Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Combinatorial Press

The Rise of Online Litigation Based on Time Proof Consensus Algorithms Challenges the Traditional Trial Model in the Framework of the Code of Civil Procedure

Qian Wang[1,] ✉

[1] *Law School of Xiangtan University, Xiangtan, Hunan, 411105, China*

ABSTRACT

The integration of modern information technology and civil litigation promotes the electronic civil litigation, online litigation as a kind of litigation behavior, promoting the development of traditional trial mode. This paper starts from analyzing the relationship and conflict between civil e-litigation and traditional civil litigation, and organizes the relationship between online trial mode and traditional court trial, and the relationship between civil online trial mode and traditional trial mode respectively. Based on the influencing factors of civil trial, the time proof consensus algorithm and data security transmission algorithm are respectively proposed to combine the network nature of online litigation and blockchain storage data information to optimize the online litigation electronic evidence storage. Summarizing the litigation efficiency of online trial and traditional trial under different control variables, from the point of view of the complexity of the case, the litigation efficiency of online trial mode for more complex cases is significantly higher than that of traditional trial mode. For non-complex cases, the efficiency increases but the difference is not significant. The online litigation mode is a part of the civil online trial mode and serves the traditional civil trial mode.

Keywords: blockchain technology, consensus algorithm, data security transmission, online litigation, traditional trial mode

1. Introduction

Online civil litigation is an overall concept, while e-litigation and online civil litigation focus more on the use of technical means and online methods. In a broad sense, online litigation includes online filing, online responding to lawsuits, online mediation, online trial, online execution, etc. [1-3]. Online litigation can be understood from the following aspects. First, as far as the subject of litigation is concerned, the participating subjects of online litigation include the people's court, the parties and

✉ Corresponding author.
E-mail address: 13683971193@163.com (Q. Wang).
Received 05 March 2024; Revised 25 May 2024; Accepted 05 December 2024; Published Online 15 April 2025.
DOI: 10.61091/jcmcc127a-473

other relevant litigation participants, and in criminal cases, the people's procuratorate is also included, which is consistent with the scope of the subject in traditional litigation [4-6]. Secondly, as far as the litigation mode is concerned, online litigation is a litigation activity conducted through the network. Further, as far as the platform carrier is concerned, online litigation activities mainly rely on the electronic litigation platform. At present, some common electronic litigation platform, including the familiar "China mobile micro court", as well as the court's own online litigation platform [7-8]. Finally, as far as the form of expression is concerned, whether it is "full process online" or "part of the litigation process online", all belong to the form of online litigation. For example, some cases may be filed offline, but in the mediation process online [9-10]. In some cases, the parties may actively choose the way of online trial due to geographic location and other reasons. Comprehensively speaking, online litigation has rich connotation and diverse forms, which can be flexibly applied according to specific cases [11-12].

Admittedly, the vigorous development of online litigation for the civil trial field has brought a lot of new experience and new results, but new situations and new problems also come. Online litigation is certainly in the alleviation of "litigation explosion", reduce the threshold of access to judicial resources, resolve the epidemic risk and other aspects of the advantages are significant, but it is obvious that the online litigation system in the process of operation is also facing a lot of challenges, such as the impact of the traditional litigation culture of direct speech, judicial openness, reduce the sense of courtroom rituals, the construction of the existing platforms. It is difficult to meet the litigation subject's vigorous judicial demand, etc. [13-16]. Not only that, looking around the world, the courts of various countries are still mainly on-site hearings, supplemented by online trials, and even the United States of America, the implementation of online justice is not satisfactory, however, China is able to achieve leapfrog development in such a world situation, the courage to explore the tide of Internet justice [17-18].

This paper clarifies the relationship between online litigation, civil online litigation, and traditional civil litigation, and discusses the relationship and conflict between civil online litigation and traditional civil litigation. For the online trial mode and traditional trial, respectively from the trial mode and trial mode two categories to explore. Analyze the key technology of civil online trial, and propose the electronic evidence storage model based on blockchain for the problem of online litigation data and information storage. The performance of time synchronization consensus algorithm is examined, as well as the implementability of the improved AES algorithm. Compare and analyze the operational efficiency of online litigation and traditional litigation by organizing online trial model cases.

2. Online civil proceedings versus traditional authorization

2.1. Online litigation

Online litigation is a kind of litigation trial mode that utilizes computer network technology to realize the whole litigation process in the fastest and most effective way [19]. Court staff on the online litigation platform parties to submit materials and information for centralized and batch processing, and timely feedback to the parties, the cost of communication between the two is significantly reduced, the communication becomes smooth and efficient. In addition, online litigation to promote the development of "paperless justice" process, the popularization of electronic files, can reduce the number of paper files formed during the trial of cases, saving paper resources. The online litigation trial mode can intelligently and efficiently solve the problem of long and time-consuming traditional litigation, saving litigation time and economic costs, effectively alleviating the burden of litigation, and improving the efficiency of judges in handling cases.

2.2. Civil online proceedings

From the viewpoint of the nature of civil online litigation, civil online litigation is a litigation activity relying on the Internet. The Internet is only the platform on which civil litigation activities are based,

and the core is still civil litigation. Civil litigation refers to the equal subjects because of personal or property relationship dispute, based on the legal relationship to the people's court with jurisdiction. The court, with the participation of all parties, conducts a trial and makes a decision on the dispute in accordance with the law. Traditional civil litigation requires the judge, litigation participants in a specific location for direct communication, so the traditional civil litigation behavior is mainly used offline tools, usually oral or paper documents for communication. With the arrival of the digital information age, the traditional form of litigation activities continue to highlight the defects, to digital information technology as the carrier of civil online litigation came into being.

2.3. Civil e-litigation versus traditional civil litigation

2.3.1. Relationship:

1) Prosecution and filing. In traditional civil litigation, the parties or their authorized representatives are required to go to the competent court to submit a complaint or file an oral complaint during the court's working hours. After the filing court accepts the materials, it usually issues a notice of acceptance of the case and a notice of payment of fees within seven days. If the materials are lacking, the parties shall be reminded on the spot to complete the materials.

In e-litigation, the parties can log on to the court's filing system at any time and submit the pleadings and related documents and materials without being restricted by working days. The court receives the electronic complaint and examines it, deciding whether or not to accept it. If the materials submitted by the parties are missing and do not yet meet the conditions for filing a case, the court can directly reply to the parties on the platform, informing them of the additional litigation materials they need in one go. After completing the registration of the case, the court can send the plaintiff's complaint to the defendant, and the defendant can also log on the electronic platform to submit a defense and related evidence materials for litigation activities.

