Vilnius University

The Faculty of Law

The Department of Private Law

Valentyna Kondratenko,
A second year student
LL.M programme

Master Thesis

EMERGING LEGAL ASPECTS OF THE BLOCKCHAIN APPICATION IN THE PUBLIC SECTOR: EXPERIENCE OF THE UKRAINIAN DECENTRALIZED ONLINE AUCTION SYSTEM

Advisor: Dr. S. Drazdauskas
Reviewer: Dr. P.Miliauskas

Vilnius 2017

TABLE OF CONTENT

INTRODUCTION

Information technology has already had a huge impact on many dimensions of our lives, such as communication, socio-economic relationships, information and its delivery, order and control etc. The Internet has had enormous implications for electronic trading, collection of borderless networks, and newly distributed infrastructure. These developments raised countless substantive legal issues at the intersection of law and technology. However, the new evolving technological advances are moving quickly, while the law and legal services are slow. Lawyers should properly address the meaning of such innovations within existing relationships; particularly, they should be proficient and capable of counseling their clients not only utilize technology properly, but also assess related risks.

The recently developed technology is called blockchain, which brings tremendous opportunities and unique challenges for many spheres of our life including transfer of value, trade, communication, politics and law. The innovative technology attracts researchers from various fields to understand its disruptive potential. Primarily applied as a solution underpinning cryptocurrency and payment systems, the blockchain technology is not limited to simple electronic transfers of value.

The motive of my research is to understand why the blockchain technology is so revolutionary. The innovation of blockchain combines knowledge of computer science, mathematics, cryptography, and ideas of decentralization. Together, these advances could potentially shape people's affairs within the private and public sectors. Scientists predict that smart contracts may take an important place in the existing contract world. In the digital age, smart contracts propose sophisticated solutions for the enforcement of contractual rights and obligations. As such, the blockchain technology raises a number of questions for its adopters, as well as for the lawmakers. Lawyers are seeking to find out the place of smart contracts in specific contractual relationships.

Current research on blockchain technology is still lacking due to its novelty; a significant amount of research is focused on cryptocurrencies. The blockchain technology started to attract researchers' attention about three years ago. Law scholars focus on the innovative features of blockchain, coupled with smart contracts ideas; additionally, there are issues concerning ownership titles and their transfers, as well as other aspects of digital dimension relationships. The business sector, professional service providers, and governments have all taken interest in blockchain, especially financial institutions as they are looking for relevant solutions for payment systems.

In my paper I will focus on blockchain technology and its application, particularly the smart contracts concept. Within the scope of my topic, I will discuss the blockchain-based eAuction system run by public authorities and its potential benefits.

My research aims to perform the following:

- Introduce the blockchain technology and its potential applications;
- Consider the importance of decentralization, and the category of "trust" over digital dimension;
- Clarify the vision on blockchain-based smart contracts and its benefits;
- Discover how the concept of smart contracts can be embedded into existing systems, as well as facilitate efficiency, automation, accountability etc;
- Highlight the example of blockchain technology application to electronic decentralized auctions run by the Ukrainian government and how it can be implemented within the current system;
- Figure out the importance of further research in the area of blockchain solutions from a legal perspective.

For the purpose of my research, I apply logical analyses (e.g. description of the main elements of blockchains to show the entire innovation of the technology), synthesis method (e.g. examination of the combination of the attributes of blockchain tied with smart contracts), genetic method (e.g. outlining how technology can shift the paradigm in humans affairs and redefine trust in the digital environment), comparative method (e.g. comparison the enforcement of contracts to the mechanism of enforcement of smart contracts), method of systematic analyses (e.g. overview the applications of blockchain technology which may reshape various services and how smart contract have potential to enhance traditional contract law) and others. Moreover, I received information on present projects, particularly decentralized eAuction, from brief interviews with experts in that field. I chose the mentioned methods above because they provide a comprehensive approach that allows one to discover the full potential of the blockchain technology.

In the first part of my paper, I will provide some overview from the technical standpoint, which is necessary to understand the full range of potential that blockchain technology has across various industries. I will also touch the concept of cryptocurrency, particularly Bitcoin, since it was the first evolved application of the blockchain. Technical features facilitated by the blochchain technology offer a huge range of potential applications beyond Bitcoin. One of the most obvious advantages of blockchains is the concept of smart contracts.

I will dedicate the second part of the paper to exploring the idea of smart contracts. The central issues for lawyers are the mechanism of automated enforcement, the possibility to turn contract provisions into software code, and the tools that enable the writing of smart contracts. Smart contracts are also associated

with the concept of smart property, which may make sense of digitally automated transactions. There are also extended concepts of smart contracts which aim to govern so-called “digital organizations”, however we will leave the latest matters aside the scope of our paper since it raises a more complex discussion. The problem lies in incomplete understanding of the possibilities of transactions executed on blockchain.

Smart contracts run on blockchain can potentially be applied in many commercial spheres. The mentioned technologies are promising to include important benefits such as transparency and accountability for various transactions in private and public sectors. Within the scope of my work, I will consider how the blockchain innovations can be applied to the system of state and municipal property privatization and lease. In Ukraine, this process is conducted through an inefficient and obscure auction systems. I will explain how mathematical certainty can solve existing problems and establish transparency of the process.

In the conclusions and recommendations section, I will summarize the current notable aspects within blockchain technology applications regarding the legal realm. I will also provide light to issues that blockchain may potentially answer, particularly within the public sector (i.e. lack of transparency, centralization).

1. INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

In the last decades, there were many advances in different field of cryptography science, decentralized computer networks. The results of innovations have its significant impact on information society as well as on economic interaction between people. The Internet apparently opened new horizons for people's communication. The other next great thing which summarizes significant advances in the mentioned fields is technology known as blockchain.

It is important to examine the technical theories and concepts that gave rise to Blockchain and distributed ledger technologies, particularly Bitcoin. There is perhaps some ambiguity in the terminology between "blockchain technology" and "distributed ledger technology" (further – DLTs, ledger). "Further, the blockchain is just one of a variety of similar technologies often referred to as decentralized public ledgers or trustless public ledgers.", - Fairfield stresses in his research [24]. From the deep technological standpoint, the separation of these terms may make sense, however, for the purposes of the paper I will use both terms interchangeably.

The following subsections are aiming to introduce the main characteristics of the concept of the blockchain technology and explain why it is so revolutionary. The discussion frequently will be referred to Bitcoin cryptocurrency as the most well known application of blockchain technology to explain how blockchain works and why it is so revolutionary. Also we will consider its major attributes which supposes to bring a lot of potential benefits across industries, and how it can change traditional approaches in a wide range of contexts.

1.1 Blockchain background in the context of bitcoin invention

Recent developments of the Internet services and improvement of technical innovations made possible on-line economy (on a distance via electronic means). It seems necessary to start with novelties that were provided by the Bitcoin invention. Thus, an intriguing appearance of cryptocurrency called Bitcoin forced to focus many researcher from various fields to discover its peculiarities. The nature of Bitcoin combines itself unique features which were discovered before, however, only combined together its composition resolves many issues between its users. Swan highlights the importance of such revolution on the Internet "alternative currency called Bitcoin that was issued and backed not by a central authority, but by automated consensus among networked users." [10]. This subdivision is aiming to clarify the roots of Bitcoin and why it opens new horizons not only for cryptographic currencies. Despite this, it is not just about technological mechanisms. It is about how the technology, which is supported with concepts on alternative economic models, changes the paradigm in the society.

The technological concepts underpinning the appearance of Bitcoin as first cryptographic currency actually are not so new. Cryptography, computer science, the Internet were developed several decades ago. Also the idea of privatization of money is not so new. Separately, these concepts existed for a long time, however, combined together they can bring unique opportunities across industries in sense of shifting the paradigm from centralized architecture to decentralization. Not to mention, storage technologies are getting dramatically cheaper nowadays.

Recordkeeping is a crucial element within human socio-economical relationships. Ledgers existed in a system of books, producing social effects that exceeded transcription and calculation. Taken together, these books established a mode of government. The simple mathematics used in the ledger transformed abstract representations into usable facts for governance [29, p. 9-10]. Davidson et Al. in their research [25] state that ledgers since inventing of double entry bookkeeping in the 15th century were not dramatically changed till digitizing in the 20th century. However, during all these time ledgers were centralized. The ledger is a technology of accounting, of keeping track of who owns what, and is instrumental to modern capitalism."But so too is trust in the ledger, which is most effective when it is centralized and strong, and so centralized ledgers for property titling, contracts, money etc., are also critical in connecting government to modern capitalism." [25, p.3].

Nowadays information technologies make possible distributed economy. "Replacing very expensive centralized ledgers with decentralized distributive ledgers captures huge cost savings and efficiencies." [25, p.3]. Decentralized distributive ledgers ride three exponentially declining cost curves:

1. Moore's Law: the cost of processing digital information (speed), halves every 18 months;[1]
2. Kryder's Law: the cost of storing digital information (memory) halves every 12 months;[2]
3. Nielson's Law: the cost of shipping digital information (bandwidth) halves every 24 months.[3]

Peer-to-peer networks have also been used since late 1970s, and gained mainstream acceptance in the early 2000s.[4].Transactions within such networks take place directly between users, without intermediaries (e.g. similar to BitTorrent which is used for file sharing). As outlined at [8, p.29], blockchain technology (akin Web protocol) needs the Internet, so that it cannot exist without the Internet. The

[1] MOORE, G. E. *Cramming More Components onto Integrated Circuits*. Proceedings of the IEEE, Vol. 86, No.1, January 1998), available at: <http://www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf.>

[2] KRYDER, K. *Kryder's Law*. Scientific American (August 2005) available (as a reprint) at: <https://web.archive.org/web/20060329004626>

[3] NIELSON, J, *Nielson's Law of Internet Bandwidth*, Nielson Normal Group, available at: <https://www.nngroup.com/articles/law-of-bandwidth>]

[4] ORAM, A. *Peer-to-peer: harnessing the benefits of a disruptive technology* (2001) (providing a history of peer-to-peer applications online and noting that Usenet, introduced in 1979, was the "grandfather of today's peer-topeer networks.").

blockchain may be built directly on the Internet protocol (by omitting Web), or it could be mixed with web-applications.

Efforts to launch digital currencies began in the 1980s. Antonopoulos explains that before Bitcoin there were attempts to issue digital currencies by using cryptography. However, they could not solve the core issues such as trust, 'double-spend' problem, and centralization. In contrast with earlier findings, "Bitcoin is such a system, completely decentralized by design, and free of any central authority or point of control that can be attacked or corrupted." [4, p.3].

Describing the reasons of fails of digital money inventions of that period Tapscott points on the Internet's problems of privacy, security, and inclusion with cryptography. But the main issue was with inability to avoid third party involvement. The technical facilities were too expensive that time that transactions on the Internet were unreasonably expensive and really not secure. Then in the middle of nineties there was David Chaum's eCash digital payment system which "a technically perfect product which made it possible to safely and anonymously pay over the Internet. It was perfectly suited to sending electronic pennies, nickels, and dimes over the Internet." [11, p.20]. But it also had insufficient level of privacy and security. There was also published a theoretical paper "The God Protocol" by Nick Szabo [65]. The core of this technology protocol is that 'God' is trusted third party between transactions. "All the parties would send their inputs to God. God would reliably determine the results and return the outputs. God being the ultimate in confessional discretion, no party would learn anything more about the other parties' inputs than they could learn from their own inputs and the output." [65]. At that time the only possible way to securely arrange transactions between not trusted parties is to use numerous intermediaries services, especially in the Internet.

The idea of cryptocurrency is believed to originate from Wei Dai, who published a description of `B-money' in 1998 [58]. B-money is described as an anonymous distributed electronic cash system and was thought of as a conceptual idea, rather than practical. Buterin argues that the relying on trusted computing party also led to fail of the next generation of ideas on creating cryptocurrency through computational puzzles and decentralized consensus [51]. Another theoretical concept of digital currency called Bit-Gold [64] was presented by Nick Szabo in 2005, which was commonly view as a precursor to Bitcoin, relied on cryptographic solutions, however it was not successful. Thus, there is a lot to learn from the efforts to launch digital currency or cryptocurrency, so that complex of technical innovations can be extensively applied even beyond the main aim.

Considering the history of cryptographic payment systems, both e-cash and credit card based technologies, Jeremy Clark claims that the most notable is PayPal, but it survived "only because it quickly

pivoted away from its original idea of cryptographic payments on hand-held devices". [9]. However, it is still fiat money (issued and backed by government) since its value is based on currency.

Another key thing to figure out the point of mentioned ideas, that debates on money as means for payment and money issuers are pretty old. In his research Hayek argues on a new type of economy. He claims that money is a legal fiction to satisfy formalized relationships within state [6, p.57]. Moreover, in 1991 it was discussed by scholars that full privatisation of currency requires that government currency be fully replaced by privately issued bank notes and token coins [46, pp. 86–87].

"…although we usually assume there is a sharp line of distinction between what is money and what is not-and the law generally tries to make such a distinction- so far as the causal effects of monetary events are concerned, there is no such clear difference. What we find is rather a continuum in which objects of various degrees of liquidity, or with values which can fluctuate independently of each other, shade into each other in the degree to which they function as money"

-F.A Hayek [6]

Described ideas on alternative money did not take hold successfully until in 2008, a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" [59] appearanced on the Internet by Satoshi Nakamoto who is thought to be a pseudonym used by either a single person or a group of people; it is still unknown who invented Bitcoin. However, by combining the knowledge studied from previous online payment systems Nakamoto created essentially novel "decentralized electronic cash system that does not rely on a central authority for currency issuance or settlement and validation of transactions" [4, p.3]. Bitcoin is the world's first decentralized digital currency. "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution." [59, p.1]. So within the system described by Nakamoto we can avoid issues which were not solved by decades of research in certain fields.

For users it does not really matter who launched the system. The software and the network could be developed without the creator. Since the source code is available in the Internet (i.e. open source), many programmers inspected the system which operates based on "fully transparent mathematical principles." It ensures security and resilience. Antonopoulos calls the invention "groundbreaking" so that it got its further research in the fields of distributed computing, economics, econometrics [4, p4]. The principal difference is decentralized nature of Bitcoin, therefore its issuance is controlled by protocols run by set of nodes (currently around 7000 computers ensure the system).

Swan [10] helps us to distinguish ambiguous meaning of Bitcoin. She points out three levels of Bitcoin understanding. Thus, the first dimension of it is Bitcoin cryptocurrency as internal token. Secondly,

it is Bitcoin protocol as software which allows transfer assets. Thirdly, it is Blockchain bitcoin as a ledger to store every transaction. Swan argues that this structure is similarly applicable to any modern cryptocurrency [10, p.1-2]. So far there are already exists hundreds of distinct from Bitcoin currencies which use the same principles.

Researchers come to idea that the most notable contribution of Bitcoin is the blockchain, which is a distributed public ledger. Hence, Bitcoin is only one option of the Blockchain implications. The disruptive character of blockchain as underlying technology of Bitcoin is determined by its unique features which allow to apply it beyond money transfers and payments. According to Nakamoto's paper [59], the core features which raise a lot of attention to technologies used in Bitcoin are:

- Peer-to-peer electronic transactions (possibility to interact directly)
- Without financial institutions (time saving, cost cutting)
- Cryptographic proof instead of central trust (reliable data)
- Put trust in the network instead of in a central institution (no single point of failure)

Indeed, Antonopoulos states that "Bitcoin is a technology, but it expresses money that is fundamentally a language for exchanging value between people." [4, p4]. Savelyev argues that mathematical algorithm is a basis of Bitcoin value [40, p.4]. Issuing new Bitcoins is a result of the work performed by nodes to ensure the network, and build the blockchain (these mechanisms will be considered further). However, the overall number of Bitcoin units is limited by the protocol, its amount is 21 million Bitcoins [59].

Scholars [10; 50] define this particular Bitcoin blockchain as first generation of blockchain technology application, so-called Blockchain 1.0 (or Bitcoin 1.0). The main idea of it is conducting payments akin described above Bitcoin system. However, it is basic but not only one stage of distributed ledger technology. Blockchain 2.0 (or Bitcoin 2.0) by its structure allows us to apply it beyond simple transfer system. Swan argues, that "Whereas Blockchain 1.0 is for the decentralization of money and payments, Blockchain 2.0 is for the decentralization of markets more generally, and contemplates the transfer of many other kinds of assets beyond currency using the blockchain, from the creation of a unit of value through every time it is transferred or divided." (these matters will be discussed more detailed in Subdivision 1.3). Hence, additional protocols attribute basic concept with additional features.

In general, the researchers have gone a long way developing the concepts of alternative money and electronic cash. Bitcoin as digital unit that could be characterized as money which could successfully function without any central authority (i.e. bank, financial institution, state). The consequences of the recent advances in the fields of cryptography and decentralized computer networks go much further than just

decentralized payment system. Hence, it was necessary to overview retrospect on efforts to create cryptocurrency in the context of Bitcoin, which became possible due to the blockchain technology. Within the scope of this paper we will show how the technology which was invented due to the creation of Bitcoin cryptocurrency can potentially bring benefits to various services we use akin the Internet changed our relationships twenty years ago. The next subdivision will specify more precisely the key properties and opportunities of blockchain as such.

