Introduction

With the development and popularization of information technology, electronic contracts have gradually replaced paper-based written contracts in the process of enterprise resource management, which plays an increasingly important role. According to the relevant provisions of China’s “Contract Law” and “Electronic Signature Law”, electronic contracts mainly refer to: Agreement between two parties or multi-party transaction parties in the form of electronic data regarding the establishment, alteration, and termination of property civil rights and obligations. Compared with traditional paper contracts, the time, place, and form of signatures of electronic contracts have changed. The legal system brings shocks and challenges. William C Maloney and Mark A Singleton [1] give a system which provided for controlling, real-time logging, and archiving complex commercial transactions such as the purchase and financing of an automobile. J. Reed Smith et al. [2] examine a model of supply chain contracting with a purchaser that desires to acquire as much of a product as possible by a low price.

The above literature has studied the legal validity of electronic contracts, the time and place of signing, and the supervision of electronic contracts. However, the contracting parties of the electronic contract are all data user identities. Because of the transmission of electronic data, user fraud and contract modification challenge the authenticity and legality of the electronic contract, which seriously affects the fairness and security of online transactions. Therefore, when signing an electronic contract, it is necessary to protect the interests of both parties fairly. How to prevent traders from denial and counterfeiting and prevent data from being tampered with will be of great significance.
2. The Problems Faced by Electronic Contracts
Compared with paper contracts, electronic contracts have undergone major changes in the signing environment and signing methods. There are also the following three problems in the way of online electronic contract transactions.

2.1. The Identity of Contracted User is Used Fraudulently
In the process of concluding a traditional paper contract, the contracted user determines the rights and obligations of both parties by signing or stamping on the written contract in person. Electronic contract offers and commitments are transmitted in the form of electronic data, and its establishment, change, and termination do not require paper written forms. If the contractor has the only corresponding user data (user name + password) on the Internet, the intention is expressed through "user name + password". When the contractor has no intention to disclose information or is hacked by a hacker using a database collision attack method, it is illegal to implement theft and modification of user information. In order to enhance the security identification of the user's identity, the combination of the USB Key and the user's password is currently used to store the digital certificate. It corresponds private key in the security area of the USB Key chip, which ensures the information security of the user's identity to a certain degree. However, Chen et al. [3] pointed out that a variety of attacks against USB hardware interfaces have appeared, causing related systems to face serious security risks. As an important part of the USB Key, the security chip is an intruder Using semi-invasive attacks, differential energy attacks, laser attacks and other attack methods [4], it is possible to crack the digital certificates and corresponding private keys it stores, so there is a risk that the USB Key will be cracked and copied. Intruders can therefore use the identity of the contracted user to perform abnormal signing operations. As a result, there are signing risks and disputes.

2.2. Tampering with Electronic Contracts Easily
Electronic contracts are usually displayed in the form of data messages, through the electronic data exchange (EDI) of computer networking, the standard agreement of Internet is used to electronically transmit and reach the rights and obligations of both parties. The carrier for concluding electronic contracts is different from traditional contracts. Unlike traditional paper contracts, electronic contract information is stored electronically in a carrier such as a computer or disk, and its modification, transmission, and storage are all carried out in the computer. Electronic data has the characteristics of intangibility and easy modification. In order to ensure the safe transmission of electronic contract data, the common encryption method is the symmetric encryption algorithm, which has the advantages of high efficiency, high performance and flexibility. The symmetric encryption algorithm is used to encrypt and transmit the electronic contract information, but the symmetric encryption key may be cracked. When the key is cracked by the attacker, the content of the transmitted electronic contract data will be intercepted and tampered by the attacker, which will undoubtedly cause damage to the legitimate rights and interests of the transaction subject.

2.3. Evidence of Electronic Contract
With the transformation of the contract from paper to electronic form in the process of enterprise resource management, the signing form becomes more efficient and faster. At present, most third-party electronic contract platforms provide electronic contract signing services for both contract parties. The digital watermark technology and electronic signature technology used by them lack the supporting management of regulatory agencies. It is difficult for third-party platforms to effectively guarantee the integrity and reliability of electronic contracts. The main body of both parties may have disputes due to the content of the electronic contract. Unlike the proof of traditional contracts, the so-called "electronic contract" in the form of ordinary data messages needs to be judicial evidence. To become a judicial evidence, the data message needs to be accompanied by a notary agency for evidence collection, custody, and identification in accordance with judicial regulations. By determining the security of the electronic contract signing environment, the time and credibility of the
establishment of the electronic contract, the process is cumbersome and costly. And the result of the proof may not be approved by the court, which will affect the validity of the electronic contract evidence [5].

