Blockchain As a New Vehicle of Electronic Evidence in China

Yong Zhang *
Faculty of Law, University of Macau
ORCID 0009-0002-0748-5779

Qianyi Yan **
Faculty of Law, University of Macau
ORCID 0009-0008-3740-2106

DOI: 10.54103/milanoup.215.c449

Abstract

The rapid development of blockchain technology has prompted its application to e-commerce anti-counterfeiting, personal identity authentication, transparency of transaction information, and other aspects. Meanwhile, social communication has gradually tended to be dominated by electronic data. Against this background, electronic evidence storage on blockchain came into being. This paper, firstly, through a literature review, will address the extension of the concept of digital evidence in the new era of blockchain, relevant legal provisions of China on the legal effect of electronic evidence stored in the blockchain, as well as the significance of the application of blockchain in generating digital evidence in the Chinese legal system. Secondly, through case analysis, it will analyze the first case decided in China based on digital evidence preserved by blockchain technology. Including the storage, collection, and verification procedures of electronic evidence in the blockchain, as well as technical and legal issues of applying electronic evidence stored in the blockchain. Such as the technical risk of the password being cracked, the legal problem that the authenticity of the evidence is difficult to determine, and so on. Thirdly, through a comparative law perspective, it will analyze how the USA treats electronic evidence stored in the blockchain, the ways that they solve the above problems, and whether it can achieve cross-border blockchain electronic evidence

* Yong Zhang, Ph.D. Candidate, University Teaching Assistant, Faculty of Law, University of Macau, Macau Special Administrative Region, China. Research fields: Technology Law, Digital Law.

** Qianyi Yan, Lecturer, Xianda College of Economics and Humanities, Shanghai International Studies University, Shanghai, China. Research fields: Artificial Intelligence, Blockchain.

assistance. Fourthly, it will be discussed the possibility that in the coming future, while increasing the credibility of the digital evidence generation system and strengthening the evidence preservation process, the generality of judicial entities could recognize the legal status of digital evidence preserved by blockchain technology.

Keywords

Electronic Evidence; Arbitration Chain; Blockchain Evidence; The USA; Authenticity of Blockchain Evidence

1. Introduction

With the rapid popularization of the Internet, the volume of online transactions is increasing day by day. Among them, online transactions in banking, securities, insurance, e-commerce, and other fields are very significant. For example, in 2017, the scale of e-commerce transactions in China was 28.66 trillion yuan, up 24.77% year on year. Among them, the B2B turnover was 20.5 trillion yuan, the online retail turnover was 7.17 trillion yuan, and the domestic service e-commerce turnover was 998.6 billion yuan.[1] Online transactions have become an increasingly important part of people's lives, and even overtaken cash transactions and physical store transactions. Electronic bills are inevitable during the process. The transaction volume of online transfers is huge, and real-time statistics of platform transaction volume have become a problem that financial institutions need to solve at present. Many financial institutions currently conduct online statistics to ensure the authenticity of their data as much as possible. Considering the characteristics of electronic data such as virtuality and falsifiability, once online disputes occur, it becomes a problem whether these data can be recognized by judicial institutions.[2]

On the other hand, because electronic evidence involves strong professional skills and most judicial personnel lack high-tech knowledge, they are limited by professional knowledge in the process of adopting electronic evidence. At present, although there are relevant laws and regulations on the identification of electronic evidence, there has not yet been any organization that is engaged in such business for society, which will bring about difficulties in the identification of electronic evidence in litigation. Given the system dependence and high technology of electronic evidence, the collection process of electronic evidence is highly demanding for technology. It is difficult even for those who

1 E-commerce Research Center, '2017 China E-commerce Market Data Monitoring Report' (*China Economic Net*, 1 June 2018) <www.100ec.cn/zt/17market_data_report/> accessed 15 April 2023.

2 Ethel, 'Blockchain Joins Arbitration Industry First Arbitration Chain Appears in Shenzhen' (*Chaintiao*, 1 May 2020).

have been engaged in judicial work for a long time to extract electronic evidence professionally.[3]

2. Literature review

2.1 Characteristics, legal provisions, and evidence collection methods of e-evidence

Electronic evidence has appeared and has been applied in judicial practice in China for more than 20 years. Its legal status was formally established in the Criminal Procedure Law [4]and Civil Procedure Law[5], which came into effect in 2013. The prototype of electronic evidence has been reflected in the Contract Law 1999[6] and the Electronic Signature Law 2004[7]. E-mail, electronic data exchange, online chat records, online blogs, mobile phone SMS, electronic signatures, domain names, etc. were defined as the form of electronic evidence for the first time in the Provisions on Several Issues Concerning Examination and Judgment of Evidence in Death Penalty Cases jointly issued by the Supreme People's Court, the Supreme People's Procuratorate and other departments in 2010.[8] In the field of civil procedure law, electronic data has officially appeared as an independent type of evidence in the Civil Procedure Law revised in 2012.[9] The judicial interpretation of the Civil Procedure Law issued in 2015 defines in detail electronic data as the type of civil evidence and clearly distinguishes between electronic data and audio-visual materials. It also clearly points out that electronic data refers to information formed or stored in electronic media through e-mail, electronic data exchange, online chat records, blogs, microblogs, mobile phone SMS, electronic signatures, domain names, etc.[10]

Regarding the characteristics of electronic evidence, Du Chunpeng put forward the intangibility and vulnerability of electronic evidence.[11] Electronic evidence is intangible in that it exists in the media in the form of sound, light, electricity, magnetism, etc, and is an electromagnetic wave and binary data coding in

3 Liu Huijie, 'Collection Measures, Methods and Precautions of Electronic Evidence' (*Baidu Wenku*, 2 November 2012) <https://wenku.baidu.com/view/6e63e1156edb6f1aff001f5d.html?re=view> accessed 15 April 2023.

4 Criminal Procedure Law of the People's Republic of China 2013, art 48.

5 Civil Procedure Law of the People's Republic of China 2013.

6 Contract Law of the People's Republic of China 1999, art 11.

7 Electronic Signature Law of the People's Republic of China 2004, art 2.

8 Provisions on Several Issues Concerning Examination and Judgment of Evidence in Death Penalty Cases 2019, art 29.

9 Civil Procedure Law of the People's Republic of China 2013, art 63.

10 Judicial Interpretation of the Civil Procedure Law 2015, art 116.

11 Chunpeng Du, *Collection and Identification of Electronic Evidence* (China University of Political Science and Law Press 2014).

nature, so it is difficult to collect. Because of its intangibility, its security and authenticity are easily damaged by the outside world, and even sometimes the facts it reflects are not the essential truth, but only the apparent truth. Examples are filmed images of disguised persons or objects, audio recordings imitated, link titles inconsistent with link web addresses and contents, virtual screen names inconsistent with real identities, web pages tampered with by 'hackers', forged e-mails, etc. If these evidences are not corroborated by third-party evidence, there is a high possibility that they will be misjudged. Regarding the vulnerability of electronic evidence, whether in digital or analog form, it is extremely vulnerable to external damages, such as monitoring, eavesdropping, interception, tampering, and deletion during its storage, transmission, and use, because it is stored on erasable data recording media, such as magnetic tape, magnetic disk, erasable optical disk, and is easily damaged due to misoperation in use. In addition, Zhou Lingling also proposed the technical and composite characteristics of electronic evidence.[12] The technical characteristic of electronic evidence refers to that electronic evidence depends on certain technical equipment and means. In addition, the electronic evidence integrates text, images, pictures, sounds, pictures, and other forms and, therefore, has a significant composite characteristic in the form of expression. DU Wei and others also put forward the massiveness of electronic evidence.[13] With the continuous increase of network bandwidth, the data generated in computer systems and networks every day are complex and massive. How to identify the electronic evidence related to the case and reflecting the objective facts of the case from the massive data is also a difficult task.

Regarding the collection of electronic evidence, the relevant party, mainly through the real-time monitoring and analysis of network data flow, audit trail, host system log, etc, detects the intrusion behavior to the network system and identifies, saves, and legally submits the digital evidence.[14] Therefore, the sources of electronic forensics mainly include system logs, intrusion detection systems, firewalls, FTP, anti-virus software logs, e-mail, and card connecting equipment (including all kinds of modems, network cards, routers, and hubs). At present, electronic forensics technology shows the trend of integration, intelligence, and automation. The main technologies include IP address acquisition technology, IDS (Intrusion Detection System) forensics technology, massive data forensics technology based on data mining, automatic forensics technology in a collaborative environment, data recovery technology, data analysis technology, and data

12 Lingling Zhou, 'Overview of Electronic Evidence and Its Collection and Identification' (*China Court*, 7 December 2012).