2) Witness Testimony. In civil litigation, witness testimony is an important guarantee to restore the facts of the case and promote the formation of a correct decision by the trial judge, and witness testimony is also an important element to safeguard the litigation rights and interests of the parties.

In traditional civil litigation, witnesses generally need to testify in court, stating what they have seen and heard. If there are indeed unable to appear in court, you can submit written testimony.

In the Internet era, if the witness is unable to testify in court due to subjective and objective reasons, he or she can use Internet communication technology to connect with the court and the parties in the form of remote video. In remote testimony, the witness can communicate normally with the trial personnel as well as the parties, accept the other party's inquiry, and state the facts more accurately.

3) Courtroom Activities. In traditional offline civil litigation, the parties need to go to the court under appeal to appear in court on the day of the trial. In the fixed trial space to complete the evidence, court investigation and other trial links.

In civil e-litigation, trial activities can be carried out in the form of cloud video conferencing. Parties, witnesses, experts, etc. do not need to go to the court of jurisdiction to accept the security check, enter the courtroom to wait for the trial. They only need to log into the online trial platform to enter the live broadcast room in the place equipped with qualified audio-visual communication equipment, and conduct online trial by video + voice with the judge, the other party, witnesses and other people connected to the trial.

4) Mode of Service. In traditional civil litigation, the court generally delivers paper-based documents and materials to the parties and their attorneys in person or by mail.

In electronic litigation, the parties have the right to choose whether to use electronic service and

which means to complete the service.

2.3.2. Conflict between the two. The hybrid operation of civil electronic litigation and traditional civil litigation is an inevitable trend in the development of electronic civil litigation. The implementation of electronic litigation is developed on the basis of traditional litigation procedures. In the context of the integration of the old and new systems, the traditional litigation idea still has strong support, the electronic litigation reflects the characteristics of "service-oriented justice", in line with the trend of the construction of e-court.

In the wave of big data and internet era, the principle of civil litigation in the face of the collision of electronic litigation, in some aspects appear to be insufficient.

First, weakened the application of direct speech basis.

Civil e-litigation, screen-to-screen online communication mode of litigation, breaking the principle of direct speech requires the courtroom personnel to participate in the trial site restrictions.

Secondly, it weakens the effect of the application of the principle of equality.

Although civil electronic litigation increased the transparency and openness of the litigation, but the gap between the two parties litigation means application, it is impossible to ensure that the two parties in the litigation to maintain equal confrontation status, will also weaken the principle of equality in the litigation.

Third, it has a certain impact on the public trial system.

Fourth, it weakens the ceremonial nature of the courtroom.

The court from the external environment and the inner courtroom norms are revealed its unique atmosphere and sacred sense of majesty. In the civil electronic litigation, the judge and the parties to the communication are separated from the screen, through the audio-visual transmission technology to complete the online communication, the impact of the traditional civil litigation court structure.

2.4. Online versus traditional trial models

2.4.1. Relationship between online trial models and traditional court trials. The online trial model, a new concept and theory, has attracted widespread attention in the theoretical, academic and practical circles. Some scholars believe that the online trial mode of trial concept, trial mode, trial thinking and the traditional court trial is completely different. It subverted the traditional face-to-face courtroom trial mode, transformed into the entire trial process in the virtual cyberspace, through the virtual cyberspace to achieve synchronous trial of different geographical space. They believe that this trial mode should be attributed to a new trial mode, a new dispute resolution mechanism in parallel with the traditional court trial. However, this paper believes that the online trial mode is not a new mode juxtaposed to the traditional court trial, but an extension and expansion of the traditional court trial mode in the context of the Internet.

First of all, a stable system and a unified decree is essential for a country to make continuous progress and development, to realize judicial justice and promote social harmony.

The application of uniform procedures is more conducive to safeguarding judicial authority and maintaining judicial justice. Online trial is a choice in the context of the new environment, but it cannot leave behind the basis of the traditional court trial.

Secondly, although the online trial in improving litigation efficiency, reduce litigation costs, promote judicial transparency, judicial openness has traditional court incomparable advantages, but its identity in the party identification, case mediation, proof, evidence and other aspects of the advantages are not stronger than the traditional court trial.

Finally, the online trial mode is not a new procedure completely different from the traditional trial, but rather a new attempt to resolve disputes in the traditional trial in the context of Internet thinking and the development of scientific and technological innovation.

2.4.2. Relationship between online and traditional civil trial methods. First of all, the unity of the law is the primary premise for the guarantee of judicial authority, and procedural law should follow this premise, and the mode of trial, as the content of the trial system, is no exception. Therefore, this paper believes that a country's judicial authority to guarantee the logical premise should be the unity of the trial mode, only the application of a unified trial mode, will not be applied to different people different trial mode, in order to ensure procedural justice. Therefore, the traditional trial mode formed under the rules of civil procedure is the only trial mode, it is impossible to appear independent of the traditional trial mode of another completely new trial mode.

Secondly, the online trial mode although there is a difference from the traditional trial mode. For example, because of the two characteristics are very different, so the online trial mode in improving the efficiency of litigation, litigation cost savings and other aspects to be significantly better than the traditional trial mode. While the traditional way of trial in the court to verify the identity of the parties, court investigation, court mediation and other aspects but very convenient. It can be said that the two in the realization of the litigation function, each has its own advantages. But the online trial is still relying on the traditional rules of civil litigation, although in the process of litigation into a more scientific and technological factors, making the trial more convenient and efficient, but it will still comply with the trial procedures in the Civil Procedure Law, which in the overall construction of the traditional way of trial is not essentially different, and even in some parts of the litigation function of the online trial mode of realization also need to resort to traditional trial mode to realize. In some aspects, the realization of the litigation function of online trial mode also needs to rely on the traditional trial mode to realize.

Therefore, this paper that the online trial is only an extension of the traditional way of trial and supplement, not independent of the traditional way of trial is another new way of trial.

3. Civil trials from a web-enabled perspective

3.1. Factors affecting the efficiency of civil trials

1) Party factors. In civil trial activities, the parties' behavior is one of the important factors affecting the efficiency of civil trial. In judicial practice, the parties' behavioral style, especially the defendant's behavioral style, can cause serious litigation delay phenomenon.

2) Judge factor. In the process of civil trial, most of the judges take the lead in deciding whether or not to use network technology in the trial. The parties or litigation agents apply for the use of network technology in the trial, but also still need to be agreed by the presiding judge can be used. The judge's decision-making power over the use of network technology is too high, which will affect the efficiency of civil trials.

3) Litigation Procedure Factors. Civil litigation procedures are the norms and processes for solving civil disputes.

To serve as an example, as one of the basic procedures of civil litigation, timely and effective delivery of legal documents in order to play the due value of legal documents, litigation participants can more accurately know the content of the document, so that they can exercise their litigation rights on time. If there is a delay in the service of process, the trial of the case will not proceed normally.

