Scientific Research Publishing

Chinese Studies, 2023, 12, 103-112
https://www.scirp.org/journal/chnstd
ISSN Online: 2168-541X
ISSN Print: 2168-5428

Embedded Fusion: The Certainty of Blockchain Technology Complements the High Degree of Probability of Legal Presumption

Yueyue Wu

Department of Computer Science and Technology, Institute for Internet Judiciary, Tsinghua University, Beijing, China
Email: na.jiang@bnu.edu.cn

How to cite this paper: Wu, Y. Y. (2023). Embedded Fusion: The Certainty of Blockchain Technology Complements the High Degree of Probability of Legal Presumption. *Chinese Studies*, *12*, 103-112.
https://doi.org/10.4236/chnstd.2023.122010

Received: January 28, 2023
Accepted: February 27, 2023
Published: March 2, 2023

Abstract

This paper aims to analyze the technical basis and theoretical rationality of the People's Court Online Litigation Rules of China regarding the provision that blockchain-stored data has the effect of presumption of authenticity. The presumption is a legal technique to resolve facts proving difficulties. The traditional presumption of certainty is based on naive rules of thumb, while the presumption of certainty in information technology is based on the objective foundation of technological certainty. This paper adopts the research methods of case study and law analysis, analyzes in detail the characteristics of data certainty, rule certainty, and identity certainty of blockchain technology and argues that the certainty of blockchain technology has a complementary effect on the high probability of legal presumption.

Keywords

Blockchain Technology, Legal Presumption, Certainty

1. Introduction

Dispute over copyright infringement by "Phoenix Reading": the defendant, Beijing Tianying Kyushu Network Technology Co., Ltd, used the plaintiff's photography works in the "Phoenix Reading" section of its "Phoenix.com" website without permission. The plaintiff sued for economic loss of RMB 6000 *and reasonable expenses of RMB* 1000.

Through blockchain technology, the Beijing Internet Court retrieved the copyright registration materials of the pictures involved in the case archived by the Beijing Copyright Protection Centre and conducted cross-chain verification of the blockchain. The defendant acknowledged the authenticity of the above copy-

right registration information. In the absence of evidence to the contrary, the court found that the plaintiff was the copyright owner of the works in question, and that the defendant had infringed the plaintiff's right to information network dissemination of the works in question and should bear the corresponding infringement liability. The court decided that the defendant should compensate the plaintiff for economic loss of RMB 900 and reasonable expenses of RMB 100.[1]

This is a copyright case in which the Beijing Internet Court in China relied on blockchain for evidence and authentication. The court can retrieve the copyright registration materials of the works involved in the case archived by the Beijing Copyright Protection Center with one click and conduct cross-chain verification of the blockchain, realizing real-time interaction and efficient retrieval of copyright registration information and ensuring the authenticity and credibility of copyright data.

In June 2021, the Supreme People's Court of the People's Republic of China promulgated the *People's Court Online Litigation Rules* (hereinafter referred to as the "Rules"), which contain 39 articles that stipulate the legal effects, basic principles, and applicable conditions of online litigation, and thus for the first time systematically formulate an online litigation rule system based on judicial interpretation. The "Rules" utilize the concepts, mechanisms and functions of information technology such as "user-centred" computer thinking, parallel computing, and the certainty of blockchain technology. This "embedded fusion" provides a reasonable path for breaking through the "instrument" attribute of technology and promoting the technology to meet the intrinsic value of judicial justice.

Article 16 of the "Rules" stipulates, "If the electronic data submitted by the parties as evidence is stored using blockchain technology and is consistent with technical verifications, the people's court may determine that the electronic data have not been tampered with after being uploaded to the blockchain, except when there is sufficient evidence to the contrary to reject it". The "Rules" confirm the validity of the authenticity presumption of data stored on the blockchain from the legislative level and regulate the acceptance standards for electronic data stored on the blockchain.

In recent years, the application of blockchain technology in various fields has gained the attention of researchers (Al Hamrani & Al Hamrani, 2021; Wu & Tran, 2018), but not enough attention has been paid to the technology and its application in the judicial field. This paper aims to analyze the technical basis and theoretical rationality of the "Rules" regarding the provision that blockchain-stored data has the effect of presumption of authenticity.