13 Wei Du, Jianxin Peng and Li Mao, 'Overview of Internet Electronic Evidence Collection Technology' (2011) 2 Forensic Science and Technology 54.

14 'How to Lock Black Hands in Electronic Forensics in Big Data Era' (*Legal Daily*, 22 September 2017) <http://www.xinhuanet.com/> accessed 15 April 2023.

preservation technology.[15] With the development of the Internet and computer technology, electronic data collection, examination, and judgment have become basic and common work in criminal justice activities. However, the current electronic forensics technology still has great limitations and is difficult to meet the objective requirements of society and judicial practice for electronic forensics. For example, the market demand space for public cloud computing driven by big data and artificial intelligence makes data increasingly migrate from terminal devices to the cloud. At the same time, many cyber-related crimes also migrate to the cloud. Electronic forensics in the cloud environment has gradually increased. For example, how to collect cloud platform data, how to analyze the data, and how to locate data in the collection. For another example, IP on the cloud is not necessarily real IP and involves jurisdiction issues. In addition, since cloud storage data will be released at any time after use, how to fix it also poses a problem.

2.2 Blockchain characteristics and relevant laws and regulations

The government departments paid attention to the blockchain when it emerged in China. In 2013, the government departments noticed the risks of blockchain tokens and carried out relevant rectification work. In October 2016, under the guidance of the Ministry of Industry and Information Technology (MIIT), the China Blockchain Technology and Industrial Development Forum released the White Paper on China Blockchain Technology and Application Development which is the first technical document of blockchain under the guidance of the government.[16], Since then, the MIIT has actively promoted the development of core technologies and standards of blockchain, marking that blockchain technology as a whole has entered the government's vision of governance. At present, a legal and regulatory system has been initially formed to regulate the blockchain, including laws, administrative regulations, departmental rules, other normative documents, and relevant policy documents. Specifically, there mainly are the Cybersecurity Law[17], Criminal Law[18], Decision of the Standing Committee of the National People's Congress on Safeguarding Internet Security (Amendment 2019)[19], Decision of the Standing Committee of the National People's Congress on Strengthening the Protection

15 Wei Du, Jianxin Peng and Li Mao (n 13) 58.

16 'White Paper on Application of Blockchain Technology' (*Institute of Internet Industry*, 19 December 2018) <https://wxappres.feeyan.com/block/report240/240.pdf> accessed 15 April 2023.

17 Cybersecurity Law of the People's Republic of China 2016, art 22.

18 Criminal Law of the People's Republic of China 2023, arts 253, 286 and 287.

19 Decision of the Standing Committee of the National People's Congress on Safeguarding Internet Security 2019, art 7.

of Internet Information[20], Regulations of the People's Republic of China on the Security Protection of Computer Information Systems[21], Measures for the Administration of Internet Information Services[22], Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts[23], and Provisions on the Administration of Blockchain Information Services[24]. Generally speaking, the legal, regulatory, and policy system of blockchain in China can be divided into two parts: one is to encourage technological exploration and standardize technological application; and the other is to strengthen the information security management of the blockchain network.

Regarding the characteristics of the blockchain, Wang Yuandi and others proposed that the blockchain has the main advantages of decentralization, detrust, traceability, collective maintenance, security and non-comparability, openness, anonymity, etc.[25] Wang Faming and others proposed that decentralization is the core advantage of blockchain. Decentralization refers to the decentralized distributed structure.[26] The whole network has neither centralized hardware or organization nor a centralized core system, which saves a lot of intermediary costs in reality. This is also one of the most important reasons for the wide application of blockchain. Specifically, the blockchain is a distributed database ledger, and transaction information data are stored in public ledgers on various nodes. Distributed ledgers are jointly maintained and synchronized in real-time (via network broadcasting) by multiple nodes, while account dealing rules based on complex cryptographic algorithms (Hash algorithm, etc) must be followed at the same time. The rights and obligations of all nodes in the system are the same, and the failure at any node will not affect the integrity of the system. It has the characteristics of distributed accounting, distributed propagation, and distributed storage. Regarding the non-comparability of blockchain information, Jesse and others mentioned that each node in the system has a complete database.[27] One has to control 51% of the nodes at the same time to falsify transaction data in the network, otherwise, the data tampering of individual nodes will not affect the data of other nodes, and the integrity and correctness

20 Decision of the Standing Committee of the National People's Congress on Strengthening the Protection of Internet Information 2012, art 2.

21 Regulations of the People's Republic of China on the Security Protection of Computer Information Systems 2011, art 5.

22 Measures for the Administration of Internet Information Services 2021, art 1.

23 Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts 2018, art 11.

24 Provisions on the Administration of Blockchain Information Services 2019, art 1.

25 Yuandi Wang, Li Li and Die Hu, 'Review of Blockchain Studies' (2018) 3 Journal of China University of Mining & Technology 75.

26 Faming Wang and Meijuan Zhu, 'Bibliometric Analysis of Domestic Hot Spots in Blockchain Research' (2017) 12 Journal of Intelligence 70.

27 Yli-Huumo and others, 'Where is current research on blockchain technology? A systematic review' (2016) 11(10) PLoS ONE e0163477.

of the entire ledger in the system will not be affected. Lin Xiaochi and others pointed out that traceability means that timestamp technology is adopted on the blockchain to add time dimension to the data and record the order of transactions, making the data traceable and easy to supervise and track.[28] Zhang Rui pointed out that the essence of de-trust is that the system converts the previous 'trust in humans' into 'trust in machines', that is, the blockchain grants credit with technical rules.[29] The trust granted does not come from the endorsement of a third party but the recognition of a consensus mechanism by all participants. In this way, the blockchain changes the previous contract and trust mechanism and realizes the exchange of trustworthy values, which will greatly reduce the dishonest behavior in the contract. Ma Ang and others put forward that collective maintainability means that the data in the system are collectively maintained by all participating nodes with maintenance functions, and anyone can participate. At the same time, the fault of any node will not affect the operation of the whole system, thus ensuring the stable operation of the whole system.[30]

2.3 Legal effect of blockchain data as e-evidence

Legislation recognizes the validity of blockchain data as electronic evidence. Evidence validity of electronic data has experienced a period of development in China from scratch, from conceptualization to specific operating procedures for implementation. In 2002, the Supreme People's Court issued the Provisions of the Supreme People's Court on Several Issues Concerning Evidence in Administrative Proceedings, of which art 64 stipulates that electronic evidence shall have the same evidential effect as the original, but has not yet been defined as a statutory type of evidence.[31] For example, previously in the process of hearing securities administrative cases, electronic data evidence such as electronic transaction information, network IP address, communication records, and e-mail were of vital importance in securities administrative cases due to the electronic, network-based, and wireless characteristics of securities transaction and information transmission. In 2011, the Supreme People's Court promulgated the Summary of the Symposium on Several Issues Concerning Evidence in Hearing Securities Administrative Punishment Cases. The summary specifically stated that "due to the characteristics of electronic data evidence such as

28 Xiaochi Lin and Qianwen Hu, 'Review of Research on Blockchain Technology' (2016) 2 Financial Market Research 100.

29 Rui Zhang, 'Traditional Financial Reform and Innovation Based on Blockchain' (2016) 10 Southwest Finance 15.

30 Ang Ma, Xiao Pan and Lei Wu, 'Summary of Research on Blockchain Technology Foundation and Application' (2017) 11 Journal of Information Security Research 970.

31 Provisions of the Supreme People's Court on Several Issues Concerning Evidence in Administrative Proceedings 2002, art 64.

diverse carriers, simple duplication, easy correction, deletion, and forgery, the requirements on the form of evidence and the verification of electronic data evidence should be stricter than other evidence methods."[32] Electronic data can only be submitted as evidence if it meets certain requirements. However, the Administrative Procedure Law of the People's Republic of China was amended in 2014 to include the category of electronic data in the provisions of art 33 on types of evidence.[33] It is recognized from the legal level that electronic data can be used as the basis for determining the facts of a case if verified by the court. Subsequently, art 8 of the Electronic Signature Law revised in 2015 also stipulates the factors that should be considered for the authenticity of electronic data as evidence.[34] As a decentralized electronic data retention technology, blockchain has the characteristics of openness, distribution, and irreversibility. The data retained through blockchain technology are still electronic and fall within legal data types and, therefore, can be submitted and used as evidence materials in the administrative trial process.

