Value and Method: the Application of Blockchain Technology in the Field of Criminal Evidence

Ying Zang(✉), Siyou Li, Yuchao Lou, and Shanshan Liu

Law School of Yunnan University, Kunming, Yunnan, China
568141279@qq.com

Abstract. In the era of data, applying blockchain technology to electronic data storage has become an important judicial practice. However, it appears more in civil and administrative scenes, and the use in criminal activities remains in its infancy. The introduction of this technology into the field of criminal evidence can help cater to the trend of networked crime, cope with the difficulties in the application of electronic evidence, supplement judicial trust with technical trust, and solve the absence of rules in judicial practice, which reflects the values of efficiency, fairness, trust and demand. Specifically, in terms of criminal rules, the storage object of blockchain should be eight types of legal evidence, while the access nodes should not be unlimited. When making regulations on blockchain evidence, it is essential to combine objectivity, legality, authenticity and "the rule of best evidence" to determine its evidentiary capacity and withstand the tests of "the rule of relevance" and "the rule of corroboration" to ascertain its probative force. Finally, some measures should be taken to prevent the corresponding technical and legal risks.

Keywords: blockchain · electronic data · authenticity · rules of evidence

1 Introduction

The iterative upgrading of information technology has brought society into the era of "everything can be data", which has invariably triggered the reshaping of social development and governance. Blockchain is a kind of distributed ledger technology maintained by multiple parties to achieve consistent data. It is difficult to be tampered with, and it can prevent repudiation. Now, blockchain debuts in the judicial practice and it is mainly applied in the field of electronic data: for example, using ordered chained structures to preserve data, using consensus algorithms to update data, using cryptography and decentralization techniques to secure data, and using hashes and timestamps to verify data.

Briefly, the judicial blockchain can be positioned as "a storage system for electronic data", and play a function in the extraction, demonstration, questioning and identification of electronic data. In 2018, the Supreme People's Court issued the "Provisions on Several Issues Concerning Case Trial in the Internet Court" for the first time to confirm

G. Ali et al. (Eds.): ISEMSS 2022, ASSEHR 687, pp. 2514–2522, 2022.
https://doi.org/10.2991/978-2-494069-31-2_296

the legal effect of blockchain evidence. Article 11 stated, If the electronic data submitted by the parties can prove its authenticity through technical means such as electronic signature, trusted time stamp, hash verification, blockchain or be authenticated by electronic storage platform, the Internet Court shall confirm it. And later, the "2019 White Paper on the Application of Judicial Blockchain" clarified that blockchain technology can be used to solve the problem of storing electronic data. In 2020, The second article of the "Opinions on Strengthening the Protection of Copyright and Copyright-Related Rights" also stated that parties are allowed to use blockchain technology to empower intellectual property business. However, all the above legal documents are only applicable to civil and administrative cases, and blockchain technology has not yet landed in the criminal judicial scene. Blockchain technology was not implemented into the field of criminal evidence until 2021, when the Supreme People's Court issued the "Rules of Online Litigation of the People's Courts". And this rule guided the authenticity identification of blockchain evidence in Articles 16 to 19.

For the application of blockchain technology in the field of criminal evidence, on the one hand, it will help solve the problem of being difficult to store and identify electronic data, and guarantee the authenticity of the evidentiary materials stored on the chain, thus avoiding wrongful convictions caused by evidence missing and tampering, and catering to the judicial needs of criminal online litigation [1]. On the other hand, someone believes that the penetration of new technologies into criminal activities will increase the complexity of identifying evidence, and it have not yet been integrated with "Rules on Collecting, Extracting and Reviewing the Electronic Data When Handling Criminal Cases" "Rules on Obtaining Electronic Evidence by Public Security Organs When Handling Criminal Cases". It also adds technical risks, such as the destruction of storage system and the leakage of electronic information. Based on this, two questions are raised: Is it necessary for blockchain technology to enter the field of criminal evidence? How to further regulate the application of blockchain technology in the field of criminal evidence? After answering these two questions, the value and method of applying blockchain technology will be emphasized, which is significant to bring the rules of evidence up to date.