The rest of this article is structured as follows: part two introduces the reasons for the creation of legal presumptions, arguing that the overriding factor is the most important reason for the creation of legal presumptions. Part three ana-

[1]*Beijing Court's Top Ten Cases of Judicial Protection of Intellectual Property Rights in* 2021. (https://baijiahao.baidu.com/s?id=1731919308319298481&wfr=spider&for=pc).

lyzes that blockchain has certainty from a technical perspective. Part four argues for the principle of complementarity of blockchain technological certainty to the high degree of legal presumption of conclusiveness. This article points out that the judicial application of blockchain technology solves the inner uncertainty regarding the court's judgement on the authenticity of electronic data on the technical level, improves the efficiency of judicial litigation, reduces litigation costs and ultimately promotes judicial justice.

2. The Prerequisite for the Legality of Legal Presumptions Is That Presumed Facts Have a High Degree of Probability

Presumptions, also known as legal presumptions, refer to the rules clearly stipulated by the law based on which presumed facts are established on the basis basic facts. The essential difference between presumption and inference (also called factual presumption or indirect proof) lies in that the inference relationship between basic facts and presumed facts is clearly stipulated by the law, without the need for arguments based on empirical rules. The purpose of legal presumption is to resolve the difficulty of proof in the litigation process.

To solve the difficulty of proof, many methods have been tried in human history. In ancient Roman times, the method of setting aside judgment was adopted, and in the slavery societies of Asia and Europe, the method of judgment by God was generally practiced, in which, the difficulty of proof was solved by obtaining the will of God through a certain form. Since the 13th century, the legal evidence system has penetrated and developed in the main feudal countries of Western Europe and has negated the subjectivity of proof, has legalized torture and thus has eliminated the possibility of unclear authenticity at the system level. The inner conviction system came into being after negating the legal evidence system and has gone through a process from complete inner conviction to limited inner conviction. A series of evidence rules is the solution to the difficulty of proof under the inner conviction system.

In essence, the process of litigation is the process of resolving who should bear the adverse consequences when authenticity is unknown. The so-called state of unclear authenticity occurs when the facts to be proven are difficult to prove. The reasons for the difficulty in proving facts are multifaceted. First, information regarding the evidence may be limited. Second, almost all physical evidence must be proven by people, and human subjectivity is insurmountable; therefore, the reliability of evidence is limited. Finally, a judge's knowledge is subjective, and the process of inner conviction is a subjective process in which subjectivity must transition to objectivity, which is restricted by the knowledge of the judge.

In fact, difficulty in proving facts occurs to varying degrees in every case. Under normal circumstances, the burden of proof mechanism can be used to solve the problem of who bears the adverse consequences when authenticity is unclear. However, based on factors such as the convenience of proof, the estima-

tion of probability, and judicial policies, in certain specific cases, through the establishment of legal presumptions, the norms of allocating the burden of proof are broken to reduce the difficulty of proving for the claimant, so that the judge can make an acceptable judgement based on the facts ascertained to be as accurate as possible. Therefore, legal presumptions appear as an exception to the conventional proving process (including direct proof and indirect proof), which must be carefully considered by legislators and be predicated on the clear provisions of the law.

Legal presumption should be bounded by the reasonable connection between basic facts and presumed facts. Based on whether a judge has discretion over the establishment of presumed facts under the premise of recognized basic facts, presumption can be divided into two categories: permissive presumptions and compulsory presumptions. According to McCormick, the most important factor in creating a presumption is probability: "If all the evidence in the case is considered, there is a reasonable connection between the basic facts proved by the prosecutor and the basic facts of the presumption, and the latter is very likely derived from the former; then, in the constitution, this arbitrary presumption is acceptable" (Strong, 2004). In other words, a permissible legal presumption should be based on a certain degree of association, and this association is often reflected through probability. Taguchi Morikazu, a Japanese criminal procedural law scholar, also believes that there must be a "general and reasonably close relationship" (Taguchi, 2000) between presumed facts and premise facts. The probabilistic presumption based on empirical rules is the logical premise for the establishment of presumption. Legislators believe that the proof of basic facts is likely to lead to the existence of presumed facts. Evidently, it is difficult to find a legal presumption based on an extremely low probability event. In this sense, it can be said that probability is the main factor leading to the creation of legal presumptions.