In summary, the identity fraud of electronic contract users, the falsification of electronic contracts, and the complexity of electronic contract forensics have restricted the widespread application of electronic contracts. For both parties to the online transaction, how to ensure that the identity of transaction subject is true and credible, that the electronic contract is true and complete, and that the electronic contract can be easily verified has become a key issue which needs to be resolved. This article will combine identity authentication technology, reliable digital signature technology, and blockchain ledger technology to design and implement an electronic contract service platform. The platform realizes the certainty of trader's identity, the non-repudiation of information sent, the confidentiality of information transmission, the integrity of data exchange, and the speed of complete evidence chain query, thereby ensuring the security and fairness of the platform.

3. Design Principles of Electronic Contract Platform

3.1. Basic Model of Electronic Contract Platform

Under the premise of ensuring strong user identity authentication and electronic contract verification services, a basic model of the electronic contract platform is given. This model describes the overall process for users to use the platform, as shown in Figure 1.

As a service platform for signing electronic contracts, its main users are contracted users and verifiers. The contracted user refers to each transaction party related to the contract, and completes the uploading and signing operations of the electronic contract through the transmission interface. The verifiers mainly provide the electronic contract verification and notarization services through the electronic contract signing process data information stored in the block ledger subsystem. Among them, the contracted user needs to perform identity authentication when logging in to the platform, and verify that the user account is used by himself, which effectively prevents the identity of the contracted user from taking risks. The electronic contract is encrypted by digital signature technology to ensure the security of the electronic contract transmission. The block ledger subsystem only records the process information of the electronic contract signing, and does not involve the content of the electronic contract, so as to achieve the confidentiality of the electronic contract. In addition, the platform also includes system administrators, which mainly perform daily monitoring and maintenance of the system.
3.2. Design Principles of Electronic Contract Platform

In order to ensure the fairness and security of the electronic contract platform, solve the problems of the identity of the contracted user, the electronic contract has been tampered with, and the contract cannot be verified. This paper builds a signing platform based on a combination of software and hardware identity authentication subsystem, encrypted transmission of electronic contracts, and block ledger. The specific design principle is shown in Figure 2.

![Design principles of electronic contract platform](image)

**Figure 2.** Design principles of electronic contract platform.

3.2.1. Identity Authentication Subsystem. The electronic contract signing method has changed from traditional face-to-face signing to online signing. "User name + password" has become the online identification credential of the user's identity. When intercepted by hackers or the user's own unintentional disclosure, identity fraud is used to sign the electronic contract. The electronic contract disputes caused will undoubtedly affect the application efficiency of the contracted platform. Therefore, the identity authentication subsystem based on the FIDO protocol and the physical unclonable function (PUF) is designed as the second factor of user identity authentication. After the "password" authentication is passed, the second authentication of the authentication token is performed, thereby effectively ensuring the unique correspondence between the data user and the physical user.

The identity authentication subsystem uses a combination of software and hardware authentication, where the interaction between the hardware and the server is developed based on the FIDO U2F protocol with national secret algorithm (SM2/SM3/SM4), and the physical non-cloning technology (PUF) [6] integrated in the authentication token, fully guarantee the non-copyability of the authentication token. It is mainly divided into two parts: user registration protocol and user authentication protocol.
The chip of the hardware device adopts the national secret security chip, which fully guarantees the unbreakability of the hardware data information. At the same time, in order to enhance the replication resistance of the hardware device, the token supports physical non-cloning functions to ensure that the user has the uniqueness of the device. The technical principle of PUF is to generate encrypted "random differences" introduced by the integrated circuit in the hardware chip due to process limitations during the manufacturing process. The PUF response signal is automatically generated when the device is powered on, and when the device is powered off, the response signal is automatically annihilated. By using the physical unclonable function algorithm, the unique digital fingerprint information of the hardware chip is extracted under power-on, and the extracted encryption information (root key) is used to encrypt the signature key or decrypt the key handle. The authentication token has physical characteristics of the chip cannot be copied and the root key is generated at power-on, and the authentication token does not store the signature public key, key handle and root key information, which can fundamentally guarantee the non-copyability of the token.

3.2.2. Electronic Contracts Subsystem. Electronic contracts are transmitted using digital signature technology to prevent them from being intercepted and tampered with during the transmission process. Due to the length of the contract, the hash technology is used to compress the files to be transmitted into fixed-length hash values before encryption. At present, the most hash functions used commonly are SHA1 and MD5, 128-bit or longer. Its working principle is using hash function to hash a variable-length string into a fixed-length hash value, even if the string changes difference smally, the generated hash value will also be different. The hash function can be used to associate the search term with the index value to generate a hash table that is easy to search. This hash function is a one-way irreversible calculation method. From a fixed-length hash value, it is basically impossible to restore it to the original one. This allows the hashing technology to ensure the integrity of the document information, and the hash value comparison can effectively check and detect whether the electronic file has been tampered with.