2 Value: The Necessity of Blockchain Technology Entering the Field of Criminal Evidence

The combination of blockchain technology and criminal evidence mainly refers to the effective storage of electronic data on the "judicial alliance chain", which is composed of many nodes such as public security organs, procuratorates, courts, notary offices, judicial expertise centers, Internet platforms, and so on. It can better complete the extraction, storage, demonstration, questioning and identification of electronic data, and better determine facts of each criminal case. The values embodied in a series of evidentiary activities determine its necessity. Then, the related discussion is broadly divided into four progressions: efficiency, fairness, trust and demand.

2.1 Efficiency — Catering to the Trend of Networked Crime

The popularity of the Internet has triggered some networked crimes, resulting in a more important status of electronic data. Although "Criminal Procedure Law" defined electronic data as a legal type of evidence, and other relevant legal documents also regulated the whole process from extraction to identification of electronic data, "low efficiency" is still the problem of criminal proceedings. There are two reasons. Firstly, traditional crimes involving the network often have a large number of victims and they tend to be widely distributed. Relying on traditional means to collect evidences is time-consuming and labor-intensive. Secondly, the professional nature of computer crimes makes judicial official require to rely on expert opinions to identify case facts, which undoubtedly delays the litigant process. By introducing blockchain, its peer-to-peer transmission technology can realize fast synchronization of data among nodes on the chain and capture data under the chain automatically. At the same time, it is a kind of self "endorsement" with high proof power, so its trust mechanism weakens the high dependence on judicial appraisal of electronic data [2].

2.2 Fairness — Coping with the Difficulties in the Application of Electronic Evidence

For the application of electronic evidence, judicial authorities are too strict or blindly rely on it, which ultimately results in valid evidence not entering the judgment and invalid evidence being used to decide on a verdict. It goes against the value of fairness, which can be attributed to a series of evidentiary activities. In the extraction, it is difficult to extract the original, and even the original may be unilaterally modified. In the storage, storage security can not be guaranteed, because electronic media are vulnerable to attack, tampering and loss. In the demonstration, it is not all electronic data can be displayed and fixed on paper, which increases the demand for notarization, and seriously increases the burden of proof on both the prosecution and the defence. In the questioning, if the data adduced by both parties differ and the authenticity is hard to identify, the judge will allocate the consequences of failure according to the burden of proof, so the party who actively tampered with the data may benefit instead. In the identification, it is difficult to determine the nature of electronic data. Accordingly, we can use technical means to identify blockchain evidence as a original copy, use the hash-nested chain to ensure that the content stored in each block is difficult to tamper with, use intelligent contracts to promote automated demonstration, use digital signatures and timestamps to verify its integrity and authenticity [3]. Thus, blockchain technology can help eliminate the concerns of judicial authorities about the application of electronic evidence, so that it can maximize the function of fairness in criminal judicature.

2.3 Trust — Supplementing the Judicial Trust with Technical Trust

The law has always designed various trust mechanisms to maintain a stable social order. For example, in countries under the rule of law, trust has been developed between individuals and judicial authorities, letting objective prosecutors to accuse of crimes and

monitor the application of laws on behalf of victims, and letting neutral judges to adjudicate and enforce laws. It can be argued that the rule of law is a mechanism of trust, but this trust is not entirely stable. The judicial authorities, which are supposed to ascertain facts and govern crimes impartially, can be biased due to profit-seeking, and have difficulty in advancing case due to some new types of crime. In the end, public trust will be lost. At this point, the decentralized judicial blockchain is suitable for solving the above-mentioned problems. The nodes on this chain (including public security organs, procuratorates, courts, Internet platforms, individuals, etc.) can reach a consensus on the stored data without any intermediaries, which eliminates the space for power abuse. Then, based on the relevant technology of ensuring the consistency of data, its integrity and authenticity can be determined more efficiently. The neutral blockchain technology forms a kind of "technical trust", which cannot be said to be a squeeze on "judicial trust", but on the contrary, it is a supplement to "judicial trust" when the technical solution is more convenient than the legal one [4].

2.4 Demand — Pioneering Judicial Practice

Before considering whether blockchain technology can be applied in the field of criminal evidence, this proposition had entered reality for a long time. In July 2019, the first criminal case involving blockchain technology was announced, in which the defendant tricked 175 victims into transferring money to his WeChat or Alipay on the pretext of losing his wallet. There are many victims and they are geographically scattered, meanwhile the property involved is characterized by a small amount, multiple transactions and networking. So this case adopts blockchain technology to store electronic evidences, using encryption algorithms to upload the hash of original data to the "Legal Chain" of "Ant Blockchain" in order to avoid the loss or tampering during the transferred process of electronic evidence. Thus, the whole storage process is recorded, the whole chain is credible and the whole nodes witness. Finally, the judge verified that the hash of the CD issued by Alipay was consistent with that stored on the "Legal Chain". Therefore, the validity of electronic data was directly recognized, and there was no need to conduct an in-depth review or have it authenticated or notarized by professional technicians [5].

