MACIEJ HULICKI[1]

PAWEŁ LUSTOFIN[2]

USE OF THE BLOCKCHAIN CONCEPT IN THE PERFORMANCE OF CONTRACTUAL OBLIGATIONS[3]

1. INTRODUCTION

We are now living in the digital revolution, also referenced by some as the digital transformation. It would not have develop was it not for the technical tools for data transfer, processing speed and availability of mobile devices. At present, the greatest hope is placed in such techniques and technologies as: *Internet of things*, *3D printing*, *augmented reality*, *artificial intelligence* and *machine learning*, *big data*, coupled with the concept of distributed databases in the form of *blockchain*, which tends to come under the name of *disruptive innovation*[4] - the subject matter hereof. All these technical tools imply major changes in our daily environment and are, at the same time, highly complex. We believe this calls for a thorough legal analysis.

In late 2015 the World Economic Forum published a report on breakthrough technologies ("Deep Shift - Technology Tipping Points and Societal Impact"). It contained the opinions of more than 800 managers and experts and ranked 'Bitcoin and Blockchain' 16th[5]. Since 2015, blockchain concepts and their use in many areas of the economy has established its potentially importance in public awareness. Every year, the World Economic Forum's New Technologies Council, in collaboration with Scientific American magazine, ranks the most groundbreaking technologies (The Top 10 Emerging Technologies 2016 list) with the paramount impact on life enhancement, transformation of various sectors of the economy, and environmental protection. In 2016, the third place in this ranking was taken by the concept of a distributed 'blockchain' database[6]. This coincides

[1] Assistant professor, Faculty of Law and Administration, Cardinal Wyszyński University in Warsaw.

[2] Doctoral student, Cracow University of Economics.

[3] Artykuł przetłumaczony ze środków finansowanych przez Ministerstwo Nauki i Szkolnictwa Wyższego na działalność upowszechniającą naukę (DUN), nr decyzji 810/P-DUN/2018. Article translated from funds financed by the Ministry of Science and Higher Education for the dissemination of science (DUN), Decision No. 810 / P-DUN / 2018.

[4] C.M. CHRISTENSEN, M. E. RAYNOR, R. MCDONALD, *What is disruptive innovation?*, Harvard Business Review, 12/1995.

[5] P. ROSATI, B. NAIR, T. LYNN; *Bitcoin Vs Blockchain: The Role of trust in disrupting financial services*; Proceedings of 7th European Business Research Conference 15 – 16 December 2016, University of Roma Tre, Rome, 10.2016, p. 1.

[6] O. CANN, *These are the top 10 emerging technologies of 2016*, World Economic Forum, available at:

with the surge in academic publications addressing and examining blockchain. A search of the 'Web of Science' database, which covers but a fraction of all scientific publications, returned 109 papers on this issue. Even such a small sample shows a discernible trend. More than 70% of publications were published in 2016, with more than 90% in IT, telecommunications and related areas. Given the potentially enormous impact on many areas of the economy, coupled with the development of the state and societies, research related to distributed blockchain databases is expected to further come into spotlight, on the one hand, and work will reach out for the areas beyond the IT area, on the other.

The article first outlines the concept of a distributed database in the form of a chain of blocks. Further on, its architecture and implementation are described, and then the potential legal consequences of its application in the area of law, with particular emphasis on *smart contracts,* are analysed.

2. BLOCKCHAIN SOLUTION CONCEPT

As already mentioned, breakthrough innovation is an innovation that creates new markets and value networks, replaces existing ones and eliminates existing market leaders, products and services. It should be emphasized that the blockchain concept is one of the leading and most promising technical solutions that are currently being developed, but it is difficult to predict whether it will also prove a breakthrough innovation for the time being. The financial sector was identified as the primary area of application of this solution (the blockchain concept has been used for the first time to form the basis of the Bitcoin currency). Conversely, this solution is more and more often claimed to be a tool to eliminate the imperfections of the current financial system, not an immediate threat to its main actors[7]. It should be noted that the financial sector appreciates the opportunities and potential importance of a distributed blockchain database, which has already been reflected in significant capital investments by institutions such as Santander, Citi Group or Barclays[8]. October 2015 saw 13 banks joining the consortium formed by start-up R3CEV along with 9 banks, primarily to develop a dispersed general ledger for the transfer of financial assets between financial institutions[9]. In late 2016 the consortium included app. 70 financial sector institutions[10]. The blockchain concept is expected to

[7] M. MASSIMO*, From 'Blockchain Hype' to a Real Business Case for Financial Markets*; Banca IMI; Bocconi University; 21.12.2016.

[8] K. MARZANTOWICZ, *Największe banki na świecie inwestują w Blockchain, podstawę Bitcoin*, available at: http://itwiz.pl/najwieksze-banki-na-swiecie-inwestuja-w-blockchain-podstawe-bitcoin; visited on 30.01.2017.

[9] Ibid.

