Blockchain Router: A Cross-Chain Communication Protocol

Hui Wang
ZhongAn Information Technology Service Co.,Ltd
No.4, Huqiu Road,
Huangpu District, Shanghai
wanghui@zhongan.com

Yuanyuan Cen
ZhongAn Information Technology Service Co.,Ltd
No.4, Huqiu Road,
Huangpu District, Shanghai
cenyuanyuan@zhongan.com

Xuefeng Li
ZhongAn Information Technology Service Co.,Ltd
No.4, Huqiu Road,
Huangpu District, Shanghai
linco.li@zhongan.com

ABSTRACT

Cross-chain communication is one of the major design considerations in current blockchain systems [4-7] such as Ethereum[8]. Currently, Blockchain operates like information isolated island, they cannot obtain external data or execute transactions on their own.

Motivated by recent studies [1-3] on blockchain's multiChain framework, we investigate the cross-chain communication. We introduces blockchain router, which empowers blockchains to connect and communicate cross chains. By establishing an economic model, blockchain router enables different blockchains in the network communicate with each other same like Internet network. In the network of blockchain router, some blockchain plays the role of a router which, according to the communication protocol, analyzes and transmits communication requests, dynamically maintaining a topology structure of the blockchain network.

CCS Concepts

• Networks → Network protocols → Network protocol design.

Keywords

Blockchain technology; communication; economic model; network.

1. INTRODUCTION

Telecommunication systems heralded the coming of Internet age, today a new technology—Blockchain—gets the potential to decentralize the way we store data and manage information, furthermore removing central intermediators, one of the most important regulatory actors in our society.

Blockchain technology brings to us decentralized currencies, self-executing digital contracts (smart contracts) and intelligent assets that can be controlled over the Internet (smart property). Blockchain also introduces a new governance system with a more democratic decision-making mechanism, and decentralized (autonomous) organizations that can operate over a network of computers without any human intervention. Many has pointed out Blockchain shall have the same magnitude as Internet, and some more audacious prediction says that this technology would shift the balance of power away from centralized authorities in communications, business, and even politics and law.

Reviewing the development of Internet and the changes it brings out, we cannot deny the tremendous power of telecommunication. In fact, the birth of the blockchain itself is a prospective product of Internet. Without relying on centralized service, the blockchain nodes establish mutual trust through P2P communication, consensus, back-up data. Developed so far, Internet encounters many problems, such as, the increasing load of backbone network and frequent attacks, and seeks for solutions actively. For example, IPFS[6], the content-based distributed network file storage protocol can now deal with the problems faced by the traditional IP address based network protocol.

By analogy with the Internet, it is not difficult to find that, in the current phase, blockchain's network capacity is only carried out to the extent similar to LAN, and different chains cannot communicate and has no mutual trust at all. For a single blockchain, we also suffer from its various limitations. Meanwhile, the consensus mechanism, in providing security, also greatly limits the development of blockchain system at the same time, which leaves us no way of improving the processing capacity of the transaction by increasing nodes.

This paper is organized as follows. The second section introduces the design concept of the blockchain router, including design inspiration and vision. The third chapter explains architecture of the blockchain router. The fourth chapter explains the economic model in the blockchain router network.

2. DESIGN CONCEPT

In the face of various problems, we put forward the concept of "blockchain router". The design concept of blockchain router is derived from the routing architecture of Internet. A simple routing network consists of routers and terminal devices. In our design, the blockchain systems, such as bitcoin, Ethereum, AnChain, etc, corresponds to the terminal equipment in the routing network, which is called “sub-chain”. A sub-chain can receive messages from a chain router, or send messages to another sub-chain via the chain router, but cannot communicate directly with each other.

A blockchain router dynamically maintains all the related information registered on sub-chains. The router is used to link sub-chains in the chain network. To communicate with other sub-chains, a sub-chain must firstly establish connection with the blockchain router following cross-chain communication protocol.

IEEA'17, March 29-31, 2017, Jeju , Republic of Korea.
© 2017 ACM. ISBN 978-1-4503-5230-7/17/03…$15.00.
DOI: http://dx.doi.org/10.1145/3070617.3070634

A blockchain router can communicate with a sub-chain or other blockchain routers. By exchanging information with its connected sub-chains, the blockchain router maintains the smoothness of the network communication.

