Responsible Land Governance:
Towards an Evidence Based Approach
Annual World Bank Conference on Land and Poverty
Washington DC, March 20-24, 2017

# Blockchain – can this new technology really revolutionize the land registry system?

**Maurice BARBIERI**
The Council of European Geodetic Surveyors

maurice.barbieri@clge.eu

and

**Dr. Dominik GASSEN**
German Federal Chamber of Civil Law Notaries

d.gassen@notarnet.de

**Paper prepared for presentation at the**
**“2017 WORLD BANK CONFERENCE ON LAND AND POVERTY”**
**The World Bank - Washington DC, March 20 -24, 2017**

## 1. Introduction

*"Of the 7.3 billion people in the world, only two billion have a title that is legal and effective and public regarding their control over an asset. […] When something is not legally on record as being owned, it can therefore not be used […] as collateral to get credit, as a credential that you can be able to transfer part of your property to invite investment in. Things are owned, but when they're not adequately paperized or recorded, they cannot fill the functions of creating capital and credit."*[1] This quote of the well-known economist *Hernando De Soto* underlines the **need for efficient land administration systems**. The Doing Business Report 2016 shows that over the past five years **37 economies computerized their land registry** and that in these countries, the **time required to transfer property** has fallen by 38% since 2011.[2] However, the time required to transfer property is not decisive if the **reliability of information on property titles**, which is a crucial function of the register, cannot be ensured.

In this context, some claim that a **blockchain-based approach** to registering property titles could significantly **increase the efficiency** of conveyancing and even **prevent fraud**.[3] It is also alleged that **property transactions** could be handled on a blockchain in a similar way to payments between parties using digital currencies.[4] In simple terms, a blockchain is a type of distributed ledger of digital records or transactions that is accessible to all computers running the same protocol. Although the blockchain technology has almost exclusively been used for the digital currency named "Bitcoin" so far, the potential use of this technology is currently being explored in various other fields. Last year, for instance, a project to blockchain the **land register** of **Honduras** was launched. One of the purposes of the project was to give the owners of the nearly 60 per cent of undocumented land an incentive to register their property officially.[5] Apparently, the project has stalled. But there are more developing countries considering blockchain a promising technology to build their land registry system on.[6] Even **Sweden** is currently discussing opportunities for a blockchain-based system.[7]

Against this background, this paper will briefly set out the **main features** of the blockchain technology (2). Based thereon, it will describe in more detail for what **purposes** blockchain-based solutions are currently being used or promoted (3). Finally, this paper will thoroughly assess the **risks and legal impacts** that are related to the use of the blockchain technology in **judicial matters** and more specifically **for land registers** (4).

[1] Shin, *Republic Of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto, BitFury*, available at http://www.forbes.com/sites/laurashin/#1143578f655d (Accessed 08 February 2017).

[2] World Bank. 2016. Doing Business 2016: Measuring Regulatory Quality and Efficiency. Washington, DC, p.78.

[3] Shelkovnikov, *Blockchain applications in the public sector,* available at https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-app-in-public-sector.pdf (Accessed 08 February 2017).

[4] McLean/Deane-Johns, *Demystifying Blockchain and Distributed Ledger Technology – Hype or Hero*, Cri 4/2016, 97.

[5] Dale, *Three Small Economies Where Land Title Could Use Blockchain to Leapfrog the US*, available at http://observer.com/2016/10/benben-factom-bitfury-ghana-georgia-honduras/ (Accessed 08 February 2017).

[6] Dale, Ibid.

[7] Chavez-Dreyfuss, *Sweden tests blockchain technology for land registry*, available at http://www.reuters.com/article/us-sweden-blockchain-idUSKCN0Z22KV (Accessed 08 February 2017).