The judicial interpretation clarifies the validity of blockchain data as electronic evidence. On the technical level, the distributed IT architecture of the blockchain has the characteristics of decentralization, transparency and openness, consistent state, and high dependence on cryptography. At the data level, the blockchain can keep the data consistent based on multi-party consensus, prevent data from being tampered with, and trace the whole process of data-based applications.[35] Based on this technical feature, blockchain technology is highly suitable for the preservation and authenticity examination of electronic evidence. At present, the examination and judgment of the authenticity of electronic data mainly rely on notarization procedures, which are formal examinations, complicated and cumbersome procedures, with weak probative force. The characteristics of Internet court cases, ie, online trials and a large amount of online evidence, objectively require breaking through the single way

32 Summary of the Symposium on Several Issues Concerning Evidence in Hearing Securities Administrative Punishment Cases 2011, s 2(1).

33 Art 33 of the Administrative Litigation Law of the People's Republic of China 2017, "Evidence includes: (1) documentary evidence; (2) physical evidence;(3) audio and video recordings; (4) electronic data; (5) witness testimony; (6) statement of a party; (7) opinion of a forensic identification or evaluation expert; (8) survey transcripts and on-site disposition transcripts."

34 Art 8 of Electronic Signature Law of the People's Republic of China 2019, "The following factors shall be taken into consideration when making examination on the truthfulness of any data message as evidence: 1. The reliability of the methods for creation, storage or transmission of data message; 2. The reliability of the methods for keeping the integrality of the contents; 3. The reliability of the methods for identifying the addresser; 4. Other relevant factors."

35 'Research Report on China's Blockchain Technology and Application Development' (*Chain Tower Think Tank*, December 2018) <http://pdf.dfcfw.com/pdf/H3_AP201804021115378434_1.pdf> accessed 15 April 2023.

of determining the authenticity through notarization procedures but making the substantive determination of the authenticity of electronic data through technical means and relevant supporting mechanisms.[36] In September 2018, the Supreme People's Court promulgated the Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts, which put forward clear standards for the authenticity review of electronic data and further explicitly recognized that blockchain can be used as technical methods for electronic data collection.[37]

The recognition of blockchain data as effective evidence in trial practice. In judicial trial practice, before the promulgation of the Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts, Internet courts have begun to recognize the authenticity and reliability of blockchain technology in preserving electronic evidence. In June 2018, the Hangzhou Internet Court heard the case filed by *HuataiYimei Cultural Media Co., Ltd. (hereinafter referred to as HuataiYimei) v Shenzhen Daotong Science and Technology Development Co., Ltd. (hereinafter referred to as Daotong Technology)*[38] for the latter's violation of the former's right of online works information communication, which was the first time that a Chinese court confirmed the legal effect of electronic evidence storage by blockchain technology. In this case, the plaintiff HuataiYimei took screenshots of the web page where Daotong Technology published the infringing art, obtained the source code of the web page, packed and compressed the operation log, call time record, and other contents, calculated the hash value and uploaded it to FACTOM blockchain and Bitcoin blockchain for electronic data storage. According to the account number and password submitted by HuataiYimei, the Hangzhou Internet Court downloaded the preserved file package from www.baoquan.com. The web page contained therein showed that ladyfirst.com.cn had published the alleged infringing art. Upon examination, the body part was the same as the art involved in the case. The source code operation of the web page shows that the source code is www.ladyfirst.com.cn. Upon inquiry, the filing body of the website is Daotong Company. Through calculating the hash value of the preserved file package, and inquiring according to the inquiry methods and steps of the FACTOM blockchain and Bitcoin blockchain provided by Chain Forensic Science, it can be seen that the hash value exists in the blockchain, and the uploading time and the file package forming time are reasonable. According to the blockchain

36 Hu Shihao, He Fan and Li Chengqi. 'Understanding and Application of Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts' (2018) 28 People's Judicature ·Application, 24.

37 Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts 2018, art 11.

38 *HuataiYimei Cultural Media Co., Ltd. v Shenzhen Daotong Science and Technology Development Co., Ltd.* [2018] Hangzhou Court of the Internet Z 0192 Ming Chu No.81.

mechanism, it is known that the involved electronic evidence has been uploaded to the blockchain for preservation and has not been modified.[39] The judge of Hangzhou Internet Court held that the legal effect of this electronic evidence storage method should be comprehensively recognized based on the principles of technical neutrality, technical explanation, and case review in practical trials. Neither should the identification standard be excluded or improved because the blockchain and other technologies are new and complicated technical means at present, nor should the identification standard be lowered because of the technology's tamper and deletion-proofing features, but its evidence effect should be comprehensively judged according to the relevant legal provisions on electronic data. Because of the blockchain's tamper and deletion-proofing features, it is reliable as a method of maintaining content integrity after confirming that the contested electronic data has been saved in the blockchain. In October 2018, in the case filed by *COL Digital Publishing Group Co., Ltd. v Beijing Jingdong 360 Degree Electric Commerce Co., Ltd.* [40]for the latter's infringement upon the former's online works information communication, Beijing Dongcheng District Court held as follows in terms of the integrity and method reliability of electronic data preserved in the blockchain: after evidence collection through a third-party storage platform, the platform automatically generated a unique corresponding and encrypted digital fingerprint (hash value), and then generated a data preservation certificate containing hash value, blockchain security ID, time of evidence collection and other information, thus ensuring the integrity of electronic data. On 24 January 2019, in a case filed to the *Beijing Internet Court over right of online works information communication among Beijing Microlive Vision Technology Co., Ltd. vs Baidu Online Network Technology (Beijing) Co., Ltd. and Beijing Baidu Netcom Science and Technology Co., Ltd.*,[41] the plaintiff provided its evidences, including ICP filing information inquiry, screenshots of the homepage of Tik Tok website, screenshots of the developer information of Tik Tok APP (Android system and iOS system), authorization letter issued by XIE, (2018) Jing Dong Fang Nei Min Zheng Zi No 10028 Notarial Deed, (2018) Yue Guang Nan Yue No 8614 Notarial Deed, the screenshots of developers' information of HuoPai APP (Android system and iOS system) and the corresponding blockchain certificate of evidence, the screenshots of web page showing 'the total participation of the national party media platform in interactive activity of commemorating

39 Yichun Lu, 'Determination of Legal Effect of Blockchain Electronic Evidence' (*IPLEAD*, 2 December 2018) <https://www.zhichanli.com/> accessed 15 April 2023.

40 *COL Digital Publishing Group Co., Ltd. v Beijing Jingdong 360 Degree Electric Commerce Co., Ltd.* [2018] Dongcheng District Court J 73 Ming Zhong No.2163.

41 *Beijing Microlive Vision Technology Co., Ltd. vs Baidu Online Network Technology (Beijing) Co., Ltd. and Beijing Baidu Netcom Science and Technology Co., Ltd.* [2018] Beijing Internet Court J 0491 Ming Chu N0.1.

the "5.12" exceeds 600 million' and blockchain certificate of evidence, and the evidences were accepted by the courts.

The construction of the judicial blockchain of Internet court promotes the credibility of the whole process of electronic evidence. In addition to adopting blockchain data as electronic evidence in specific cases, Hangzhou Internet Court and Beijing Internet Court have respectively promoted the construction of judicial blockchain for the preservation of electronic evidence in copyright protection, contracts, financial disputes, and other fields, and promoted the production, storage, dissemination, and use of electronic data to realize credibility of the whole process.[42] The judicial blockchain constructed by Hangzhou Internet Court consists of three layers: first is blockchain procedure, through which users can directly record the entire process of operation in the blockchain, such as online submission of electronic evidence such as electronic contracts, rights protection process, and service process details; second is the full link capability layer of the blockchain, which mainly provides credibility service of real name authentication, electronic signature, timestamp, data storage, and the whole process of the blockchain; third is the judicial consortium layer, which connects notary offices, CA/RA institutions, judicial authentication centers and courts with blockchain technology, with each unit becoming a node in the chain.

To sum up, more and more cyber-related crimes are migrating to the cloud, which increases the difficulty of electronic evidence collection. As electronic evidence, blockchain data has legal effect. At the same time, the advantages of blockchain, such as de-centralization, de-trust, traceability, collective maintenance, security, non-comparability, openness, and anonymity exactly solve the problems of intangibility, vulnerability, and other characteristics of electronic evidence. The importance of the construction of a blockchain electronic evidence collection system is evident. For example, given the traceability of blockchain, timestamp technology is adopted to ensure the traceability, integrity, and non-comparability of data, thus addressing the intangibility of electronic evidence. For another example, given the security feature of the blockchain, the data is encrypted with the encryption technology to ensure the security of the data, plus the strong calculation capacity formed by consensus algorithm, to resist external attacks and ensure non-comparability and unforgeability of the blockchain data, thus solving the vulnerability problem of electronic evidence. However, the application of blockchain electronic evidence storage is still a new thing, and the research on the application of blockchain characteristics in the collection and preservation of electronic evidence is very weak at home and abroad. This paper is to make up for this loophole.