[10] K. JEMIMA, *Exclusive: Blockchain platform developed by banks to be open-source*, Reuters UK, visited on 20.10.2016.

be of great importance not only for the financial sector, but also for many applications in the commercial and public services sectors. Moreover, looking ahead, this solution may materially bear upon the implementation of internal business processes (by way of illustration in the area of corporate governance), and also facilitated closer cooperation between companies within an extended supply chain. Before detailing out the potential applications of the dispersed database concept, one must highlight the features that distinguish it from other information processing techniques. The architecture of the distributed 'blockchain' database was first proposed by the creator of the first digital currency Satoshi Nakamoto in 2008[11] (Satoshi Nakamoto being a pseudonym for the author(s) of the first digital currency and the blockchain concept). The Bitcoin currency entered the market in January 2009. Bitcoin has been the first global system of electronic trading operations (purchase, sale), which is not based on confidence in a central institution (in the context of currency, the Central Bank is such an institution, responsible for creating money and controlling money supply in the economy). Lack of trust between system users has been eliminated via several complex cryptographic mechanisms such as: cryptographic *hash* functions to determine short and easy to verify signatures for any large data files, electronic signature using asymmetric cryptography, *consensus* building mechanism between system users[12] and time stamp. The opinion-forming weekly *The Economist* referred to the blockage concept as the "*trust machine*"[13]. The distributed ('democratic') bitcoin architecture allows each user to review the full history of the transaction while ensuring anonymity (in other words, the system users are visible under the public key number).

The 'blockchain' distributed database is a decentralized register of data stored in a chain of blocks. The data register is controlled by all users of the decentralised system. As already mentioned in the bitcoin system (based on the first 'traditional' blockchain solution), no central institution shall be responsible for its control. For the banking system, those are banks that play the role of trust institutions. Banks verify the correctness of transactions by, among other things, preventing double issuance of the same currency unit. On the other hand, Satoshi Nakamoto noted that transactions within the traditional financial system are not irreversible. In the event of disputes between transaction participants, banks and other financial institutions are the mediators. According to Nakamoto, this boosts the transaction costs. Transactions in the bitcoin system (and other public blockchain solutions)

[11] S. NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System.*

[12] Z. ZHENG, S. XIE, H.N. DAI, H. WANG, *Blockchain Challenges and Opportunities: A Survey*, International Journal of Electric and Hybrid Vehicles, 01.2017

[13] J. BERKLEY, *The promise of the blockchain The trust machine*, The Economist, 31.10.2015

are irreversible[14]. This concept has showed a material evolution since the first digital currency and the first implementation of the block chain.

Currently, three main types of blockchain solutions may be identified: public, corporate and private. They differ in particular in the degree of trust between system users, ranging from a total lack of trust in the public system to a relatively high level of trust in the private system, which is reflected in their different architecture. The only truly decentralized blockchain solution takes the form of an open-end public system. A private blockchain solution is fully controlled by one organisation and cannot be considered as decentralised, while the corporate system will only be partially decentralised. What else distinguishes the above solutions in technical terms is changing historical data. No change is allowed in a public system, while other systems allow it if the main users so wish.

3. DISTRIBUTED BLOCKCHAIN DATABASE ARCHITECTURE

This section will address the structure of a distributed database in the form of a chain of blocks, focusing on the bitcoin system as an example. Although it is the bitcoin solution that illustrates blockchain system processes, general rules apply also to other systems which use blockchain concept. As this concept is evolving to conform to specific applications, not all elements of the bitcoin system are present in other public systems that operate on a chain of blocks. As previously noted, the public blockchain system has a decentralized architecture[15].

For decentralised databases, their daily maintenance is carried out by a person acting as controller, who is often entitled to write and read data, which naturally creates the risk of abuse and manipulation. In the blockchain system, this risk is eliminated. The blockchain solution has been first used to exchange assets. In the blockchain system such transactions are performed by users who do not know each other, which implies a complete lack of trust. Such systems and mass-scale transactions, combined with no central institution in place responsible for control and security arises from a unique use of several cryptographic methods. In the bitcoin system, the user/owner who transfers currency units uses the *hash* function of the previous transaction and the public key of the subsequent owner to sign (this process is well illustrated in the diagram below)[16].

[14] S. NAKAMOTO, op. cit.

[15] See e.g. P. BARAN, *On distributed communication networks*, Rand Corporation, 1962, p. 4 (Fig. 1).

[16] S. NAKAMOTO, op. cit.

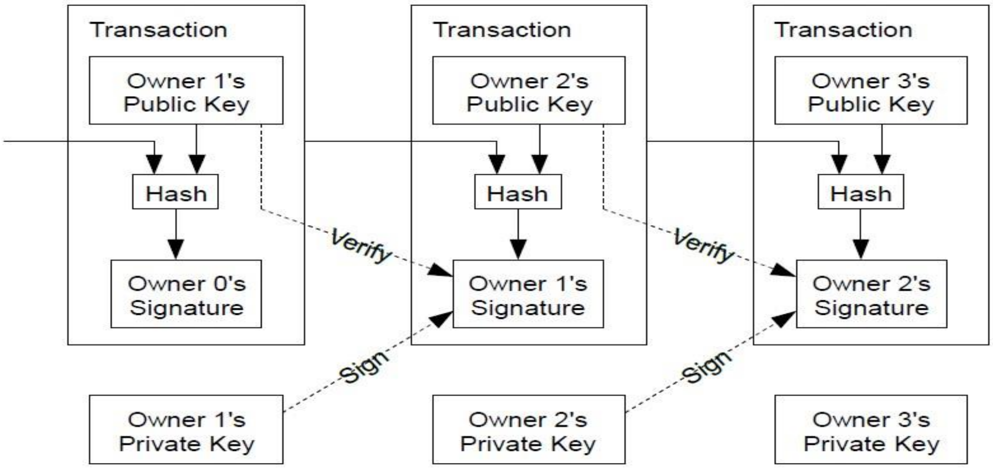

Fig. 1: Bitcoin transactions [Source: S. NAKAMOTO, Bitcoin: A Peer-to-Peer Electronic Cash System].

