Application and Research of Hard Wallet Business Based on Smart Contract Technology

Tong He*, Yimeng Li, Yongjie Li

State Grid Huitongjincai(Beijing) Information Technology Co., Ltd., Beijing 100053, China

*hetonghb@163.com

Abstract. The application of smart contract technology in the field of cryptocurrency has attracted extensive attention. A hard wallet is a device for storing encrypted money, and its private key is usually stored inside the device. However, there are still some challenges in the security and reliability of hard wallets, such as the damage, loss or theft of equipment. Smart contract technology can provide a new method to enhance the security and reliability of hard wallet. This paper introduces the application and research of hard wallet business based on smart contract technology. Firstly, the basic concept and principle of smart contract technology and its application in the field of cryptocurrency are introduced. Secondly, the basic principle and existing security risks of hard wallet are discussed. Then, a hard wallet solution based on smart contract technology is proposed, and the design and implementation of the solution are introduced in detail. Finally, through the test and evaluation of the scheme, it is proved that the scheme can effectively improve the security and reliability of the hard wallet.

Keywords: Smart contracts; Hard wallet; Blockchain

1 Introduction

Intelligent contract technology is a programming method based on blockchain technology, which can realize programmable and automatic transactions and protocols in decentralized networks. Smart contract is a special program in essence, which is composed of a series of predefined code logic and rules, and can be deployed and executed on the blockchain. The core idea of smart contract is to write the contract terms and rules into the blockchain in the form of code, so as to realize automatic execution, verification and execution of the contract terms. Smart contracts can realize all kinds of complicated transactions and agreements, such as digital currency transactions, voting, insurance claims, supply chain management, etc., without the need of a third party organization. At the same time, smart contracts can also avoid errors and disputes caused by human factors and improve the reliability and security of transactions. The language and programming tools used in writing smart contracts are similar to traditional software programming, such as Solidity, Vyper, etc. After writing, the smart contract can be deployed and executed on the blockchain. In the execution process, the smart contract will automatically verify the conditions and rules in the contract, and automatically

C. Chen et al. (eds.), *Proceedings of the 3rd International Conference on Digital Economy and Computer Application (DECA 2023)*, Atlantis Highlights in Computer Sciences 17,
https://doi.org/10.2991/978-94-6463-304-7_6

perform corresponding operations according to the code logic in the contract, and finally save the transaction results to the blockchain [1]. Intelligent contract technology can realize programmable and automatic transactions and protocols, thus improving the reliability and security of transactions. Smart contracts have been widely used in digital currency, finance, supply chain management and other fields, and have a very broad development prospect. Compared with traditional contracts, smart contracts have many advantages, as shown in Table 1:

Table 1. Comparison between Smart Contract and Traditional Contract

Comparative dimension	Smart contract	Traditional contract
Automation dimension	Automatic judgment trigger condition	Manual judgment trigger condition
Subjective and objective dimensions	A request suitable for objectivity	A request suitable for subjectivity
Cost dimension	Low cost	High cost
Execution time dimension	Pre-prevention	Ex post facto execution
Penalty dimension of breach of contract	Rely on mortgage assets	Depend on punishment
Scope of application dimension	Globality	Limited by specific jurisdictions

Smart contract technology is a blockchain based programming technology that allows automatic execution of contracts without intermediaries. The smart contract uses a decentralized computer network, such as Ethereum, to ensure the security and transparency of the contract. The following are some common uses of smart contract technology:

1. Decentralized finance (DeFi): Smart contracts can be used to build decentralized financial applications, such as lending platforms, decentralized exchanges (DEX), Stablecoin and asset management tools. These applications allow users to borrow, trade, and invest without traditional financial institutions.

2. Supply chain management: Smart contracts can be used to improve the transparency and traceability of supply chain management. By recording transactions and information in the supply chain on the blockchain, real-time tracking, verification, and automatic execution of contract terms can be achieved, thereby reducing fraud, reducing costs, and improving efficiency.

3. Digital identity verification: Smart contracts can be used to build a secure and reliable Digital identity verification system. By recording personal identity information on the blockchain and using smart contracts to verify identity, Identity theft and fraud can be reduced and better personal data privacy protection can be provided.