1.2 Key characteristics of blockchain technology, and its features

The following subsection is aiming to characterize the blockchain technology and how its intrinsic properties make its application as distributed ledger applications so revolutionary.

Decentralized ledger technologies "combin[e] peer-to-peer networks cryptographic algorithms, distributed data storage, and […] decentralize consensus mechanisms" to enable "people to agree on a particular state of affairs and record that agreement in a secure and verifiable manner."[47, p.4-5]. The following statement pretty accurately characterizes the essentials of blockchain, however each attribute of blockchain needs to be explained at a basic level to obtain better understanding of its advantages and disadvantages.

"The blockchain is essentially just what the name says: a chain of blocks [which are stored not on a single server but blocks are] run on a widespread network of computers as a distributed ledger" [15]. This network consists of peer-to-peer nodes (computers, platforms) with people behind them. In regards to the peer-to-peer network, Swan assumes, "The blockchain is the decentralized transparent ledger with the transaction records—the database that is shared by all network nodes […] monitored by everyone, and owned and controlled by no one. It is like a giant interactive spreadsheet that everyone has access to and updates and confirms that the digital transactions transferring funds are unique." [10]. Typically such distributed networks of computers are unstoppable, resistant to power cuts as long as it is globally distributed.

Explaining how blockchain network runs Christidis admits [20, p. 2293] that "this is a set of nodes (clients) that operate on the same blockchain via the copy each one holds." In other words, nodes maintain shared database by forming peer-to-peer network. Through cryptographic mechanisms they create new blocks, put on the ledger, and verify them." In sum, globally distributed network comprises set of computers which directly interact among each other, and synchronize the data to keep shared tracking of accurate records.

The security within the network is facilitated due to cryptography. It is necessary element because the users move value within the system. All the transactions are signed with electronic digital signatures

(further – EDS) which are facilitated by the public key encryption method. Witte explains this idea with example where Alice generates two keys (in simple words, mathematical proofs, could be expressed as qr-code) public and private. Public key Alice can freely share, but private key akin password is supposed to keep in secret. Bob can use Alice's public key and send transaction to her, then only Alice can encrypt the transaction using corresponding private key [gentle intro]. In case of Bitcoin the person who keeps the pare of keys is supposed to be the owner of particular wallet (address). However, there is no identity behind such an address. Any blockchain user in order to send transaction to the network signs it with its public key.

Nodes (computer) which maintain the network also use cryptography to create new blocks. It is combined with timestamping. These attributes allow nodes to build the chain by putting accelerated transactions into blocks with particular hash linked to the previous block plus timestamp [9, p.16].

The block as a core element of the blockchain can be explained as a structurised container (files with data) which aggregates transactions for inclusion to the chain [AA, p160]. Each new block contains cryptographical hash (data) with regards to the previous one, so that the last added to the ledger block is linked with the all blocks in this ledger. The speed of block creation and the number of transactions in these blocks vary depending on the protocol properties (e.g. in average Bitcoin block is generated every 10 minutes). The size (number of included transactions) of blocks may also vary regarding the different protocols.

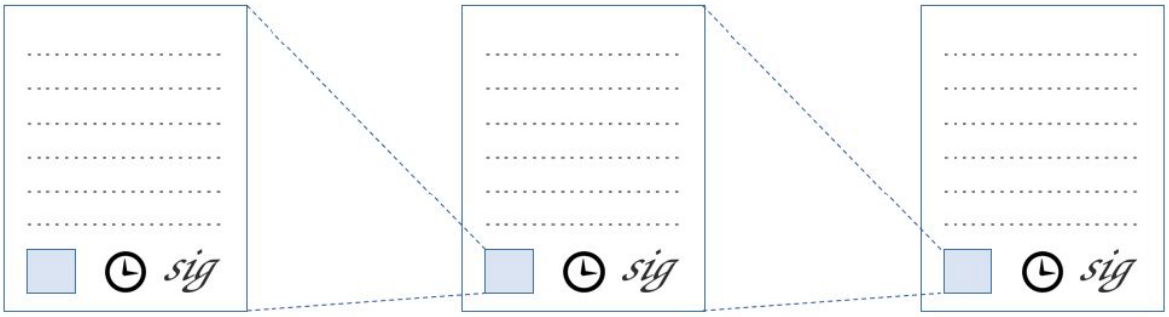


Table 1. Schematical explanation of building new blocks. [9, p.16]

Blockchain not only continually grows, but also it is being verified through cryptographical tools, and synchronized on the current state. Transactions which are included into blocks are cryptographically hashed, so that every entire block is also encrypted by hash regarding the previous block and submitted transactions, and time stamp. The authors of a report for Vermont [54] describe the method of cryptographic hashing as metadata (data about data) which is encrypted using a mathematical algorithm (cryptographic hash function). In other words, every electronic record (input) runs through the cryptographic algorithms, as a result there is produced short standardized analogue of such record (output). "It is not possible to

decrypt a hash maintained in the blockchain and produce the original document, but it is possible to use the hash to verify a copy of a transaction or document maintained outside of the blockchain" [54, p.7], explaned in the mentioned report. Any changes in the stored data, which was encrypted through cryptography, are practically impossible since the result of such changes will not fit to the chain.

The existence of distributed network allows to solve so-called double-spend problem which was a significant issue until Bitcoin Blockchain innovation. In cryptography theory, it is also associated with Byzantine Generals Problem which arises between at least two nodes within network, where at least one deviates (e.g. not sending any messages at all, or sending different and wrong messages to different neighbors, or lying about the input value) [12, p.41]. A key problem regarding double-spend is that "there was no way to confirm that a certain batch of digital cash had not already been spent without a central intermediary", digital asset was copiable just like e-mail, argues Swan [10]. The transaction recorded on the blockchain are validated and confirmed by the existing network which maintains shared mutual ledger akin chain. Swan adds that "The "blocks" in the chain are groups of transactions posted sequentially to the ledger—that is, added to the "chain.""[10]. This means, that there is no way no change or erase already stored data, it is only possible to add new information chronologically. For example, in case of Bitcoin "[user] can be sure that no one else can claim that this money belongs to them and not [him]." Unlike traditional money where such problem does not exist because "the same paper note cannot be in two places at once" [4]. By contrast, in case of traditional electronic money this problem is solved through centralized intermediaries. So that distributed network allows to rely on the data recorded in order to time, and omit any middleman.

Talking about the confirmation of absence of duplicated transactions without a trusted party, Nakamoto highlights the necessity of "a system for participants to agree on a single history of the order in which they were received". [59, p.2]. The ledger keeps tracking of the transactions executed on it so that we can aware about the all transactions, consequently information on digitized internal tokens. Sams specializes this uniqueness of DLT technologies: "each node on the networks takes a set of settlement instructions, applies them to the current state of the ledger and returns a new ledger state…then the nodes follow a consensus algorithm to come to agreement with each other on the new ledger state that each node computed independently." [61]. So that one of the main properties of blockchain is immutable verifiable data recorded on it.

The core mechanism which allows users to trust the ledger maintained and shared between number of nodes is called consensus. These concept allow users seeking trust entirely rely on technology. In the UK report there were mentioned that DLTs pose a threat to any hierarchical structure through an ability to

connect and operate in a distributed network, without trusted or necessary intermediaries, by replacing top-down control with consensus [68, p.61]. “Every time a consensus is reached, a transaction is recorded on a “block” which is a storage space.” [8, p.38]. It is simply impossible to add new block by omitting consensus between nodes.

Thus decentralized consensus is a crucial reason for trust to recorded on blockchain accurate transactions between unrelated actors, it significantly differs from the centralized one (where the third trusted party is present). “Decentralized consensus breaks the old paradigm of centralized consensus, that is, when one central database used to rule transaction validity” [8]. In other words, all records on blockchain must be approved by certain quorum of its users. “A consequence of decentralized verification and consensus is that all transactions are readable by everyone in records stored in a widely replicated data structure.” [19, p.3].

However, just using a simple consensus by majority votes of connected users is not secure since bad actors on the network can easily hack it (by creating multiple fake peers). In order to prevent frauds over networks, there were created numerous types of consensus models. However, mainly in practice blockchains use Proof of Work and Proof of Stake mechanisms, and their customized versions. The consensus over the network is necessary condition of creation of new blocks with transactions (the process is called “mining”).

As an example of Proof of Work mechanism we can consider Bitcoin where implementation of this algorithm through uses the computational power of nodes (nodes use hardware and consume electricity to maintain the ledger) solved the problem of spending the same item twice. Antonopoulos describes it as “a global election” every 10 minutes, allowing the decentralized network to arrive at consensus about the state of transactions” [4, p.3-4]. Nakamoto in his paper clarifies that if once the consensus on certain block state is reached, the data on it cannot be changed. Moreover, “later blocks are chained after it, the work to change the block would include redoing all the blocks after it” [59, p.3]. Therefore, it is a practical approach to set trust and security within the network by its architecture to validate accuracy of stored data in a distributed manner. Due to algorithms, each node is represented by its computation power and accordingly has one vote to participate in majority decision-making process on the state of blocks. In other words, each node should do some work by solving the cryptographic task to make a transaction.

An alternative to Proof of Work mechanism of reaching consensus to protect against reversal of the blockchain state is so-called Proof of Stake (also called virtual mining). Buterin describes it as “proof of stake relies on coins inside of the blockchain itself”. Thus it does not require to contribute any computational power (no need to solve cryptographical tasks to obtain the vote over the system). Embedded

coins into the system allow to determine the amount of nodes needed for approval the adding new data into new block. In words of Buterin, "security comes from putting up economic value-at-loss" [51].

The process of consensus is finalized with new block creation added to the chain. However, each of the described consensus systems contains also its disadvantages (e.g. proof-of-work mechanism is characterized by huge energy spending; proof-of-stake is not enough elaborated for immediate adoption). Currently scientists (in the area of cryptography, game theory etc.) are seeking for efficient solutions. There are exist different consensus models implied to other decentralized ledger technologies, however they attract less attention from the researchers side [38, p. 198; 17, p. 13].

As Robert Sams [61] hypothesizes: "Whatever proof-of-work or proof-of-stake system you have, there will exist another system design that will protect against reversal better if you have transparent validators subject to reputation and, perhaps, legal recourse. […] A consensus network based on authenticating the real identities of validators is an alternative to the PoW/PoS solution". Nevertheless, in requires validators to be held accountable for the data they verify which leads to the censoring of transactions [61]. In future practice, it will heavily depend on the users of the ledger, authorization of their identity and other issues. Reyes sums up that "regardless of the consensus method used, these decentralized public ledgers all share key qualities that make the technology revolutionary": e.g. distributed immutable transaction storages that eliminate the need for centralized authority between multiple users [38, p. 199].

Wright et Al. underlines the immutability of distributed ledgers: "after a block has been added to the blockchain, it can no longer be deleted and the transactions it contains can be accessed and verified by everyone on the network. It becomes a permanent record that all of the computers on the network can use to coordinate an action or verify an event" [47, p. 8]. That is to say, that individuals who do not trust each other may rely on the protocols and securely interact (e.g. send Bitcoins without any institution involved).

Also integral part of blockchains is so-called token. Originally, tokens play role of incentive for nodes (platforms) maintaining the distributed network. This means that for the participation in the blocks creation and reaching the consensus nodes supposed to get reward such as digital tokens. With regards to Bitcoin Blockchain the process of creating Bitcoins is called "mining," which involves competing to find solutions to a mathematical problem while processing bitcoin transactions [4]. In this case internal tokens execute two functions. Firstly, it is a reward for network maintaining by the protocol architecture, and secondly, it is currency as such which has certain value. Explaining the concept of digital tokens Brett Scott notes that "all the Bitcoin system actually does is enable digital tokens to be moved between participants, with the help of miners who volunteer their computer power to move the tokens around" [50, p. 2]. Thus,

numbers of nodes (platforms) maintain the blockchain properly, for the conducted work they get tokens as a reward.

However, internal tokens could be used in many other ways. Thus, Swanson [62] paraphrases Buterin's differentiating between possible tokens, for example, exclusion of network token at all, or "network token exists, but its use is primarily for transaction fees and protocol-required deposits and is otherwise not heavily emphasized" [62, p. 57]. Antonopoulos also argues that in such a case issuing currency is not the idea of certain blockchain system [4, p. 226]. Token is associated with certain value. It can represent broad range of digital or physical assets from ownership of a car to votes within company (shares).

Another core thing to remember is the regime of access to the network. Blockchain as a database contains blocks which includes certain data (e.g. transactions, data on the ownership of digital assets). Accordingly to the possibilities of nodes to validate data recorded on blocks, specialists distinguish permissionless and permissioned ledgers. Tim Swanson: permissionless system of consensus is characterized by pseudonymous or even anonymous identity of participants. (e.g. Bitcoin – everybody can validate transactions). In contrast, in permissioned systems the identities of participants are managed by whitelists (blacklists). In the latest case only certain groups of nodes are able to validate transactions, it allows "to legally host off-chain assets due to their authenticated, permissioned approach to validation". [62, p.5]. Mills et Al. consider permissioned DLT more widely than just through the criteria of validation. When participants of the permissionless DLT are allowed to perform all activities, the participants of permissioned ledgers contain arrangements which may allow for some participants send and receive asset transfer for existing assets, other participants may have access only to issue new assets, others may validate transactions, or update the ledger, others could be allowed only to read the ledger. [34, p. 12].

At the same time, there are also division into private and public blockchains due to the access to the data recorded on blocks. In a public blockchain the data is allowed to read for everybody (which still may be encrypted) and also allowed submitting transactions for inclusion into the blockchain. Instead, a private blockchain is a blockchain with limited access to stored data and restricted right to record new transactions on it [56, p.10]. It is also important to notice that "permissioned does not necessarily mean private; two core aspects of blockchain technology – decentralization and trustlessness – are fully leveraged only if access to the blockchain protocol and contents is provided to the end users." [56].

However, we don't agree with determination given by Christidis, where he considers public as equal to permission-less network, and private as permissioned network. [20, p. 2297] In addition, ECB (European Central Bank) uses other terms to point on the distinctions between ledger types within securities

field: unrestricted (i.e. public), and restricted (i.e. private) [60]. Nonetheless, the main essence remains, due to these types it is possible to combine different levels of users' access to a blockchain (i.e. permissionless public ledger for Bitcoin) [56, p.10]:

1. reading transactions from the blockchain, perhaps with further restrictions (e.g., a user may have access only to transactions that involve him directly)

2. proposing new transactions for the inclusion into the blockchain

3. creating new blocks of transactions and adding them into the blockchain.

Ainsworth et Al. argue that list of ledger participants, and the mechanism of consensus indirectly affect the efficiency of such a network. [13, p.8]. This allows adopters of blockchain to choose appropriate solution due to their needs. It is also critical to note, that reaching the consensus on the public blockchain state is much more costly that within a private network, and its security needs incentives for nodes which are participating in the validation.

Taken together distributed network and cryptographical algorithms lead to lessing role of the trusted central intermediaries between transaction parties. In other words, users can rely on the simple mathematical principles embedded into protocols. "Continuously growing list of data is recorded in a public ledger, including information of every transaction ever completed." [31] "The goal of Blockchain technology is to create a decentralized environment where no third party is in control of the transactions and data." . [31] Thus, the trust to third parties is not needed anymore to validate the transfer of digital units (e.g. cryptocurrency) between users, they are supposed to trust to computer protocols.

"The blockchain technology is trustless, meaning that it does not require third party verification (i.e. trust), but instead uses a powerful consensus mechanism with cryptoeconomic incentives to verify authenticity of a transaction in the database, which also makes it safe, even in the presence of powerful or hostile third parties trying to prevent users from participating. "

De Filippi [25, p.3]

The mentioned above features of blockchains ensure obvious advantages of the technology. Within blockchain environment users can rely on computer protocols and cryptography. Furthermore, it is possible to customize blockchain patterns by choosing the type of consensus, setting the limits on access to the ledger, embedding different tokens to reach suitable for certain purposes system. Vogel proposes us to look at blockchain as a large, public spreadsheet in which everyone has the ability to check that each digital exchange is unique (because everyone can see the ledger, and spot fraudulent transaction) [44, p.139].

Champagne in his research [52] highlights the following features of blockchain technology as:

- *Decentralization*: It means that it can run entirely through all the nodes of the network. Set of computers within the network each keeps the copy of ledger state.
- *Transparency*: Users within network can observe the transactions stored on the legder, and nobody can change previous data.
- *Autonomy*: The entire network is ruled by computer protocol regardless any centralized point of governance.
- *Security*: The Blockchain network is secured thanks to cryptographic algorithms that are set by the members of the network and the consensus set among all the participants.

To sum up, blockchain technology is useful one since it relies on mathematical principles. Its implications can facilitate decentralization, which means that instead of one computer, person, or organization which is supposed to manage the process, blockchain uses network with a huge number of computers. The concept of decentralization (peer-to-peer networks) has been existed for a long time, however the blockchain may completely change our approach to it. All data about transactions sequently recorded on blockchain is available for verification, transactions signed with private key could be revised by public key. Every transaction contains cryptographical proofs. When transaction is sent to blockchain, the network of computers forms a new block, generates consensus on the state that the transaction happened on certain time. Consequently, it is impossible to refuse existence of such transaction since it was impossibly to change stored data. Blockchain technology uses entire cryptography knowledge developed for last decades, which is combined with computer science advances, it impacts our relationships by various set of applications.

