DOI 10.52468/2542-1514.2022.6(1).134-149

TOPICAL ISSUES OF THE REALIZATION AND PROTECTION OF HUMAN RIGHTS IN THE PRACTICE OF SMART CONTRACT TECHNOLOGY APPLICATION**

Svetlana S. Kuznetsova
Ural State Law University, Yekaterinburg, Russia

Article info
Received –
2021 November 14
Accepted –
2021 December 10
Available online –
2022 March 20

Keywords
Blockchain, smart contract, freedom of contract, individual's will, right to protection, personal data, internet of things, contract

The subject and the aim of the study. The article analyzes the approach to smart contract technology, which is reflected in the scientific literature and legislation of Russia and foreign countries, formulates the advantages and disadvantages of a smart contract that affect the implementation and protection of certain constitutional rights, including freedom of contract, the right to protect, the right to manage personal data.

Methodology. Guided by formal dogmatic and comparative law methods in research, the author formulates approaches to the concept of a smart contract that has been developed in the practice of foreign countries and deduces how each of the approaches affects the implementation of constitutional human rights. The paper notes that the use of a smart contract based on the federal blockchain does not allow the full implementation of such rights as freedom of contract, the right to self-defense, and the right to manage personal data. In addition, the transnational nature of smart contracts usage, their pseudonymity and failure to unified concept of legal regulation create obstacles to the effective implementation of the right to judicial protection.

The main results. The practice of legal regulation of smart contracts in foreign countries, aimed at minimizing the negative consequences of the use of technology is considered. Some countries follow to the concept of recognizing a smart contract as a form of contract (Italy, United States, Republic of Belarus) and a way of guaranteeing fulfilment of obligations (China, Italy, Republic of Belarus, Russian Federation). The second concept is considered as being the most restrictive for digital progress from one side but being able to guarantee protection of human rights such as right to judicial protection or freedom of contract. The first concept which shows smart contract being a type of contract carries additional risks associated with conclusion of a treaty - inconsistency of the smart contract with the actual will of the parties. The third concept considered smart contract as a type of contract is accepted in the Republic of Malta. The Republic of Malta regulated procedure of voluntary certification for smart contracts that allow to eliminate such threats as violation of human rights and the use of smart contracts for criminal purposes. The experience of legal regulation of smart contracts in the Republic of Malta is recognized as reasonable and effective, however, it is concluded that certification will achieve its goals only if it will be implemented in the legal system of wide range of the countries.

Conclusions. It is concluded that despite the fact that the smart contract technology has high potential for its implementation in various fields of social and economic life, the effective implementation of smart contract technology in various spheres of society requires the formation of general legal principles for their application, the definition of areas in which the use of smart contracts is prohibited, as well as the development of international standards for their safe execution.

** The study was funded with the financial support of the Russian Foundation for Basic Research for the project 18-29-16204 "The Legal Model of Realisation and Protection of Human Rights and Freedoms in the Internet".

ISSN 2658-4050 (Online)

1. Introduction.

For the first time, the concept of a smart contract was presented in the 1990's by the programmer Niko Sabo, who revealed its concept as "a set of promises, specified in digital form, including protocols within which the parties comply with these promises" [1] … The creation of a smart contract became possible with the emergence of blockchain technology, and its popularization and availability are associated with the establishment of the Ethereum online platform, the functionality of which allows anyone to contract using the Solidity programming language. By March 2020, more than two million such contracts were signed on the Ethereum platform; as of June 2021, about a quarter of Ethers were invested in smart contracts[1]. Smart contracts are concluded by legal entities and individuals throughout the world, in the Russian Federation they are used in the banking system[2], in the field of transportation[3], enforcement of supply contracts[4] and so on. The transformation of legal relations in the context of digitalization of society requires legal science and the state to take actions to determine the legal nature of a smart contract, its role in ensuring various types of relations, formulating legal means of implementing and protecting the rights of contract participants and other persons to minimize the negative consequences of its execution.

Smart contracts are the subject of research in various sciences: mathematics, energy, physics and astronomy, ecology, biology, chemistry and medicine, economics, finance, management, and social sciences (including jurisprudence), however, the main application is in the field of programming and engineering [2, p. 10]. In legal science, a smart contract is researched mainly within civil law relations: the problems of correlation of traditional contracts with smart contracts [3; 4, p. 40], the civil legislation is assessed in terms of its applicability to legal relations arising under smart contracts [5; 6, p. 322-328], the effectiveness of a smart contract as a guarantee of fulfillment of obligations, and also determines the type of contractual relationship that can be settled by smart contracts [7, p. 185] and so on. However, the scope of application of smart contracts is expanding every day: their potential, based on decentralized data storage, access to them by all trusted persons and self-executability, is used in the field of medicine [8, p. 23], energy [9], research activities, technologies of the Internet of things [10, p. 191] and artificial intelligence, and even when committing crimes. Considering the wide possibilities of using smart contracts, their study solely from the standpoint of assessing the potential in contractual relations does not allow the formation of a comprehensive understanding of the legal nature of a smart contract and current issues of its legal regulation, the impact of smart contracts on the implementation and protection of human rights. This work includes an analysis of scientific articles, legislation and law enforcement practice of the Russian Federation and some foreign countries to identify the existing concepts of a smart contract, formulate legal methods and means of their most effective application and minimize the negative consequences of execution. We also analyzed the impact of a smart contract on the implementation of freedom of contract, the right to protection (both jurisdictional and non-jurisdictional).

2. Smart contract legal concepts.

A smart contract is essentially a self-executing computer code developed based on a decentralized blockchain system. Since its capabilities were originally aimed at automating the fulfillment of obligations within the framework of

[1] Nearly 25% of All Ethereum Locked in Smart Contracts. URL: https://finance.yahoo.com/news/nearly-25-ethereum-locked-smart-051423561.html (date accessed: 17.07.2021).

[2] Sberbank was the first in Russia to receive a patent for blockchain REPO. URL: https://www.sberbank.ru/ru/press_center/all/article?newsID=a72d2afc-4991-4b38-bdd6-79630c64eae6&blockID=1303&regionID=77&lang=ru&type=NEWS (date accessed: 17.07.2021).

[3] Russian Railways and FESCO will implement a transportation smart contract. URL: https://company.rzd.ru/ru/9397/page/104069?id=263195 (date accessed: 17.07.2021).