42 'White Paper on Application of Judicial Evidence Stored on Blockchain' (*Information Center of the Supreme People's Court*, 8 June 2019) <http://www.caict.ac.cn/> accessed 15 April 2023.

3. Case analysis of blockchain evidence

The arbitration chain is established based on the underlying open-source platform of the FISCO BCOS blockchain. FISCO BCOS is an underlying open-source blockchain platform tailored for the financial industry with financial business practices as a reference sample and a financial branch version of the BCOS open-source platform created under the leadership of several members of the FISCO open-source working group such as WeBank, Shenzhen Securities Communication Co., Ltd., and Tencent Cloud. FISCO BCOS provides a comprehensive supervision and audit support module, including access control, CA identity authentication, account management system, and security monitoring, to support mass data capacity storage and flexible expansion. It also has the key management mechanism and privacy protection mechanism to fully meet the technical requirements of evidence storage in arbitration.[43]

3.1 Working principle of arbitration chain

The arbitration chain is governed in a consortium blockchain way. Figure 1 shows the business architecture diagram of the arbitration chain.[44] In this network, WeBank, evidence storage institutions, arbitration institutions, and other related parties can join as chain nodes to form a reliable consortium chain network.

43 'Arbitration Chain: Evidence Storage Practice Based on Blockchain' (*WeBank*, 2 October 2017) <https://fisco-bcos-documentation.readthedocs.io/zh-cn/release-1.3/docs/applications/%E4%BB%B2%E8%A3%81%E9%93%BE%EF%BC%9A%E5%9F%BA%E4%BA%8E%E5%8C%BA%E5%9D%97%E9%93%BE%E7%9A%84%E5%AD%98%E8%AF%81%E5%AE%9E%E8%B7%B5/README.html>

44 ibid.

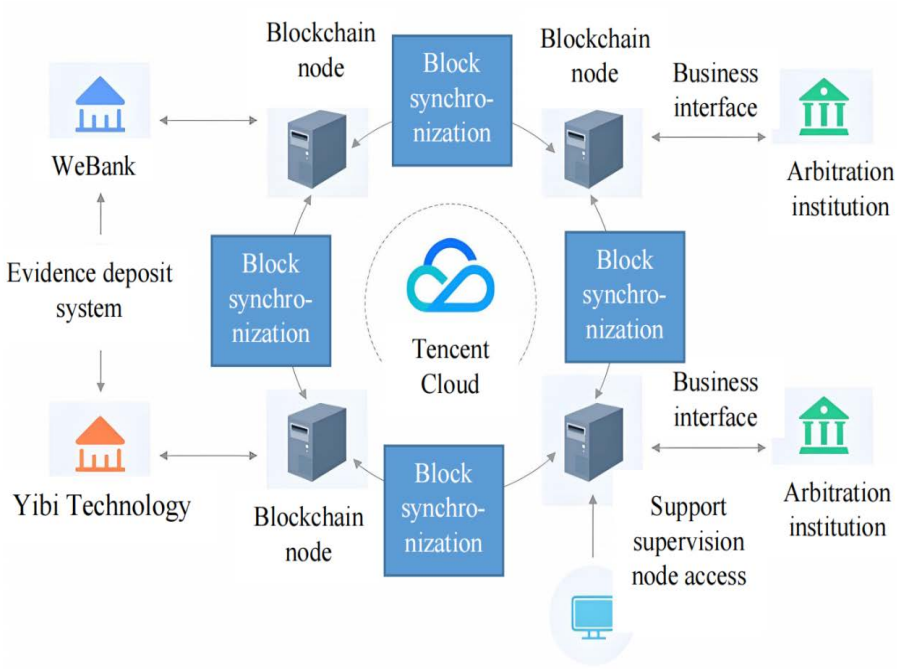

Figure 1. The business architecture diagram of the arbitration chain. Source: Arbitration Chain: Evidence Storage Practice Based on Blockchain (fisco-dev, 21 June 2019), at <www.bookstack.cn/read/fisco-bcos-v1.3/9c02182012f53485.md> (translated by the authors).

The arbitration chain adopts a governance method that conforms to the characteristics of the arbitration business to ensure good security features and privacy protection capabilities in its business setup, and in-depth research is conducted on how to clearly and conveniently monitor the operation status of the consortium chain, and support supervision and auditing demands, to ensure that the requirements of the financial industry on data structure, visualization, supervision, and auditing are met. Specifically: 1) only permitted members are allowed to join, thus avoiding the hidden danger of data leakage caused by irrelevant members joining the chain; 2) the consortium chain has a good management mechanism enabled by a variety of mechanisms such as joint governance, legal organization governance, leadership member governance to deal with various problems and optimize the management process; 3) each participant can be assigned with different operation privileges and their responsibilities clearly defined to prevent data privacy from being leaked to inappropriate members; 4) the activities on the chain can be monitored in real-time and abnormal activities intervened by setting up independent observation nodes, calling API data interfaces, deploying specific intelligent contracts, etc. Blockchain browser, monitoring system, monitoring node, and anti-money laundering interface are all the

implementation links of governance. Specifically, 1) the arbitration chain provides a blockchain browser, which can visualize the data on the blockchain and display it in real-time. Users can easily obtain the deployed blockchain nodes, blocks, and transaction information through the web page even if they have no technical background; 2) the monitoring statistics log is optimized to enable developers to quickly obtain important parameters in the running process of the blockchain system and evaluate the running state of the system from multiple dimensions; 3) the supervisory or auditing department can be integrated as a special supervisory node, so that they can synchronize data in real-time and monitor or audit the integrity and validity of the data, and can also carry out compliance inspection of business processes, anti-money laundering and other operations at the same time.

3.2 Workflow of arbitration chain

The application of electronic evidence in the arbitration chain mainly includes three parts: evidence storage, evidence collection, and evidence authentication. Evidence storage is the core part. Before initiating storage, an intelligent contract of initial conditions for storage shall be deployed to stipulate the conditions required for the evidence storage to take effect. Fig. 2 is a schematic flow chart of evidence storage. In the so-called evidence storage, business data is uploaded after being signed by the WeBank evidence storage system, and the evidence storage institution and arbitration institution are notified to confirm the data signature after successful uploading. After receiving the notice, the evidence storage institution and arbitration institution will take out the data uploaded onto the chain to verify and sign, thus completing the whole storage process. In the whole process of storage, the intelligent contract guarantees that no party can change the data stored, but only can add data to the stored data. Meanwhile, the quasi-real-time asynchronous upload of the evidence storage system does not influence the normal business logic. The evidence storage business process includes five steps: first, all parties involved in the storage need to agree on the conditions required for the storage to take effect in advance, and then one party will call SDK API to create and deploy a factory contract, which will come into effect through consensus; secondly, the storage business party calls the factory contract through SDK API to create a new evidence contract with its signature; thirdly, the storage institution calls SDK API to sign and confirm the evidence; fourthly, the arbitration institution calls SDK API to sign and confirm the evidence; finally, the arbitration institution obtains the evidence information on the chain through SDK API, and verifies the correctness and completeness of the existing signature of the evidence.

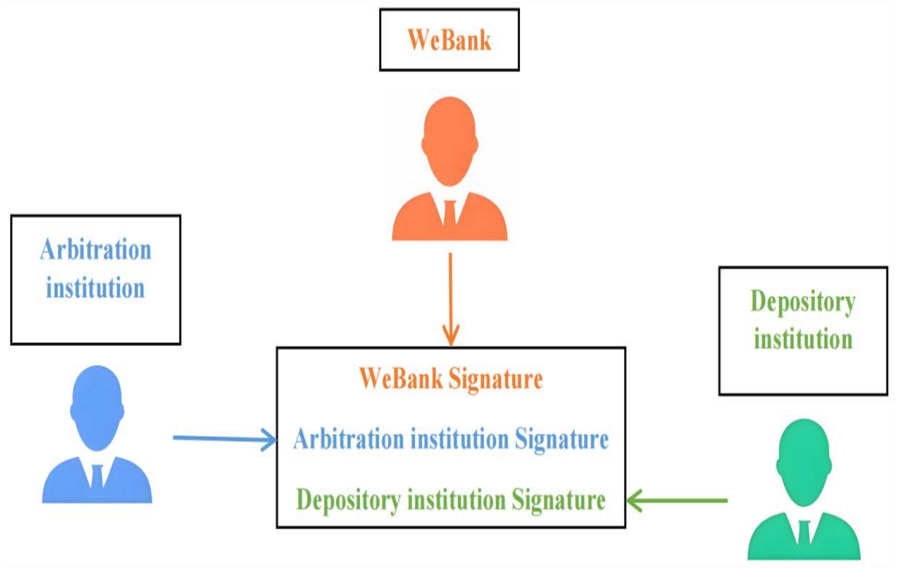

Figure 2. Schematic flow chart of evidence storage. Source: Arbitration Chain: Evidence Storage Practice Based on Blockchain (fisco-dev, 21 June 2019), at www.bookstack.cn/read/fisco-bcos-v1.3/9c02182012f53485.md (translated by the authors).