In a system missing a central institution responsible for verifying payments (avoiding double spending of the same currency unit), the acceptance of transactions is by *consensus*, meaning that more than half of the nodes must confirm the (commercial) operation and agree on the sequence of transactions. This is due to the public nature of the transaction registry which operates as a chain of blocks, and uses a *timestamp to* mark the time of operation. Every 10 minutes, *nodes* are collected in packages that form blocks.

A block must be verified by special *miners* whose combined computing power represents at least 51% of the total computing power of all miners in the system (which is equivalent to the consensus). The mechanism described is the so-called *proof-of-work* certificate, the basis for several operating mathematical algorithms used to reach this consensus in a decentralised system. After collecting the transactions in the block, specialized *miners* compete against each other in solving a mathematical task. The difficulty of the task is adjusted to the total computing power of these *miners* so as to ensure the validation of subsequent blocks at intervals of approximately 10 minutes. Once the mathematical problem has been solved, the block spreads in the system and its transactions are verified. Interestingly, such a specialized miner (data processing), which first solved a mathematical task, receives a salary. The incentive system is necessary to ensure a sufficient number of participants in the processing (information) process, which translates directly into the system security. The energy- and cost-intensive processing process is one of the drawbacks of the above certificate of processing. This issue will be explicated below. As Satoshi Nakamoto highlights, the remuneration system encourages the miners to act honestly[17]. Today, the total power of specialized miners is more than 1000 times greater than the power of the 500 largest supercomputers[18]. This demonstrates the high level of security of the bitcoin system, that is how much computing power and financial effort would be required to commit fraud. Satoshi Nakamoto lists the following phases of the bitcoin system:

1) new transactions are sent to all miners in the system,
2) each miner collects transactions in a block,
3) each miner seeks a processing certificate for its block,
4) after finding a solution, the block is sent to all other miners,
5) block acceptance only when all transactions contained in it are correct,
6) the proof of block acceptance is to start processing the following block, which assumes the *hash* of the accepted block[19].

Interestingly, successive blocks form an inseparable chain (which, among other things, proves that transactions in the system are irreversible). In practice, attempting to make a change in one of the blocks would force all subsequent blocks to be reconfirmed. The cryptographic "fusion" of blocks is very well illustrated by the drawing below.

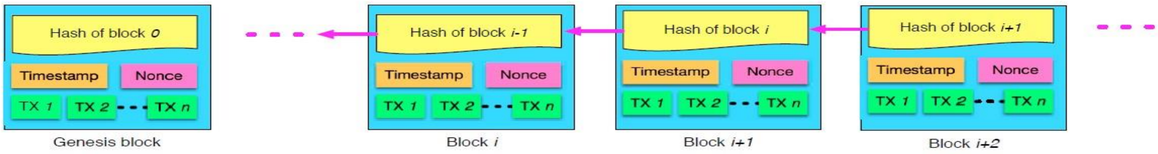

Fig. 2: Block chain structure [Source: Z. ZHENG, S. XIE, H.N. DAI, H. WANG, *Blockchain Challenges and Opportunities: A Survey*, International Journal of Electric and Hybrid Vehicles,

01.2017, p. 4]

The main alternative to *proof-of-work* is the *proof-of-stake* algorithm, with the richest node playing a dominant role. Using the participation certificate algorithm, it is assumed that the richest nodes are the least likely to be abused and stolen.

[17] Ibid.

[18] K. PIECH, *Leksykon pojęć na temat technologii blockchain i kryptowalut*, 08.11.2016, available at: https://mc.gov.pl/files/leksykon_pojec_na_temat_technologii_blockchain_i_kryptowalut.pdf.

[19] S. NAKAMOTO, op. cit.

Despite numerous advantages, at the present stage of development, the concept of blockchain is not free of defects, being considerably limited by its scalability, construed as the potential to process hundreds of thousands of transactions per second. For comparison, the bitcoin system currently executes about 7 transactions per second. Moreover, in order to validate new blocks, each system miner stores the entire transaction history. In the absence of absolute anonymity, it is a serious source of risk. Further, blockchain shall be susceptible to attack from machinery with a total computing power equivalent to at least 51% of the total computing power of the system[20]. It is important in view a centralization of miners in the bitcoin system. A similar phenomenon may possibly develop in other public blockchain systems. Centralisation contradicts the main idea (democratic character) of the blockchain solution. The phenomenon can also be observed in private systems (dominance of large companies). Another potential source of risk is the public nature of blockchain transactions. Algorithms, for establishing the consensus in the system, are not free of defects, that is their implementation (issue of a processing certificate) absorbs very high computing power and thus generates high costs. In turn, the *proof-of-stake* algorithm means that decision making is concentrated in the richest nodes.

4. APPLICATION OF THE BLOCKCHAIN CONCEPT

From the viewpoint of its function, the blockchain solution assumes the decentralization of various types of data registers as its the major advantage. What is more, thanks to the transparency of the above registers, people who are blockchain system users enjoy a full insight into the transaction history, which, combined with the use of consensus algorithms and cryptographic tools, makes the blockchain concept the basis for a stable and secure "value" exchange system (however, the risks briefly described in the previous paragraph must be considered). It follows that in a system an intermediary institution can be eliminated, whose primary goal is to ensure the security of the system and control the correctness of its internal developments. Was it not for the above institutions, people who did not know each other could not engage in large-scale cross-borders transaction until the first application of the blockchain concept, that is the bitcoin system. It is direct cooperation between foreign entities that makes the blockchain solution a breakthrough. As shown in the table below, the spectrum of application of this solution is very wide. Given the innovative nature of the solution, most of the applications presented below are still in the process of consideration or *proof-ofconcept* phase.