The principle of smart contract technology is based on the decentralization and non-tampering of blockchain technology. The emergence of blockchain is accompanied by bitcoin. As the foundation and underlying technology of Bitcoin, blockchain is a distributed data storage mode and a public account book for storing encrypted currency transaction records. In the White Paper on the Development of Blockchain Technology and Application in China issued by the Ministry of Industry and Information Technology in 2016, it was pointed out that blockchain, as the underlying and basic technology

of digital currency such as Bitcoin, has a wide range of application modes. This technology realizes the storage or operation of data in the distributed computer network, the whole network records, traceability and tamper-proof, thus improving efficiency and reducing costs while ensuring safety. So far, blockchain technology has roughly experienced three development stages, as shown in Figure 1.

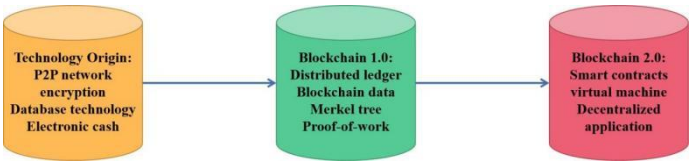

Fig. 1. Evolution Path of Blockchain

From the perspective of the evolution path of blockchain, if blockchain 1.0 is represented by Bitcoin and focuses on solving the decentralization problem in the process of monetary payment, then blockchain 2.0 is to decentralize the whole market more macroscopically and create the value of different assets through conversion. The decentralized ledger function of blockchain technology can be used to create, confirm and transfer various types of assets and contracts. Smart contracts based on blockchain technology can not only give full play to the advantages of smart contracts in terms of cost efficiency, but also avoid the interference of malicious behaviors on the normal execution of contracts. Digitize the content in the smart contract in the form of coding and write it into the blockchain. The characteristics of blockchain technology ensure that the whole process of storage, reading and execution is transparent, traceable and tamper-proof. At the same time, a set of state machine system is constructed by the consensus algorithm of the blockchain, so that the smart contract can run efficiently [2].

On the blockchain, all transactions and records are open, transparent and cannot be tampered with, and every participant can see the details and information of all transactions. Through intelligent contract technology, the terms and rules of the contract can be written into the blockchain in the form of code, and the corresponding operations can be automatically performed when the contract meets certain conditions. Smart contracts can realize all kinds of complex transactions and agreements, such as payment, voting, proof, etc., without intermediaries. Intelligent contract technology is widely used in the field of cryptocurrency. The following are several common application scenarios: issuing tokens, and smart contracts can be used to issue tokens, such as ERC-20 standard tokens. The smart contract for issuing tokens defines the attributes and behaviors of tokens, including the total amount, name, symbol, transfer and other functions of tokens. Once the token is issued, it can be traded and transferred on the blockchain. Automated transactions, smart contracts can be used for automated transactions, such as transactions in decentralized exchanges. Smart contracts can automatically execute buying and selling orders and match them according to preset rules and conditions. Users of the exchange can trade directly through smart contracts without trusting the exchange or intermediaries. Voting and governance, smart contracts can be used for voting and governance, such as DAO (decentralized autonomous organization). DAO's voting and governance decisions are made through smart contracts, and every DAO

member can participate in voting and governance. This decentralized governance model avoids the problems of single point of failure and centralized power, making decision-making more democratic and fair. Digital identity, smart contracts can be used to create digital identities, such as ENS (Ethereum Domain Name Service) on Ethereum. ENS can bind an Ethernet address to an easy-to-remember domain name to realize decentralized naming service. ENS smart contract can guarantee the one-to-one correspondence between domain names and addresses, and at the same time realize the transfer and transaction of domain names [3].

These application scenarios are just the tip of the iceberg of smart contract technology in the field of cryptocurrency. With the continuous development and improvement of smart contract technology, more application scenarios will emerge. In a word, the intelligent contract technology realizes the automatic execution of contracts by taking advantage of the decentralization and non-tampering of blockchain technology, improves the reliability and security of transactions, and has broad application prospects.

