A Blockchain Based Security Scheme for Legal Electronic Service

Dongsheng Hou(✉), Yu Du, Yukun Hao, and Jingting Ji

Shanghai Buqin Network Technology Co., Ltd., Blockchain Lab, Shanghai, China
{houdongsheng,ydu,haoyukun,jijingting}@wxblockchain.com

Abstract. Electronic service has long been regarded as a significant legal service method for the optimal distribution of limited judicial resources. However, information security remains the major concerns within academia and judicial authorities during the actual application. Within current legal framework, digitization of the whole process was studied systematically and a practical technical scheme was proposed to enhance the security of electronic service system. Based on the research, the information security relies on three aspects, namely the ability for litigants to judge the authenticity of legal documents, identification, encryption and management of crucial data, reliable non-repudiation of key behaviors. To assure the system security, anti-counterfeiting and fidelity techniques were applied to realize the generation and processing of electronic judicial documents; Identification encryption and key partitioning techniques were used to get the document exposed for data safety in transmission; Key behavioral data of the whole process were fixed and stored on alliance chain with network slicing technique to balance the strength and efficiency. Besides, neutrality, confidentiality and convenience of service system were also considered in the architecture. Finally, the innovated scheme was developed and all results were displayed in the paper.

Keywords: Electronic Service · Information Security · Blockchain

1 Introduction

China is comprehensively deepening the construction of intelligent courts. The implementation of electronic service of judicial documents within Chinese legislate system has its significant necessity at contemporary times. (1) Conventional legal service methods, such as direct service, may encounter "service difficulty" in some cases, for example, where the addresses of relevant litigant are not available due to vacant residence registration. (2) Optimal distribution of judicial resources is required to improve the gap between demand and supply. The Supreme People's Court accepted 38,498 cases in 2019 with an increase of 140.8% from that of 2015, as for local courts, it was 31.567 million cases with a rise of 143.9%. (3) Current information technology promotion in China can support the enhancement of Chinese legislate operation efficiency. Up to December 2020, the number of internet users in China has reached 989 million, and the proportion of those using mobile is 99.7%.

© The Author(s) 2023
D. Qiu et al. (Eds.): ICBBEM 2022, AHIS 5, pp. 957–966, 2023.
https://doi.org/10.2991/978-94-6463-030-5_94

The electronic service practice in Chinese legislate system can be traced back to the "Special Procedures for Maritime Procedure Law" taking effect in 2003, mainly for foreign-related litigations. However, for domestic judicial cases, especially civil cases, electronic service has not been extensively promoted. Electronic service of judicial documents relies on the courts' hardware platform and software system, and the information security remains the major concern among academia and the legislate system.

Key procedures that the security issue of legal electronic service lied in were generally summarized as data generation and processing, data storage, data conversion, data transmission, neutrality and security of the third-party platforms, data confidentiality and security assurance, etc. [6] Existing technical measures for security improvement basically depend on experiences from general network systems, such as firewall and antivirus software [5]. Some research in the judicial fields proposed technical solutions with single specific judicial scenario taken into account. Zhou [8] introduced an electronic service system applying login signature and Hash function to ensure subject authenticity. Hu [2] mentioned the encryption, digital signature and access control techniques for the security of information transmission, but did not provide enough technical details. Germany digital signature practice were recommended when the served party was signing judicial documents [3], and security keys were also suggested in the study. However, the research above are more prospective proposals than practical technical schemes.

A blockchain is fundamentally a decentralized, distributed, shared, and immutable database ledger that stores registry of information across a peer-to-peer (P2P) network [4]. With the help of cryptographic hash functions, digital signatures, and distributed consensus mechanisms, once a record enters the database, it cannot be altered without the consensus of the other network participants [1]. This research, for the first time, proposed a decentralized mechanism based on the blockchain technique to systematically solve the data reliability, security, and privacy issues that may be encountered in the conventional legal electronic service systems. Considering the original defects of highly required computing power and possibly low TPS when blockchain applied, the innovated scheme applied network slicing technique to balance the strength and efficiency. Finally, all technical solutions were developed for actual electronic service cases, and the results were displayed.

