An Achieving Data Exchange Cross-Chain Alliance Protocol

To cite this article: Qianwen Wang *et al* 2019 *J. Phys.: Conf. Ser.* **1213** 042037

An Achieving Data Exchange Cross-Chain Alliance Protocol

Qianwen Wang*, Shen Wang, Pan Zhang, Li He, Xiao Li, Sijin Cheng, Shenshen Zhou

Aisino Corporation

* Corresponding Author's Email: wangqianwen@aisino.com

Abstract: This paper provides a method and system for establishing and communicating cross-chain alliances between blockchains. The method for establishing the cross-chain alliance includes: obtaining communication requirements of each communication node in multiple blockchains, each node establishing a cross-chain alliance and configuring identity certificates and transaction certificates and establishing cross-chain smart contracts.The blockchain cross-chain communication method includes: obtaining a communication request by using each blockchain in the cross-chain alliance established above, and establishing a node smart contract for each node; if a communication request is initiated, performing an endorsement policy verification on the communication request, and then performing the full sequence signature verification and data consistency verification, when the communication request is verified, the communication between the nodes is implemented according to the cross-chain smart contract.

1. INTRODUCTION

A blockchain is a chained data structure in which data blocks are sequentially connected in a chronological order, and cryptographically guaranteed non-tamperable and unforgeable distributed ledgers. Broadly speaking, blockchain technology uses blockchain data structures to validate and store data, uses distributed node consensus algorithms to generate and update data, and uses cryptography to ensure data transmission and access security, using automated scripts. The code consists of a smart contract to program and manipulate data in a completely new distributed infrastructure and computing paradigm.

With the development of blockchain technology, more and more chains, including public chains, alliance chains, and private chains, are beginning to emerge. The interconnection between chains and chains is becoming more and more important. It comes from this. Cross-chain technology can be understood as a bridge between the various blockchains. They do not have the natural cross-chain capability. Cross-chain is a complex process that requires independent verification of the nodes in the chain, decentralized input, and the acquisition and verification of information in the extra-chain world, and the acquisition and verification of information in the extra-chain world. At present, the main cross-chain technologies are: Notary schemes, Sidechains/relays, Hash-locking, etc. These cross-chain technologies are generally used for the transfer of cross-chain assets. The form is relatively simple and can only serve simple business scenarios, such as asset transactions between two entities across the chain, and cannot realize cross-chain communication of complex services. At present, smart contracts can only be run on nodes of a blockchain. The parties involved in smart contracts generally only have two parties at a time, and cannot implement cross-chain communication of complex rules.

2. MATERIAL AND METHODS

The alliance chain represented by R3, Hyperledger and Golden Chain Alliance emphasizes the strong correlation between value and synergy between institutions or organizations in the industry or across industries and the weak centralization within the alliance. The main goal is to reduce costs and improve efficiency. Strong identity licensing, security privacy, high performance, massive data, etc. are the main technical features. In general, the consensus nodes of the coalition chain are verifiable and have high governance structures or business rules. In the event of an abnormal situation, regulatory mechanisms and governance measures can be enabled to make follow-up penalties or further governance measures to reduce losses.

According to the characteristics of the alliance chain, our main purpose is as follows:

Establish cross-chain alliances for each node according to communication requirements, establish cross-chain alliance intelligent contracts, and configure identity certificates and transaction certificates for each node in the cross-chain alliance, thus realizing the establishment of cross-chain alliances, which is a cross-chain alliance. The various nodes provide the basis for communication.

By establishing a node smart contract in the cross-chain alliance, the communication request is verified accordingly, and each node realizes information communication according to the identity certificate, the transaction certificate and the node smart contract. Thereby, information interaction between different blockchains, cross-chain communication of complex services and multi-party complex rules, sharing of data resources in different blockchains, and resource utilization efficiency are realized.

Obtain communication requirements of each communication node in multiple blockchains; establish cross-chain alliances for each node belonging to communication requirements on different blockchains according to communication requirements, and configure identity certificates and transaction certificates for each node; according to communication requirements Establish cross-chain smart contracts for cross-chain alliances. The cross-chain smart contract is used for communication verification of each node; the identity certificate is used to implement communication authorization of the node.

