Mariam Chilachava*

Specific Private-Legal Aspects of the Blockchain System Functioning

In the 21st century, humanity is facing a fourth – technological revolution, characterized by an amazing pace and scale of development of digital technology. The cause of this revolution is blockchain technology, one of the most relevant, discussed and promising systems today, which is also becoming the basis of the new digital economy.

The goal of the work is to introduce the essence and structure of the blockchain technology to readers, to analyze the blockchain system in the private-legal context, to discuss private-legal endogenous and exogenous problems reasoned by DLT implemented transactions, to contradict the autonomy of the blockchain system with national legislation, to offer legislative alternative for legal regulation of the blockchain system, to define the necessity for symbiotic coexistence of technologies and the Law and to offer the ways for finding the compromises needed for such coexistence.

Keywords: *Blockchain, Distributed Ledger Technologies, endogenous problems, bona fide purchaser, cryptography, private key, irreversibility of transactions, property, public key, hash.*

1. Introduction

Given the current trend, the need to understand cryptocurrency as an object of civil law is on the agenda. This means protecting the property right over it and preventing unauthorized disposal by the illegal owner. Therefore, the existence of such a legal mechanism, which prohibits the unauthorized owner from entering into a new transaction, which in turn will prevent irreparable damage to the real owner. In addition, the question of the typological attribution of crypto-assets to types of legal entities is a significant one- whether it is movable or immovable property? What is the legal regime for the emergence of property rights and, therefore, protection? The article considers the problem of unauthorized use of a blockchain personal key by an unlawful owner and its legal consequences.

The goal and objective of the paper is to provide necessary information on blockchain technologies to readers and to give in-depth presentation of legal problems related to them, to offer compromises necessary for coexistence of information technologies and the Law and solutions to problems to be solved by all means, along with providing information about existing practices and standards.

Considering the goals of the article, have been used the logical and systemic analysis research and comparative law methods. As result of using those methods, has been created an essential representation of approaches and regulations in relation to blockchain technologies in different countries. Have been discussed private-legal problems reasoned by blockchain technology transactions

* Master of Law, Ivane Javakhishvili Tbilisi State University Faculty of Law; Founder and Managing Partner at the Legal Company “MC Law Group”.

and have been offered solutions to those problems through integration of Private Law into the blockchain technology.

2. Blockchain as the Distributed Ledger Technology (DLT). Essence, Structure and Brief Review of Its Development

Although blockchain is a new word in science, the idea of the Distributed Ledger Technologies (DLT[1]), which blockchain is based on, is not a novelty.

First research on DLT was published in 1976, in the scientific article *The Directions in Cryptography*[2], however, its realization was believed to be too complicated and unsecure for quite a long time.

At the end of the 20th century, namely in 1991, was published the first work authored by *Stewart Haber* and *Scott Sornetta*[3], describing the chain of blocks produced through cryptographically protected calculations. Main goal of *Haber* and *Sornetta* was to create such a system that would unite several documents in one block.[4] In the system, documents were hashed (transformation of input data into cryptographic data by using mathematical algorithms), for getting unified unique hash.[5]

In 2008, in social network was published the article, which was later recognized as a scientific article. As an author of the article[6] was named *Satoshi Nakamoto*. It was after the publication of the article under the nickname of *Satoshi Nakamoto* when raising awareness on blockchain and blockchain-based bitcoin (during later period on other cryptocurrencies) started.

Blockchain is a permanently growing list of records, which forms the chain of blocks through unity of predefined rules of transaction records, in which, each of such transactions may be movement of money, different goods or secure data.[7]

Blockchain is protected cryptographically, meaning that each block consists of hash-figures, which means sign, time figure and transaction data connected to the previous block.[8] It is actually impossible to change information existing in a blockchain. Any specific person does not manage database. Every user of the network has a copy of the whole database. Old blocks are saved eternally,

---

1 Distributed Ledger Technologies.

2 *Kekelia V., Kotrikadze G.,* Methods and Models of Symmetrical System of Blockchain, Book I, Tbilisi, 2016, 4 (in Georgian).

3 *Bayer D., Haber S., Stornetta W. S.,* How to TIme-Stamp a Digital Document, Journal of Cryptology, № 3, 1991, 99–111.

4 *Bayer D., Haber S., Stornetta W. S.,* Improving the Efficiency and Reliability of Digital Time-Stamping, New York, 1992, 329–334.

5 Ibid.

6 *Nakamoto S.,* Bitcoin: A Peer-to-Peer Electronic Cash System, Decentralized Business Review, October, 2008, 1-9.

7 *Kotrikadze K., Kipshidze D.,* Blockchain Technologies, as Self-Organized Systems, Tbilisi, 2019, 1 (in Georgian).