In this part we outlined the main technology advances which enable users to use blockchains to facilitate benefits which were impossible previously. A brief review of the technical advances of Blockchain technology is important to understand the implications of the different architectures with respect to performance, privacy, security and regulation. Decentralized nature and trust to mathematical certainty may raise potential opportunities and unique challenges for adopters of the technology.

1.3 Opportunities of the blockchain technology implications

Previously we considered some basic categories which make blockchain technology applications unique in cases when we need trustless digital environment without intermediaries. In the following section we will overview potential opportunities in regards with blockchain as technology taken from cryptocurrency innovation. Yli-Huumo et Al. originally defined a blockchain application as a solution that has been developed with blockchain technology as long as idea of a public ledger and a decentralized environment can be implicated within various ways in different industries [31, p. 21].

"Blockchains offer scope for rethinking political organization, including enabling novel ways of creating, managing and maintaining systems of voting rights, property rights and other legal agreements."[37, p.134], as explained by Reijers et Al. in regards to technological possibilities of blockchains.

The one mere reason for adoption blockchain solutions is 'trust' in digital environment between unrelated individuals, who normally use intermediaries services to facilitate secure interaction with each other. Werbach explains that the blockchain technology proposes entirely new type of trust models. "Until now, there were two primary trust architectures: Leviathan (deference to a central enforcement authority)[5] and peer-to-peer (reliance on social norms and other governance mechanisms in tightly-knit communities)[6]. The blockchain offers a third: trustless trust." [45, p. 5]. The reshaped trust paradigm influences the way humans interact within economic, and legal realms.

In literature opportunities of blockchain technology are often determined by the layers (protocolas) applied within particular applicatin. Thus Blockchain 1.0 (also called Bitcoin 1.0) is devoted to conduct payments, and move tokens within its network. Blockchain 2.0 contains layers which enable more benefits, so that additionally it may facilitate legal application (titles, programmable assets, contracts, escrow, wills, identity). And consequently, Blockchain 3.0 among financial and legal implications also combines non-economical applications (health, governance, science, intellectual property etc.)[10; 50, p16]. Due to the novelty of the technology many of potential uses are on the stage of exploration, however, some of the most obvious implication are already being tested or implemented by certain organizations (however, it is far to the mass adoption).

It is apparent, that technology which was successfully applied to run a cryptocurrency, also would be useful to other financial services. Many experts view the first application of blockchain technology within financial services. It is important application, DLTs could allow users with access to the shared database to directly clear and settle transfers related securities and cash with one another without relying on an intermediary [60].

However, the inherent benefits of blockchain technology tend to change wider range of areas beyond application in the financial sector. De Filippi argues: "Initially developed as part of the Bitcoin network, the blockchain is a general purpose technology that can be used for many other kinds of applications which formerly required the existence of a trusted third party: from decentralized domain name systems

[5] Hobbes, T. *Leviathan, or, the matter, forme, & power of a common-wealth ecclesiasticall and civill* (1676).
[6] Ostrom, E. *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge University Press. ISBN 0-521-40599-8.

(Namecoin[7]) to decentralized land and commercial registries (Factom[8]) or any decentralized application that can be run on the Ethereum blockchain." [28, p.8] At the very beginning (around 3-5 years ago) developers created numerous one-purpose (or several specific uses) applications, however then enthusiasts realized that can be developed multi-purpose platforms (Ethereum, which will be discussed in the part 2 of this paper).

The potential of blockchain innovation sometimes compared to the invention of the Internet [10, p.9; 8; 47, p.2]. But the fields, which blockchain application may influence, differs. The authors of the UK report claim that "[Distributed ledger technologies] are involved in potentially revolutionary innovations in a number of related areas: virtual currencies, distributed open and transparent record keeping, non-hierarchical networked systems, cryptography, and software engineering." [68, p.56]. Consequently, particular UK governmental bodies are attracted by "disruptive innovations" (as mentioned in the report) within "financial markets, supply chains, consumer and business-to-business services, and publicly-held registers." [68]

Swan argues that alternative currencies run on Blockchain have obvious benefits such as reducing time spent on transaction (e.g. due to the mutual ledger parties receive payments immediately), and cutting huge transaction fees (e.g. with Bitcoin you can transfer any amount of money and pay several cents because of peer-to-peer network). Furthermore, since cryptocurrency plays role of secure digital money for the Internet, it enables the development of the Internet of Things (i.e. number of devices with the Internet access which exchange data among the network). [10, p.5]. Tapscott et Al. underline the value innovation of Bitcoin Blockchain. They argue that open source protocols could be redesigned to handle securely other financial assets within the network (i.e. despite currency, it may be any asset or liability, physical or digital—a corporate stock or bond, a barrel of oil, a bar of gold, a car, a car payment, a receivable or a payable) [11, p.56].

Indeed, numerous potential applications of blockchain technology are willing to reshape the financial services industry. The authors of a report for the World Economic Forum 2016 state that "Distributed ledger technology has great potential to drive simplicity and efficiency through the establishment of new financial services infrastructure and processes."[69] They stand on that the new distributed infrastructure has transformative characteristics such as immutability of record-keeping (through providing historical single version of transactions), transparency (enabling balance among market

[7] Detailed information available at <https://namecoin.org/>
[8] Detailed information available at <https://factmom.com/>

participants, and cooperation between regulators and regulated entities), and autonomy (no need for intermediaries to ensure agreements) [69, p.24].

Payments on blockchains enable many variety of streamlining transactions, such as consumer-to-consumer, consumer-to-business, international operations, machine-to-machine. In case of Bitcoin system people spend less time on transfer, and save costs without dealing with third parties (e.g. Bitcoin has the potential to save poor foreign workers and their families tens of billions of dollars every year) [50, p.21]. Within the internet activity, low transaction costs enable new horizons for micropayments (e.g. crowdfunding, donation, fair payments for content distribution). New business models might eventually emerge based on the execution of a large number of micro-payments by a very large number of people [10]. De Filippi [28] highlights that "blockchain technology can be used to create new types of securities (cryptoequity) which represent shares of the project for which the funds are sought." The elimination of the middleman establishes much more trust and transparency. Now funds could be collected successfully without centralized entity, and the costs for such a crowdfunding could be significantly reduced. [28, p 7].

The other large opportunity is inspired by possibility to record on blockchain not only simple transactions, but information on property, contracts etc. In terms of technical concept, these possibilities are facilitated due to additional metaprotocols. Swan in her book outlines the current vision on areas where blockchain could be potentially applied (see the Table below).

General	Escrow transactions, bonded contracts, third-party arbitration, multiparty signature transactions
Financial transactions	Stock, private equity, crowdfunding, bonds, mutual funds, derivatives, annuities, pensions
Public records	**Land and property titles, vehicle registrations, business licenses, marriage certificates, death certificates**
Identification	**Driver's licenses, identity cards, passports, voter registrations**
Private records	Loans, contracts, bets, signatures, wills, trusts, escrows
Attestation	**Proof of insurance, proof of ownership, notarized documents**
Physical asset keys	Home, hotel rooms, rental cars, automobile access
Intangible assets	**Patents, trademarks, copyrights, reservations, domain names**

Table 2. Potential usecases of blockchain technology [10]

To provide and example of public records, there is Land registry system in Honduras which is characterized as ineffective and highly uncertain [53, p.4]. In 2015 with cooperation with Factom there was developed Blockchain-based Land Title Registry, which is aiming to protect the records from manipulations as long as data stored on blockchain (it was decided to use Bitcoin Blockchain as public

ledger) is immutable and auditable (write once data is never eraised). Such a solution promises to establish proper property rights protection system with reliable rules [53].

One of the most important concepts after cryptocurrency are so-called smart contracts. Combined with blockchain it became real to create self-enforcing transactions with multiple parties. The concept of such automated contracts we will consider in the next chapter since it raises an interesting discussion.

The next important implication is so-called smart property. Swan argues, that the purpose of using smart property is possibility to control the asset ownership via blockchain with access through private key. It could be digitized tangible property (e.g. real world stuff such as car, computer etc.), and intangible assets (e.g. reservations, stock shares, copyrights etc.). Smart property makes possible its using within smart contracts. Since the blockchain is a decentralized ledger, Schroeder claims that it could be used to store different kind of property or other legal claims, but in practice it should comply with existing legal framework can limit such blockchain registration (e.g. requirements on documents on real estate property) [41, p.65]. Mougayar asserts that "[blockchain-based] smart contracts are ideal for interacting with real-world assets, smart property, Internet of Things (IoT), and financial services instruments. They are not limited to money movements. They apply to almost anything that changes its state over time, and could have a value attached to it" [8, p.57]. So in this aspect blockchain could be considered as universal register of ownership.

Wright et Al. [47] investigate that blockchain akin the Internet can shift the balance of power from centralized architecture to decentralized one in the fields of communication, business, and even politics or law. The technology promises to change the way people organize their affairs. "It enables collective organizations and social institutions to become more fluid and promote greater participation, potentially transforming how corporate governance and democratic institutions operate. The technology could impact capital markets, by enabling everyday citizens to issue financial securities using only a few lines of code." [47, p.3] Smart contracts could be extended to creation of decentralized autonomous organizations (further - DAOs, also related to this category are Dapps, DAOs, DACs, and DASs - decentralized applications, decentralized autonomous organizations, decentralized autonomous corporations, and decentralized autonomous societies, respectively). Software can govern corporate structure, and manage resources within network facilitating certain blockchain features. In simple, words DAO is just a digital entity created by code and specific rules, and which is able to exercise certain mission (they can accumulate capitals, provide services etc.).

The next big promise of blockchain, as mentioned by Swan [10], is "fundamentally a new paradigm for organizing activity with less friction and more efficiency, and at much greater scale than current

paradigms. It is not just that blockchain technology is decentralized and that decentralization as a general model can work well now because there is a liquid enough underlying network with the Web interconnecting all humans, including for disintermediated transactions: blockchain technology affords a universal and global scope and scale that was previously impossible." [10, p.27]. Blockchain features could be applied to diverse segments as government, health, science, literacy, publishing, economic development, art, and culture.

Wright et Al. presents interesting concept of distributed real-time governance which could be implicated within corporate affairs (e.g. secure elections of the director by shareholders). It is also applicable to create non-hierarchical communities to facilitate cooperation and collaboration since blockchain technologies can provide transparent decision-making process. The authors give us an example of citizens of particular possible town, who may take part in its political life through voting for budget etc. [47, p.36-39]. The further idea of highly optimized systems is algorithmic governance: "a new normative system capable of regulating society more efficiently, reducing the costs of law enforcement and allowing for a more customized system of rules that is personalized to every citizen, and that is constantly revised based on their corresponding preferences and profiles." [47].

Another concept (related to idea 'code is law' which was developed after the rise of the Internet) within blockchain paradigm develops De Filippi et Al.: "Blockchain technology reinforces the tendency to rely on code (rather than on the law) to regulate individual actions and transactions. The blockchain enables a whole new type of regulation by code, which — combined with smart contracts — also promotes a new way of thinking about the law." [27]. It opens a new prospect of legal governance when the law is turning into the code. The authors argues, that "blockchain progressively acquires the status of a "regulatory technology" — i.e., a technology that can be used both to define and incorporate legal or contractual provisions into code, and to enforce them irrespectively of whether or not there subsists an underlying legal rule." [27].

After all, the mentioned blockchain implications are at their early beginning. The specialists mainly focused on the technical issues. The applications of blockchain technology are being investigated by global companies as well as by public institutions. In the report published by UK's Government Chief Scientific Adviser mentioned some opportunities for governmental authorities offered by blockchain technology [68, p.65]:

- Reduced cost of operations, including reducing fraud and error in payments (i.e. mathematical certainty has potential to replace many services provided by intermediaries)

- Greater transparency of transactions between government agencies and citizens (depending on system unrestricted access to stored information)
- Greater financial inclusion of people currently on the fringes of the financial system (simplicity of transactions, e.g. Bitcoin)
- Reduced costs of protecting citizens' data while creating the possibility to share data between different entities, allowing for the creation of information marketplaces (encrypted data is ruled by protocols with no single point of failure)
- Reduced market friction, making it easier for small and medium-sized enterprises to interact with local and national authorities (facilitated by automation and transparency)
- Promotion of innovation and economic growth possibilities for small and medium-sized enterprises (possibility for collaboration, automation, cutting costs).

The significant point of blockchain applications is elimination of the need for intermediaries which normally reduce risk between counterparties to a transaction and establish trust. Werbach explains, "possibility of legal enforcement gives parties confidence they can take the risks of entering into a relationship, such as a contract" [werbach, p11], this way legal system can facilitate cognitive trust. As Cross provides, "The law [22] provides a form of hedging against the risk that my trust was misplaced." [22]. Kiviat claims that blockchain programmable and self-enforcing transactions could be used for design of contractual relationships which are automatically executed without additional costs for monitoring or enforcement [32, p. 606]. It means possibility to transact with total strangers securely without using centralized intermediaries.

As we see, blockchain technology offers a wide range of applications across various realms of our life. No doubts, it has potential to change existing systems, or create new relationship which can facilitate significant benefits by using blockchains. However, the real limits of the blockchain applications are unknown, the researchers are intensively investigating this exciting field. The blockchain technology applications need a deep understanding of technical issues, as well as legal consequences related to digital dimension within such applications.

PART 2: CONCEPT OF BLOCKCHAIN-BASED SMART CONTRACTS

Due to the range of potential applications of blockchain technology across industries there is one essential concept called 'smart contracts'. The blockchain technology combined with cryptography enables enforcing and execution of different transactions by itself. The following chapter is dedicated to explain the idea of smart contracts run on blockchains.

2.1 Novelty of smart contracts within the rise of blockchain technology

The idea and term 'smart contract' has been existed for about 20 last years. As a simple explanation of smart contract given by Nick Szabo could be a vending machine. In his paper he explains it as a primitive precursor of smart contracts, enforcing the agreement that a coin can be traded for e.g. a candy bar [szabo, 1997]. In this case actual (candy bar) property is controlled and secured by physical properties of the vending machine. PdF et Al. [27] also give us several examples contracts by electronic means such as phone locking by telecom providers; DRM systems (DRM - digital rights management, e.g. iTunes, eBooks etc); cars incorporating automated speed limitations; etc. Bourque et Al. propose us an analogy for smart contracts as an administrator or a servicer of a contract (an executor) [18, p.4]. That is to say, blockchain with its properties such as reliable time stamped records, decentralization, set new possibilities for automated relationships.

Smart contracts could be explained in simple words as vending machine in the digital world. Savelyev argues that smart contracts allow to automate the process of performance contractual process of both parties, whereas the vending machine automated only from the one party side and still needs involvement of the second party [40, p.9]. Szabo, a lawyer and technologist, in the middle of nineties defined smart contracts as contractual clauses embedded into hardware and software in such a way that makes breach more expensive. However, such a concept of execution contracts between participants required other trusted third party. So such automation was pointless until the notion of cryptocurrencies and programmable payments came into existence. The same technologies, which enable secure ownership control over cryptotokens within particular network, allow to digitize other assets beyond currencies. Bourque et Al. also highlight that previously smart contracts concept was impossible due to the apparent information security reasons. First, actual cash exists in physical world when smart contracts limited within the Internet. Secondly, even regular digital cash is heavily regulated which restricts its use [18].

Hence, the rise of cryptocurrency technologies made the concept of automated contracts possible. "Now two programs blockchain and smart contract can work together to trigger payments when a preprogrammed condition of a contractual agreement is triggered.", -argue authors of Berkeley report on

blockchain.[66]. Due to the immutable ledger, it has become much easier to register, verify and execute self-enforceable contracts. Smart contracts are contracts which are automatically enforced by computer protocols across the globe. The dynamics of the networks have determined the future of contracting,

The practice of implementation agreement into code is not new. De Filippi et Al. points out that the distinction between DRM systems and blockchain-based smart contracts is the latest can eliminate the need of trusted intermediaries, however, it is not necessary in case of DRM. The true advent is that "smart contracts are actually meant to replace legal contracts" [27]. De Filippi calls blockchain a "regulatory technology" (i.e. piece of code can potentially define and enforce legal and contractual obligations akin law). [27]. In other words, blockchain makes a distinction between contracts executed by electronic means and smart contracts run on it.

Wright et Al. claim "creation smart contracts [as] one of the first truly disruptive technological advancements to the practice of law since the invention of the printing press." [47, p.10]. Since blockchain technology offers recording accurate and reliable data on transactions, it enables to enforce smart contracts within trustless cryptoledger. By decreasing the costs of mediation, self-enforcement, and arbitration, Szabo saw smart contracts as representing a fundamental shift in the world away from paper and towards digital systems. This shift was not to take place immediately, however, as Szabo recognized the value of the "long history" of paper [43]. Albeit, escape from paperwork is not only advantage of the concept of smart contracts.

The novelty of smart contracts within blockchain context is (1) transparency of the agreement and its execution; (2) independence of the agreement's execution and the parties; (3) automation of the agreement's obligations [18, p.7]. The Estonian legal scholars consider a paradigm shift in the decentralized practice of smart contracting, e.g. it allows to leave banks, lawyers, and different intermediaries aside, what lead to efficiency and cheaper transactions. "A computer program takes care of the whole contracting cycle" which simplifies the whole process and makes easy to handle as possible [7, p.134]. Moreover, transactions via blockchain do not depend on holidays, weekends (e.g. returning to vending machine, it theoretically always works); the time required to complete a transaction is shorten.