## 2. What is the blockchain?

Technically speaking, the blockchain is a **decentralized** or **distributed database** consisting of consecutive blocks that contain pieces of information. There is **no central authority** defining the correct state of the database.[8] The database is not under the control of a (central) individual or institution; on principle, every user with access to the blockchain via software can possess his own copy of the complete database. **Cryptography** ensures that nobody can alter the data contained in the blocks without being noticed: each block of the blockchain contains a cryptographic reference to its prior block. A **trust relationship** between users is therefore deemed **unnecessary**. The **main features** of the blockchain can be summarized as follows:

### Networked Integrity

The blockchain is based on the principle of **hash values**. A hash value is a cryptographic, ideally unambiguous value connected to a file, often referred to as its “fingerprint”. The blockchain does not only generate specific hash values for electronic documents or other information (as compared to electronic signature processes) but also stores signed hash values serially in a kind of register (***ledger function***). A new hash value and the corresponding signature are added to the blockchain file as a **new block**. In order to ensure the **integrity** (invariability) of the stored hash values, blockchain applications do not use a central authority (like a trust service provider/certification authority), but rather rely on "swarm intelligence" because the integrity of the ledger is protected by the multitude of its distributed copies on computers all over the internet (***distributed ledger***).

For that reason, high availability is one of the advantages of a blockchain system in its pure form. For the same reason, blockchain neither “proves” the authenticity of a transaction (= addition of a new hash value to the register) nor is the integrity of all hash values guaranteed by a central authority – for example as part of a public administration. Blockchains rely on "swarm intelligence" insofar as information that is added to the chain will be acknowledged as valid if a majority of the ledgers recognizes it as such.

In order to carry out a transaction, a signature is created with a private cryptographic key that comprises the information of the transaction. The signed transaction is then published to the network. Now all participants can verify it by extracting the public key of the signature of the sender and verifying the validity of the signature. If the signature corresponds to the transaction, the participants validate it. Thus, with blockchain, two parties who don’t know each other should to be able to agree that something is "true" without need for confirmation from an intermediary or a central authority.

[8] Values do not exist in an absolute manner in the blockchain. The available value is rather composed of the history of all prior transactions. That is why the entire blockchain has to be taken into account when verifying a value.

### Distributed Power

The blockchain is based on an ideology that has an inbred skepticism towards public authorities. It tries to protect itself from interference by such authorities by subscribing to a distributed approach that cannot be easily controlled even by a central player. The flip side of this idea is that the trust needs to be placed in the system and its mathematical and computational tenets because there is nothing else that will serve as a trust anchor.

### Publicity

Due to its decentralization, the blockchain has to be public – otherwise there would be no way to generate the necessary number of participants to achieve the necessary degree of distribution. Because only hash values are stored, it is not possible without further information to connect actual transactions to a blockchain proof - no conclusions can be drawn from them regarding content data.

### Anonymity

At its core, blockchain systems are anonymous: transactions are connected by certificates. Blockchain itself does not reveal the identity of participants, neither will it provide information on which natural or legal person is connected to the certificate in real life.

### Irrevocability

The blockchain does not forget: the deletion or change of a value that has become part of the blockchain is virtually impossible.

## 3. For what purposes are blockchain systems used or promoted?

Blockchain technology has so far mainly been *used* for **virtual currencies, the main example being** "Bitcoin"-system. However, more and more companies ("legaltech") explore using blockchain technology to secure the integrity of electronic documents or to indirectly verify the authenticity of a document. As of now, these services seem little more than a functional variation of the results that can be achieved by using qualified electronic signatures. The only difference being the lack of necessity for a central trust service.

One of the core targets of the introduction of blockchain technology today is *a proposed reduction or even elimination of* so-called "intermediaries" which will reduce **transaction costs**. Banks and stock exchanges (payment and accounting systems, clearing and settlement systems), registers of all types (commercial register, land register), but also authorities such as tax authorities, social services, road traffic authorities and notaries (in the latter case mainly as far as the certification of signatures, the preservation of evidence and notary escrow accounts are concerned) are some of the "intermediaries" whose roles are questioned.

