Science of Law Journal (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2024.030403
ISSN 2616-2296 Vol. 3 Num. 4

Legal dilemma and standardized evidence collection model for property embezzlement cases: An empirical analysis based on 214 Chinese criminal judgment documents

Ziyu Xu, Qing Wang, Pei Li

Shanghai University of International Business and Economics, Shanghai, 201620, China

Keywords: Blockchain; Virtual Currency; Fraud; Electronic Data; Forensics

Abstract: The emergence and multi-channel application of blockchain have provided new criminal tools for property crimes in China, and discussions on the authenticity and legitimacy of electronic data under blockchain evidence preservation have gradually emerged in criminal justice practice. Nevertheless, the legal dilemma that the evidence collection system is not perfect also appears. Based on the Chinese criminal judgments of 214 judgment documents from 2012 to 2023, this paper empirically analyzes the identity of electronic evidence collection and content, clarifies the obstacles to authenticity. The paper combines blockchain evidence preservation technology to design a blockchain model for electronic data evidence collection, supporting the penetration of blockchain technology into the criminal justice field as a new evidence preservation technology. Simulatanously it regulates the identification path of electronic evidence in China and improves the construction of the rule of law in China with the assistance of more complete statutory evidence collection and evidence preservation procedures.

1. Introduction

With the rapid development of modern Internet technology, the number of crimes committed using the Internet has been increasing. According to the Judicial Big Data Special Report on Characteristics and Trends of Crimes Involving Information Networks (2017.1-2021.12) officially released to the public by the China Judicial Big Data Research Institute, cybercrime cases have shown a year-on-year upward trend. Among them, the rise was particularly obvious in 2021, with the year-on-year increase of 104.56% in the number of cases concluded, and about 40% of the cases involving information network crimes involved fraud. At present, new virtual currency fraud cases have become an important part of criminal cases in China.

In the judicial trial process of cybercrime cases, the use of electronic data shows explosive growth characteristics. According to the Rules of Public Security Organs Handling Criminal Cases Electronic Data Forensics, electronic data forensics must follow the principles of legality, timeliness and efficiency and supervision of electronic evidence. Electronic data forensics has put forward higher standards for the operation of investigators, information extraction, preservation and identification and supervision of evidence collection process. In judicial practice, the illegal

procedure of electronic data forensics is a common reason not accepted by the court. Taking "electronic data" as the key word, the period from 2012 to October 2022 was selected for case retrieval. There were 1291 cases involving the authenticity of electronic evidence, of which 787 cases were affirmed, accounting for 61%, and the remaining 504 cases did not directly admit or even directly deny their authenticity.

Academically, blockchain electronic data deposit is still a forward-looking research issue, most scholars hold a positive attitude towards blockchain electronic data deposit, think that it can effectively guarantee the original state of electronic data by virtue of the unique decentralization of distributed ledger technology [1]. However, some scholars believe that blockchain certificates cannot guarantee the authenticity of electronic data generated before the chain. This paper will focus on China's new virtual currency fraud cases, on the one hand, through a large number of related cases empirical analysis, explore the adoption rate of electronic evidence judicial practice and the impact factors of electronic evidence authenticity. On the other hand, the paper explores the specific application of blockchain electronic data forensics by combining the literature of relevant scholars at home and abroad, and improves the corresponding forensics norms in China. Finally, a feasible model of legal electronic evidence forensics is built through interdisciplinary integration to break through the limitations of blockchain technology.

2. The empirical investigation on the authenticity of the three natures features of electronic data

In China, money laundering, fraud, pyramid schemes, and gambling are the four most common crinimal forms of virtual currency[2]. According to the analysis of data from the third research institute of the ministry of public security in China，54.72% of virtual currency crimes were related to money laundering and 21.13% were related to fraud.The paper based on such foundation and data, enlarged the forms of criminal cases of new virtual currency and finally explored the similar cases from Chinese Peking University magic weapon database as the samples. All the criminal samples are apt to the cause action of criminology, terms of judgement documents, names of Assault on Property, time spans from 2012 to 2023, including the discuss and topics of the electronic datas or electronic evidences from the judges. Above all, the paper collected totally 224 judgements to give furthur analysis.