[20] Ibid.

The multitude of potential applications demonstrate importance of a thorough legal analysis of all events that may infer from the application of this solution.

Table 1 - Examples of blockchain applications

Area of application	**Illustratory application**
Banking, **Finance,** **Enterprise sector**	• *Peer-to-peer* financial markets (for instance trading of various types of assets, debt securities, etc.). As implied by the IBM survey, 15% of banks and 14% of institutions operating in financial markets plan to introduce a blockchain solution in 2017; 65% (out of 400 respondents) confirmed that they plan to implement the blockchain concept within the coming 3 years[21]. • Unified databases of transactions in banking systems (which should translate into a significant acceleration of transaction execution and reduction of operating costs in banking); • Opportunities for closer cooperation between companies[22,23] including closer cooperation in an extended supply chain[24.] Such an application may translate into cost optimization within the supply chain through better coordination of activities between cooperating companies; • *Open production networks* - a concept of full transparency within the entire supply chain[25]. The consequences of implementing the idea of scientists would mean the emergence of a powerful tool

[21] M. HABLEN, *Financial sector expands use of blockchain databases*, available at: www.cio.com (the article was originally published by Computerworld), 28.09.2016. Visited on 05.02.2016.

[22] A. NORTA, *Establishing distributed governance infrastructure for enacting cross-organizational collaborations*, 01.2016, p. 1-13.

[23] I. WEBER, X. XU, R. RIVERT, G. GOVERNATORI, A. PONOMAREV, J. MENDLING; *Untrusted Business Process Monitoring and Execution Using Blockchain*, 08.09.2016, p. 1-16.

[24] B. GOERTZEL, T. GOERTZEL, Z. GOERTZEL, *The global brain and the emergance of the world of abundance, Mutualism, open collaboration, exchange networks and the automated commons*, Technological forecasting and Social Change, 114/2017, p. 65-73.

[25] Ibid, p. 68.

	for verifying the country of origin of individual components of a given product (control of changes at each stage of the supply chain), quality control, etc. Quality certificates seem to be a particular application[26]. • *Smart contracts* – autonomous software launched automatically, which guarantees irreversible implementation of provisions between the contracting "parties". (more on smart contracts will be discussed later in this article). • Support for management systems.
Medicine	• Prevention of manipulation of clinical trial results[27]. Employing blockchain technology to control the clinical trial process will increase confidence in the results and eliminate the authorisation of drugs with low clinical efficacy and low safety profile.
Internet of Things (IoT)	• Integration of blockchain technology and Internet of Things can help to increase the anonymity of IoT applications[28]. In turn, the use of smart contracts as an essential part of blockchain 2.0 will contribute to increasing the predictability on the Internet of Things. IBM presented a *proof-of-concept* for a new ADEPT (*Autonomous Decentralized Peer-to-Peer Telemetry*) system to facilitate the construction of a decentralized Internet of Things[29].

[26] G. R.T. WHITE, J. HOLDEN, *Future Applications of Blockchain: toward a value-based socjety*, INCITE Conference, Amity University, India, 10.2016, p. 3.

[27] G. IRVING, J. HOLDEN , *How blockchain-timestamped protocols could improve the trustworthiness of medical science*, 31.05.2016, p. 1-6.

[28] Z. ZHENG, S. XIE, H.N. DAI, H. WANG, op. cit., p. 12.

[29] Ibid., p. 12.

Public services	• Confirmation of ownership title including registration of buildings, land, patents, etc. Blockchain solution is robustly resistant to manipulation of data contained in the chain of blocks, which is of fundamental importance in the context of the sensitivity of data stored in the above registers. What is more, the blockchain solution is corruption-proof. • The schemes encouraging the use of green technologies[30]. Some concepts for incentive schemes (remuneration of solar energy producers) operate on blockchain solutions. • The blockchain solution has been recommended as a tool for protection against computer piracy and the one that supports protection against censorship on the Internet.
Security	• Source literature proposes to apply a blockchain string to privacy aspects in terms of: 1) ownership titles to data; 2) data transparency and auditing, and 3) access control[31]. • Improving the security of the Public Key Infrastructure (PKI).
Authentication systems	• Verification of customer reviews[32]. There is a concept of using blockchain to limit the number of unreliable/suspicious reviews. • Verification of the *due diligence* process (*Verified Corporate Due Diligence*)[33]. The blockchain concept can also be used to secure intellectual property rights in the event of strategic alliances and mergers termination. • Digital identity management systems.

[30] N. GOGERTY, J. ZITOLI, *An electricity-backed currencey proposal*, 2011, available at: http://bravenewcoin.com/assets/Whitepapers/DeKo-An-Electricity-Backed-Currency-Proposal.pdf, visited on 05.02.2017.

[31] G. ZYSKIND, O. NATHAN (et al.), *Decentralizing privacy: Using blockchain to protect personal data*, Security and Privacy Workshops (SPW), 2015, p. 180-184.

[32] G. R.T. WHITE, K. BROWN, op. cit., p. 3.

[33] Ibid., p. 3.