3. Blockchain Technology Imparts Certainty

According to the definition in the *China Blockchain Technology and Application Development White Paper* 2016 issued by the Ministry of Industry and Information Technology, in a narrow sense, a blockchain is a type of chained data structure that sequentially combines data blocks in chronological order, with a distributed ledger that cannot be tampered with and is guaranteed by cryptography. Broadly speaking, blockchain technology is a novel distributed infrastructure and computing paradigm that uses blockchain data structures to verify and store data, uses distributed node consensus algorithms to generate and update data, uses cryptographical methods to ensure the security of data transmission and access, and uses smart contracts composed of automated script codes to program and manipulate data (MIIT, 2016). Blockchain technology is a deterministic information technology, and its technical certainty is manifested in three aspects: data certainty, rule certainty and identity certainty.

Data certainty with regard to blockchain technology refers to tamper-proof data stored in the blockchain, supported and realized through information technologies such as hash algorithms, chain storage structures, and distributed data management. First, hash function-based algorithms support data certainty from the algorithm principal level. All hash functions have the basic characteristic of certainty: if two hash values obtained from the same function are not identical, then the original inputs of the two hash values are also not identical. Additionally, the irreversibility of the hash function also prevents data from being tampered with. The basic principle of hash algorithms is to map an infinite set to a finite set, accompanied with information compressing loss effects. Therefore, hashing is many-to-one mapping, with countless possibilities for each hash value, making it extremely difficult to calculate inverse mapping. The "difficulty" here means that the calculation is not feasible or that it takes a very long time or a great deal of computing power that exceeds the objective and reasonable expectations for current computing resources. Second, the hash-based chained data block storage structure supports data certainty from the level of computing power possibility. Blockchains are composed of chained data blocks with a block as the unit. The block header contains the hash value of the previous block and that of the current block, and in this way, the blocks are nested in series and ultimately form a blockchain. It requires considerable computing power to tamper with the chain structure constructed based on hash values because to modify any of the transactions, the hash values of the parent blocks of all blocks after the block to be tampered with have to be changed simultaneously while ensuring that the forgery speed of the new transaction chain exceeds the generation speed of new blocks in the original blockchain. As long as there are enough nodes in the network, it is almost impossible for the calculation speeds of continuously forged blocks to exceed those of the other nodes. Another feasible way to calculate and modify blockchains is to use the characteristic that the minority obeys the majority in blockchains. The transaction history can be tampered with by having more than 50% of the computing power of the entire network, which is impossible to achieve if there are enough participating nodes in a blockchain network. However, the current judicial alliance chain "Tianping blockchain" has only 21 nodes, which is much fewer node than in other alliance chains at varying orders of magnitude.[2] Last, the accounting method, which is different from traditional distributed databases, supports data certainty from the management technology level. Compared with traditional distributed database systems, blockchains provide better distribution, transparency and credibility in accounting (Yu et al., 2019). The distributed data management of blockchains is a decentralized topology without a master-slave structure and adopts a replicated data distribution method that allows each participating node to store a shared ledger with the same data model and consistent data. All users can access the complete data,

[2] *Chinese Academy of Engineering Releases Application Case of a Judicial Alliance Chain*: (http://www.zqrb.cn/jrjg/hlwjr/2021-08-03/A1627979903638.html); accessed August 24, 2021.

thus avoiding the credibility problem caused when the traditional distributed database centre node becomes a black box.

Rule certainty with regard to blockchain technology refers to the existence of a consensus mechanism between blocks. The certainty, security and decentralization characteristics of the consensus mechanism can guarantee the certainty of the rules. First, the consensus rules are clear. The consensus mechanism of blockchains allows all nodes to agree to the block proposer election, block generation, node verification and other blockchain update processes completed through a specific algorithm to determine the validity of the record. There are multiple classifications of consensus mechanisms based on different classification standards. For example, it can be divided into two categories based on the block proposer election process: weak consensus and strong consensus; it can be divided into two categories based on whether the node needs identity authentication: permission consensus and permissionless consensus; and it can be divided into two categories based on the qualifications of the block proposer: proof of work consensus and proof of stake consensus, etc. According to different applicable scenarios, current mainstream consensus mechanisms can be divided into four categories: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT). Second, the consensus mechanism is safe. The following describes the security of a blockchain consensus mechanism: when an adversary exists and can control certain network resources and other resources, honest users can reach a final agreement in an untrusted network environment and resist certain attacks targeting the consensus mechanism. Security is the most basic and important attribute that a consensus mechanism should satisfy. For example, the PBFT-type voting-based consensus algorithm is designed to ensure that once a transaction is recorded, it cannot be tampered with and that the ledger of honest nodes remains consistent as long as the proportion of malicious nodes does not exceed one-third. Blockchain systems with the PoW algorithm as the consensus algorithm is extremely difficult and expensive to tamper with. To tamper with such a system, an attacker needs to control more than 51% of the computing power of the entire system. Finally, consensus mechanisms impart decentralization. Regarding decentralization, there is no trusted third party in the consensus mechanism adopted by a blockchain, and decisions are made jointly by all the nodes participating in the consensus rather than by a few nodes.

