Research on Application of Blockchain and Identity-Based Cryptography

Xingsxong Zhu*, Tao Fan

1 State Grid Power Finance and E-Commerce Laboratory, State Grid Electronic Commerce Co., Ltd., Beijing, China
2 State Grid Electronic Commerce Co., Ltd., Beijing, China

*Corresponding author e-mail: zhuxx@pku.org.cn

Abstract. The signing of electronic contracts and the certification of important documents are realized by utilizing blockchain, identity-based cryptography and electronic signature technology. Blockchain technology can realize the data distributed ledgers through the entire system nodes, the whole processes, and the entire transactions. Identity-based cryptography and electronic signature technology can achieve data integrity, privacy, and nonrepudiation. All data is shared by all participating nodes, the information in the cyberspace is more transparent, and the behavior is more traceable. A complete and compliant contract signing process and data certification is achieved.

1. Introduction
Blockchain technology and cryptographic algorithm are important directions in the field of information communication. It is of great significance to explore its application in e-commerce, financial services, new energy applications and judicial certifications. In the e-commerce and financial services business, the credible blockchain and the identification cryptosystem service are fully applied, replacing the traditional CA certification, reducing costs and increasing efficiency, and ensuring security. It is important to develop trusted blockchain certification, laying a solid foundation for the application of trusted blockchain.

In the contract signing and document certification of e-commerce and financial services, the traditional technical solutions is that use the database to store e-commerce data [1], financial service transaction data, and contract data. With traditional PKI/CA-based electronic signatures, the system is complex. Disadvantages of the traditional technical solutions: The prior solution uses a database to store data which is easily falsified; the electronic signature based on the traditional PKI/CA is complicated, and the construction cost is high [2]; Lack of evidence record in the electronic contract signing process.

Blockchain is a new application mode of computer technology such as distributed data storage [3], point-to-point transmission, consensus mechanism, and encryption algorithm [4]. An electronic signature is specific data in an electronic message that is used to identify the identity of the signer in an electronic form and to indicate that the signer recognizes the content therein [5]. It is a signature of the electronic form of the electronic document by cryptography [6]. The Identity-Based Cryptograph (IBC) is an asymmetric public key cryptosystem. Use the user's ID such as ID number, email address,
mobile number, etc., as the public key [7]. The user's private key is calculated by the key generation center based on the system master key and user ID [8]. The user's public key is uniquely determined by the user ID, so that it is not need a third party to guarantee the authenticity of the public key.

The signing of electronic contracts and the certification of important documents can be realized by utilizing blockchain, electronic signature technology and identity-based cryptography.

2. Key technology

2.1. Reliable electronic signature mechanism based on identity authentication chain
An electronic signature method based on identity-based cryptography algorithm uses distributed nodes of blockchain to track the entire process of key application, signature application, signature implementation, decryption, verification, and establishes records of the signer, event, and signature time. The whole process of signature authentication is traceable. The signature behavior is open and can be supervised and traceable. Through the blockchain technology, the tamper-proof and nonrepudiation can achieve reliable electronic signature.

2.2. Time-based user private key model
Based on the uniqueness and nonrepudiation requirements of the signature key, the timestamp concept is introduced. The request time is added in the user private key generation model. The three-element private key model includes user attribute information, contract protocol ID, and timestamp. Introduce an ageing mechanism for private key request, publish, and signature applications. Ensure the feasibility of the cloud electronic signature.

3. Technical solutions
In e-commerce and financial services, Hash values of important data and files are distributed and stored in the blockchain. Compare the hash value of the file with the hash value stored in the blockchain, and determine whether the files are consistent. Through the distributed nodes of the blockchain, trace the data source, event, time, location, etc., of the signature behavior. Reliable electronic signatures are achieved using the signature behavior evidence chain stored in the blockchain. The combination of blockchain technology and electronic signature technology supports the authenticity and credibility of each service, and provides trusted blockchain technology services for the business.

The solution consists of three key technologies, blockchain technology, identity-based cryptography and electronic signature technology. With the three technology convergence applications, it has the characteristics of lightweight, support massive users, simple key management and flexible key applications. Identity-based cryptography supports identity authentication, digital signatures, and privacy protection for electronic contracts.