2 Key Techniques on Electronic Service Security

2.1 Data Anti-counterfeiting and Fidelity Technique

Judicial documents could be tampered by a third party in the process of electronic service. The lack of anti-counterfeiting and fidelity measures would result in the inability of relevant parties to judge the authenticity of received documents, and thus hinder the normal progress of judicial procedures. To solve this, a combination of digital signature, fragile digital watermark, two-dimensional code, visual seal, and credible timestamp techniques were applied to realize the generation and processing of electronic judicial documents.

2.1.1 Digital Signature Technique

Digital signature is based on asymmetric key encryption technique and digital digest technique. The technique is most widely applied to ensure the integrity and authenticity of the transmitted electronic files. Common digital signature algorithms include RSA, ElGamal, Fiat-Shamir, etc.

Original judicial documents are generally generated in the internal working system of a court; a judge or clerk accesses the system through a browser. To avoid the possible incompatibility problem between browsers and controls, a real-time online status of the digital certificate would be maintained by establishing a long connection between the client and the application server. In this way, operators could always perform digital signature as a response to HTTP requests, instead of system modules.

2.1.2 Two-Dimensional Code Technique

Two-dimensional code is a pattern of black and white binary squares representing data, also known as QR code. Changing the data encoded within alters the pattern of the QR code accordingly. There are two types of QR codes, i.e. static code and live code. The former encodes character strings such as letters, symbols, numbers, etc. It is constrained by the display size when used, but is adaptable for situations without internet. By contrast, the latter encodes a fixed short URL, and then jumps to a webpage after scanned. Contents on the webpage can be designed and updated dynamically, while the QR code remains unchanged.

Advantages of both alternatives could be taken in trials. Namely, the characteristic information of judicial document was converted to a binary static code, and the QR code adopted the GB2312 mode; the website of a court or a third-party was converted to a binary live code, and the QR code adopted a mixed character mode.

2.1.3 Fragile Digital Watermark Technique

Digital watermark technique is a type of computer information hiding technology based on content and non-password mechanism. It can embed some identification information directly into the digital carrier or indirectly express the information by modifying the structure of a specific area. The embedded information does not affect the utility of the original carrier, and is unlikely to be detected and modified by people other than its producer. Through the "hidden" information, the producer or its purchaser can confirm if the carrier has been tampered.

A watermark can be divided into robust digital watermark and fragile digital watermark. Robust watermark is primarily used to identify the copyright information of digital work, such as creator, owner, and purchaser etc., while fragile watermark is mainly used for integrity protection and authentication.

Electronic judicial documents may be in the format of PDF or image. When fragile digital watermark substitutes static QR code and combines with live code, the mode can break through the size limit of official documents and cover all essential characteristic data, as shown in Fig. 1.

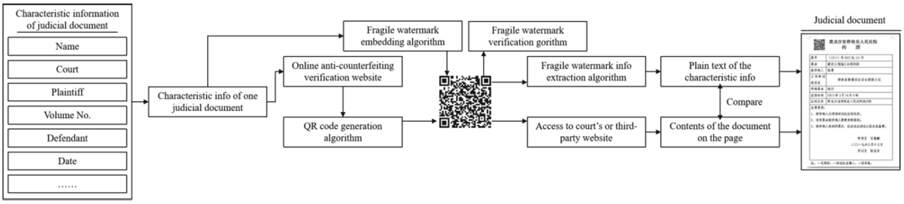

Characteristic information of judicial document
Name
Court
Plaintiff
Volume No.
Defendant
Date
……
Characteristic info of one judicial document
Fragile watermark embedding algorithm
Online anti-counterfeiting verification website
QR code generation algorithm
Fragile watermark verification gorithm
Fragile watermark info extraction algorithm
Access to court's or third-party website
Plain text of the characteristic info
Compare
Contents of the document on the page
Judicial document

Fig. 1. An anti-counterfeiting document with live QR code and fragile digital watermark