## 4. What are the risks and legal impacts related to the use of the blockchain technology for land registers?

There are a number of aspects that raise **serious concerns** with regards to the use of blockchain technology in **judicial matters** (a) and more specifically in the **land registry system** (b):

### a) General reservations against blockchain technology in judicial matters

#### Networked Integrity is not secure enough.

Blockchain is assumed to secure the integrity of a transaction by relying on the fact that the majority of systems participating in the blockchain at hand will recognize a transaction as being “authentic”. Only with this assumption two parties who do not know each other can agree that a transaction is "true" and can be relied on without need for official confirmation from an intermediary or a central authority.

In the recent past, even advanced blockchain systems have already been proven **insecure**. The use of a great amount of computing resources made it possible to "capture" a blockchain and to “steal” Bitcoins worth millions of dollars.[9] If you have access to the majority of systems hosting a certain blockchain’ s ledgers you can in fact decide which transactions will be regarded as true and become part of the blockchain. This problem is only thrown into sharper contrast once you take into consideration that with the proliferation of blockchain systems it cannot be expected, that every blockchain will find the critical number of distributed hosts to validate the assumption of swarm intelligence. If one single person or interested group can hijack a blockchain system with few participants, they will have the power to alter or falsify the blockchain as they see fit. The anonymity principle of blockchain makes prosecution of such fraudsters difficult if not impossible.

Next, developments in Bitcoin suggest that trusted third parties as intermediaries will not become obsolete, but merely replaced by clusters within the system that – by marshalling a large amount of computing resources will assume this de facto role. Currently, more and more "Bitcoin miners" are joining to form so-called "mining pools". At the same time, a trend towards special hardware, application-specific, integrated circuits, used specifically to calculate as many hash values per second as possible (so-called ASICs) leads to a shift away from the "democratic" assumption that each participant with his home PC can assume an equal role in the system. Both trends lead to a **decrease in the decentralization of the system**.[10] Today, only four mining pools control the majority of the Bitcoin's blockchain.[11]

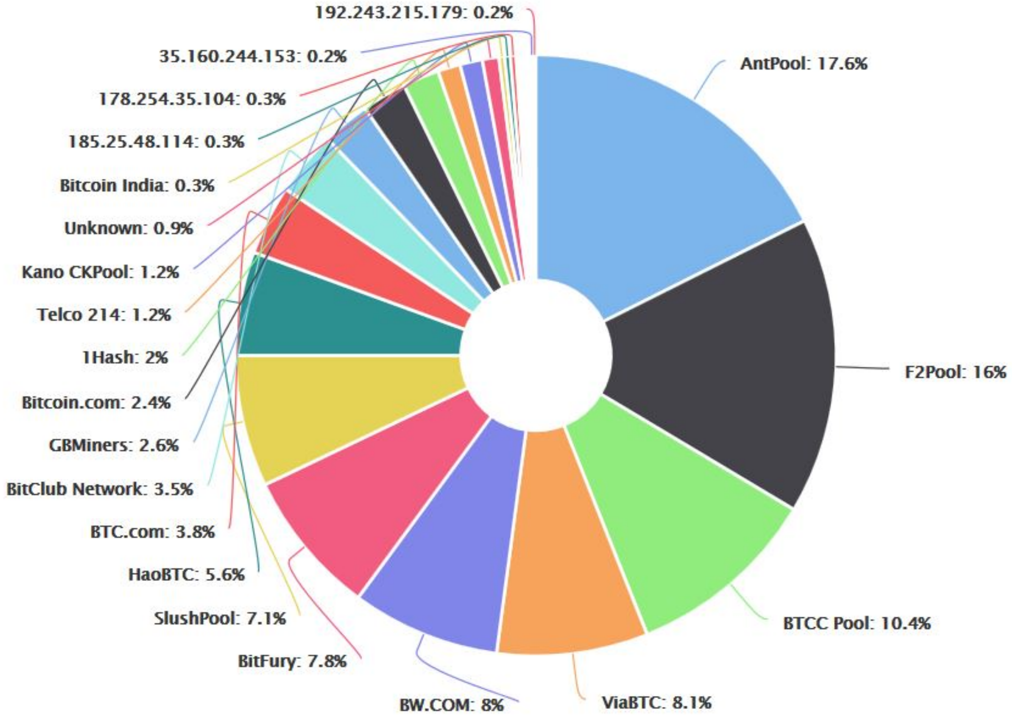
[9] http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/bitcoin-anleger-verlieren-rund-ein-drittel-ihrer-einlagen-14377697.html; https://bitcoinblog.de/2016/06/20/zwoelf-der-groessten-bitcoin-hacks/.