Owing to the classification of such cases, the paper found that there are four distinct factors(data, content, term and procedure) which could be reviewed as the paramout impediments or considreation when it comes to the authenticity of electronic data by the Chinese judicial attitudes. From the perspective of empirical analysis, such factors affecting the authenticity of electronic data in judicial practice is conducive to clarifying the details that affect the authenticity of electronic data in the criminal field in the current Chinses judicial environment.

2.1 General Discriprion of relevant cases

2.1.1 Temporal distribution

From the aspect to number to cases, judicial precedents for electronic data and electronic evidence have gradually appeared in China from 2015. At the same time, from 2017 to 2021, the number of crime cases connected with electronic data is predominant. In those 214 cases, most of the cases orginated from the year of 2019 and 2020.With a small gap, it is of greater significance for current research and guarantees and liablity of the case analysis (Table 1).

Table 1: Distrubition of the date to cases

Date	Account	Percentage
2023	2	0.9%
2022	2	0.9%
2021	14	6.5%
2020	47	22.0%
2019	47	22.0%
2018	42	19.6%
2017	30	14.0%
2016	12	5.6%
2015	10	4.7%
2014	5	2.3%
2013	2	0.9%
2012	1	0.5%
Total	214	100%

2.1.2 Area distribution

It is been widely used in related crimes that electronic data had been acceped frequently in every zone for the past few years. According to 214 samples and cases, privince where has the largest number of applying electronic data is found in Shangdong, followed by Hunan Province and Jiangsu Province, and the rest of the provinces, such as Sichuan Province and Zhejiang Province, have a higher proporation. (Table 2).

Table 2: Precentage of main distribution of provinces in retrieved cases

Area(in China)	Acount	Percentage
Shangdong	23	10.8%
Huannan	19	8.9%
Jiangsu	16	7.5%
Sichuan	13	6.1%
Heilongjiang	12	5.6%
Zhejiang	11	5.2%
Fujian	10	4.7%
Henan	10	4.7%
Chongqin	10	4.7%
Guangdong	9	4.2%

2.1.3 Accusation distribution

Table 3: Search the distribution of convictions in cases

Accusation	Number	Percentage
Fraud	79	37.1%
Organizing and leading pyramid schemes	44	20.5%
The crime of illegally absorbing deposits from the Public	11	5.1%
Burglary	8	3.7%
Illegal business operations	8	3.7%
Other crime forms	64	29.9%
Total	214	100%

According to those 214 cases, the Crime of Fraud accounted for the largest share, up to 37.1% of all offences relating to electronic evidence against property which is enough to identify that virtual currancise had been one of the emerging form of crime of fraud recently. In all of those relating crimes, the crime of organising and leading pyramid selling activity accounted for 20.5%, total of 44 cases which is more than one-fifth of the numeber of cases retrieved. Acutually, in practice, the usage of virtual currency in pyramid schemes greatly reduced the risks and costs so that it is inevitably to inculde the phenomenon of fraud in the facts of cases which made it to be included in the category of virtual currency fraud cases.(Table 3)

2.1.4 Distribution of influencing factors

Based on the specificities of electronic evidence and electronic data as a type pf evidence, in the boom age of information, the tribunal always chose to accept or not accept the evidence which mentioned before in practice. By means of summarising and extracting, those 214 samples are devided into four parts including procedures, content, data and format by identifying the effective element of the acceptance about eletronic evidence andelectronic data. The highest percentage of influence is given to procedure, which accounts for 65 percent of the total number of factors relative to the other three, folled by the content. It is should be noticed that procedure and content are always considered together by courts during divided those case, which are used in arguments affecting th admissibility of electronic evidence.(Table 4)

Table 4: Precentage of factors influent the admission of electronic evidence

Influencing factors	Numer	Percentage
Procedures	169	65.0%
Content	64	24.6%
Data	15	5.8%
Format	12	4.6%
Total	260	100%

2.2 Analysis of the authenticity factors

Accroding to the Chinses Law of Evidence, the elecronic data is reviewed as the formaland legal evidence, which set the important three features (Authenticity, legitimacy, integrity) to proof. That is only after the satisfaction of these features do the elecronic evidence would be considered to use as the evidence for judgement and crinimal facts. To clarify the factors that affect authenticity, it is necessary to analyze from multiple perspectives. Based on the case screening and other scholars' explanations, four key factors were summarized: procedure, content, data and form.

