TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 8589 - 8594

Concepts and Basic Features of Smart Contracts

Oksana Safonchyk, Kateryna Hlyniana and Svetlana Mazurenko
Civil Law Department, National University «Odesa Law Academy», Odesa, Ukraine.
Civil Law Department, National University «Odesa Law Academy», Odesa, Ukraine.
Intellectual Property and Corporate Law Department,National University «Odesa Law Academy», Odesa, Ukraine.

Article Info
Volume 83
Page Number: 8589 - 8594
Publication Issue:
May - June 2020

Article History
Article Received*: 19 November 2019*
Revised*: 27 January 2020*
Accepted*: 24 February 2020*
Publication*: 18 May 2020*

Abstract:
The authors of the article analyze the features of using of the smart contracts for civil circulation. Smart contracts are made up of a code that secures the parties' agreements, and therefore the rights and obligations related to the performance of the contract are already implemented in the smart contract, even before it is enforced. This ensures a higher degree of protection of the rights and interests of the parties to the contract with respect to traditional contracts. Despite certain problems with the use of smart contracts, which still remain relevant, including the conflict of jurisdiction in the conclusion of smart contracts by residents of different countries, the technical difficulties associated with the possible settlement of disputes that may arise from such contracts in courts, the lack of proper regulation of relationships related to the use of this technology, etc., smart contracts are an innovation that can over time completely replace traditional business contracts.

Keywords: *blockchain, internet technologies, smart contracts, legal regulation, IT sphere, computer program.*

I. INTRODUCTION

The concept of smart contracts dates back to 1994 and was introduced by Nick Szabo, who, as a programmer, cryptographer, and lawyer, wanted to come up with an innovative way to settle contractual relationships, which would be a contract, as an electronic protocol of an agreement aimed at automatically based on a fully deterministic model of contracting and executing a contract similar to a computer program. Nick Szabo determined the smart fulfillment of her conditions. However, at that time, the concept of smart contracts was not widespread, mainly due to the lack of technical feasibility of its implementation.

In the future, some of the conceptual principles proposed by Nick Szabo were embodied in the so-called "Ricardian contracts", which are considered to be a continuation of the development of the concept of smart contracts. However, in the Ricardian contracts, this concept has been interpreted somewhat differently and aimed exclusively at meeting the needs of the financial sector, which is why it has not become widespread. In this regard, the concept of smart contracts has long been neglected by the general public for a long time.

Today there is no established definition of the term "smart contract". Even programmers are still debating what should be understood by this term.

The first definition of the term "smart contract" was given by the creator of their concept Nick Szabo, who gave the term the following definition: "Smart contract is an electronic protocol of the agreement aimed at the automatic fulfillment of its terms" (Szabo, 1997).

II. METHODOLOGY

During the writing of the article, different methods of scientific research were used. Among them, there can be distinguished the methods of analysis and synthesis.

Thus, an analysis is a method of cognition, consisting of logical techniques of the theoretical or empirical division of a research subject into its elements, properties, and relations. This method allowed us to identify the imperfection of the current legislation in the area of smart contracts use and to determine the ways of its reformation.

Moreover, the synthesis is a method of cognition, consisting of logical techniques of theoretical or empirical connection of selected elements of an object into a whole (or into a system). This method has helped the authors of the article to summarize information regarding the use of smart contracts and to propose the improvement of legal regulation of the mentioned relations.

TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 8589 - 8594

III. ANALYSIS OF RECENT RESEARCH

Nowadays, authors from different fields of scientific search turn their views on the study of smart contracts. In this case, the authors of the article were interested in the study of smart contracts in terms of computer science and law, because it is these sciences that allow the implementation of many innovations that are emerging more and more.

So, Stark D. believes that the term "smart contract" refers to the use of computer code in the form of a programming language, such as JavaScript or HTML, to formulate, validate and execute an agreement between the parties, which in effect becomes equivalent to a contract written in the natural human language. In doing so, a reasonable contract is "executed" by the computer, subject to the terms of the agreement.

Moreover, in a paper dealing with cross-border aspects, Khurani S. believes that smart contracts are program codes that embed contract terms and operate on the network, leading to partial or full automated self-fulfillment of the contract.

Furthermore, smart contracts by M. Raskin are agreements that are executed automatically by computer programs that have control over physical or digital objects, which are implemented without human influence and in court.

However, the most relevant one seems to be the definition proposed by British scientist Bashir Imran, who defined the term "smart contract" as follows: "A smart contract is an immutable, secure and irresponsible computer program that reflects an automatically executed agreement and operates in a distributed decentralized block chain network. This definition of the smart contract is the most widespread in the legal and specialized technical literature, so it is worth considering it in the future (Grigg, 2003).