[10] As far as mining pools are concerned, the reason is that the miners integrated in the mining pool do not operate themselves their own so-called “full node“ (i.e. the entire blockchain), but only one full node together in order to transfer their calculations as quickly as possible to the central server of the mining pool. As a consequence, the number of full nodes is continually decreasing.

[11] https://blockchain.info/de/pools (accessed 10 February 2017).

Thus, a blockchain can be hijacked by acquiring enough computing power. It does not take a lot of imagination to see interested countries taking over blockchains with the use of states' resources.

***Table 1*****:** *Hashrate Distribution - An estimation of hashrate distribution amongst the largest bitcoin mining pools*[12]



For a decentralized system it is extremely dangerous if large blocks of the blockchain are generated successively by one or few actors. This manipulation is called a "structural majority attack" (also "51% attack").[13]

[12] https://blockchain.info/de/pools (accessed 10 February 2017). Note: The graph shows the market share of the most popular bitcoin mining pools. It should only be used as a rough estimate and for various reasons will not be 100% accurate.

[13] A consensus on the last block of the blockchain is found when all participants systematically accept the longest chain. Depending on the method for the proof of work, attacks are possible by creating an artificial majority with a different consensus than the honest rest of the network. This type of attack is therefore called "51% attack", even if it is quite possible to carry out attacks on a network with a significantly smaller share. If, by accident, two miners solve a block at the same time, some of the participants, in particular the miners who first learned about the block variant A, will consider this as the correct one, whereas the rest of the participants will focus on variant B. It depends on the group which solves the next block more quickly which block will be continued. In an attack, malicious miners would practice the so-called “selfish mining“, which means that they would withhold their findings and start to calculate on the basis of the next block without the other miners knowing about it. By retaining blocks, they gain a time advantage in the first place. From the moment Group A has secretly completed a block, it can make its calculations exclusively on the next block. This strategy allows the attacker to pursue several objectives. On the one hand, he can benefit from a time advantage by solving a new block, which gives him a reward (block reward) (= money). On the other hand, the attacker can also decide which transactions enter the blocks for the blockchain (= power). An attacker could also trigger a payment to a service provider or a mail-order company via the regular public network if he knows that he has a lead in the calculation of blocks. He could then calculate a parallel chain and, if he publishes it – contrary to the expectations of all other participants – decide not to include a single transaction in the blocks. Since all participants accept the longest chain, the transactions from the previously publicly known block fall back

## Distributed Power is undemocratic if concentrated in the hands of a few individuals

If the power to generate new blocks is concentrated in the hands of a few individuals or groups the intrinsic lack of democratic legitimation becomes increasingly apparent. Traditionally, central (state) authorities, who are democratically legitimized, will guarantee the identity of persons participating in an important public system and the authenticity of the transactions performed. Blockchain, being beyond state supervision and control by design will lead to a lack of individual and organizational responsibility. It replaces the trust put into stable public organizations by putting it into the hands of anonymous (interested) actors who are by design hard to identify and even harder to control.

## Protection against seismic shifts in political systems will prove a pipe dream

It is an illusion to expect that a system of major political and economic significance – such as a land register or a country's currency will survive a major political shift such as a coup solely because it relies on a distributed registry. Political players acting on this level have other avenues of action such as disavowing the prior system by law and introducing a different system that is again under the influence of a state authority.