2.2.1 Procedures for taking and depositing evidence and explanations of corrections

Electronic evidence collection procedure is an important part of effecting the authenticity of electronic evidence, which should comply with the principle of legality, the principle of timely and efficiently and the principle of chain of custody of electronic evidence. All of those three principles emphasise the procedural issues in the process of electronic evidence collection. It should be noticed that China's judicial practice for criminal cases of electronic evidence collection process does not have a relevant legal basis and the regulatory guidances which are used to judge and the corresponding regulatory guidance nowadays.

According to this 214 cases, a total of 169 judical precedents discussed the issue of the procedure for collecting electronic evidence, which identify the lack of standardisation and clarity of the

procedure for evidence collecting will lead to a significant influence that will weaken the authenticity of the electronic evidence. At the same time, this ultimately affect the adoption of electronic in practice. Among the 169 precedents with procedual disputes, there are total of 157 cases with disputed electronic evidence were finally adopted by the tribunal.(Table 5) Most of evidence which were provided by the investigative organ.compared with the 157 cases,there are 11 cases were not admitted,4 cases of it involved the provision of releavant electronic by the defendant or the victim as well as the rest cases evidence were provided by the investigating authorities. In the opinion of the tribunal in these 11 cases, the court exolicitly stated that the evidence does not comply with the relevent provisions of the evidence collection procedure, which made the lack of extracted transcripts, procedural requirements for self-initiated retrieval and so on. Among the evidences which were not admitted, most of them had the program such as doubtful evidence collection procedures and the risk of contamination of the evidence.

Table 5: Percentage of electronic evidence procedures accepted

Accepted or not	Account	Percentage
Accepted	158	93.5%
Not accepted	11	6.5%
Total	169	100%

In contrast, in the 158 precedents which evidence was adopted, the evidences provided by the defendant or the invsetigating organ were not perfect as usual. A total of 32 cases supplemented the flaws in the electronic evidence collection procedures through explanations or mutual corroboration which made the electronic evidence in the issue was adopted. Through statistical research, according to the 32 cases which electronic evidences was adopted by interpreting, there are two ways to adopted these evidences: (1) investigation organ interpret it; (2) Court interpretation. In the court interpretation, there are two method to used: one is compared mutually with other evidence to ensure the authenticity of evidence, the other is that the court believe that those defects does not effect the evidence on the power of proof, so that the court tends to adopt this evidence.

Through the classification of two types of implements which are listed above, (Table 6) most of these cases, although court consider that there are procedural defects, its defects are smll or does not have a legal basis which will not effect the power of evidence. All of those procedural defects were shown by lawer in the court, and due to the investigative organs's implement and interpretation of the evidence, evidences were adopted which in turn affected the penalties to te defendants ultimately.

Table 6: Method of correction of defects in electronic evidence

Method	Account	Percentage
Investigation organ correction	10	31.3%
Interpretation by court	22	68.7%
Total	32	100%

In the comparison of judicial precedents on the admission or non-admission of electronic evidence, there is no obvious difference in the procedural defects experienced by the electronic evidence itself, therefore the admission of such evidence relies mainly on the interpretation and understanding of the court, while the requirements for the procedure for obtaining evidence are not sufficiently clear.