Blockchain 2.0 technology paved the way for the implementation of the first smart contracts. In a coded form, smart contracts can be disseminated in distributed data registers of such networks as Corda, Ethereum, Hypeledger[34]. The basis for this network is the concept of a chain of blocks, which allows computer software to be automatically executed (smart contract code) when a consensus is reached. In practice, this is to ensure absolutely fulfilment of the contractual obligations. In this context, however, possible errors in the contract code must be mentioned. An error in the code will result in the implementation of conditions that contradict the intentions of the parties or in the absence of any action. On the other hand, an error in the code may entail hacker attacks such as the one against the (Etherum-based) DAO in 2016, as a result of which 55 million USD was stolen. This implies that, at present, implementation of contracts must assume supervision and possible third-party corrective action. Moreover, there is no commonly accepted programming language for writing smart contracts, although model contracts are being developed with the necessary parameters for their operationalization[35]. The absence of universally recognised standards in smart contracts can be an important factor in slowing down their broad and rapid adoption.

5. REGULATORY ASPECTS OF THE USE OF BLOCKCHAIN CONCEPTS

This part of the article will examine the regulatory aspects that appear in the context of the application of the concept of distributed databases in the form of a chain of blocks, to be called a blockchain solution in short. First, it should be clearly emphasized that blockchain is a relatively new concept, whose use in the legal area is only in its initial phase, and its individual applications may show considerable differences. Thus, the following considerations are not exhaustive, but rather contribute to further discussion in this area, in particular by highlighting the importance of such solutions in the legal environment[36]. Apparently, the said model may be extensively applied in the area of law. Blockchain has been first tested in the financial contract market, nonetheless projects are underway to apply this solution in many other areas of law[37]. The potential impact of this concept

[34] C. Clack (et al.), *Smart Contract Templates: foundations, design landscape and research directions*, available at: http://www0.cs.ucl.ac.uk/staff/C.Clack/SCT2016.pdf , p. 2.

[35] Ibid., p. 3.

[36] The rapidly growing importance of this concept is well illustrated by the number of relevant new patent applications. In practice, there are already opinions that this solution could lead to a new "patent war". See *A rush to patent the blockchain is a sign of the technology's promise*, The Economist, 14.01.2017, available at: http://www.economist.com/, visited on 30.01.2017.

[37] M. GARSTKA, K. PIECHCH (ed.), *Konsorcja i rady blockchain na świecie*, Analytical Material Stream on trends in joint blockchain initiatives pursued worldwide, 18.01.2017, Available at: https://mc.gov.pl/files/porozumienia-v1.pdf

seems to be very broad. This paper essentially focuses on the use of blockchain solutions for the performance of contractual obligations.

When considering technical merits of a solution, in many cases, from the perspective of existing legislation, the effects of using a relevant technology may be problematic. Legislation is often not well adapted to new social, economic and technical developments. When analysing the formal aspect of the blockchain solution, it should be pointed out that the Polish legal system misses provisions which address it directly or which could feed into a specific normative qualification. Accordingly, the mere use of the blockchain solution in business transactions is fully legal, as the legislation does not differentiate the legal situation of this solution[38].

In the academic literature, many publications have already described the most popular emanation of the blockchain concept, that is the bitcoin[39] system, also from the legal point of view.

As proven by the comparative legal analysis, even in this respect this issue is omitted in the vast majority of jurisdictions, leaving the development of solutions to jurisprudence and theoreticians. However, where cryptocurrency legislation are in place, they are usually restrictive (prohibitive)[40]. Notwithstanding indefinite legal standard of bitcoin in Poland, no major objections has be raised so far to its legal status[41], and its legality has also been confirmed in the judgment of the Court[42]. However, academics and practitioners are concerned with bitcoin as a cryptocurrency, not with the very application of the underlying blockchain solution. It should be noted that this Article will not apply in principle to digital currencies and their legal and fiscal aspects and to the penal elements of their unlawful operation.

With no specific rules in place, this solution should be qualified - at least for the time being, at the present stage of its development – tantamount to other IT tools applied in business transactions. Within the scope of contractual obligations, this formula may make possible such things as making and accepting declarations of intent, performing legal actions, but above all, it will serve to automate the process of fulfilling obligations. Civil law provisions do not seem properly adapted to cover this type of situation as well. As per a fundamental principle of civil law, the parties are free to choose the

[38] As per *quod lege non prohibitum, licitum est*.

[39] In Poland this subject was addressed in particular by K. Zacharzewski. See K. ZACHARZEWSKI, *Bitcoin jako przedmiot stosunków prawa prywatnego*, Monitor Prawniczy, Issue 21/2014; K. ZACHARZEWSKI, *Praktyczne znaczenie bitcoina na wybranych obszarach prawa prywatnego*, Monitor Prawniczy, Issue 4/2015.

[40] G. SOBIECKI, *Regulowanie Bitcoina*, Presentation for III International Cashless Congress, 03.2015, available at: http://www.kongresplatnosci.pl/

[41]The bitcoin is assumed a property right under civil law. After: K. Zacharzewski, *Bitcoin...*, p. 1133.

[42] As pointed out by the Court of Justice, the bitcoin constitutes a means of payment. See Judgment of the Court of Justice of the European Union of 22.10.2015 in the case of *Skatteverket v. David Hedqvist* (C-264/14).

contract form, unless the law requires a specific form[43], so little doubt, dispersed networks and systems may be used to conclude contracts.