[4] Smart revolution: Gazprom Aero introduces a smart contract based on blockchain technology. URL: https://www.gazprom-neft.ru/press-center/sibneft-online/archive/2018-october/1986863/ (date accessed: 17.07.2021).

ISSN 2542-1514 (Print)

civil law relations, a smart contract is often defined as “a computer protocol containing the terms of a contract. The initial conditions are embedded in the executable computer code that can work in the network” [11, p. 2901].

In legal science and practice, there are three main approaches to understanding smart contracts:

1. a special type of contract [12, p. 26];
2. the way of fulfilling contractual obligations [13, p. 15];
3. the form of the contract [14, p. 27-28].

The first concept is based on the distinction between the concepts of a smart contract and a smart legal contract. The proponents of that approach rightly note that a smart contract is by its nature a digital code, therefore such definitions as “self-executing electronic instructions drafted in computer code”, “a computer code stored in the blockchain, and access to which can be provided to one or more parties” [15, p. 179]. At the same time, a legal smart contract is a contract in which such technology is applied, “it is (i) a self-executing contract; (ii) whose text includes algorithm (iii) is stored in the DLT; (iv) which performs its predefined functions after the fulfillment of preconditions (v) and links two or more parties", and the implementation of which is possible within the framework of the legislation regulating traditional types of contracts. [15, p. 179; 16, p. 74; 17, p. 12].

The concept of a legal smart contract is used in the legislation of the Republic of Malta: in accordance with Article 2 of the Law on the Digital Innovation Authority, a smart contract means “a form of innovative technology arrangement consisting of a computer protocol and an agreement concluded wholly or partly in an electronic form, which is automatable and enforceable by execution of computer code, although some parts may require human input and control and which may be also enforceable by ordinary legal methods or by a mixture of both»[5]. In this definition, the emphasis is on the form of the contract and on the ability to ensure its conditions not only by automated, but also by legal means. In accordance with article 966 of the Civil Code of the Republic of Malta, the validity of a civil contract directly depends on compliance with four conditions - the legal personality of the parties to the contractual relationship, the presence of an expressed consent to accept certain obligations, the subject of the contract and the existence of a legitimate aim[6]. Omitting the problems of pseudonymization of smart contracts on some platforms, for example, Etherium, which often contributes to the conclusion and execution of smart contracts in relation to illegal objects of the contract, let us pay attention to the requirement of civil law - the legality of the goal. A feature of smart contracts is their ability to reflect only the objective elements of the contract, and therefore the purpose of the contract in a digital code cannot be fixed. If the parties to the agreement, following the laws of Malta, reflect the terms of the agreement both in writing (formulating the purpose of the agreement, identifying the parties to the agreement in order to confirm their legal personality, fixing all the terms of the agreement, the implementation of which requires the direct participation of the parties) and digital form of a smart contract, then there are no contradictions between the civil legislation of the Republic of Malta and the legislation on digital innovation. The reflection of all contractual conditions in a smart contract does not in any way interfere with the fulfillment of contractual obligations, however, the question arises of how the jurisdictional protection of the rights of a person whose rights were violated during its execution will be carried out. The legislator guaranteed an equal degree of protection to the parties to the smart contract in comparison with the subjects entering the traditional type of contractual relationship, but is the smart contract subject to assessment from the point of view of its compliance with civil law in case of applying for such protection? In our opinion - yes, however, in such a situation, it is difficult to perform such actions as assessing the legal personality of the parties (if a smart contract is concluded on a decentralized or federated blockchain platform) and determining the purpose of the contract.

In the United States of America, there is no

[5] Malta Digital Innovation Authority Act (MDIA), No. XXXI of 2018.

[6] Civil Code (Cap. 16) of Malta, 1868.

ISSN 2658-4050 (Online)

legislative regulation of smart contracts at the federal level, and therefore measures to introduce them into the legal space are taken by states. The legislation on blockchain and smart contracts has been adopted in the states of Arizona, Arkansas, Illinois, Nevada, North Dakota, Tennessee, the draft law is also being considered in the state of New York. A legal analysis of state legislation allows us to conclude that two main concepts of a smart contract have been formed in the United States - "some states have taken the path of recognizing a smart contract as a regular contract, other states have refused to recognize smart contracts as contracts, defining them as ordinary computer programs" [18, p. 82].

1. In the states of Arizona, North Dakota, New York, a smart contract refers to «an event driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger»[7]. In accordance with Arkansas law, a smart contract, as a program, performs not only the function of enforcing the terms of the contract, but also ensures the agreement of its terms, as well as verification of the contract.

2. In the state of Illinois, a smart contract is usually understood as a contract stored as electronic record which is verified using a blockchain.

The first approach is based on the recognition of the great potential of a smart contract, its ability to integrate into any type of legal relationship, where the possibilities of decentralized storage of information, resistance to its changes and automation of processes are in demand. While the second defines the limits of legal regulation of smart contracts exclusively by the scope of contractual relations. In our opinion, the first approach is preferable since it allows us to formulate the general principles of using the smart contract technology in any sphere, bridge a gap that can lead to a violation of human rights.

Assessing the legal nature of a smart contract, Yu. V. Truntsevsky and V. V. Sevalnev rightly note that, first of all, it is necessary to take into account its key feature - automatic execution: “a smart contract is software called a contract or not, but which allows you to automate the execution of an agreement contained directly in the SC itself or acting as an enforcement of an ordinary contract and recorded on the blockchain ”[19, p. 129]. This approach, in our opinion, is closest to the second legal concept of a smart contract, within which it is recognized as a way of fulfilling contractual obligations. This approach to new technology was recognized in France [20, p. 77] and the People's Republic of China. The People's Republic of China, being the world leader in the use of blockchain technology, including blockchain 2.0 - smart contracts, has not legally formulated the concept of a smart contract and its role in contractual and other legal relations. However, at the scientific symposium "Digital Economy, Blockchain and Law", the opinion was expressed that "a smart contract cannot be considered as a legal contract, it is rather a tool for the execution of contracts or an addition to a traditional contract"[8].