3.2. Online litigation data information storage

The use of blockchain to store data and information coincides with the networked nature of online litigation. On the one hand, with the help of time stamps and hash encryption, blockchain puts a unique and certain “digital signature” on the “erratic” electronic data, shaping the process of a new regulatory environment. In this process, once the electronic data is entered into the chain, it can prevent the

electronic data from being tampered with after it is entered into the chain, safeguard the authenticity and homogeneity of the electronic data, and realize the authenticity of the certified electronic data.

On the other hand, using blockchain to store data information on distributed nodes, even if part of the nodes are attacked by hackers or part of the data is destroyed, it will not affect the integrity and authenticity of the blockchain data information, so as to guarantee the storage security. Promoting the mutual integration of blockchain technology and law is the trend and advantage of future judicial development. It is therefore necessary to increase the application and development of blockchain technology in online litigation.

3.2.1. Design of Time Proof Consensus Algorithm. The innovations of the proof-of-time consensus algorithm designed in this paper are:

1) Enabling the consensus algorithm to avoid centralization while enabling the algorithm's performance to not degrade significantly with large-scale node participation [20-21].

2) Enabling the consensus algorithm to support the sequencing of transactions while possessing the potential to develop instantaneous applications.

Meanwhile, a consensus algorithm based on proof of time is designed using already synchronized time. Therefore, this consensus algorithm is divided into two parts. One is to synchronize the node time for all nodes within the network. The second is to use the synchronized time to complete the consensus.

The whole network node time synchronization process is specifically:

Step1: The node that wants to be the initiator of the network-wide time synchronization performs the calculation of VRF once locally. And then initiates a network-wide time synchronization. When other nodes receive multiple messages initiating the network-wide synchronization, only the request from the node with the smallest value of the VRF calculation result is responded to. A node such as $Nodei$ is finally identified as the initiator of this time synchronization.

Step2: Segment other nodes based on the routing table K-bucket (range of distance from other nodes to node i) of $Nodei$ and the total number of segments is Ni.

Step3: $Nodei$ randomly selects one node from each slice as the leader node of the slice (assuming the leader node of slice 1 is $No\ de1$), $Nodei$ sends a message to the leader node of each slice to start time synchronization.

Step4: A certain number of nodes in each slice are elected to participate in time synchronization using the improved VRF election method.

Step5: $Node1$ Verify that the received VRF_Resultn is not faked, and then start the PBFT time consensus with the time tolerance range determination as shown below:

$$|curTimen - curTime1| \le T_b \tag{1}$$

where Tb is the tolerance time specified by the system. If the curTime error between $Node1$ and the other elected nodes $Noden$ in the slice is within Tb, the $Noden$ time is considered reasonable and can be accepted as synchronized system time. If the number of nodes with unreasonable time received by the current packet exceeds 1/3 of the number of elected nodes in the slice. The time synchronization fails for that slice and a time synchronization failure message is returned $Nodei$. If the synchronization succeeds, it is calculated using the formula for $Time1$. The synchronization result $Time1$ is then broadcast to the other nodes in the slice as the time step result of the slice. Then return $Nodei$ a message of successful synchronization and the time after synchronization $Time1$, where N1 is the number of elected nodes in slice 1. In this way, even if the time synchronization of the nodes in the whole network is not successfully completed, the nodes in the current slice have carried out a small-scale synchronization:

$$Time_1 = \frac{1}{N1}\sum_{1}^{N2} curTime_n, n = (2,3,4,5.....) \tag{2}$$

Step6: If $Nodei$ receives more than $Ni/3$ synchronization failure messages, this synchronization fails. Return the synchronization failure message and re-initiate a network-wide time synchronization. If the number of successful synchronization messages received exceeds $2/3*(Ni-1)+1$, the synchronization is successful. Calculate time $Time_i$ using the formula, send a synchronization success message and broadcast $Time_i$ to all nodes in the whole network as the system time after synchronization. I.e:

$$Time_i = \frac{1}{Ni}\sum_{1}^{Ni} Time_n, n = (1,2,3,4.....) \tag{3}$$

Step7: Since most of the nodes in the network are in the state of unsynchronized time at the beginning, there is a high probability that the synchronization will fail. However, the time of the synchronized nodes in the slices that are successfully synchronized will be retained. This means that even if the network-wide synchronization fails, the number of nodes in each slice of the network that have synchronized the time of the nodes within the slice will increase. The time of the nodes in the whole network converges towards the direction of successful synchronization of the time of the nodes in the whole network, and at the same time the speed of synchronization becomes faster as the number of nodes in the whole network completing the synchronization increases.

3.2.2. Algorithms for secure data transfer. DES data encryption algorithm is a symmetric packet cipher algorithm. Advanced Data Encryption Standard AES is a symmetric packet cipher algorithm. Unlike the DES algorithm, its encryption key is no longer a single fixed. The AES algorithm has a great improvement in security.

1) AES data encryption algorithm flow. Step1: Byte Replacement

In the AES encryption round function is the first byte replacement, byte replacement, also known as S-box replacement, is a nonlinear transformation process.

Let the elements before a certain mapping be:

$$\alpha = (a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0) \tag{4}$$

Its high four bits are set to the value x and its low four bits are set to the value y. If α is mapped to its multiplicative inverse in the finite domain $GF(2^8)$, then there must exist an element $\beta \in GF(2^8)$. Utilizing the Euclidean Extension Algorithm (EEA), such that:

$$\alpha \cdot \beta = \beta\alpha = 1 mod p(x) \tag{5}$$

where $p(x) = (x^8 + x^4 + x + x + 1)$. Element β is the result of the multiplicative inverse mapping of α, denoted $\beta = (b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0)$, and the inverse mapping has initially changed element α. Note that the multiplicative inverse of 0 remains 0. The second and third steps of byte substitution are then carried out by the affine mapping and addition operations, and the transformation formulas are as follows:

$$b_i = a_i \oplus a_{(i+4)\bmod} \oplus a_{(i+5)\bmod} \oplus a_{(i+6)\bmod 8} \oplus a_{(i+7)\bmod 8} \oplus c_i, i = 0,1,2,\cdots,7 \tag{6}$$

After the inverse elemental mapping and affine mapping, the elemental data of its original finite domain is greatly altered, making the elemental bytes before and after replacement become irregular, and its degree of nonlinearity is improved, effectively resisting unknown attacks. The byte replacement mapping process can be expressed by the following mathematical matrix:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{7}$$

Step2: row shift transformation

Step3: Column Mixed Transform

Column Mixed Transform is a linear transform, after the above transformations, you need to perform the Column Mixed Transform operation to calculate the byte-level multiplication of the elements on each column.