8 *Lansiti M., Lakhani K. R.,* The Truth About Blockchain, Harvard Business Review, Januar-February, 2017, 1, citation: "The technology at the heart of bitcoin and other virtual currencies, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way."

while new blocks are added to the ledger making it impossible to manipulate through forging documents, transactions and other data. Therefore, falsification of one record will result in the falsification of the whole chain.

Hence, blockchain is an independent "open ledger of transactions implemented between two parties",[9] which is completely decentralized and secure.

Blockchain is a self-organized system, featuring two parameters: first – any type of change made in any block results in cancellation of validity of following blocks. This means that change of transactions record log is in fact impossible. The system recovers its by means of systems of other members of a network, while undesired changes are cancelled automatically.[10]

Second, no less important parameter is that rules in blockchain are backed mathematically – it is not necessary to engage any central managing body in order to find out if your transaction is wrong or not at any moment of time.[11]

Structurally blockchain consists of two elements. First – hash and second – previous hash. Hash is the "fingerprint" of data or information. Hash consists of special cryptographic algorithms and is a hexadecimal number. It is possible to hash any word of sentence. Hashes can be calculated by means of any online-calculator.[12] In other words, block hash is a fingerprint, making each block unique. In order for information block to be created, along with individual hash, it is necessary to have certain data and time-stamp. It is noteworthy that along with the first hash, each new block consists of both, its own and previous block fingerprint. First block and hash are called genesis[13], consisting of probability-set algorithm, which is impossible to be calculated. Sequence of hashes forms the blockchain (chain of blocks). If we change anything inside the block, the aforementioned will result in the change of the whole hash (the change will be shown), which will cause invalidity of all following blocks. First block is the special block, as it does not have the previous valid hash, (previous block does not exist).

As I have already mentioned, each user has the complete copy of a blockchain database, while as of today, the size of the database is 200 gigabytes.[14] When a new block is created, it depends on the system user, if the new block will be approved or not. Approval needs majority of votes – 51%. Therefore, any previous hash creates the chain of blocks, ensuring that the system is secure and protected.

Blockchain is a platform on which cryptocurrencies, smart contracts, NFT[15], etc., are created. Thus, the subject of research is the need for a legal regulation of blockchain, as it is a platform for creating cryptocurrencies and circulating autonomous currencies, a means of concluding and executing

---

9 *Siraj R.,* What Is a Decentralized Application, USA, 2016, 1-2.

10 *Kotrikadze K., Kipshidze D.,* Blockchain Technologies, as Self-Organized Systems, Tbilisi, 2019, 2 (in Georgian).

11 Ibid.

12 *Nakamoto S.,* Bitcoin: A Peer-to-Peer Electronic Cash System, Decentralized Business Review, October, 2008, 2.

13 <https://www.investopedia.com/terms/g/genesis-block.asp> [04.02.2022].

14 <https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/> [26.12.2021].

15 <https://www.bbc.com/news/technology-56371912> [04.02.2022].

smart contracts, and NFT as the basis for unique digital property turnover, resulting in both property rights and the need to create and regulate other legal norms.

3. Necessity for Existence of the Blockchain Legal Regulation

Distributed Ledger Technology (DLT) is an alternative to legal regulation. DLT was created for eliminating negative sides of banking system.[16] Main goal of *Satoshi Nakamoto* was to simplify transactions by means of that system, in which transactions would be of decentralized nature and their conducting would be possible without third persons.[17]

There are several contradictory ideas about the blockchain. DLT supporters claim that autonomous cryptocurrency is the guarantee for protection of human rights from government interference.[18] This is because the DLT will make government lose monopoly on issuing money and decrease its role. *Laurence Lessig*[19] believes that – the code is law. *Lessig* is one of those scholars who put code and technology over the Law and claim that the blockchain technology does not need any regulation, as it is ideal. *Lessig's* opinion can be counted right only in endogenous part, but not in relation to the exogenous problem, which remains outside of this ideal system.

Indeed, if we follow *Laurence Lessig's* opinion, we will see how technology replaces the Law, as far as it is possible to conduct thousands of secure transactions without participation of any third persons. Transaction process is fully free from any type of regulation. Transaction is made directly by the person who wants to do it, by using his own private key. This transaction is after checked and approved by other participants of the system. For the cause it not necessary to involve a lawyer, Notary, bank or depositary. This is not implemented based on any special contract or other legal document. All this is replaced by one code. Right by this one code the Law is simplified or even replaced.

