

NOTES AND REFLECTIONS

PROBLEMS OF EVALUATION OF DIGITAL EVIDENCE BASED ON BLOCKCHAIN TECHNOLOGIES¹

OTABEK PIRMATOV

pirmatov.otabek.89@inbox.ru

Assistant Professor of the Department of Civil Procedural and Economic Procedural Law,
Tashkent State University of Law (Uzbekistan), Doctor of Philosophy in Law (PhD)

Introduction

Digital evidence is fundamentally different from physical evidence and written evidence. Securing physical evidence is primarily to prevent it from being lost or difficult to obtain in the future.

Compared to traditional evidence, electronic evidence is fragile, easy to change and delete, and difficult to guarantee its authenticity. For example, data on a personal computer may be lost due to misuse, virus attack, etc. During the preparation of the case, the video can be deleted in order to hide the facts. In fact, most electronic evidence is stored in a central database. If the database is unreliable, the validity of the data is not guaranteed. Obviously, how to ensure the authenticity and integrity of digital evidence is very important when storing it.

Because digital evidence is created by special high-tech, it is easier to change it in practice. More attention should be paid to its authenticity. Digital evidence is more likely to be tampered with in practice.

The main methods of digital evidence storage (pre-trial provision) in civil court proceedings are as follows:

- 1) sealing or closing the means of keeping the original of evidence;
- 2) printing, photographing and sound or visual recording;

¹ This text is devoted the issues of evaluation of digital evidence based on blockchain technologies in civil court proceedings. The article states that since it is not possible to change and delete evidence based on block-chain technology, contracts based on blockchain technology and documents issued by government bodies are considered acceptable evidence by the courts. It is highlighted that the usage of evidence based on block-chain technology in conducting civil court cases will prevent the need for notarization of digital evidence by the parties in the future.



- 3) drawing up reports;
- 4) authentication;
- 5) provision through a notary office;
- 6) storage through block-chain;
- 7) casting a time stamp (time stamp).

Block-chain is a database where data is securely stored. This is achieved by connecting each new record with the previous one, resulting in a chain consisting of data blocks ("block chain" in English)—hence the name. Physically, the blockchain database is distributed, allowing authorized users to independently add data. It is impossible to make changes to previously stored data, as this action will break the chain, and it is "immutability" that makes the block-chain a safe and reliable means of storing digital records in public databases².

Officially, the history of "blocks and chains" begins on October 31, 2008, when someone under the pseudonym Satoshi Nakamoto mentioned the blockchain in a white paper (base document) about the network of the first cryptocurrency - bitcoin. The fundamental principles for applying decentralization and immutability to document accounting were laid down as early as the 1960s and 1970s, but the closest to them are the works of scientists Stuart Haber and W. Scott Stornett, who in 1991 described a scheme for sequentially creating blocks in which a hash is located. The technology was even patented, but for its time it became a Da Vinci helicopter - there was no technical possibility to implement the idea, and interest in it disappeared. The patent expired in 2004, just four years before Satoshi and his white paper appeared³.

1. Literature review

S.S. Gulyamov defines block-chain as follows: blockchain (chain of blocks) is a distributed set of data, in which data storage devices are not connected to a common server. These data sets are called blocks and are stored in an ever-growing list of ordered records. Each block will have a timestamp and a reference to the previous block. The use of encryption ensures that users cannot write to the file without them, while the presence of private keys can only modify a certain part of the blockchains.

In addition, encryption ensures synchronization of all users' copies of the distributed chain of blocks (Gulyamov, 2019: 114).

Primavera De Filippi and Aaron Wright (2018) point out that block-chain technology is different from other electronic evidence because it cannot be forgotten. The technology itself has evidential value for the judicial system.

Markus Kaulartz, Jonas Gross, Constantin Lichti, Philipp Sandner define block-chain technology is getting increasingly renowned, as more and more companies develop blockchain-based prototypes, e.g., in the context of payments, digital identities, and the

² <https://www.gazeta.uz/uz/2022/08/26/blockchain-technology/>

³ <https://www.forbes.ru/mneniya/456381-cto-takoe-blokcejn-vse-cto-nuzno-znat-o-tehnologii>



supply chain. One use case of blockchain is often seen in the tamper-proof storage of information and documentation of facts. This is due to the fact that records on a blockchain are “practically resistant” to manipulation as a consequence of the underlying cryptography and the consensus mechanism.

If a block-chain is used for storing information, the question arises whether the data stored on a block-chain can be used as evidence in court. In the following article, we will analyze this question⁴.

