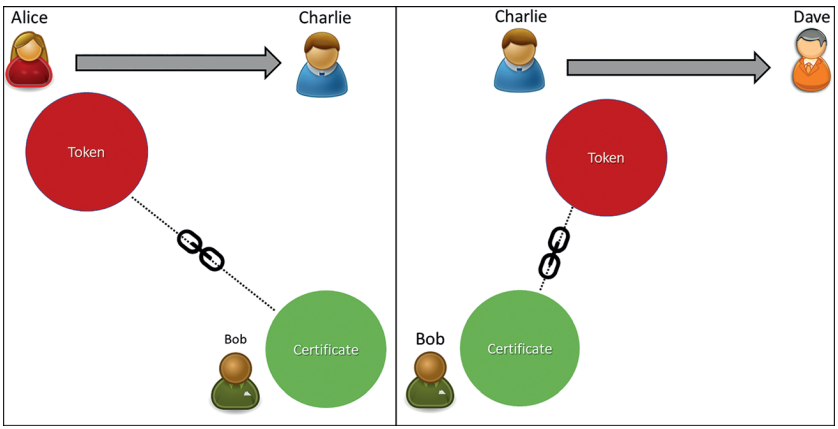


Fig. 8: Title Token transfer. Alice transfers her token to Charlie. Then Charlie transfers Dave. In both cases, Bob initially certified the token; this connection remains in all subsequent transactions. There is no need to register a deed because blockchain is the registry.

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.

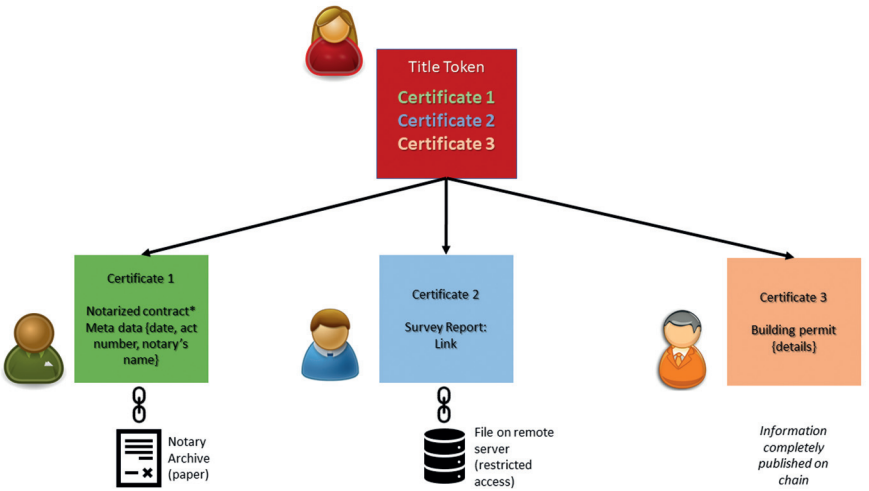


Fig. 9: Title token transaction authorized by multiple bodies. Notary acts may be performed in a rudimentary form (paper); thus, the notary publishes the token that declared that the act had been performed, token contains metadata of the act. The survey report may be published on the blockchain or included 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.

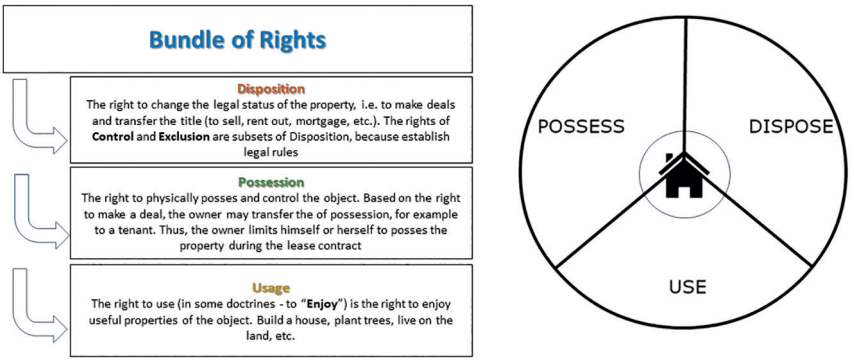


Fig. 10: Bundle of rights: to dispose of, to possess, to use (enjoy)

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.

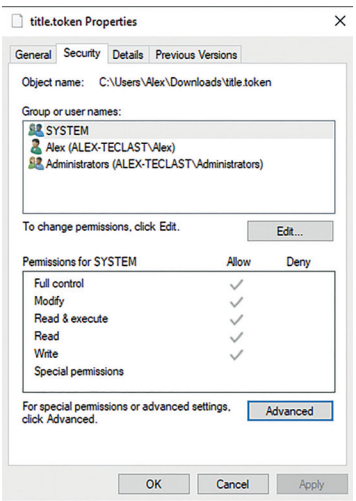


Fig. 14: Windows CHMOD

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.

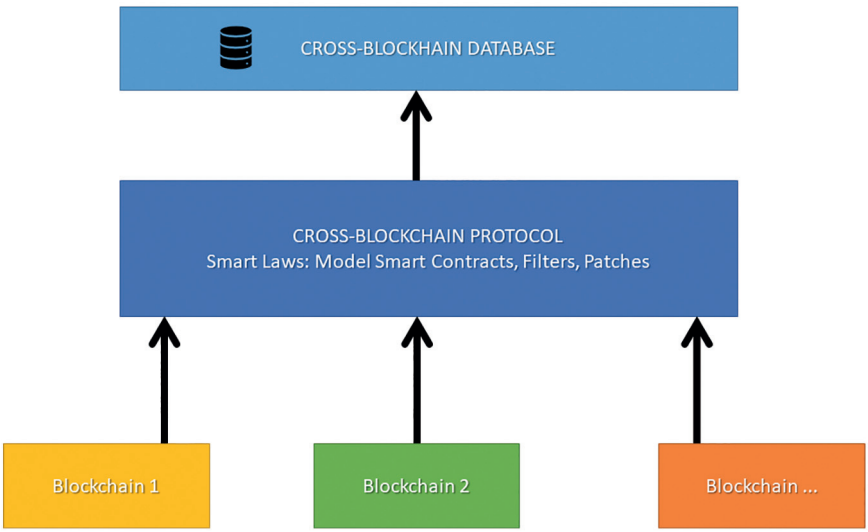


Fig. 15: Three layers of a smart law system. 1. Blockchains are public repositories with mechanisms of ownership and P2P transactions. 2. The Cross-blockchain protocol unites blockchains in the bundle and contains "filters," i.e., the rules which are applied to transactions when they are published, model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