The above approach can be used directly in blockchain transactions, but not in the case of blockchain technology product NFT, which technically can be thought of as a digitally exclusive sample owned by the creator – author and acquirer – owner.[20]

However, the above mentioned does not exclude existence of legal regulation. The system may be unique and absolutely perfect from inside, but it is not protected from (external) exogenous problems. Hence, it absolutely logical and expected that in the nearest future will appear the new field of Law – *lex cryptographica*.[21]

---

16 *Nakamoto N.,* Bitcoin: A Peer-to-Peer Electronic Cash System, Decentralized Business Review, October, 2008, 1-3.

17 Ibid.

18 Comp. *Levy S.,* Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age, USA, 2001, 78-79.

19 Comp. *Lessig L.*, Code Is Law, USA, 2000, 4-6; See also, *Lessig L.*, Code: Version 2.0, USA, 2006, 1-8.

20 <https://www.bbc.com/news/technology-56371912> [04.02.2022].

21 *Wright A., De Filippi P.,* Decentralized Blockchain Technology and the Rise of Lex Cryptographia, USA, 2015, 48.

4. Private-Legal Problems Caused by DLT-Conducted Transactions

As it is often said, receiver of transaction becomes owner of a bitcoin.[22] Terms – owner, holder, property and others are also used in relation to cryptocurrency[23], as long as cryptocurrency is a legal benefit. Therefore, the DLT connection with property is clearly apparent. But, despite all that, it is still obscure to what extent cryptocurrency, including Bitcoin, is able to position itself as property.[24] This is a problematic, however often ignored issue. As I have already noted, in the nearest future, the new field of Law – *lex cryptographica* – is to become an essential, demanded and usable field of Law.

Considering that the world is divided into states and every state has its own legal system, it is logical that property rights are individually regulated in each of them at the national legislative level.[25] In the first place it is necessary to look at property law from the collusive legal angle and only after that to use it in virtual and real world.

There is an opinion that search for relevant Private Law is an anathema.[26] As far as, fully independently from the Law the DLT ensures any type of transaction in shortest period of time, with maximum guarantee of security, which cannot be guaranteed by any lawyer of legal system in general. Still, this relates to endogenous issues, not exogenous. Therefore, let us discuss problems arising during endogenous and exogenous transactions.

4.1. Endogenous and Exogenous Problems of Transaction

Endogenous problem is the one appearing inside the system,[27] or a technical problem that can appear or happen by participation of oracle[28]. For example, executor of transaction may make a mistake, type figure 1 instead of 10, or the system may shut off due to electricity failure for several minutes, and transaction may be late.

It is enough to use the correct code for successful and efficient transaction. One transaction takes exactly the time that is needed for the system to confirm relevance of the private key with the public key[29]. However, the technology is unable to consider the way of obtaining that key, which may

---

22 *Meiklejohn S.,* A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, IMC'13 – Proceedings of the 13th Conference on Internet Measurement, USA, 2013, 127. Also, see, *Tu K.,* Perfecting Bitcoin, USA, 2017, 505, 548.

23 *Abramowicz M.,* Cryptocurrency-Based Law, USA, 2016, 414; Also, *Bayern S.,* Dynamic Common Law and Technological Change: The Classification of Bitcoin, USA, 2014, 22, 29.

24 *Cutts T*., Bitcoin Ownership and its Impact on Fungibility, USA, 2015, 23; Also, *Low K., Teo E.,* Legal Risks of Owning Cryptocurrencies, Handbook of Blockchain, Digital Finance and Inclusion, USA, 2018, 47.

25 *Rose C. M*., Possession as the Origin of Property, USA, 1985, 84-85.

26 *Bayer D., Haber S., Stornetta W. S.,* Improving the Efficiency and Reliability of Digital Time-Stamping, USA, 1992, 325.

27 *De Filippi P., Mcmullen G.,* Governance of Blockchain Systems: Governance of and by Distributed Infrastructure, USA, 2018, 16.

28 This will be discussed in following chapters.

29 <https://www.gemini.com/cryptopedia/public-private-keys-cryptography#section-what-is-public-key cryptography> [04.02.2022].

not be legal and may be connected to scam and etc. This is not the task of algorithms or technology; therefore, it is one of exogenous problems.

Exogenous problem is the one not resulting from the blockchain platform. Its source comes externally, but affects those persons who own the cryptocurrency.[30]

Among exogenous problems is obtaining a private key through scam, distortion of facts, falsification, deception and other means.[31] All these ways of executing transaction are illegal by means of Law, but it is acceptable for the blockchain technology. Therefore, the contract (i.e. transaction) is not considered effective legally, when it is about such circumstances. For example, person X illegally obtained a private key from another person's computer and illegally transferred bitcoin to his account. The way of obtaining the key is legally unacceptable, although, the efficiency/executability of transaction is present.

Situation is the same when it is about Inheritance Law and Institute of Succession. In all the legal systems, property of a deceased goes to successors.[32] This is done automatically. It is possible for such handover to consider in case of giving cryptocurrency that a deceased owned,[33] as far as it is the legal benefit.