Based on the above definition, it can be said that essentially the two basic properties of smart contracts that characterize their essence are their immutability and automatic execution, which need to be considered in more detail.

In addition, well-known scientists and young scientists in Ukraine are beginning to explore the topic of smart contracts in Ukraine (Kharytonov, Kharytonova, Kharytonova, Kolodin, &Tolmachevska, 2019). Moreover, Maren K. Woebbeking(2019) studied the impact of smart contracts on traditional concepts of contract law. Also, Tulsidas(2018) and Ting (2017)paid attention to the legal perspective of the smart contracts.

However, many problems of legal regulation of relations regarding the use of smart contracts remain out of the limelight of researchers. For example, more detailed research requires the issue of liability for breach of obligations under smart contracts.

IV. RESULTS AND DISCUSSION

Information society plays an important role in information and communication technologies that allow collecting, processing, receiving and transmitting information at the local, national and international levels (Kharytonov, Kharytonova, Tolmachevska, Fasii, & Tkalych, 2019).

The latest information technologies are changing almost all spheres of public life. The world community is only beginning to realize the real and potential nuances of the influence of fully automated systems on the vital areas of social relations, on the growth of ethical, social and legal problems associated with this trend (Kolodin, Telychko, Rekun, Tkalych, &Yamkovyi, 2020).

Unlike traditional contracts, which depend on the independent actions of the parties, it can be argued that smart contracts are capable of fulfilling (or at least partially fulfilling) contractual arrangements by computer without direct intervention by the parties. Smart contracts are made up of a code that secures the parties' agreements, and therefore the rights and obligations related to the performance of the contract are already implemented in the smart contract, even before it is enforced. These coded agreements can be regarded as terms and their associated consequences, for example, if conditions A and B coincide, the effect of B will be executed automatically by the smart contract. Smart contracts, unlike traditional contracts, act as autonomous agents that operate entirely on block chain and "eliminate a person from the accomplishment cycle." Therefore, block chain smart contracts are self-executing, based solely on the instructions implemented in its code. In the context of this, a smart contract can independently verify the fulfillment of the terms of the contract, if the pre-designed criteria are the same (Hu, Liyanage, Manzoor, &Thilakarathna, 2019).

Moreover, it is important to understand that a smart contract is different from a traditional computer-based contract, such as automated bank transfer. Most people today use online banking and set up several automated

May – June 2020
ISSN: 0193-4120 Page No. 8589 - 8594

bank transfers to other people, meaning they don't have to contact the bank every time they want to make a payment. A simple example is the payment of monthly lease payments: in the event of a stipulated date at the end of the month, the bank automatically transfers the predetermined amount to the lessor on behalf of the tenant. However, the final choice regarding the transfer of a predetermined amount remains within the "sphere of influence" of the bank or tenant, because the tenant or bank may intervene, suspend or change the payment at any time. Smart contracts, on the contrary, are executed automatically, without the possibility of third-party intervention and the risk of counterfeiting. In essence, a smart contract code will simply perform a transfer if an automated transfer has been implemented into a smart contract, making the third-party intervention unnecessary and impossible. Accordingly, the automated nature of self-fulfillment of rights and obligations is the basis for making smart contracts actually "smart" (Kukman, Jakomin, Kranjc, Mele, Mavsar, Dragar, Zibrat, &Vlacic, 2018).

It should be noted that avoiding third-party intervention is seen as a great benefit of using smart contracts. Not only does this minimize the costs of third-party involvement, but it also makes the smart contract less dependent on their intervention. Therefore, a smart contract is less dependent on the will of third parties.

While revealing the characteristics of the automatic performance of smart contracts, it should be emphasized that it occurs only in the presence of coincidence of predefined conditions. In this regard, it seems appropriate to clarify exactly how smart contracts receive information about the occurrence of certain circumstances, which is necessary for the implementation of the program instructions contained therein.

Therefore, obtaining the smart contract with the necessary information depends on such fundamental elements of their ecosystem as oracles (oracle). Oracle is an interface that delivers data from an external source to smart contracts.

Depending on the industry and requirements, oracles can deliver different types of data, from weather reports, real-world news, and corporate data to data coming from the Internet of Things (IoT) devices. Oracle is a trusted "person" who uses a secure channel to transmit smart contract data (McDermott, Nagle, Horowitz, & Johnson, 2017).

The oracles are also capable of digitally authenticating their source. Smart contracts can "subscribe" to an oracle and either extract or download data from an oracle independently.

