An Electronic Evidence Transfer Model based on Blockchain Technology

Hai-Yan Chen

Abstract: With the rise and maturity of blockchain technology, its application in various fields has been widely carried out. This paper analyses the shortcomings of traditional electronic evidence in the judicial system, such as preserving, transferring and presenting, and proposes an electronic evidence transfer model based on blockchain technology. Combining with the model, the paper presents the transfer scheme of electronic evidence in every link in the judicial system. Eventually, the shortcomings of the model and the direction of future research are analysed.

Keywords: Electronic Evidence, Blockchain, Judicial System.

Introduction

With the arriving of information age, people's daily lives become more and more inseparable from all sorts of electronic equipment. Benefiting from these devices to get access to the Internet to realize various functions such as social networking, shopping, entertainment, games, which results increased crime, disputes and the explosive, Electronic evidence becomes the key to the crime and disputes.

Electronic evidence is evidence that is based on electronic media as a carrier which includes video recording, monitoring, chat records, transfer voucher, trade order information, files, images, etc. It is that people use electronic equipment or recorded in the electronic equipment in the process of...
accessing to the network or with network equipment of various data, or to prove the authenticity of the case electronic information, records, and items.

Compared with traditional evidence, electronic evidence is fragile, and easy to be modified and deleted, and on the other hand, authenticity is difficult to be guaranteed. For example, data in a personal computer is likely to be lost due to disoperation, virus attacks, etc. The evidence collected by the court is stored in a specialized database, and the risk of data tampering should be faced only if the database manager bribes.

At present, although there are strict rules about the collection, storage and analysis of the electronic evidence in China, there are still many problems, such as: in the process of collecting evidence, the public security departments need a complex examination and approval procedures and it is easy to lose key evidence facing electronic evidence fleeing away. The electronic evidence collected by the parties, such as civil, commercial, knowledge and administrative disputes, lacks the necessary encryption and authentication measures, resulting in a significant reduction in the collection of evidence. In the process of submitting the evidence to the various departments of the judicial system, it is inevitable that the middle part of the process is falsified and cannot be verified. Finally, the judge has doubts about the integrity of the evidence. The traditional storage of electronic evidence is also vulnerable to the electronic evidence database. Some cloud computing platforms have the characteristics of mass and real time, which are difficult to obtain and store. Traditional databases cannot store such large amount of data. The following figure shows a set of transfer process diagram of traditional electronic evidence from collection.
Block chain technique

Block chain technology is considered to be the fifth subvert computing paradigm after the large computers, personal computers and the Internet and mobile social. It is the fourth milestone after Kin credit, precious metals credit, the central bank credit notes. Blockchain is a shared distributed database technology [1], with four characteristics of consensus: decentralization, lack of trust, collective maintenance, reliable database. It is easy to understand the blockchain as a complete, untampered, multi-party, and supervised way of recording.

The underlying technical support of block chain includes a timestamp hash chain and the proof of work mechanism which is to solve the problem of double pay and Byzantine generals. Namely, guaranteeing a summary of currency will not be in two addresses at the same time [3], and on the basis of reliable channel. All nodes can make other nodes to receive their true intentions, and ultimately act in concert.

The architecture of electronic evidence transfer model

While electronic evidence is transferred between the various subjects of the
law, there is possibility of being tampered with and deleted. Therefore, this paper presents an electronic evidence storage model based on block chain technology, as shown below:

![Figure 2. The electronic evidence transfer model based on blockchain technology.](image)

In the diagram: Type A node represents the department of public security; Type B node represents the department of procurator rate; Type C node represents the court department; Type D node represents the identification centre department; Type E node represents the department of justice; F Type node represents the department of law; Type G node represents research institutes and corporate departments; N nodes are all non-bookkeeping end users. Node containments all participants of the judicial system, have extensive sex, representative, authoritative. They jointly maintain the Hash value of the electronic evidence and the signature which is submitted by every terminal customer, and recorded in the books of block chain, only fall of more than 50% of the nodes can modify one record. At the same time, the block chain ledger also records the actions of participants in various judicial systems, such as reporting, filing, appearing in court, trial and so on.

The scheme of node creation: to apply for becoming the terminal of the billing node, the registration information of the unit name, industrial and commercial tax and other registration information shall be submitted. The state organ shall submit the name of the unit, legal person and other information. In addition, the corresponding node is also required to provide its hardware information, software information and system configuration. Then, approved by the billing of unification of all nodes, completely through to become a node of charge to an account, and to be put on record and access.
system. If there is a node that charge to an account application node is illegal, a request to apply for will be rejected.

Blocks creation solutions: each part of accounting departments node maintains a record which record electronic evidence hash values and behaviour by the department of books together, which make any evidence of primordial germ can be verified in the book, any department can get back in the block chain, accountability mechanism can be implemented. When the node to accept to the new electronic evidence, but in the chain the block has been full of cases, it has the right to create a new block, after verification by the other accounting node, hang the block at the end of the far block chain, at the same time to receive the electronic evidence hash value written and electronic signature block.

Users electronic evidence submitted plans: User register at the right node, when registration shall provide the legal proof of identity, billing node will return a pair of public and private keys to the customer and put a chain of customer information and the public key to the whole block webcasts, and recorded in the block of chain. The electronic evidence submitted by the user is passed into the cloud database platform storage after the private key is encrypted, and the hash value and signature are extracted and broadcast to the block chain node of the district.

Acknowledgements
The corresponding author of this paper is CHEN Hai-Yan. This paper is supported by Projects of the National Social Science Fund (No.06BFX051); Shanghai university training and selection of outstanding young teachers in special research fund (No.hzf05046).

Conclusions and prospects
In this paper, a transfer model of electronic evidence in the judicial system, using block chain tamper-resistant features to ensure the authenticity of electronic evidence. Electronic evidence of digital fingerprint will only save the chain block, which avoid block chain being too large. And, at the same time, the behaviour of the various departments in the process of transfer of evidence will be recorded in the chain of blocks so that we can trace evidence in the circulation process through departments. The electronic evidence in this model can satisfy the special needs of massive electronic evidence in cloud computing environment.
References

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. https://bitcoin.org/bitcoin.pdf.
[2] Swan M. Blockchain: blueprint for a new economy[M]. USA: O’Reilly Media Inc., 2015.
[3] Andreas M Antonopoulos. Mastering Bitcoin: Unlocking Digital Cryptocurrencies [M]. CA: O'Reilly Media, Inc
[4] The deep discussion of the Byzantine general question [EB/OL]. (2015-10-16)[2016-08-10].http://www.8btc.com/baizhantingjiangjun
[5] Yuan Y, Wang F Y. Block chain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.