Another type of exogenous problem is bankruptcy. Often, bankruptcy manager is in the role of debtor and manages all assents in order to satisfy creditors.[34] This also considers virtual assets, such as Bitcoin too, as it can be certain part of debtor's property. Despite any kind of description, it is apparent that crypto-assets are ordinary property, which must be protected just as any other property or property right.

After a fact of death takes place, according to the Inheritance Law, property of deceased is handed over to successor. This considers any property of a deceased, including cryptocurrency. This is executed not depending on whether or not a successor is aware of the private key, crypto-assets still go into his property, which means that technically successor may not be owning/holding a private key, but based on Law successor becomes legal owner of such crypto-assets.

The Law is unable to put blockchain into restraints is the hypothetic inheritance. Let us imagine that person X passed away, left the Will with his private key, which is kept in his office work computer. X's co-worker has access to that computer. According to Inheritance Law, all the assets go to X's successor.[35] Including the private key kept in X's office computer. However, X's co-worker, having access to that computer, is able to make blockchain transactions by using this private key,

---

30 *De Filippi P., McMullen G*, Governance of Blockchain Systems: Governance of and by Distributed Infrastructure, USA, 2018, 44.

31 *Miranda C.,* How to Avoid a Bitcoin Blackmail Scam, USA, 2018, 8.

32 *De Waal M. J.,* Law of Succession, in Introduction to the Law of South Africa, USA 2004, 169; Also, *Dyson H.,* French Property and Inheritance Law: Principles and Practice, USA, 2003, 313.

33 *Anitei A. C.,* Digital Inheritance: Problems, Cases and Solutions, International Conference Education and Creativity for a Knowledge-Based Society, 2017, 32; Also, see, *Cahn N.,* Probate Law Meets the Digital Age, USA, 2014, 67.

34 *Campbell B. H.,* A Treatise on the Law and Practice of Bankruptcy: The Act of Congress of 1998 and Its Amendments, 3rd ed., Kansas City, 1922, 4.

35 *McGovern Jr. W., Kurtz S., English D. M.,* Wills, Trusts and Estates, Including Taxation and Future Interests, USA, 2010, 57.

which means that he obtains factual ownership of Bitcoin. Neither the legal successor nor the Will Executor will be able to manage the deceased's crypto-assets if they will not have the private key. Blockchain cannot be responsible for that or control the process, as the blockchain records neither deaths nor other factors, which stay outside of its algorithm functioning.

In order for this system to be perfect, it is in the first place necessary to globally recognize cryptocurrency as property, object of right to property and second – a mechanism must be developed that will restrict unauthorized holder to execute new transactions, i.e. to use private key. Therefore, not depending on what kind of problem we are dealing with, be it endogenous or exogenous, it in the first place considers property of a person and any kind of violations must be regulated based on the Law.

5. Legal Problems of Relevance with Legislation

It is enough to adapt the DLT to Private Law in order to solve all the above discussed problems. At first glance, this means that all transactions will be checked according to local national legislation, which will in return increase the gap between technologies and the Law.

5.1. Blockchain Autonomy VS. National Legislation

First complication existing between the DLT and the Law is the autonomy of DLT, as it always functions independently from any law and the legal system in general. Aside from that, there is the threat of legal restraint of the blockchain and putting it into some frames. For illustrating the aforementioned let us analyze the following case: a person, who illegally obtained another person's private key, made transaction and created another, new private key produced from that key.[36] Legally, such transaction must be annulled, as the property was taken away from the true owner of the Bitcoin without their awareness, through misappropriating their private key. But, when a private key is used and transaction is confirmed, technically a new key is created, the owner of which becomes another – third person. This third persons now appears as a new, honest owner, who has the right to use the key as desired.[37] This can legally be compared to an honest purchaser, who did and could not know about the true case.

It is technically impossible to interfere with the actions of a person illegally misappropriating a private key, as every new transaction creates a new private key, which is available to those persons who received the aforementioned transactions and it is also impossible to find that key too, as it can be located in any part of the world. This private key is able to create a new private key and this exceeds the legal process and becomes of irreversible character.

DLT – is a perfect mechanism, which has digital image and is seen on screen. Very beneficial and efficient is transferring crypto-assets through blockchain, when it happens by using private and public keys, although, there still is the risk of hacker misappropriation, as result of which an

---

[36] *Garrison J.,* 2 Men Arrested in Elaborate Plot to Steal $550K in Cryptocurrency by Hacking Social Media Accounts, USA Today, 2019, <https://www.usatoday.com/story/news/nation/2019/11/15/massachusetts-men-arrested-plot-steal-cryptocurrency-bitcoin-social-media-threats/4201763002/> [24.12.2021].