2 Hardware wallet principle and existing security risks

Hardware wallet is a kind of cryptocurrency storage device. Its basic principle is to store the private key of cryptocurrency in offline devices to ensure that the private key will not be attacked by hackers or infected by viruses. Hardware wallets usually use special chips to store private keys. These chips are strictly tested and certified, and have the characteristics of tamper resistance, encryption and safe storage. Users can use the hardware wallet to manage and transfer their cryptocurrency assets, and communicate with the blockchain network by connecting the hardware wallet to the Internet to realize the operation of trading and transferring cryptocurrency. Although hardware wallets have obvious advantages in providing security, they still have some security risks. One of the risks is that the hardware wallet is stolen or lost. If the user's hardware wallet is stolen or lost, they will not be able to access their cryptocurrency assets because the private key is only stored in the hardware wallet [4-5]. Therefore, users need to take good care of their hardware wallets and take necessary measures to prevent the risk of theft or loss. Another risk is the software vulnerability in the hardware wallet. Although hardware wallets usually use dedicated chips and operating systems to protect private keys, they may still have software vulnerabilities or security vulnerabilities. Hackers can exploit these vulnerabilities to steal users' private keys and encrypted currency assets. Therefore, manufacturers of hardware wallets need to constantly update their firmware and software to fix known vulnerabilities and timely fix newly discovered vulnerabilities. Generally speaking, hardware wallet provides a relatively safe way to store and manage cryptocurrency assets. However, users still need to take necessary measures to prevent the risk of theft or loss of their hardware wallets, and choose trusted and reliable hardware wallet brands to minimize the possibility of security risks (Figure 2).

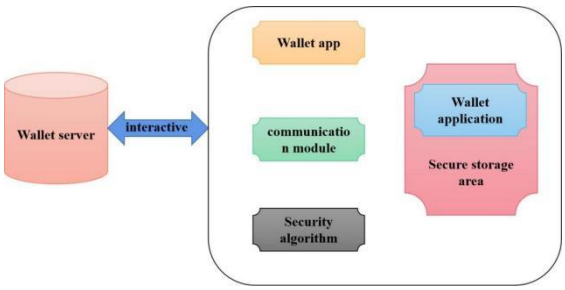

Fig. 2. A method for upgrading digital currency hardware wallet application.

3 Hard Wallet Solution Based on Smart Contract Technology

The hard wallet solution based on smart contract technology is a secure storage solution that combines smart contract and hardware wallet. By combining smart contracts with hardware wallets, it enables users to store and manage encrypted assets more safely. The basic principle of this solution is to store the user's private key in the hardware wallet and deploy the smart contract code to the blockchain network [6]. When users need to execute a transaction, they need to authenticate through the hardware wallet and sign the transaction. The smart contract will check the legitimacy of the transaction and submit it to the blockchain network for execution. The advantage of this solution is that it stores the private key in the offline device, which greatly reduces the risk of the private key being stolen or leaked. At the same time, the deployment and implementation of smart contracts can ensure the security and reliability of transactions. However, the hard wallet solution based on smart contract technology also has some security risks. For example, there may be loopholes or errors in the smart contract code itself, which may lead to the theft or loss of assets. In addition, the speed of smart contract execution may be affected by the congestion and transaction costs of blockchain networks. Therefore, when using the hard wallet solution based on smart contract technology, users need to carefully evaluate its security and reliability, and take necessary measures to protect their assets.

4 Testing and evaluation

Suppose there is a hardware wallet based on Ethereum, and the smart contract is used to realize the secure transfer function. This hardware wallet has a button to confirm the transfer operation. When users want to transfer money, they need to connect the hardware wallet to the computer and use their private key for authentication. Then, they can enter the receiving address and amount on the computer and press the button on the hardware wallet to confirm the transfer. After the confirmation button is pressed, the smart contract will automatically verify the user's identity and transfer information. If all the conditions are met, the smart contract will perform the transfer operation and

transfer the funds from the user's account to the receiver's account. In this process, the user's private key will be kept in the hardware wallet and not exposed to the network, which makes it very secure [7]. The following is an example of testing and evaluating a hard wallet solution based on smart contract technology:

Security testing: Security testing of the hardware wallet, including attack simulation test, to test whether the hardware wallet can resist the risk of hacking and stealing private keys. During the test, many kinds of attack methods are used, such as side channel attack, violent cracking and so on. The test results show that the hardware wallet can effectively protect users' private keys and encrypted monetary assets, and the security is very high.

Function test: Test whether the functions of the hardware wallet, including the transfer function and other functions (such as reminders and restrictions) can work normally. The test results show that the function of the hardware wallet is normal and the transfer operation is fast and accurate [8-9].

Compatibility test: Test whether the hardware wallet is compatible with various operating systems and software platforms. During the test, different operating systems and common wallet software are tested. The test results show that the hardware wallet can be compatible with many operating systems and wallet software.