Obviously, contracts concluded via blockchain solutions will be governed by a whole range of laws, which provide for transactions concluded by electronic means, such as consumer law or personal data protection rules. They will not be discussed here because, as the civil law rules, they are suitable for a proper application. As per the analysis carried out by Stream "Blockchain i kryptowaluty", under "Od papierowej do cyfrowej Polski" programme of the Ministry of Digitisation, the current legal status of blockchain solutions is sufficient and there is no reason for special legal adjustment in this area[44]. Still, the assumptions of implemented blockchain projects often assume the need for normative analysis and contemplation of legislative changes that will adapt the use of networks and distributed systems to the existing legislation[45]. In this context, it is proposed to introduce the so-called *regulatory sandbox,* that is legal solutions that will facilitate, especially for start-up companies, to continue research and development and implement work based on the operation of blockchain solutions. It is emphasised that, in developing such solutions, these actors undertake considerable risks and should therefore count on state support to ensure the security of the legal ecosystem[46].

Legislation can be expected to amend gradually as this option evolves, although many aspects are likely to be subject to a self-regulatory mechanism similar to that of the Internet[47]. In the first instance, by applying the *de lege ferenda* principle, *where* legislation requires a third-party consent or specific verification (for example qualified electronic signature), these requirements can be eliminated over time by the very nature of the operation of networks and distributed systems. Eliminating an intermediary from the transaction process does not make the transaction less certain and secure, these functions being decentralised for blockchain solution, as it is independent entities that verify the transaction concluded. Decentralisation via *peer-to-peer* networking, on the other hand, is conducive to full globalisation and does not discriminate against users. Interestingly, the blockchain solution,

[43] The principle of freedom to choose the form of contract is a part of a broader principle of freedom of contract, defined in Article 353^1 of the Civil Code.

[44] K. ZACHARZEWSKI, K. PIECH (ed.), *Przegląd polskiego prawa w kontekście zastosowań technologii rozproszonych rejestrów oraz walut cyfrowych*, Stance of the Stream on the directions of possible legislative works and regulatory actions of public institutions, 19 January 2017. Available on: https://mc.gov.pl/files/przeglad_polskiego_prawa_w_kontekscie_zastosowan_technologii_rozproszonych_rejestrow_oraz_walut_cyfrowych.pdf

[45] M. GARSTKA, K. PIECH (ed.), op. cit.

[46] K. ZACHARZEWSKI, K. PIECH (ed.), op. cit.

[47] J. DOGUET, *The Nature of the Form: Legal ad Regulatory Issues Surrounding the Bitcoin Digital Currency System*, Louisiana Law Review, Issue 73/2012, p. 1143-1147.

which works on a similar basis to that described above for the bitcoin system, provides anonymity, but also full transparency of transactions through access to the public register. The elimination of a third party does not attenuate legal certainty of the transaction, but is intended to enhance it.

6. APPLICATION OF BLOCKCHAIN CONCEPT AND SMART CONTRACTS

As mentioned above, the blockchain concept has great potential for applications for contractual obligations. This solution may create the so-called small contracts, with their terms and conditions defined and performed fully automatically with no third-party interaction.

Currently, not only the largest companies, but also a whole range of start-up institutions are working on such smart contracts. The very idea of a smart contract is attributed to Nick Szabo, who introduced this concept in the 1990s, describing it as a computerised protocol fulfilling the contractual terms[48]. In pursuit of a synthetic definition of a smart contract, it can be defined as a "digital representation of the principles or processes in a business organization that govern the manner in which transactions are made and the course of their execution". (...) and may control 'assets or may cause events, as determined by programming techniques' [49] or, in simple terms, as computer software that can make decisions if certain conditions are met[50]. Indeed, however, smart contracts are distinguished by their "self-executability". The usefulness of this software may manifest itself throughout the life cycle of a contract, from negotiation to completion. As a result, the parties can carry out the entire transaction process in a smooth and swift manner, without the participation of third parties, such as a civil law notary.

Smart contracts can be implemented as blockchain solution in the bitcoin system, but this kind of distributed databases may be introduced via another form of distributed registers. The literature highlights that a bitcoin system can transfer any digital good, but also things connected to a network/system which use the concept of blockchain[51].

One of the most extensive examples of developing a smart contracts mechanism, although still in the development phase, the R3CEV project, includes many of the largest international financial

[48] D. HE (et. al.), *Virtual Currencies and Beyond: Initial Considerations*, International Monetary Fund, 01.2016, SDN/16/03for N. Szabo, *Smart Contracts,* 1994.

[49] K. PIECH (ed.), *Leksykon...*

[50] M. KÕLVART (et al.), *Smart Contracts*, [in:] *The Future of Law and eTechnologies*, T. Kerikmäe, A. Rull (ed.), Springer 2016, p. 134.

[51] P. FRANCO, *Understanding Bitcoin: Cryptography, engineering and economics*, Chichester 2014, p. 183-186.

institutions[52]. The project has been primarily designed to determine how smart contracts using blockchain solutions could link to actual contracts. This is why the project is currently focused on developing templates for smart contract[53]. Such templates are developed to be used in the negotiation and for conclusion of contracts between counterparties, to facilitate automatic performance of the obligation and, in dispute, to provide a reference to the relevant legal documentation[54]. It is worth noting that access to the register in this case is not public, but exclusive in order to ensure an appropriate degree of confidentiality[55].