The second concept is reflected in civil legislation of the Russian Federation. In accordance with Article 160 of the Civil Code of the Russian Federation, “the written form of a transaction is also considered to be complied with if it is performed by a person using electronic or other technical means that make it possible to reproduce the contents of the transaction on a physical medium unchanged, and the requirement for a signature is considered fulfilled if used any way that allows you to reliably identify the person who expressed the will"[9]. The interpretation of this rule allows us to conclude that a smart contract as a computer protocol cannot be considered as an independent way of implementing the written form of a transaction. Since the creation and operation of a smart contract is carried out exclusively within the framework of a distributed blockchain network, it is not possible to reproduce its content on a physical medium. At the same time, in accordance with Article 309 of the Civil Code of the Russian Federation, a smart contract is recognized as a way of fulfilling promises under an

[7] Electronic Transactions Act, ARS § 44-7061; N. D. Cent. Code §9-16-19; NY Assembly Bill A3760.

[8] URL: http://www.zhonglun.com/Content/2020/01-09/1556473454.html (date accessed: 04.09.2021).

[9] Civil Code of the Russian Federation, part 1, 30th November of 1994, № 51.

ISSN 2542-1514 (Print)

agreement - “the terms of a transaction may provide for the performance by its parties of obligations arising from it upon the occurrence of certain circumstances without a separate expression of the will of its parties aimed at fulfilling the obligation through the use of information technology, determined by the terms of the transaction". It seems that the legislation of the Russian Federation does not prevent the conclusion of Ricardian contracts, which, being executed on the blockchain, unlike smart contracts, have a tangible form and represent not only a machine-readable digital code, but also a text that is readable by a person.

In some countries, the second and third concepts of the smart contract are equally recognized. So, for example, in accordance with the Decree of the President of the Republic of Belarus No. 8 dated December 21, 2017, a smart contract is understood as “software code intended for functioning in the register of transaction blocks (blockchain), another distributed information system for the purpose of automated execution and (or) execution of transactions or performance of other legally significant actions "(paragraph 9 of Appendix 1). The smart contract is testing and can be applied by a limited number of subjects - residents of the High Technologies Park[10] in contractual relations with each other (clause 5 of Decree No. 8) and in the field of banking services by the National Bank of the Republic of Belarus and participants of the identification system in legal relations with any individuals and legal entities (Clause 1.13 of the Decree of the President of the Republic of Belarus No. 148 dated April 18, 2019). The concept of a smart contract formulated in the legislation of the Republic of Belarus is broad, which does not limit the scope of application of a smart contract solely to civil law relations.

In the Italian Republic, a smart contract is also considered as a form of a contract and a way of fulfilling promises. In accordance with paragraph 2 of Article 8 of Law No. 12 of February 11, 2019, a smart contract is “a computer program that works based on distributed ledger technologies, and the execution of which leads to the automatic fulfillment of conditions previously agreed by two or more parties. Smart contracts meet the requirements of the written form of the contract, subject to identification of interested parties in the manner established by the Italian Digitalization Agency"[11]. Assessing the consolidated concept of a smart contract, the National Council of Notaries of Italy noted that to consider a smart contract as a form of the agreement is necessary with a certain degree of conditionality, since the structure of a smart contract is rather primitive, being “a computer program written in a programming language, a smart contract contains only executive instructions. It does not contain the "descriptive" part of the contract, since it is not necessary for processing by a computer ... but contains a payment order for a certain amount, while the obligation to pay can arise under different types of contracts (as a price under a sales contract, as a donation, how to fulfill credit obligations) "[12]. Thus, several options are proposed for adapting legislation to the operation of smart contracts: the inclusion in the text of smart contracts of elements that qualify the type of contract, the use of a smart contract in conjunction with a written contract, or

[10] In accordance with paragraph 1.13 of the Decree of the President of the Republic of Belarus "On Digital Banking Technologies" No. 148 dated April 18, 2019, the resident of the Park of High Technologies in accordance with the regulation "On the Park of High Technologies" (Appendix 3 to the Decree) can be legal entities and individual entrepreneurs carrying out activities in one or more areas (for example, design, software information systems, fundamental and applied research in natural and technical sciences, technical and cryptographic data protection, development and production of technologies, devices and systems of mechatronics, data transmission systems, technologies, devices and systems of radar, radio navigation, radio communications, radio control, radio frequency identification, high-tech materials, technologies, high-tech devices and systems and so on), registered in the manner prescribed by the regulation.

[11] Act № 12 of 11th February, 2019.

[12] L.12/2019– Smart Contract Technology Based on distributed ledger –Prime Note. National Counsil of Notaries. P.7. URL: https://www.notartel.it/notartel/contenuti/news/pdf-news/S-1-2019-DI.pdf (date accessed: 04.09.2021).

typification of smart contracts.

3. Freedom of contract and the problems of implementing the will of the individual in the process of executing a smart contract.

A smart contract is a new phenomenon in law, but its merits quickly attracted the attention of both business and ordinary network users. Its active implementation in various spheres of life of society and the state is due to such features as resistance to changes in information in a distributed blockchain system, transparency of transactions, automation of the execution of contractual promises. However, having several advantages, smart contracts are characterized by specific disadvantages.

First, the lack of understanding of the content of a smart contract for most of the potential participants. Since a smart contract is a digital code, its development, configuration and reading are possible only with the participation of specialists - programmers. Thus, the possibility of concluding a smart contract directly depends on the availability of a technical specialist and the level of trust of the parties to the contract.

The second disadvantage of smart contracts is technical vulnerability. The development of a smart contract requires professional knowledge; at the same time, there are often cases of errors in their preparation, the occurrence of bugs that can lead to hacking of a smart contract. For example, in 2016, more than 3.6 million ethers were stolen from the crowdfunding platform The Dao due to the imperfection of a smart contract[13]. In 2017, a code error in the Parity smart contract led to the illegal withdrawal of more than 150,000 ethers[14], and the error in the Tether smart contract cost about $ 30,000,000[15]. In 2018, more than $ 500,000,000 worth of cryptocurrencies were stolen from Coincheck.

The third drawback is the flip side of the inherent dignity of a smart contract - resistance to changes. On the one hand, the immutability of a decentralized smart contract with many nodes is an obstacle to the elimination of code errors that make smart contracts vulnerable. In addition, smart contracts are not always able to adapt to changing political, economic, social, and natural circumstances. Even though the problem of force majeure can be solved with the use of oracles, referring to them is effective only if the circumstance that prevents the execution of the contract can be foreseen by the parties to the contract. So, for example, the parties to the agreement can provide for a natural force majeure in the smart contract (an earthquake in a seismically hazardous area), and the oracle can daily check the occurrence of the corresponding condition - the fact of an earthquake. However, when smart contracts were concluded in 2019, no one could have foreseen the announcement in 2020 of the Covid-19 pandemic, respectively, and the oracle that checks the occurrence of this condition could not be launched either. Thus, the solution of the corresponding problems solely by technological measures is a rather complicated, high-cost process.