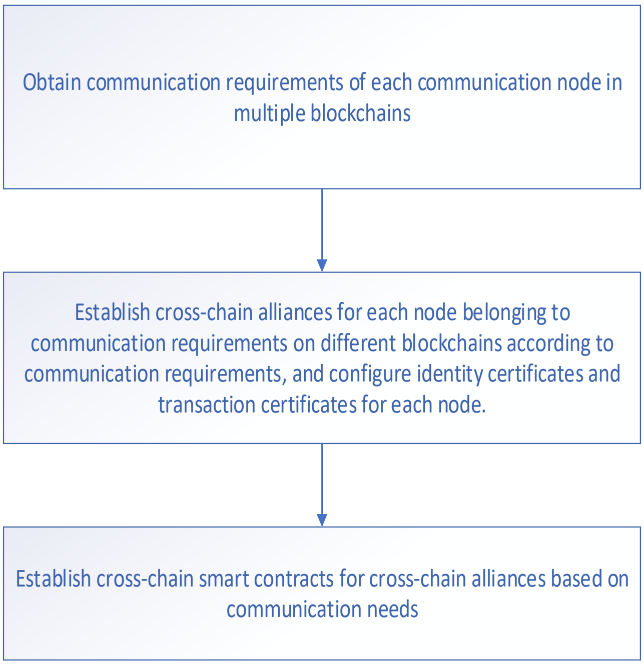
Obtain communication requirements of each communication node in multiple blockchains
Establish cross-chain alliances for each node belonging to communication requirements on different blockchains according to communication requirements, and configure identity certificates and transaction certificates for each node.
Establish cross-chain smart contracts for cross-chain alliances based on communication needs

Figure 1. Cross-chain alliance workflow

The cross-chain communication method between the blockchains we establish is to establish each blockchain in the cross-chain alliance to obtain communication requests, identity certificates, transaction certificates and cross-chain smart contracts, and establish node smart contracts for each node; When a communication request is initiated, the endorsement policy verification is performed according to the node smart contract, the identity certificate, the transaction certificate, and the communication request, and the communication request verified by the endorsement policy is sent to the cross-chain alliance; the cross-chain alliance performs full-sequence signature verification and data on the communication request. Consistency verification; when communication requests pass full-sequence signature verification and data consistency verification, nodes communicate between nodes according to cross-chain smart contracts.

The endorsement policy verification is performed according to the node smart contract, the identity certificate, the transaction certificate and the communication request, and the communication request verified by the endorsement policy is sent to the cross-chain alliance, and the node smart contract generates a communication suggestion result according to the identity certificate and the associated communication request, and the communication is generated. The proposed result is sent to the endorsement verification node; the node generates the actual execution result according to the communication request and the transaction certificate, and sends the actual execution result to the endorsement verification node; the endorsement verification node performs the endorsement policy verification on the actual execution result of the node according to the communication suggestion result; When the endorsement policy is verified, the cross-chain alliance sends a communication request verified by the endorsement policy to the cross-chain alliance.

The cross-chain communication method between the blockchains further includes: when the communication request fails the full-sequence signature verification and the data consistency verification, the cross-chain alliance marks the communication request as an invalid request, and sends an error information to the node that initiates the communication request.