Wright et Al. argue, that software developers see a lot of uses within blockchain technology. As first application was creation of digital currencies, then self-executing smart contracts, and "cryptographic tokens that can represent property or ownership interest in emerging services" [47, p.8]. Twenty years ago, Nick Szabo used a specific name for some of these instruments: synthetic assets. Synthetic assets, in his words, "are formed by combining securities (such as bonds) and derivatives (options and futures) in a wide variety of ways. Very complex term structures for payments (i.e., what payments get made when, the rate

of interest, etc.) can now be built into standardized contracts and traded with low transaction costs, due to computerized analysis of these complex term structures." [63].Today, both lawyers and software programmers have the ability to create these types of instruments [62, p.17] whereas lawyers focus on using code in place with traditional contractual agreements.

Nowadays crypto-ledgers such as blockchain technology make smart contracts powerful, they provide a possibility to issue "secure and tradable tokens via distributed networks" [7, p.127]. The researchers notice that sometimes tokens tend to be explained as cryptocurrency, however it has much more wider range of applications. "This has led to the development of crypto-equity, involving so-called representative assets. This instrument is very similar to representative money, being backed by certain asset." The authors compare representative assets as crypto equity to representative money, being backed by certain asset. Due to their research these assets could be divided into 4 groups: (1) shares in a project that serve a function similar to stock, allowing participation in the decision-making and participation in financial upside; (2) tokens which represent ownership in something other than a company, for example intellectual property; (3) product tokens which are redeemable for some product, perhaps one consumable in the context of a decentralised technology (i.e. Ethereum); (4) access tokens which provide access to a particular set of benefits within a network, similar to a membership [7, p.127]. Persuasive, the blockchain technology makes possible for code to manage the mentioned categories via corresponding digital analogues.

This differentiation lead us to the concept of smart property which is another related concept regarding controlling the ownership of a property or asset via blockchain using smart contracts. Tokens can be represented by physical property such as car, house, smartphone etc. or it can be non-physical such as shares of a company. Even Bitcoin idea is not really money concept "[it] is all about controlling the ownership of money." [66]. Mougayar underlines that smart property is "an asset or thing that knows who owns it" [8, p.54]. In particular, the owner of such assets is person who owns the key to access it (secret key encryption), which means the access may be transferred just passing the key to someone else. Thus smart contracts and smart property are very closely related in the digital world, combined together they enable new opportunities from transfer ownership and other digital rights management within network to new not yet discovered revolutionary implications.

Actually, the discussions deemed across smart contracts are very broad. For example, Solarte-Vasquez et al. [7, p. 148] consider transactional design as an expression (transition to the direction) of smart contracting within further development of proactive law movement (i.e. developed from conflict

management, and a set of dispute prevention techniques). Huckle and White [ ] argue that blockchain technologies, particularly smart contracts enhance Socialist forms of governance.

The concept of smart contracts run on the blockchain could be considered from many aspects. Lawyers can are looking for relevant applications, and regards with traditional contract law and ownership relationships. The novelty of smart contracts appears with the blockchain technology, which facilitate automatic execution and verifiable record in a distributed manner. Nowadays it becomes possible to manage digital assets via blockchain, and even digitize physical objects into software means. However, it is early stage of the development of the concept of smart contracts, limits are yet unclear. In the next subsection we propose to explore closer what actually smart contracts are.

2.2 The essence of the concept of smart contracts

The understanding of the concept of smart contracts probably differs depending on the field of science, and due to its comparative novelty. It is important to distinguish smart contracts based on blockchain from traditional electronic, or automated contracts. In this subchapter we clarify the main attributes which constitute actual smart contract.

Despite the recent advances the vision of smart contracting is not certain. The numerous issues arise. For example, scientists distinguish different vision of the concept of smart contracts. Thus, for computer programmers it is "automated jurisdiction-free arrangements". For lawyers, "smart contracts are automated arrangements aside legal contracts because it is not possible to avoid jurisdiction". By itself smart contract does not create legal consequences. In contrast, contract in traditional meaning creates rights and obligations enforceable by law. Estonian scholars argue, that "A smart contract by itself is not a legal contract." [7, p.135]. However, it is possible to digitize traditional contractual clauses into smart contracts as software run on blockchain (i.e. due to its immutability and timestamping attributes). Yet, smart contract concept is considered broadly, so that smart contract may be seen as any transaction expressed by code put on blockchain.

Kolvart categorizes smart contracts aside traditional e-contracting (deep e-contractiong and shallow e-contracting) where the focus is on the level of automation which may or not lead to a creation of new business process. He argues that from a legal point of view it is not easy to differentiate automated e-contracts and smart contracts. However, it is obvious that both e-contracts, and smart contracts may operate outside legal contracts realm. The categorizing is getting possible only on the level of particular contracting process [7, p136]. Perugini claims that electronic contract model (not smart) may be modified and suspended any time, so that its enforcement would require the third parties to enforce its terms [36, p.21].

However, as a rule smart contracts do not need judicial enforcement (we will consider this category more detailed in the other subsection).

Mougayar in his book distinguishes smart contracts concept from other terms which could be mixed together. Smart contracts control a real-world-valuable property via "digital means", and it could be enforced by certain external data as triggers if certain conditions met (e.g. payment). However, it is not the same as contractual agreement neither Ricardian contract. [8, p.56].

Smart contracts rather software code than law, "but the consequence of their actions can be made part of a legal agreement, for example a smart contract could transfer shares ownerships from one party to another". Mougayar also argues that blockchain records on smart contracts could prove if terms of legal agreement were followed. Smart contracts represent business logic which are triggered by event-driven construct. There are no Artificial Intelligence. "Smart contracts are usually part of a decentralized (blockchain) application." Smart contracts are programmed through using specific smart contract language, and additionally "oracles" which implement external data into smart contract. Smart contracts development tends to creation of easy interface for any business user. [8, p.57]. Thus, just using smart contracts does not mean enforcing legal agreement, however, it is possible to compose it within certain legal content and blockchain technology, which would lead to legal consequences.

According to the academic definition of contract as "an agreement which is intended to give rise to a binding legal relationship or to have some other legal effect. It is a bilateral or multilateral act" [2], so that Savelyev argues that "Smart contract can be regarded as a legally-binding agreement" [40, p.10].

Another significant matter is that N Szabo in his research distinguishes concepts of so-called wet code and dry code. He explains wet code as traditional law, and dry code as software code [43]. Only combined together law code composed by humans and software code available for computer to read make sense of smart contract, and the blockchain enables facilities for self-enforcement of such a contract.

Wright et al. differentiate cases of using smart contracts. For example, "smart contracts represent the implementation of a contractual agreement, whose legal provisions have been formalized into source code". This means that parties arrange their contractual relationships through more accurate way, and more efficiently. It is easier to foresee the agreement's performance through source code. In other cases, "smart contracts introduce new codified relationships that are both defined and automatically enforced by code, but which are not linked to any underlying contractual rights or obligations." Researchers argue that, a blockchain allows parties to omit standard contractual agreement, however, it does not necessarily mean that no written smart contract is needed [47, p.11].

Clack et Al. give us a clear definition of a smart contract: “an agreement whose execution is both automatable and enforceable. Automatable by computer, although some parts may require human input and control. Enforceable by either legal enforcement of rights and obligations or tamper-proof execution.” [21, p.2]. This definition combines smart contracts’ legal side as well as technical side. Clack et Al. highlight that in case of smart legal contracts, they cover not only individual actions (rights and obligations) but additionally time dependent and sequence dependent sets of actions [21, p.3]. This approach is pretty complex to explain how automation and enforcement work on a specific platform.

The authors of Bekeley report define smart contracts run on blockchain as “computer programs that can automatically execute the terms of a contract. When a pre-configured condition in a smart contract among participating entities is met then the parties involved in a contractual agreement can be automatically made payments as per the contract in a transparent manner.”[66]. They stress the automation of predicted by script conditions within contractual relationships.

However, there are still remain many issues. For example, De Filippi outlines the question of whether “[smart contracts] code [(as written contract drafted in a computer language)] is “legally binding” upon the parties interacting with these contracts.” [27].

Consequently, in a wide sense smart contract could be any transaction script run on blockchain. The concept of smart contracting cannot be considered separately from its technical side. It is possible to personify part of legal contract into software code, moreover, the code executed on blockchain can lead to legal consequences. We can facilitate the automation of execution of stipulated by contracting parties scenario. At the same time, blockchain based smart contracts are distinct from other electronic contracts. In opposite to traditional contracts, which are enforced by parties, smart contracts are enforced due to pre-defined rules combined with other triggers (including communication to other smart contracts, machines etc.). On the logical grounds, it is apparent requirement for any smart contract to contain machine-readable code to be understood by electronic means.

2.3 Smart contracting technologies

Buterin maintaines “A blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publically visible, and which carries a very strong cryptoeconomically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies. … Blockchains are not about bringing to the world any one particular ruleset, they’re about creating the freedom to create a new mechanism with a new ruleset extremely quickly and pushing it out. They’re Lego Mindstorms for building economic and social institutions.”[51].

Buterin is founder of so-called Ethereum, a prominent platform which was aimed to eliminate Bitcoin Blockchain limitations, and extend its possibilities to create more advanced scripts within separate blockchain. Actually Ethereum provides its users with broad possibilities which enable smart contracts.

Swan describes the platform as "foundational general purpose cryptocurrency platform [it has its own internal tokens] that is a Turing-complete virtual machine (meaning that it can run any coin, script, or cryptocurrency project)" [10, p.21]. Indeed, Ethereum could be characterized as universal development platform to write smart contracts that can multiple other blockchains and protocols, including new cryptocurrencies.

Today Ethereum is the second-longest and fastest-growing public blockchain [11, p.71]. Narayanan et Al. notice that, in contrast of Bitcoin as transaction- based ledger, Ethereum uses an account- based model. In other words, Ethereum operates with more powerful data structure than Bitcoin as part of its ledger[Narayanan p290]. However, since the development of the smart contracts increasingly fast, Ethereum is not only one project with such a purpose. There are also CryptoLaw[9], BitHalo[10], CounterParty[11], Mastercoin[12],Corda [48],Hyperledger[13], Contractvm[14] etc. – which were developed to program smart contracts. In this part of the paper we will mainly focus on Ethereum as one of the most notable platforms.

De Filippi outlines that Ethereum enables to create software applications deployed directly on its blockchain what means that such a smart contract run, and automatically executed in a distributed manner, by every node in the network. [28, p.8]. Likewise Bitcoin, Ethereum nodes are incentivized by the built-in cryptocurrency "ether", so that they maintain distributed system and get reward for the conducted verification (consensus within network is reached by the slim majority). However, blocks in Ethereum are created faster (every 15 seconds instead of 10 min).

Delmolino et Al. in their guide article [26] explain that the Ethereum blockchain system keeps track of "ownership" of the currency (ether) by tying each unit of currency to an "address"(not linked to identity, thus could be countless), which are differentiated as addresses for users with public key, and addresses for contracts for its execution. Contract in such a case as a computer program consists of program code, storage, and an account balance, within blockchain system.

[9] Information available at: <www.cryptolaw.com>
[10] Information available at: <www.bithalo.org>
[11] Information available at: <www.counterparty.co>
[12] Information available at: <www.mastercoin.org>
[13] Information available at: <www.hyperledger.org>
[14] Bartoletti M, et Al. Contractvm: decentralized applications on Bitcoin (whitepaper), available at: < https://contractvm.github.io/cvm-whitepaper.pdf>

Anybody can create a contract, once it recorded on blockchain – the record remains securely stored and resistant to changes. The contract's execution can be triggered by message, payment from user or another contract. The code of the contract determines the behavior in case of stipulated scenarios [26, p.4-5]. Since anybody can create a contract with no size limits on blockchain, this "function" is requires payment by internal currency "ether" (similarly to Bitcoin, has value, could be purchased and traded). In other words, ether (the smallest unit of it is called "satoshi") is fuel (within system it is called gas) ensured by smart contract's creator to run their code on blockchain. So that users which support the system – get reward for updating the system which run the contract. Anyone can take part in the network consensus process for Ethereum Blockchain system. This mechanism prevents unreasonable redundancy of the blockchain size.

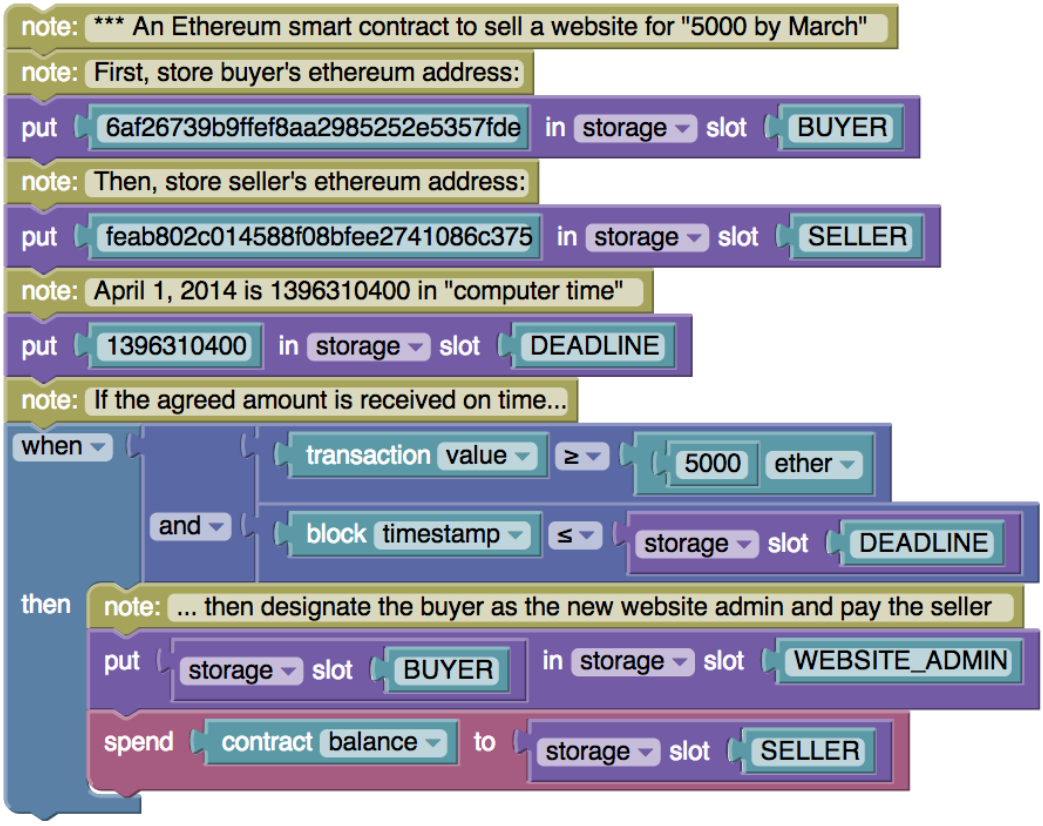


Table 3. EtherScripter (visual smart contract builder).

2.4 Enforcement of smart contract clauses within blockchain

The blockchain enables decentralized smart contracts—in other words, digitized set of rules that leverage a secure public ledger as an enforcement mechanism without relying on a trusted third-party institution or server for centralized recordkeeping or enforcement [32, p. 605-606]. Indeed, the concept of

smart contracts enables parties to conclude self-enforcing disintermediated agreement. In this subsection we will consider peculiarities of enforcement of smart contracts, particularly from the lawyers perspective.

According to Hobbes, the state - mythical Leviathan is central enforcement authority which can enforce contracts and property rights. Individual enter into contractual relationships based on penalties for breach and other remedies established by state frameworks [45, p.6]. Deference to central authority ensured through the simplest way to expand the radius of trust is to delegate it to powerful intermediaries (e.g. banks, courts, governments) [45, p.17]. It is standard historical view, that the state is necessary to enforce contracts.

Werbach claims, that even legal enforcement comes from the Leviathan of state power, "law may create necessary space for the informal arrangements of peer-to-peer trust." [45, p.18] Moreover, "A trust architecture that paired the stability of Leviathan with the autonomy of peer-to-peer trust might allow for new kinds of relationships, or better configuration of existing ones." [45]. This leads us to blockchain and smart contracts, which enable impossible previously tools for potential enforcement of rights and obligations. Computer code and cryptographic mechanism can establish replace the traditional way of enforcement (based on trust to number intermediaries) in contractual relationships.

Enforcement of the contract is necessary for hedging parties from the break of the contractual terms. In case of blockchain and smart contract contractual provisions could be potentially enforced by software rules verified through consensus within globally decentralized network. Swanson describes smart contracts as "a proposed tool to automate human interactions: it is a computer protocol – an algorithm – that can self-execute, self-enforce, self-verify, and self-constrain the performance of a contract." [42, p.17]

Scholars make a reasonable distinction between enforcement of traditional contracts and smart contracts. In case of traditional system it is inherent ex-post enforcement (*i.e.*, after the fact, e.g. police, court). In contrast with the previous method, regulation by code, particularly smart contracts, use ex-ante enforcement (i.e. the rules simply in advance does not comprise possibilities to breach the obligations) [35].

