

# Research on the Validity of Electronic Evidence

Fanqi Zhou

School of Law, Qingdao University of Science and Technology, Shandong, China

## Abstract

With the development of internet and other science and technology, the number of electronic data in judicial cases is increasing. Although the three major procedural laws have included electronic data into the types of legal evidence, the definition and types of electronic data are clearly defined in the form of legal provisions, but the definition of electronic evidence and its effectiveness identification standard have not been specified in the legislation, therefore, based on the judicial practice and the status quo of relevant legislation, it is essential to determine a more perfect identification standard for electronic evidence. This paper first analyzes the relevant cases of electronic evidence, and further discuss how to examine the electronic evidence in specific cases, that is, from the authenticity, legitimacy, relevance, probative force and other aspects of electronic evidence, and analyzes the problems in the legislation and practice of electronic evidence, so as to provide relevant suggestions and explore the establishment and improvement of the identification rules of electronic evidence.

## Keywords

Electronic Evidence; Electronic Data; Identification Standards; Evidence Acceptance.

## 1. Introduction

### 1.1. Research Background

With the development of information network technologies such as the Internet, electronic data has emerged in large numbers in judicial cases. Although China's three major procedural laws have added electronic data as a new type of evidence to statutory types of evidence after the revision, and its definition has been clarified, the provisions do not clarify the meaning of electronic evidence and how it should be reviewed in specific cases. Whether the data can be identified as evidence is still a big controversy, and even led to different judgments in the same case in some cases. Due to the unclear standard of evidence determination, unsound legislation, and excessive discretion of judges, compared with traditional evidence, electronic evidence is hardly adopted in cases, but electronic evidence and traditional evidence are not in conflict with each other. In a case, it is difficult to achieve judicial justice only by identifying traditional evidence, and achieve the purpose of safeguarding the legitimate rights and interests of the parties.

### 1.2. Research Significance

Out of the urgent need for the identification of electronic evidence in judicial cases, it discusses the problems and deficiencies of electronic evidence in legislation and judicial practice, and provides improvements in identification standards, legislation, judges' discretion, and specific cases. It is hoped that the development and improvement of electronic evidence identification standards can promote the progress of China's evidence law to a certain extent, promote the soundness of the legal system of electronic evidence, and effectively protect the legitimate rights and interests of the parties, and make judicial trials more fair. Improve the level of judicial practice in our country.

### 1.3. Research Ideas

In the Internet era, electronic data has been established as an independent type of evidence. Although the law clearly stipulates its definition and types, due to the fact that electronic data is easily tampered with and the relevant legal provisions are not sound, many people question the admissibility and probative power of electronic evidence. This article will start with the relevant cases of electronic evidence, analyze the current situation of electronic evidence in judicial practice, legal provisions and other aspects, analyze the problems of electronic evidence in legislation and judicial practice, and propose relevant solutions and suggestions for improvement.

## 2. Case Overview

In the second instance of Shidexiong's entrusted contract dispute with Haikou Private Travel Agency Co, Ltd. Shenyang Branch, the main dispute in this case was whether the appellant Haikou Private Travel Agency Co, Ltd. (defendant in the original trial) provided the appellant Shidexiong (plaintiff in the original trial) with multiple persons Travel services, whether the appellant needs to pay the appellee related expenses. During the first instance of the case, both parties cross-examined the evidence provided by the plaintiff on the financial statements provided by the plaintiff, chat records between the plaintiff's employees and the defendant, and details of the delegation. When the two parties cross-examined the evidence, the defendant retorted that I did not sign and approve the evidence submitted by the plaintiff, and the plaintiff collected the evidence in the case. I did not submit any evidence and could not fully conduct the case. Therefore, the defendant found that the plaintiff's evidence was insufficient and the evidence did not have Admissibility. Therefore, on the basis of no factual and legal basis, the evidence submitted by the plaintiff cannot fully prove the facts of the case, so the court should not support the claim made by the plaintiff. However, the court of first instance held that although the defendant did not sign and confirm the financial statement and the details of the delegation, the chat record between the plaintiff and the defendant can determine that the defendant has a clear understanding of the facts and amount of arrears, and knows that the plaintiff provided the defendant. The fact of multi-person travel services, and the evidences can be mutually corroborated, forming a complete chain of evidence in the determination of the facts of the case, thus proving that the plaintiff's claim is established. Moreover, the defendant also questioned the authenticity of the WeChat chat records, believing that the WeChat chat records may be deleted, but he refused the court to appraise its authenticity, and failed to provide contrary evidence to refute the authenticity of the WeChat chat records. Therefore, the WeChat chat records are admissible as electronic data and can be used as the basis for determining the facts of the case. Therefore, the plaintiff's evidence is not flawed, and the court of first instance determined that the plaintiff's litigation request was established. In the second instance of the case, the court of second instance reorganized the facts of the case and determined that: the court of first instance clearly investigated the facts of the case and used the law accurately. The court of second instance made it clear in the judgment that if it wants to prove the parties' claims based on objective facts of the case, or if contrary evidence is presented to overturn the opposing party's litigation claims, the parties themselves shall bear the burden of proof. Due to various reasons, the parties are unable to collect evidence, or the collected evidence cannot fully support their claims, and the party who bears the burden of proof shall bear the adverse effects of the proof. The appellant neither provided relevant evidence to refute the other party, nor applied for the appraisal of the authenticity of the other party's evidence, and should bear the unfavorable consequences of proof. Therefore, the court of second instance rejected the appellant's litigation request.