[37] *Agrawal H.,* How Long Does It Take to Transfer Bitcoins and Why?, Coinsutra, 2019, <https://coinsutra.com/bitcoin-transfer-time/> [25.12.2021].

unauthorized person gains the right to manage Bitcoin, while the person having real right to those assets faces loss. In order for the DLT to become fully compatible with the Law, it must be substantively studied and even changed, as the result cannot be achieved superficially.

5.2. Irreversibility of Transactions as the Characteristic Feature of the Blockchain

Opposition of the Law and technologies can be avoided if we suspend the distribution of the illegally obtained block. For example, at the time of illegal obtaining of a private key, the case must not be based on claiming that it is a property "of that one" and requesting it back from an illegal owner, but on recognizing the produced chain as illegal and annulling it, meaning recreating the initial situation.

Same mechanism must be used if an unauthorized person takes over bitcoin; for example: not a successor after decease of property owner. It seems that the blockchain itself must be changed for the cause, not to lose justice in such a context. However, this cannot be achieved as a bitcoin, as already programmed and systemically launched mechanism is impossible to be changed to transformed.[38] As I have noted several times, blockchain-bitcoin technology is programmed the way that the information already reflected in the chain (of an executed transaction) cannot be erased or changed. This is the result of its irreversible nature. Hence, any transaction is added to the DLT and passed over to next block owner in a unified way. The basis for the guarantee of the blockchain itself is right its unchangeability and irreversibility.

Still, it is possible to modify or reorganize any system, but the question is how justified it is to make such modification. Quite often, such actions bring more losses than benefits. Let us recall the years 2013 and 2016. In 2013 Bitcoin reorganization[39] took place, which considered adding of smart-contacts and in 2016, forceful reorganization of Ethereum was done, reasoned by large volume of crypto-assets misappropriated by hackers, pointing to weakness of the program.[40] In both cases, new version of blockchain was developed. Reorganization did not cause such serious loss in case of Bitcoin as in case of Ethereum. Ethereum was divided into two generations: Ethereum (One) and Ethereum Classic. Hacked ledger in fact "passed away" and all those faced losses who had purchased the first generation of Ethereum.[41]

This means, any reorganization, modification, be it forceful or voluntary, has negative impact on public confidence, while the value of cryptocurrencies directly depends on public trust and demand.

5.3. Legislative Alternative in the Context of Legal Collision

As it said, Private Law has as many expressions as there are number of different countries. In order to give legal evaluation to symbiotic coexistence of technologies and the Law and functioning of

---

38 *Wright A., De Filippi P.,* Decentralized Blockchain Technology and the Rise of Lex Cryptographia, USA, 2015, 37.

39 *Buterin V.,* Bitcoin Network Shaken by Blockchain Fork, USA, 2013, 7.

40 *Gomez E.,* The Ethereum Hard Fork & Ethereum Classic, USA 2016, 11.

41 *Low L., Teo E.,* Legal Risks of Owning Cryptocurrencies, USA, 2018, 19.

blockchain system it needs to be identified if any country's legislation regulates the aforementioned and if yes, which country it is and how they do it. This falls under the authority of the Private International Law regulation sphere.[42] Collision Law is based on affiliation of facts and relations to the country's law, which the tightest contacts are identified with.[43] Such methodology is a great challenge to the DLT. Blockchain is a global and transnational mechanism not affiliated with any country. Blockchain transactions are made by using private and public keys, without identification of location of parties. In order to use the Private International Law, it is necessary to define location of contract parties or to specify location of action, while this is inadmissible in blockchain, as it is against the general principles of the blockchain technology. Information reflected in blockchain is kept in different computers worldwide. Any person can take part in such permissionless system, as Bitcoin. Approval of transaction is done by confirmation from all the participants throughout the world. Therefore, it would be right to say that the permissionless system is fully decentralized and it not tied to any country. Another challenge that complicates solution of aforementioned problem is the non-uniform approach to blockchain-bitcoin.

It is quite difficult, but still possible to connect the blockchain and the Law, as far as any transaction is made by two parties.[44] Furthermore when it is possible to classify cryptocurrency as property, as it has value. Therefore, it is the case to be discussed by property right and the law.