The definition of the nature of a smart contract, in our opinion, should be carried out not only from the position of its role in ensuring contractual relations, but also the implementation of other, including constitutional rights. In accordance with the Resolution of the Constitutional Court of the Russian Federation dated 02.23.1999 No. 4-P, freedom of contract is one of the constitutional freedoms guaranteed by the state, arising from the meaning of constitutional norms on freedom in the economic sphere (part 1 of Article 8, Articles 34 and

[13] Analytical review of Sberbank «Smart contracts», october, 2018. P. 12. URL: https://www.cbr.ru/Content/Document/File/47862/SmartKontrakt_18-10.pdf (date accessed: 09.09.2021).

[14] Hackers have stolen $32 million in Ethereum in the second heist this week. URL: https://www.businessinsider.com/report-hackers-stole-32-million-in-ethereum-after-a-parity-breach-2017-7 (date accessed: 09.09.2021).

[15] More than $30 million worth of cryptocurrency was just stolen by hackers, company says.URL: https://www.cnbc.com/2017/11/21/tether-hack-attacker-reportedly-steals-30-million-of-digital-tokens.html (date accessed: 09.09.2021).

ISSN 2542-1514 (Print)

35 of the Constitution)[16]. Freedom of contract in the 20th century was recognized as a constitutional principle, and often as a constitutional freedom, in the practice of many countries. For example, article 19 of the Chilean Constitution guarantees everyone the freedom to conclude contracts and freedom of work. " The Supreme Court of the United States was the first constitutional court in the world which adopted doctrine of constitutional protection of contractual freedom." [21, p. 17], in *Lochner v. New York* court ruled that the right to contract is guaranteed as freedom within the meaning of the 14th Amendment[17]. The Constitutional Tribunal of the Republic of Poland also recognized the existence of the principle of freedom of contract, noticed that it “should be considered in the light of guarantees of personal freedom, the concept of “autonomy of will” and requires that no one be forced to conclude a contract or refuse to conclude it, to choose a particular contractor or to include certain conditions in a contract, unless otherwise provided by law”[18]. In civil relations, there are two complementary principles - the principle of freedom of contract and the principle of binding contracts [22, p. 9].

Freedom of contract in accordance with Article 421 of the Civil Code of the Russian Federation includes such powers as freedom from coercion to conclude a contract, freedom to choose a counterparty, freedom to determine the subject of the contract and its type. However, in addition to these elements, the freedom to amend and terminate the contract cannot be denied as an authority within the framework of the freedom of contract: “those who have the right to conclude a contract of their own free will should be just as free in matters of terminating it or changing certain contractual conditions” [23, p. 48]. The peculiarities of the smart contract technology are manifested in the fact that after the development of an appropriate electronic protocol based on a distributed register, its execution is completely separated from the will of the parties: the fulfillment of promises is not in any way due to the need to commit acts, but changes in the content of a smart contract, suspension its execution or early termination when it operates in a decentralized blockchain with a large number of storage nodes is virtually impossible. Thus, the recognition of a smart contract as an independent type of contract, which can be concluded exclusively in electronic form, leads to derogation of the constitutional freedom of the contract.

During executing a smart contract, its parties may also face another problem related to the will in contractual relationship - the compliance of the content of the smart contract with their actual will. Being a digital protocol, a smart contract is readable only by programmers; in this case, the parties to the contract can hope that the specialist has correctly reflected their will in the self-executing code. In the Republic of Belarus, in clause 5.3 of the Decree of the President of the Republic of Belarus No. 8 of December 21, 2017, it is stipulated that "a person who made a transaction using a smart contract is considered to be duly aware of its conditions, including those expressed by the program code, until proven otherwise"[19]. ... Thus, the legislator has created a presumption of the actual will of the parties, which, on the one hand, imposes on the parties the obligation to take all reasonable measures to assess the smart contract from the position of reflecting the will of the parties, on the other, to prove the fact of receiving inaccurate information about the content of the smart contract in case of appeal for jurisdictional protection of their rights. To avoid a situation when a mistake is made by the encoder in the process of drawing up a smart contract, the UK Legal Commission considers it a potential opportunity for interested parties to contact at least two programmers, one of whom is developing a digital protocol project, and the second is an independent

[16] Decision of the Constitutional Court of the Russian Federation No. 4-P/1999.
[17] Lochner v. New York,198 U.S. 45 (1905).
[18] Wyrok Trybunału Konstytucyjnego z dnia 29 kwietnia 2003 r. sygn. akt SK 24/02.
[19] Decree of the President of Republic Belarus № 8, 21st of December 2017 «On the development of digital technologies ». URL: https://president.gov.by/ru/documents/dekret-8-ot-21-dekabrja-2017-g-17716 (date accessed: 19.09.2021).

ISSN 2658-4050 (Online)

audit[20]. Of course, this approach is quite reasonable, but it means that concluding an agreement exclusively in the form of a smart contract is still a lengthy process and no less financially costly, since intermediaries (encoders) will continue to play an important role. A smart contract can be economically beneficial for large market players who, having developed such a contract, will further conclude it with a wide range of persons, since they will reduce the costs associated with fulfilling promises.