This case implies that there is a real need to introduce judicial blockchain into the field of criminal evidence. As far as the judgment is concerned, it also reflects the following three issues. Firstly, instead of the traditional way of determining the "three characteristics" of electronic evidence, the court presumes their authenticity and integrity by verifying the consistency of hashes and directly recognizes their validity. Nevertheless, there is no legitimate explanations for this. Secondly, although the data security after uploading to the "Legal Chain" is sufficient to guarantee, it is not known whether the data before uploading is true and complete. Thirdly, the verdict only states that "the hash of the CD issued by Alipay is consistent with the hash stored on the blockchain", which lacks sufficient reasons for this practice.

3 Method: Construction of Criminal Rules Concerning Blockchain Technology

As previously mentioned, the "Rules of Online Litigation of the People's Courts" issued by the Supreme People's Court in 2021 introduced blockchain technology into the field of criminal evidence for the first time, and determined the scope of validity and evaluation standards of blockchain evidence. However, relevant provisions are limited to Articles 16 to 19, which are not yet sufficient to meet the needs of the practice. In the next section, existing provisions will be introduced and ideas for further construction of criminal rules will be proposed.

3.1 Clarifying Storage Objects and Access Nodes

3.1.1 Eight Types of Legal Evidence Should Be the Storage Object of Blockchain

At present, blockchain technology is oriented to "electronic data" in a narrow sense, which only refers to the eighth category of legal evidence. Actually, any legal evidences recorded in digital form (for example, videos of witness testimony, electronic photos of physical evidence) have the risk of loss and tampering. Only in the case of the existence of the original, the value of such evidence is not high, and the risk is not as great as electronic data. However, expanding the storage object to a broad sense of "electronic data" is still necessary. If someone has a corresponding willingness to store, it should be allowed.

3.1.2 Access Nodes Should not Be Unlimited

Nodes refer to the computers connected to the blockchain, which include both institutions and individuals. The server used by an institution for data storage and operation is a node, and when an individual operates the blockchain on his computer, his computer server is also a node. Current civil judicature did not make restrictions on the scope of nodes, because any civil subject may be caught in a civil dispute, and the blockchain may help them prevent legal risks. The difference is that crimes are not universal phenomena in society. It is not all subjects will be involved in criminal proceedings, and not all of them can anticipate the occurrence of crimes. Therefore, completely opening nodes in criminal judicature not only do the individuals who are not involved in the lawsuit have no awareness of storing data, but also the access of high-risk users will pose a threat to electronic data. In conclusion, access nodes ought to be limited to specific institutions and litigant participants. As far as specific institutions, judicial institutions and internet enterprises should be accessed. The former are subjects who apply the law, carry out notarization and make judicial expertise, meanwhile, the latter are most platforms for generating electronic data. For litigant participants, the operable period should be limited to the course of litigation and the scope of data they can view should be limited to their own case. In addition, all nodes should undergo strict identity checks.

3.2 Constructing the Regulation of Blockchain Evidence

3.2.1 The Evidentiary Capacity of Blockchain Evidence

The evidentiary capacity of blockchain evidence refers to its eligibility to be accepted by the court and included in the judicial investigation. The rules of its evidentiary capacity come from three bases. Firstly, just as requirements of general evidence, blockchain evidence also needs to possess the natures of objectivity and legality. Secondly, its evidentiary capacity lies in the characteristics of blockchain evidence itself too, and its "virtuality" "digitalization" bring the need for reviewing the authenticity. Thirdly, this kind of evidence is stored on the chain, and some of them are copies or backups of the original evidence, which raises the consideration of "the rule of best evidence".

First of all, review the objectivity and legality of blockchain evidence. On the one hand, objectivity means that the electronic data can present objective case facts comprehensively and completely without intentional tampering or technical errors by human factors [6]. Therefore, the review of objectivity means to exclude the interference of tampering and errors. Based on technical trust, it can be proved as long as the blockchain platform issues explanatory materials that no such errors occurred during the storage stage. On the other hand, legality means that the subject of obtaining evidence, the form of evidence, the procedure of obtaining evidence and the way of evidence preservation and application should be legal, which are all closely related to laws. The restriction of access nodes and the clarity of storage objects are guarantees of the first two. As for the latter two, in addition to following general provisions of evidence, a formal qualification review of blockchain platforms should be attached in order to exclude illegal factors.