According to Alexey Sereda, the correct usage of blockchain technologies will eliminate the need for lawyers to perform certain mechanical tasks to a significant extent: checking counterparties, contacting other experts (bodies), the need for notarization, etc. All this allows lawyers to focus their efforts on solving other more important tasks⁵.

Vivien Chan and Anna Mae Koo define blockchain is a decentralized and open distributed ledger technology. Electronic data (e.g. in a transaction on an e-shopping platform, the transaction time, purchase amount, currency and participants, etc.) will be uploaded to a network of computers in “blocks”. Since the data saved in a blockchain is stored in a network of computers in a specific form and is publicly available for anyone to view, the data is irreversible and difficult to be manipulated.

Anyone who has handled an online infringement case knows the race against time in preserving evidence. However, screenshots saved in PDF formats are easy to be tampered with and are of scant probative value before the Chinese courts, unless notarized. Making an appointment with, and appearing before a notary is another time-consuming and expensive process.

With blockchain, these procedures can be simplified and improved in the following ways: -

1. E-evidence can be saved as blockchain online instantaneously without a notary public;
2. Cost for generating blockchain evidence is lower than traditional notarization;
3. Admissibility of block-chain evidence has been confirmed by statute and many courts in China because of the tamper-free nature of block-chain technology;
4. Possible combination of online monitoring and evidence collection process: with blockchain technology and collaboration with different prominent online platforms (e.g. Weixin), it is possible to automate online monitoring of your intellectual property—blockchain evidence is saved automatically when potential infringing contents are found⁶.

According to Matej Michalko, in the previous trials of dispute cases, evidence preservation usually requires the involvement of a third-party authority such as a notary office, and relevant persons are required to fix the evidence under the witness of the notary. With the more frequent use of electronic evidence, most of the third-party electronic data preservation platforms have investigated the pattern of “block-chain + evidence

⁴ www.jonasgross.medium.com/legal-aspects-of-blockchain-technology-part-1-blockchain-as-evidence-in-court-704ab7255cf5

⁵ <https://blockchain24.pro/blokcheyn-i-yurisprudentsiya>

⁶ <https://www.lexology.com/library/detail.aspx?q=1631e87b-155a-40b4-a6aa-5260a2e4b9bb>



collection and preservation”, which is applying blockchain technology to the traditional electronic evidence preservation practice (i.e., uploading the preserved evidence to a block-chain platform). If it is necessary, you can apply online for an expert opinion from the judicial expertise center. (Michalko, 2019: 7).

Today, the task of providing electronic evidence before the court is carried out by notaries.

Data recorded on a blockchain is in essence a chronological chain of digitally signed transactions. Thus, admissibility of block-chain evidence is highly correlated to acceptance of electronic signatures in a legal setting. Not all electronic signatures provide the same level of assurance. (Murray, 2016: 517-519).

The usage of this technology when concluding transactions or receiving any official documents from the state greatly simplifies the process of proof, as it allows to track the entire history of changes made to the information stored in the blockchain. It also reliably protects them from illegal attempts to tamper or forge. Such evidence will be nearly impossible to challenge, although the risk of hacking or fraudulent activity remains.

Second, if the court session is conducted using video conferencing, the blockchain can be easily used by the participants in the court session. Given the development of remote technologies caused by the coronavirus pandemic, this situation must be taken into account. Thus, thanks to the use of blockchain, it is possible to significantly reduce the time for consideration of cases in courts, increase the transparency of court proceedings and ensure the necessary confidentiality of information.

If the contracts concluded by the parties are based on the blockchain technology or if the state authorities draw up their documents based on the blockchain technology, then it would be possible to evaluate the blockchain technology as evidence by the courts. Now in our country, government bodies are signing their documents with Q-code.

According to Boris Glushenkov, the successful implementation of the blockchain will also change the courts: firstly, there will be no need to make decisions for concrete things. Second, evidence changes: electronic evidence is viewed with skepticism in courts. Maybe blockchain can change that⁷.

In civil litigation, evidence was evaluated as evidence only if it met each of the criteria of relevance, admissibility, and reliability. Likewise, numerical evidence must meet the requirements of relevance, acceptability, and reliability of evidence evaluation criteria. Failure to evaluate digital evidence with one of the evidentiary evaluation criteria may result in its inadmissibility as evidence in court.

According to Yuhei Okakita, In civil litigation, any form of evidence can generally be submitted to the court. That is, the court accepts not only physical documents but also digital data as evidence. Of course, civil procedure laws vary from country to country, but electronic evidence is recognized in many legislations such as the EU, the United States, or Japan. Since it can be said that blockchain certificates are a kind of digital data, it should be accepted in most courts as admissible evidence.

