LEGAL PRACTICE IN THE BLOCKCHAIN ERA: THE USE OF ELECTRONIC EVIDENCE

Denis Grigoryevich Zaprutin
Galina Nikiporets-Takigawa
Vitaly V. Goncharov
Vladimir Dmitriyevich Sekerin
Anna Evgenievna Gorokhova

Abstract: This article examines the current trends in the development of the justice system due to the influence of digitalization in the Russian Federation, expressed in the use of digital technologies that complement the traditional system of evidence. The use of evidence obtained using e-mail, electronic digital signature, electronic documents, etc. is becoming more widespread. The purpose of this article is to study the current state and assess the prospects for using electronic evidence, the nature of which is related to the blockchain technology, in legal practice. Based on the legal provisions of criminal and civil proceedings, the types of electronic evidence that are reduced to written and physical evidence, explanations of persons involved in the case, expert opinions, expert consultations, witness statements, as well as audio and video recordings are systematized. The methods of using electronic evidence in litigation existing in international law enforcement practice are described, which, on the one hand, are limited to their interpretation based on the use of electronic signatures and, on the other hand, the application of the norms of traditional civil, criminal and administrative processes establishing general procedural features for evaluating evidence. The problems of using electronic evidence in Russian legal proceedings are highlighted. The absence of a legally established definition of an electronic document as
evidence and the grounds on which it can be attached by the court to the materials of the case under consideration, the discussion on the form in which electronic documents should be presented as evidence, as well as the problems of evaluating digital evidence from the position of admissibility, relevance, and reliability are analyzed.

**Keywords:** electronic evidence, digital technologies, blockchain, trial, proof

**Introduction**

The rapid development of information technologies has led to the emergence of blockchain technology, which is a way to store information by decentralizing data regarding transactions with a certain digital asset and building chains of blocks of hashed records about such transactions (Vasyukov et al., 2019; Kuteynikov et al., 2020; Kirillova et al., 2020). Such a technological solution makes it possible to simultaneously ensure the direct transfer of such assets and record reliable data about their ownership to the relevant persons (Savelev, 2014). The first well-known application of this file storage method was the formation of the transaction registry of the widely known Bitcoin cryptocurrency in 2008. At that time, the idea of blockchain was not fully appreciated, since it was the basis of a new phenomenon of cryptocurrencies and was not positioned as a self-sufficient concept. However, its potential has been appreciated over time and is currently being successfully developed in the framework of such innovative methods as, for example, conducting ICO (Initial Coin Offering) business projects or creating public registers of property rights. Leading companies in the world are beginning to take advantage of the use of blockchain. For example, the financial conglomerate HSBC and the investment division of Bank of America use blockchain to simplify operations under international agreements. Financial and technological startups based on blockchain technology attract significant amounts of investment (Daneeva, 2018).

At this time, there is an increased interest in the prospects of using blockchain from not only international corporations but also several states, which can be seen in the increased number of corporate and academic research published in recent years. Thus, in 2016, the UK State Department of Science released a report on blockchain development trends
(Distributed Ledger Technology: beyond blockchain, 2016). It noted that the blockchain can be effectively used not only in the financial sector but in all industries that require confirmation of any events. The digital register can be programmed to safely store any information, including legally significant ones: birth, marriage, and death certificates, higher education diplomas, electoral votes, and many other data that can be represented as a code. It will be possible to register any information and protect it from unplanned or illegal changes with the help of the blockchain. The Oxford researcher Joshua Broggi is the founder of a training organization in Malta, operating based on blockchain technology. The new university plans to use blockchain to reduce operating costs by automating administrative procedures. The impossibility of changing data in the blockchain will serve as proof of the reliability of the education received by the student (Ark, 2018). Blockchain technologies, in this context, can serve, for example, as a technological form of notarization, intellectual property management (Bayón, 2019), as an evidence base for the originality and novelty of the intellectual property object, or as a confirmation of primary ownership. Thus, blockchain technology is promising in the context of determining the possibility and effectiveness of its use in a modern system for storing data on significant legal facts, including taking into account its possible extraterritorial effect. This perspective, in turn, opens up opportunities for its use in evidentiary procedures in the administration of justice in civil, arbitration, criminal, and administrative processes.