Identity certainty with regard to blockchain technology refers to the certainty of the digital signature of a blockchain. A digital signature is some data attached to a node or a cryptographic exchange made to the node. These data or transformations allow the recipient of the node to confirm the source and integrity of the data unit and ensure that the data are protected from being forged and tampered with. Digital signatures allow the implementation of permission control, the identification of the legal identity of a transaction initiator, and the prevention of identity theft by malicious nodes. Digital signatures usually use asym-

metric encryption algorithms, through which the sender uses a private key to encrypt the hashed digest and sends it together with the original data; the verifier uses the sender's public key to decrypt the digest and compares the original digest value with the original data through the same hash operation. If the two are identical, then the signature verification is confirmed. The security of a digital signature is based on the difficulty calculating the decryption key (private key) with a known encryption key (public key). Take the classic RSA public key encryption algorithm as an example; even with the best factorization method, it will take several years or longer to determine the original prime number. "Today, no one has been able to find an effective method to decrypt messages encrypted based on the RSA encryption algorithm without knowing the decryption key" (Brookshear, 2011).

4. Certainty of Blockchain Technology Complements the High Degree of Probability of Legal Presumptions

"Due to unclear validity and review rules, there are various chaotic incidents in the blockchain evidence field, such as exaggerating the validity of blockchain evidence, misleading the parties to record evidence, intentionally confusing the boundary between the application of blockchain technology in the court and blockchain evidence, and using court endorsements, etc."[3]Article 16 of the "Rules" confirms the validity of the authenticity presumption of data stored on the blockchain at the legislative level and regulates the acceptance standards for electronic data stored on the blockchain.

First, the authenticity presumption stipulated in Article 16 of the "Rules" is permissible presumption. Second, the basic fact of presumption is that the data stored on the blockchain has been technically verified to be consistent, and the presumed fact is that the electronic data have not been tampered with after being uploaded to the blockchain. Third, the effect of the presumption is the conversion of the evidence from content proof to formal proof, thereby reducing the burden of proof. Finally, the legislative basis for presumption is that the data stored in the blockchain has a high degree of probability of authenticity and that this probability does not stem from subjective rules of thumb but from the objective certainty of blockchain technology.

The creation of traditional probabilistic presumption is based on simple rules of thumb, i.e., a legislator, based on subjective experience, believes that the existence of basic facts is likely to lead to the existence of presumed facts. However, the probabilistic presumption of information technology is based on the objective foundation of technological certainty. As mentioned above, the certainty of blockchain technology is realized through data certainty, rule certainty and identity certainty. Technological certainty is the product of the development of information technology to a certain stage, and with the further maturity of tech-

[3] *Understanding and Application of "People's Court Online Litigation Rules"* (http://www.court.gov.cn/zixun-xiangqing-309561.html); accessed August 10, 2021.

nology, information technology may promote the transformation of the presumption mechanism of litigation from the rule of experience to the law of causation and from probabilistic presumption to deterministic presumption; the digitalization trust created by information technology may have a profound impact on the promotion of digital justice.

In the "Phoenix Reading" case mentioned at the beginning of the article, the judge presumed the authenticity of the copyright registration materials after blockchain verification, based on the certainty of blockchain technology, which reduced the plaintiff's burden of proving the authenticity of the content of the evidence and presumed the authenticity of the evidence materials with a high degree of probability of authenticity.

5. Conclusion

The "Rules" manifest the embedded fusion of information technology and litigation procedures and provide a standardized basis for the functional positioning of information technology transcending instrumentalism at the level of judicial interpretation as well as a path to achieve a breakthrough in improving judicial efficiency and judicial justice through information technology. Additionally, in the process of the embedded integration of information technology and the judicial system, we should pay special attention to the following issues.