Secondly, review the authenticity of blockchain evidence. According to Articles 16, 17 and 18 of the "Rules of Online Litigation of the People's Courts", it needs to be discussed in two situations. For electronic evidences generated on the chain (the electronic data automatically captured on the chain by blockchain technology), the whole process of generating, storing and transmitting such evidence is completed under technical specifications. The possibility of artificial addition, deletion and tampering is very small, so "the rule of technical self-certification" is applied to presume their authenticity without the help of notarization or judicial appraisal, unless there is a sufficient evidence to the contrary [7]. For electronic evidences generated under the chain (the evidences uploaded to the blockchain platform after obtaining under the chain), it is necessary to review the specific source, generation mechanism, storage process, notarization, third-party witness and associated data before uploading to the chain. It is also necessary to judge whether it can constitute a complete evidentiary chain with other litigant evidences.

Finally, apply "the rule of best evidence". Foreign theories on the original electronic evidence include "Multiple Original Doctrine" in Common Law and "Original Carrier Doctrine" in Civil Law. The former doctrine is generally applicable to the situation where a document has duplicate or multiple copies, as exemplified by the "N copies in duplicate, each with equal effect" in a contract. The latter doctrine means that to be considered original, the electronic data must be the data originally generated or be stored in the original medium [8]. Both can be cited to explain the issue whether blockchain evidence is an original or a copy, and to design a dual system of identification. The "Multiple Original Doctrine" can be used as a theoretical basis for arguing that "the evidence generated on the chain is the original". Because all nodes in the chain update

and form copies synchronously, and the contents of these copies are identical to the original data, there is no need to determine which data is the original one. The "Original Carrier Doctrine" emphasizes the importance of the original carrier to the evidence. It can support the claim that "the evidence generated under the chain is not the original", so in criminal trials, the original of such evidences should be provided as much as possible. If blockchain evidence is offered as a substitute for the original, sufficient reasons must be provided to justify it, otherwise, it will not be admissible.

3.2.2 The Probative Force of Blockchain Evidence

The probative force of blockchain evidence refers to the degree of proof in final determination, which is to be discussed around "the rule of relevance" and "the rule of corroboration". On the one hand, the content proved by blockchain evidence must be related to the case facts. Judges can gain the factual content reflected by electronic data and judge its relevance to factum probandum based on the subsidiary information such as the time of data generating, storing and modifying, as well as the trace information such as log records and source code [9]. On the other hand, to strengthen the probative force of blockchain evidence, according to Article 19 of the "Rules of Online Litigation of the People's Courts", the parties may apply for an opinion from a person with specialized knowledge on technical issues related to blockchain. Based on the application or authority, the People's Court can commission judicial expertise centers to authenticate electronic data stored in blockchain or extract other relevant evidences for verification.

3.3 Preventing the Risks of Technology and Law

Blockchain technology changes not only the form of evidence but also the traditional rule of law system. The emergence of this new thing makes the identification of electronic data no longer depend on the fiduciary endorsement or authoritative determination from the public power. And in some cases, the verdicts were subjugated to the scientific nature and self-certification of technology [10]. However, this is not to say that a technological view is superior to a legal view in terms of the evidence, and the pros and cons of judicial blockchain are far from being analyzed in depth. In criminal judicature, there are also risks of infringing on personal information, triggering computer crimes and weakening the seriousness of litigation. Therefore, we should be cautious in applying judicial blockchain to realize the benign interaction between technology and law. Firstly, strengthen some supervisory measures of blockchain technology, and concretize the operational norms based on the "Provisions on the Administration of Blockchain Information Services". Secondly, the right of choosing blockchain technology should be guaranteed. Blockchain technology only provides an alternative to traditional ways of storing evidences, and its purpose is to circumvent drawbacks of electronic evidences, so saving evidences on the chain ought to be supported and facilitated. But if someone do not agree to the application, they shall not be forced to adopt this technology. Thirdly, the technical trust advocated by blockchain technology can never completely replace judicial trust. But they should become two types of trust mechanisms that complement each other, and develop into two parallel sets of evidentiary rules. Thus, we can use both of them optionally in different cases.