For evidence collection, when there is a need for evidence collection, WeBank selects data from the arbitration chain and submits the data to the arbitration institution. The arbitration institution analyzes the data provided by WeBank to obtain the relevant address information of the blockchain, and then retrieves the data on the chain through the address; finally, in blockchain authentication, the arbitration institution calls the related SDK interface after obtaining evidence to judge whether the evidence storage meets the initial conditions for the storage to take effect.

3.3 Application Effect of Arbitration Chain

The arbitration chain is based on a multi-centralized, tamper-proof, and trustworthy blockchain. With distributed data storage, encryption algorithms, and other technologies, the transaction data is signed with consensus and uploaded, the real-time preserved data forms the evidence chain through intelligent contracts to meet the requirements of authenticity, legality, and relevance of evidence and realize standardized evidence and trial.[45] In February 2018, the

45 Wanyun Shao, 'Guangzhou's First Arbitration Chain Judgment Released' (*China Economic*, 13 March 2018) <http://m.ce.cn/cj/gd/201803/13/t20180313_28446837.shtml> accessed 15 April 2023.

Guangzhou Arbitration Commission announced the feasibility of the arbitration chain in the industry's first award issued based on the arbitration chain. Since the release of the arbitration chain, more than 10 evidence storage institutions and arbitration institutions have joined the arbitration chain ecology. As of the fourth quarter of 2018, more than 10 million contracts have been stored, involving a capital scale of 100 billion yuan.[46]

After being applied in the arbitration industry, the blockchain has played a very important role in the collection of judicial evidence because of its traceability of records. A trustworthy blockchain network is currently incorporated into our transactions to complete the fixation and uploading of evidence in real-time. At the same time, it also allows the judicial institutions to participate in the bookkeeping of the blockchain and connect with the network arbitration tribunal to form a fast dispute resolution channel. With the establishment of the smart city, the city's transaction information will be recorded on the transaction chain in real-time. During evidence collection for judicial arbitration, it enables rapid trace back directly through the blockchain, and at the same time ensures the authenticity of the information, thus avoiding the step of evidence authentication and saving a lot of human resources. In addition, in the trial of cases involving over 2000 yuan to 50000 yuan, the lawyer's fees and travel costs are about 2000 yuan. If the online trial is adopted, the judicial cost is greatly reduced to only 500 yuan. Regarding the trial cycle, it, generally takes more than 6 months or even 1 year to complete filing, hearing, and delivery, while online arbitration only takes 7 to 15 days.[47] Specifically, when a default occurs and a party needs to apply for arbitration, it only needs to click 'One-key Arbitration' in the back-end system, and the data of the default transaction will be restored to the original data and sent to the arbitration platform of the arbitration commission. After receiving the original data, the arbitration commission will compare it with the previously stored data and issue an arbitration award after confirming the authenticity and integrity of the data. The time taken from clicking 'One-key Arbitration' to receiving the arbitration award can be as short as 7 days. At the same time, the arbitration fee can be as low as 500 yuan to 600 yuan for each transaction.[48] For arbitration institutions, the arbitration chain ensures that the transaction information on the chain will not be tampered with and helps arbitration institutions to quickly authenticate evidence, resolve disputes, reduce the labor, material, and time costs in the arbitration process, improve judicial

46 'China Blockchain Technology and Application Development Research Report' (*China Environmental Library*, 18 December 2018).

47 Yiming Liu, 'Public Consortium Chain Is the Key to the Door of Distributed Business Model' (*China Technology*, 8 June 2021).

48 ibid.

efficiency, and reduce overall arbitration costs.[49] For the parties involved, the arbitration chain will quickly and effectively resolve disputes and improve the operation and risk control efficiency.[50]

It can be seen that the application of the objective and transparent blockchain technology and operation mechanism makes the evidence or contracts more disaster-tolerant, reliable, and fault-tolerant, thus avoiding many expenses arising from conflicts and disputes, effectively reducing the risks of manual operation and moral hazard, and effectively solving the pain points of difficult evidence collection and arbitration. Moreover, through the arbitration chain, the arbitration institution can participate in the process of the evidence storage business, and together reach a consensus and witness in real time. In case of disputes, the signed and authenticated evidence storage data can be taken as direct evidence, to greatly reduce the arbitration process, help the arbitration institution to quickly complete the authentication of evidence and quickly resolve disputes, to further improve judicial efficiency, and reduce arbitration costs. At the same time, it is also conducive to maintaining law enforcement transparency, judicial justice, and social harmony.

49 According to the China International Commercial Arbitration Annual Report (2017) issued by the China International Economic and Trade Arbitration Commission on 16 September 2018, in 2017, 253 arbitration commissions nationwide accepted and heard 239,360 cases, an increase of 30,815 cases or 15% over 2016. Each arbitration commission received 946 cases on average, an increase of 115 cases or 14% over 2016. Among them, 6 arbitration committees handled 85,399 cases through online arbitration, accounting for 36% of the total number of cases nationwide. These data not only show that the arbitration chain has a huge market in China, but also play an important role in easing the work pressure of the arbitration commission. See China International Economic and Trade Arbitration Commission, 'China International Commercial Arbitration Annual Report (2017)' (China International Economic and Trade Arbitration Commission official website,16 September 2018) <http://www.cietac.org/> accessed 15 April 2023.

50 The China Arbitration Credibility Evaluation Report (2018) shows that 20.14% of the parties chose arbitration because of its high efficiency, 15.56% because of its professionalism and 15.00% because of its fairness. It can be seen that one of the important factors for the parties to choose arbitration to resolve disputes is that arbitration is usually more efficient than litigation and can more smoothly stop loss in a timely manner. For example, both the CIETAC and the Beijing Arbitration Commission decide domestic arbitration cases within 4 months and international arbitration cases within 6 months from the date of the court organizing. The use of arbitration chain for arbitration greatly shortens the duration and facilitates rapid resolution of disputes by the parties. See China University of Political Science and Law, 'China Arbitration Credibility Evaluation Report (2018)' (China University of Political Science and Law Newspaper Website, 11 June 2019) <https://newspaper.cupl.edu.cn/index/article/articleinfo?doc_id=8142> accessed 15 April 2023.

4. Problem analysis of blockchain evidence and its authenticity

4.1 Security risks at the technical level

The transmission and storage of blockchain data are open to the public, which is the advantage of blockchain-distributed bookkeeping, but at the same time, it also makes security threats the most significant problem faced by blockchain. For the application of blockchain electronic evidence involving a large number of personal privacy, business secrets, and even state secrets, unsafe data do not meet the legal standards for the identification of evidence. At this point, the evidence will become worthless. From the perspective of blockchain security analysis, the challenges come from algorithm security, protocol security, and cryptography security.[51]

4.1.1 Algorithm security risks

At present, there has not been any mainframe (super) computer serving as the node of the blockchain network. With the development of computational mathematics, cryptography, and computational capability, the blockchain will soon face the possibility of the algorithm being cracked.[52] Once the main data link is cracked, all the data will never be recovered. In April 2017, a foreign organization cracked 30 Bitcoin wallets with 3,000 trillion keys. In addition, as quantum computers become possible, the asymmetric encryption algorithm used in the blockchain in the future may be cracked by hackers, which is a potential security threat to the algorithm that the blockchain technology has to face.[53]

4.1.2 Protocol security risks

Blockchain technology is based on POW and other consensus mechanisms and its security risk lies in the 51% computing power attack. When a blockchain node is passed by a computer with more than 51% computing power, it can successfully tamper with and forge blockchain data.[54] Although no organization or institution has mastered 51% computing power at present, due to the uneven distribution of ore pools and miners, some ore pools have enough computing power to have administration privileges to some extent. If these large ore pools are broken through, 51% of the network nodes will be controlled by malicious

51 Yuandi Wang, Li Li and Die Hu (n 25) 81.

52 Jian Zhang, *Blockchain: Defining the Future of Finance and Economics* (China Machine Press 2017).

53 'Is bitcoin secure? The organization cracked 30 wallets with 3000 trillion ciphers' (*Chain Node*, 10 July 2019).