## Software layers between blockchain and user interface are vulnerable

For any user, the trust invested in a blockchain system must not only comprise the mathematical and conceptional foundations of blockchain – but also the integrity of any and all levels of software that are necessary to participate in the system and effect a transaction. That means not only the software running the actual blockchain entries must be trusted but also the "wallet" software, the software enabling the transactions on a transfer level over the internet, the local operating system, browser and add-ons. This adds up to a level of complexity that cannot sensibly be verified to be trustworthy in its entirety. On the contrary, it opens a multitude of possible avenues of attack that would make it much easier for an interested party to sabotage or defraud a transaction than attacking the blockchain at its core. In the past, attacks against these software levels have often proved successful. As of now, there is no system in place that will offer at least a modicum of certainty by independently certifying suggested software components or system setups that can be deemed secure.

into a pool of unconfirmed transactions and are suddenly considered potentially unsafe because they are no longer confirmed. Thereby, some transactions will be rejected before they find their way into the next block of an honest miner. Merchants may have already sent goods and suddenly, they will have to worry again about the payment.

## Risk of key loss jeopardizes legal security

Apart from that, simple hacker attacks on private computers and trading platforms can lead to the loss of cryptographic keys that are indispensable to prove ones participation in an transaction – or simpler: to prove ownership. This way, value can be irrevocably lost.[14] In current systems, private keys are often stored in a central "hot wallet" system which makes them particularly vulnerable. Wallet files of users have already been stolen via targeted attacks. Passwords to use private keys can simply be recorded with the well-established use of keylogging software, installed by a hacker on the computer.

More to the core of the concept of bitcoin it seems a difficult proposal to expect citizens without special affinity to computer systems to be expected to recognize the importance of such cryptic key files – especially for transactions that will only occur a few times in their lifetime (like the purchase of real estate). Computer systems crash, get replaced, hardware fails, mobile phones get exchanged every so often – new technology keeps replacing the older. Every experience proves that that vital data will get lost along the way – never to be recovered. There is good reason that every system that handles items of significant value (i.e. banking, land registers, citizen registration) has other failsafes and means of certifying ownership – even if electronic online systems and tokens are used for day to day transactions.

## Anonymity favours fraudsters

Contrary to what is suggested by some consulting firms,[15] transactions using blockchain technology are highly suitable for tax fraud, money laundering and terrorist financing because the system cannot identify individual behind a transaction. It can only link it to an electronic certificate that might belong to anybody. Nobody controls ownership of a certificate or its disposal. There is no control of personal data. The blockchain is anonymous and actually prevents the identification of the actual parties of a transaction unidentified.

## Irrevocability creates serious data protection issues

The deletion of hash values and keys used is (almost) impossible when using blockchain technology. The resulting data protection issues are still completely unresolved – the possibility that data can be deleted is a major component of any data protection regulation. For that reason, controlling what is registered in a relevant blockchain system becomes even more important, especially if automatized processes are triggered by entries in the blockchain.

[14] If a private key gets lost, its owner loses all transactions addressed to the corresponding public key. If a third person gets access to the private key, he or she can perform transactions without the knowledge or intervention of the owner. In this case, it is not possible to reverse the transaction, as, after a valid signature has been entered, the participants of the network confirm the validity of the transactions and make them irreversible by integrating them in the blockchain.

[15] Shelkovnikov, *Blockchain applications in the public sector*, available at https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-app-in-public-sector.pdf (Accessed 08 February 2017).

## Preservation of evidence cannot be ensured

Blockchain by itself cannot permanently ensure the validity of its information as evidence. It is an accepted fact that all systems that rely on encryption such as hash functions and public key signatures (which are at the core of blockchain technology) will lose their structural security with the advance of computer systems, which is why in signature systems keys and algorithms have to be replaced in regular intervals. For that reason re-encryption/re-hashing for the purposes of permanent encryption and preservation of evidence is an unavoidable necessity. For blockchain systems, as of now, there are no "external safety shells" that will allow re-encryption. They are not suitable for the long-term storage of relevant information.