2.2 Data Security Technique

2.2.1 Identification Encryption Technique

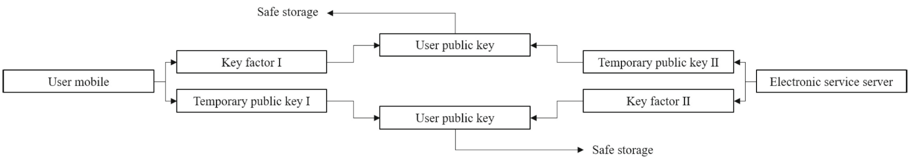
In the electronic service practice through emails or SMS, the court's official website and the judicial document extraction code are generally sent simultaneously from the internet area of an official server. If the contents of the text messages or emails to be sent are intercepted, the sensitive information of litigants is leaked, which impairs individual's privacy and legal authority. Therefore, the identification of the addressee is necessary. The technical scheme is as follows.

(1) Encrypt and store using litigant's identification.
Through bilinear mapping cryptographic algorithm SM9, encrypt judicial documents by using the served party's phone number or email address as the generation factor of public key.
(2) Re-verify the identity of the party to be served.
When litigant receives the SMS or email from electronic service system, he may open the attached link of judicial document. Before one can look up the document, he shall confirm his identification by proving the ownership of the phone number or email.
(3) Decrypt and access to the judicial document.
Recipient applies for the private key from the server with the exact phone number or email. The verification information for private key can only be delivered if corresponding identification is correct. Then, decrypt the document using the private key.
(4) Issue an RSA digital certificate and return the "Confirmation of Service" with the consent.

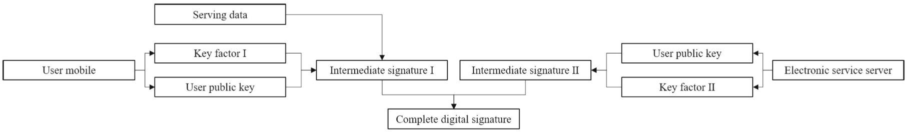
2.2.2 Key Partitioning Management Technique

In the electronic service practice through official APP, mobile terminal is more rigorous than the cloud server for the secure digital certificate storage. However, existing mobile phones generally lack such special hardware modules, so the complete key is currently maintained within the mobile storage. In this way, the integral plaintext is exposed during the signature calculation in the mobile memory, where the security largely depends on the operating system.

Key partitioning technology [7] is therefore applied for the storage and access of private key. The management process is mainly divided into two procedures: partitioning



(a) Partitioning key generation



(b) Partitioning key signature

Fig. 2. Key partitioning management technique

key generation and signature processing with the partitioning keys, as shown in Fig. 2. Partition the digital certificate key that identifies the party's trusted identity, and store them separately on the mobile phones and servers. Neither party can fully hold the original private key, nor can they complete the electronic signature independently. This mechanism eliminates the risk of key loss due to single-point breakthrough.

Besides, the user subkey on mobile is generated by a random number derived by local secure random number hybrid calculation, and is protected by encryption measures with the user PIN code and the device characteristic value. The user subkey on server is generated using a random number generated by the encryption machine, and is protected relying on the machine security.

2.3 Data Fixation and Tracing Technique

Traditional legal electronic service system lacks reliable non-repudiation measures for key behaviors in the whole process. This may result in less effectiveness of relevant data as crucial legal evidence and difficulty in responsibility determination.

2.3.1 Evidence Fixation Technique

Electronic service involves four behavioral events concerned with judicial documents: generation, transmission, receiving, and signing. Each behavior includes six elements: subject, object, time, intention, action and location.