Through the analysis of the case, the following conclusions can be drawn: First, electronic data such as We chat records can be used as evidence to determine the facts of the case; second, the court reviews whether the evidence meets the authenticity requirements, and both parties Cross-examination, the probative power of electronic evidence can be determined; third, in order to prove the facts of the case, when a party provides electronic evidence as a basis, it must combine other evidence to form a complete chain of evidence to prove the facts of the case, thereby enhancing the power of electronic evidence Proof; Fourth, the parties themselves must be cautious about their statements during the trial. If the electronic evidence collected by them cannot prove the facts of the case, I must prevent my statements from putting my claims at a disadvantage. Withstand adverse effects. At the same time, if I question the authenticity of the electronic evidence of the opposing party, even if the evidence collected by the opposing party seems to be strong, I must apply to the court for a re-examination of whether the electronic evidence is authentic. Fifth, under normal circumstances, due to the rigor of adopting evidence, the court prefers that the party submit the original evidence. Therefore, the party should properly keep the original record of the electronic evidence. Electronic evidence is processed.

### 3. Determination of the Validity of Electronic Evidence

#### 3.1. Electronic Evidence and Electronic Data

After the revision of China's Criminal Procedure Law, Civil Procedure Law, and Administrative Procedure Law, the three major procedural laws have incorporated electronic data into the legal evidence types, and their evidence status has been confirmed through legal provisions. The definition of evidence and the standard for determining its validity have not been clearly stipulated by law. In academia, scholars are concerned about how to define electronic certificates According to data, there is no agreement. In the past, scholars originally defined electronic evidence as "computer evidence" because most of the electronic data was mainly stored in electronic equipment such as computers. Compared with "computer evidence", the definition of electronic evidence covers The content of is more extensive, that is, it is electronic or digital data information in electronic or digital form. It can be seen that electronic evidence is mainly composed of data messages.

Electronic evidence and electronic data [1]are not the same concept, and the two concepts should not be confused. This point is worth emphasizing. For "electronic evidence", there is currently no clear concept to identify it, but through investigation and research on the relevant literature of electronic evidence, from the perspective of the characteristics of electronic evidence, two different definitions have been formed. Some scholars believe that " "Electronic evidence" refers to files stored in computers and other electronic devices, or information and data generated during the operation of electronic devices, and can objectively prove facts associated with the case. This concept shows the "electronic" or "digital" characteristics of electronic evidence and its role in proving the facts of the case. Another part of scholars believes that "electronic evidence" is used to prove the facts of a case and extract data such as documents from electronic devices. This concept emphasizes the "electronic" nature of electronic evidence. Current scholars have not reached agreement on how to define electronic data. Some scholars believe that electronic data is mainly composed of digital information. It uses electronic, optical, magnetic and other means to perform operations such as data generation, storage, and transmission. Other scholars believe that it is a variety of documents and data information in electronic form, and it also has the function of being able to prove a certain fact. The first concept emphasizes the "electronic" nature of electronic data. The second concept not only reaffirms the "electronic" characteristics of electronic data, but also clarifies the function of electronic data to prove the facts of the case. All in all, electronic data and electronic evidence cannot be treated the same. Electronic data is only a kind of digital information material, and

electronic evidence is a kind of evidence stipulated by law. Electronic data is mainly composed of data information, and is generated and transmitted electronically. The connotation of electronic evidence is more abundant. In addition to electronic data, its main component is also required to have the power to prove objective case facts. That is to say, compared with electronic data, electronic evidence also has the function of objectively proving the facts of the case[2].

The Supreme People's Court's interpretation of the "Civil Procedure Law" Article 116 clearly stipulates the concept of electronic data, which is generated with the help of electronic technology, stored in digital form in electronic equipment, and the content of electronic data can be compatible with the carrier. Separated, and can be transferred to another device carrier by copying. The Supreme People's Court promulgated Article 14 of the "Decision on Amending the "Several Provisions on Evidence in Civil Litigation""", which stipulates that it regulates the manifestation of electronic data in the form of legal provisions, which covers judicial cases to a certain extent. The emerging forms of electronic evidence conform to the development of contemporary judicial practice. Article 7 of the "Electronic Signature Law" clarifies that data messages should be adopted when they meet the criteria for determining evidence. In judging activities, electronic data cannot be prejudiced due to differences in production methods and storage media from traditional evidence, denying its legal evidence status, and refusing to use electronic evidence as evidence. It must be considered that the collected electronic evidence must prove the facts of the case, and there is no flaw in effectiveness. The judgment of whether the evidence can be adopted must be combined with the determination standard in the specific case.