## Additional document storage is necessary

A blockchain system will not store any documents – just reference information and – to a certain extent – metadata. Consequently, the relevant documents would still have to be stored in a central repository for users to make sense of the transactions stored in the blockchain. Because this will require storage capacities a number of times greater that the blockchain itself it will not lend itself to a distributed approach. This is another place where the mirage of a system without a centrally maintained infrastructure breaks down.[16]

## Data accumulation makes blockchains cumbersome

The blockchain constantly increases in size: over time huge amounts of data accumulate, because the blockchain must always remain as a whole. As a result, one of its greatest advantages, high availability, might not be real in the long run.[17] Suitability and efficiency of the basic technology has yet to be proven for large volumes of data. Tendencies apparent in Bitcoin systems paint a sobering picture.

## Energy consumption remains an unsolved issue

Blockchain technology is not sustainable. Since blockchains are decentralized, have to be stored on a large number of computers and constantly checked and updated, they also require significant resources (gross computing capacity, gross memory space, gross bandwidth, power, etc.) in comparison to centrally stored databases. For instance, a single bitcoin transaction requires as much energy as 1.6 US households per day, and requires more than 5,000 times more energy than the VISA credit card system.[18] Estimates liken the bitcoin network's energy consumption to the power use by nearly 700 average US homes at the low end of the spectrum and to the energy consumed by the island of Cyprus at the high end.[19] That is more than 3.9 billion kilowatt-hours,[20]

[16] However, there are already providers that offer both services: http://www.silicon.de/41635542/storage-und-blockchain-wachsen-zusammen/.

[17] For example, in order to participate in Bitcoin, one already has to download a file of 95 GB.

[18] http://motherboard.vice.com/de/read/das-oeko-problem-von-bitcoin-darum-ist-die-krypto-waehrung-nicht-nachhaltig-3920; vgl. auch https://bitcoinblog.de/2014/10/15/wie-viel-strom-verbrat-das-bitcoin-netzwerk/.

[19] Izabella Kaminska, *"Bitcoin's Wasted Power – and How It Could Be Used to Heat Homes*", FT Alphaville, *Financial Times*, September 5, 2014.

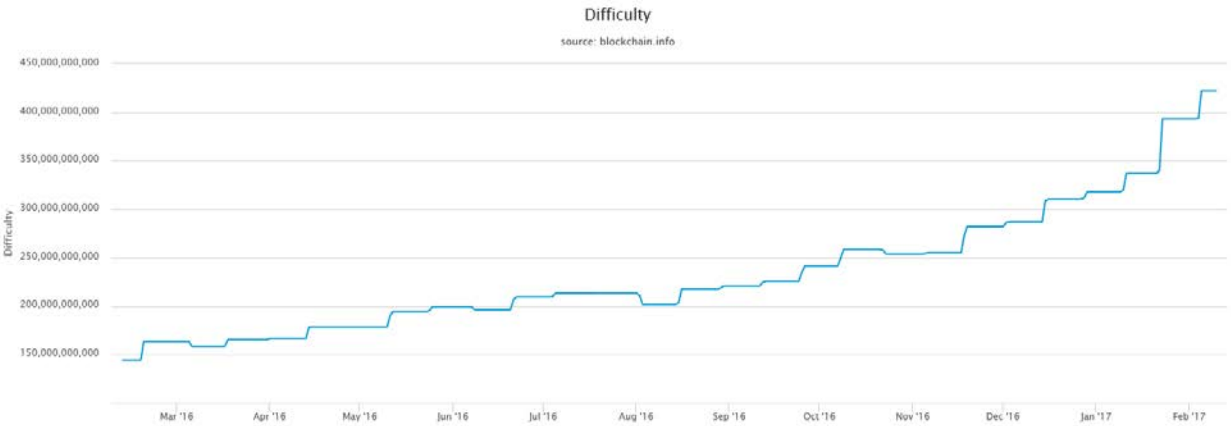
[20] CIA, "The World Factbook, "www.cia.gov, 2017; http://tinyurl.com/noxwvle (accessed on 10 February 2017).