2.2.2 Research on the electronic data itself

Electronic data ontology refers to the data that carries the data content. The influence of data ontology on the authenticity of evidence mainly comes from the unity of its internal and external

carriers, and the state of litigation circulation. Data is the basis of content, and the destruction of data authenticity will affect the admissibility of evidence content, which will lead to collateral distortion, and at the same time, the transformation of the internal carrier of electronic data to the external carrier is the responsibility of the investigating agency, which will inevitably involve the relevant rules of evidence collection procedures, and the irregularity of the relevant evidence collection procedures will also affect the authenticity of the data. The analysis of 23 cases related to data ontology factors (Table 7) shows that some human operations (procedures, means) lead to the distortion of the data itself. The authenticity of the data itself requires that after the data is retrieved, it should maintain uniqueness and integrity throughout the litigation process, which is a clear requirement for the investigators' means, that is, the chain of custody is not destroyed, so the authenticity of the data itself requires procedural legitimacy.

Table 7: Analysis and research of the electronic data

Adoption factors	The unification of internal and external carriers	Tampering or alteration
The number of adoption	14	4
adoption rate	78.57%	75.00%

2.3 Analysis of blockchain electronic evidence in the criminal field

At present, blockchain certificate deposit method is rarely used in judicial field, and only one case in criminal field uses blockchain certificate deposit technology to trial. In 2019, the People's Court of Shangyu District, Shaoxing City, Zhejiang Province, used ant blockchain technology for the first time to judge the criminal case[3], which also became the first criminal case of camp member blockchain certificate deposit in China. In this case, the defendant Wang uses the "borrowing" method in many places to defraud other people's property with the amount involved in the case of nearly 10,000 yuan. The victims are numerous and distributed throughout the country, with obvious characteristics of cybercrime. Therefore, relevant judicial organs cooperate with blockchain team to encrypt relevant electronic evidence by using blockchain technology, and effectively ensure the authenticity of the evidence of capital flow recorded in the CD through later hash value comparison.

From the perspective of the operation mechanism of blockchain, blockchain is a kind of chained data structure that combines data blocks in a sequential manner in accordance with the chronological order. With the unique decentralized and untampering technical advantages of blockchain which are distributed ledger technology, it can effectively guarantee the original state of electronic data, thus ensuring the objective authenticity of electronic data. In addition, the distributed ledger technology in the blockchain allows each transaction record to be timestamped, which meets the proof requirements of the chain of custody in external authentication that each forensic process has the proof of time. Therefore, the application of blockchain certificate storage technology can not only guarantee the objective authenticity of electronic data and make the self-authentication of electronic data come true, but also effectively record the electronic data into the chain and realize the external authentication of electronic data.

Based on the characteristics, decentralization and not easy to be exchange, the blockchain, which combined with this case, electronic evidence can be transformed into hash value electronic language through blockchain technology, and stored on multiple nodes of blockchain synchronously. Through special signature verification, electronic identity authentication, data encryption and decoding technologies [1], the electronic evidence such as capital flow data will be well preserved and not easily tampered. From this judicial practice, the technology of blockchain certificate deposit has

also been unanimously recognized by police organs and procuratorial organs in the application of evidence circulation. It can be seen that blockchain technology is of great significance for electronic data deposit, and the legal and effective application of blockchain certificate deposit technology in the judicial field will improve the efficiency of trial.

3. Issues and analysis on the determination of the authenticity of electronic data in the criminal field

3.1 Electronic data and authenticity

3.1.1 Electronic evidence and its transformation evidence

From the perspective of the forensic process, data is the basis of content performance, so that anything affects the authenticity of the data will affect the content factor simultaneously. In view of the integrity of data and content, according to the Chinese Provisions on Criminal Electronic Data, China relies on reviewing whether the data medium and backup, as well as the extraction and preservation procedures comply with the regulations, in terms of testing the integrity of evidence. However, it does not make a clear distinction between electronic data and traditional evidence materials such as documentary evidence. In the past, the Chinese Evidence Law did not define the status of electronic data, and the legal practice always shows that electronic data would be converted into expert opinions and documentary evidence.

The conversion to other types of evidence indicates a also change in the rules and regulations of evidence investigation apartment would apply. What's more, it should be taken for granted that electronic data is quite different from other evidence in terms of characteristics, production process, and other aspects. That's why if the transformed evidence ules are used at once, it will have a certain degree of impact on its authenticity and cross-examination.