In comparison with traditional contracts, which have prescriptive nature, define what is permissible, and define the consequences if something goes wrong, smart contracts define only possible ways to transact by triggers and other described in particular contract tools. The difference is that the parties have less possibilities to deviate within concluded contract. Once such a smart contract is initiated, the agreement is enforced. Parties cannot influence the automated execution of the contract they concluded, otherwise they predefined some special functions. It is impossible to breach smart contract terms, unlike traditional contracts since the execution of the code is controlled by digital means.

In [21] the authors investigated the category of smart legal contracts highlighting the connection of enforcement with automation. The part of legal agreement, which is supposed to be enforced by digital means, should be capable of being embedded into code. The concept of smart legal contracts must cover individual actions, time dependent and sequence dependent sets of actions, to be properly enforced by shared network or other electronic means.

De Filippi et Al. argue that smart contracts emulate the logic of contractual clauses so that specific integrated enforcement mechanism can provide trustless transactions [27]. The challenging issue here is to transpose such clauses into deterministic conditions to enforced them.

It is not disputable, that any contract should be valid to be enforceable (respect specific formalities as mutual consent, consideration, capacity, legality), so that smart contract to facilitate legal consequences also should follow the requirements established by common legal principles of contracting, and particular law. Kolvart et Al. consider PECL [3], UNIDROIT [1], DCFR [2], provisions to be obeyed while parties agree to use smart contracting solution to implement the contract terms on the blockchain. In other case, the scholar notice that such a smart contracting part is not legally binding. "Smart contracting is legally binding only if parties have agreed upon all essential requirements needed for the conclusion of the contract. [7, p.140] However, it raises many other questions such as what if the self-enforced contract colludes with law requirements, illegal contract, jurisdiction etc [40, p.20]. By today there is no elaborated private law approaches specified on smart contracts application.

Bourque S. et al. gives us an example when smart contract does not necessarily constitute a contract as enforceable. In case of smart contract which contains "one programmatic event, which is that whenever deposits are made to its wallet, it simply re-deposits them to another wallet. This, in TCP/IP terms, would be a simple redirect". [18, p.10] Within another similar scenario smart contract splits the funds in half to two wallets, thus it represents a partnership entity, however, not a contract in Law.

Raskin assumes some probable scenarios for adoption such a method of enforcement provided by smart contracts. On the one hand, state's approach is to permit ex-ante enforcement (i.e. as collateral matters). On the other hand, there is prohibition of ex-ante method (e.g. through banning of certain forms of contractware). And the last opt is the average approach, allowing ex-post to enable remedies[15]. However, it is pretty early to determine more precise model of co-existing self-enforcing contracts within traditional ways of enforcement of contractual clauses in case of their breach.

[15] RASKIN, M., *The Law of Smart Contracts* (September 22, 2016, draft). Georgetown Technology Review, Forthcoming. Available at SSRN:<https://ssrn.com/abstract=2842258>

In conclusion, the ultimate goal of smart contract is to facilitate its self-enforcement and eliminate the possibility of breach of its clauses. According to smart contract, the parties have no other choice rather than comply with the designed rules. It is important to bear in mind there are could be many types of smart contract, so that our approach depends on certain situation. Blockchain-based smart contract provide new opportunities for traditional enforcement of rights and obligations. By omitting traditional system of contract enforcement (courts, investigators etc.) contractual obligations can be supported by smart contracts to facilitate efficiency, reducing costs, verification, speed. Turning legal obligations into self-executing transactions potentially makes breach of such obligations impossible.

2.5 Challenges and limitations

Blockchain-based smart contracting is still on its experimenting phase. The technology offers us certain benefits, however, they accompanied with limitations. Smart contracts as a code could represent simple transactions, as well as contracts with legal consequences. On the one hand, there are issues on proper code use, its accuracy. On the other hand, depending of the particular type of smart contract there are issues on co-existing digital dimension with real world.

Since any smart contract is a computer code, the most obvious matter is designing the proper code. In other words, every transaction should include all predictable possible functions to avoid misuse and fraud. By today, one of the brightest examples is variation of smart contract called TheDAO[16]. It is a smart contract run in Ethereum blockchain to collect users' money as virtual venture capital (smart contract owns the money). The rules of TheDAO were immutable, the governance was given to its participants due to their votes. Indeed, many users joined it, and by fact created decentralized digital company which had raised issued on its liability within legal realm. However, the main point is the imperfect code, which allowed loophole used by individual to extract money on the benefit of subsequent smart contract. Before this incident it was presumed that code is law (in the meaning that unchangeable software code governs relationships in the digital sphere), but by now this statement is pretty disputable. From the technical perspective it was actually possible to reverse fraud blocks with transaction, but it would destroy the entire idea (i.e. global agreement on the blocks content) which stipulated the creation of such smart contract. This lesson should be taken into account when we think about designing any pre-defined set of rules. Because once we put these set of rules (code) on the blockchain, it is cannot be easily changed and it acts by its own pre-defined way. Currently, computer scientists [16; 66] investigate possible ways to pursue correctness and functionality of the code by applying software designer's tools.

[16] Detailed information available at: <http://www.coindesk.com/understanding-dao-hack-journalists/>

Particularly, for lawyers the most intriguing application of smart contracts is contractual clauses enforced on blockchain. Such a provisions is supposed to have binding effect for parties, but it significantly differs from traditional contract law approach. Whereas traditional contract terms are expressed in normal language, the smart contract terms are defined by code scripts. Comparatively to traditional contracts digitized terms pose limitations caused by the strict meaning of code. Scientists [43] distinguish wet code (i.e. traditional law as a result of humans mind) and dry code (i.e. smart contracts' code, understood also by machines). It is not easy to transpose flexible abstract rules into rigid code, even within simple conditions. So that, it poses challenges for lawyers to combine human and technical part to facilitate efficiency in particular relationships. The necessity of smart contracts application should be deemed to have sense for contractual relationships.

Nonetheless, the dimension of smart contracts which contain or may cause legally binging consequences is supposed to meet the regulation. There are several aspects where lack of regulatory certainty hinders the adoption of smart contracts.

PART 3: DECENTRALIZED SYSTEM OF BLOCKCHAIN - AUCTIONS

This chapter is dedicated to application of blockchain technology within public sector, particularly we describe peculiarities of electronic auction process including smart contracts run on blockchain. The mentioned technology evolves apparent benefits such as transparency, efficiency etc. Furthermore, it allows users of the auction to rely on cryptographical protocols instead of corrupted institutions during the trading procedure. Ukraine is one of the first countries to experiment with blockchain technologies within services in the public sector, in particular electronic auction system run by government is supposed to be the first one to enhance the decentralized auction procedure within blockchain technology. The foregoing discussion also comprises issues on implementation new concept of electronic auction based on blockchain into existing system. The term "auction" is used to refer to the mechanism of the sale, and the legal consequences of the sale. Generally adopted definition of auctions comprises the following factors: (1) the sale is organised by public competition (i.e. the sale goes to the best bidder), (2) the sale involves a relationship of agency (it is run by an auctioneer with the legal authority to commit the parties) [39, p.9].

3.1 Context and the present state of affairs of auction procedures in Ukraine

State property is one of the most important tools of the economic system. It comprises enormous piece, which should be proper instrument for supporting sustainable economic development and social welfare of the nation. The efficiency of the management of state property impacts socio-economic development of the country.

Among the main tasks of the efficient managing of the property, one is to make the structure of the state property closer to the level of the developed countries. One of the ways to provide the solution is conducting efficient sale and lease of such property.

Ukrainian government uses auction for selling and lease state and municipal owned property. In such a model of auction one seller is auctioning one item to a set of buyers interested in privatization [5]. Scholars assume that auctions as a kind of economic activity have a long history, nowadays they has been widely spread in the modern community by the Internet. [5, p.257]. Accordingly to the literature on auctioning, the auction for the purposes of selling and leasing of state owned property could be categorized as so-called "First-price sealed-bid auctions". In this case, bidders submit simultaneous "sealed bids" to the seller. The highest bidder (best bidder) wins the lot and pays the value of the bid. Authors notice that "value of [the] bid not only affects whether [participant] win[s] but also how much [he] pay[s]" The point is that bidders in a first-price auction will tend to bid lower [5, p.257]. In contradiction with theory, there is a serious

weakness, the current Ukrainian Auction system is centralized and not transparent. It is managed by governmental institution, due to such circumstances the systems allows misconduct in the process.

The present Ukrainian auction system could be characterized through the following features as:

- *Corruptional risks*.

  Lengwiler et Al. define corruption as situation when the person who runs the auction, the auctioneer, twists the auction rules in favor of some bidder(s) in exchange for bribes." [33, p.1]
- *Possible manipulations during the process of selling and outcome of the auction results* (e.g. person who is in position of trust has access to the auction procedure and may distort the data)
- *Impossibility to monitor and control* (because access to the data has only limited group of institutions)
- *Funding from budget sources* (the issue is that the centralized service needs huge budget resources to be maintained, however, the system used only by small proportion of citizens)
- *Single center which allows manipulations* (only minimum efforts are needed to change information internally which stored there, as well as comparatively easy to hack for external attacks)

All mentioned aspects of the system arguably do not stipulate building of sustainable future. In the current system of electronic auctions, mainly there are three core problems: centralization of all data and resources, corruption, fraud, and the possibility of data change. Moreover, frequently on the local levels, the auction mechanism is provided completely offline (i.e. just by attending natural persons particular authorities).

Basically the process of state property lease and privatization comprises three stages. The first stage is initiated by the owner of certain property, and includes formation of the lot. The second one includes bidding, which finished with the last – contract conclusion.

Evidently, the current regime of auctioning of state and municipal property needs to be reformed via innovative proposal. There have been discussions on reforming the state institutions in relation to the current system of selling and leasing of state owned property. Innovation and Development Fund offers a decentralized model of data storage and computing experience using open source and innovative advanced. The team has already prepared a draft law for the electronic auction on lease and trade of state property, elaborated model of conducting electronic trade. Further subsections will clarify the main peculiarities and benefits of this approach.

3.2 Goals and principles of the creating the blockchain- based system

Due to the blockchain technology characteristics it became possible to maintain electronic auction more automated, and to minimize the influence of humans factor on its results. As we considered in the previous chapters the blockchain innovation could affect many sectors of society. It allows to transfer digital units within the networks, it stores an accurate data immutably, it is distributed between numerous platforms.

Electronic Auctions Reform minimizes corruption component and provides fair opportunity and parity to all participants of the market. Decentralized auction project (e-Auction 3.0)[17] is based on innovative system - Blockchain. The designers of the e-Auction 3.0 [48] has a significant experience in the area of creating innovative solutions for business as well as for public institutions.

The new system [48] which was elaborated in 2016 and it already has been spread in several districts of Ukraine comprises innovative approach to the auction process:

- *Involved in the market ecosystem which stipulates development* (various market players are involved in the support and maintaining the system, they have certain economic incentives)
- *Possibility to monitor the whole process and systems through API* (the users of the system have possibility to access data with regards to their role in the system)
- *The process of auction is appeared for every participant separately and automatically* (machine readable protocols make the process easier and faster, the accurate data is generated with mathematical certainty and without humans impact on it in the meaning of previous archaic system. Of course, protocols are designed by people but conditions are the same for everybody)
- *The bids and actions are recorded in the block and synchronized with platforms* (as we know, blockchain evolves immutable storage of data, we can rely on records due to the architecture of the system of consensus)
- *Automatical connection* (there are provided simple, understandable interface, potential participant clear understand the auction stages, he is only required to follow the rules to be involved into the process)
- *Impossibility to influence on the results* (by automation of processes with software protocols the system is impartial, additionally, there are no centralized authorities which could access it and change something. Data and calculations are distributed)

The main reason of seeking for blockchain solutions is breaking up the corruption element in the existing system. The aim indicated in the White paper of the project is “to build up a transparent,

[17] More information available at:< http://www.eauction.idf.solutions/>

decentralized e-Auction system for state property privatization and lease, in order to minimize the existing corruption and mismanagement risks, to reduce the state budget expenditure and as a consequence eliminate corruption component in the management of state assets." [48]. It also supposes drafting new law framework which would properly regulate the existing affairs.

Due to the White paper [48] on the Concept of the Decentralized Auction system' functions are to perform the following tasks:

- *"Maximum transparency"*. In other words, any document, any information relating to the rent and sale of state property should be available online for all interested parties.

- "*Open auction"*. It means simple, understandable and easy to use method of state-owned property rent and sale.

- "*All auctions should only be performed online*". This requirement allows to maintain all the data on auction procedure between platforms and ensure its accuracy.

- "*Starting price of the auction should be known in advance*." In case of omitting this requirement there is a risk of corruption.

- "*A participant cannot offer less than starting oriented price*." It follows from basic auction theory for this category of auction. Participants can increase the minimum bid by defined auction "step".

- "*The documents from administrative agencies* [(such as the company registration license, tax clearance certificate, credential of the absence of bankruptcy proceedings, etc.)] *are provided only at the end and only by the candidate who offered the highest price*." It obviously reduce paper work and simplifies the auction process for potential bidders.

- "*The auction winner is determined under the rule pass/fail*", e.g. on the principle of plus/minus the matching of a participant and his offer with the technical requirements. Due to the automated execution of auction procedures it is easy to determine the matching to the technical requirements first-price seal bidder. The assessment of participants starts in order top down. If the participant with the highest offered price satisfies technical and qualifying requirements, "he is considered as a winner and other participants are deferred".

- "*Any participant of the system may request information regarding the auction documentation*." Unrestricted access to the auction documentation should ensure more clear rules and provide efficiency. Any participant has the right to ask the auction organizer and get the reply within the time limit. "All answers should become an element of the auction documentation at once and be available for all participants."

- "*Any member may appeal an ongoing auction*." In case of a denied appeal, the participant has the right to use the transactional data from the blockchain to start a court case. This point is extremely important since it states that transactional data from the blockchain could be used to start a court procedure in case of dispute. The recognition of stored data is apparently highlights one of the core characteristics of blockchains – accuracy and immutability of its data.

- *"Self-sustainable economic model*." The creators of the system argues, that "financial independence must be ensured by self-financing mechanisms and legal independence - by changing the order of auctions and legislatively fixed standard technical requirements that are developed by a community and composed of representatives of the state authorities and civil society."

- *"Any concerned person should have possibility to receive all the information connected to the specific auctions through Internet",* including: Auction announcements; Auction documentation; Auction participant offers; Auctions records; Payment confirmations of deposits and registration fees; All the correspondence relating to the auction; Contracts with winners of the auction [github].

The performance of the mentioned tasks would lead to innovative Auction system. The architecture of the system is built by following this statements. There is still remains some paper work. However the key technological solutions allow to maintain fair rules and competitiveness between participants during the important auction stages.

Thus exploration the use of blockchain technology aims to move more of its paperwork to cheaper systems. The shift from old system to new digitized and distributed system is obviously useful for transfer of many kinds of assets. In this case therefore the blockchain technology could be useful not only for data integration, but also for providing transparent rules during particular auction phases.

3.3 Classification of auction actors and their main functions

David Easley et Al. [5] consider auctions as "simplified form of buyer-seller interaction". Due to the auction rules, these relationships are put in order to gain the final fair result. The eAuction 3.0 is a system which comprises users which are interested to sell or buy something, moreover, it includes the platforms which support the system, banks, and observers. The relationships in the eAuction 3.0 are ruled by the protocols and software, which excludes unpredictable scenarios of the procedure. All the materials are available open-source, so that everybody can revise it before entering into the process. This subchapter will describe the main features of each subject and their role in the eAuction 3.0. For more coherent vision of the described procedure I attach Appendix 2 which gives an illustration of the new mechanism.

According to the concept of the eAuction the organizer (i.e. seller) is interested in obtaining the highest possible price for the auction lot, through open competition among auction participants. The

organizer owns certain property or property rights, and due to his capabilities took a decision to sale it or transfer for a lease to the auction winner (i.e. best bidder).

The organizer could be represented by a state entity or local commune entity as long as we consider sale and lease of state and municipal property. Moreover, in case of extension of the system the organizer (seller) can be also private entity or person. The organizer is capable to execute following tasks within the system [48]:

- announce the auction holding and publish the auction conditions;
- answer questions concerning the auction conditions;
- publish the complaint investigation result;
- publish the result of the auction holding;
- publish the banking particulars of the contract with the winner;
- publish the result of the court decision on the auction.

These provisions embedded into the system and they enable the organizer to act as permissioned by the software. Actually, there is longer list of organizers rights and obligations, we have mentioned the most notable ones. The software (application) allows the organizer to enter necessary data regarding the auction through user interface. The organizer's Application forms structured package (i.e. XML standard) of data and sends it to the ledger (blockchain), then in a response the Application of the Organizer receives a unique ID code and the auction lot code, which controls the auction lot (including sending and receiving messages on clarifying the conditions of the auction, the removal of the lot from the auction, etc.)

Other subject of the eAuction is participant (i.e. potential buyer). The participant could be represented by any natural or legal person eligible to conclude certain contracts. The participant of the eAuction is interested in implicity and transparency of the auction; equality, complete and real-time access to information about all the auctions; fair competition with other participants of the auction [48].