a Godzilla-sized carbon footprint, and it is by design. It is necessary to secure the network and keep the nodes honest.[21]

### Increasing complexity exacerbates energy consumption issue

In addition, the consumption of resources necessarily keeps increasing because the level of difficulty for adding a new block rises as a consequence of the increase in computing power within the network.[22]

***Table 2:*** *Difficulty - A relative measure of how difficult it is to find a new block. The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners*



## b) Specific reservations against blockchain technology for land registers

In addition to the reservations blockchain technology encounters in general in judicial matters, any decision to consider blockchain technology for **land registers** should be preceded by a thorough assessment of its risks and legal impacts:

### Consensus about legal owner is a precondition

First of all, blockchain requires that all property is assigned to a transaction output. That **output** belongs to the initial owner recorded by the system.[23] As a precondition, there must be a consensus about the legal owner. But especially in developing countries not only the ownership but also the plot size and boundaries of a specific land parcel are often in legal dispute.

[21] Tapscott/Tapscott, *Blockchain revolution - How the technology behind bitcoin is changing money, business and the world*, 1st edition 2016, p. 259.

[22] https://blockchain.info/de/charts/difficulty (downloaded on 10 February 2017).

[23] Mizrahi, *A blockchainbased property ownership recording system*, available at http://chromaway.com/papers/A-blockchain-based-property-registry.pdf (Accessed 08 February 2017).

## Risk of key loss jeopardizes legal security

In a blockchain-based system property ownership is associated with a certain private key. It is assumed that the person who has the key is the legitimate land owner. Yet, as mentioned above, there is a non-neglectable possibility that a key will be lost or stolen.[24] In this case the legitimate owner would not be able to perform any legal transactions with respect to the property anymore. The use of the blockchain technology would require a true *behavioral change*. Most people who own real property would not be in the habit of backing up their proof of the legal title on a flash drive or a second device, securing their private keys, or keeping these backups in separate locations so that, if their lose their computer and all other possessions, e.g. in a house fire, they do not lose all their means to prove their legal title to property. There is good reason, that land register systems will tie the ownership of real estate to the identity of a person which can be proven in other ways, even if for example an identification paper has been lost. It is also one of the basic tenets of computer security that the ownership of a token of data (cryptographic key) is not enough to secure the identity of a person in systems with a higher level of security.

## Complexity of real estate transactions cannot be reflected in a blockchain

Apart from that, even if the transfer history of a property was securely preserved in a blockchain, it is not clear how the multitude of possible entries that comprise a modern land register can be transferred to a blockchain. These entries have a high legal complexity such as pre-emptive rights, easements and different types of mortgages can be recorded in this system; they have complex relationships as well – like rank or other interdependencies. This becomes even more obvious when regarding cross-border conveyancing because of the significant differences between real estate regimes in common law and civil law countries. Those differences concern not only the various types of rights *in rem* but also the functions and effects of document or data registration. As a matter of fact, there is no way to compare the legal framework of transferring and administering real property to trade of the single currency bitcoins. The legal complexity of property transfers also produces the need for the involvement of qualified (and trusted) third parties who would have to certify information to be entered into the blockchain. If the quality of the data "input" for registration is not checked and data is not filtered the quality of the "output" will not be sufficient for a system of such immense economic importance as a land registry.

## Vulnerability of the blockchain technology has especially grave consequences in the real estate sector

The security concerns against the general use of blockchain also apply in judicial matters (e.g. tax fraud, money laundering, terrorist financing, centralization through mining farms). They might even have more distinctive negative consequences for the real estate sector. For example, a ledger might be "captured" if someone was able to control the majority of ledgers[25] and, as a result, legitimate owners could be deprived of their property. *Satoshi Nakamoto* wrote, "*You will not find a solution to political problems in cryptography*."[26] A cure-all to big government has to be found elsewhere. What is to prevent a Rogue State from aiming all its state processing assets and all its mining pools at a "real estate blockchain" to stage a 51 per cent attack or at minimum destabilize

[24] Mizrahi, Ibid.