### **3.2. Identification Standards of Electronic Evidence**

In conjunction with the determination of the validity of traditional evidence, it is necessary to specifically judge whether the evidence can be adopted from the aspects of legality, authenticity, relevance, and power of proof. First, the objectivity of evidence is mainly whether the form and content of the evidence meet the standards of objectivity; secondly, the relevance of evidence is whether the evidence based on objective facts is relevant to the object of proof of the case; third, the evidence is Legitimacy refers to the form of evidence, the subject of evidence collection, the method of obtaining evidence, and the procedure of extracting evidence comply with the requirements of legality; finally, it is judged whether the evidence is probative and whether the electronic evidence itself can independently prove the facts of the case or the electronic evidence combined with others Whether the evidence can prove the facts of the case, and to what extent the evidence can confirm the facts of the case. Electronic evidence must first have authenticity. If it does not meet the determination of authenticity, then its probative power is doubtful and it will not be adopted in the case. Therefore, when judging whether electronic evidence can be adopted, the authenticity of the evidence must first be judged.

Although in the process of collecting or storing electronic evidence, the parties can use technical means to do so. However, when hearing a specific case, one cannot refuse to accept the evidence because the party uses a collection method different from traditional evidence to extract the electronic evidence, or reduce the adoption of electronic evidence in the case, nor can it be because the electronic evidence is "hard to tamper with," Delete the feature and increase its acceptance. In judicial practice, the electronic evidence used as the basis for the verdict needs to meet the relevant provisions of probative power and probative power. However, because the legal provisions do not stipulate how to review electronic evidence, the authenticity, relevance and legality of electronic evidence must be determined. Make judgments[3].

### 3.2.1. Confirmation of the Authenticity of Electronic Evidence

#### 3.2.1.1. Original and Photocopy

The determination of authenticity[4] must adhere to the principle of non-discrimination, that is, the determination of the form of electronic evidence cannot be limited to the original or copy, but depends on whether the electronic evidence retains all the information originally formed by the data. If the information it retains is complete and can objectively reflect the facts of the case, the copy has the same effect. Therefore, no matter whether the electronic evidence is the original or the photocopy, it will not affect the determination of the facts of the case. As long as the content of the electronic data is authentic, it can be initially adopted in the case. Because electronic evidence has the characteristics of virtualization and digitization, the copy and the original have the same validity and proving power and can be adopted. And although the law clearly stipulates that the evidence submitted by the parties is electronic data, the original documents of the electronic data need to be submitted. The copy provided by the original creator of the electronic data is consistent with the original, or through The original copy of the electronic data, etc., or other documents that are recognized and recognized by humans, can be considered to have the same effect as the original electronic data.

Article 23 of the Supreme People's Court's decision to amend the "Several Provisions on Evidence in Civil Litigation" stipulates that the original and photocopy should be adopted in the case. When submitting electronic data or audiovisual materials, the original documents of the materials should be submitted to the court. However, if the parties really have difficulties in providing the originals, they can submit copies of the electronic data, etc. Article 64 of the Supreme People's Court's Provisions on Several Issues Concerning Evidence in Administrative Litigation, in order to determine whether electronic data is probative or to examine whether the electronic data submitted by the opposing party meets the authenticity requirements, after confirmation by means of notarization, electronic The copy of the data is deemed to have the same effect as the original and can be adopted. However, the actual situation of the case is through printing, screenshots and other means. Although electronic evidence can be presented in court, it is still difficult for the parties to submit the original. If there are doubts about the validity of electronic evidence and the original cannot be provided, coupled with the intangible and easy-to-tamper characteristics of electronic data, the court cannot judge that the content of electronic evidence is objective and authentic, and will usually not accept it.

Review whether the electronic evidence complies with the authenticity regulations. On the one hand, the content of the electronic evidence must be reviewed. On the other hand, it must be reviewed whether the electronic evidence is objective and truthful during the process of generating, transmitting and storing electronic evidence, and from the collection of electronic evidence to the submission of electronic evidence in court. Sex and integrity. Moreover, in order to prove that the electronic evidence is complete and true, technical means are indispensable, and the technical means must be reliable and safe, otherwise the proof of evidence will be flawed and the court will not accept it.

#### 3.2.1.2. The Identity of the Subject of Electronic Evidence

In practice, it is often impossible to prove that the identity of the sender of the electronic evidence is the person involved, so the proof of the evidence is flawed and the evidence cannot be adopted in the case. Article 9 of the "Electronic Signature Law" clarifies the identity of the sender. If one of the three situations is met, the identity of the sender can be identified. However, in practice, many complicated situations will occur. Can not prove their own subject identity, which makes it more difficult to produce evidence.

In traditional evidence, the identity of the subject of the party is confirmed by handwritten signatures, or the identity of the subject of the party is confirmed by the identification of handwriting, but for electronic evidence, neither of these two methods can be implemented. In

practice, the identity of the parties cannot be proved. Article 14 of the "Electronic Signature Law" stipulates that a reliable electronic signature is considered to have the same legal effect as a handwritten signature or a seal. With reliable electronic signature electronic data, the sender's subject identity can be directly identified. For electronic data that does not use a reliable electronic signature, other evidence in the associated case is needed to verify the sender's subject identity, for example, the user's identity. Whether the account is bound to a mobile phone number, whether the user's account is authenticated by real name, are used to verify the identity of the subject.