For smart contract developers, it may be appropriate to accept oracle data provided by large, trusted third parties with a good reputation, but in this case, there remains the problem of centralization. These types of oracles can be called standard or simple oracles. For example, a data source may come from a reliable hydrometer or airport information system that reports flight delays.

Another concept that can be used to assure the reliability of data provided by Oracle to a third party is to obtain data from multiple sources; even users or members of a particular community who have access and are aware of some of the data can provide the data they need. This data can then be verified, so if a significant amount of the same information was provided from multiple sources, then there is a high chance that the data is correct and can be trusted (Clack, 2018).

Another type of oracle that has inevitably emerged from the requirements of decentralization is called a decentralized oracle. These types of oracles can be constructed based on some distributed mechanisms. It can also be assumed that the oracles themselves can find a data source from another block chain that is managed by a distributed consensus, thus ensuring the reliability of the data. For example, one institution running its private block chain may publish its data through an oracle, which can then be consumed by other block chains.

The researchers also introduced another oracle hardware concept that requires real data from physical devices. For example, this can be used in telemetry and the Internet of Things (IoT). However, this approach requires a mechanism in which hardware devices are tamper-proof. This can be achieved by providing cryptographic evidence (integrity) of the data of the Internet of Things (IoT) device and a counterfeit mechanism on such a device (IoT), rendering it unusable in the event of damage.

Currently, platforms are available that allow the smart contract to receive external data via the oracle. There are different methods that Oracle uses to write data to a block chain, depending on the type of block chain used. For example, in a Bitcoin block chain, an oracle can write data to a particular transaction, and a smart contract can control that transaction in a block chain and read data.

Various online services such as http://www.oraclize.it/ and https://www.realitykeys.com/ are available to provide

May – June 2020
ISSN: 0193-4120 Page No. 8589 - 8594

oracle services. Another service is available at https://smartcontract.com/, which provides external data and the ability to make payments using smart contracts (Tredgett, R., Blizzard, K., Schultz, E., Smith, H., Post, C., Datoo, A., Devulder, S., Streiner, J., Jho, H., Fey, K., Chin., D., Mckeever, D., Farrell, Smith, A., Lewis, P., Hay, R., Lawless, J., Bleiberg, S., Maly, V., Franks, D., Rozovsky, J., Larsen, K., &Vivies, C.-E. de. (2019).

All of these services are designed to enable the smart contract to receive the data they need to execute and make decisions. Mechanisms such as TLSnotary that confirm the relationship between the data source and the Oracle can be used to validate the data obtained by Oracle from external sources. This ensures that the data returned to the smart contract is obtained directly from their source (more details on TLSnotary can be found at https://tlsnotary.org/).

We should also mention the idea of the so-called "smart oracle", which was proposed by the laboratories of Ripple (codius). Smart oracles are objects similar to oracles, but with the added ability to execute a contract code. The smart oracles offered by Codius work with Google Native Client, which is an isolated environment for running unreliable code.

In addition to their self-fulfilling nature, smart contracts also differ from traditional contracts in their immutability. Since smart contracts are embodied in block chain programming language, it can be said that in the future they are difficult or unchanged (unilaterally) by the parties themselves. The smart contract code defines the operation and result of the contract throughout the duration of the smart contract cycle, which means that the existing arrangements in the smart contracts cannot be interpreted or otherwise influenced by external factors or the will of third parties (Çiftçi, &Aksel, 2017).

The binary construction of a smart contract code prevents it from being interpreted based on the content or circumstances of the contract. Therefore, the parties to the contract should record the content and circumstances of the agreement at the time of drawing up the smart contract. Although it can be argued that most traditional agreements also require these aspects to be taken into account at the time of drafting, their content or the circumstances of the conclusion may then be established by a court. Besides, the content and circumstances of the contract are in most cases decisive for the judge in the decision-making process.

The above-mentioned invariability can best be described from the Sabo vending machine. If someone wants to buy merchandise from a vending machine and insert a coin into the hole and press the button indicating the desired item, the seller does not need to intervene to verify that the transaction has been completed. The transaction must be autonomous and the seller should not be allowed to further intervene in it ("protection against unauthorized interference").

The same principle can also be embodied in a Bitcoin transaction: if a person confirms a valid Bitcoin transfer instruction, the transaction is automatically recorded in the Bitcoin block chain, which will not be modified until the next valid transaction is credited to it.

According to the smart contract, you must have the ability to certify the execution in a way that depends on the completion of the autonomous technological process ("if ... then") to have the property of protecting execution against third-party interference, such as vending machine and Bitcoin transaction. The definition of "protection against unauthorized interference" concerning smart contracts is understood to mean that the possibility of executing a smart contract may not necessarily be that it may be enforced by a court, but in the alternative sense of "enforcement" that may be embodied through an autonomous process that cannot be unilaterally intervened by the parties once it has been initiated (Cohen, Jacobs, Roszak, &Regan, 2016).