54 Yong Yuan and Feiyue Wang, 'Development Status and Prospect of Blockchain Technology' (2016) 4 Acta Automatica Sinica 481, 494.

people, then tampering and forgery of blockchain information will become completely possible, the authenticity of electronic evidence will be seriously questioned, and blockchain electronic evidence storage will be meaningless.

4.1.3 Password cracking vulnerability

Any cryptography is relatively safe. With the improvement of computing methods and power, the probability of cryptography being cracked becomes increasingly higher. Cryptography is relatively safe in a certain period, but it can hardly be safe in the long run.[55] Blockchain which uses a large number of cryptographic methods is a highly algorithm-intensive project with the computer capability at risk of being cracked on a large scale at present. GSM and WCDMA communication air interface encryption method is considered to be the most unlikely to be cracked (Encryption with snow), but it has been cracked by scholars from Israel and other countries in just ten years. Once the encryption algorithm is cracked, the entire security foundation of the blockchain will no longer exist, and all kinds of data will be exposed to the public. Electronic evidence involving personal privacy, trade secrets, and even state secrets, in particular, will bear the brunt.

4.2 Regulatory issues

After the Guangzhou Arbitration Commission issued the industry's first award based on the arbitration chain in February 2018, at 10:00 am on 28 June 2018, the judgment of the first blockchain evidence storage case in China was pronounced in the Hangzhou Internet Court which supported the plaintiff's adoption of blockchain as the evidence storage method and confirmed the corresponding infringement facts. On 7 September 2018, the Supreme People's Court also promulgated the Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts, formally acknowledging the binding force of blockchain evidence in addressing legal disputes.[56] However, in the judicial practice at present, there are still problems in the identification of the evidence authenticity and the lack of a unified and practical standard.

4.2.1 Authenticity problem of blockchain evidence

Blockchain electronic evidence storage mainly authenticates data with the timestamp function of blockchain technology and 'anchor technology'. To put its technical principle simply, it records and stores the data that appears and

55 Xin Shen, Qingqi Pei and Xuefeng Liu, 'Overview of Blockchain Technology' (2016) 11 Chinese Journal of Network and Information Security 11, 20.

56 Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts 2018, art 11.

exists at a certain moment on the blockchain through encryption protection (including electronic contracts, web screenshots, computer documents, video files, call records, and other electronic 'source files'), and affixes timestamp on the data to ensure the originality, integrity, and non-comparability of the data, thus realizing the self-authentication of the data. In the above-mentioned copyright dispute case heard by Hangzhou Internet Court, to prove that the defendant Daotong Technology published on its website the related works over which the plaintiff had copyright, the plaintiff HuataiYimei automatically called Google open source program puppeteer to capture the pictures of the infringing web pages, and at the same time called curl to obtain the source code of the target web pages, and calculated the compressed packages of the two and the called logs into Hash and uploaded them to FACTOM blockchain and Bitcoin blockchain. The arbitration chain currently in use by the Guangzhou Arbitration Commission is based on a multi-centralized, tamper-proof, and trustworthy blockchain. With distributed data storage, encryption algorithms, and other technologies, the transaction data is signed with consensus and uploaded, the real-time preserved data forms the evidence chain through intelligent contracts. According to the provisions of the Civil Procedure Law, authenticity, legality, and relevance are the criteria and principles for judging whether evidence has legal effect. In the aspect of examining the legal effect of blockchain electronic evidence storage, Hangzhou Internet Court examined and demonstrated the legal effect of the blockchain electronic evidence storage involved in the case in terms of the authenticity of the electronic data source, the reliability of storage, the integrity of content and the degree of correlation with other evidence, and finally determined that the blockchain electronic evidence submitted by the plaintiff has legal effect. However, in the first award based on 'blockchain + evidence storage' made by the Guangzhou Arbitration Commission, the electronic evidence storage of the blockchain involved in the case was directly determined to be legal and valid,[57] but its authenticity was not analyzed. The award reflects a question, namely, whether the authenticity of the electronic evidence storage of the blockchain can be directly determined on the premise that there is no evidence to the contrary to overturn it.

On 7 September 2018, the Supreme Court issued the Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts, of which art 11 is the provision on judging the authenticity of electronic data.[58] The provision stipulates that when judging the authenticity of electronic

57 MA Ce, 'From electronic evidence storage to blockchain evidence storage, where is the imagination space of judicial effect' (*Zhihu Website*, 19 March 2018) <https://zhuanlan.zhihu.com/p/34711967> accessed 15 April 2023.

58 Art 11 of Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts 2018, "If a party raises any objection to the authenticity of electronic data, an Internet court shall, in light of the cross-examination information, examine and judge the

data, the court needs to examine the authenticity of the process of electronic data generation, collection, storage, and transmission, and emphasizes the importance of examining the cleanness of the electronic data environment, the clarity of the subject and time, the accuracy and non-comparability of the content. In addition, para 2 of the provision specifically stipulates that 'the Internet court shall recognize electronic data submitted by the parties if the authenticity of the data can be proved by technical means of collection, fixation, and anti-tampering of such evidence as electronic signature, trustworthy timestamp, hash value check, blockchain or proven through electronic evidence collection and storage platform', which means that the blockchain evidence fixation and storage technology has received judicial confirmation for the first time in China and its application at the judicial level ushered in a breakthrough. At the same time, some people think that even though para 2 makes special provisions on evidence storage and fixation with the blockchain technology, the authenticity of the electronic evidence collected and fixed with this technology should be examined following the methods and principles specified in para 1, instead of regarding the data as authentic for granted.

In addition, according to art 9 of the Provisions of the Supreme People's Court on Evidence in Civil Proceedings,[59] it is not necessary for the parties involved to prove well-known facts, natural laws and theorems, and facts that have been proved by valid notarization documents. One of the major reasons is that these facts are objective facts or legal facts, which are regarded as real with no dispute in law. As the data recorded in the blockchain are true, the facts recorded and reflected in the data, including transaction behaviors, should also be true. Whether the parties involved need to prove such facts is also worth considering.

---

authenticity of the generation, collection, storage and transmission process of the electronic data, with the focus of examination put on the following: (1) Whether the hardware and software environments such as the computer system based on which electronic data is generated, collected, stored and transmitted are safe and reliable. (2) Whether the generation entity and time of the electronic data are specified, and whether the contents shown are clear, objective and accurate. (3) Whether the storage and safekeeping media of electronic data are definite, and whether the safekeeping methods and means are appropriate. (4) Whether electronic data extraction and fixation entity, and electronic data extraction and fixation tools and methods are reliable, and whether the extraction process can be reproduced. (5) Whether the contents of electronic data are added, deleted, modified or incomplete, or fall under any other circumstance. (6) Whether electronic data can be verified in specific methods."

59 Art 9 of Provisions of the Supreme People's Court on Evidence in Civil Proceedings 2008, "The facts as mentioned below need not be proved by the parties concerned by presenting evidences:1. The facts that are known by all people; 2. Natural laws and theorems; 3. The fact that can be induced according to legal provisions or known facts or the rule of experience of daily life; 4. The facts affirmed in the judgment of the People's court that has taken effect; 5. The facts affirmed in the award of the arbitration organ that has taken effect; 6. The facts that have been proved in the valid notary documents."

4.2.2 Lack of the unified and practical standard for blockchain evidence

At the current stage, if it is allowed to directly determine the authenticity of blockchain electronic evidence in judicial practice, there are still some problems. We know that notarization has been widely used in the field of judicial practice for a long time, with corresponding laws and regulations, guiding opinions, and industry rules, as well as a set of mature practical standards, and it is also easy for judicial personnel to understand. Therefore, the legal effect of notarization can be easily recognized by judicial personnel. Compared with notarization, one of the main problems faced by blockchain electronic evidence storage is the lack of a unified and practical implementation standard. At present, there is no uniform judicial approval standard for blockchain electronic evidence storage in the selection of third-party evidence storage platforms, technical standards for implementation, types of blockchains used, procedures and methods for evidence storage, standards for judicial review, etc. Because the legal effect of blockchain electronic evidence cannot be reviewed according to the established uniform standards and the fact that blockchain is a new technology, most judges do not know much about this technology, which will easily lead to inconsistent judgment standards and is not conducive to achieving fairness and justice in judgment results.