3.1.2 The battle between the carrier and data itself

From a technical point of view, Message-Digest Algorithm 5 (MD5) can only ensure the integrity of electronic data after the hashing operation, but cannot guarantee that it will not be tampered with or added or subtracted before the operation, affecting the data integrity and content source [4].

According to he Chinses law and regulations now, there is no clear distinction between the authenticity of the data itself and the carrier of electronic evidence, but the authenticity of presenting the data content belongs to the attitude towards the authenticity of the carrier. Therefore, the academic community often discusses whether the authenticity data itself is the carrier, or chooses the mode of both authenticity. Many scholars believe that there is no derivable causal relationship between the results of the original storage medium and the electronic data extracted by the authenticity, and when the data is extracted from the original medium, the data itself maintains a certain degree of independence, and even if the original medium is changed, it does not affect the authenticity of the data itself. In many new types of Internet fraud cases, it is often the electronic data and the content of the performance that are related to the facts of the crime, rather than the electronic data carrier itself. Under such circumstances, the court strictly did not consider the circumstances of the investigating organ's seizure and sealing of the original storage medium as electronic evidence, which was unreasonable. However, in the review of electronic data carriers, China not only requires the unity of internal and external carriers, but also emphasizes the source authentication of external carriers (i.e., original carriers), that is, "uniqueness proof", and relies on the original medium for the uniqueness of data verification.

Therefore, the academic community often discusses whether the authenticity data itself is the

carrier, or chooses the mode of both authenticity. Many scholars believe that there is no derivable causal relationship between the results of the original storage medium and the electronic data extracted by the authenticity, and when the data is extracted from the original medium, the data itself maintains a certain degree of independence, and even if the original medium is changed, it does not affect the authenticity of the data itself. In many new types of Internet fraud cases, it is often the electronic data and the content of the performance that are related to the facts of the crime, rather than the electronic data carrier itself. Under such circumstances, the court strictly did not consider the circumstances of the investigating organ's seizure and sealing of the original storage medium as electronic evidence, which was unreasonable. However, in the review of electronic data carriers, China not only requires the unity of internal and external carriers, but also emphasizes the source authentication of external carriers (i.e., original carriers), that is, "uniqueness proof", and relies on the original medium for the uniqueness of data verification.

3.1.3 The over-highly dependence on the chain of evidence and expert opinions by forensic

As for the electronic data carriers, according to relevant cases and papers, there are mainly problems of the unity of internal and external carriers and also the authenticity of the evidence in the process of litigation circulation.

Among the chain of data custody, procedures such as production, storage, transmission, acquisition, collection and presentation are the basic safeguards for the authenticity of electronic data in process of review the evidence circulation by judges. When it comes to the review of the unity of internal and external carriers, the original carrier (i.e., the original storage medium) is the key factor affecting the identification. In the sophisticated activities such as the fraud and financial crimes, there are many and dizzy electronic devices and mixed information with nonsense. That is why in the process of collecting and producing evidence, the investigating authorities and departments are often unable to identify, seize, and seal the specific original media.

As for the authenticity review of the content, most 213 cases were tended to adopt the methods of dual use of other evidence and expert opinions, so that it indeed spurs the status quo of relying too much on experts. Many defendants and their defenders put forward the issue of the qualifications and procedures of the these expert subject. Furthermore, owing to the professionalism and particularity of the expert opinions, the judges who have the obligation or have to reviewed the electronic data was excluded for the sake of the lack of relevant techinical knowledge.

The Chinses court and justice adopt the combined methods of other common evidence(a series of inquests, examinations, and search records) and expert opinions when confronted with the problems of authenticity in the process of evidence litigation circulation(from the investigation apartment to the final court). Although the Electronic Data Rules in China increases the obligation of the public security organs to designate personnel to testify in court to conduct data tests and issue reports, it still does not change the current status quo of trial in China, which is biased towards written authenticity verification and centered on transcripts.