In the whole column mixed transform process, it is worth noting that the multiplication and addition in the column mixed transform are performed in the finite domain $GF(2^8)$, which has a strong diffusion transform capability and is especially important in the AES algorithm. However, there is no need to perform the column mixed transform again in the last round of computation of data encryption. Because there is basically no effect on the security of the whole encryption algorithm, and it can reduce the difficulty of the implementation of the algorithm and improve the computational efficiency. That is:

$$C = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \tag{8}$$

$$c(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\} \tag{9}$$

The polynomial coefficients 01, 02 and 03 in Eq. can be expressed as polynomials 1, x and $x+1$ in the finite field $GF(2^8)$, and by setting each column of the state matrix S to $s(x)$, then the whole column mixing transformation can be expressed by the following equation. i.e:

$$s'(x) = (s(x) \cdot c(x)) mod(x^4 + 1) \tag{10}$$

Expressed by multiplying a matrix by a matrix, it can be shown in the following equation, where N_b is the number of matrix columns:

$$\begin{bmatrix} S_{0,c'} \\ S_{1,c'} \\ S_{2,c'} \\ S_{3,c'} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}, 0 \le c \le N_b \tag{11}$$

Step4: Wheel Key Addition

The last step of the wheel function transformation is the wheel key addition operation. The wheel key addition operation can be expressed by the following equation:

$$\left[s'_{0,c}, s'_{1,c}, s'_{2,c}, s'_{3,c} \right] = \left[s_{0,c}, s_{1,c}, s_{2,c}, s_{3,c} \right] \oplus w_{i+1} \tag{12}$$

The state matrix S after column mixing is used to do the different-or operation with the subkey of

each round, assuming that the subkey of round l is $W_l = (w_{l+1}, w_{l+2}, w_{l+3}, w_{l+4})$. AES needs to carry out a certain number of rounds of iterative operations, and complete the whole AES algorithm process by utilizing the subkey obtained from the key expansion algorithm.

2) AES data decryption algorithm flow. AES data decryption algorithm iteration rounds and key expansion algorithm are the same as its data encryption algorithm, only the order of the wheel transformation operation has changed.

Let the plaintext be p, the encrypted ciphertext be c, the byte substitution operation be S, the column mixing operation be M, the column mixing fixed matrix be C, the row shifting operation be R, and the state matrix after row shifting be S'. The wheel key addition operation be Ai where $i \in (0...Nr)$, the encryption wheel transformation be T_i where $i \in (0...Nr)$, and $E()$ be the data encryption function. Then its wheel transformation process can be expressed by Eq. (13) and its encryption process by Eq. (14). That is:

$$\begin{cases} T_0 = A_0 \\ T_i = A_i MRS \\ T_{N_r} = A_{N_r} \end{cases} \tag{13}$$

$$c = E(p) = T_{N_r} \cdot T_{N_{r-1}} \cdots T_1 \cdot T_0(p) \tag{14}$$

Then in the corresponding decryption process, you can set the decryption function $D()$, the inverse byte transformation operation $S-1$, the inverse row transformation as R^{-1}, the inverse column mixing transformation as M^{-1}, the inverse matrix of the fixed matrix C as C^{-1}, and the decryption round transformation T^{-1}.

The inverse byte substitution process can be expressed in the following equation, where $i = 1, 2, 3, \ldots, 7$. That is:

$$b_i = a_{(i+2)\bmod 8} \oplus a_{(i+5)\bmod 8} \oplus a_{(i+7)\bmod 8} \oplus d \tag{15}$$

The fixed value d is represented in binary as {000000101} in order to facilitate the byte substitution mapping process to be expressed in a mathematical matrix formula see Equation (16):

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{16}$$

The inverse column mixing transformation M^{-1} is computed for a state matrix of S' completed column-by-column, where C^{-1} is shown in Eq. (17) and expressed as a polynomial as shown in Eq. (18):

$$C^{-1} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}^{-1} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \tag{17}$$

$$C^{-1}(x)=\{0B\}x^3+\{0D\}x^2+\{09\}x+\{0E\} \tag{18}$$

The polynomial expression for the inverse column transformation operation is obtained from Eq. as shown in Eq. (19) and the matrix multiplication expression as shown in Eq. (20), where $c\in(0,\ldots,N_r),N_r$ is the number of columns of the state matrix. That is:

$$s(x)=(s'(x)\cdot c^{-1}(x))mod(x^4+1) \tag{19}$$

$$\begin{bmatrix}S_{0,c}\\S_{1,c}\\S_{2,c}\\S_{3,c}\end{bmatrix}=\begin{bmatrix}0E & 0B & 0D & 09\\09 & 0E & 0B & 0D\\0D & 09 & 0E & 0B\\0B & 0D & 09 & 0E\end{bmatrix}\begin{bmatrix}S'_{0,c}\\S'_{1,c}\\S'_{2,c}\\S'_{3,c}\end{bmatrix} \tag{20}$$

The specific operation procedure for a 4-byte element of a column in state matrix S' is shown in Equation (21):

$$\begin{cases}(s_{0,c}=\left(\{0e\}\cdot s'_{0,c}\right)\oplus\left(\{0b\}\cdot s'_{1,c}\right)\oplus\left(\{0d\}\cdot s'_{2,c}\right)\oplus\left(\{09\}\cdot s'_{3,c}\right)\\ s_{1,c}=\left(\{09\}\cdot s'_{0,c}\right)\oplus\left(\{0e\}\cdot s'_{1,c}\right)\oplus\left(\{0b\}\cdot s'_{2,c}\right)\oplus\left(\{0d\}\cdot s'_{3,c}\right)\\ s_{2,c}=\left(\{0d\}\cdot s'_{0,c}\right)\oplus\left(\{09\}\cdot s'_{1,c}\right)\oplus\left(\{0e\}\cdot s'_{2,c}\right)\oplus\left(\{0b\}\cdot s'_{3,c}\right)\\ s_{3,c}=\left(\{0b\}\cdot s'_{0,c}\right)\oplus\left(\{0d\}\cdot s'_{1,c}\right)\oplus\left(\{09\}\cdot s'_{2,c}\right)\oplus\left(\{0e\}\cdot s'_{3,c}\right)\end{cases} \tag{21}$$

In summary it makes the order of wheel function calculation of 10 rounds consistent with the encryption process, which reduces the difficulty of AES algorithm implementation and completes the decryption.

3) Improvement of AES algorithm. There are 2 main safety hazard problems with conventional S-boxes. The first problem is that the ATP is too small, and the second problem is that the IOP has short cycles. And these two problems are caused by with the AES algorithm does not select the appropriate affine transformation pair (u,v).