5. The USA blockchain evidence authenticity rules

5.1 How the USA treats blockchain evidence

In the USA, some states, as the pioneers of blockchain evidence rules, mainly adopt two methods to emphasize the principle of equal treatment.[60] The so-called equal treatment means that laws and regulations should treat blockchain evidence in the same way as existing legal forms of evidence. Also, the specific part of the blockchain evidence should be given the same treatment, and it will never be excluded or emphasized because it was born in a new technology environment. This principle was repeatedly stated when various new 'data messages' were born in the early years. For example, art 5 of the UNCITRAL Model Law on Electronic Commerce, with Guide to Enactment, 1996 with additional art 5 bis as adopted in 1998 stipulates: 'Information shall not be denied legal effect, the validity or enforceability solely because it is in the form of a data

60 Shelagh Dolan, 'How the Laws & Regulations Affecting Blockchain Technology and Cryptocurrencies, Like Bitcoin, Can Impact Its Adoption' (*Business Insider*, 3 March 2020) <www.businessinsider.com/blockchain-cryptocurrency-regulations-us-global> accessed 15 April 2023.

message'.[61] One is to separately stipulate the evidence status of blockchain records. For example, the Act relating to Recognizing the Validity of Distributed Ledger Technology of Washington 2019 stipulates: 'Electronic records shall not be denied legal force, the validity or enforceability solely on the ground that they are generated, communicated, received or stored using distributed ledger technology'.[62] The second is to stipulate its legal effect together with smart contracts and electronic signatures. As stipulated in the Blockchain Technology Act of Illinois,[63] which went into effect in January 2020, 'Smart contracts, records or signatures shall not be denied legal validity or enforceability simply because they are created, stored or verified by the blockchain', 'Evidence of smart contracts, records or signatures created, stored or verified on the blockchain cannot be excluded in litigation', 'If the provision of signed material is required by law, the submission of signature data electronically recorded on the blockchain or blockchain evidence to verify the intent of the signer intended to provide this condition is also met'.

Relevant bills and laws in Arizona, New York, and Ohio have also made such adjustments. In March 2017, Arizona amended the state's Revised Statutes by adding a new chapter on electronic transactions.[64] According to the newly added provisions, the signing behavior through the blockchain is regarded as a qualified electronic signature that meets the formal requirements, and the records and contracts obtained through the blockchain are deemed to meet the formal requirements and qualified records. Smart contracts may be used in commercial activities, and the legal validity, validity, or enforceability of the contract shall not be denied just because the contract contains smart contract terms. In January and March 2019, Bills No 1683 and No 4142 of the New York State Senate proposed amendments to the electronic signature and document law.[65] These two bills contain provisions to confirm that signatures and contracts can be made through the blockchain, as well as provisions to confirm the validity of

61 UN Commission on International Trade Law, 'UNCITRAL Model Law on Electronic Commerce, with Guide to Enactment, 1996 with additional article 5 bis as adopted in 1998' (United Nations Digital Library, 9 April 1999) <https://digitallibrary.un.org/record/286739?ln=en&v=pdf> accessed 15 April 2023.

62 Recognizing the validity of distributed ledger technology Act Washington Senate Bill 5638 2019, s 3.

63 The Blockchain Technology Act House Bill 3575 2020, s 10(a).

64 An Act Amending section 44-7003, Arizona revised statutes; amending title 44, Chapter 26, Arizona revised statutes, by adding article 5; relating to Electronic transactions House Bill 2417 2017.

65 An Act to amend the state technology law, in relation to blockchain technology and smart contracts Senate Bill 4142 2019; An Act to amend the state technology law, in relation to blockchain technology and smart contracts Assembly Bill 1683 2019.

smart contracts. In Ohio, Senate Bill 300,[66] introduced in May 2018, proposes to recognize smart contracts with full legal force and enforceability.

5.2 Commonalities in the blockchain evidence authenticity rules between the USA and China

On the one hand, both China and the USA generally apply existing rules on the authenticity of electronic evidence to blockchain evidence. In the USA, blockchain records fall under the broader category of electronic evidence.[67] In practice, ordinary electronic evidence can be applied to methods or rules such as insider testimony, check value verification, electronic record verification, judicial cognition, etc.[68] These methods or rules can also be used for blockchain evidence. In China, the representative rules on the authenticity of electronic evidence also be applied to blockchain evidence. For example, arts 93 and 94 of the Provisions by the Supreme People's Court on Evidence in Civil Procedures 2019[69] established a 'three-in-one' system of reasoning standards,[70] presumption standards, and cognitive standards for reviewing and judging electronic evidence. In practice, the blockchain records can completely follow the situations listed in the above provisions, making 'presumptions that are unfavorable to oneself', 'presumptions that originate from a neutral third-party platform', 'presumptions that are based on normal business records', 'presumption of archival storage', 'presumption of compliance with the agreement', etc.

Moreover, the above presumptions can usually be shared by multiple items for blockchain evidence. In the same way, the 'deemed as the original electronic data' rule implemented in my country can also be applied to blockchain evidence. For example, para 2 of art 15 of the Several Provisions on Evidence in Civil Litigation 2019[71] stipulates: 'The copy made by the producer of electronic data that is consistent with the original, or the printout directly derived from electronic data or other output media that can be displayed and identified, shall be deemed as the original electronic data'. On the other hand, US federal laws and some state laws have made amendments to blockchain evidence for

66 A Bill to amend sections 1306.01, 1306.04, and 1306.06 of the Revised Code to amend the Uniform Electronic Transactions Act to define records and contracts secured by blockchain technology as electronic records and to allow the use of smart contract terms Senate Bill 300 2018.

67 Victoria Lemieux, 'Blockchain for Recordkeeping: Help or Hype' (ResearchGate, October 2016) <https://blogs.ubc.ca/recordsinthechain/files/2018/06/FinalReport_Volume1.pdf> accessed 15 April 2023.

68 Federal Rules of Evidence 2023, Rule 901(b)(1).

69 Provisions by the Supreme People's Court on Evidence in Civil Procedures 2019, arts 93 and 94.

70 Pinxin Liu, 'On the Authenticity Standards of Electronic Evidence' (2021) 1 Social Science Series 68.

71 Several Provisions on Evidence in Civil Litigation 2019, art 15.

authenticity rules, best evidence rules, and presumption rules. The Supreme People's Court has also introduced the Special Articles on the Authenticity of Blockchain Evidence in the Rules of Online Litigation of People's Court 2021.[72]

5.3 Commentary on the USA blockchain evidence authenticity rules

Although the authenticity rules of blockchain evidence in the United States are subject to insufficient practical innovation, they also can provide many insights for enacting rules of blockchain evidence authenticity in China. This is prominently reflected in the legislation of some states by expanding the rules of 'self-authentication', 'presumption of business record exception', and 'presumption scope'. In June 2016, Vermont passed an act relating to miscellaneous economic development provisions, and a separate chapter sets out the provisions regarding the validation and admissibility of blockchain records in court.73 The act stipulates that if an electronic record registered electronically on the blockchain is sworn to be supported by a qualified person through a written statement, it is self-authenticating. The relevant written statement must indicate that itself made the written statement, indicating that the date and time when the electronic record enters the blockchain, the electronic record is kept in the blockchain as a normal business activity, and the electronic record is processed following normal business activities in line with customary practices. Certainly, this presumption (self-authentication) does not mean that the facts of the case or the content of the records are true, valid, or legal. The Act, which has the same effect as the Vermont Rules of Evidence 2011,[74] affirms the admissibility of electronic records stored on a blockchain in a trial or hearing. In September 2019, Virginia proposed a provision titled 'Business Records, Electronically Registered on a Blockchain Self-authenticating document' as House Bill No 2415 to the State House of Representatives.[75] The Bill stipulates, 'In any civil litigation, where a business record electronically registered on a blockchain is substantive and admissible, it should be presumed to be self-authenticating and extrinsic evidence of its authenticity should no longer be required'. The Bill establishes the same presumption rules as those outlined in the Act mentioned above, specifically concerning the presumption of authenticity of the record, the date and time of the record, and the maker

72 Rules of Online Litigation of people's Court 2021, arts 16 to 19.

73 An act relating to miscellaneous economic development provisions House Act 868 2016.

74 Vermont Rules of Evidence 2011, Rule 1101.

75 A Bill to amend the Code of Virginia by adding a section numbered 8.01-390.4, relating to business records electronically registered on a blockchain self-authenticating House Bill 2415 2019.

of the record. New York, California, and other states have also imitated the Act and enacted similar regulations.[76]

Looking at the above-mentioned state legislation in the USA, it is not difficult to find that the advantage of its blockchain evidence authenticity rules is that it is practically useful, and this is attributed to three consensuses. First, the focus of rule construction is the authenticity of the data after entering the chain, and the records before entering the chain are not within the scope of rule construction. The second is based on legal authenticity. Applying rules such as 'presumption of business record exceptions' to Blockchain evidence in various states in the USA shows that judicial practice does not pursue authenticity in the sense of being technically 100% unforgeable for blockchain evidence. This should inspire China's adherence to the rational truth view on the authenticity of blockchain evidence, that is, the use of blockchain evidence only needs to pursue 'truth that meets legal standards in specific cases'.[77] The third is to take the side identification mechanism as the direction. The review and judgment rules of any evidence can be cut from both sides. The former is to provide comprehensive review and judgment elements or standards on the front, and the latter is to provide methods to confirm whether the evidence is true or not. At present, when ordinary judicial personnel are still unable to positively identify the authenticity of blockchain evidence in China, it is a more feasible solution to first build a lateral identification mechanism.