Mobile electronic signature, providing authentication, signature, encryption and other related services through the SDK, suitable for large-scale financial assets, supply chain finance, credit, bidding procurement, etc. Electronic signature, combined with blockchain anti-tampering and nonrepudiation distributed ledger features, solves the problem of trust mechanism among multi-party entities, and further supports trusted blockchain technology services.

4. System structure
The Trusted Blockchain Alliance Chain provides certification and evidence collection services for important documents such as contracts and agreements. Cryptographic system provides the identity identification and cryptography service.
The system includes the following modules, as Fig.1 shows:

1. Cloud cryptography platform: A platform that supports identity and cryptography technology based on the cloud computing platform.
2. Blockchain platform: Provides blockchain related function, such as consensus mechanism, smart contract, distributed ledger, etc.
3. SDK: Provides services interfaces such as authentication, signature, and encryption.
4. Application system: includes APP and cloud, Realizing data signature, verification and distributed ledger through SDK call.
   
   All contract data are signed and encrypted, and the corresponding key operations are records in the distributed ledgers.

5. Technology Architecture

The technical architecture design of the whole system follows the layered design idea of the overall application framework design. From the underlying environment to the top-level service, the overall framework of the platform is divided into five levels, namely the cloud platform infrastructure layer, the base layer, the operation layer, application interface layer, and presentation layer.

5.1. Cloud Platform Infrastructure layer

The cloud computing physical environment that carries the blockchain and cloud electronic signature system includes various types of host servers, storage devices, routing devices, switching devices, security systems, and supporting system software.

5.2. Base layer

The blockchain base platform includes base functions such as consensus mechanisms, encryption algorithms, and distributed ledgers.

Identity-based cryptography base platform, including identity-based cryptography algorithms, trusted timestamp, key management systems, user service platforms, mobile electronic signature systems, and operation and maintenance management platforms.

1. Cryptography machine: provides key generation and cryptographic operation support for cryptographic algorithms for business applications.
2. Key management system: Provides key lifecycle management including key generation, storage, destruction, backup, recovery, and issuance.
3. Trusted timestamp: offers a trusted time source for key generation and contract signing.
4. Mobile electronic signature system: offers mobile terminal cryptographic algorithm.
5. Operation and maintenance management system: Provides cryptography application situation awareness, log management, and visual operation and maintenance.
5.3. Operation layer
The blockchain offers smart contracts function.

The cryptographic platform provides cryptographic operations for business systems, including asymmetric encryption and decryption, symmetric encryption and decryption, digital signature and verification, digital envelope encapsulation, HASH operations and random number generation, and time stamping. The cryptographic operation layer provides cryptographic operations support for identity authentication, key application, and electronic contract signing of business systems.

5.4. Application interface layer
The interface layer provides application interfaces. The business system can implement identity authentication, electronic contract encryption and decryption, asymmetric encryption and decryption, symmetric encryption and decryption, digital signature and verification, digital envelope encapsulation, HASH operation and random number generation, evidence collection and blockchain certification by calling API.

5.5. Display layer
The final form of service for users, including support for android, iOS APP and PC.

6. Process
Based on blockchain technology, identity-based cryptography algorithm and electronic signature technology realize the signing of electronic contracts and the verification and evidence collection of important documents. Identity-based cryptography and electronic signature technology can achieve data integrity, privacy, and nonrepudiation. The blockchain technology can record the data of the whole process, the whole transaction of the operation, and the records cannot be falsified. All data is shared by all nodes of the whole network, the information in the network space is more transparent, and the behavior is more traceable. A complete and compliant contract signing process and data certification is achieved.

The key processes are described below:
(1) Identity authentication: When the user logs in, the identity needs to be verified, and the identity verification mechanism is used.
(2) Key application: After identity authentication, the system applies for an identity-based cryptography key from the platform.
(3) Content encryption and signature: After obtaining the key, the content of the contract is encapsulated by the digital envelope method using the identity-based cryptography algorithm.
(4) Distributed ledger storage: The key processes, such as key application, signature, encryption, and hash values of important files, are all stored in the chain for inspection.
(5) Decryption and verification.
(6) Realize evidence collection and certification of important documents.

7. Application interface
The API interface provides platform services support for applications, including blockchain platform certification, signature service, key management interface, and cryptographic operation interface.