Performance test: test the performance of hardware wallet, including the speed of transfer operation and network delay. The test results show that the transfer operation is fast, the network delay is small, and the battery life and reliability are good.

User experience test: Test the user experience of hardware wallet. The test results show that the hardware wallet provides an intuitive and easy-to-use interface, and users have no difficulty in connecting and using the hardware wallet.

Evaluating the effectiveness of the hard wallet solution based on smart contract technology, considering the above factors, the solution has the following advantages: high security, the hardware wallet adopts smart contract technology, which can effectively protect users' private keys and encrypted monetary assets, and the security is very high. Good scalability, hardware wallet supports a variety of cryptocurrencies, and can quickly adapt to the new cryptocurrencies in the market. Easy to use, the hardware wallet provides an intuitive and easy-to-use interface, so that users can quickly and easily complete operations such as transfer. High cost-effectiveness, moderate price of hardware wallet, and high cost performance, which meets the needs of users. Strong community support, the hardware wallet solution has a strong community support, users can quickly get help and support [10].

5 Conclusion

Smart contract technology can bring many advantages to the application of hard wallet business. Hard wallet is a device for storing and managing encrypted money, and its security and privacy are very important for the security of users' assets. Smart contract technology can bring the following advantages to the hard wallet business:

Higher security: Smart contracts can be executed in hardware devices to ensure the security and privacy of encrypted currency. This is more secure than the software wallet, because the software wallet is stored on the Internet and vulnerable to hacker attacks.

More transparency: Smart contracts can provide transparency in transactions, so that users can track the transaction records of their cryptocurrencies. This allows users to manage their assets with greater confidence.

More convenient: Smart contracts can realize automatic transaction processing, eliminating the need for manual intervention and improving the speed and efficiency of transactions.

More reliable: Smart contracts are executed by nodes in the network, which means there is no single point of failure. This makes smart contracts more reliable than traditional centralized systems.

In a word, smart contract technology can bring higher security, transparency, convenience and reliability to hard wallet business applications. With the continuous development of blockchain technology, the application and research of hard wallet business will be more widely used and developed.

Acknowledgements

The work described in this paper was supported by a grant from Technology Project of State Grid Corporation of China (No. 1700/2022-87001A)

References

1. Liu, C. G. , Bodorik, P. , & Jutla, D. . (2022). Automating smart contract generation on blockchains using multi-modal modeling. Journal of Advances in Information Technology(3), 13.
2. Chen, H. . (2022). Application of blockchain technology in environmental health: literature review and prospect of visualization based on citespace. Technologies, 10.
3. Abuidris, Y. , Kumar, R. , Yang, T. , & Onginjo, J. . (2021). Secure large-scale e-voting system based on blockchain contract using a hybrid consensus model combined with sharding. ETRI Journal, 43(2).
4. Kang, Y. , & Li, Q. . (2021). Design and implementation of data sharing traceability system based on blockchain smart contract. Scientific programming(Pt.11), 2021.
5. Ziar, R. A. , Irfanullah, S. , Khan, W. U. , & Salam, A. . (2021). Privacy preservation for on-chain data in the permission less blockchain using symmetric key encryption and smart contract. Mehran University Research Journal of Engineering and Technology, 40(2), 305-313.
6. Vangala, A. , Sutrala, A. K. , Das, A. K. , & Jo, M. . (2021). Smart contract-based blockchain-envisioned authentication scheme for smart farming. IEEE Internet of Things Journal, 8(13), 10792-10806.
7. Chen, C. L. , Deng, Y. Y. , Tsaur, W. J. , Li, C. T. , Lee, C. C. , & Wu, C. M. , et al. (2021). A traceable online insurance claims system based on blockchain and smart contract technology. Sustainability, 13(16), 9386.

8. Lu, B. . (2021). Smart contract for electricity transactions and charge settlements using blockchain. Applied stochastic models in business and industry, 37(3).
9. Gourisetti, S. , Sebastian-Cardenas, D. J. , Bhattarai, B. , Wang, P. , Widergren, S. , & Borkum, M. , et al. (2021). Blockchain smart contract reference framework and program logic architecture for transactive energy systems. Applied Energy, 304, 117860-.
10. Negara, E. S. , Hidyanto, A. N. , Andryani, R. , & Erlansyah, D. . (2021). A survey blockchain and smart contract technology in government agencies. IOP Conference Series: Materials Science and Engineering, 1071(1), 012026 (7pp)..