3.2 Problems in the application of blockchain in the criminal field

3.2.1 Blockchain technology and Forensics

Blockchain is a chained data structure that combines data blocks in a sequential manner according to chronological order. It utilizes the decentralized and impenetrable characteristics of distributed ledger technology to effectively guarantee the original state of electronic data. Distributed ledger technology in blockchain makes every transaction record will have time-stamped, which means every forensic process has time proof [5].

The forensics personnel should first extract the effective information from the blockchain. After locking the suspect account address, they further search the relevant information of the account address by using the blockchain browser. Through the overlapping comparison between the account activity time and the crime time, it can be judged whether the account is related to criminal activities, so as to determine or exclude the suspicion of the account;For suspected accounts, search for other accounts related to it. Finally, by summarizing and analyzing all of those suspected accounts, it can be judged whether the criminal activity is organized, and then analyze the flow direction of these account tokens to form the final evidence collection report (Figure 1)[1].

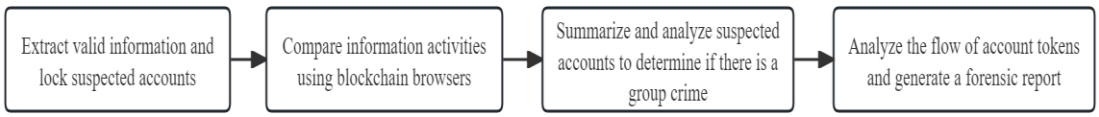

Figure 1: Process for determining whether criminal activity is a group

3.2.2 The impact of blockchain technology on electronic evidence Forensics

While blockchain technology has many advantages in electronic evidence forensics, it also has disadvantages. First, blockchain technology relate complex algorithms of multiple nodes, which increases the complexity of electronic evidence forensics, demands on the expertise and the experience of forensics personnel. Once the forensics personnel do not have the relevant expertise or are not familiar with the relevant regulations or legality requirements of blockchain forensics, the validity and admissibility of electronic evidence will be affected. Furthermore, blockchain technology needs to ensure data security and privacy. If the blockchain system is vulnerable or be hacked, it may lead to the disclosure and tampered of electronic evidence, thus affecting the reliability and accuracy of evidence.

3.3 The impact of blockchain technology on electronic evidence

3.3.1 Impact on authenticity

There are lacking of relevant laws and regulations to set corresponding standards for the qualification examine of blockchain depository platforms. In practice, although some internet courts have formulated relevant standards for the qualification checking of third-party blockchain depository platforms, it have different emphasis and there is no unified applicable standard[6]. In order to ensure the reliability of electronic data, parties tend to deposit certificates on multiple platforms which damage the neutrality of the deposit platform. Secondly, because the third-party depository platform is profit-making, in order to obtain greater benefits, it may help the parties tamper with the evidence when providing services for the them. And those action will lead to the loss of neutrality and credibility of the depository platform, thus directly affecting the authenticity of electronic evidence.

In judicial practice, most electronic evidence is deposited in the mode of pre-chain production and post-event deposit. That is, the electronic data of transactions between the parties is happening before, and then the process of both parties or one party using blockchain for deposit will occur. However, blockchain can only record and protect the data who has stored in it, whether the initial data imported into it is authentic is not within the scope of blockchain technology. Someone can still tamper with and delete it before the electronic evidence storaged or transformed into the blockchain. Therefore, the authenticity of electronic evidence is difficult to be guaranteed [7].

3.3.2 Impact on Relevance

Electronic evidence are often associated with devices, the relevance with people is not strong. Therefore, to identify the relevance of electronic evidence, both the electronic evidence in solid storage devices and in peripheral devices should be considered, and combine the technical principle and content of electronic evidence to examine the relevant electronic evidence is probative in the case. In addition, it is necessary to consider the correlation between electronic evidence and the facts to be proved in the case, to examine the text information, image, audio, video and other information in electronic evidence. Then it can be judged whether various electronic evidence can mutually confirm and support each other and whether electronic evidence can correspond to the facts [8]. Due to the inherent defects of blockchain technology and the risk of tampering or deletion of pre-chain data, the legitimacy and authenticity of electronic evidence cannot be guaranteed. The probative force of electronic evidence is low. Thus, the authenticity of its content directly affects the corresponding relationship with the facts which need to be proved, and then affects the relevance of electronic evidence.

