Security Mechanism Analysis of Blockchain Smart Contract in Cross-Border Trade Field

https://oajem.damray.com/

OPEN ACCESS

DOI:
Received: June 27, 2022
Accepted: July 23, 2022
Published: August 10, 2022

Ruirui Yuan

Daye Yufeng Mining Co., Ltd. Hubei, China.

Abstract

The current smart contract is a transaction program that can automatically execute prefabricated rules and treaties. In recent years, with the innovation and development of block chain technology, it has not only attracted much attention but also been widely used in various industries. Because smart contracts are independently self-validated and automatically executed in a network environment, there are many security problems. This article analyzes the potential security risks of smart contracts in block chain, and proposes a comprehensive and effective security mechanism based on actual business development scenarios, hoping to provide some help for the secure application of smart contracts in block chain in cross-border trade.

Keywords

Cross-border, Trade, Block chain, Smart contracts, Security mechanism

Introduction

In cross-border trade, there are many participants, such as domestic and foreign manufacturers, logistics providers, traders, financial institutions and government regulators, and many trade chains are involved, such as capital chain, logistics chain and data chain, and cross-border management is a key component of the blockchain smart contract. In cross-border trade, the automatic execution of smart contracts enables the business data of all participants to be shared collaboratively, and enables the transfer and delivery of the participants' rights in rem and funds across borders, so the security management of smart contracts is extremely critical. It is required to start the construction and application of smart contracts, explore the comprehensive and effective security control, and gradually form the security specification for the practical application of smart contracts, so as to provide a strong guarantee for the orderly development of

blockchain for cross-border trade transactions.

1. Application advantages of blockchain smart contracts

In fact, a smart contract is a computer program that does not require an intermediary and is capable of self-verification and automatic execution. Before the deployment of a smart contract, the logical process corresponding to each clause associated with the contract has been prefabricated, and a user interface exists for the smart contract to allow the user to interact with the prefabricated contract in real time, and the interaction requires strict compliance with the prefabricated logic [1]. Compared to traditional forms of contract content, there are many application advantages of blockchain smart contracts.

Smart contracts do not require a centralized authority to arbitrate on the compliance of their actual execution, and contract supervision and arbitration are done by computer, which can reduce the dependence on external parties.

After the deployment of a smart contract, the contents of the contract cannot be modified, which means that the parties involved in the contract cannot intervene in the execution of the contract, which can reduce the anomalies caused by malicious and accidental circumstances, that is, avoiding the risk of human intervention.

The execution of smart contracts does not require the participation of third-party authorities and central agents, so it can respond to users' demands at any time and strengthen the effectiveness of the transaction, which can reduce the human cost in the process of contract performance, arbitration and enforcement.

2. Security issues faced by cross-border trade blockchain smart contracts

2.1 Code development

In comparison with traditional programming, we can learn that there are differences in information application and business security.

When smart contracts are applied to cross-border trade, they have certain commercial logic, such as the application scenarios of cross-border trade parties, financial institutions and government regulatory departments. Commercial confidentiality and data security are very important in terms of financial institutions, governments and enterprises, and all the risks of data leakage and smart contract security risks will have an impact on the orderly operation of the alliance chain.

The deployment of smart contracts in the alliance chain has a unanimous consensus. Smart contracts in cross-border trade need to have fault tolerance, abnormal termination and other logic, and if there is a security vulnerability handling mechanism for smart contracts in cross-border trade, it needs to be supplemented and handled by the alliance parties in an agreed manner to avoid security risks at the commercial and governmental levels.

The development of the smart contract security programming specification can eliminate the problem of security risks in terms of privacy protection, traceability and auditing [2].

2.2 Deployment application aspects

Along with the continuous increase of cross-border trade alliance chain participants, the business chain also continues to increase, commercial interests, policy-driven participants, and nodes can have malicious behavior, and the open deployment of smart contracts can have many problems such as commercial data leakage and contract tampering. At the same time, the smart contract code is not developed and mature, and the generation of security loopholes cannot be circumvented in practical application. Therefore, the cross-border trade alliance chain has strict requirements in the deployment and application security of smart contracts.

2.3 Privacy protection aspect

Smart contracts must be planned and designed for the information that participants can access, such as complete access, partial access, inaccessibility, etc. Permissions need to be clearly marked based on the code.

If the smart contract logic in the cross-border trade blockchain requires the regulator to participate in it, the permission and scope of data access by the regulator need to be clear. The nature and scope of access to privacy data are static or dynamic, and how to introduce encryption parameters into the smart contract and design the permission and sharing mechanism for data access by new participants.

2.4 Leave a trace of audit aspects

Smart contracts are dynamic in nature, if the call is a non-deterministic system function, external system non-deterministic data sources, dynamic calls, etc. Smart contract design, to try to avoid its dynamic characteristics of

the application, if the system consistency is destroyed, will lead to an increase in the difficulty of the problem, which will affect the rational judgment of the cause of the failure problem.