The idea of auditing a smart contract was reflected in the legislation of the Republic of Malta - voluntary state certification of innovative technologies, including smart contracts, was proposed. In accordance with Appendix No. 1 to Innovative Technology Arrangements and Services Act, smart contracts are recognized as a category of innovative technologies, and services for the verification and audit of innovative technologies are innovative technological services (Appendix No. 2 to the law)[21]. In accordance with Article 7 of the Law, innovative technologies can be certified by an authorized body for use for various purposes with an assessment of such characteristics as quality, functions, parameters, execution procedure, scope of application. Based on the results of certification, a certificate of conformity is issued for a period of two years. An innovative technology can receive a certificate of conformity if the applicant complies with general (legality, good faith, transparency, compliance with the requirements of authorized bodies and accountability) and special requirements. The special requirements established for innovative technology arrangements to certification include:

a) fit and proper for the purposes for which it declares in the application to have been established and having the qualities, attributes, features, behaviors or aspects also therein declared;

b) verification of the software of the innovative technology by the system auditor, based on the results of which the latter confirms that:
- innovative technology meets reasonable standards in relation to specific aims, qualities, characteristics, functions, parameters and performance;
- the mechanism of the technology operates in the order indicated in the application, and all approvals submitted to the competent authorities, the technical administrator are working; - innovative technology meets the requirements established by the law, guidelines prepared by the Office of Digital Innovation and applicable to this type of technology.

c) the availability of a technical administrator who can demonstrate that the technology meets all the prerequisites for certification, its ability to consistently meet standards and solve critical problems, and how to solve them, the ability to change parameters or functionality in relation to those technologies for which such a requirement is established by law, and also demonstrate the availability of access of authorized bodies or a technical administrator to technology management and the correctness of its work;

d) compliance with legal requirements, including on the prevention of money laundering and terrorist financing, protection of personal data, respect for consumer rights and others; the presence of a built-in technological function that allows the technical administrator to intervene in the operation of the technology in a transparent and effective manner in the event of a significant loss to the user or violation of the law and in order to eliminate the causes of such violations;

e) the existence of an agreement on innovative technology, set out in English in an easily accessible and understandable format, on the basis of which the user is invited to use the technology, which describes the goals, characteristics, functions, parameters, quality and operation of the technology. In the event of a conflict between the English language and the basic agreement code, the English language shall prevail. If multiple languages are intended to be used in the agreement, in the event of a conflict between languages, the English version will prevail.

Thus, the law is aimed at eliminating such

[20] Smart Contracts: Call for Evidence. URL: https://www.lawcom.gov.uk/project/smart-contracts/ (date accessed: 23.09.2021).
[21] Innovative Technology Arrangements and Services Act, No XXXIII of 2018.

ISSN 2542-1514 (Print)

shortcomings of a smart contract as technical bugs that make it vulnerable to fraudulent activities, lack of transparency in the content of the digital protocol, as well as cases of human rights violations during the execution of a smart contract. To ensure the protection of human rights and ensure compliance with the legislation by the smart contract, certification provides for the mandatory provision of access of the technical administrator to the work of the smart contract, which allows making changes to it. In addition, certification of smart contracts makes it possible to ensure control over the legitimacy of their goals and the availability of its content to subjects wishing to join it. However, since this certification applies exclusively to smart contracts developed in the Republic of Malta and is optional, it cannot ensure the fight against those smart contracts that are aimed at illegal activities. In addition, the introduction of the requirement to have the text of the agreement in English, in detail and clearly reflecting the content of the smart contract, let us say that certified smart contracts are not considered a contract in the absence of a traditional form of consolidating its provisions.

In the Russian Federation, to avoid any potential difficulties with the establishment of the will of the parties to the contractual relationship, the legislation does not recognize the possibility of concluding a smart contract without reflecting the will of the parties in another form prescribed by law.

4. Smart contracts and the right to protection. The right to jurisdictional protection (by administrative and judicial authorities) is guaranteed both by international acts and by the constitutions of all countries of the world. Thus, for example, in accordance with article 8 of the Universal Declaration of Human Rights, “Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law”. In accordance with Article 45 of the Constitution of the Russian Federation, “state protection of human and civil rights and freedoms in the Russian Federation is guaranteed. Everyone has the right to defend their rights and freedoms in all ways that are not prohibited by law". The non-prohibited methods of protection should include both jurisdictional (administrative and judicial protection) and non-jurisdictional - self-defense.

Some authors are of the opinion that a well-written smart contract is an effective way to protect rights: since it provides automatic fulfillment of obligations with the help of oracles, it can contain algorithms that guarantee the effectiveness of self-defense [17, p. 32-33]. However, in our opinion, it is necessary to delimit the concepts - the effective implementation of rights and their protection: the automatic execution of the contract is a guarantee that the rights of its participants will be realized in the form in which they are reflected. If the content of a smart contract contradicts the rights, freedoms and legitimate interests of its participants or third parties, then such persons are actually deprived of the opportunity to take actions (or inaction) for the purpose of self-defense, for example, to refuse to execute it (if during execution it became clear about the illegality of its subject, if the party was misled regarding the subject of the contract, and so on).

In the framework of judicial protection of rights arising from the execution of smart contracts, it is necessary to highlight several potential problems:

- recognition of objects of a smart contract as a subject of protection; - pseudonymization of the parties to the contract;

- lack of a language accessible for understanding and interpretation by the judicial authorities;

- the order of execution of the decision of the courts.

Pseudonymization of the parties to a smart contract is carried out by cryptographic codification of user data, because of which access is retained only to the user's public key and transaction hashes. Thus, if we are talking about concluding a smart contract on a public platform, then its participants do not have sufficient information to identify each other. The service operator (the platform on which smart contracts are concluded) has access to information about the network user, but often the amount of such information is limited: ip-address, geolocation, information about the internal network. This information may not be available for the service operator or be incomplete if the user uses

ISSN 2658-4050 (Online)