The issues of using evidence obtained or stored using blockchain technology, due to the wide distribution of this technology in all areas of public relations, are becoming increasingly relevant. This is evidenced by the interest shown by researchers. The problems of using blockchain technology in the administration of justice were considered by such scientists as A. Levashov (2017), Wu, H., Zheng, G. (2020), Grigoryev VN Sukhodolov and others (2019). However, the available research is not yet sufficient to define the concept and procedure for using electronic evidence (Kostenko, Tokarenko, 2018; Kostenko, Rudin, 2018; Bekishev et al., 2019).
especially related to blockchain, as well as the possibilities of blockchain technology in proving. Therefore, new scientific research, where an attempt to solve these problems will be made, should only be welcomed. Research hypothesis. Blockchain technology can be used in the evidentiary process, ensuring the reliability and safety of evidentiary information.

**Methods**

The dialectical method of cognition of reality was taken as the basic method of this study, along with the use of methods of theoretical generalization, comparative analysis, analysis and synthesis, and the statistical method, which made it possible to justify the need to develop legal acts designed to regulate social relations arising from the use of electronic evidence in Russia and to determine their criteria. The formal legal method allowed identifying concepts that can be included in the projected regulatory regulation. The method of transition from a general concept to a particular one allowed distinguishing digital evidence from the general concept of electronics. The information basis for proving the research hypothesis was the works of Russian and foreign scientists on the nature and use of electronic evidence in court proceedings, and information about court decisions available on the Internet.

**Results**

The modern digitalization of the economic and legal space of both the world community as a whole and the Russian one, in particular, is accompanied by significant changes caused by the reform of the justice system. At the present stage, Russia is actively implementing digital technologies in the process of administration of justice. This is expressed, inter alia, in the introduction and gradual use of media technologies that complement the traditional evidence system. Thus, the existing types of evidence are supplemented by technological capabilities, which are expressed in the use of electronic signatures, electronic documents, data received from the e-mail, etc. In this regard, there is a problem of competent and legally justified use of evidence obtained through the use of various electronic devices (computers, smartphones, etc.).
One of the important points is the need to study the effects that arise in connection with the lack of theoretical and legal support for the digitalization of justice when they come in contact with the classical institutions of procedural law.

The statement by V.G. Golubtsov that the concept of evidence is uniform in all procedural branches of law seems fair, and the differences in their definition are whether the exhaustive list of types of evidence is established by the relevant code and which types of evidence are legally fixed (Golubtsov, 2019). Accordingly, the rules on the admissibility of evidence can also be considered practically general. This approach is also applied in this article when studying the opinions of processualists in the field of criminal and civil (arbitration) proceedings.

Today, there is a general trend towards the regulation of digital relations in the field of criminal law (Spasennikov, Shvyrev, Smirnov, 2015; Apergis, Kunitsyna, Dyudikova, 2020; Dudin et al., 2020) and legal proceedings, while attention is drawn to the lack of uniformity in the understanding of the rules governing digital relations in the field of criminal justice, but also common approaches to this activity (Grigorev et al., 2019). Quite literally Russian criminal proceedings were not fully prepared for "electronic" changes in public life. New phenomena of the material world are introduced into practical and scientific activities, which leads to the formation of new concepts. An electronic proof is currently in the stage of understanding and theoretical justification.

Researchers, in accordance with their positions, can be divided into those who propose to include electronic evidence in the established list, referring them to physical evidence (Krasnova, 2013) or other documents (Tkachev, 2014) and those who consider it necessary to include electronic evidence in the list of evidence as a separate type of admissible evidence (Pastukhov, 2015). It seems that the differences outlined above arise from the difficulty in determining the appropriate way to record electronic information, which would allow implementing the cognitive and authentication functions of recording most effectively. At the same time, researchers have previously noted that in relation to electronic evidence, the problem arises primarily in the
implementation of the authentication function (Chegodaeva, 2014).

