Application of Blockchain in Document Certification, Asset Trading and Payment Reconciliation

Xingxiong Zhu¹,², Dong Wang¹,²
¹State Grid Power Finance and E-Commerce Laboratory, Beijing 100053, China
²State Grid Electronic Commerce Co., Ltd., Beijing 100053, China
zhuxx@pku.org.cn

Abstract. In economic activities, there are massive contracts, transactions, and payments. The consistency, integrity, and security of these important transaction data are crucial. The application of blockchain technology in document certification, asset trading and payment reconciliation, solves the security vulnerabilities existing in traditional technical solutions, optimizes business models, improves efficiency, ensures security, and enhances core competitiveness.

1. Introduction
In economic activities, there are extremely large amounts of contracts, transactions, and payments. The consistency, integrity, and security of these important transaction data are crucial. The following sections describe the application of blockchain technology in the blockchain-based file certification system, the blockchain-based digital asset trading system, and the blockchain-based payment reconciliation system.

2. Blockchain-based file certification system
2.1. Background
In e-commerce, there are enormous important documents such as electronic agreements [1], total assets, and income records. Electronic data is easy to tamper and easy to falsify [2]. Centralized storage mode is prone to systemic risks such as loss and damage. How to make electronic data credible, traceable, and difficult to tamper is a problem that needs to be solved.

2.2. Technical solutions
- Use the Hash algorithm to generate hash values for important files and create a digital "fingerprint" of the file.
- Distributively store the hash value of the file in the blockchain node server.
- Construct a blockchain alliance chain, which consists of trustworthy alliance organs such as judicial organ, judicial appraisal center, electronic certification organ, financial institution, and Internet platform.
- Use the distributed technical characteristics of the blockchain to solve the problem of difficulty in collecting electronic evidence [3].
- Apply blockchain certification to enhance credibility in scenarios such as intellectual properties, electronic contracts, and financial services.
The blockchain certification proves that the electronic data has not been tampered with after being stored in the blockchain \(^4\), which proves the integrity and consistency of the electronic file.

Blockchain technology guarantees the stage of electronic data storage. Improve the credibility of evidence confirmation and evidence forensics.

2.3 System structure
In the application of blockchain technology in e-commerce certification and evidence collection, the key information such as the user account and the hash value of the evidence file is stored in distributed ledger to realize the certification and evidence collection of important evidence files. When the business application creates a new user, the blockchain platform service is invoked, and the corresponding blockchain user is created on the chain. The blockchain platform uses the encryption rules to generate the corresponding public and private keys, and stores the public key information on the chain.

Generate a hash value for important file. The hash value of the file is distributed and stored in the blockchain node server. The document consistency and the authenticity of the document are verified by whether the hash value of the document to be authenticated is consistent with the hash value of the certification file on the blockchain.

2.4 System solutions
The blockchain platform uses its technical features that cannot be tampered with and traceable to realize the certification and evidence collection. These records cannot be tampered with, ensuring the security of the data. Once the user has a business dispute, the authentication organization only needs to verify whether the hash value of the user's original data is in the blockchain, and the identification result can be quickly made and submitted to arbitration.

Each time the file is certificated with a timestamp record, clearly record the time of certification of the document evidence. All the certification of important documents are recorded, forming a chain of evidence. The blockchain removes the single-point authoritative credit model in the centralized system, and the multi-node records the hash digest. Which effectively prevents the hacker from attacking the single node in the centralized system and improves the security of the system.

3. Blockchain-based digital asset trading system

3.1 Background
In the traditional technical solution, digital asset trading is centralized \(^5\). The participants communicate with other parties through the centralized network mechanism. Once the centralization organization fails, it will affect the normal operation of the entire trading system. The system security will not be guaranteed. Digital asset registration data and transaction data are stored in a centralized database \(^6\). Once the database is attacked, it is easily falsified and unsafe.

3.2 Technical solutions
- Simplify the digital asset trading process, prevent data from being tampered with, and improve transaction efficiency and transaction security.
- Use blockchain data structures to store digital asset registration data and its transaction data \(^7\).
- Generate and update digital assets and their transaction data using a distributed node consensus algorithm.
- Secure the data transmission between the blockchain nodes by using encryption algorithm and digital signature.
- Use the digital signature method to ensure the authenticity of the transaction subject and ensure the non-repudiation of the transaction.
- Realize clear settlement of digital asset transactions by using smart contracts composed of programming script code.
3.3 System structure
The data of digital asset creation and transaction will be packaged into blocks, recorded in the blockchain based on the consensus mechanism, and stored in each node to form a digital asset distributed ledger.

The blockchain-based digital asset creating process is shown in Figure 1. And the blockchain-based digital asset trading process is shown in Figure 2.

Each blockchain node distributes messages through the P2P protocol. The process of verifying, accounting, storing, transmitting and maintaining are based on a distributed system structure.