anonymization tools in the online space, for example, vpn technologies. Due to the high level of pseudonymization within the blockchain platform, the question arises about the possibility of effective jurisdictional protection of persons whose rights were violated during the execution of the contract. As noted in the report of the UK Legal Commission, the fact that the parties to a smart contract do not have sufficient information about each other in accordance with the laws of England and Wales does not prevent them from accepting mutual obligations, "there is no requirement under the law of England and Wales for the parties to a contract to know each other's real identities. It is also not a concern with existing legal principles, but rather with the practicalities of being able to enforce a remedy"[22]. In the People's Republic of China, blockchain operators are responsible for identifying users, which follows from the provisions of the Law on Electronic Commerce[23]. The Chinese approach to cyberspace "is characterized by a greater state concentration on cybersecurity issues than is typical for Western democracies, which is manifested, among other things, in the adoption of measures to combat anonymity as an online phenomenon. In accordance with Article 27 of the Law "On Electronic Commerce", the operator of an online trading platform[24] must require persons who use this platform to sell goods and provide services to provide valid information about their identity, address, contact information, business license, and other necessary information, register a user, create a registration file, and check regularly for updates. Thus, if it becomes necessary to identify a participant in a smart contract, the operator of the blockchain platform is obliged to provide complete and reliable information about the user. The practice of protecting violated rights on the Internet that has developed over the past decades allows us to conclude that the very fact that a participant in a smart contract does not have information about his counterparty was not an obstacle to recourse to jurisdictional remedies. For example, in the United States of America and Canada, the practice of considering claims against persons whose data pseudonymized is widespread. Moreover, to ensure the protection of the rights of the latter, criteria for assessing the circumstances requiring disclosure of the identity of the participant in the case have also been introduced [24. p. 93-94]. A similar approach is taken in the UK: in the *Collier & Others v Bennett* case[25], the court recognized the use of the Norwich Pharmacal order to identify the defendant in the online defamation case. However, the question arises as to whether the court has real opportunities to obtain information about the participant of the smart contract due to the cross-border nature of blockchain platforms. In the People's Republic of China following the next concept of the sovereign Internet, it is not difficult to legally establish the requirement for identification of the person by an online trading platform, since only operators falling under the country's jurisdiction can operate there. At the same time, other countries are faced with the problem of cross-border operation of blockchain distributed ledger platforms, in connection with which it seems quite problematic to impose on the operators of the distributed ledger programs used to conclude smart contracts, the obligation to collect information about users, as well as requesting the relevant information in for the purposes of the jurisdictional protection of the rights of individuals.

Since not all countries carry out legal regulation of the blockchain, smart contracts, and the current regulation differs significantly from country to country, it is not necessary to count on the satisfaction of the operator of the service with the requirement of the court or other law enforcement agencies to provide information about the user. Thus, participants in a smart contract concluded on the basis of open access blockchains

[22] Smart Contracts: Call for Evidence. URL: https://www.lawcom.gov.uk/project/smart-contracts/ (date accessed: 28.09.2021).

[23] E-Commerce Law of the People's Republic of China, 2018.

[24] In accordance with Article 9 of the Law "E-Commerce", e-commerce platform operator means legal persons or other unincorporated organizations that provide online business premises, transaction matching, information distribution and other services to two or more parties to an e-commerce transaction so that the parties may engage in independent transactions

[25] [2020] EWHC 1884

should be aware that they are taking on the risk of certain adverse consequences associated with pseudonymization: the likelihood that the opposing party will be a person without the necessary legal capacity, as well as the existing probability the fact that the right to jurisdictional protection will not be fully realized due to the lack of the ability to enforce the court's decision due to the transboundary nature of the agreement.

The concept of recognizing a smart contract as a way of fulfilling obligations assumed by the parties under a civil law contract, in force in the Russian Federation, is aimed at eliminating the negative consequences associated with its execution: the parties actually cannot remain anonymous to each other, the classical form of the contract allows to guarantee protection the rights of the parties due to its recognition in all countries (that is, the likelihood of complications in the execution of decisions on the territory of other states is minimized), however, from the point of view of the development of technology, this approach is undoubtedly restrictive.

5. Smart contracts and the internet of things

The Internet of Things technology is currently used in various spheres of life: agriculture, mechanical engineering, healthcare, energy, in the market of goods and services, in the systems of "smart city", "smart home" and so on. Ensuring the reliability and security of information that is processed by devices based on the Internet of Things technology is one of the most important areas of guaranteeing the security of the technology and its performance. Therefore, with the advent of blockchain technology, the question of the possibility of its application in conjunction with the technology of the Internet of Things has become one of the most important topics of scientific research.

In 2016, Ferrer, while investigating the issue of the applicability of blockchains for robotic swarm systems, noted that blockchain is a good way to ensure distributed decision making, which is necessary to achieve consensus and a single goal within the robotic swarm system [25, p. 1041]. This study presents the integration of blockchain into robotic systems, detailing its benefits in terms of security, consensus, and transparency. In 2019, Innopolis University investigated the issue of applicability in the work of robots not only of the idea of a distributed ledger, but also of a smart contract to ensure their ability to independently make decisions based on the distribution of responsibilities between robots in multi-robotic systems and unmanned aerial vehicles [26, p. 6].

Assessing the possibility of using smart contracts in ensuring the operation of the Internet of Things technology, Gregor Schmitt et al. note that the advantages of a smart contract must be assessed considering three aspects that form the basis for companies making a decision to implement a new technology in their activities - manufacturability, organization, environment. Evaluating smart contracts from the standpoint of manufacturability, the researchers concluded that their use will certainly bring the technology of the Internet of Things to a new level, but today smart contracts have not reached the necessary technological qualities. The organizational context of the implementation of smart contracts on the Internet of Things is faced with several problematic aspects, including security issues: the complexity of programming smart contracts and the need for a high level of trust in their developers, their high professionalism, which would allow developing a smart contract strictly in accordance with specification and no code vulnerability. The context of the environment in which the implementation of a smart contract is possible is assessed in terms of relationships with society, government, competitors, and the industrial sector. Within the framework of it, it is extremely important to assess the readiness of the legal environment to ensure legal regulation of the introduction of new technology. So, for example, there is a problem of ensuring compliance by smart contract technology with European legislation on the protection of personal data (in terms of ensuring the implementation of the right to be forgotten) and civil legislation in terms of the compliance of a smart contract with its contract requirements, recognition of a smart contract as invalid, and so on [10, p. 193-195].

Indeed, the technology of the Internet of Things is based on the accumulation of information about its users [27, p. 32], and since such

ISSN 2658-4050 (Online)

information is inherently personal, its storage and processing require strict observance of the legislation on the protection of personal data, including ensuring the security of its storage, restricting access to it by third parties, and exercising the powers of the subject of law. Since individual items operating based on the Internet of Things technology often interact with each other (for example, individual items within the "smart home" system, a phone and various smart devices that track information about the user's health, track applications, and so on) create a single environment, then we can talk about the formation by them of a single user profile, information in which may contain special categories of personal data. “Decentralization is a core principle of the blockchain based smart contracts. The decentralization in blockchain makes the transaction ledger and smart contracts transparent to all peers in the network as a feature of security. User privacy is highly concerned in some significant applications of blockchain based smart contracts. The users incorporate the smart contracts are required to be private in certain circumstances. For instance, the solutions like health information systems do not prefer by the users if the personal identity information being revealed in the ledger”[28, p. 87652-87653]. Today, software engineers are taking measures to improve the blockchain and smart contract, to form a new model that could, while maintaining the transparency of information to ensure the stability of the system, preserve the confidentiality of personal data. However, it must be agreed that the use of a federated smart contract for storing personal data or its implementation of the Internet of Things technology, which allows the collection of data, is unacceptable until the moment when the blockchain technology is improved.