The authenticity of electronic evidence can be further discussed: Formal authenticity: Electronic evidence must have an exact and reliable carrier. Electronic evidence is mainly composed of electronic data. As the name implies, electronic data is data in electronic form. The tool can understand the specific information it stores. After reviewing the original and copy of the electronic evidence, it is determined that the two have the same proving power, and the copy of the electronic evidence can also be adopted; substantive authenticity: the content of the electronic evidence is clear, objective and accurate, and the content of the electronic evidence is clear, objective and accurate. It is forged; electronic evidence is based on objective case facts, and conjectures that are not based on facts cannot be adopted as evidence. To review the authenticity of electronic data, it is necessary to determine whether its content meets the requirements for completeness, that is, whether the content of electronic data has been artificially tampered with, whether the content is complete, and so on. Civil litigation should refer to this provision to examine whether the electronic evidence is objective and true. The legal provisions listed are to determine whether the content of the electronic evidence is true and objective. In summary, the key to examining whether the evidence is objective is to examine whether its content complies with the relevant provisions of authenticity. Article 5 of the Electronic Signature Law of the People's Republic of China to clarify whether the electronic evidence meets the specific requirements of the original, that is, the content of the evidence must not be damaged when the evidence is collected. The content of the evidence must be objective and cannot be modified manually. This provision also shows that it is important to review the authenticity of the content of electronic evidence. Article 8 of the "Electronic Signature Law of the People's Republic of China" states that determining whether electronic data is objective or not starts from three aspects: operators, operating procedures, and information systems. For example, when judging whether the method of generating, storing or transmitting data messages is worthy of recognition, you can check whether the process of generating, storing, and transmitting data messages by the operator complies with the law, and whether the operating system has the possibility of being invaded by unauthorized persons In the process of generating, storing, and transmitting data messages, did the operators carefully and accurately follow the process, and whether the operation steps were changed without authorization; whether the information system is trustworthy in the process of generating, storing, and transmitting data messages ; Whether outsiders can perform illegal operations on entering the system, etc. When examining whether the methods used to keep the contents of electronic data intact are trustworthy by the parties, and when judging whether the sender's methods are trustworthy by the parties, it is indispensable to use technical means for verification. For example, just signing your own name on a file is more likely to be tampered with than a digital signature, data messages with encryption measures are more reliable than data messages without encryption measures, and so on. It is impossible for the law to provide a set of very detailed and complete rules so that judges can apply to all cases. This requires judges to judge the specific circumstances of the case based on trial experience.

### **3.2.2. Determination of the Relevance of Electronic Evidence**

The relevance of electronic evidence refers to "whether the evidence based on objective facts is relevant to the proof object of the case". The premise of using electronic evidence is that the

facts contained in it need to comply with the following regulations: first, what facts can be identified by electronic evidence; second, whether the facts of the case can fundamentally deal with the difficult issues in the case; Are there any clear regulations on the content of the evidence relevance? After answering these three questions, people can understand the specific connotation of electronic evidence in more detail.

Traditional theory believes that evidence must be substantive, that is, for the facts of a case, the evidence must have a substantive proving effect, and the evidence must also be probative, that is, the objective facts in the evidence can prove the facts to be proved in the case or related disputed facts. These two properties of evidence are closely related to the relevance of the evidence. Whether the evidence is relevance depends on whether the content and information contained in the evidence can be used to identify the facts of the case. In the past, to determine whether the evidence is related to the case, it is important to determine whether the content of the electronic evidence is related to the facts of the case, as opposed to examining whether the electronic evidence carrier complies with the provisions of relevance. In the process of determining whether the electronic evidence complies with the relevance regulations, checking whether the content of the electronic evidence meets the relevance requirements and determining whether the electronic evidence carrier complies with the relevance regulations, both must be carried out, and one is indispensable.

Electronic evidence is different from traditional evidence. It is intangible and intangible. It is electronic and digitized data and information. It is stored in a complex virtual space and must be transformed into a certain physical form before it can be used by people. Therefore, in the process of determining whether the electronic evidence complies with the relevance regulations, both checking whether the content of the electronic evidence meets the relevance requirements and determining whether the electronic evidence carrier complies with the relevance regulations must be carried out. The relevance of electronic evidence is rich in connotation, which is composed of the content relevance and carrier relevance of the evidence. Content relevance refers to whether the evidence based on objective facts and the proof object of the case are related to the content of the electronic evidence. The carrier relevance refers to the relevance of the existence of electronic evidence to the parties or other litigation participants[5]. For carrier relevance, the facts in dispute in the case must be determined in conjunction with the presentation of electronic evidence in the virtual space, and it cannot be simply determined that the parties to the case or other litigation participants are associated with the carrier of electronic evidence.