In the arbitration process, electronic (digital) evidence is also a relatively recently used type of evidence in court proceedings, which in its internal content is expressed in the form of an electronic document, audio or video recording of an event (Zakharenko, 2018). The following approaches to the interpretation and use of electronic evidence have been developed in arbitration court practice: 1. The use of electronic documents as evidence by the court as a tool used in the presentation of evidence. Federal Law of July 27, 2006, N 149-FL "On Information, Information Technologies and the Protection of Information" defines an electronic document as information that, on the one hand, can be received and analyzed using electronic computers, and on the other, transmitted using information systems (Clause 11.1, Article 2) (Federal Law No. 149-FL, 2006). Thus, an electronic document is a piece of information that is recorded by electronic means of communication or on electronic media. 2. The use and assessment of electronic evidence following general rules regulated by the legislation of the Russian Federation (Lunev, Meliksetyan, Mikhnevich, 2018). In the first case, an electronic document that was received by facsimile and electronic communications, including the Internet, will be taken into account as written evidence in the manner prescribed by the relevant regulatory legal acts of the Russian Federation, in this case, part 3 of article 75 Arbitration Procedure Code of the Russian Federation (APC RF) (The Code of Arbitration Procedure of the Russian Federation N 95-FL, 2002). In particular, it implies the use of documents signed with an electronic digital signature (EDS). Accordingly, the rules of Art. 71 of the APC of the Russian Federation, establishing the procedural features of the assessment of evidence are used as part of the second approach to the assessment of electronic evidence. Thus, this method of evaluating the information provided to the court as evidence delegates its participants more opportunities for proof, which cannot be noted in the context of the first approach, for which the content of an electronic signature in an electronic document is fundamental. It is worth noting that the content of the concept of an electronic document, declared by the Federal Law of July 27, 2006, N 149-FL, does not
contradict the legal provisions presented in the framework of the APC of the Russian Federation. However, this Code, as well as many other regulatory legal acts covering procedural aspects of the use of electronic evidence, does not cover the legislatively established definition of an electronic document as evidence and does not specify what features it should possess, as well as what principles of use should be used for an electronic document to be identified as admissible evidence and based on this attached to the case (Nakhova, 2018). However, reducing the essence of an electronic document solely to the form of written evidence is not entirely justified from the point of view that the electronic document does not have the author's uniqueness, and also does not have a written form. In addition, there is such a problem of using electronic evidence in the arbitration process as the presence of debatable issues related to the assessment of digital evidence from the position of admissibility, relevance, and reliability (Article 71 of the APC of the Russian Federation). Since the APC of the Russian Federation does not specify and does not concretize the features that an electronic document must have to be accepted by the court for consideration and resolution of the case, it is possible to use only general properties that are distinctive for all types of evidence: – contains information that establishes or refute the circumstances based on which a dispute arose between participants in the arbitration process; – an electronic document should be received, processed, and accepted in the structure of the legal proceedings only subject to compliance with the procedural rules for collecting evidence. As a result, the current arbitration courts, administering justice in a particular case, in the absence of more substantive features as electronic evidence, accept material evidence in the form of audio and video recordings, and written – in the form of a text document, received and established in the manner prescribed by the legislator (Rudneva, Kraskina, Nikonova, 2020).

Discussion

However, problems related to the regulation of electronic evidence are not specific to Russian legal proceedings. The laws of some states do not recognize evidence obtained by electronic means and consider it secondary (Can Electronic Documents Be Used As Evidence International Law Essay approach to the expressive
function of international criminal justice, n.d.). A study conducted by the International Telecommunication Union concluded that the admissibility of electronic evidence in European courts is governed by general provisions that also apply to traditional evidence (Grigorev et al., 2019). There are only some elements of regulation related to this area. No country in Europe has a definition of electronic evidence in its legislation. There are also no developed national rules related to the admissibility of electronic evidence (Grigorev et al., 2019).

The vast majority of European judges perceive electronic evidence as an equivalent of traditional evidence (The Admissibility of Electronic Evidence in Court: Fighting Against High-tech Crime, 2006).

The widespread use of computers in recent years has led to the emergence of a new type of electronic evidence in criminal cases — digital evidence.

Digital evidence is conceptually the same as any other evidence — it is the information used to place people and events in time and space, to establish, for example, causality for criminal incidents (Sukhodolov et al., 2017). However, digital evidence has a broader scope, can be more sensitive, mobile, and requires training, other tools, and methods for extracting data from digital devices.

Orin Samuel Kerr (USA) considers whether traditional criminal procedure rules can effectively regulate investigations involving the use of digital evidence. Professor Kerr concludes that new methods of collecting digital evidence require new legal standards, new rules for collecting physical evidence and testimony using digital technologies (Kerr, 2005). One of these technologies is the blockchain technology.

In particular, the experience of US law enforcement agencies shows that it is possible to effectively use the publicity and transparency of blockchain technology in the investigation of crimes that somehow involved payments with cryptocurrencies (Levashov, 2017). The traditional use of analogy in the framework of case law, combined with high technological support for law enforcement, allowed them to quickly develop certain methodological approaches to the investigation of crimes related to the use of cryptocurrencies. In particular, the previously mentioned publicity property of the blockchain...
record registry is actively used, which was demonstrated in the indictment against the alleged owner of the electronic cryptocurrency exchange BTC-e, Alexander Vinnik. As stated in the conclusion, "in some cases, bitcoin payments can be effectively tracked through blockchain analysis" (Vinnik Superseding Indictment, 2017).