Non-repudiation technical measures for key electronic service operations are shown in Fig. 3. The basic procedures are: calculate hash digests based on the primary data generated by the court's sending behavior and the litigant's review of judicial documents; implement signature for relevant behaviors using time stamp; conduct a strict authenticity check of the behavioral data in the evidence chain according the national electronic signature laws and judicial logic; grant the legal validity for the qualified behavioral data by a special seal from certification agency authorized by the government; establish alliance chain among courts and other relevant institutions; upload all behavioral evidence onto the chain and maintain it among all nodes. Consequently, all

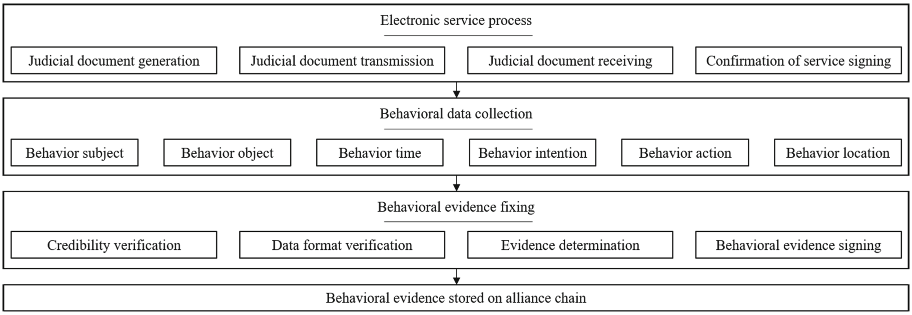

Electronic service process
Judicial document generation
Judicial document transmission
Judicial document receiving
Confirmation of service signing
Behavioral data collection
Behavior subject
Behavior object
Behavior time
Behavior intention
Behavior action
Behavior location
Behavioral evidence fixing
Credibility verification
Data format verification
Evidence determination
Behavioral evidence signing
Behavioral evidence stored on alliance chain

Fig. 3. Evidence fixation technique

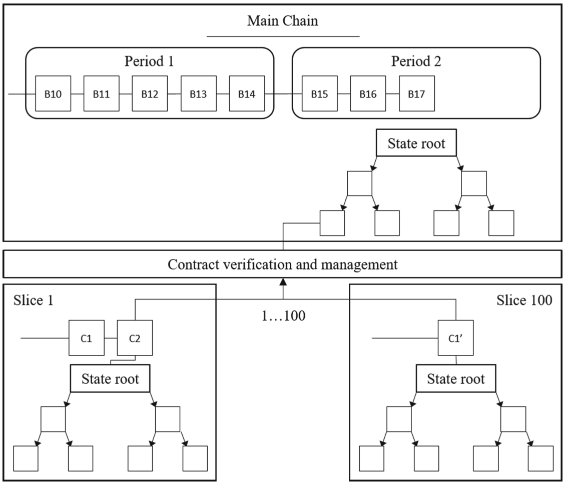


Fig. 4. Blockchain network slicing technique

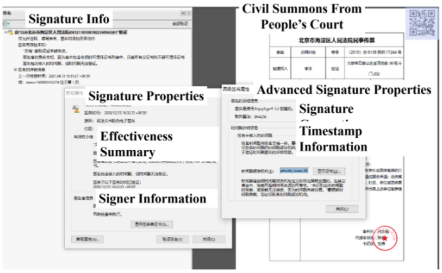
original behavior data from electronic service process become shared legal evidence of high reliability and traceability.

2.3.2 Multi-angle Slicing Technique

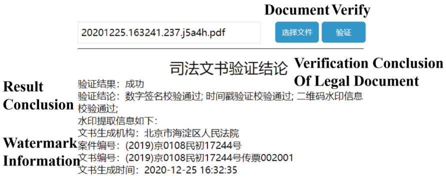
Batch service and multiple service are prevalent in many cases. But distributed network system of blockchain may introduce access peaks and cause information transmission delays. To improve throughput, asymmetric network slicing technique is applied.

Divide the blockchain network into subnets with unequal numbers of nodes based on the principles of distribution and computing power matching. Continue to superimpose existing network slices using random angles, as illustrated in Fig. 4. In this way, the asymmetry of network slicing can enhance the throughput of blockchain network without sacrificing the attack resistance of system.