The smart contract of digital asset trading implements various scripts, algorithms and contract codes. It is the basis for the programmable nature of the blockchain-based digital asset system.

3.4 System solutions
The asset issuer creates digital assets and enters information such as asset name, asset quantity, asset measurement unit, and asset description. The seller issues the asset information, the buyer issues the transaction application. The buyer and the seller agree on the transaction items and quantities.

When the transaction data is transmitted between the blockchain nodes, the sender node encrypts the transaction data using the recipient public key to form ciphertext. The sender uses the hash function to generate digest from the transaction packet, signed with the private key. The transaction data ciphertext and digital signature are sent to the recipient.

The receiver node uses its own private key to decipher the ciphertext, obtain the transaction data, and use the hash function to get a digest. The sender's digital signature is verified using the sender's public key to obtain a digest. Compare the two digests. If they are identical, the transmitted data is complete and has not been modified during the transmission. And it confirms the true identity of the sender and recipient.

The blockchain accounting node records the transaction hash, transaction time, transaction originator address, recipient address, asset name, asset issuer address, and asset trading quantity in the block. Each asset transaction has a corresponding hash value, which is unique. Smart contract of clearing and
settlement executes the settlement of assets, payment, expenses, profit sharing, accounts, etc., according to whether the clear settlement condition meets.

4. Blockchain-based payment reconciliation system

4.1. Background
Reconciliation of payments are in order to ensure the correct [8], consistent and reliable transaction payment and billing records. In the conventional technical solution, the reconciliation files are transmitted by FTP. There are payment and refund record files in the bank side, Internet payment platform side, and Internet e-commerce platform side. But the items of records among these sides are not consistent. How to find and handle these inconsistencies are crucial.

In traditional technical solutions, payment reconciliation usually initiates after 1 week or even 1 month of trade. It is long time delay for weekly or monthly reconciliation. Manual reconciliation is labour-intensive and inefficient. The use of FTP to transfer transaction data is not secure, and its data integrity is not guaranteed.

4.2. Technical solutions
- Simplify reconciliation process to prevent data from being tampered with, improving transaction efficiency and transaction security.
- Using smart contract to realize automatic payment reconciliation.
- Real-time reconciliation to improve capital turnover efficiency.
- Using blockchain multi-node to realize distributed ledger of reconciliation data.
- Track the source of the payment data and each transaction.
- Significantly reduce customer complaints caused by customer asset lost, and improve user experience and satisfaction.

4.3. System structure
The blockchain-based payment reconciliation process is shown in Figure 3.

The blockchain-based payment reconciliation system users include consumers, banks, payment platform, Internet e-commerce platform, merchants. The payment records of users are distributed in each node to form reconciliation ledger based on blockchain.
The smart contract of blockchain executes payment reconciliation process according to whether the account consistency conditions are met. It makes the entire reconciliation process automatically and intelligently, reduces the risk of trading errors, and improves efficiency.

4.4. System solutions
There is no need to transmit the payment records files. The bank does not need to provide API interface. Data is shared through distributed ledgers.

Blockchain nodes of the participating units, such as banks, payment platform, and e-commerce platform, deploy respectively, to form alliance chain. Each participant updates data respectively, including transaction serial number, payer, payee, payment amount, refund amount, transaction status, commodity order serial number, time, etc.

The smart contract check whether the values of important record fields are consistent among bank, payment platform, and e-commerce platform. Then it obtains the reconciliation result. When the payments are inconsistent, the warning information is automatically proposed. In the end, detailed report is intelligently generated.

5. Conclusion
The application of blockchain technology in document certification, asset trading and payment reconciliation, solves the security vulnerabilities existing in traditional technical solutions, optimizes business models, improves efficiency, ensures security, and enhances core competitiveness.

Author introduction
Xingxiong Zhu (1975), male, graduated from Peking University, China, master degree in software engineering, one of the main drafters of China National Standard GB/T 25656-2010 "Information Technology Chinese Linux Application Programming Interface (API) specification". Email, zhuxx@pku.org.cn.

References
[1] Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. Artificial Intelligence and Law, 26(4), 377-409.
[2] Ying, W., Jia, S., & Du, W. (2018). Digital enablement of blockchain: Evidence from HNA group. International Journal of Information Management, 39, 1-4.
[3] Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Block-VN: A distributed blockchain based vehicular network architecture in smart City. Journal of Information Processing Systems, 13(1), 84.
[4] Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".
[5] Tadelis, S. (2016). The economics of reputation and feedback systems in e-commerce marketplaces. IEEE Internet Computing, 20(1), 12-19.
[6] Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In Banking Beyond Banks and Money (pp. 239-278). Springer, Cham.
[7] Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. Harvard Business Review, 95(1), 118-127.
[8] Rose, A. J., Fischer, S. H., & Paasche-Orlow, M. K. (2017). Beyond medication reconciliation: the correct medication list. Jama, 317(20), 2057-2058.