The key management interface and the cryptographic operation interface are used for user key application, service signature, contract verification, encryption protection of service data, and data decryption on the chain.

The blockchain platform provides API interfaces for upper-layer applications, including distributed ledger API and smart contract API, which are used to implement interaction between business application and blockchain platform.
8. Application

8.1. Data certification
In the growing number of internet disputes, the role and significance of electronic certifications have gradually emerged. In traditional justice, electronic evidence is difficult to accept. Traditional data tampering can cause electronic data to be destroyed, contaminated, and modified, so affects the judgment of facts. Using the characteristics of the blockchain to solve the problem of difficulty in collecting electronic evidence. In the scenarios of intellectual property, electronic contracts, financial services, etc., the application of blockchain enhances credibility.

8.2. Data forensics
The blockchain certification proves that the electronic data has not been tampered after being stored in the blockchain. Which proves the timestamp and integrity of the electronic data. The question of the validity of traditional electronic data is often because the forensic technology and the forensic environment are not credible. The blockchain technology guarantees the electronic data storage stage. Improve the credibility of evidence confirmation and evidence forensics.

8.3. Highly trusted applications
The internet e-commerce platform, financial institution, judicial institution, and electronic certification agencies jointly build blockchain alliance chains. The agencies store electronic evidence in e-commerce, financial services, and judicial services in blockchain nodes, which return the certification number. Determine the authenticity, completeness, time of certification of electronic evidence, and establish highly trusted alliance applications.

8.4. Convergence application of blockchain and electronic signature technology
Using the mobile phone as a private key medium, the security and qualification requirements of cryptography and security products can reach the security level of the traditional hardware shield, and achieve the effect of free additional media. The identity information of the user's real name authentication, and the public key, are stored in the blockchain, and the identity of the user is endorsed by multiple institutions.
After the user signs the electronic file with the private key, the signature process, result, and context are stored in distributed ledger. Thereby construct a technical system for reliable electronic signatures and trusted data, greatly improve convenience, and complete electronic signing with security and low cost.

9. Conclusion
The signing of electronic contracts and the certification of important documents are realized by utilizing blockchain, identity-based cryptography and electronic signature technology. Blockchain technology can realize the data distributed ledgers through the entire system nodes, the whole processes, and the entire transactions. Identity-based cryptography and electronic signature technology can achieve data integrity, privacy, and nonrepudiation. All data is shared by all participating nodes, the information in the cyberspace is more transparent, and the behavior is more traceable. A complete and compliant contract signing process and data certification is achieved.

Acknowledgments
This work was supported by the science and technology project of State Grid Corporation of China under the Grants No. 9900/2018-72003B, deepening research and application of blockchain platform project of State Grid E-commerce.

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 – Specification for Chinese Linux Application Programming Interface (API) ”. Email, zhuxx@pku.org.cn.

References
[1] Akter S, Wamba S F. Big data analytics in E-commerce: a systematic review and agenda for future research [J]. Electronic Markets, 2016, 26 (2): 173-194.
[2] Matsumoto S, Reischuk R M. IKP: Turning a PKI around with decentralized automated incentives [C] // Security and Privacy (SP), 2017 IEEE Symposium on. IEEE, 2017: 410-426.
[3] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts [C] // 2016 IEEE symposium on security and privacy (SP). IEEE, 2016: 839-858.
[4] Xingxiong Zhu, Qingsu He, Shanqi Guo. Application of block chain technology in supply chain finance [J]. China's circulation economy, 2018,32 (03): 111-119.
[5] McCabe A D, Gonser T H. Systems and methods for distributed electronic signature documents: U.S. Patent 8,949,706 [P]. 2015-2-3.
[6] Idzik J S, Mercea C, Fergusson A A. System and method of authentication of an electronic signature: U.S. Patent 9,280,219 [P]. 2016-3-8.
[7] Ben-Othman J, Saavedra Benitez Y I. IBC-HWMP: a novel secure identity-based cryptography-based scheme for Hybrid Wireless Mesh Protocol for IEEE 802.11s [J]. Concurrency and Computation: Practice and Experience, 2013, 25 (5): 686-700.
[8] Li J, Li J, Chen X, et al. Identity-based encryption with outsourced revocation in cloud computing [J]. Ieee Transactions on computers, 2015, 64 (2): 425-437.