The elements of any case are specific. The elements specifically include characters, events, time, space, location and other elements. When the characters, events, time, space, location and other elements of the virtual space change, the parties in the physical space or others The relationship between the litigation participants and the characters, events, time, space, location and other elements of the virtual space will be manifested through the carrier of electronic evidence. Space is considered in isolation, and the two must be connected for judgment.

### **3.2.3. Determination of the Legality of Electronic Evidence**

The legality of evidence refers to the collection and use of evidence in accordance with the law. The legitimacy of the review shall be determined in terms of the subject of evidence collection, the source of evidence, the form of evidence, and the procedure for obtaining evidence. Before reviewing the authenticity and relevance of the evidence, the legality of the evidence must be determined first, so as to confirm that the evidence has legal effect.

As for the electronic data itself, it is impossible to determine whether it is legal or illegal. In judicial practice, only when electronic data has the function of identifying the object of proof, that is, when it becomes electronic evidence, the law will judge whether it is legal or illegal. At this time, it will check whether the evidence is legal. Specific identifications are made in terms

of sources, collection subjects, and collection procedures. For example, the law stipulates that the number of forensics personnel who collect and extract electronic evidence and the method of obtaining evidence shall be reviewed to determine whether the electronic evidence meets the regulations; whether the records, lists and other materials and witnesses are recorded during the collection of electronic evidence. The signature or seal of the person to indicate the recognition of the electronic effect; whether the equipment is used to record the process of collecting and extracting electronic evidence, whether the professional confirms the equipment access of the electronic data, etc.

Whether electronic evidence meets the regulations can be used to prove the facts of the case. However, in the specific judicial and law enforcement process, evidence that cannot be determined to be connected to the facts of the case can be adopted. Because the adoption of electronic evidence must comply with legality regulations. Compared with traditional evidence, electronic evidence is a newly emerging form of evidence, so the relevant regulations on the adoption of electronic evidence are different from traditional evidence. Although electronic data is stored in electronic equipment such as computers, the electronic data in the equipment may be destroyed. Therefore, the data stored in the computer should be printed and preserved by tangible means. In addition, criminals who master the decryption technology may be. The encrypted information is decrypted, resulting in the information being obtained by lawbreakers or being leaked or tampered with, and it is impossible to guarantee whether the information and data of the parties are safe and not tampered with. When both parties have a dispute, as long as the original data is slightly changed, the original document data may change accordingly, resulting in electronic evidence that does not comply with the relevant regulations on authenticity, and the power of proof is reduced. The evidence has flaws in validity and is rejected by the court. among.

Evidence collected through illegal means shall be excluded in accordance with legal provisions. For example, Article 27 of the Regulations on Several Issues Concerning the Collection, Extraction, and Review and Judgment of Electronic Data in Handling Criminal Cases stipulates that when evidence is flawed, it should be processed. Corrections or reasonable explanations for the flaws can be made so that the evidence can be adopted. If the validity of the evidence cannot be corrected or a reasonable explanation for the flaws cannot be made, the electronic evidence cannot be adopted. The "Civil Procedure Law" also clearly explains the rules for the exclusion of illegal evidence. The purpose of formulating the rules for exclusion of illegal evidence is to protect the legitimate rights and interests of others, ensure compliance with legal provisions, and maintain public order and good customs. Electronic data itself is intangible, fragile, and vulnerable to tampering. Criminals can easily obtain evidence illegally through electronic information systems such as computers or tamper with electronic evidence, infringe on the privacy of the parties, obstruct the trial of the case, and even undermine judicial justice. Damage to the legitimate rights and interests of the parties, therefore, the judge should carefully review the electronic evidence and exclude illegal evidence, so as to maintain judicial justice and protect the legitimate rights and interests of the parties.

The law clearly states that "in any civil litigation, electronic evidence with one of the following conditions should be excluded: (1) Electronic evidence not obtained through verification procedures; (2) Electronic evidence that has been modified or attacked after verification. Evidence; (3) Electronic evidence obtained through illegal recording, search, seizure, etc.; (4) For computer-generated electronic evidence, there is evidence that the computer system was in an abnormal state when the evidence was generated; (5) Ordinary evidence laws and regulations to exclude other circumstances; (6) For the electronic evidence stored in the computer, there is evidence that there is a substantial error in the transcription process." The law clearly states: "If an electronic report, memorandum, record or data compilation is produced in the normal course of business activities, the memorandum, report, record or data

compilation shall not be excluded on the grounds of hearsay, but If there is evidence to prove that the memorandum, report, record or data compilation is inaccurate in the way of communication, storage, or environment, it should be ruled out[6]."

### **3.2.4. Determination of the Probative Power of Electronic Evidence**

Electronic evidence indeed but notarization is more difficult. Therefore, notary agencies urgently need more detailed standards to determine the probative power of electronic evidence, and to verify whether there are problems in the production, transmission, storage, and collection of electronic evidence. The quality of appraisers needs to be improved urgently and an expert appraisal system should be introduced. Professional and technical personnel are required to deal with professional issues in the field of evidence; second, electronic evidence should be data normally generated in the information system, rather than artificial forgery and tampering, otherwise it will reduce the proving power of the evidence; third, not the parties themselves But when the other party saves the evidence, the effectiveness is the highest. In the process of storing electronic evidence on the third-party evidence storage platform, the effectiveness of the evidence is at a general level, and the party himself saves the evidence with the lowest effectiveness. The field of electronic evidence also agrees with these evidence deposit rules.