This platform uses the encryption algorithm RSA and AES mixed encryption system [7] to transmit interface data, and uses the SHA256 hash algorithm to verify the integrity of electronic contracts, effectively ensuring that electronic contracts are not tampered with, and achieving data transmission security. The process is shown in Figure 3.

**Figure 3.** Electronic contract encrypted transmission process.

The signing sender User1 calculates the electronic contract information $F$ using the SHA256 algorithm to obtain a hash value $H_1$. We can generate the symmetric key $E$ according to the predetermined AES random algorithm or random number table. Then we use the high-efficiency encryption feature of $E$ to encrypt the electronic contract $F$ to obtain $F^1$. In order to ensure the
security of the AES key $E$ and hash $H_1$, we use the RSA public key received to encrypt $E$ and $H_1$ to obtain the encrypted information $E_1$ and $S$ respectively. The receiver $User_2$ uses RSA private key to decrypt information received to obtain $E$ and $H_1$ one by one. He calculates the digital signature $F_1$ to obtain the electronic contract $F$, and uses the SHA256 algorithm to calculate the new hash value $H_2$ of the electronic contract. If $H_1$ and $H_2$ are consistent, the electronic contract is transmitted securely. Otherwise, it will prompt that the electronic contract has been tampered with.

After the electronic contract is signed by both parties. The block ledger server uses digital signatures to digitally sign the electronic contract, uses the SHA256 algorithm to generate a new hash value, and together with the basic information of the contracting parties, generates block data and distributes it to the block ledger database. The digitally signed electronic contract is distributed to the business database.

3.2.3. Block ledger subsystem. An electronic contract is an agreement between two parties or multi-party transaction parties in the form of electronic data regarding the establishment, alteration, and termination of property civil rights and obligations. Electronic contracts and paper contracts have the same legal effect. If the contracting parties have contract disputes that cannot be resolved through negotiation, contract verification and litigation may be required.

We store the electronic contract process data as blocks, and each block is linked as a blockchain; the block body stores the original data. The block ledger includes data such as block headers, contract transaction details, transaction counters, and block size, as shown in Figure 4.

The block header contains all information except the contract transaction information. It mainly includes:
- previous block head hash value, which is used to ensure that the blocks are connected in sequence;
- time stamp, record the generation time of the block;
- random array, the number of random arrays and the generation algorithm are defined in advance;
- transaction counter, record the number of transactions contained in each block;
- block size, record the size of each block of data, each block is currently limited to less than 1MB.

The main body of the block is the contract transaction details, which mainly records key information such as transaction participants, transaction time, digital signature, and contract hash value, which is used to verify the authenticity and integrity of the contract and has not been tampered with.

![Figure 4. Block data structure diagram.](image-url)

4. Conclusion
This article proposes an electronic contract platform based on block ledgers, which ensures the fairness and security of the platform through user identity authentication, data transmission encryption,
and block storage during the signing process. Introduce the blockchain storage format and the underlying cryptographic technology to form a daily contract transaction into a block, and use the signature information to link the blocks to form a chain relationship. Changing the data of one block in this way must affect the entire chain behind. When an attacker needs to tamper with a block, in addition to obtaining encryption machine decryption authority and database operation authority, it must spend a lot of time to reconstruct the entire chain. At the same time, the identity authentication is strengthened through the second factor of identity, which effectively guarantees the non-counterfeiting and non-replicability of the contracted users. The data encryption ensures the transmission of the electronic contract network. The block account book guarantees that the signing process can be traced back and the electronic contract can be verified. We provide a convenient way for Internet transactions of enterprises.

Acknowledgments
Corresponding author is Ma Feng. Email: mafeng1@sgepri.sgcc.com.cn.

References
[1] Maloney W C and Singleton M A 2018 Transaction automation and archival system using electronic contract disclosure units [P] US9916018,2018-03-13.
[2] Smith J R, Yost F, and Lopez H 2020 Electronic data interchange and enterprise resource planning technology in supply chain contracts Computers & Industrial Engineering 142(04) 106330.1-106330.12.
[3] Chen X, Huang Z, and Yu J 2020 Research on safety test methods for USB interface Communication Technology 53(01) 251-5
[4] Zhang J Y and Chen Q M 2014 Security chip penetration test evaluation based on attack tree Computer Engineering 2014(06)115-119+124
[5] Xia Q F 2019 Application Proposition of Blockchain Smart Contract East Methodology 2019(03) 30-43
[6] Liu W Q, Cui Y J, Wang C H 2016 Design and implementation of a low-cost physical unclonable function structure and its RFID application Acta Electronica Sinica 2016(07) 1772-6
[7] Xiao Z J, Hu C, Jiang Z T, Chen H 2014 AES and RSA algorithm optimization and its mixed encryption system Computer Application Research 2014(04) 1189-1194 +1198