According to the study by the International Monetary Fund, reliance on smart contracts carries the following benefits: increased speed, efficiency and certainty that the contract will be implemented as agreed between the parties. Moreover, they can lead to elimination of potential fraud and reduce the costs of contract verification and implementation[56]. It appears that cost reduction may affect the entire contract conclusion process, while additional advantages are greater confidentiality, transparency, security and control of the transaction process. In the context of the benefits of blockchain solution it is also worth noting that the contractual terms becomes virtually unbreachable, because it is implemented in real time, which at the same time reduces the judicial and enforcement system's workload[57].

Regardless of obvious potential, this solution also carries a number of risks. Like any other concept, a blockchain solution can also be used for illegal purposes. However, such a threat should not limit the development of this solution, since, like any other tool, it can be used for both legal and criminal purposes. This is an indispensable element of the risk involved in the implementation of new technical solutions and technologies. In the longer term, along with the introduction of new technical solutions in this area, it will be appropriate to examine the legal possibilities for preventing abuse of such solutions in order to achieve illegal objectives. Still, in the current legal status, agreements that

[52] See information at http://www.r3cev.com/about/

[53] L. BRAINE, *Smart Contract Templates*, Presentation to CoinDesk, 25 April 2016, available at: http://www.coindesk.com/barclays-smart-contracts-templates-demo-r3-corda/, visited on: 30.01.2017.

[54] C. CLACK (et al.), op. cit., p. 1.

[55] P. RIZZO, *How Barclays Used R3's Tech to Build a Smart Contracts Prototype*, 26 April 2016, available at: http://www.coindesk.com/barclays-smart-contracts-templates-demo-r3-corda/.

[56] D. HE (et. al.), op. cit., p. 23.

[57] This can also be considered a threat to the operation of the blockchain solution. Namely, it is pointed out that freedom to breach the provisions of the agreement is an element of traditional contracts, where the performance of an obligation is *ex post*. Default carries specific sanctions – such as damages. Respectively, the agreement being unbreakable may *de facto lead to a* restriction of the freedom and autonomy of the parties. A. WRIGHT, P. DE FILIPPI, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, SSRN Scholarly Paper ID 2580664. Social Science Research Network, Rochester 2015, pp. 26 and 43.

would aim at circumventing the law or would be contrary to the principles of community life would be void by definition[58, 59].

Some authors point out that implementing the idea of an smart contract and "taking over" by the system of the role of a lawyer in the transaction process, who could assess the complexity of many elements of the contract (for instance differences between particular jurisdictions) would require the involvement of artificial intelligence[60]. It should be noted, however, that the state of the art in this area is at a very early stage of development. Contrary to their name, smart contracts do not need artificial intelligence to implement[61]. This highly complex cognitive issue falls outside the scope of this article. Yet, smart contract templates created in the R3CEV project must be recalled in this context. Namely, their originators, as part of their work, analyse the issue of the "significance" of the agreement and its interpretation. In this context, they propose to presume two interpretations of the contract: "*operational semantics*" and "*denotational semantics"*. While the former assumes contract interpretation whereby precise actions to be undertaken by the parties is determined, the latter constitutes a legal interpretation of the entire contract and the relevant documentation, that is the significance of the contractual provisions for legal professionals. According to the authors of these assumptions, these semantics do not constitute different elements of the contract, but they are oriented towards different objectives. Unlike denotational semantics (which can be very complex even for a short text), operational semantics can be easily programmed for automatic execution[62]. A meaningful interpretation may be needed only at the stage of a potential dispute.

At this point, we come to an interesting conclusion, relating to the essence of smart contracts. Namely, within the framework of smart contracts, the algorithm expressed in the programming language is the content of the legal norms, under the '*code is law'* principle. This entails serious legal consequences. Namely, for smart contracts to fulfil their role, the underpinning algorithms must be precise, otherwise it will give rise to abuse and the contracts will not bring the expected benefits. The correctness of the code is crucial for the legal certainty of program users (contracting parties) that

[58] See Article 58 of the Civil Code.

[59] The Bitcoin has been abused for illegal purposes practically since its launch. T. SIMONITE, *Bitcoin's Dark Side Could Get Darker,* 13 August 2015, MIT Technology Review, available at: https://www.technologyreview.com/s/540151/bitcoins-dark-side-could-get-darker/; visited on 30.01.2017.

[60] M. KÕLVART (et al.), op. cit. , p. 135.

[61] L. LAUSLAHTI (et al.), *Smart Contracts–How will Blockchain Technology Affect Contractual Practices?* The Research Institute of the Finnish Economy, ETLA Reports, Issue 68, 9.01.2017, p. 3.

[62] C. CLACK (et al.), op. cit., p. 5.

such contracts will fulfil the intentions of the parties[63]. Moreover, translation of the software language into the contractual wording raises the additional problem given that the programming languages are not commonly known. Development and understanding of a smart contract may require extensive/thorough knowledge[64], and this problem may in particular affect consumers, for whom grasping the essence of the contract will constitute an additional challenge[65].

In this context, the question arises as to the relationship between a smart contract and a real legal contract or agreement by and between the parties. Is this contract a real contract-in-law, one has to wonder. Without going into detail on the formal elements of the contract conclusion, the mutual agreement of the parties to enter into the contract is a necessary prerequisite[66]. All this being said, a smart contract does not need to be a legal agreement at all. As a general rule, it exists as if it were in addition to the actual agreement, and in order for it to "merge", the parties must wish to enter into a binding contract or agreement with all its legal effects[67]. Accordingly, smart contracts evade clear legal qualification at the moment, as it will depend on the practical implementation of such an idea in a relevant solution[68]. Those instruments will possibly only serve as a tool to implement the commitments, the terms of a smart contract deriving from a real agreement between the parties[69]. Another possible solution is to conclude an agreement in a smart formula and next remotely transform it into a physical document written in a natural language[70].