4. A judicial path model for electronic data evidence collection in new virtual currency fraud cases

The authentication method of electronic data authenticity in Chinese criminal field is the chain of custody proof of external authentication nowadays. The cost of external authentication is high, and it is easy to appear defects, which will weaken the authenticity and probative power of evidence. Based on it, when adopting the above new judicial model of custody chain of evidence, it should also adopt the self-authentication method of blockchain deposit certificate.

To ensure the authenticity of electronic data from generation to entering the chain, Figure 2 shows the blockchain certificate model designed based on the characteristics of electronic data.

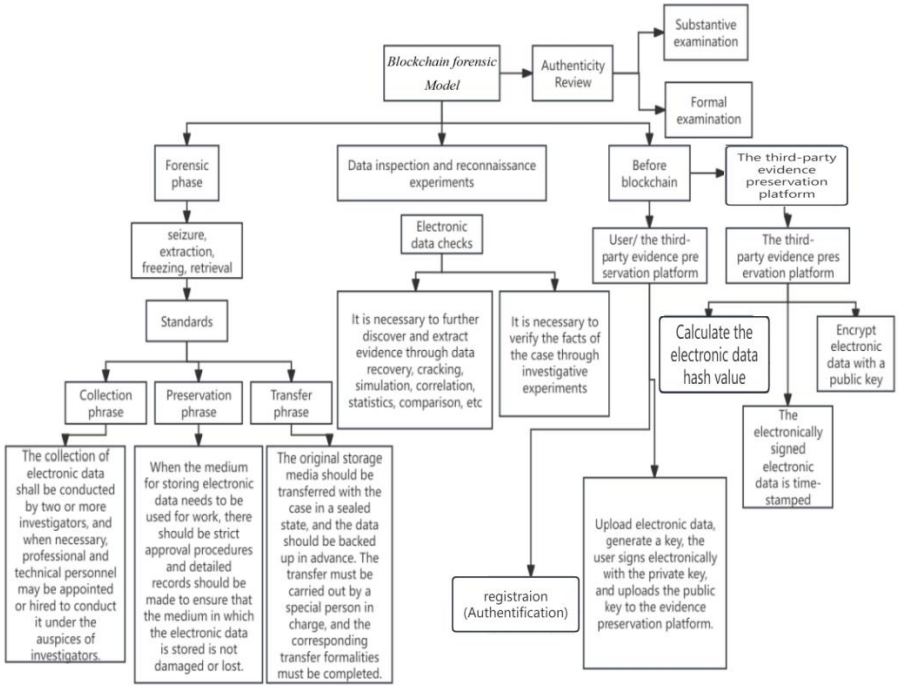

Figure 2: Blockchain certificate deposit model for virtual currency fraud cases

Firstly, faced the complexity, ambiguity, disorder and lack of unified standard of electronic data, it should be extracted according to its characteristics in the forensic stage. For example, fulfil the

conditions for on-site extraction, the electronic data shall be extracted on site;if the conditions for online extraction are met, the evidence shall be extracted online from the network. It is beneficial to improve the efficiency of forensics based on the characteristics of electronic data. In the standard of evidence collection, it should be carried out by more than two investigators, and under the supervision of investigators, by assigning or employing professional and technical personnel when necessary; In the evidence preservation stage, the electronic data should be backed up in the process of obtaining evidence, and the backup data should be encrypted to prevent data loss or tampering; In the evidence transfer stage, the original storage medium should be transferred with the case in a sealed state, and corresponding data should be backed up in advance, then the evidence that cannot be transferred should be verified by idenification and court investigation.