6. Conclusions

Blockchain technology originated as the backbone of the government-free Bitcoin payment system. Its decentralized nature, ensuring resistance to changes in the information stored in it, was seen as a guarantee of the implementation of the rights of its users, where the user community acted as a guarantor. A smart contract developed based on blockchain technology, in its essence, also assumed self-regulation, the ability to ensure the rights of participants in contractual relations without resorting to jurisdictional methods of protecting rights. However, the practice of using smart contracts, their implementation in various spheres of human life, requires once again to turn to the question of whether smart contract technology can act as an effective alternative means of ensuring the protection of human rights in the digital space. A number of authors adhere to the position that, due to the rapid development of digital technologies, their state legal regulation is losing its significance, since the state is not able to quickly respond to the challenges that society faces with the emergence of new technologies. Therefore, self-regulation is the most acceptable means of resolving current issues [29, p. 255]. Other researchers note that freedom from government regulation in the digital space can become a threat: “While allowing for anyone to implement and deploy their own techno-legal frameworks has strong democratic potential, if coopted by the current economic or political order, the process might possibly lead to a regime of inflexible (perhaps even totalitarian) networked governmentality” [30]. The need to bring legislation and smart contract technology to a single consensus to ensure the protection of human rights is also mentioned in a thematic report prepared within the framework of the European Union's Blockchain Observatory and Forum program[26]. In our opinion, blockchain technology and smart contracts require state legal regulation, which is due to several circumstances:

1. A smart contract as an innovative technology has a direct impact on the implementation and protection of human rights. As noted earlier, resistance to change, as an integral feature of a smart contract, prevents the implementation of constitutional freedom of contract in the form of changing the terms of the contract and refusing to fulfill obligations. The digitally codified form of a smart contract does not

[26] Legal and regulatory framework of blockchains and Smart Contracts: Thematic report. 2019. P. 11 URL: https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf (date accessed: 21.10.2021)

ISSN 2542-1514 (Print)

allow technology users to familiarize themselves with the content of a smart contract, which can lead to distortion of the will of the parties. Its transparency and controllability by a wide range of users raises concerns about the ability of smart contract technology to protect the information stored in it containing personal data of individuals, as well as to amend or delete the relevant information. The pseudonymization of treaty parties and the global nature of the platforms on which smart contracts are concluded give rise to the risk of impossibility of jurisdictional protection of rights violated during its execution. Since the implementation and protection of these rights directly depends on the fulfillment by the state of its obligations to provide the individual with appropriate legal means, ignoring the problems that a person encounters when working with a smart contract is unacceptable.

2. Smart contracts are not only an object, but also an instrument of crime, in connection with which the term “criminal smart contracts” began to be used in science [31, p. 283]. The pseudonymous nature of smart contracts, in conjunction with the use of digital currency, allows them to be used to finance criminal activities, including terrorism, transfer funds to commit "ordered" crimes, sell information classified as secrets, and launder money illegally obtained and create a "zero-day vulnerability". The wide possibility of using smart contracts in criminal activity requires regulation of its status not only from the position of ensuring the implementation of civil law relations, but also ensuring national security. However, today there is no comprehensive legislation in this area; the fight against cybercrime using smart contracts is carried out through the legal regulation of token circulation.

Speaking about what the regulation of smart contracts must be, several important aspects should be noted:

- The legislative definition of smart contracts should be the broadest, which would allow the law to adapt to changing conditions, to changes in the digital space. Thus, the definition of a smart contract as a technology directly related exclusively to civil law relations may constrain its development potential.

- Legal regulation of smart contracts is necessary to the extent that will ensure the implementation of human rights and their protection, for example, by establishing areas in which the use of smart contracts should be prohibited to comply with the principles of humanism, the rule of law (for example, when conducting medical interventions, for military purposes, and so on). The experience of the Republic of Malta in establishing requirements for smart contracts as a technology for their certification is also interesting.

– - Due to the transnational nature of the use of smart contract technology, ensuring the observance and protection of human rights is possible when forming international standards for the safe execution of smart contracts, as well as the interaction of states in the fight against criminal smart contracts and promoting the protection of human rights.

ISSN 2658-4050 (Online)

REFERENCES

1. Szabo N. Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought*, 1996, no. 16, vol. 8, iss. 1, pp. 50–53, 61.

2. Salmerón-Manzano E., Manzano-Agugliaro F. The Role of Smart Contracts in Sustainability: Worldwide Research Trends. *Sustainability*, 2019, vol. 11, iss. 11, art. 3049. DOI: 10.3390/su11113049.

3. Diadkin D., Usoltsev Y., Usoltseva N. Smart-Contracts in Russia: Prospects for Legislative Regulation. *Universum: Ekonomika i yurisprudentsiya*, 2018, no. 5 (50), available: http://7universum.com/ru/economy/archive/item/5806. (In Russ.).

4. Savelyev A.I. Contract Law 2.0: "Smart Contracts" and the Beginning of the End of the Classic Contract Law. *Vestnik grazhdanskogo prava = Civil Law Review,* 2016, no. 3, pp. 32–60. (In Russ.).

5. Chub D.V. Legal Regulation of Smart contracts in France. *Aktual'nye problemy rossiiskogo prava = Actual Problems of Russian Law,* 2019, no. 8 (105), pp. 151–158. DOI: 10.17803/1994-1471.2019.105.8.151-158. (In Russ.).

6. Raskin M. The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, 2017, vol. 1, iss. 2, pp. 305–341.

7. Rodionova O.M. Civil-Legal Nature of the Consequences of Signing Smart Contracts. *Probely v rossiiskom zakonodatel'stve = Gaps in Russian Legislation*, 2017, no. 6, pp. 183–185. (In Russ.).

8. Khatoon A. A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics*, 2020, vol. 9, iss. 1, art. 94. DOI: 10.3390/electronics9010094.