7. IS BLOCKCHAIN SOLUTION A BREAKTHROUGH COMMENSURATE WITH THE BIRTH OF THE INTERNET?

Academic literature hints that the introduction of blockchain solutions may be a breakthrough of a rank matching the outset of the Internet, which will transform many areas of community activities, including the legal sector. Smart contracts are an emanation of the second generation of this solution, which goes far beyond the interest in cryptocurrencies. It allows one to program various transactions

[63] G. PETERS, P. EFSTATHIOS, *Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money*, Banking Beyond Banks and Money. Springer, 2016. p. 246-247.

[64] T. SIMONITE, op. cit.

[65] D. HE (et. al.), op. cit.

[66] In order to conclude a contract under civil law, a consensual agreement is required, that is a consensual declaration of will of the parties. See Article 65 of the Civil Code. The very form of contract that the parties could conclude will rather depend on the specific solution applied.

[67] M. KÕLVART (et al.), op. cit. , p. 135.

[68] L. LAUSLAHTI [et al.], op. cit. , p. 13.

[69] Ibid., p. 21.

[70] Ibid., pp. 21-22.

to implement the relevant business logics. In this sense, the second generation blockchain provides a digital and open system of transactions between network users, where databases have been decentralized[71].

The concept of "*lex cryptographia*" has been suggested, as a new field of legal science, on self-regulatory contracts and decentralised autonomous organisations (hereafter: DAO)[72]. The authors of this concept claim that a new digital revolution is coming with the decentralization of the Internet, and that for the legal industry it is a breakthrough comparable to the invention of printing[73]. DAO play a key role in this process. They are autonomous by virtue of their mere inclusion in a register and self-sufficient by virtue of the fact that they can raise capital and charge users for their services[74].

As underlined earlier, solutions based on the blockchain concept are still underdeveloped. For this reason, it is difficult to unequivocally determined whether, and to what extent, they will imply certain consequences for the legal system. As a consequence of far-reaching changes in this area, the existing rules may require adaptation. No doubt, especially due to their decentralization, specific applications of the blockchain concept can give rise to major legal problems. At the moment, the substance of smart contracts spark more questions than answers. It is unclear whether the nature of the blockchain solution will ultimately cause that the legal qualification of contracts concluded with its help will be significantly different from the currently available means of concluding contracts by electronic means. However, this is arguably going to happen, as in addition to the above advantages, automation of the process of fulfilling obligations may yield material changes in the practice of law, and more broadly even in socio-economic relations. The implementation of this solution will chiefly eliminate the intermediary in transactions in favour of a decentralised, dispersed register[75].

Obviously, many processes pertinent to the automation of law are indispensable. Combined with communication between network users and the Internet of Things concept, the blockchain

[71] R. BECK, C. MÜLLER-BLOCH, *Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers as Incumbent Organization*, Proceedings of the 50th Hawaii International Conference on System Sciences, 2017, p. 3-4.

[72] A decentralised autonomous organisation is a 'robust programming code with the characteristics of a smart contract, extending it to a large extent of autonomy', which is most often 'implemented as a series of smart contracts linked to each other by a common domain of activities and sharing their API'. What distinguishes them from ordinary smart ones is the role of the DAO, which "can be autonomous asset management, decision making and active interaction with the environment (contracting parties, network, external world, etc.) as a party/person". After: K. PIECH (ed.), *Leksykon...*

[73] A. WRIGHT, P. DE FILIPPI, op. cit.*, p.*2, 10.

[74] Ibid., p. 17.

[75] It is worth noting, however, that even for smart contracts based on blockchain solutions, a trusted third party may be necessary. At the moment, fully automatic, that is self-executing contracts is limited in many areas. It should be assumed that in certain areas external data will be necessary to supply the contract. Accordingly, it may turn out that the values for a parameter will have to be supplied from outside through a trusted third party.

solution can prove a genuine turning point. Currently, there hopes are running high for it, but ultimately the its full implementation will depend on the actual applications created by its use.

8. Final conclusions

Solutions based on the blockchain model, described in the article, are tools whose application in the legal area may have serious implications for legal practice. As outlined, the use of this solution is not currently subject to any specific regulations and the current legal situation appears well-prepared in this respect. While the evidence implies that no additional legislation for blockchain solutions is necessary, this will depend on the actual way in which they are applied.

Looking ahead, smart contracts are likely to expand gradually and gain in importance in business trade. As highlighted, an important feature that distinguishes smart contracts is their self-execution function, thanks to distributed networks. It should be reiterated, however, that the current work on the introduction of smart contracts is not yet advanced, and they cannot be examined in details. On the other hand, potential advantages to smart contracts are easy to identify. These are mainly the speed of contract execution, transaction security and reduction of transaction costs by reducing the role of a third party. Nonetheless, this kind of solution is not risk-free, and one of threats is the transformation of legal norms into programming algorithms. The relationship between legal and programming language should undoubtedly be the subject of further research. It is not feasible to establish unambiguous whether a smart contract overlaps with a contract or agreement concluded and implemented in a traditional manner. The implementation of solutions based on smart contracts and DAOs can be a real revolution in this area.