After strictly following the standard of electronic evidence collection, electronic evidence should be examined, investigated or verified according to different situations, so as to preliminarily examine the authenticity of electronic data. After the preliminary examination, the electronic evidence should be uploaded to the third-party certificate deposit platform. Users can collect and upload electronic evidence by themselves or entrust a third party institution to upload the collected electronic data to the third party certificate deposit platform. After the third-party certificate deposit platform generates two keys, the user signs on the electronic data with the private key, the third-party certificate deposit platform encrypts the electronic data with the public key, and converts the original electronic data into a hash. Because Hash is a deterministic algorithm, different input data will produce different Hash, which is unique. Therefore, the judicial department can compare the hash uploaded by the third-party certificate deposit platform with the background hash to identify whether the original data has been tampered or not. In addition, the third-party depository platform also utilizes distributed ledger technology to stamp electronic data with time stamps and effectively record electronic data, which can further prevent data from being tampered with.

Finally, to further standardize the process of the authenticity examination of electronic data, the court should combine formal examination with substantive examination when examining the authenticity of electronic data. If the parties raises objections to the authenticity of the electronic data before the chain, the judge should conduct formal examination and substantive examination respectively based on the evidence. If the proposer has submitted relevant evidence before the electronic data is linked to the chain, the proposer of the objection is required to present contrary evidence or reasonable explanation; On the contrary, if the proposer does not submit relevant evidence before the electronic data is put into the chain when the objection is raised, the judge only needs to conduct a formal review at this time. Finally, once the objection meets the statutory requirements, an electronic data substantive review should be conducted. The judge should determine the authenticity of electronic data before it is uploaded either after ex officio access to the evidence or after the proposer has presented the evidence.

5. Conclusions

Recently, the technology of internet fraud is constantly changing. Many cases have seen the emergence of new types of scams by blockchain virtual currency, and there is no unified standard for the collection of electronic evidence in Internet fraud in China. Resulting in the determination of the authenticity of electronic evidence and the court's acceptance gradually becoming a dilemma in China's criminal procedure practice. According to the empirical analysis of relevant criminal judgment documents, there are four main types of factors affecting the authenticity of electronic evidence: evidence collection procedures, electronic data itself, the content and form of expression. According to the characteristics of China's traditional evidence chain of custody and new virtual currency fraud cases, the investigation authorities often adopt the system or method of

self-examination and self-approval. At the same time, the fraudulent transaction is anonymous, it is necessary to build a new remote evidence collection and chain of custody model. Combining the blockchain technology of the virtual currency circulation medium to establish a blockchain evidence preservation and consolidation model, it is necessary to ensure that the fraudulent transaction can collect evidence before and during the criminal activity, and also ensure the authenticity of the evidence after the activity.

References

[1] Lu Yu, Wang Huiui, Zhang Yong. Application and Approach of Electronic Data Block Chain Storage Certificate [J].Journal Of Dalian University, 2023, 44(01):77-85.

[2] Li Dameng, Sun Jie. Virtual currency crime situation and security governance review[J].Police Techonology, 2023, (02): 33-41.

[3] Criminal Judgment of Shangyu District People's Court, Shaoxing City, Zhejiang Province, China, 2019.

[4] Cui Shiqun. Research on the Authenticity Examination of Blockchian Evidence[J].Business and Economic Law Review, 2021(03):142-158.

[5] Xie Dengke. The Rules of Electronic Data Authenticity Review: Its Reflection and Improvement[J].Academic Exchange, 2021,(03):62-69.

[6] Jiang Airu. Research on Digital Forensics Based on Blockchain Technologe[D].Beijing:People's Public Security University of China, 2022:31.

[7] Hu Boyuan, Zhang Huaizhi. Research on Electronic Data Forensics under the Perspective of Blockchain [J]. China-Arab States Science and Technology Forum, 2023,(03):103-107.

[8] Guo Jing, Jia Xulong. Review and judgment of electronic data[C].National Prosecutors College, Office of the Research and Guidance Group for Punishing Cybercrime and Safeguarding Cyber Security of the Supreme People's Procuratorate, Law School of Chinese University: Theory and Practice of Cybercrime Governance for Excellence in Criminal Prosecution - Proceedings of the 16th National Senior Prosecutors Forum, 2020:5.