⁷ <https://blockchain24.pro/blokcheyn-i-yurisprudentsiya>



So, you can submit the certificate to the court. However, the question is how judges evaluate the evidence. Let's to through an example relevant for e.g. the German or Japanese system: in these systems, it is up to the discretion of the judge to decide whether the certificate will be taken into consideration. If the judge believes the authenticity of the certificate, it will become the basis of the judgment.

Let's suppose that the claim of a defendant in a dispute could be validated with the data certified with a blockchain transaction. The judge decides on the authenticity of the submitted evidence based on the opinions of both parties. The defendant will explain the concept of blockchain immutability achieved with the consensus mechanism, and the other party will argue the possibility that the information on the blockchain has been tampered with. After the judge considers both stories and takes a position regarding the authenticity of the information, s/he will make a decision accordingly⁸.

According to Zihui (Katt) Gu, For the blockchain evidence to be admissible, the authenticity of the source of the electronic data must first be confirmed, whether through examination of the original or comprehensive consideration of all the evidence at hand⁹.

The admissibility of digital evidence is one of the problems of judicial evaluation of evidence in civil litigation.

In ensuring the admissibility of electronic evidence in foreign countries, transferring it to the blockchain software or evaluating the evidence in the blockchain software as admissible evidence is of great importance.

According to Van Yojun, if blockchain technology can be applied to any digital evidence, regardless of whether it is a criminal or civil trial, the general expected benefits can be achieved, including: ensuring the integrity and accuracy of data, preventing the tampering of data or evidence, increasing the transparency of legal proceedings, Court proceedings are easy to follow, accelerated and simplified¹⁰.

2. Issues of application of blockchain technology in the legislation of foreign countries

The Federal Government of the United States has not exercised its constitutional power to implement legislation regulating the admissibility of blockchain evidence in court. Thus, states enjoy residual power to implement their own legislation. The Federal Rules of Evidence establish a minimum requirement in what is referred to as the 'best evidence rule which establishes that the best evidence must be used at trial. Rule 1002 of the Federal Rules of Evidence states "An original writing, recording, or photograph is required in order to prove its content unless these rules or a federal statute provides otherwise".

Several states have regulated blockchain through introducing their own legislation and rules, particularly with regard to the regulation of cryptocurrency – or as termed by various legislators, virtual currencies. New York kickstarted legislative developments in

⁸ <https://www.bernstein.io/blog/2020/1/17/can-digital-data-stored-on-blockchain-be-a-valid-evidence-in-ip-litigation>

⁹ <http://illinoisjltip.com/timelytech/blockchain-based-evidence-preservation-opportunities-and-concerns/>

¹⁰ <https://www.ithome.com.tw/news/130752>



the USA through the regulation of virtual currency companies, and eventually several states followed suit, with 32 states implementing their own rules and regulations. The states of Illinois, Vermont, Virginia, Washington, Arizona, New York and Ohio have passed or introduced legislation which specifically regulates the admissibility of blockchain evidence in court¹¹.

In April 2018, 12 member states signed the Declaration for a European Blockchain Partnership (EBP) in order to "cooperate on the development of a European Blockchain Services Infrastructure."² With its ambitious goal of identifying initial use cases and developing functional specifications by the end of the year, the EBP should be an important catalyst for the use of blockchain technology by European government agencies¹².

In October 2018, discussions were underway among the Azerbaijani Internet Forum (AIF) for the Ministry of Justice to implement blockchain technology in several departments within its remit. Currently, the Ministry provides more than 30 electronic services and 15 information systems and registries, including "electronic notary, electronic courts, penitentiary service, information systems of non-governmental organizations", and the register of the population, among others. Part of the AIF's plans is to introduce a "mobile notary office" which would involve the notarization of electronic documents. Through this process, the registry's entries will be stored on blockchain which parties will be able to access but not change, thus preventing falsification. Future plans also include employing smart contracts in public utility services such as water, gas and electricity¹³.

Blockchain technology is a new way to build a network. Today, almost all service systems in the Internet system work on the basis of a centralized network, that is, the data warehouse is located on a central server, and users receive data by connecting to this server. The main difference of blockchain technology is that there is no need for a central server and all network participants have equal rights. The network database is kept by each user.

One of the main reasons why evidence based on blockchain technology is considered admissible by courts is that blockchain technology is transparent, that is, it is not affected by the human factor.