Smart contracts must be able to be terminated, and they do not take up unlimited time and resources. Downtime is a theoretical problem that can be computed in logic and mathematics. Downtime can determine the problems related to the end of the program running in a limited time, and smart contracts can be terminated, otherwise they will generate unlimited resources and time consumption. The downtime problem cannot be predicted, and it is difficult to predict the downtime problem of a program when it is not running. In the actual implementation of audit work, auditors and security experts must judge the dead loop problem of blockchain design workers, and at the same time control the dead loop problem of smart contracts based on resource control methods, and require smart contract audit workers to make reasonable judgments and choose reasonable and effective measures to deal with the problems in terms of downtime and resource control.

3. Security mechanism of smart contracts in cross-border trade blockchain

3.1 Principles

Reasonable simplification of smart contracts can strengthen their security, effectively coordinate the relationship between business and security around the customer as the center, effectively simplify the complexity of smart contracts, make complex contracts into multiple simpler contract contents, and reduce the risk control barriers arising from complexity [3].

The security policy aspect of smart contracts needs to reduce the amount of manual processing, which consumes a lot of time to manually perform security risk processing, and needs to find a rapid expansion of related operations to achieve the goal of proper resolution of security issues. Make security measurement simpler and more transparent, develop automated tools to automatically determine risk decisions, make security policies available to each participant, and continuously optimize security decisions.

Smart contracts are similar to book contracts in real-life audits, which require multiple, rigorous reviews involving business processes, code run dynamics, testing processes, security, and expert review. For complex and large capital smart contracts, the code must be strictly reviewed and the correctness of the smart contract must be verified based on various ways.

The blockchain alliance of cross-border trade needs to issue security control standards that can be referred to by each blockchain participant, so that the content can be effectively controlled by programmers, users, managers, etc.

3.2 Development Process

Smart contract designers and security workers must clarify the requirements and security risks, and build the smart contract model based on the modeling language, which needs to be communicated and confirmed with all smart contract participants several times, based on which the preliminary design is done.

When writing smart contract code, professional smart contract writers are required to refer to the security specifications for smart savings and analyze the vulnerabilities based on audit tools. Before the smart contract is released, a comprehensive and in-depth code design is required to ensure that the code after the audit is the actual content of the smart contract applied by the user.

Smart contract testers deploy smart contracts in the test chain and test smart contracts, such as boundary, business logic and vulnerability testing, testers must clearly set test boundaries with business and security experts, analyze security results based on test results, and audit and security experts jointly issue audit reports. The content of the report involves the testing of vulnerability attacks, the existence or potential vulnerability of the contract content, and how the contract needs to be responded to, terminated and replaced after the vulnerability has occurred. The smart contract code report can clarify its generality, that is, whether the contract scenario can be reused, whether it can be applied to other smart contracts, and the need to report the status of fixes to each participant. The smart contract will be ready for release only when all participants reach consensus and approval based on the audit report, vulnerability fixes, and many other issues [4].

3.3 Security specifications

Smart contracts in cross-border trade chains need to regulate the ownership, based on the form of digital certificates to clarify the ownership of the corresponding smart contracts, based on the clear marking of the visibility of functions and state variables to clarify who can call the smart contract and who has access rights to the contract variables. Some smart contracts in cross-border trade will be called from outside, and the data called must be secure and trusted and re-

lied upon. All external calls must be set as potential security risks, and information about the level of security risk parameters must be set to the occurrence result when designing the smart contract, so that it can be used appropriately for auditing and traceability.

When dealing with the problem of errors in external calls, the return value needs to be checked, and if the use of matching, pattern verification, the return value of unsuccessful calls need to be called to deal with the contract code to take into account all the possibilities of unsuccessful calls for reasonable processing. Call specification of the agreement, can not use the return value of external calls for logic control judgment, because the results of external calls exist dangerous and uncertainty, in the important logic judgment can not call the results of external functions for logic judgment, so as to avoid the risk of double attack problem. Smart contracts based on external resource calls, its input, out of the time there will be left traces and audit and many other operational design, such as financial scenarios, smart contract application layer must be rolled back to provide and access control to ensure that the smart contract can be re-restricted to avoid the problem of security vulnerabilities.

Based on the code of the smart contract to name functions and many other identifiers, so as to meet the coding specifications, when interacting with external contracts, the code level needs to be named on the methods, contract interfaces, variables, and external contracts, external dependencies, etc., which are not clear audit, need to be clearly identified, based on clear and explicit interaction with data, smart contracts when there are security risks.

Fast failure principle, which says that before the implementation of the core logic of the smart contract, the contract entry data should be fully checked, the data content if it can not meet the rules of the contract verification, to quickly return to the failure results, so as to avoid the actual implementation of the smart contract anomalies. The fast failure principle can reduce the actual execution time of the smart contract to avoid risk problems such as stack overflow due to unknown exceptions. The design process should be aware that data checks will apply to a default value if they fail, allowing the contract to continue execution. Find unsuccessful executions as soon as possible, for example, blockchain scripting languages are often based on try syntax mechanisms to quickly locate and capture the cause of failure. To avoid the impact of inconsistent and unstable state on other callers, state, etc.