Network slicing needs to balance the number of subnets and the depth of transaction Merkel tree. The increasing number of slices results in a rise in the time complexity of



(a) Judicial documents with anti-counterfeiting measures



20201225.163241.237.j5a4h.pdf

司法文书验证结论

验证结果：成功
验证结论：数字签名校验通过; 时间戳验证校验通过; 二维码水印信息校验通过;
水印提取信息如下：
文书生成机构：北京市海淀区人民法院
案件编号：(2019)京0108民初17244号
文书编号：(2019)京0108民初17244号传票002001
文书生成时间：2020-12-25 16:32:35

(b) Fidelity verification results

Fig. 5. Implementation of anti-counterfeiting and fidelity measures

management (T(n) = O(n)), while the decreasing number of transactions within a slice results in a reduction in the time complexity of consensus (T(n) = O(logn))). Combine the caused computing power dispersion by network slicing, and the empirical value is obtained. Namely, when the Merkel tree with a depth of 3 is used for transaction slicing, internal transaction number in a slice has greater effects on the transaction depth than the number of slicing network nodes.

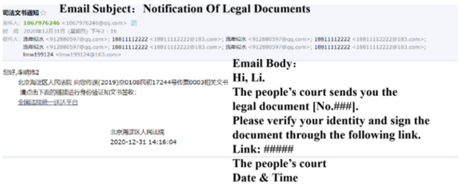
3 Implementation of Electronic Service Security Based on Blockchain Technique

3.1 Judicial Documents with Anti-counterfeiting and Fidelity Features

The innovated system performs five-fold anti-counterfeiting and fidelity operations on one judicial document. The served party can directly see the verifying QR code with fragile watermark, and the digital seal of the court, and can also look up time stamp by referring to the electronic signature, as shown in Fig. 5(a). The relevant litigant can further verify the authenticity of the document through a designated website, the displaying results are illustrated in a way like Fig. 5(b).

3.2 Secure Transmission of Judicial Documents

The innovated system integrates multiple electronic service channels such as official website, APP, SMS, email, WeChat, etc. For instance, the served party receives a notification of judicial document by an email like Fig. 6(a), which contains a link to access to the document. Identification and key partitioning storage techniques are applied to get the document exposed for safety. Meanwhile, letter of Confirmation of Service will be sent back automatically with the consent of litigant, as illustrated in Fig. 6(b).



司法文书通知 Email Subject: Notification Of Legal Documents

发件人: 1067976246 <1067976246@qq.com>

时 间: 2020年12月31日 (星期四) 下午2:16

收件人: 流年似水 <912880597@qq.com>; 18811112222 <18811112222@183.com>; 流年似水 <912880597@qq.com>; 18811112222 <18811112222@183.com>; 流年似水 <912880597@qq.com>; 18811112222 <18811112222@183.com>; 流年似水 <912880597@qq.com>; 18811112222 <18811112222@183.com>; lmw199124 <lmw199124@163.com>

您好,李明伟2

北京海淀区人民法院 向您传送(2019)京0108民初17244号传票0003相关文书

请点击下面的链接进行身份验证和文书签收:

全国法院统一送达平台

北京海淀区人民法院

2020-12-31 14:16:04

Email Body:

Hi, Li.

The people's court sends you the legal document [No.###].

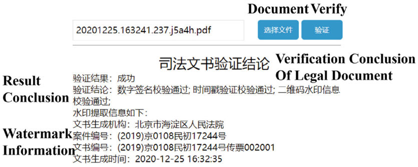
Please verify your identity and sign the document through the following link.

Link: #####

The people's court

Date & Time

(a) Notification with ID verification and encryption



Document Verify

20201225.163241.237.j5a4h.pdf

司法文书验证结论 Verification Conclusion Of Legal Document

Result Conclusion

验证结果: 成功

验证结论: 数字签名校验通过; 时间戳验证校验通过; 二维码水印信息校验通过;

Watermark Information

水印提取信息如下:

文书生成机构: 北京市海淀区人民法院

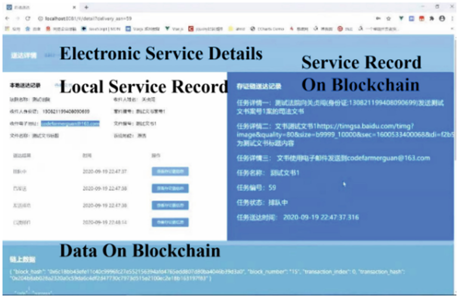
案件编号: (2019)京0108民初17244号

文书编号: (2019)京0108民初17244号传票002001

文书生成时间: 2020-12-25 16:32:35

(b) Confirmation of service with ID

Fig. 6. Implementation of secure transmission of judicial documents



Electronic Service Details

Local Service Record

2020-09-19 22:47:37

2020-09-19 22:47:38

2020-09-19 22:47:38

2020-09-19 22:48:14

Service Record On Blockchain

存证链送达记录

任务详情三: 文书使用电子邮件发送到codefarmerguan@163.com

任务名称: 测试文书1

任务编号: 59

任务状态: 排队中

任务送达时间: 2020-09-19 22:47:37.316

Data On Blockchain

链上数据

Fig. 7. Implementation of key behavior evidence fixation and reservation on blockchain

3.3 Legal Evidence Fixation and Reservation

Key behavioral data in the whole process of electronic service is fixed and stored on blockchain. Relevant parties can conduct retrospective query and obtain the results like Fig. 7. In the innovated system, the Practical Byzantine Fault Tolerant (pBFT) algorithm was adopted as the consensus mechanism. In the 15-node alliance chain, a distribution of 3 network slices and 3 transaction slices was used, consequently the overall throughput of the alliance chain was enhanced to approximately 100,000 TPS from normal 40,000 TPS.

4 Conclusions

Electronic service of judicial documents is an important implementation of the informatization of Chinese legislate system, and information security is the major concern. A blockchain based security scheme was proposed to enhance the whole process, an innovated system was accordingly developed and the results were displayed in the paper. Main conclusions and highlights of the presented study were as follows. Anti-counterfeiting documents were generated and processed with a combination of digital signatures, visual seal, QR code, fragile digital watermark, and time stamp techniques. By referring to certification authority, the fidelity of judicial documents can be ensured. Safe judicial document transmission was realized through identification encryption and key partitioning management. In this way, privacy leakage and information interception can be avoid. The Confirmation of Service can be automatically returned with the consent of litigant. Complete behavioral data were fixed after rigorous verification and reserved on alliance chain. Relevant parties can retrospect the trusted legal evidence for query or responsibility determination. Multi-angle slicing was applied for the balance of strength and efficiency of blockchain network. For further research, the balance of information security and privacy preservation requires more technical and practical investigation for widely used electronic service in judicial system.

Acknowledgements. This work was supported by the National Key R&D Program of China (Grant No. 2018YFC0830200).

References

1. Cong, T., Hoang, D., Nguyen, D., Niyato, D., Ngugen, H., Dutkiewicz, E., 2019. Proof-of-Stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. In *IEEE Access*. 7, 85727–85745.
2. Hu, J., 2018. The difficulties and solutions exploration of the service system in the civil procedure. Dissertation. Chongqing University.
3. Jin, X., 2019. Research on service by electronic means in China's civil procedure. Dissertation. Guangxi Normal University.
4. Khan, M., Salah, K., 2017. IoT security: review, blockchain solutions, and open challenges. J. Future Generations Computer Systems. 82, 395–411.
5. Shi, C., 2015. Investigation on the civil electronic service in China. J. Journal of Liaocheng University (Social Science Edition). 3, 120–128.
6. Wang, G., 2020. Study on electronic service of the people's courts. Dissertation. Graduate school of Chinese academy of social sciences.
7. Zhang, L., Wu, L., Chen, Y., 2018. Implementation and application of distributed key split digital signature based on RSA algorithm. In *Power Industry Informatization Annual Meeting 2018*.
8. Zhou, Q., 2015. Discussion on the reform and improvement of the electronic service regulation in China. J. Journal of Huanggang Polytechnic. 000(004), 68–70.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.