First, the certainty of information technology is relative. Some scholars have questioned the certainty of blockchain technology. Some representative viewpoints are that "the unmodifiability and credibility of transaction records in the simple sense of blockchain technology is obviously not enough to support certainty" (Yang, 2021) and that although a "blockchain is not easy to tamper, blockchains are not tamper-proof" (Shi et al., 2019). Certainly, in theory, blockchain technology cannot be tampered with, but it can only be considered impossible in the context of relatively fixed technological development. However, with the development of information technology, the scope and degree of calculation difficulties may change. The calculations that currently take hundreds of years or a nation's computing power to complete may be more feasible in the future. Therefore, the certainty discussed here must be understood from a developable and dynamic perspective.

Second, the category of embedded fusion is relative. According to the "Rules", the validity of the presumed authenticity of data stored on blockchains is limited to the authenticity proof of the form of data on blockchains. The degree and scope of the embedded integration of information technology and litigation procedures are developing and changing. With the in-depth study of litigation theories, such as the principle of direct verbal adjudication, the purpose of criminal litigation, and presumed probability, as well as the innovative development of computing theories and application technologies, such as the parallel computing structure of digital technology, encryption algorithms and virtual reality, the scope of, degree of and methods for the embedded integration of information

technology and litigation will be further enriched and deepened.

Third, the role of embedded fusion is relative. This paper aims to provide a new way of thinking that can break through instrumentalism when exploring ways to assist in improving judicial efficiency and judicial fairness by analysing the embedded fusion of information technology and litigation procedures manifested in the "Rules" at the functional level; however, this assistance role in embedded fusion is relative. For example, regarding the role of blockchain technology in proof, some argue that although blockchain technology "has extremely high reliability that is different from other computer technologies, there is still a gap in terms of the 'accuracy' required for judicial proof". [4] As mentioned above, the role of certainty of blockchain technology in judicial proof is to complement the high degree of presumed facts, which is equivalent to reaching an "accurate and correct" standard of proof and inner conviction standard suitable for a judge to make a judgement. The proof standard of China's civil procedure law has a high degree of probability. The proof standard of criminal procedures is that the evidence is reliable and sufficient. We have not found a source of the legal requirements for "accurate and correct" as a standard of proof. Information technology can assist judges by providing bases for judgement on factual issues; however, whether the evidence standards are reached is a legal issue and should be at the discretion of the judge. Information technology cannot and should not be a substitute for a judge to make a judgement.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

Al Hamrani, N. R., & Al Hamrani, A. R. (2021). People of Determination (Disabilities) Recruitment Model Based on Blockchain and Smart Contract Technology. *Technology and Investment, 12,* 136-150. https://doi.org/10.4236/ti.2021.123008

Beijing Court's Top Ten Cases of Judicial Protection of Intellectual Property Rights in 2021. https://baijiahao.baidu.com/s?id=1731919308319298481&wfr=spider&for=pc

Brookshear, J. G. (2011). *Computer Science: An Overview* (11th ed., p. 388). Translated by Liu Yi et al., Posts and Telecommunications Press.

Chinese Academy of Engineering Releases Application Case of a Judicial Alliance Chain. http://www.zqrb.cn/jrjg/hlwjr/2021-08-03/A1627979903638.html

MIIT (2016). *China Blockchain Technology and Application Development White Paper.* http://www.caict.ac.cn/english/research/whitepapers/202101/P020210127494158921362.pdf

Shi, P. P., et al. (2019). The Evidence Value of Blockchain Technology (p. 3). *Procuratorate Daily*, April 17.

Strong, J. W. (2004). *McCormick on Evidence* (5th ed. p. 682). Translated by Tang Wei-

[4]Shi et al. (2019). *The Evidence Value of Blockchain Technology,* Procuratorate Daily, April 17, (p.3).

jian et al., China University of Political Science and Law Press.

Taguchi, M. (2000). *Criminal Procedure Law* (p. 29). Translated by Liu Di et al., Law Press.

Understanding and Application of "People's Court Online Litigation Rules". http://www.court.gov.cn/zixun-xiangqing-309561.html

Wu, J., & Tran, N. K. (2018). Application of Blockchain Technology in Sustainable Energy Systems: An Overview. *Sustainability, 10,* Article 3067. https://doi.org/10.3390/su10093067

Yang, J. W. (2021). Blockchain Evidence Rule System. *Journal of Soochow University (Philosophy and Social Sciences Edition), 3,* 91.

Yu, G. et al. (2019). The Challenge and Prospect of Distributed Data Management Techniques in Blockchain Systems. *Chinese Journal of Computers, 44,* 28-53.