Contractual qualification – takes us to autonomy of parties in which parties will be able to agree on anything.[45] Based on that, parties will have the right to use the Law, which mostly complies with transaction made by them. In such cases, DLT regulation is defined in each specific case, by individual legislation; but, the aforementioned may be incompatible with the blockchain technology itself. This is because other participants will not know about the Law that the parties have chosen, while the validity of transaction depends on the confirmation from those participants. This means that this is technically impossible to do. Thus, it would be advisable to create one unified law or new field/direction of law, which would regulate the DLT and relations and actions connected to it. Meanwhile, the latter contradicts with the Bitcoin ideology. Usage of one law is admissible only for permissioned systems, which are managed by one of several persons, but fully contradicts with the permissionless system, which is accessible and functional worldwide, without any type of supervision. Anonymity principle, which the blockchain technology stands on will be breached, if it will be publicized which countries a transaction is made between in order to define relevant law. The latter is necessary for the Private International Law as it is based on the territoriality principle.

If we look at cryptocurrency and transactions as property and their owners and those with the right for property, then we will get *Lex Rei Sitae*, when an object of property is defined and it an item. Information on blockchain and cryptocurrency based on it is not material item, which exists only as records in ledger, without possibility to detect location. Bitcoin does not have any factual address and geographical home; although, it is also possible to change the *Lex Rei Sitae Rule*. For example, many

---

42 *Fawcett J., Carruthers K., Cheshire N. F.,* Private International Law, USA, 2008, 19.

43 *Fawcett J. C., Cheshire N. F.*, Private International Law, USA, 2008, 85.

44 *Wright A., De Filippi P.,* Decentralized Blockchain Technology and the Rise of Lex Cryptographia, USA, 2015, 184.

45 *Weintraub J.,* Functional Developments in Choice of Law for Contracts, Germany, 1984, 239, 271.

countries use PRIMA rule in relation to intangible securities, which indicates usage of legislation of the country, in which an intermediary is.[46] The aforementioned would be possible to be used if there was an intermediary party in a transaction, but the permissionless system involves only two parties and there is no intermediary institute. Therefore, the PRIMA rule is absolutely incompatible with the blockchain. DLT is possible to be used for transferring property assets, be it immovable or movable property – by means of tokenization. These assets require individual approach.

Eventually, none of the collision law regulated cases are relevant to DLT. This problem needs comprehensive and in-depth study and development of new approaches, which will bring technologies and the Law closer together. One of the solutions is modernization of property law or recognition of Bitcoin as property worldwide. Still, in both cases, it is necessary to thing and understand globally, for one not to contradict with the principles of another.

6. Private Law Integration with the DLT

6.1. Coexistence of Technology and the Law – Search from Compromises

When speaking about the coexistence of the blockchain and of the Private Law, three aspects discussed in previous chapters must by all means be considered: DLT autonomy, irreversibility of transactions and blockchain independence from any country – or its decentralized nature. It is necessary to create such a mechanism that will define the number and quality of transaction, but that will not be controlled by national legislation of any country. The new Law must be acceptable to all the countries and must not contradict with the international legislations of states. The given offer satisfied all the above discussed criteria, although, it may be criticized both by lawyers and technologies. In order to avoid such criticism, let us discuss where this offer comes from and what its advantages are.

It must be said in the first place that blockchain is an innovation related to the future that will be useful and beneficial for both a country and people. If we presume that there will be no scam and illegal actions in the blockchain functioning, it is a fact that as a technology, it will function ideally even without laws.[47] If lawyers will attempt to make changes to its functioning, it will be damaged as a mechanism. Even selection of regulating law may have negative impact, as the aforementioned contradicts with DLT autonomy and anonymity principles, along with the decentralized character of the blockchain.

It is noteworthy that the law must not interfere with the blockchain functioning. After the development of the law, the technology must continue functioning as usual; conduct transactions the same way, by protecting autonomy and anonymity and by using private and public keys. The main power of a private key owner is that he has the latter. The law and legal system should not take this power away in general from the legal owner. Every new transaction creates new private key and this

---

[46] Hague Convention on the Law Applicable to Certain Rights in Respect of Securities Held with an Intermediary Art, 05/06/2006.

[47] Please see Bitcoin circulation statistics, <https://www.statista.com/statistics/730806/daily-number-of-bitcoin-transactions/> [26.12.2021].

process is irreversible. The Law is unable to stop the process that is called irreversibility of creation of new keys[48] and should not even have claims for it. Irreversibility of transactions is the fact that needs to be recognized and accepted by the legal society. Otherwise, the desired result will not be achieved. This case looks like the following: for example, a person who knows a card pin-code is withdrawing cash from an ATM, but he does not have a permission to withdraw the money. ATM thinks that an authorized person is withdrawing cash, as there is a correct pin-code entered – as result money is given. Let us discuss a second case – the case of honest owner (purchaser). If a thief is selling an item, this item becomes property of an honest purchaser and previous owner cannot claim it back. The situation is the same here – the right to get back this key exists until the latter executes a new transaction.[49]

The Law must not fully control the blockchain; it must regulate the part that relates to the illegal misappropriation of the key.