V. CONCLUSIONS

1. The use of smart contracts has many advantages over conventional written contracts, which is due primarily to their basic properties such as immutability and automatic execution. In particular, this reduces the risks associated with the conclusion and execution of the contract, reduces the corresponding costs, and provides a higher degree of protection of the parties to the contract. However, the expediency of completely replacing smart contacts with traditional ways of contracting is still an open and rather debatable issue, given the shortcomings of this mechanism.

2. Today, smart contracts are becoming an integral part of people's daily lives and are increasingly intertwined with those traditional contractual arrangements that govern various types of social relations. As of now, smart contracts have been most heavily influenced by international maritime freight and insurance contracts, as evidenced by the many successful projects in these areas, such as CargoX, CargoCoin,

May – June 2020
ISSN: 0193-4120 Page No. 8589 - 8594

fizzy, Etherisk and PolicyPal Network. However, the practice of furthering smart contracts and other types of contracts is quite expected, given their many benefits that cannot be overlooked. Therefore, we can conclude that in the near future, the prospects of modernization of various contractual legal institutions will increase, driven by the rapid development of innovative technologies such as block chain and smart contracts.

3. It is indispensable to develop special legal rules regarding smart contracts in Ukrainian legislation. However, there are many difficulties to date for the legal implementation of smart contracts in the regulatory framework. These difficulties are both technological and legal in nature. In particular, the main ones are the technical limitations inherent in smart contracts in the current state of development of this technology. There are also several difficulties associated with the conversion of certain legal concepts into program code, in the development of smart contracts, which in turn can lead to inaccurate expression of intentions of the parties to the contract. Besides, it seems problematic to come up with an appropriate legislative definition of the term "smart contract", since even in the professional sphere of its use; there is no unambiguous opinion in this regard. There are also problematic issues regarding the resolution of disputes that could potentially arise from smart contracts, which, for the most part, relate to determining the jurisdiction of the court to which the dispute will be litigated. Undoubtedly, the implementation of legislative regulation at the national level alone seems to be insufficient, since smart contracts, for the most part, give rise to private legal relations with a foreign element, and therefore also require the improvement of relevant conflict-of-law rules that must take place at the international level. However, it should be noted that all these difficulties can be overcome in the future, and therefore their presence is not a critical impediment to the further implementation of the relevant legislation on smart contracts.

VI. REFERENCES

1. Çiftçi, I., &Aksel, K. (2017). Smart Contracts (Code Vs. Contract): An Overview Of Blockchain Technology And Legal Implications Of Smart Contracts From A Turkish Law Perspective. YeginCiftci Attorney Partnership. Retrieved from https://www.yeginciftci.av.tr/content/site-ycap/en/publications/previous-publications/2017/smart-contracts-code-vs-contract-an-overview-of-blockchain-technology-and-legal-implications-of-smart-contracts-from-a-turkish-law-perspective/_jcr_content/parsys_article/download/file.res/Client%20Briefing_Smart%20Contracts%20(Code%20vs.%20Contract).pdf.
2. Kandi, Shrishail, ANTRIKSH MUTHA, and ABHAY KULKARNI. "Centralization and Decentralization in Supply Chain Management." International Journal of Industrial Engineering &Technology (IJIET) 7.3 (2017): 5-10.
3. AZEEMI, N. ZAFAR. "DELIVERING 4G (LTE) TO 5G MIGRATION WITH SUPPLY CHAIN MANAGEMENT." International Journal of Electronics and Communication Engineering 6.1 (2017): 21-32.
4. Clack, C. D. (2018). Smart Contract Templates: legal semantics and code validation. The Centre for Blockchain Technologies. Retrieved from http://www0.cs.ucl.ac.uk/staff/C.Clack/research/JDigitalBanking-Clack-AuthorPreprint.pdf.
5. Cohen, L., Jacobs, J., Roszak, M., & Regan, J. (2016). Smart Contracts: 12 Use Cases for Business & Beyond The Chamber of Digital Commerce. Retrieved from http://digitalchamber.org/assets/smart-contracts-12-use-cases-for-business-and-beyond.pdf.
6. Kolodin, D., Telychko, O., Rekun, V., Tkalych, M., &Yamkovyi, V. (2020). Artificial Intelligence in E-Commerce: Legal Aspects. Advances In Economics, Business And Management Research, 129, 96-102. Retrieved from https://www.atlantis-press.com/proceedings/isc-sai-20/125937200
7. Okyere, Stephen, Jiaqi Yang, and Monde Aminatou. "Influence of Multimodal Transport System Dynamics on LogisticsResponsiveness: An Ordinal LogisticRegressionApproach." International Journal of Civil Engineering (IJCE) 6.6 (2017): 9-24.
8. Grigg, I. (2003). The Ricardian Contract. Retrieved from https://iang.org/papers/ricardian_contract.html.
9. Hu, Y., Liyanage, M., Manzoor, A., &Thilakarathna, K. (2019). Blockchain-based Smart Contracts – Applications and Challenges. Retrieved from https://www.researchgate.net/publication/32823086