If several different functions and smart contracts need to be called in a smart contract, there will be a problem of sequential dependency to finish the internal function work first, and then make external function calls afterwards. At the same time, there are some smart contracts based on locking mechanism to call the call dependency problem, mutual exclusion lock can lock the code block, based on locking the access rights to resources for effective protection.

In the actual execution of smart contracts, transaction processing can be very different due to different transaction order, and different transaction states can lead to different output results. The smart contract problem is also the dependence of the transaction order on the contract. Malicious participants will intentionally modify the execution order of the smart contract, which will have a destructive impact on the legality of the contract, so when designing the smart contract of the cross-border blockchain, the transaction order needs to be strictly designed and verified.

Smart contracts rely on block timestamps or follow timestamps for random number provisioning, which can affect the results of executing smart contracts when there are deviations in the timestamps of network nodes. The attacker changes the result of the execution of the smart contract based on the timestamp in the blockchain timestamp to make the result favorable to himself. Therefore, if the smart contract in the cross-border trade blockchain relies only on the timestamp, the scope of the contract time error needs to be verified and multiple participants reach a consensus at the timestamp time range level so that the smart contract can be executed in an orderly manner so that the smart contract cannot be executed in an orderly manner [5].

Smart contracts differ from traditional programming in that the programming design of smart contracts requires fault tolerance and abnormal termination logic to be written into the contract. Smart contract fallback should be as simple as possible, all smart contracts need to set the fallback function, function fallback must be recorded for the fallback action, if more cumbersome fallback function is needed, test evaluation should be done first so that the fallback is not too complicated.

When designing the code of a smart contract, you want to ensure that the contract is realized by considering the boundary conditions and preparing for the adverse conditions that may arise in the actual operation of the smart contract, and if there are vulnerabilities in the smart contract, the recovery methods and processes are effectively regulated so that the smart contract can be recovered as soon as possible and safely. The fault-tolerant solution in the cross-border trade domain can provide a backup solution for all smart contracts. Fault tolerance can use the contract stop mechanism, contract management workers can use the freeze method for emergency processing, the contract stop, the need to use offline, contract amendments and other ways to compensate for business logic. In the design and optimization of the contract, the nodes affecting the contract should be considered, taking into account how to deal with the contract data. If the new contract and the old contract use the same data, after a period of parallelism with the old contract and the new con-

tract, the old contract can be closed or scrapped.

3.4 Depository audit

The security audit mechanism of smart contracts is improved, which includes the audit verification of code, depositing process, execution records, etc. Smart contracts in cross-border blockchain can be solved by using super ledger, distributed ledger, etc. If the blockchain external application needs to access the ledger, it will make a call, based on a variety of programming languages to reach the goal.

3.5 Privacy protection

Smart contracts can be based on centralized identity for identity management, which includes many functions, identity authentication, such as information registration in LDAP, the issuance of security certificates, the issuance of transaction certificates, etc., to ensure the security of information data related to platform transactions, while requiring that the certificate can be updated and revoked.

There are many cross-border transaction scenarios, all scenarios will have a corresponding smart contract, and based on the channel to isolate them, all channels have a part of the authorized participants, its ability to view the channel contract with cap, transaction data, etc. The channel is restricted based on visibility to strength visibility. When processing the intermediate data and results of the contract, they can be uploaded and stored based on encryption. The data in the chain storage medium should be encrypted based on the national secret algorithm to ensure the security of data information.

3.6 Asset protection

Based on blockchain technology, the security of digital assets is guaranteed, and the encryption technology of data can ensure the authenticity and traceability of data. Based on the depository contract, it can ensure the effective solution of digital asset security related issues based on forensics and arbitration when a dispute arises over digital assets. Smart contracts in the actual operation of digital assets, the need for continuous healthy transaction behavior, and rapid warning to ensure that digital assets will not be attacked, vulnerability, or in the event of an attack, vulnerability can be found and dealt with in a timely manner to avoid serious economic losses.

4. Conclusion

In summary, smart contracts corresponding to the development of security technology innovation, supporting technologies, rules and so on also keep improving. It can provide security guarantees for the efficient operation of smart contracts.

References

[1] Zeng Li. (2020). Blockchain-based intelligent processing transmission method and platform for cross-border e-commerce big data, CN111461840A [P]. 2020.

[2] Wang, D., Xie, Z., Zhen Zhen. (2020). The application path and legal regulation framework of blockchain technology in the collaborative development of cross-border e-commerce [J]. Journal of Xinjiang University of Finance and Economics, 2020(3): 8.

[3] Lin Binhui. (2020). Research on the impact of blockchain technology on traditional cross-border trade settlement methods [J]. 2020.

[4] Li Xiaofeng, Xu Jinlin. (2021). A blockchain-based cross-border trade privacy data management system and method: CN112417512A [P]. 2021.

[5] Lu Fang. (2021). Research on blockchain smart contract security mechanism in cross-border trade [J]. Network Security Technology and Applications, 2021(07): 161-164.