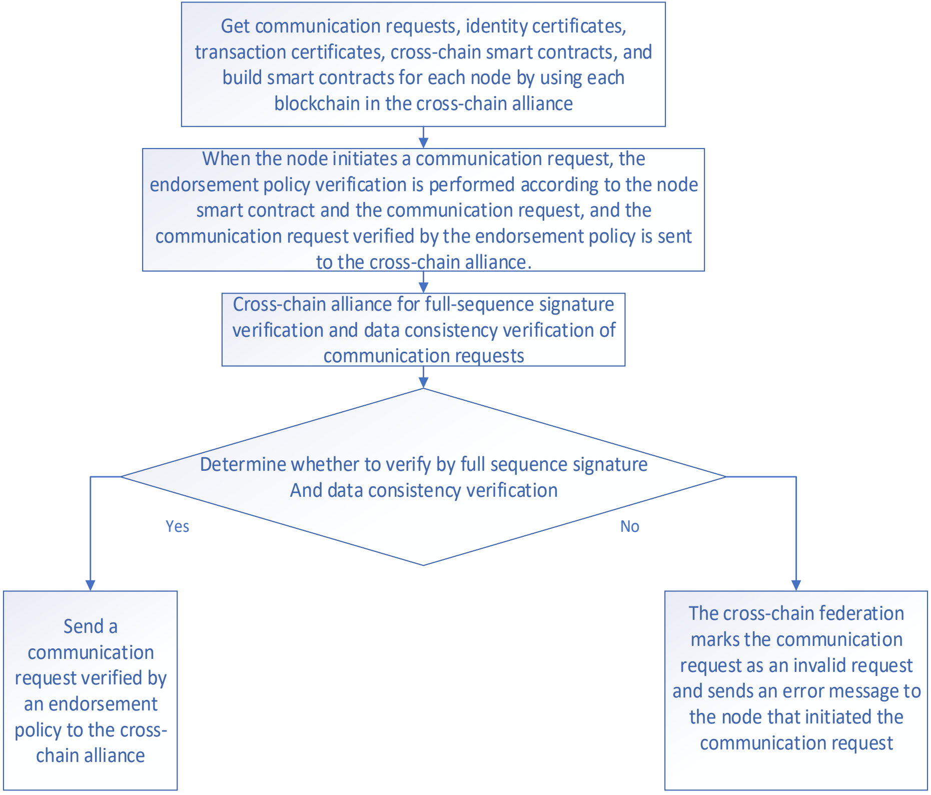
Get communication requests, identity certificates, transaction certificates, cross-chain smart contracts, and build smart contracts for each node by using each blockchain in the cross-chain alliance
When the node initiates a communication request, the endorsement policy verification is performed according to the node smart contract and the communication request, and the communication request verified by the endorsement policy is sent to the cross-chain alliance.
Cross-chain alliance for full-sequence signature verification and data consistency verification of communication requests
Determine whether to verify by full sequence signature And data consistency verification
Yes
No
Send a communication request verified by an endorsement policy to the cross-chain alliance
The cross-chain federation marks the communication request as an invalid request and sends an error message to the node that initiated the communication request

Figure 2. Cross-chain alliance endorsement strategy

a communication requirement acquisition module, configured to acquire communication requirements of each communication node in a plurality of blockchains; and a cross-chain alliance establishment module, configured to establish a cross-chain alliance of each node belonging to a communication requirement on different blockchains according to communication requirements, And configure identity certificates and transaction certificates for each node; a cross-chain smart contract establishment module is used to establish a cross-chain smart contract for the cross-chain alliance according to communication requirements. a node smart contract establishing module for acquiring communication requests, identity certificates, transaction certificates, and cross-chain smart contracts by using the blockchains in the cross-chain alliance established by the establishment system in the aforementioned manner, and establishing nodes for each point The smart contract; the endorsement policy verification module, when the node initiates the communication request, the endorsement policy verification module is used for endorsement policy verification according to the node smart contract, identity certificate, transaction certificate and communication request, and sends the communication request verified by the endorsement policy to the cross Chain alliance; a full-sequence signature verification module for enabling cross-chain alliance to perform full-sequence signature verification and data consistency verification for communication requests; a node communication module for enabling nodes to implement nodes according to node smart contracts, identity certificates, and transaction certificates Communication.

The endorsement policy verification module includes: a communication suggestion result generation sub-module, configured to enable the node smart contract to generate a communication suggestion result according to the identity certificate and the associated communication request, and send the communication suggestion result to the endorsement verification node; the actual execution result generation sub-module is used The node is configured to generate an actual execution result according to the communication request and the transaction certificate, and send the actual execution result to the endorsement verification node; the endorsement policy verification sub-module is configured to enable the endorsement verification node to endorse the actual execution result of the node according to the communication suggestion result. The communication request sending sub-module, when the end-book policy verification is passed, the communication request sending sub-module is used to send the communication request verified by the endorsement policy to the cross-link alliance.