The new S-box construction is mainly done by the following steps:

Perform the multiplicative inverse operation in the finite domain $GF\left(2^8\right)$ and set input $w\in GF\left(2^8\right)$ to find $v\in GF\left(2^8\right)$ satisfying the following equation:

$$w\cdot v=1mod(x^8+x^4+x^3+x+1) \tag{22}$$

The resulting v is the multiplicative inverse of w.

Let $x=v$, then the affine transformation is used to perform affine and finite domain $GF\left(2^8\right)$ addition operations on (1C,DA), which is expressed as shown in the following equation:

$$y=La\cdot x+'DA'=La^{-1}=\begin{bmatrix}1&1&0&1&0&1&1&0\\0&1&1&0&1&0&1&1\\1&0&1&1&0&1&0&1\\1&1&0&1&1&0&1&1\\0&1&1&0&1&1&0&1\\1&0&1&1&0&1&1&0\\0&1&0&1&1&0&1&1\\1&0&1&0&1&1&0&1\end{bmatrix}\begin{bmatrix}x_7\\x_6\\x_5\\x_4\\x_3\\x_2\\x_1\\x_0\end{bmatrix}+\begin{bmatrix}1\\1\\0\\1\\1\\0\\1\\0\end{bmatrix} \tag{23}$$

The final value of the improved S-box, La^{-1} is obtained as shown in Eq. (24):

$$La^{-1} = \begin{bmatrix} 1\,1\,0\,1\,0\,1\,1\,0 \\ 0\,1\,1\,0\,1\,0\,1\,1 \\ 1\;0\,1\,1\,0\,1\,0\,1 \\ 1\,1\,0\,1\,1\;0\,1\,1 \\ 0\,1\,1\,0\,1\,1\,0\,1 \\ 1\,0\,1\,1\,0\,1\,1\,0 \\ 0\,1\,0\,1\,1\,0\,1\,1 \\ 1\,0\,1\,0\,1\,1\,0\,1 \end{bmatrix} \tag{24}$$

4. Blockchain-based optimization of the efficiency of electronic evidence storage

4.1. Time synchronization performance simulation analysis

Sync message sending period, i.e., the time interval between master and slave nodes to complete one synchronization. In this paper, different Sync message sending periods are configured to conduct simulation experiments to analyze the synchronization deviation under different synchronization periods. The sending period is set to 3s, 2s, 1s, 0.5s, 0.25s, 0.125s, 0.0625s, respectively, and the deviation changes under different Sync message sending periods are shown in Fig. 1. When the time interval of Sync period is (0.0625s, 1s), the variance is the smallest at this time, and the deviation is stable within 20 μs . In the interval (0.0625s, 3s), the larger the synchronization period, the larger the deviation. However, the synchronization period is not the smaller the better, the synchronization period is too small, resulting in too much network traffic, the synchronization deviation increases. Therefore, too large or too small synchronization period will make the deviation increase. In this paper, we choose 0.0625s as the optimal Sync message sending period.

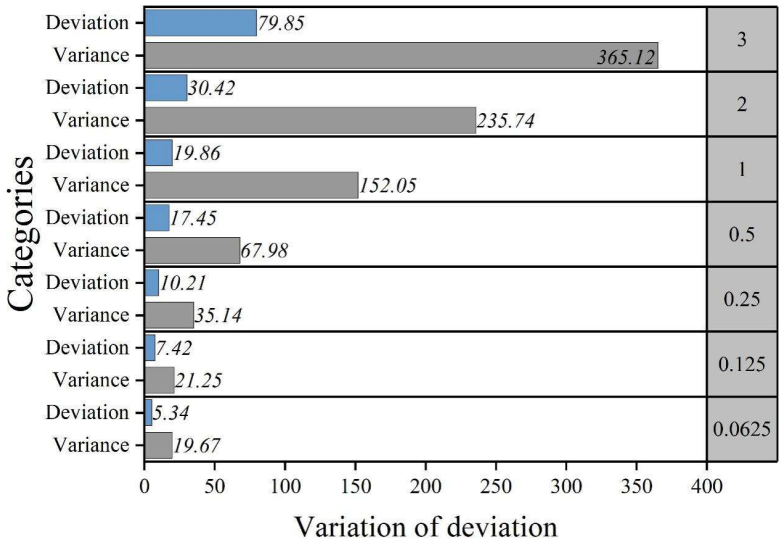


Fig. 1. Variation in the deviation of the different sync message

4.2. MATLAB implementation of improved AES algorithm

In this paper, an improvement scheme is proposed for the AES algorithm, and it is proved that the proposed improvement scheme enhances the security of the AES algorithm, then it is necessary to continue to verify whether the improvement scheme affects the encryption and decryption performance of the AES algorithm, and whether the functions of each part of the components are

correct.

The experimental platform and operating environment are as follows:

CPU: Intel(R)Core(TM)i7-4200H 2.80GHz 2.80GHz

Memory: 8GB

Hard disk: Intel SSD 1TB

OS: Windows 8.1 Pro 64-bit

Experimental platform: Matlab R2023b

Matlab language is chosen to implement the AES algorithm because Matlab programming is efficient and simple, and the code written in Matlab language is much shorter than C/C++ for the same function. And with efficient and convenient matrix and array operations, the AES algorithm using the state matrix is very practical to deal with, comes with a lot of modules and functions can be reasonably used to achieve data fitting and visualization and other functions.

The test in this section is mainly to verify whether the ciphertext output by the encryption algorithm is correct after inputting the plaintext, as well as to test whether the plaintext output by the decryption algorithm is correct when inputting the ciphertext.

The improved AES algorithm proposed in this paper is investigated from two parts, the S-box and the key extension, and the improvement of each part is relatively independent, which is attributed to the modular design of the AES algorithm, and the changes to each module will not affect the correct operation of other modules. In order to compare more intuitively the effects of the improvements in the S-box and key expansion on the encryption and decryption of the whole algorithm, five test methods are designed.

1) Using the new S-box for encryption and decryption and keeping the key extension following the design of the AES algorithm.

2) Using the key extension algorithm of the improved scheme I and keeping the S-box along the design of the AES algorithm.

3) Adopting the key expansion algorithm of the improved scheme II, and keeping the S-box following the design of AES algorithm.

4) Adopting the new S-box and combining it with the improved key expansion algorithm of Scheme I, and adopting the new S-box in the composite function that generates the round key.

5) Adopting the new S-box and combining the key expansion algorithm with the improved scheme II, the new S-box is also used in the composite function for generating the round key.