According to the Decision of the President of the Republic of Uzbekistan dated July 3, 2018, "On measures to develop the digital economy in the Republic of Uzbekistan":

- basic concepts in the field of "blockchain" technologies and principles of its operation;
- powers of state bodies, as well as process participants in the field of "blockchain" technologies;
- measures of responsibility for using "blockchain" technologies for illegal purposes.

The State Services Agency of the Republic of Uzbekistan has decided that starting from December 2020, the country's registry offices will operate based on blockchain technology. However, as of today, this system has not yet been launched. It would be

¹¹ <https://blog.bcas.io/blockchain-court-evidence>

¹² <https://www.eublockchainforum.eu/reports>

¹³ <https://blog.bcas.io/blockchain-court-evidence>



appropriate if the documents issued not only by registry authorities, but also by tax authorities, cadastral departments, transactions concluded by notary offices, and most importantly, decisions of district and city mayors and reports issued by electronic auction, e-active, would be accepted based on blockchain technology.

Agreements concluded by notary offices in civil courts, decisions of district and city mayors, and reports issued by electronic auction serve as the main written evidence confirming ownership rights.

Due to the widespread involvement of information technologies in all spheres of social life in our country, the above bodies are also moving to receive documents in electronic form.

Also, distribution of electricity based on blockchain technology is being carried out in Uzbekistan based on South Korean technology. Perhaps, in the future, electricity contracts in our country may be concluded on the basis of blockchain technology.

3. Discussion

With the development of the Internet and information technology, digital data has gradually become an important part of the evidence system in civil court cases, which cannot be ignored. Among all types of digital data, blockchain evidence is a relatively new type.

A proper blockchain is not a proof itself, but a technical implementation method of storing, transporting and correcting digital data.

Blockchain is just a storage technology, the purpose of which is to ensure the authenticity and reliability of digital data. The most important thing is to determine the authenticity of the digital data.

Improvements in blockchain technology can make electronic documents flow more quickly and improve the efficiency of their assessment in courts. However, compared to the traditional notarization method of securing electronic evidence, blockchain-based evidence storage lags behind. That is, there are not enough normative legal documents on the implementation of blockchain technologies in the field of justice. Notarization, which has become a means of preventing falsification of electronic documents, is rarely used in legal practice, because notarization of electronic evidence requires excessive time and money for the parties.

It includes digital signatures, reliable time stamps and hash value verification to prove the authenticity of the submitted data using blockchain technology. Parties must be able to demonstrate how blockchain technology has been used to collect and store evidence.

Due to the decentralization of information in the blockchain network, it is very difficult for hackers to exploit. Additionally, since each block contains the hash of the previous block, any transaction within the blockchain is done by changing it.

Check Hash Value: After computing any electronic file using hash algorithm, only one hash value can be obtained. If the content of the electronic file changes, the resulting hash value will also change. The uniqueness and non-repeatability of the hash value ensures the immutability of electronic files.



The verifier can use the hash value written to the blockchain to verify the original data to verify that the data is valid and has not been tampered with.

Encrypting evidence can also ensure its safe storage. At a basic level, encryption uses a secret key to ensure that only those with access can read the file by encrypting the file's contents.

It is possible to prepare documents based on blockchain technology in applications such as SharpShark, SynPat, WordProof, Waves, EUCD, DMCA.

The main reason why evidence based on blockchain technology is considered acceptable evidence in foreign countries is its technological structure. We can see the following unique features of it:

- at the discretion of one of the parties, it is not possible to change and add (falsify and destroy) documents based on blockchain technology;
- documents based on blockchain technology are a technology resistant to hacker attacks, which means that electronic evidence based on blockchain technology cannot be tampered with by third parties;
- in blockchain technology, there is no need for a central server, and all network participants have equal rights. A network database stores every user in it.

The lack of possibility of falsification and alteration of the evidence based on blockchain technology makes it considered acceptable evidence by the courts.

According to the civil procedural law, the admissibility of the evidence must be confirmed by certain means of proof according to this law.

In order to ensure the admissibility of electronic evidence, it is appropriate to create electronic documents, electronic transactions using blockchain technology, and to improve the legislation in this regard.

The following features of blockchain evidence should be considered:

1. To review the authenticity of the blockchain evidence. Specifically, it means that the court should examine whether the blockchain evidence is likely to be tampered with in the process of formation, transmission, extraction and display, and to the extent of such possibility.
2. To review the legitimacy of the blockchain evidence. Specifically, it means that the court should examine whether the collection, storage and extraction methods of blockchain evidence comply with the law, and whether they infringe on the legitimate rights and interests of others.
3. To review the relevance of blockchain evidence. Specifically, it means that the court should examine whether there is a substantial connection between the blockchain evidence and the facts to be proved¹⁴.