Participants besides obligation to comply with the Auction rules, have certain rights:

- familiarize with the auction conditions;
- ask questions concerning the auction conditions;
- register bids in the auction;
- file complaints to the auction organizer;

In this case the draft of the Law [70] also extends the list of functions and determines it as not exhausting, however, during the bidding phase participants are supposed to follow the architecture of the process. The system allows them to enter through interface data to register and bid, and other necessary

actions due to the auction rules. All the proper actions are registered in a form of transaction associated with the lot of the auction. Every bid has its identifier and a bid code to control it within the system.

The next subject is Platform (Publisher). Platform could be an organization or individual providing access to the System through a special software and which is interested in a maximum inflow of organizers and registration of auction through itself, to promptly inform potential participants in short terms; and maximum inflow of participants since it charges fixed fee for participation in the auction.

Platforms are supposed to:

- identify the organizers and participants of the auction and provide access to special software for the auction holding;

- provide the following services (e.g. entering registration information about the auction and the organizer's decisions about the auction results; informing auction participants regarding upcoming auctions);

- publish the court decision, if acted as the registrar for the auction organizer;

The next subject in the eAuction is observer. They are represented by public and state organizations which are only tracking and monitoring the process of the auctions, this option is also available for journalists and other individuals who has no status of participant or organizer. Observers are interested in:

- public availability of all materials related to the organization and holding of auctions;

- transparency of all taken decisions on the results of the auction;

- the presence of several solutions from different manufacturers, allowing an access to the auctions data in a human-readable format.

Observers conduct online monitoring of the availability of the system data. This is an additional instrument ensuring the transparency of the system.

Every eligible person can be a user of the eAuction. Furthermore, every entrepreneur can become a part of the system by running the open source software as a platform. Also other are connected to execute functions to support the decentralized system, such as banks, providers, observers etc. All together integrated within blockchain these subjects supervise each other, and validate proper information.

The subjects of the auction are required to pass the registration of their account (address). The participants are linked to certain platform – so that their digital address will contain platform's address. It means, that the number of participants tied with the platform influences the proportion of platform votes aiming to reach the consensus on the blockchain state.

The proposed scenario of holding eAuction supposes certain architecture which maintain transparent and efficient system. It mainly relates to the decentralization of calculation and storage of data, which is

received from subjects of the auction and recorded in blocks. It requires universal format for the data exchange, "the rules of holding of the auction must be defined by public standard". Each participant should have freedom of choice for the ways (themselves or through platforms) and means (with a help of self-developed software, or purchased or leased) of participating in the auction upon one condition - compliance with the format standards and data exchange procedure. And as the core there were proposed advanced solutions should be used as basis, based on the open source code, working without down time access, censorship, fraud, or third party intervention.

3.4 Proposed blockchain-based smart contracts solutions

3.4.1 Architecture of the decentralized auction system

The complexity of the system is supported by the 'https' protocols, and data base with implied blockchain technology. The system imposes the same rules for every user, they are supposed to use the same data standards.

The entire system of the eAuction 3.0 (see Appendix 2) ensures high efficiency, transparency, and security due to its architecture and blockchain technology support. Decentralized eAuction meets requirement on real-time mode which mainly relates to period from registration of the lot until determination of the winner (best bidder). These properties are possible due to the applied Blockchain technology and smart contracts which guarantee the integrity of each lot and auction bids. Thus, any participant is allowed at any time to receive a copy of the lots base and auction bids. Proposed technical decisions ensure high availability and failure safety levels of above mentioned services of the network due to distribution (i.e. no single server to fail). The concept of the eAuction describes it as "ability to store data about the lot and the auction bid in the form of interconnected electronic contracts, the functionality of which can be easily extended and completed by the electronic services and integration with other automated systems." [48].

Also successful implementation of the system supposes existence of certain applications with user's interface for Organizers and Participants. These applications are working in compliance with other elements of the system and established rules. For example, application of eAuction organizer generates packages according to standards with data about the auction lot, answers for participant's complaints, auction results, and sends these packages to "electronic contract about the lot of the auction to a Virtual machine of the electronic auction" [48]. It also contains such obvious functions as displaying the time before the start and the end of the auction, shows other relevant information. Accordingly, the participant's application provides other corresponding functions, for example, generates and sends packages with data about registration data, bids, and complaints to the organizer, including intelligent search and monitoring of the current state of the

lot. Consequently, all the data concerning the process of eAuction is supposed to be recorded and stored on the Blockchain.

3.4.2 Auction phases in the proposed architecture

The auction used in case of selling and leasing the state owned property has simple format. It supposes certain rules to manage the behavior of the participants and other actors. However, in eAuction these rules also represented by the architecture (software code) and provides certain phases. We can think about phases of the eAuction procedure as 4 parts due to each the seller and participants act to facilitate their aims (related Appendix 2 is attached to illustrate these matters). These parts of the process are provided within blockchain run by decentralized platforms, every act therefore is automatically recorded on the distributed ledger.

The first phase is called pre-exposition. It comprises editing and **lot registration** by the organizer who finishes this stage by implying digital signature.

The next one, called **exposition** begins just after the registration of the lot. During this period participants can register in the Auction. After they transferred security deposit and registration fee they are allowed to the next stage. The duration of the exposition period depends on the lot and its value. For example, the exposition period of the lot for selling apparently differs from the exposition period for the lot which is subject of a lease agreement.

The next stage, called **electronic trading** starts at 10:00, on the next working day after the end of exposition period. "E-trading lasts two hours for all the lots. if there is no registered participants on the lot the bidding on the auction lot will not start and the auction is automatically removed from the trading. If there is only one participant the procedure is carried out according to the standards and participant should submit at least one bid on the lot." explained in the concept of the eAuction 3.0. The bids are only accepted if the requirement on the registration fee in fulfilled (i.e. it is proved by the bank statement attached with digital signature).

There are certain requirement to the participants bids (fee proposals) to satisfy basic rules of the auction. The system is supposed to accept only proper inputs (i.e. respect the amount of the bid, not satisfying inputs are not accepted). After displaying the auction lot, its holding for all participants begins automatically at the specified moment, then after expiration of time allotted to auction bidding, the auction is completed and receive of the bids on lot is terminated. Participants are free to observe others' bids. The next part after the submitting the bids is determination of the winner. The system automatically defines the rating, and consequently it chooses the participant who holds the highest bid (the best bidder).

The phase of the **contract conclusion** with the proper winner is off-line, however, it is notably that in such a case reliable data from blockchain is used as a proof to conclude the contract.

In sum, the mentioned phases are important within blockchain application. The data with regards to deposits, bids, other fees is recorded in blocks, so that it is proper information for the further procedures (i.e. concluding the contract with the winner, proofs at the court).

3.4.3 Vulnerabilities of proposed solution

The described architecture is an attempt to formalize the algorithmic procedure, however some issues are related with external functions. While all the actions are provided by the code and participant has the right to ask question Organizer, the latest may ignore questions and complaints. For these purposes, such behavior will be displayed with the results on the particular lot. Additionally, the participant has a right to go to court by presenting the auction transaction log as the evidence of the complaint and unsatisfactory reply on it.

There is no single failure of the database, but hackers can try to attack separate platforms or Participants. In this case, the creators solve this issue "by long trading period in order to maximize the value of the attack, and at the same time to give enough period to participants to switch to another platform/communication channel." [48].

The problem of the previous auction system is that participants overvalue their bids, and then they just quit the process. So that it allowed manipulation of the consideration on the lots by other participants. In the proposed system the bids are accepted independently from all participants, their bid rating is generated and the system defines the winner. In case of misbehavior, the Participant gets disqualification and refused to return the secure deposit. In such a way, it is economically inefficient to break the rules [48].

3.4.4 Model of reaching consensus on the state of the blockchain

One of the main points of creation the auction system using blockchain is possibility to store immutably accurate and transparent data, pursue automation and reliable access to the elements of the data. In relation to proper functioning of the distributed ledger technology one of the key issues is the model of reaching consensus on the ledger state between nodes (platforms). The parameters set for the consensus mechanism determines how the "network of nodes" verifies changes to every block in the system. Originally the blockchain (Bitcoin blockchain [59], Ethereum blockchain [51] etc) works due to the cryptocurrency as tokens embedded into its system. That means that nodes get remuneration as crypto coins (tokens) for proper maintaining the ledger and composing new blocks. Such model of reaching consensus is called Proof of work which was explained in the Part 1 of this paper. However, the creators of the eAuction 3.0 faced with apparent issues, due to the regulatory uncertainty and other circumstances it was impossible to use any cryptocurrency in the procedure run by governmental institution. Thus, there was invented alternative sophisticated solution.

The developers [48] put the concept Proof of stake as consensus for the Decentralized Auction System. More precisely this variation of participation in the maintaining the system, researchers call proof-of-deposit [17, p.13]. So called virtual mining is considered enough secure within the system with registered participants (not entirely public ledger since users are identified). This means that participants are required to deposit certain coins (stake) in time-locked bond account, during which they cannot be moved.

In case of the decentralized auction as a stake there are used participants' security deposits put on the off-ledgers of the private banks which they cannot move during the participation. The bank not only keeps the deposits for the purposes of the Auction procedure but it also counts accordingly to the amount of participants' deposits, and by this way it determines the proportion of votes for reaching the consensus. Proposing the model of consensus the creators argue that "the ownership ratio will be the number of registered participants "standing" behind the platform". [48] In other words, the platforms are incentivized to attract more participants as long as they get reward for number of connected users.

The proposed model of achieving the consensus is enough secure for use by the government system: "only platforms [behind which there are registered participants] have right to form blocks." [48]. This solves the problem of identification, there is applied principle called KYC (know your customer). Only real persons are allowed to participate in the system. "Formation of blocks is not tied to the platform of the organizer of the auction and the auction lot," [48] this means that the centralized authority does not have possibilities to influence the process of the auction and the results. "The fact of registration of the user on any auction lot should be registered and easily verifiable." [48]. In such a case, the system comprises the unique users, unique sellers, and unique lots.

"At the first stage the fact of payment of the registration fee on a particular Lot in the System should be displayed by decentralized database of the bank statement, signed by electronic digital signature of the registrar's bank, which the Platform should receive at the end of Lot's exposition period from its registrar bank. Each Platform independently performs integration with its registrar bank to obtain extracts on the Lot in automatic mode." [48]. This approach constitutes redistribution of power. The governmental institution is not a monopolist anymore. Its functions are held by private companies (platforms), however, it does not mean private monopoly. The private platforms execute governments' duties through protocols, and get renumeration for it. There is no restrictions on the platforms which want to provide such services (i.e. no territorial restrictions).

Another proposed potential scenario of achieving the consensus tends to more 'traditional crypto graphical' views on the blockchain. It does not need any registrar bank in the procedure. "Platforms and the Participants who integrated their relationship with crypto-currency systems can pay and receive

payments of the registration fee. In this case the payment should be confirmed by an extract and a Platform's digital signature."[48] However, this option currently is not available due to the regulation uncertainty in the field of cryptocurrency law framework.

In relation to technical concepts of ledgers, the following blockchain which underpins the eAuction 3.0 is public permissioned ledger. This means that new participants can join the network after they satisfy pre-determined set of requirements (i.e. registration fee, deposit for the lot).

This is done using the login and password, received by the Organizer or the Participant through account registration at the Platform of the e-auction system. In this case the Platform bears legal responsibility for the compliance of the user's registration and documents data in the system. The private key (wallet) received with the account can be stored at the Platform (then there will be binding with a concrete platform) or at the removable device of the Organizer/Participant (then one can work at from platform) [48].

In regards to registration fee there are strict rules provided by software code. The participants' bids on the lot are only accepted in terms of payment of the registration fee. The bank confirms such transactions by statement with bank's electronic digital signature (EDS). The system prevents the participation without completed conditions on the identification of participants. For certain lots (e.g. sales of the enterprises) there is requirement to ensure the participation by security deposits. Participants transfer money on integrated within the system bank account (separate bank, not the same which accepted registration fees). Likewise in case of registration fees, the bank guarantee confirms such transactions by statement with bank's EDS. Every single transaction and change of state is recorded on the blockchain.

3.5 Main peculiarities of blockchain-based smart contracts within the decentralized auction system

As there were discovered in the previous part of the paper, smart contract is rather softaware code which contains pre-defined rules. "From a technical point of view, the contract of the electronic auction should be a kind of email address in an environment of decentralized electronic auction, which has its own executable code and is run with the help of this code.", explained by the developres [48]. The activation of this code should be available for any participant who made external transaction with regard to the contract to the address of the contract (i.e. paid required registration fee, placed the security deposit). If the addressee posted the transaction will be another contract (i.e. input, produced by calculations, bank confirmations etc.), then the contracts should be able to exchange a certain numbers of tokens, but if the contract still will be a final recipient then execution of the code of this contract should be activated (triggered).

In general auction procedure is regulated by a set of rules. These rules are being formalized into software code to compose the architecture. Hence, the rules become accurate and automated (i.e. no

ambiguity within the procedure). The same input always generate the same output. Particularly, auction's electronic contract code should provide:

- start of the auction trading on the date and time indicated by the Organizer of the auction;
- end of auction trading on the date and time indicated by the Organizer of the auction;
- registration of the related contract on the registration of the auction bid (i.e. registered participants receive the address with private/public key and user's account);
- verification of compliance of the bid with the minimum value of the auction bid (provided in a deterministic manner <if>, <then>, only proper input leads to output);
- verification of compliance of the bid with the minimum and maximum value step growth rate of the auction bid;
- definition of a candidate to the winner of the auction on the related contracts with the auction bids and contracts to exit the auction (i.e. the highest bidder is determined by machine due to placed bids).

Furthermore, the compositions of the additional attributes (tags) of the auction electronic contract necessary for the implementation of these requirements are the name of the auction lot; the description of the auction lot; a reference to the image of the auction lot; picture hash of the auction lot; a reference to the documentation of the auction lot; documentation hash of the auction lot; date and time of the auction bidding start; date and time of the auction bidding; minimum starting price; minimum step of the auction price; maximum step of the auction price; the current price of the auction lot. Mentioned toold are sctrictly provided by the system architecture. This allows standardizing the procedure, making mechanism of the sale more transparent, accurate. The result of the bidding procedure is accurate, all transactions recorded on blockchain within bidding are reliable and immutable.

The transactions within decentralized auction system are recorded, stored and verified on the blockchain. The system uses traditional cryptographical tools (which were described in the Part 1 of this paper), so that each transaction of the decentralized electronic auction contains a hash signed (akin fingerprint) by previous transactions initiator in such a way that the previous transaction becomes the "entrance" for the current transaction. The public key or the address of the new recipient ("exit") is indicated. The system automatically checks the validity of digital signatures, which users apply to send transactions (inputs in kind of payments, bids etc.). It is impossible to cancel a standard transaction, even with the apparent error or fraud [48] (i.e. it will be stored on blockchain unchangeably).

The collected transaction are being included into block which are added to the ledger (the structure of transactional blocks is explained in the Part 1 of this paper). The recorded transactional blocks does not allow to alter any transactions included into these blocks. The blockchain is encrtypted (SHA-256 function

[59]) and secure, at the same time, the transactions are not encrypted, that allows to verify the information faster.

Every created block is supposed to comprise 250 transactions. The period of block creation (i.e. therefore blockchain verification) is 2 seconds, so that one minute allows to create 30 blocks with 7500 transactions [48]. Likewise every distributed ledger these blocks are marked with validated time stamp. For the security purposes (i.e. to prevent Denial-of-service attacks, which are aiming to create obstacle for users to the system) block has some limitations: it may contain up to 10 % of transactions on new participant registration, and no more than 30 % of transactions on new lot registration, the rest of these transactions is supposed to compose the next block. Each new block begins with transactions, which executes the renumeration to nodes (computers) which participate in the process of the reaching the consensus. Every transaction has digital signature linked to the content of this transaction including time. All the digital signatures are verified for purposes of adding new block to the ledger. The conditions of transactions inclusion into new block are strictly related to validity of digital signature, and requirements to particular lot (e.g. statement on security deposits attached by digital signature of the bank, registration fee). Every time the block is recorded on the chain – the whole ledger is verified [48].Each new block is considered to be an additional "proof" of transactions from the previous blocks.

3.6 Implementation of the decentralized auction mechanism into current system

In this subsection the discussion points to implementation of the decentralized auction system eAuction 3.0 into existing relationships within the scope of state property lease and sale.

The team which developed the software also drafted the law [70] to regulate the new emerged relationships within proper approach. The provisions of the draft specify usual conditions to ensure the auction procedure (principles, definitions, scope etc). It is notable to mention the rules provided by code are completely identical (at least by effect which they supposed to cause) to the future legislation act provisions.

In view on law draft there was elaborated instruction (substitute law) [71] for local administrative entities for the purposes of municipal property sale and lease. It became possible due to recent changes into the legislation on local executive entities, which granted 25 Ukrainian districts more autonomy to manage within their capabilities. By today (2 Jan 2017) the memorandum [74] on the adoption the decentralized auction system eAuction 3.0 was signed by 8 cities (district centers) and 7 governmental bodies (Fund on deposits guarantee, The Ministry of Agricultural policy, State Land Cadaster etc).