According to P.S. Pastukhov, "The cryptographically secure hash function of the blockchain technology can be used to confirm any electronic information, including audio and video files recorded using various technical means. When copying such information to an external storage device, it is necessary to calculate a hash function that will serve as a confirmation of the immutability of the original information" (Pastukhov, 2015). Moreover, documentation involves the most complete description of the technical means by which the creation and subsequent logical interaction with data in an electronic environment took place (Pastukhov, 2015). Information about the files being examined should also be recorded. The described procedures will collectively meet the standards of the IOCE (International Organization on Digital evidence), established in 2000, and containing basic principles and approaches to the collection of electronic evidence (Grigorev et al., 2019). The specifics of the electronic environment as a system of objects interacting based on formal rules for processing, storing, and transmitting information presented in digital form (Kukarnikova, 2003) require the development of fundamentally new approaches to the investigation of cybercrime. It seems that the existing forensic techniques, tactics, and methods are in many ways not applicable for the formation of the evidence base, which suggests a possible need "to abandon the existing list of sources of evidence, which is given in part 2 of Art. 74 of the Code of Criminal Procedure of the Russian Federation as an obsolete anachronism" (Pastukhov, 2015). At the same time, it is reasonable to make the most in-depth analysis of publicly available information in electronic networks.

At the moment, international practice is discussing the use of blockchain technology in the administration of justice, as, for example, this possibility was considered by the Ministry of justice of the United Kingdom in 2018 (Shobhit, 2018). The Chinese court has already confirmed the
possibility of introducing blockchain into the judicial system in 2017. The first court in China to accept electronic proof based on blockchain was the Internet court in Hangzhou (Wu, Zheng, 2020). In June 2018, this court issued a decision confirming that electronic data stored using blockchain technology can be considered as electronic evidence (Zheng, 2018). Subsequently, another court decision recognized the authenticity and integrity of electronic evidence, which is no longer just stored, but also formed through the use of blockchain technology (Wu, Zheng, 2020) (approx. – author's translation).

Currently, the position of the Chinese courts is based on the recognition of the unique characteristics of evidence based on blockchain, which makes it necessary to have a special mechanism for verifying them (Wu, Zheng, 2020). Thus, the proof and its structure today face the onslaught of new entities and will inevitably undergo a transformation, primarily at the international level.

Conclusion

Networks form is a new environment that has no borders and, therefore, is not under the jurisdiction of any one state. Thus, the standards of proof and the procedure for collecting, checking, and evaluating digital evidence should be formed taking into account the rules of proof that are laid down at the international level. Justice should not ignore the emergence and spread of new information technologies, such as blockchain technology. Moreover, the organizers of the administration of justice (legislators, the Ministry of Justice, the highest judiciary, local judicial authorities) should consider the possibilities of using the useful properties of digital technologies, including in evidence. Blockchain technology, the primary use of which was aimed at the production and storage of virtual currencies, as shown in this study, is now beginning to influence the legal system and, in particular, the rules of proof. In practice, by storing, sharing, and syncing data in a network of dispersed computers, a decentralized and "trusted" blockchain can effectively solve the problem of data loss and forgery in a centralized system, thereby allowing for the more efficient performance of the electronic evidence capture functions mentioned above. At the same time, the use of blockchain will affect the economy of legal proceedings in the form of reducing the cost of storing...
and protecting information. Thus, blockchain technology can be used as a relatively inexpensive and most reliable method of confirming the reliability of electronic evidence, which confirms the research hypothesis. The possibility of continuing the presented research is seen in an attempt to develop fundamentally new approaches, using blockchain technology, to the investigation of cybercrimes.

References:


Grigorev, V.N., Sukhodolov, A.P., Ovanesyan, S.S., Spasennikova, M.G.,
Tyunkov, V.V. (2019). Tsifrovye informatsionnye platformy kak predmet normativno-pravovovogo regulirovaniya v sfere ugolovnogo sudoproizvodstva [Digital information platforms as a subject of legal regulation in the field of criminal proceedings]. Vserossiiskii kriminologicheskii zhurnal, 13(6), 873.


Zakharenko, V.V. (2018). Problema predstavleniya elektronnogo dokumenta v kachestve dokazatelstva v grazhdanskom i arbitrazhnom protsessakh [The problem of submitting an electronic document as evidence in civil and arbitration proceedings]. Vestnik nauki i obrazovaniya, 2(7(43)), 56.

Federal Law No. 149-FL. (July 27, 2006). On Information, Information Technologies and Information


herencia. JURÍDICAS CUC, 16(1), 287–302