May – June 2020
ISSN: 0193-4120 Page No. 8589 - 8594

5_Blockchain-based_Smart_Contracts_-_Applications_and_Challenges.

Kharytonov, E., Kharytonova, O., Kharytonova, T., Kolodin, D., &Tolmachevska, Y. (2019). Human rights as the basic value of the concept of private law in modern Europe. Amazonia Investiga, 8(20), 477-485. Retrieved from https://www.amazoniainvestiga.info/index.php/amazonia/article/view/177

10. Kharytonov, E., Kharytonova, O., Tolmachevska, Y., Fasii, B., &Tkalych, M. (2019). Information Security and Means of Its Legal Support. Amazonia Investiga, 8(19), 255-265. Retrieved from https://www.amazoniainvestiga.info/index.php/amazonia/article/view/227.
11. Kukman, S., Jakomin, I., Kranjc, J., Mele, J., Mavsar, P., Dragar, I., Zibrat, R., &Vlacic, P. (2018). Business Overview and Technology Bluepaper.CargoX. Retrieved from https://cargox.io/CargoX-Business-Overview-Technology-Bluepaper.pdf.
12. GAI, Shuangshuang, and Xueli LIU. "The Internationalized Actuality of the Research of Information Science & Library Science in China——Based on the Citation Analysis of High Impact Journals of Information Science & Library Science Based on SSCI Social Sciences Citation Index." Sci-Tech Information Development&Economy 11 (2015): 62.
13. McDermott, C., Nagle, J., Horowitz, M., & Johnson, S. (2017). From Bills Of Lading ToBlockchain Structures: Part 1. New York: Law360. Retrieved from https://www.cadwalader.com/uploads/books/85a389ea712b15e94fa5b94fe3dcf892.pdf.
14. Shyshka, R., &Tkalych, M. (2020). The world in 2020: what are the threats to humanity? Amazonia Investiga, 9(26), 3-5.
15. Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. First Monday. Retrieved from https://firstmonday.org/ojs/index.php/fm/article/view/548
16. Tamimi, FA Moutasm, and AhidYaseen. "A Systematic Snapshot Review Of Custom-Made Software Enterprises From The Development Perspectives." (International Journal of Information Systems Management Research&Development (IJISMRD 9 (2019): 1-22.
17. Tredgett, R., Blizzard, K., Schultz, E., Smith, H., Post, C., Datoo, A., Devulder, S., Streiner, J., Jho, H., Fey, K., Chin., D., Mckeever, D., Farrell, Smith, A., Lewis, P., Hay, R., Lawless, J., Bleiberg, S., Maly, V., Franks, D., Rozovsky, J., Larsen, K., &Vivies, C.-E. de. (2019). Legal Guidelines For Smart Derivatives Contracts: The Isda Master Agreemen. International Swaps and Derivatives Association. Retrieved from https://www.isda.org/a/23iME/Legal-Guidelines-for-Smart-Derivatives-Contracts-ISDA-Master-Agreement.pdf.
18. Woebbeking, M. K. (2019). The Impact of Smart Contracts on Traditional Concepts of Contract Law. JIPITEC, 1, 106–113.
19. Tien, YuSeng, et al. "DecisionMakingwith Multi-CriteriaAssessment: How Firms to Select Appropriate Collaboration Partner?." International Journal of Business Management &Research (IJBMR) ISSN (P) (2016): 2249-6920.
20. Tulsidas, T. (2018). Smart Contracts froma Legal Perspective. Alicante:Universidad de Alicante. Retrieved from https://rua.ua.es/dspace/bitstream/10045/78007/1/Smart_Contracts_from_a_Legal_Perspective_Utamchandani_Tulsidas_Tanash.pdf.
21. Ting, D. (2017). Will Smart Contracts Disrupt the Legal Industry? TECHUP LAW. Retrieved from https://www.monash.edu/__data/assets/pdf_file/0006/973023/TechUp-Law-Publication-Final-1.pdf.