The intelligent link-based blockchain cross-chain communication system further includes: a communication request error correction module, when the communication request fails the full sequence signature verification and the data consistency verification, the communication request error correction module is configured to enable the cross-chain alliance to communicate the request Marked as an invalid request and sent an error message to the node that initiated the communication request.

3. RESULTS

3.1. DATA EXCHANGE

An example is described here. Suppose that in the module established by the node smart contract described above, the communication request is a request for data exchange between nodes, and the node smart contract is a protocol for data calling the node. For example, node smart contract 1 (chain code CC1) calls the corresponding request node of CC1, and the local request node accepts the call of CC1, performs state transition processing, and records the communication suggestion result and actual execution result of the request, and generates corresponding Status version. CC1's communication suggestion results include the state key value of the transaction that needs to be modified, as well as the value and state key value that the new state's Value and change depend on, and the current version value. The result of the communication suggestion of the node smart contract 1 is sent to the endorsement verification node specified in the CC1 deployment. The endorsement verification node also accepts the call of CC1, and verifies the communication suggestion result, and checks the proposed state modification and state dependency with the actual on the node. Whether the execution result is consistent. If the signature of the node is consistently added, the result is returned to the requesting node. The requesting node collects the feedback of the endorsement verification node, and reaches the endorsement verification strategy arrangement set by the node smart contract, and then verifies the endorsement of the communication suggestion result. The endorsement verification policy can be set to the corresponding weight of each verification node. If the total weight of the nodes participating in the verification exceeds 50% after verification and passes the verification, the endorsement verification by the communication recommendation result is determined.

3.2. COMMUNICATION REQUEST ERROR CORRECTION

When the communication request fails the full sequence signature verification and the data consistency verification, the communication request error correction module is configured to cause the cross-chain alliance to mark the communication request as an invalid request, and send the error information to the node that initiated the communication request. Each communication request is verified to ensure that the data it reads is not altered by other transactions, ensuring that the data read during chain execution does not change since the end of the endorsement verification. If the read data is altered by another transaction, the request initiated by the node in the blockchain will be marked as an invalid request and will not be written to the ledger state database. The cross-chain alliance sends the error information to the client corresponding to the node that initiated the transaction. After receiving the message indicating the error, the client performs error correction or appropriate retry. If the node making the communication request submits the communication recommendation result of the same state dependency verified by the endorsement policy to the cross-chain alliance twice, the cross-chain alliance will assign two serial numbers to the two transactions and send them to the respective nodes, and the node performs When the local state version relies on authentication, the first accepted transaction has been updated because the local state has been added. Later, the same transaction is dependent on an outdated version, and the second transaction proposal submitted does not pass the state version dependency. Verification, and is discarded as an illegal transaction.

4. CONCLUSIONS

By establishing a cross-chain alliance, cross-chain communication between different blockchains is realized, so that data resources in different blockchains can be shared, and resource utilization efficiency is improved.

ACKNOWLEDGEMENTS

This research was financially supported by National Key R&D Program of China (Grant No. 2017YFB0802701).

REFERENCES

[1] M. Ali, J. Nelson, R. Shea, and M. Freedman. Blockstack: A global naming and storage system secured by blockchains. In Proc. USENIX Annual Technical Conference (ATC ’16), June 2016.

[2] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In Proc. IEEE Symposium on Security and Privacy, May 2015.

[3] Ethereum. http://gavwood.com/Paper.pdf

[4] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse. Bitcoin-NG: A Scalable Blockchain Protocol. In 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), pages 45--59. USENIX Association, 2016.

[5] Giuliana Santos Veronese , Miguel Correia , Alysson Neves Bessani , Lau Cheuk Lung , Paulo Verissimo, Efficient Byzantine Fault-Tolerance, IEEE Transactions on Computers, v.62 n.1, p.16-30, January 2013

[6] Hyperledger -- Blockchain Technologies for Business. https://www.hyperledger.org/