¹⁴ <https://www.chinajusticeobserver.com/a/when-blockchain-meets-electronic-evidence-in-china-s-internet-courts>



Conclusion

Blockchain storage solves the problem of securely storing digital data. In a sense, blockchain storage is an authentication or auxiliary storage method. Currently, blockchain storage is a more indirect authentication method.

One of the peculiarities of blockchain technology in legal science is that the use of this technology when concluding transactions or obtaining any official documents from government authorities greatly simplifies the process of proof. Due to this, the blockchain allows to track the entire history of changes made to the data stored in the "data" and reliably protects against illegal attempts to tamper with or falsify the data. Such evidence would be nearly impossible to challenge, but the risk of hacking or fraudulent activity remains, albeit partially. Second, if court hearings are held online, the possibility of blockchain use by court hearing participants will increase even more. Thus, due to the use of blockchain, it is possible to significantly reduce the time of consideration of cases in civil courts and to increase the transparency of judicial processes and ensure the necessary confidentiality of information.

Because public offering of goods and services on social networks has become popular in our country. Purchase of goods and services on social networks is carried out through mutual correspondence. Correspondence in the social network can be deleted or changed. This creates problems in evaluating social network correspondence as evidence in civil courts.

The adoption of blockchain technologies by social networks may also lead to the use of social media correspondence as evidence in courts in the future.

References

Blockchain 24, consulted online, available at <https://blockchain24.pro/blokcheyn-i-yurisprudentsiya>

Chan, Vivienne (2020). Blockchain Evidence in Internet Courts in China: The Fast Track for Evidence Collection for Online Disputes. Consulted online, available at <https://www.lexology.com/library/detail.aspx?g=1631e87b-155a-40b4-a6aa-5260a2e4b9bb>

De Filippi, Primavera and Wright, Aaron (2018). *Blockchain and the Law: The Rule of Code*. Harvard University Press.

Du, Guodong and Yu, Meng (2021). "When Blockchain Meets Electronic Evidence in China's Internet Courts", *China Justice Observer* Consulted online, available at <https://www.chinajusticeobserver.com/a/when-blockchain-meets-electronic-evidence-in-china-s-internet-courts>

European Union blockchain observatory & forum, blockchain for government and public services (Dec. 7, 2018), <https://www.eublockchainforum.eu/reports>



Fedorov, Pavel (2022). "What is blockchain: everything you need to know about the technology", Forbes, consulted online, available at <https://www.forbes.ru/mneniya/456381-cto-takoe-blokcejn-vse-cto-nuzno-znat-o-tehnologii>

Gazeta.uz (2022). *Blockchain technology is not a problem, but it is a problem that has to be solved*. Consulted online, available at <https://www.gazeta.uz/uz/2022/08/26/blockchain-technology/>

Gross, Jonas (2020). Legal aspects of blockchain technology. Consulted online, available at www.jonassgross.medium.com/legal-aspects-of-blockchain-technology-part-1-blockchain-as-evidence-in-court-704ab7255cf5

Gulyamov, S. (2019). *Blockchain technologies in the digital economy*. Textbook, p. 114.

iThome (2022). *Taiwan Takes the Lead in Judicial Blockchain Applications] An Inventory of Global Judicial Blockchain Applications*, consulted online, available at <https://www.ithome.com.tw/news/130752>

Michalko, Matej (2019). "Blockchain 'witness': a new evidence model in consumer disputes". *International journal on consumer law and practice*. V.7., p.7.

Murray, Andrew (2016). *Information Technology Law*, p. 517-519.

Okakita, Yuhei (2020). *Can digital data stored on Blockchain be valid evidence in IP litigation?*. Consulted online, available at <https://www.bernstein.io/blog/2020/1/17/can-digital-data-stored-on-blockchain-be-a-valid-evidence-in-ip-litigation>

Pollacco, Alexia (2020). *The Interaction between Blockchain Evidence and Courts – A cross-jurisdictional analysis*. Consulted online, available at <https://blog.bcas.io/blockchain-court-evidence>

The Illinois Journal of Law, Technology & Policy, consulted online, available at <http://illinoisjltp.com/timelytech/blockchain-based-evidence-preservation-opportunities-and-concerns/>

How to cite this note

Pirmatov, Otabek (2023). Problems of evaluation of digital evidence based on blockchain technologies. Notes and Reflections in *Janus.net, e-journal of international relations*. Vol. 14, N^o 1, May-October 2023. Consulted [online] on date of last visit, <https://doi.org/10.26619/1647-7251.14.1.01>