4 Conclusion

To sum up, the introduction of blockchain technology into the field of criminal evidence is in line with the development trend of law and technology. The values of efficiency, fairness, trust and demand determine the necessity of the introduction; the appropriate expansion of storage object reflects the advantages of blockchain technology; and the strict restriction on access nodes is an effective prevention of the law against technical risks. At the same time, some special regulations of the evidence relating to this technology should be attached. Firstly, it should be reviewed whether it possesses the natures of objectivity, legality and authenticity and whether it meets the requirements of "the rule of best evidence" to judge its evidentiary capacity. Secondly, "the rule of relevance" and "the rule of corroboration" should be used to determine its probative force.

Since this introduction is still in its infancy, there are no sufficient theoretical bases to support its justification and no thorough legal provisions to regulate its application. Hence, it is important to conduct relevant research from the perspectives of both value and method in this paper. Humanity has now entered a new phase that goes beyond the enforcement of law through code and instead relies on code to draft and articulate rules [11]. Blockchain technology, which preserves and stores the electronic data by executing code, has demonstrated the interaction between code and law. But the judicial application of blockchain technology does not stop there. In future research, the integration of the law and blockchain technology should be discussed in more detail. As for blockchain evidence itself, whether its probative force can be quantified and how to solve the problem of infringing on personal information are unsolved contents in this paper. In addition to blockchain evidence, the introduction of blockchain technology into the fields of making case files and executing property-oriented penalties is also promising, and the corresponding methods are yet to be explored. But in any case, blockchain technology should not overstep the law, and its application should be limited by the status of tools.

Acknowledgments. This research was supported by the 12th graduate research innovation project (general project) of Law School of Yunnan University "Practical Dilemma and Approach of electronic evidence—Discussion based on judicial blockchain".

Authors' Contributions. All authors designed the research, developed the ideas and wrote the paper. The primary author also contributed to refining the ideas, carrying out additional analyses and finalizing this paper.

References

1. Lin, X.F. (2021). The Big Data Evidence in criminal Justice: A Preliminary Investigation. *Legal Forum*, 36(3), 27.
2. Zhang, Y.J. (2019). Judicial Application, systematic Problems and Evidence Law Reform of Blockchain Technology. *Oriental Law*, (3), 103. DOI: https://doi.org/10.19404/j.cnki.dffx.20190129.002

3. Liu, P.X. (2020). On the Institutional Value of Electronic Data's Storage and Authentication Based on Blockchain. *Archives Science Bulletin*, (1), 22. DOI: https://doi.org/10.16113/j.cnki.daxtx.2020.01.004
4. Zheng, G. (2018). Blockchain and Future Law. *Oriental Law*, (3), 79. DOI: https://doi.org/10.19404/j.cnki.dffx.2018.03.008
5. Criminal Verdict of First Instance on Wang Yumin's Crime of Fraud. (2019). Retrieved 1 May 2022, from https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=5d4079e4af5746128f0eaaaf00a0a8a8
6. Ding, C.Y. (2021). Analysis on the Evidential Ability of Blockchain Electronic Data: from the Perspective of Criminal Litigation of Agricultural Insurance Fraud. *Law Science Magazine*, 42(5), 80. DOI: https://doi.org/10.16092/j.cnki.1001-618x.2021.05.008
7. Chu, F.M. (2018). Three Levels of Authenticity of Electronic Evidence -- A Case Study of Criminal Procedure. *Chinese Journal Of Law*, 40(4), 123.
8. Chen, Q.Z. (2019). Judicial Practice of Applying Blockchain to Store Electronic Data. *People's Judicature*, (4), 84. DOI: https://doi.org/10.19684/j.cnki.1002-4603.2019.04.018
9. Shi, G.B., & Chen, Q.Z. (2021). The Advantage and Judicial Review Path of Electronic Data Stored on the Blockchain. *Journal Of Southwest Minzu University(Humanities And Social Science)*, 42(1), 72.
10. Yu, C.F. (2018). The "Death" of Law: Legal Function Crisis in the Age of Artificial Intelligence. *ECUPL Journal*, 21(2), 20.
11. Kaeseberg, T. (2019). The Code-ification of Law and Its Potential Effects. *Stanford Journal Of Blockchain Law & Policy*, (2), 232-239. DOI: https://doi.org/10.9785/cri-2019-200403