6.2. Modification of Transaction Irreversibility

Blockchain transactions are almost irreversible – which means they are final.[50] Although it is impossible to erase or annul an already created block, the Law is able to change the value of sequence. For example, although it is impossible to erase already existing, it is possible to get back that transaction. Such an obligation may be imposed on a party, when the second one did not execute its share of obligation, i.e. recreation of initial situation. Although, from technical viewpoint, the initial situation cannot be recreated, as a transactor does not return the old key, but is forced to create the new one, receiver of which will be the old owner. Such a solution can be offered to parties by a defined law or a new field of law. However, there is one circumstance – execution of transaction depends on the will of receiver. He must use his own private key to give back cryptocurrency, while there is no guarantee that he will do so.[51] Although, it is possible to conduct forcing action, recognized by the Law. Such a forcing action may be court verdict, sanction or anther document having legal force.[52] Of course, these legal means are not as efficient as erasing transaction technically, but in this case, there is no other way of using.

Therefore, transaction concept must be transformed the way to adapt to property law, based on liabilities. In this case, it will not be needed to change the Law or legal system itself. Analysis of transactions in relation to property right has several positive aspects. For example: after identification of aforementioned it will not be necessary to check validity of all transactions. DLT works without failures, while the Law regulates external violators as result of which we will get an ideal mechanism.

---

48 *De Filippi P., Wright A.,* Blockchain and the Law, Harvard University Press, USA, 2018, 24.

49 Miller v. Race, [1758], 1Ch 1151-1155.

50 *Nakamoto S.,* Bitcoin: A Peer-to-Peer Electronic Cash System, Decentralized Business Review, October, 2008, 1, 8.

51 *Raskin M. I.,* Realm of the Coin: Bitcoin and Civil Procedure, Fordham Journal of Corporate & Financial Law, Vol. 20, Issue 4, 2015, 969, 975.

52 Ibid.

Still, this cannot be regulated just by the Private Law, as scam for instance is not subject of study of Private Law.

Bitcoin transaction is not a contract, but this action is an implementation of an abstract contract. The aforementioned looks like a Purchase and Sale Agreement. Similar to the international Private Law, here it is also possible to use location of parties or execution location for determining the applicable law. Alternatively, based on – *lex loci delicti*, which is recognized by majority of States in their legislation.

7. Conclusion

Joshua Fairfield claims that it is necessary to bring technology and Law closer together, in order to not only achieve efficient functioning of the system, but also to maximally protect user rights, which will, in return, result in the formation of new direction in Law.[53] To solidify this point of view, according to other scholars, in relevant fields of Law must until now have been introduced such notions as: "Bitcoin – new type of property"[54], "crypto-robbery", "crypto-scam" and etc.[55] Following in the footsteps of modern trends, the irreversible process of convergence of technology and law is remarkable. For the legal interest and protection of any user using the block chain system, its legal regulation is inevitable. Based on the analysis presented in the paper, it can be said that the protection of the person using the block chain system is carried out in the same way as in the case of traditional property ownership. This creates the need to understand cryptocurrency as an object of law, to present it as property, and as an object of property rights. It is true that Bitcoin does not have an actual address or geographical location, but based on the reasoning and examples discussed in the study, it can be concluded that cryptocurrency is a protected legal good. In addition, the information on the block chain and the cryptocurrency based on it is immaterialized, which exists only in the form of records in the registry. Thus, the increasing development of technology shows that the field of private law protection is not limited to traditional property; it goes beyond the boundaries of this tradition.

Although the blockchain is of autonomous nature, DLT still needs legal regulation. Therefore, if we wish to achieve a unified and completely secure and protected mechanism, symbiotic coexistence of technologies and the Law is necessary. Both sides must make compromise for the cause, as result of which will be created a new direction of law – *lex cryptographica* – which will discuss all the aforementioned problematic issues and not only those.

Bibliography:

1. Hague Convention on the Law Applicable to Certain Rights in Respect of Securities Held with an Intermediary Art, 05/06/2006.
2. *Abramowicz M.,* Cryptocurrency-Based Law, USA, 2016, 414.

53 *Bayern S.,* Dynamic Common Law and Technological Change: The Classification of Bitcoin, USA, 2014, 29.
54 Ibid.
55 *Zaytoun H.,* Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft, USA, 2019, 395, 401.