In addition, the decentralized auction system is attached with contract patterns which are aiming to support the proper implementation within existing procedures. These documents are available open source

(so that everybody can access it on the internet with no restrictions). For example, there was drafted pattern [72] for agreement between platform (operator) and organizer (seller). The object of that contract is services provided by platform to ensure the proper work of the system, the provisions of the contract are linked to the corresponding provisions of supposed legislation and substantive laws. Another contract pattern [73] (which is also available open source within the system) is contract to put in order relationships between bank and the platform (operator). Particularly, it relates to opening a new bank account, and other provisions which are aiming to ensure the functioning of the decentralized auction system.

The mentioned entities have tested the system. However, legislation requires the decision of local council to entire implementation of the decentralized auction system. The system is expected to be launched in 2017 within the framework on current reforms. The core thing which deter the full implementation is lack of adopted law, however, the draft [70; 71] and all supporting documents are drafted.

Above all, the decentralized auction system provides significant part for the state and municipal property lease and sale, which particularly digitizes the phases of lot registration, exposition, electronic trade. However, the conclusion the traditional contract with the winner is still remains. The novelty is caused by recognizing blockchain data as grounds to conclude the contract with the auction winner. Another key thing to notice is possibility to present data taken from blockchain before the court in case of dispute.

It seems rational, that the innovation recognized by public sector actors who launched decentralized auction system supported by blockchain technology, for encouraging the further development of the technology. In conclusion, the innovation is moving forward step by step to its adoption by increasing number of businesses, governments.

CONCLUSIONS

Information Age Technologies offer both opportunities and challenges for the socio-economic life of mankind. Certainly the legal realm should be prepared, along with an elaborate comprehensive approach to these new relationships and adaptation of legal services to understand and respond to human problems. At the same time, lawyers may embrace innovative changes within digital dimensions to find productive solutions. A review of technical concepts such as blockchain technology is necessary to understand the revolutionary potential with regards to value exchange, formalization of law etc.

1) The technological advances which underpin cryptocurrencies (e.g. Bitcoin) enable secure control of ownership over digital units. Complexity of hardware improvements, cryptographic features, protocols, mathematics and the game theory force us to rethink value transfer between individuals which are lacking trust within the digital world. Blockchain technology can potentially eliminate the need for centralized intermediaries in the world of digital payments by deploying mathematical certainty, which provide users with core benefits such as cost cutting, speed, clarity etc.

2) Blockchain stores immutable reliable data collection with timestamps, however, it is not just a database. It can execute software code in a decentralized manner. In other words, a set of computers on a peer-to-peer basis can run and verify the same code to facilitate real-time execution and validation of transactions. There is no single point of failure since each computer has its own copy of the storage and constantly synchronizes it amongst the network. Moreover, attacks on such network are unreasonably costly in practice because the system is highly resistant to hacks. So it is therefore impossible to alter data recorded on blockchain.

3) Smart contract is just software code with programmed logic, however, it is possible to turn certain contractual clauses into code to facilitate enforcement of rights and obligations between multiple parties by a set of distributed computers. Parties may conclude a contract and attach their agreement with smart contract terms (readable by machine) to ensure predictable automated enforcement by a “trusted computer” and avoid third party involvement. Smart contracts enhanced with blockchain conceptually differ from traditional electronic contracts since the digitized terms are being enforced due to specific protocols in a decentralized manner.

4) In a more general sense, a blockchain-based smart contract is any script or piece of code recorded unchangeably on blockchain. Such smart contracts could be triggered by particular transactions (signed by corresponding cryptographic signatures), they are able to communicate to other smart contracts and machines. The range of use allows embedment into code, from simple transactions to sophisticated

algorithmic structures. There are elaborated special platforms (e.g. Ethereum project) to simplify the creation and execution of smart contracts.

5) Relevance of blockchain technology application depends on a particular situation. It is also important to take into consideration properties and attributes proposed by different blockchains so that the blockchain implications varies from financial services, data integration, to creation of decentralized governance. Smart property concept is an important category with regards to operating digital assets (digital units also may represent physical objects, access to certain resources etc) on the blockchain.

6) The blockchain technology finds its application in private as well as public sectors. In the first case, there are numerous startups aiming to elaborate creative solutions with regards to alternative payment systems, copyright titles etc. Also large consortiums of banks are trying to deploy blockchain technology to enhance their services. In case of governments, blockchain technology is deemed innovative, however, there are several countries attracted by blockchain technology implications. States see the blockchain technology application improvement in transparency, efficiency, accountability, saving budget costs etc.

7) Ukrainian auction systems on state and municipal property lease and sale appear to be a good example for blockchain deployment considering there is an applied "first-price auction model". The auction, run by single governmental institutions, allows manipulation within the non-transparent system. The level of trust to corrupted centralized government is extremely low as long as some users can exploit the rules and procedures. Blockchain technology promises to replace algorithmic actions of centralized entities which ensure the procedure of auctioning.

8) Regarding reforms to pursue transparency and efficiency, there was elaborate decentralized auction system called eAuction 3.0. The new platform, which applies blockchain-based smart contracts, is aiming to establish clear rules and conforming architecture for the auction procedure. Particularly, users may enjoy full transparency during lot registration, authorization, bidding, and fair results. Automated smart contracts control the procedure and calculate proper results. The functions of maintaining the blockchain are outsourced among different private platforms which are incentivized to run the software, hence the state budget is released from duty to support expensive centralized database.

9) There still remains the paper work of concluding the final contract with the auction winner. However, the great achievement is recognizing the data recorded on blockchain as grounds for conclusion of contracts. Moreover, the data recorded on blockchain regarding auction phases could be used as evidence at state court.

10) There were drafted corresponding legislation to support the mechanism. But the key point is that the adoption of the eAuction 3.0 platform is made to a bottom-up method. The memorandum and substantive regulations already signed by local administrations of 10 cities as well as 7 governmental bodies (each time the system was successfully tested). It seems to be a reasonable approach to start blockchain-

based platform implementation into existing systems through public authority approvement. Step by step, the technology recognized by public sector is tempting to be developed in general.

However, it is only the very beginning of embracing the blockchain technology by various industries. The limits are unknown yet. There are many technical issues which remain. The regulatory uncertainty deters the massive adoption. Above all**,** the recommendations of the paper are summarized as follows:

1) The blockchain technology evolved from cryptocurrency invention. Presently, many blockchains are attached with internal cryptotokens which aim to ensure security and privacy of the network. Experts experiment with different variations of blockchains to explore the best solutions so the wider audience accepts cryptocurrency ideas. The issues on privacy and security are closely tied with identity determination within blockchains and it raises reasonable questions due to proper blockchain technology applications.

2) There is no regulatory certainty about the information stored on various blockchains. It heavily depends on particular situations regarding the access to the data validation and storage. It will certainly take time for an extensive common approach to blockchain capabilities on data collection.

3) The ownership and transfer of digital assets (as well as physical objects translated into digital realm; i.e. smart property) within blockchain is challenging regarding traditional value transfer. It should be deeply investigated to reach the adoption by existing framework.

4) New smart contracting solutions require lawyers to be prepared to look for matching legal solutions. Particularly, it relates to representing contractual clauses (not always written) by bits of code, looking for appropriate linking law part with programming part to pursue legally binding efficient enforcement of rights and obligations. There are increasing challenges for copyright, consumer protection fields, jurisdiction etc.

5) Also, the further research in the area of blockchain-based smart contracts may include designing agreements between multiple parties in order to regulate relationships in a decentralized manner, collaborate people etc. In any case, algorithmic thinking is required to acquire basic proficiency.

6) The decentralized system eAuction 3.0 developed in Ukraine is promising in order to bring transparency and efficiency to particular public services spheres, however, it takes time for full adoption through bottom-up method and rig by legislation.

Current research confirms the need to continue to identify more issues and propose solutions to overcome blockchain specific features as a decentralized ledger, which is transparent and trustless. Obvious benefits are encouraging to develop blockchain based applications beyond cryptocurrency systems. For some blockchain applications it is tempting to wait for regulatory framework (e.g. financial services). At last, further research in the field of transactions executed and recorded on blockchain must take into account evaluation of effectiveness and necessity of the proposed solutions within private and public sectors.

SUMMARY

The rapid technological advances within digital dimensions are causing people to reimagine socio-economic relationships in fundamental ways. Innovations constantly create new questions in traditional areas of law; therefore technology and law are becoming much closer. The most important recent innovation in digital transactions is blockchain technology. Therefore,understanding the increasing range of blockchain implications is required in new emerging areas of law practice.

In regards to effectively exploring blockchain application and its full potential, I completed the following tasks: (1) systematically reviewed existing literature regarding blockchain technology, including academic papers and various reports; (2) learned the basic technological vision of blockchain features and the ability of customizing them in particular applications; (3) discussed how blockchain technology may shift the paradigm of trust and decentralization in digital environments, like elimination the need for trusted third parties; (4) examined the concept of smart contracts, which are run on blockchain as tools for value transfer transactions and digitizing; (5) focused on smart contracts as solutions for the efficient automation of enforcing–legal rights and obligations; (6) considered the concept of decentralized eAuction 3.0 supported by blockchain-based smart contracts, which are run by Ukrainian governmental institutions; and other related tasks.

The research was conducted by applying research methodology (e.g. logical analyze method, genetic method, comparative method, synthesis method). Due to the novelty of blockchain technology, to be aware of general directions of investigation I communicated with pioneering specialists, who are proficient in blockchain technology and its implications within various industries. The paper comprises three parts, which sequentially uncover blockchain technology's underpinnings, opportunities facilitated by these technological implications, and potential legal consequences of deploying blockchain solutions. The last part of the paper explains how mentioned technology may reshape the auction systems run by government institutions, by reaching transparency, efficiency, and clear rules through mathematical certainty.

Current research appears to validate the view that blockchain technology is revolutionary, regarding its ability to securely transfer value over the digital realm. This aspect of blockchain application facilitates automation, speed, cost-cutting, etc. Moreover, blockchains can be viewed as decentralized storages with immutable reliable data on executed transactions. Hence, blockchain technology, combined with the smart contracts concept, may potentially have an effect on regulating relationships both in digital and real world realms.

All things considered, there are numerous blockchain technology applications, primarily in the area of value transfer, payments, etc. But the technology offers a significantly wider range of applications, which is not clearly seen due to technological peculiarities and lack of regulatory uncertainty. In each case, the

blockchain implications must be evaluated based on its relevance; as long as it is more than just an efficient database, it is not a solution for random problem; blockchain has may replace or contribute trustworthy transactions. Blockchains combined with smart contracts may change the way contractual clauses are enforced. However, the legal realm should be prepared to properly meet challenges far beyond contract law. Digitized algorithmic rules executed and stored on blockchain are promising to make regulation possible by decentralized architectures. Thus, the Ukrainian decentralized auction system, which is run by the government, is an example of combining legal construction with blockchain technology features, which notably differs from its centralized analogues.

LIST OF SOURCES

I LEGAL ACTS

1. UNIDROIT Principles, 2010.
2. Draft Common Frame of Reference (DCFR), 2009.
3. Principles of European Contract Law, 2002.

II SCIENTIFIC LITERATURE

Published books

4. ANTONOPOULOS, A. 2014. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol, CA: O'Reilly Media.

5. EASLEY D., AND KLEINBERG, K. *Networks, Crowds, and Markets: Reasoning about a Highly Connected World.* (Chapter 9. Auctions). Cambridge University Press, 2010, pp.249-273. Available at: <http://www.cs.cornell.edu/home/kleinber/networks-book> [Date accessed on 4 December 2016].

6. HAYEK, F.A.*The Denationalisation of Money The Argument Refined.*: Institute for Economic Affairs. London, 1978.

7. KERIKMÄE, T., & RULL, A. *Future of law and e-technologies*. Cham, Switzerland: Springer, 2016.

8. MOUGAYAR, W. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*, 2016, 208 pp.

9. NARAYANAN, A., BONNEAU, J., FELTEN, E., MILLER A., AND GOLDFEDER, S. *Bitcoin and Cryptocurrency Technologies*:A Comprehensive Introduction Princeton University Press, 2016 , 336p.

10. SWAN, M. *Blockchain: Blueprint for a New Economy*. Sebastopol, CA: O'Reilly Media, 2015.

11. Tapscott, D., & Tapscott, A. *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. New York: Portfolio / Penguin, 2016.

12. Wattenhofer, R. *The science of the blockchain*. Erscheinungsort nicht ermittelbar: Inverted Forest Publishing, 2016.

Scientific articles

13. AINSWORTH, R. T., & SHACT, A. *Blockchain (distributed ledger technology) solves VAT fraud*. Boston: Boston University School of Law Law & Economics Working Paper No. 16-41, 2016, Available at: <http://www.bu.edu/law/faculty-scholarship/working-paper-series/> [Date accessed on 10 January 2017].

14. ATZORI, M. *Blockchain Technology and Decentralized Governance: Is the State Still Necessary*? SSRN, 2015. Available at: <https://ssrn.com/abstract=2709713 or http://dx.doi.org/10.2139/ssrn.2709713> [Date accessed on 10 January 2017].

15. BECK, R; STENUM CZEPLUCH, J.; LOLLIKE, N.; AND MALONE, S. *Blockchain – the gateway to trustfree cryptographic transactions*. Twenty-Fourth European Conference on Information Systems (ECIS), İstanbul,Turkey, 2016. Available at:. <http://aisel.aisnet.org/ecis2016_rp/153>[Date accessed on 10 January 2017].

16. BHARGAVAN K., et al. *Formal Verification of Smart Contracts*. Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, Vienna, 2016, p.91-96.

17. BONNEAU, J., MILLER, A. CLARK, J., NARAYANAN, A, J. A. KROLL and E. W. FELTEN. *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*. IEEE Security & Privacy. San Francisco, 2015.

18. BOURQUE S., TSUI, S. F. L., *A Lawyer's Introduction to Smart Contract*. Scientia Nobilitat ReDate accessed Legal Studies, Lask, 2014, pp 4-23.

19. BÖHME, R., et Al. *Bitcoin*. Boston: Harvard Business School, Journal of Economic Perspectives, 2014.

20. CHRISTIDIS, K., DEVETSIKIOTIS, M. *Blockchains and Smart Contracts for the Internet of Things*. IEEE Access, vol. 4, no. , pp. 2292-2303, 2016. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7467408> [Date accessed on 10 January 2017].

21. CLACK, C.D., BAKSHI, V.A., BRAINE, L. *Smart Contract Templates: foundations, design landscape and research directions*. Barclays Bank PLC 2016, London. 2016. Available at: <http://arxiv.org/abs/1608.00771> [Date accessed on 10 January 2017].

22. CROSS, F. B., *Law and Trust*. Georgetown Law, Forthcoming. McCombs Working Paper No. IROM-05-05; U of Texas Law, Law and Econ Research Paper No. 064. Available at SSRN:<https://ssrn.com/abstract=813028> [Date accessed on 10 January 2017].

23. CHAUM, D.*Untraceable Electronic Cash*. Proceedings of Crypto 88, Springer-Verlag, vol 403, pp. 319-327, 1990.

24. FAIRFIELD, J, *BitProperty*. Southern California Law Review, Vol. 88, 2015, Forthcoming; Washington & Lee Legal Studies Paper No. 2014-17. Available at:<https://ssrn.com/abstract=2504710> [Date accessed on 10 January 2017].

25. DAVIDSON, S., DE FILIPPI, P., POTTS, J. *Economics of Blockchain*. 2016, available at: <http://ssrn.com/abstract=2744751> [Date accessed on 10 January 2017].

26. DELMOLINO K., ARNETT M., KOSBA, A., MILLER, A *Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab*. IACR Cryptology ePrint Archive 2015, 460.

27. DE FILIPPI, P., HASSAN, S.. *Blockchain technology as a regulatory technology: From code is law to law is code*. First Monday, [S.l.], nov. 2016. ISSN 13960466. Available at: <http://firstmonday.org/ojs/index.php/fm/article/view/7113/5657>. [Date accessed on 10 January 2017].

28. DE FILIPPI, P. *The interplay between decentralization and privacy: the case of blockchain technologies*. Journal of Peer Production, Issue n.7: Alternative Internets . (September 14, 2016). Available at: <https://ssrn.com/abstract=2852689> [Date accessed on 10 January 2017].

29. DUPONT, Q., MAURER, B., *Ledgers And The Law In Blockchain*. Kings Review. N.p., 2015. Web. 27 Mar. 2016.

30. HUCKLE, S., WHITE, M. *Socialism and the blockchain*. Future Internet, 8 (4). 2016, p. 49. Available at: <http://dx.doi.org/10.3390/fi8040049> [Date accessed on 10 January 2017].

31. YLI-HUUMO J, KO D, CHOI S, PARK S, SMOLANDER K.*Where Is Current Research on Blockchain Technology* – A Systematic Review. PLoS ONE 11(10), 2016, pp.1–27.

32. KIVIAT, T.I. *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*. Duke Law Journal, 2015, pp.569-608. Available at: <http://scholarship.law.duke.edu/dlj/vol65/iss3/4,> [Date accessed on 01 December 2016].

33. LENGWILER, Y., WOLFSTETTER, E. *Corruption in Procurement Auctions*. (Handbook of Procurement — Theory and Practice for Managers, Cambridge University Press). 2006. Available at:<https://ssrn.com/abstract=874705> [Date accessed on 10 January 2017].