The plaintext and initial key are kept the same as in the AES-128 test standard, and each test method encrypts/decrypts the plaintext/ciphertext five times respectively. Then the average value is taken to ensure the reliability and accuracy of the data. The running time of these five test methods is counted and finally compared with the test results of AES-128 algorithm.

The comparison of encryption time of AES-128 algorithm with different test methods is shown in Figure 2. The encryption time of AES-128 algorithm for five tests is always maintained at 0.43~0.44s, and the average encryption time is 0.4411 s. The average value of five encryptions of test method (4) is 0.05281s, which is higher than that of AES-128 algorithm by 0.0087s.

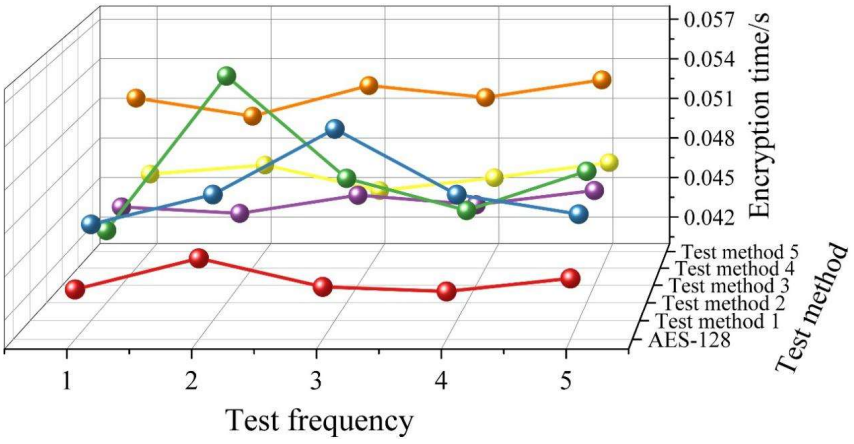


Fig. 2. The aes-128 algorithm and the encryption time of different test methods

The decryption time of the AES-128 algorithm with different test methods is shown in Fig. 3, and the decryption time of the improved AES-128 algorithm designed in this paper is always smaller than that of the other four test methods, and the average value of the five decryption times is 0.04805s.

The combined encryption and decryption time of the improved AES-128 algorithm shows that only the S-box is replaced in the test method (1), the key expansion algorithm is unchanged, and the overall encryption and decryption time of the algorithm is smaller than the rest of the methods. In the improved key expansion algorithm, the use of the composite function and the complexity of the wheel key generation increases both encryption and decryption times to varying degrees. The decryption time is greater than the encryption time in all the tested methods due to the fact that the polynomial coefficients of the inverse column mixing are larger than those of the proportional mixing, which leads to an increase in the time of matrix multiplication operations. By comparing the average values it is found that the improved S-box and key expansion algorithms do not have much effect on the efficiency of the overall algorithm implementation and both are able to participate in the algorithm for normal operations.

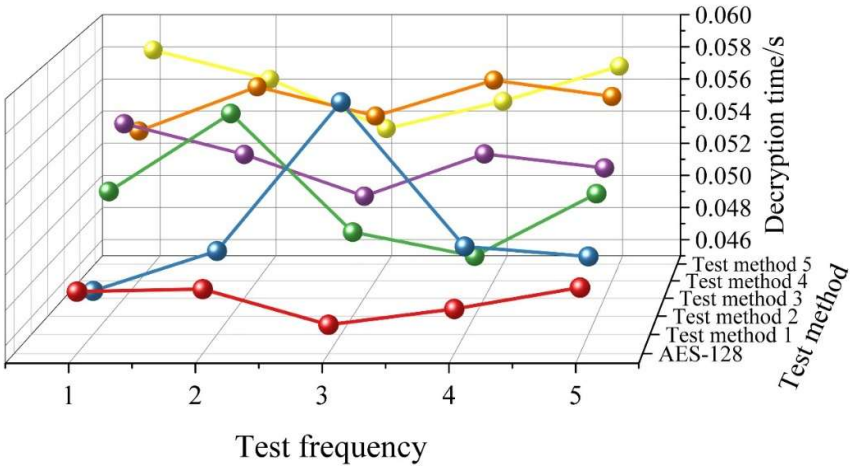


Fig. 3. The aes-128 algorithm and the decryption time of different testing methods

4.3. Analysis of the efficiency of electronic evidence storage

As electronic evidence is generated on the basis of electronic technology, it is highly dependent on science and technology. Conventional digital storage and transmission methods make electronic evidence subject to the risk of attack and tampering, and cannot guarantee the integrity and authenticity of electronic evidence. In judicial practice, electronic evidence is often faced with the

problem of authenticity and integrity is not recognized.

For the traditional electronic evidence storage method is difficult to ensure the security of evidence, as well as related research in data storage is difficult to balance the problem of overhead and efficiency. Based on blockchain and combined with IPFS, an electronic evidence storage model is proposed, which uses IPFS to reduce the storage overhead on the chain and optimizes the storage efficiency of the model based on the directed acyclic graph, which makes the electronic evidence storage secure and trustworthy and at the same time, reduces the overhead of the storage on the chain, eases the storage pressure and improves the storage efficiency.

FISCO BCOS is an enterprise-level financial blockchain underlying technology platform independently developed and completely open-sourced by the Open Source Working Group of Golden Chain Alliance, featuring high-performance, high-security, high-availability, and ease-of-use, etc. FISCO BCOS supports multi-cluster architecture and introduces control mechanisms such as node access, CA blacklisting, and distributed permissions to guarantee the security of data access between blockchain nodes. FISCO BCOS also provides many application development components to help developers develop blockchain applications efficiently and agilely. It contains a set of lightweight open source development components, including smart contract library components, contract compilation plug-ins and application development scaffolding, covering smart contract development, debugging, application development and other aspects. Developers can freely choose the corresponding development tools according to the actual, to improve the development efficiency of decentralized application DApp.

Experimental environment information:

System: Ubuntu 16.04

Processor: Intel i7-6500U 64-bit 4-core

Memory: 8GB

FISCO BCOS version: 3.0

A single cluster 4-node FISCO BCOS federation chain was built based on the above experimental environment, and the evidence storage smart contract algorithm was written in Solidity language. 1000 new test users were created and the generated user information was saved in userinfo, and 1000, 2000, 4000, 6000, 8000 and 10000 transactions were sent respectively. And 40% transaction mutual exclusion is set between transactions. In the experiments of this paper, a randomly generated 46-byte string starting with Qm using a string generator is used to simulate the CID value generated by IPFS in the real case.

Web3SDK provides APIs to access FISCO BCOS nodes with many extended features, such as providing contract deployment tools and contract usage tools, supporting the use of state secret algorithms to issue transactions, and supporting the conversion of smart contract code into Java code. Transactions are generated through 3 Web3SDKs, and tests related to storage and query are completed.