3. *Anitei A. C.,* Digital Inheritance: Problems, Cases and Solutions, International Conference Education and Creativity for a Knowledge-Based Society, 2017, 32.
4. *Agrawal H.,* How Long Does It Take to Transfer Bitcoins and Why?, Coinsutra, 2019, <https://coinsutra.com/bitcoin-transfer-time/> [25.12.2021].
5. *Bayer D., Haber S., Stornetta W. S.,* How to time-stamp a digital document, Journal of Cryptology, № 3, 1991, 99–111.
6. *Bayer D., Haber S., Stornetta W. S.,* Improving the Efficiency and Reliability of Digital Time-Stamping, 1992, 325, 329–334.
7. *Bayern S.,* Dynamic Common Law and Technological Change: The Classification of Bitcoin, USA, 2014, 22, 29.
8. *Buterin V.,* Bitcoin Network Shaken by Blockchain Fork, USA, 2013, 7.
9. *Cahn N.,* Probate Law Meets the Digital Age, USA, 2014, 67.
10. *Campbell B. H.,* A Treatise on the Law and Practice of Bankruptcy: The Act of Congress of 1998 and its Amendments, 3rd ed., Kansas City 1922, 4.
11. *Rose C. M*., Possession as the Origin of Property, USA, 1985, 84-85.
12. *Cutts T*., Bitcoin Ownership and Its Impact on Fungibility, USA, 2015, 23.
13. *De Filippi P., Mcmullen G.,* Governance of Blockchain Systems: Governance of and by Distributed Infrastructure, USA, 2018, 16, 24, 44.
14. *De Waal M. J.,* Law of Succession, in Introduction to the Law of South Africa, 2004, 169.
15. *Dyson H.,* French Property and Inheritance Law: Principles and Practice, USA, 2003, 313.
16. *Fawcett J. C., Cheshire N. F*., Private International Law, USA, 2008, 85.
17. *Garrison J.,* 2 Men Arrested in Elaborate Plot to Steal $550K in Cryptocurrency by Hacking Social Media Accounts, USA Today, 2019, <https://www.usatoday.com/story/news/nation/2019/11/15/massachusetts-men-arrested-plot-steal-cryptocurrency-bitcoin-social-media-threats/4201763002/> [24.12.2021].
18. *Gomez E.,* The Ethereum Hard Fork & Ethereum Classic, USA 2016, 11.
19. *Kekelia V., Kotrikadze G.,* Methods and Models of Symmetrical System of Blockchain, Book I, Tbilisi, 2016, 4 (in Georgian).
20. *Kotrikadze K., Kipshidze D.,* Blockchain Technologies, as Self-Organized Systems, Tbilisi, 2019, 1-2 (in Georgian).
21. *Low K., Teo E.,* Legal Risks of Owning Cryptocurrencies, Handbook of Blockchain, Digital Finance and Inclusion, USA, 2018, 47.
22. *Lansiti M., Lakhani K. R.,* The Truth About Blockchain, Harvard Business Review, Januar-February, 2017, 1.
23. *Lessig L*., Code is Law, USA, 2000, 4-6.
24. *Lessig L*., Code: Version 2.0, USA, 2006, 1-8.
25. *Levy S.,* Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age, USA, 2001, 78-79.
26. *Mcgovern Jr. W., Kurtz S., Eenglish D. M.,* Wills, Trusts and Estates, Including Taxation and Future Interests, USA, 2010, 57.
27. *Meiklejohn S.,* A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, IMC'13 – Proceedings of the 13th Conference on Internet Measurement, USA, 2013, 127.
28. *Miranda C.,* How to Avoid a Bitcoin Blackmail Scam, USA, 2018, 8.

29. *Nakamoto N.,* Bitcoin: A Peer-to-Peer Electronic Cash System, Decentralized Business Review, October, 2008, 1-3, 8.
30. *Siraj R.,* What Is a Decentralized Application, USA, 2016, 1-2.
31. *Tu K.,* Perfecting Bitcoin, USA, 2017, 505, 548.
32. *Raskin M. I,* Realm of the Coin: Bitcoin and Civil Procedure, Fordham Journal of Corporate & Financial Law, Vol. 20, Issue 4, 2015, 969, 975.
33. *Weintraub J.,* Functional Developments in Choice of Law for Contracts, Germany, 1984, 239, 271.
34. *Wright A., De Filippi P.,* Decentralized Blockchain Technology and the Rise of Lex Cryptographia, USA, 2015, 37, 45, 48.
35. *Zaytoun H.,* Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft, USA, 2019, 395, 401.
36. Case of Miller v. Race, England, 1758.
37. *HashFast Technologies LLC v. Lowe,* (2016), 307 US 25.
38. <www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/> [26.12.2021].
39. <https://www.investopedia.com/terms/g/genesis-block.asp> [04.02.2022].
40. <https://www.bbc.com/news/technology-56371912> [04.02.2022].
41. <https://www.gemini.com/cryptopedia/public-private-keys-cryptography#section-what-is-public-key-cryptography> [04.02.2022].
42. <https://www.statista.com/statistics/730806/daily-number-of-bitcoin-transactions/> [26.12.2021].