Electronic data is the application of science and technology in the evidence law. It involves a new technology. Therefore, the determination of the probative power of electronic data requires proficiency in professional technical knowledge. Therefore, when determining electronic evidence In the process of proving the power of the blockchain, the assistance of experts with relevant professional technical knowledge is needed. The testimony of the experts has a greater supplementary effect on the proving power of the blockchain evidence. The Supreme People's Court's Interpretation on the Application of the "Civil Procedure Law of the People's Republic of China" Article 122 provides relevant provisions on the professional opinions provided by experts: During the course of the case, professionals are required to provide opinions on professional issues and answer related majors. Questions and supplement the probative power of the evidence.

## **3.3. The Burden of Proof for Electronic Evidence**

### **3.3.1. Legal Regulations**

Legal regulations Article 64 of the "Civil Procedure Law of the People's Republic of China" [Prescribes the burden of proof: Generally, the parties claim that the parties provide evidence, and the parties have the obligation and responsibility to prove their claims. However, in special circumstances, a court is required Obtain evidence in a comprehensive and objective manner based on the principles of good faith and fairness, so that the legitimate rights and interests of the parties are protected. With the development of judicial practice, the adoption of evidence cannot be limited to traditional physical evidence. New electronic evidence should also be adopted as evidence in the case when it meets the standards of evidence collection. After the parties have collected the evidence, they are handed over to judicial staff for review. During the trial, both parties cross-examine the evidence. According to the Supreme People's Court's interpretation of the "Civil Procedure Law of the People's Republic of China," Article 104: Review whether electronic evidence is authentic, whether it complies with legal provisions, whether it is related to the facts of the case, and whether the evidence is probative and its The extent to which the facts of the case can be proved, and whether the evidence is admissible.

### **3.3.2. Perfect**

"The Supreme People's Court's Provisions on Several Issues Concerning the Trial of Cases by Internet Courts" Article 9: The parties shall submit electronic evidence via the Internet and transmit it to the litigation platform, or process the electronic data into an electronic form by

scanning, re-photographing, transcribing, etc., Transmit to the litigation platform for proof, and the electronic evidence has been uploaded to the litigation platform, and the parties can directly use the electronic evidence for proof.

This article specifies in detail the specific procedures for submitting electronic evidence, which saves the cost of evidence preservation, improves the efficiency of evidence collection, and ensures the authenticity and integrity of data to a certain extent, and conforms to the development of judicial practice.

Article 2 of the "Several Provisions of the Supreme People's Court on Evidence in Civil Litigation" states the basic principles that should be observed when the parties bear the burden of proof, and the parties should bear the burden of proof conscientiously and responsibly. When the parties are unable to collect evidence on their own due to objective reasons or it is difficult for them to collect evidence on their own, the court shall assist the parties in obtaining evidence in accordance with the party's application.

The people's court judges whether a party can bear the burden of proof is based on whether the party has the ability to bear the burden of proof, that is, the party's ability to produce evidence. The party's ability to produce evidence is mainly limited by the following factors. The second is whether the parties have an objective connection with the facts of the case, and the third is whether the parties have the financial ability to bear the burden of proof.

## **4. Problems Faced by Electronic Evidence in Legislation and Judicial Practice**

### **4.1. The Legislative Issues of Electronic Evidence**

The law has imperfect regulations on electronic evidence, and does not clarify the definition and validity criteria of electronic evidence. The regulations on electronic evidence are scattered and general. Most of the laws and regulations only stipulate the types of electronic evidence, and there are few detailed regulations such as the criteria for judging electronic evidence. In some cases, electronic evidence can only be applied through the legal provisions of evidence.

When determining evidence, the judge has greater discretion. Because the legal provisions on the standard of evidence determination are not sound, the judges in the case mainly determine whether the evidence should be adopted based on trial experience and relevant legal regulations, which leads to the judges' determination of whether the evidence is adopted in the same or similar cases. Inconsistent. Although some judges make comprehensive, comprehensive and detailed judgments on electronic evidence, most judges are more conservative in the determination of electronic evidence and generally do not determine the validity of the proof, which leads to the unfair and rigorous determination of the acceptance of electronic evidence in the case.

When notarizing electronic evidence, the key is whether the process of obtaining evidence complies with the relevant provisions of the law and whether it complies with the requirements of the integrity of the electronic evidence, rather than determining whether the content of the electronic evidence itself complies with the relevant provisions of authenticity. For notarization, it cannot prove whether the evidence is related to the identity of the parties concerned.