34. MILLS, D., WANG, K., MALONE, B. et Al. *Distributed ledger technology in payments, clearing, and settlement.* Finance and Economics Discussion Series 2016-095. Washington: Board of Governors of the Federal Reserve System, 2016. Available at: <https://doi.org/10.17016/FEDS.2016.095> [Date accessed on 10 January 2017].

35. LESSIG, L. *The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation*. COMM LAW CONSPECTUS, 1997. Available at: <http://scholarship.law.edu/commlaw/vol5/iss2/5> [Date accessed on 10 January 2017].

36. PERUGINI, M.L., DAL CHECCO, P. *Smart Contracts: A Preliminary Evaluation*. 2015. Available at : <https://ssrn.com/abstract=2729548>[Date accessed on 10 January 2017].

37. REIJERS, W.; O'BROLCHÁIN, F.; HAYNES, P. *Governance in Blockchain Technologies & Social Contract Theories*. Ledger, [S.l.], v. 1, p. 134-151, dec. 2016. Available at:

<http://www.ledgerjournal.org/ojs/index.php/ledger/article/view/62>. [Date accessed on 10 January 2017].

38. REYES, C.L., *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation*: An Initial Proposal, 61 Vill. L. Rev. 191 (2016). Available at: <http://digitalcommons.law.villanova.edu/vlr/vol61/iss1/5> [Date accessed on 10 January 2017]

39. RIEFA, C. *Recommended changes to the definitions of "auction" and "public auction" in the proposal for a directive on consumer rights.* European Consumer Protection: Theory and Practice. Cambridge: Cambridge University Press, .2010. Available at SSRN: <https://ssrn.com/abstract=1679677> [Date accessed on 10 January 2017].

40. SAVELYEV, A, *Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law*. Higher School of Economics Research Paper. 2016. Available at SSRN:<https://ssrn.com/abstract=2885241> [Date accessed on 10 January 2017].

41. SCHROEDER, J.L., *Bitcoin and the Uniform Commercial Code*, 24 U. Miami Bus. L. Rev. 1 (2016) Available at: <http://repository.law.miami.edu/umblr/vol24/iss3/3> [Date accessed on 10 January 2017].

42. SWANSON, T. *Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management*. Kindle Edition. 2014. Available at: <https://s3-us-west-2.amazonaws.com/chainbook/Great+Chain+of+Numbers+A+Guide+to+Smart+Contracts,+Smart+Property+and+Trustless+Asset+Management+-+Tim+Swanson.pdf> [Date accessed on 10 January 2017].

43. SZABO, N. *Formalizing and Securing Relationships on Public Networks.* First Monday, [S.l.], sep. 1997. ISSN 13960466. Available at: <http://firstmonday.org/ojs/index.php/fm/article/view/548/469>. Date accessed: 12 Jan. 2017.

44. VOGEL, N. *The great decentralization: how WEB 3.0 will weaken copyrights*. John Marshall Review of Intellectual Property Law, Vol. 15, No. 1, 2016. Available at: <https://ssrn.com/abstract=2738357> [Date accessed on 10 January 2017].

45. WERBACH, K.D., *Trustless Trust.* 2016. Available at SSRN: <https://ssrn.com/abstract=2844409> [Date accessed on 10 January 2017].

46. WOOLSEY W.W. *Full privatization of currency in a nearly conventional money and banking system*. Cato J 11(1):86–87, 1991. Available at: < https://object.cato.org/sites/cato.org/files/serials/files/cato-journal/1991/5/cj11n1-6.pdf> [Date accessed on 12 January 2017].

47. WRIGHT, A., DE FILIPPI, P., *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* . Rochester, NY: Social Science Research Network, 2015. Available at SSRN:<https://ssrn.com/abstract=2580664> [Date accessed on 10 January 2017].

III Reports and other documents

48. ANTADZE L. et Al. *Decentralised System of Blockchain - Auctions eAuction* https://github.com/idfgithub/e-Auction-3.0/wiki [Date accessed on 10 January 2017].

49. BROWN R. G., Introducing R3 Corda: A distributed ledger designed for financial services, 2016. Available at: <http://r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributedledger-designed-for-financial-services> [Date accessed on 10 January 2017].

50. BURGESS, K., COLANGELO, J. *The Promise of Bitcoin and the Blockchain.* Report. Consumers' Research, Bretton Woods, 2015. Available at:< http://bravenewcoin.com/assets/Industry-Reports-2016/Bretton-Woods-2015-White-Paper-The-promise-of-Bitcoin-and-the-Blockchain.pdf>

51. BUTERIN, V. Ethereum Whitepaper. A Next Generation Smart Contract & Decentralized Application Platform. 2014. Available at: <https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf> [Date accessed on 10 January 2017].

52. CHAMPAGNE, P. (2014). The Book Of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto.

53. COLLINDRES, J. Regan, M. et Al. *Using Blockchain to Secure Honduran Land Titles* (casestudy), Available at: < https://s3.amazonaws.com/ipri2016/casestudy_collindres.pdf> [Date accessed on 12 January 2017].

54. CONDOS, J., SORRELL, W.H., DONEGAN, S.L., *Blockchain technology: opportunities and risks*. (A report of findings and recommendations concerning the potential opportunities and risks of creating a presumption of validity for electronic facts and records that employ blockchain technology and addressing any unresolved regulatory issues.) Vermont, 2016.

55. DELMOLINO K., ARNETT M., KOSBA, A., MILLER, A. *A Programmer's Guide to Ethereum and Serpent*, 2015. Available at:< https://www.cs.umd.edu/~elaine/smartcontract/guide.pdf>. [Date accessed on 10 January 2017].

56. GARZIK, J. *Public versus Private Blockchains Part 1: Permissioned Blockchains* White Paper BitFury group. Available at: <http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1–1.pdf> [Date accessed on 10 January 2017].

57. GRANT T., R3 & Distributed Ledger Technology , Available at: <https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/10.40%20D%20Grant.pdf>

58. DAI, W. B-money [1998]. Retrieved: 29 April 2015. URL: http://www.weidai.com/bmoney.txt.

59. NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf [Date accessed on 12 January 2017].

60. PINNA A., RUTTENBERG, W. *European Central Bank, Occasional Paper* No. 172, *Distributed ledger technologies in securities post-trading*. 2016, available at <https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf> [Date accessed on 10 January 2017].

61. SAMS R. statement re: Blockchain Available at: http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/tac022316_sams.pdf [Date accessed on 10 January 2017].

62. SWANSON, T.. *Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger systems*. Report, Apr. 2015. Available at: <http://www.ofnumbers.com/ wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf> [Date accessed on 10 January 2017].

63. SZABO, N. *The Idea of Smart Contracts*. 1997. Available at: < https://perma.cc/V6AZ-7V8W> [Date accessed on 10 January 2017].

64. SZABO, N. *Bit-gold*. Available at: <https://unenumerated.blogspot.co.at/2005/12/bit-gold.html> [Date accessed on 10 January 2017].

65. SZABO, N. *The God Protocols*. 1997.Available at: < http://nakamotoinstitute.org/the-god-protocols> [Date accessed on 12 January 2017].

66. Berkeley report on blockchain, Sutardja Center for Entrepreneurship & Technology Technical Report, Date: October 16, 2015. Available at: < http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf>. [Date accessed on 10 January 2017].

67. *MySQL Reference Manual Using Stored Routines (Procedures and Functions)*, accessed on Mar. 15, 2016. Available: http://dev.mysql.com/doc/refman/5.7/en/stored-routines.html

68. UK Chief Scientific Advisor, '*DLT'* Government Office for Science 2016. Available at <https://www.gov.uk/government/uploads/> [Date accessed on 10 January 2017].

69. WEF (Davos) 2016: *An ambitious look at how blockchain can reshape financial services. Report,* Part of the Future of Financial Services Series, World Economic Forum 2016. Available at:<http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf>

IV Sources in Ukrainian Language.

70. ПРОЕКТ ЗАКОНУ УКРАЇНИ «*Про систему децентралізованого аукціону*». Available at:<https://drive.google.com/open?id=1eoy7Cxqfl1NzkK8UlHXCe_AP582PXfdm5RpsqqI572w>

71. ПОЛОЖЕННЯ "*Про порядок продажу та передачі в оренду майна і майнових прав, земель, що є комунальною власністю територіальної громади «N» із застосуванням системи децентралізованого електронного аукціону*» (2016). Available at:<https://docs.google.com/document/d/1jB5WEao_vfIypFzCmhxwV7WXfR3fSPVcmNCAZl9fp2U/edit>

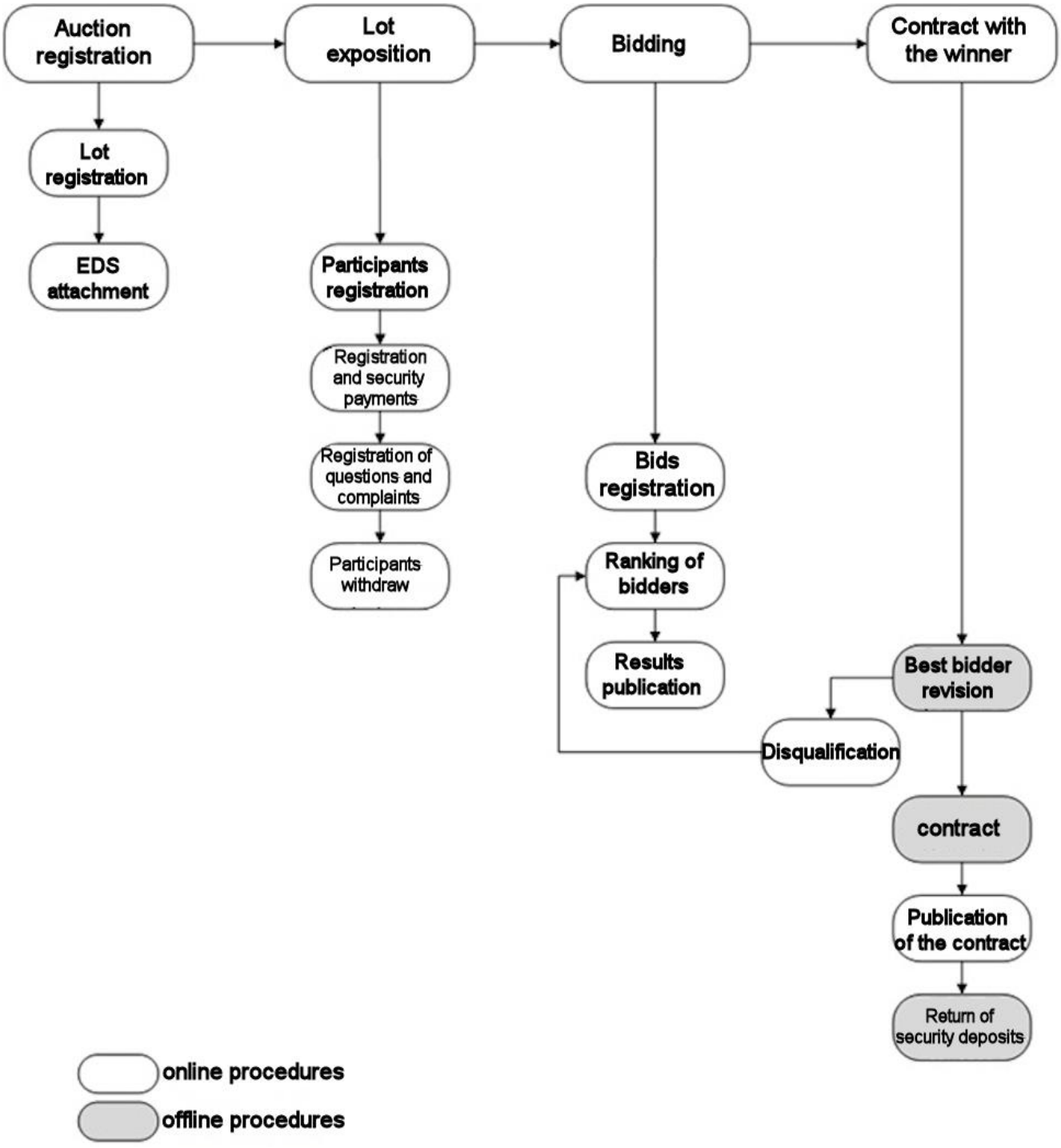
72. ТИПОВИЙ ДОГОВІР *про використання системи децентралізованого аукціону*. Available at:<https://docs.google.com/document/d/1RoFUbcgQD9rUGP08k3jZgkZuSchjDvjJJIoy4oVsGFA/edit

73. ДОГОВІР *про відкриття банківського рахунку для підтримання функціонування системи децентралізованого аукціону*. Available at: <https://docs.google.com/document/d/1sVPgYgI7ES1B5_zjcm1V_Y0w2-4dyQ-A7NkriuJ-1CY/edit>

74. МЕМОРАНДУМ *щодо розвитку та імплементації системи децентралізованого аукціону* (Memorandum on Development and Implementation of the Decentralized Online Auction System). Available at: <https://docs.google.com/document/d/1A2COHwAVf0uD36_FocsgqlMwBNWxkdfU2mvwxGndurQ/edit>

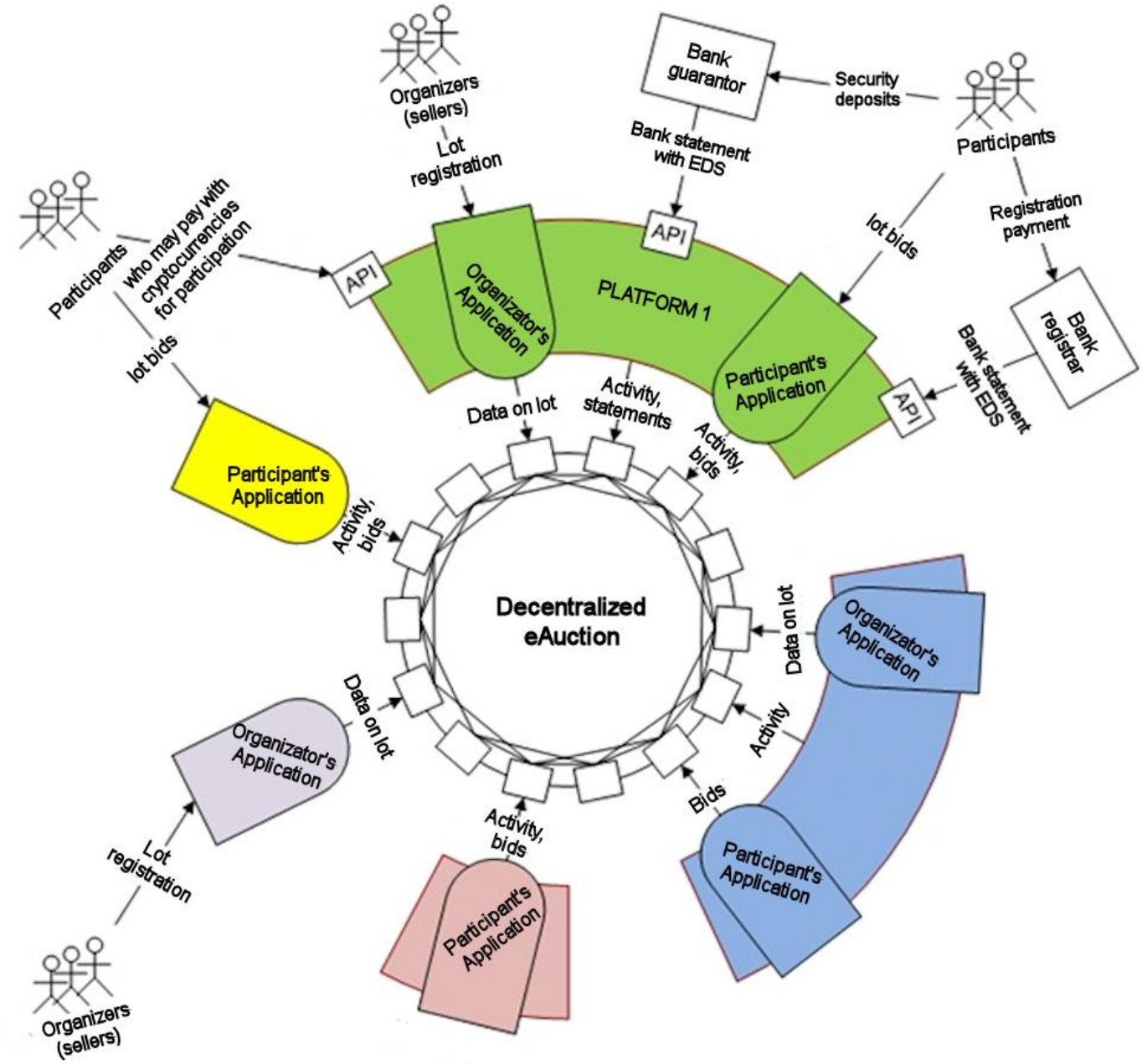
ANNEXES

Appendix 1. **Phases of decentralized auction system** [18]



[18] The scheme is provided by the developers of the decentralized auction system

Appendix 2. **The architecture and main element of the decentralized auction system** [19]



[19] The scheme is translated due to the source provided by the developers of the system. More information available at: http://www.eauction.idf.solutions/

[20] EDS – electronic digital signature