9. Kirli D., Couraud B., Robu V., Salgado-Bravo M., Norbu S., Andoni M., Antonopoulos I., Negrete-Pincetic M., Flynn D., Kiprakis A. Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*, 2022, vol. 158, art. 112013. DOI: 10.1016/j.rser.2021.112013.

10. Schmitt G., Mladenow A., Strauss C., Schaffhauser-Linzatti M. Smart Contracts and Internet of Things: A Qualitative Content Analysis using the Technology-Organization-Environment Framework to Identify Key-Determinants. *Procedia Computer Science*, 2019, vol. 160, pp. 189–196. DOI: 10/1016/j.procs.2019.09.460.

11. Khan S.N., Loukil F., Ghedira-Guegan C., Benkhelifa E., Bani-Hani A. Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Networking and Applications,* 2021, no. 14, pp. 2901–2925.

12. Efimova L.G., Sizemova O.B. The Legal Nature of a Smart Contract. *Bankovskoe pravo = Banking law*, 2019, no. 1, pp. 21–28. DOI: 10.18572/1812-3945-2019-1-21-28. (In Russ.).

13. Vashkevich A.M. *Smart Contracts: what, why and how*. Moscow, Simploer Publ., 2018. 89 p. (In Russ.).

14. Volos A.A. (ed.) *The Concept of the Legal Regulation of Relations Connected with Smart Contracts*. Moscow, Prospekt Publ., 2021. 224 p. DOI: 10.31085/9785392335817-2021-224. (In Russ.).

15. O'Shields R. Smart Contracts: Legal Agreements for the Blockchain. *North Carolina Banking Institute*, 2017, vol. 21, iss. 1, pp. 177–195.

16. Durovic M., Janssen A. The Formation of Smart Contracts and Beyond: Shaking the Fundamentals of Contract Law?, in: DiMatteo L., Cannarsa M., Poncibo C. (eds.) *Smart Contracts and Blockchain Technology: Role of Contract Law*, Cambridge University Press, 2019, pp. 61–79. DOI: 10.1017/9781108592239.

17. Camilleri L. *Blockchain based Smart-Contracts' Legal Enforceability in Malta and the UK: a Square peg in a Round Hole?* University of York Publ., 2019. 58 p.

18. Efimova L.G., Mikheeva I.V., Chub D.V. Comparative Analysis of Doctrinal Concepts of Legal Regulating Smart Contracts in Russia and Foreign States. *Pravo. Zhurnal Vysshei shkoly ekonomiki = Law. Journal of the Higher School of Economics*, 2020, no. 4, pp. 78–105. DOI: 10.17323/2072-8166.2020.4.78.105. (In Russ.).

19. Truntsevky Yu.V., Sevalnev V.V. Smart Contracts: from Identification to Certainty. *Pravo. Zhurnal Vysshei shkoly ekonomiki = Law. Journal of the Higher School of Economics*, 2020, no. 1, pp. 118–147. DOI: 10.17323/2072-8166.2020.1.118.147. (In Russ.).

20. Barbry E. Smart contracts... Aspects juridiques! *Réalités Industrielles*, 2017, August, pp. 77–80. (In France).

21. Szwed M. *Constitutional protection of freedom of contract in the European Union, Poland and the United States and its potential impact on the European contract law*. Central European University Publ., 2014. 87 p. Available at: http://www.etd.ceu.hu/2014/szwed_marcin.pdf.

22. Karapetov A.G., Savel'ev A.I. *Freedom of contract and its limits*, in 2 volumes. Moscow, Statut Publ., 2021. Vol. 1. 452 p. (In Russ.).

23. Braginskii M.I., Vitryanskii V.V. *Contract Law: general provisions.* Moscow, Statut Publ., 2020. 848 p. (In

Russ.).

24. Salikov M.S. (ed.) *The right to access the Internet, anonymity and identification of users (constitutional legal problems)*. Yekaterinburg, UMC UPI Publ., 2020. 167 p. (In Russ.).

25. Ferrer E.C. The blockchain: A New Framework for Robotic Swarm Systems, in: Arai K., Bhatia R., Kapoor S. (eds.) *Proceedings of the Future Technologies Conference (FTC) 2018*, Springer Publ., 2018, vol. 2, pp. 1037–1058. DOI: 10.1007/978-3-030-02683-7_77.

26. Afanasyev I., Kolotov A., Rezin R., Danilov K., Mazzara M., Chakraborty S., Kashevnik A., Chechulin A., Kapitonov A., Jotsov V., Topalov A., Shakev N., Ahmed S. *Towards Blockchain-based Multi-Agent Robotic Systems: Analysis, Classification and Applications.* 2019. 10 p. Available at: https://arxiv.org/abs/1907.07433.

27. Pasquier T., Bacon J., Eyers D. Personal Data and The Internet of Things. *Communications of the ACM*, 2019, vol. 62, no. 6, pp. 32–34. DOI: 10.1145/3322933.

28. Hewa T., Hu Y., Liyanage M., Kanhare S., Ylianttila M. Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research. *IEEE Access*, 2021, no. 9, pp. 87643–87662. DOI: 10.1109/ACCESS.2021.3068178.

29. Minbaleev A.V. The Place and Role of Self-regulation in the Development of Digital Technologies. *Obrazovanie i pravo*, 2019, no. 1, pp. 253–256. (In Russ.).

30. Filippi P., Hassan S. Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday*, 2016, vol. 21, no. 12. DOI: 10.5210/fm.v21i12.7113.

31. Juels A., Kosba A., Shi E. The Ring of Gyges: Investigating the future of criminal smart contracts, in: *CCS '16*, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, United States, Association for Computing Machinery Publ., 2016, pp. 283–295. DOI: 10.1145/2976749.2978362.

INFORMATION ABOUT AUTHOR

Svetlana S. Kuznetsova – PhD in Law, Associate Professor, Department of Constitutional Law
Ural State Law University
21, Komsomol'skaya ul., Yekaterinburg, 620137, Russia
E-mail: kss001@usla.ru
RSCI SPIN-code: 3387-9420; AuthorID: 804404
ORCID: 0000-0003-2426-8055

BIBLIOGRAPHIC DESCRIPTION

Kuznetsova S.S. Topical issues of the realization and protection of human rights in the practice of smart contract technology application. *Pravoprimenenie = Law Enforcement Review*, 2022, vol. 6, no. 1, pp. 134–149. DOI: 10.52468/2542-1514.2022.6(1).134-149. (In Russ.).