[25] McLean/Deane-Johns, Ibid.

[26] Satoshi Nakamoto, „Re: Bitcoin P2P E-cash Paper", *The Mail Archive*, November 7, 2008; www.mail-archive.com/, http://tinyurl.com/oofvok7.

the process? What if some wealthy despot decides that blockchain technology has become so influential that it is eroding his power? He might seize all the mining power within reach and purchase the rest from countries that still tolerate his regime, to put him over the 50 per cent has rate threshold. He could then decide which transactions to include and which to reject.[27] Alternatively, blockchain technology could be simply banned by the State or the despot. The result would be same: legitimate owners would be deprived of their property.

## Well established interplay between cadaster, land register and notaries provides more benefit to a functioning economy than blockchain

There are some good reasons why most land register systems are kept by the government or other public agencies controlling the register's content. Trusted third parties such as notaries and surveyors who are strictly supervised be government agencies have to make sure that the information entered into the register is accurate and complete. The surveyors are responsible for the **technical integrity and correctness** of the land data, the notaries are responsible for the **legal integrity and correctness** of the documents and the transactions, both are responsible in their respective fields for carefully identifying the parties and providing comprehensive advice. Checking and verifying the authenticity of the documents prevent false entries and distort fraudsters.

In many jurisdictions **public faith** is attributed to the entries to facilitate transfers and make the transactions **less costly**: Anyone may fully trust the information kept in the register and as a result additional private legal examinations and expensive certificates are not required. If the information in the register (in exceptional cases as entries are checked carefully) proves to be wrong, the state, the registrars and the trusted third parties are liable. But who would be liable if damage is caused by false entries in the blockchain-based system? And who would be able to control the input into the blockchain and who would be able to supervise these controllers?

If in the interest of a functioning economy, land is to be made **fungible** and a **secure real estate loan** is to be provided, the land register must be endowed with the function of **presumption** and **public faith**. This, in turn, requires the **highest possible data quality**, which must be ensured by a **control of legality and identity**. The effects of **public disclosure** and ***bona fide*** **acquisition** of real property cannot be put into question as this would affect the **safety of real estate transactions**. This would not only be to the detriment of legal culture, but also with regard to the **domestic and European protection of property** (e.g. Art. 14 of the German Fundamental Law; Art. 17 Charter of Fundamental Rights): the loss of rights which the true beneficiary has to accept in the context of good-faith acquisition **can only be justified** if the medium in which the legal presumption of correctness resides is ***extremely reliable***. Also, **transaction costs** in real estate transactions would significantly increase due to **extended due diligence exercises** and the **requirement of title insurances**.

[27] Tapscott/Tapscott, Ibid, p. 335, 340.

## 5. Conclusion

With respect to the potential use of the blockchain technology in *judicial matters* it must be concluded that the blockchain raises serious security concerns, promotes tax fraud and money laundering and itself does not offer any solutions for

- Document and data storage;
- Data transport and data protection;
- Issue of certificates and the transfer of ownership to users; genuine authentication (= identification) of users;
- Preservation of evidence and encryption;
- Protection against key loss; and
- Sustainable management.

Particularly when it comes to the use of the blockchain technology for *land registers*, it appears that the well-established interplay between cadaster and the land register and especially the role of the notary in the framework of the preventive administration of justice has not been fully understood by the advocates of blockchain-based solutions.

From today's perspective, blockchain technology seems to be useful only in the context of machine-to-machine communication, e.g. the "Internet of Things" (fridge, lawn mower, car, heating, etc.) because of the high affinity of the blockchain for standards: the more participants and transaction types exist, the more complex the adoption of new standards becomes.

***