### **4.2. Problems of Electronic Evidence in Judicial Practice**

The standards of electronic evidence collection are not standardized. China's law does not specify the standards for obtaining evidence for electronic evidence. Therefore, the standards for obtaining electronic evidence are not uniform, and relevant industry technical standards have not been formulated at the national level. This has led to the lack of standardization of the forensic process of electronic evidence. In judicial practice, evidence collection is chaotic frequently, and the evidence collected may not meet the requirements of the completeness and

authenticity of the evidence, and has flaws in effectiveness. In the case, it will be considered as illegal evidence and be excluded.

It is difficult to produce electronic evidence[7]. Compared with traditional physical evidence, electronic evidence exists in a special form, and certain carriers must be used to display and exchange evidence in court trials. However, some evidence carriers are inconvenient to transport or costly to transport, which makes it impossible to show evidence, and some Electronic evidence is linked to a specific environment and depends on a specific environment to be read.

The forensics personnel have low literacy. To a certain extent, the quality of the forensics personnel is related to whether the evidence is adopted, and whether the collection of electronic evidence meets the standards of forensics has a decisive effect on the success of the case. The literacy of forensics personnel includes professional literacy and moral literacy. Professional literacy is related to the professionalism of the forensic process. Because some electronic evidence is more difficult to obtain, the forensic personnel need to have strong professionalism. For the forensic personnel with high professionalism, they can screen out the evidence related to the facts of the case among the many pieces of evidence. However, in the actual evidence collection process, because some forensics personnel are less professional, they will all be detained without screening the evidence. To a certain extent, it increases the cost of judicial evidence collection, reduces the efficiency of evidence collection, and wastes judicial resources; moral literacy refers to whether the forensic personnel can guarantee the integrity and authenticity of the original evidence, and do not damage or damage the original evidence for reasons such as monetary benefits. The forgery of evidence or the indulgence of parties who are closely related to the interests of the case destroy or tamper with the evidence. In the process of obtaining evidence, first-hand evidence is easy to be leaked and tampered with, resulting in unclear identification of the facts of the case, failure to protect the legitimate rights and interests of the parties, and the failure of judicial justice in the case.

### **4.3. Problems of Electronic Evidence in Cross-examination**

Problems of electronic evidence in Cross-examination In specific cases, some lawyers believe that as long as electronic evidence has not been notarized by a notary office, the evidence cannot be considered to be probative and the evidence cannot be adopted. Some judges believe that electronic evidence has no probative force without notarization by a notary agency and will not be accepted in court. Judicial staff have prejudice in understanding the carrier form of electronic evidence, and neglect to pay attention to the objective facts presented by electronic evidence itself.

## **5. Solutions to Problems**

### **5.1. Legislative Level**

Legislative level Improving the relevant legal provisions of electronic evidence does not require the law to specify all aspects of electronic evidence in detail. Of course, the law cannot be precise, but the identification standards of electronic evidence and the requirements of forensics personnel should be clarified. The regulations provide a legal basis for determining the probative power of evidence in practice, thereby improving the legal system of electronic evidence. At the same time, based on the specific practice of our country, learn and learn from foreign laws and regulations, improve the operability and technicality of legislation, and be forward-looking and advance with the times in the legislative process, so that the legislation has both stability and flexibility., In order to adapt to the development of contemporary judicial practice.

Through the detailed description of the legal standards for determining electronic evidence, in specific cases, the adoption of electronic evidence will be more cautious and rigorous, and to a certain extent, the acceptance of evidence will be increased, enabling judges to hear cases in accordance with the law. Reduce the arbitrariness of judges in hearing cases, thereby restricting the discretion of judges, better safeguarding the legitimate rights and interests of the parties, and making judicial trials more fair.

## 5.2. Improving Relevant Regulations for Evidence Collection

### 5.2.1. Determine a Unified Forensics Standard

Unify the evidence collection standards at the legislative level, establish unified industry standards at the practical level, regulate the collection standards from the legislative and practical levels, make the adoption of electronic evidence comply with the regulations, and enhance the availability of electronic evidence in cases from the standard.

### 5.2.2. Improve the Quality of Forensics Personnel

It is necessary to improve the professional quality of forensics personnel in terms of professional knowledge level and specific practical ability. First of all, at the knowledge level, the school should establish an electronic forensics major, increase the intensity of training for forensics talents, and improve their professional knowledge; second, in terms of practice, it is necessary to improve the ability of forensics personnel to investigate and collect evidence from participating in simple cases. Start, collect evidence, and gradually improve the level of evidence collection. In the process of collecting electronic evidence, forensics personnel should pay attention to the protection of related computers and other electronic equipment to prevent the damage of evidence, and also pay attention to the screening of key electronic data when placing electronic equipment. Protect citizens' right to privacy and other legitimate rights and interests, improve the efficiency of judicial evidence collection, reduce the cost of evidence collection, thereby saving judicial resources; finally, for some cases that are more difficult to obtain evidence, professional forensic experts are invited to participate and give guidance so as to enable the forensics personnel It can accurately collect evidence related to the facts of the case, reduce the cost of evidence collection, and improve the efficiency of evidence collection. Improve the ethics of the forensics personnel, earnestly perform their duties, and abide by the rules for obtaining evidence. After completing the collection of electronic evidence, strengthen the protection of electronic evidence, and prohibit people who have nothing to do with the case from viewing it to prevent them from damaging and tampering with the evidence. Evidence collectors themselves shall not use the convenience of obtaining evidence to destroy or tamper with evidence related to the case, or condone persons who have an interest in the case to forge or damage the evidence, and penalize forensic personnel's violations by formulating corresponding severe punishment mechanisms to reduce violations of the law, Occurrence of violations.