Transactions per second (TPS) represents the number of transactions processed per second, which reflects the transaction throughput rate and is an indicator for evaluating system performance. Usually, TPS is calculated as:

$$TPS = \frac{Total\ transaction\ number}{Pressure\ end\ time - Pressure\ start\ time} \tag{25}$$

The test results for storage and query are shown in Figure 4. The average TPS of set storage method in this experimental environment is 344 and the average TPS of get query method is 862.

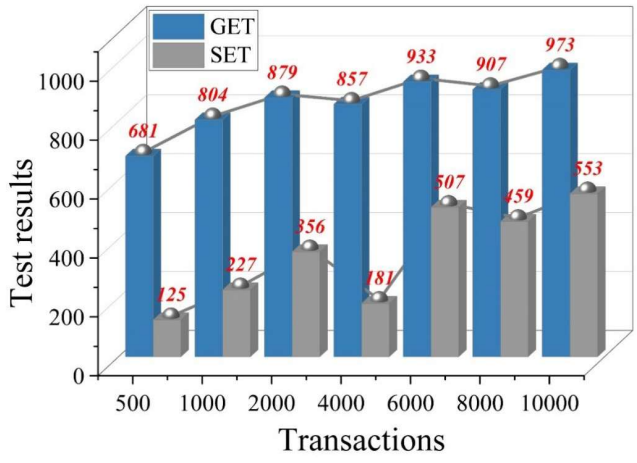
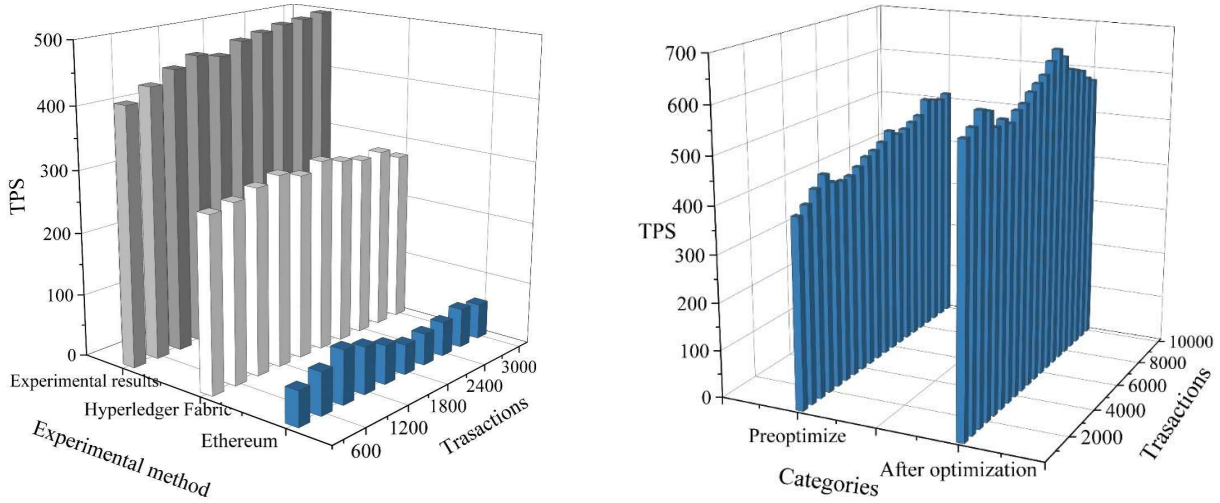


Fig. 4. Test results of storage and query

The results of the storage experiment are shown in Figure 5. The storage method set() is set to 300, 600, 900, 1500, 3000, 6000 transactions for the experiment. And the experimental results are compared with the results of the adopted Hyperledger Fabric, adopted Ethereum, and the results are shown in Fig. (a). Send 1000, 2000, 4000, 6000, 8000, 10000 transactions respectively to test the set() method before optimization and after optimization, and the results are compared as shown in Fig. (b).

As can be seen from Fig. (a), the experimental results of this paper's environment are more efficient than Hyperledger Fabric and Ethereum under the conventional. As can be seen from Fig. (b), the TPS of the storage methodset after DAG optimization is about 630, which is an efficiency improvement of about 37.01%. This is due to the 40% mutex set between transactions, these mutex transactions will be executed in parallel and can save the execution time of transactions. In the case where the transactions are completely mutually exclusive, the optimization performance can theoretically be improved by several times, which mainly depends on the number of CPU cores, which shows that the model has good practicality and scalability.



(a) Experimental results

(b) Optimized result

Fig. 5. Stored experimental results

5. Analysis of the advantages of online litigation

In the process of searching for online trial mode cases, this paper found that 99% of the online trial

cases were from an Internet court, and the years of online trial cases were concentrated in 2019 to 2021.

Since the online trial mode is mainly applied to summary procedure cases, in order to increase the comparability between online trial mode cases and traditional trial mode cases, this paper limits all samples to cases in which the trial court is an Internet court applying summary procedure between 2019 and 2021.

All variable data were obtained from an intelligent legal database (Judicial Case Bank), and by eliminating some samples with missing data, 6,375 sample cases were finally obtained, including 1,204 cases applying the online trial mode. Among them, there are 446 online trial mode cases in 2019, 365 in 2020 and 393 in 2021. The descriptive statistics of the litigation efficiency of online versus traditional hearings are shown in Table 1, which summarizes the litigation efficiency of online versus traditional hearings with different control variables. In terms of the litigation efficiency of all cases, the average litigation efficiency of cases applying the online trial mode is higher than that of cases applying the traditional trial mode, and the data distribution of the former is more concentrated.

From the point of view of the complexity of cases, the online trial mode for the more complex cases is significantly more efficient than the traditional trial mode. For non-complex cases, the efficiency has increased but the difference is not obvious.

From the point of view of the subject matter, in loan contract disputes, the litigation efficiency of cases applying the online trial mode is much higher than that of cases applying the traditional trial mode. However, in intellectual property and competition disputes and bank card disputes, the efficiency of the former is slightly lower than that of the latter, and there is no significant difference in the efficiency of the two in other cases.

In terms of the presence or absence of legal representation, the litigation efficiency of the online trial mode is significantly higher than that of the traditional trial mode with legal representation. The efficiency of the former was slightly higher than that of the latter in the absence of legal representation.

From the perspective of trial organization, only 15 online trial cases are collegial. Moreover, the litigation efficiency of the online trial mode under the collegial system is lower than that of the traditional trial, while the former is slightly higher than the latter under the solo system. In terms of the year in which the cases were concluded, the efficiency of the online mode of adjudication was the same as that of the traditional mode of adjudication in 2019, and the former was significantly higher than the latter in 2020 and 2021.