6. Suggestions for blockchain evidence system improvement

6.1 To determine the authenticity of the blockchain evidence, the party claiming that the data has been damaged before uploaded shall bear the burden of proof

Art 69 of the Civil Procedure Law stipulates that 'the people's court shall take legal facts and documents notarized through legal procedures as the basis for ascertaining the facts unless there is evidence to the contrary sufficient to overturn the notarized evidence', which gives the notarized evidence direct legal effect unless there is evidence to the contrary sufficient to overturn it. One of the main reasons why notarized evidence is believed to be authentic is the introduction of a neutral third-party notarization institution to notarize the collection, fixation, and preservation of evidence. Unless there is evidence

76 Caytas Joanna, 'Blockchain in the U.S. Regulatory Setting: Evidentiary Use in Vermont, Delaware, and Elsewhere' (2017) 3 Columbia Science & Technology Law Review <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2988363> accessed 15 April 2023.

77 Pinxin Liu (n 70) 62.

to the contrary, notarized evidence will be considered authentic, but there is no judicial review on whether the generation, storage, and fixation of original data, information, and materials formed before notarization have been damaged, modified, or changed.

The authenticity of electronic evidence requires the authenticity of electronic evidence carrier, electronic data, and electronic evidence content.[78] Authenticity of electronic evidence carrier is aimed at the storage medium used as electronic evidence carrier and requires the originality, identity of the source, and the identity and integrity of evidence in the process of transfer and circulation, to ensure that the evidence carrier has not been forged, altered, replaced or destroyed; authenticity of electronic data requires the originality, identity of the source and the identity and integrity of the evidence in the process of litigation, to ensure that it has been deleted, modified or added; authenticity of the content of electronic evidence mainly targets at the information contained in the electronic evidence, whether the information can be mutually authenticated with the information contained in other evidence and whether the facts of the case can be accurately proved.

It is known that the blockchain adopts computer technologies such as distributed data storage, de-centralization, encryption algorithm, and consensus mechanism to make the data recorded in the blockchain tamper-proof and irreversible, which means that once authenticated and added to the blockchain, the data will be permanently stored, and there is almost no possibility of human modification, deletion, adjustment or change. Therefore, the data is highly trustworthy and reliable, and the trust problem between users is effectively solved. In this process, the blockchain acts as a neutral third-party organization, with the same function and function as the notarization institution, i.e., to ensure that the data are truly recorded. Since the authenticity of notarized evidence can be directly recognized, similarly, on the premise of no evidence to the contrary to overturn, the authenticity of electronic data stored and authenticated by blockchain technology should also be directly recognized, ie the authenticity of electronic evidence carrier, electronic data, and electronic evidence content. As for whether it has been damaged, modified, or adjusted before being uploaded, and whether it is complete, accurate, and objective, the other party should prove it and produce the evidence on the contrary mentioned above.

6.2 Implementation of access mechanism for third-party evidence storage platform

At present, there is a lack of a unified and practical standard for blockchain electronic evidence. We can consider implementing an access system

78 Fumin Chu, 'Three Levels of Authenticity of Electronic Evidence-Analysis Based on Criminal Procedure' (2018) 4 Chinese Journal of Law 121, 138.

for third-party evidence storage platforms, that is, only blockchain electronic evidence storage carried out by third-party evidence storage platforms with corresponding qualifications can be recognized by judicial authorities. This is similar to notarization institutions and judicial authentication institutions in that all of them need to obtain the corresponding qualifications. At the same time, it is also necessary to actively promote cooperation between the third-party evidence storage platform vs. the judicial services institutions such as courts, arbitration authorities, notarization institutions, and judicial authentication institutions to realize the sharing of resources and data. At present, the arbitration chain of the Guangzhou Arbitration Commission has been set up by WeBank in conjunction with the Guangzhou Arbitration Commission and Hangzhou Yibi Technology based on blockchain technology, and Hangzhou Internet Court has also launched its electronic evidence platform. Such blockchain electronic evidence platform directly built by arbitration institutions or courts undoubtedly greatly improves the credibility and practicability of blockchain electronic evidence. The establishment of the arbitration chain and the successful practice of Hangzhou's Internet electronic evidence platform both illustrate the importance of the access mechanism of the third-party evidence storage platform in promoting and improving the blockchain electronic evidence storage system and enhancing the efficiency and reliability of electronic evidence collection.

6.3 Comprehensive application of network security technology

In the face of the above-mentioned security problems encountered by the blockchain system, it is necessary to comprehensively use network security technologies such as cryptography and mimic defense to improve the security of blockchain from the aspects of algorithms, protocols, passwords, implementations, and systems, etc, in this way to further meet the existing security challenges. For example, institutions or organizations from more countries can be introduced to join the network nodes, nodes with computing power per node of no more than 20% join the entire network and system security experts adopt the best defense technology for blockchain systems.[79]

6.4 Future Development Direction

On the one hand, arbitration has many advantages over litigation. Firstly, the parties involved in arbitration have higher autonomy and can choose the arbitration institution, arbitrator, place of arbitration, arbitration language, arbitration rules, etc. Secondly, arbitration is more efficient than litigation. It takes 6 months for the court to complete the first trial, there may be a second trial after the first trial and still a retrial after the second trial, while arbitration produces

79 Haitao Mei and Jie Liu, 'Industrial Status, Existing Problems and Policy Recommendations of Blockchain' (2016) 11 Telecommunications Science 134, 138.

the final decision. Thirdly, arbitration provides better confidentiality. Although court decisions may not be held in public sometimes, such as those involving international secrets and trade secrets, the parties themselves need to apply for it. In contrast, the content of the arbitration agreement is restricted among the parties, arbitrators, and others in a small range. It can be said that these characteristics of arbitration win the favor of many companies and enterprises. According to the above analysis, China's arbitration market is a very large one.[80] Therefore, the arbitration chain should improve its technology and promote its wider application in the future.

On the other hand, the application of blockchain technology in the judicial field should be faster than that in other industries, because the judicial field itself is a multi-department and multi-institution assistance mechanism, and there is a need for data transmission and case information sharing among the public security bureau, procuratorate, court, and judicial bureau. Although this can be realized with the traditional technology, it is not trustworthy due to the system and mechanism problems and the efficiency is also low. Blockchain technology can be used as assistance. In the future, under the environment of Big Justice, courts and procuratorates may have consortium chains with cross-chain interaction among them. They will be both independent and cooperative with each other. After being approved by the judicial institution, blockchain technology will have very great reference and promotion significance for other industries.

7. Conclusion

The emergence of blockchain electronic evidence storage has brought us many conveniences, which are reflected in both daily life and judicial practice. However, they also bring challenges to the existing state and order. In essence, the emergence of each new technology will impact and change the existing things, and the law is no exception.[81] In this era when new technologies will always present new requirements and challenges to the existing legal system and legal regulations, we should always maintain an open and inclusive attitude, embrace the development of technology, keep up with the pace of the times, constantly revise and improve relevant laws and regulations, and make laws boosters of technological progress. In addition, although the academic circle has already started extensive discussions on the blockchain, most of the documents in the initial stage focus on some simple conceptual issues. Therefore, future research on the blockchain will focus more on the solutions to the problems existing in the blockchain and the application research of the blockchain,

80 Yli-Huumo, Jesse and others (n 27) 56.

81 Jun Zou and Haining Zhang, *Technical Guide for Blockchain* (China Machine Press 2016).

namely the research on putting blockchain technology into practice. With the maturity of blockchain technology and the deepening of people's understanding of blockchain, the problem of blockchain will eventually be solved. When mature blockchain technology is widely used in various fields, the era of 'blockchain+' will follow.