## 6. Conclusion

After the revision of the three major litigation laws, electronic data has become one of the types of statutory evidence. On the one hand, it not only conforms to the development requirements of judicial practice, but also reflects the progress of the rule of law. Electronic data can be adopted as evidence when it meets the requirements for authenticity, legality, relevance, etc., and it proves the facts of the case. Due to its intangibility and fragility, and related legislation is not sound, it is inevitable to encounter difficult problems in judicial practice. This article first discusses the case of electronic data, and then the three characteristics of evidence, the power of proof, and the burden of proof of evidence, etc. Discuss, and put forward corresponding suggestions for improvement of problems found at the legislative level and judicial practice

level to promote the improvement of the legal system of evidence law, thereby promoting the improvement of contemporary electronic evidence judicial practice.

## Acknowledgments

In just a few months, time flies. Once I was an ordinary college student, but now I have finished writing my graduation thesis, and I am ready to participate in the work. I feel a little nervous and expectant, and I am more thankful.

Thank you to everyone who helped me in the process of writing my paper, thank you teachers, classmates, and parents. Every long night of essays has your company and patient guidance. I don't feel too much. I finished my thesis with a lot of confusion and frustration. Thank you for your support and dedication.

I was stupid by nature, but I also firmly believed that diligence could make up for the clumsiness. After I decided on the topic, I began to collect information. The process was bumpy, but the result was full of accomplishments. I can get timely answers from the teacher for every confusion in academics. I can also get valuable reference experience from my classmates when encountering bottlenecks in the process of collating documents. They are the people I trust most and they also help me. The biggest person.

The writing of the thesis is boring and boring. I never wavered, insisting on writing every word of this thesis by myself, and with my sweat and hard work, I proved that I was indeed capable and worthy of the diploma and degree that I was about to have. I sincerely hope that every colleague can be as self-confident as I am and will not make detours.

I am also growing up while writing my thesis. Once upon a time, I was just an academic novice who didn't even know how to list the outline.

Looking at the revised documents one after another on the computer, I was deeply moved. Bao Jianfeng has been sharpened, and the fragrance of plum blossoms has come from the bitter cold. I firmly believe that I, who have withstood the test of my graduation thesis, will become more and more courageous in my study, work and life in the future. Thank you for your care and help to me. Thank you again!

## References

- [1] J. Ni: The authenticity of electronic evidence in civil litigation, Journal of Beijing University of Aeronautics and Astronautics (Social Science Edition), Vol. 29 (2016) No.02, p.55-63.
- [2] M.Y. Wang: The formation and authenticity of electronic evidence, Law Science, (2017) No.06, p.183-192.
- [3] X. Ding: Research on the Attestation of Blockchain Deposit Evidence(MS., Huaqiao University, China, 2019), p.14-15.
- [4] J.Y. Li, Z.S. Li: Discussion on the authenticity of electronic data based on blockchain storage evidence, Software, Vol. 39 (2018) No.6, p.109-112.
- [5] P.X. Liu: The relevance of electronic evidence, Chinese prosecutors, (2017) No.09, p.178-180.
- [6] L.L. Lin: Research on the Evidence Effect of Electronic Data in Civil Litigation(MS., Yantai University, China, 2015), p.16.
- [7] Z.Y. Song: Research on the authenticity of electronic evidence in civil litigation,(MS., Northwest Normal University, China, 2020), p.21-27.
- [8] S.L. Ma: A doctrinal analysis of the rules of illegal electronic data exclusion,(MS., Anhui University, China, 2020), p.10-15.
- [9] X.X. Luo: On the exclusion of illegal electronic data(MS., Chongqing University of Posts and Telecommunications, China, 2019), p.10-25.

- [10] S.G. Zhan, C. Wang: From legal electronic data to electronic data legal, Journal of Hubei University (Philosophy and Social Sciences Edition), Vol. 48 (2021) No.02, p.110-119.
- [11] M. Hu: Analysis of the effectiveness of block chain electronic evidence and standardization path, Evidence Science, Vol.29(2021) No.01, p.31-40.
- [12] L. Wang: Research on the Application of Electronic Evidence in Civil Litigation in China (MS.,Central China Normal University, China,2020), p22-25.
- [13] L. Zhang: Research on the authentication rules of electronic data in civil litigation(MS., East China University of Political Science and Law, China,2016), p30-35.
- [14] S.J. Chen, C.Q. Zhao, L.L Huang, J.Yuan and M.Z. Liu: Study and implementation on the application of blockchain in electronic evidence generation,Forensic Science International: Digital Investigation, Vol. 35 (2020), p.5-10.
- [15] Strategic Leadership in Digital Evidence(Elsevier Inc,2020).