Table 1. Descriptive statistics on online hearing and traditional hearing action efficiency

		Online trial			Traditional hearing		
		Observed value	Mean	Standard deviation	Observed value	Mean	Standard deviation
	Full case	1204	3.687	0.754	4283	4.128	0.821
Complexity of cases	Complex cases: above sample mean	475	3.568	0.691	2964	4.489	0.677
	Non-complex cases, below the sample mean	729	3.429	0.295	1899	3.415	0.896
The origin of the case	Intellectual property and competition disputes	79	4.795	0.452	1053	4.426	0.531
	Loan contract dispute	906	3.605	0.551	1529	4.639	0.741
	Bank card dispute (credit card)	185	3.326	0.054	1215	2.968	0.352
	Other disputes	34	4.865	0.721	1365	4.852	0.612
Lawyer	Have	695	3.869	0.521	2643	4.567	0.582
	No	509	3.246	0.416	2017	3.671	0.841
The form of the	Collegial system	15	5.893	0.016	374	5.468	0.235

judicial group	Independence system	1189	3.741	0.513	4651	4.235	0.896
Year	2019	446	3.425	0.507	1685	3.521	0.857
	2020	365	3.864	0.431	2232	4.153	0.531
	2021	393	3.606	0.521	4865	4.529	0.892

6. Conclusion

This paper utilizes blockchain technology to encrypt and store electronic evidence to accelerate online litigation advancement. Analyze the differences and similarities between online trial mode and traditional trial mode, and select the complexity of the case, the cause of the case, the lawyer, and the form of approval organization as the variables, and compare and analyze the litigation efficiency of online trial and traditional trial mode.

1) Propose time-proof consensus algorithm and AES algorithm, synthesize the encryption and decryption time of the improved AES-128 algorithm can be seen, the encryption time of the five tests AES-128 algorithm is always maintained at 0.43~0.44s, and the decryption time is always smaller than the other four test methods. The use of blockchain to store data information ensures the authenticity and homogeneity of electronic data in the online litigation link, and realizes the authentication of the deposited electronic data. Guarantee storage security and promote the mutual integration of blockchain technology and law.

2) Select the case of online trial mode and summarize the litigation efficiency of online trial and traditional trial under different control variables. From the perspective of the litigation efficiency of all cases, the average litigation efficiency of cases applying the online trial mode is higher than that of cases applying the traditional trial mode, and the data distribution of the former is more centralized.

Online trial mode as a traditional court trial mode in the Internet background of an extension and expansion. Online trial mode relies on traditional civil litigation rules, and online litigation mode promotes more convenient and efficient trials. Online trial mode is significantly better than traditional trial mode in improving litigation efficiency and saving litigation costs.

Funding

This work was supported by Hunan Graduate Research Innovation Project: Research on the Thinking Mode of Judges in the "Smart Court" Background, project number 431000188.

References

[1] Yadav, S. P. (2020). Effective citizenship, civil action, and prospects for post-conflict justice in yemen. International Journal of Middle East Studies, 52, 754 - 758.

[2] Fong, E., Yeoh, B. S. A., Yeoh, B. S. A., Goh, C., & Wee, K. (2020). Social protection for migrant domestic workers in singapore: international conventions, the law, and civil society action:. American Behavioral Scientist, 64(6), 841-858.

[3] Goldscheid, Julie, Kathawala, & Rene. (2018). State civil rights remedies for gender violence: a tool for accountability. University of Cincinnati Law Review.

[4] Dughera, S., & Giraudo, M. (2020). Privacy rights in online interactions and litigation dynamics: a social custom view. European Journal of Political Economy, 101967.

[5] Gunderson, A. (2021). Ideology, disadvantage, and federal district court inmate civil rights filings: the troubling effects of pro se status. Journal of Empirical Legal Studies, 18(3).

[6] Abedi, F., Zeleznikow, J., & Brien, C. (2019). Developing regulatory standards for the concept of security in online dispute resolution systems. Computer Law & Security Review, 35(5).

[7] Dumas, & Marion. (2017). Taking the law to court: citizen suits and the legislative process. American Journal of Political Science.

[8] Von Wiegen, L., & Oltmann, S. M. (2020). A different democratic divide: how the current u.s. online court record system exacerbates inequality. Law library journal(2), 112.

[9] Park, H. J. (2020). Class action scarcity: an empirical analysis of the securities class action in korea. European Business Organization Law Review, 21(3), 665-708.

[10] Menashe, D. (2018). A critical analysis of the online court. University of Pennsylvania Journal of International Law, 39(4), 921-953.

[11] McMannon, Erin, & E. (2019). The demise of § 1983 malicious prosecution: separating tort law from the fourth amendment. Notre Dame Law Review.

[12] Swelmiyeen, A., Ibrahim, Al-Nuemat, & Ahmed. (2017). Facebook e-court: online justice for online disputes. Computer Law & Security Review.

[13] Pelet, del, Toro, Valeria, & M. (2019). Beyond the critique of rights: the puerto rico legal project and civil rights litigation in america's colony. The Yale law journal, 128(3), 4-4.

[14] Ross, S., & Aitken, S. (2022). "if it hadn't been online i don't think i would have applied": applicant experiences of an online family violence intervention order process:. Journal of Interpersonal Violence, 37(1-2), 221-238.

[15] Erichson, Howard, & M. (2018). Civil litigation reform in the trump era: threats and opportunitiessearching for salvageable ideas in ficala. Fordham Law Review.

[16] Schmitz, Amy, & J. (2019). Expanding access to remedies through e-court initiatives. Buffalo Law Review.

[17] Ciulla, M. T. (2017). A disproportionate response? the 2015 proportionality amendments to federal rule of civil procedure 26(b). Notre Dame Law Review, 92, 1395.

[18] Weinshall, K., & Epstein, L. (2020). Developing High-Quality Data Infrastructure for Legal Analytics: Introducing the Israeli Supreme Court Database. Journal of Empirical Legal Studies(4).

[19] Liyuan Wang. (2024). Application of information technology in judicial field: The development model of online litigation in China. Computer Law & Security Review: The International Journal of Technology Law and Practice105936-.

[20] Jing Xiao,Tao Luo,Chaoqun Li,Jie Zhou & Zhigang Li. (2024). CE-PBFT: A high availability consensus algorithm for large-scale consortium blockchain. Journal of King Saud University - Computer and Information Sciences(2),101957-.

[21] Zhiqiang Du,Jiaheng Zhang,Yanfang Fu,Muhong Huang,Liangxin Liu & Yunliang Li. (2023). A Scalable and Trust-Value-Based Consensus Algorithm for Internet of Vehicles. Applied Sciences(19).