In this structure, we can deploy blockchain network system according to different business logic and user requirements. The important function of the blockchain router is to break down communication barrier among sub-chains, and establish trust bridge cross-chains. The sub-chains connected to blockchain routers can communicate with each other and work together to achieve the effect of "1+1>2". We can also deploy a number of blockchain router systems, with isomerism sub-chains including Bitcoin, Ethereum, etc. Thus, each blockchain router can serve a more complete business ecosystem. Similarly, we can deploy different blockchain router clusters according to nodes numbers, geographical location, and business requirements. Following the Routing algorithm, different processing requests can be assigned to appropriate cluster.

The final form of the blockchain router network is a complex blockchain star network, which is connected to each other by the infinite extension of the blockchain router and connectors, creating a blockchain network which is interconnected with internal communication and trust.

3. BLOCKCHAIN ROUTER

In this section, we introduce the blockchain router architecture. More details will be described in the extended version of this paper.

3.1 Participants

There are four different participants in the blockchain router: validator, connector, surveillant, and nominator.

Validators: The validators are the most important participants in the blockchain router network. They verify, concatenate and forward blocks to the correct destination.

A validator must run a full client of the blockchain router. The validator collects and ratifies blocks from the registered sub-chains of blockchain routers. This process involves receiving, validating, and republishing candidate blocks. It is not possible for a blockchain router to synchronize blocks of all sub-chains, so it is desirable to assign the task of block collecting to a third party, which is called connector.

Nominators: The nominator is rewarded by contributing its own funds to validators. Note that nominator bears no additional function. The validator is responsible for maintaining the state of the network on behalf of the nominator. The nominator obtains corresponding payoff based on the amount of the contribution. If the validator is punished, its supporting nominators will also be punished accordingly.

Surveillants: Survellants' task is not to verify the honesty of the blcok information, but to monitor the blockchain router's behavior. The Surveillant role is set to reduce the incidents of evil behavior. Improper behavior by accident rather than malicious can be tolerated conditionally.

Connectors: Connector link blockchain router with sub-chains. Connectors are responsible for: sending the information of sub-chain to blockchain router and vise versa. Connectors of each sub-chain form a consensus system.

Connectors collect information on sub-chain blocks for validators. A connector maintains the full-node of a particular sub-chain. This means that it maintains all the required information for the sub-chain and is able to execute transactions. A connector executes transaction and provides the information to be passed to validators along with their corresponding signature.

3.2 Consensus Algorithm

The consensus algorithm used by blockchain router is similar to PBFT. In PBFT, some reliable nodes are called validators who have the chance to become leaders. In the process of blockchain generation, a new validator shall become this round's leader in default, and this leader is responsible to package the new block and broadcasts the reasonable block to every validator. Only after two rounds of more than 2/3 voting among all the validators, can the new block be confirmed in consensus.

Undeniably, the Byzantine fault tolerant algorithm used in PBFT can guarantee the network security whose Byzantine nodes is less than 1/3. However, in practical application, especially when associated with economic benefits, even if the validator is reliable nodes selected, we cannot simply rely on the 1/3 security without punishment mechanism. To ensure security, there must be immediate reward with persuasion and immediate penalty with punishment, also the reward and penalty must be associated with economic interests. Therefore, we modified the original consensus mechanism, to make the validators' voting rights correspond to the token they mortgaged on the blockchain.

In this way, the blockchain generation mechanism is changed to over 2/3 voting stakes confirmation from over 2/3 voters. Besides, in PBFT consensus algorithm, the common nodes only synchronize the new block information from leader's nodes without taking part in the consensus. Its security only rely on the validation nodes, thus the increasing in common nodes number cannot improve the security of Byzantine fault tolerant. In our new consensus mechanism, we increased the non-verification nodes' involvement. A validation node shall be bonded with a validator account, and the non-validators can authorize their stakes to validators winning benefits. In consideration of their benefit interests, the non-validators shall choose their authorized validator with great care. This consensus mechanism ensures all snodes get involved in the consensus while reducing the low efficiency problem.

Every ZAC owner will have opportunity to become a participants by mortgaging his ZAC to a shared ZAC fund. The commit weight of each validator is decided by the portion of his ZAC in the fund.

This consensus algorithm is called Delegated Stake-PBFT, referred to as DS-PBFT.

3.3 Communication Protocol

Blockchain Router Network's telecommunication protocol is delegated as follows. At first, the cross-chain communication request should be written into sub-chain in the form of transaction. Then, the connector collect the blocks of sub-chain and detect the cross-chain communication request. Once a cross-chain communication transaction is triggered, the connector send the transaction with proof to validators. At last, validators verifies the transaction and record the result on validators' block. The connectors of target sub-chain collect the blocks of blockchain router and forward the information and corresponding proof information to target sub-chain.

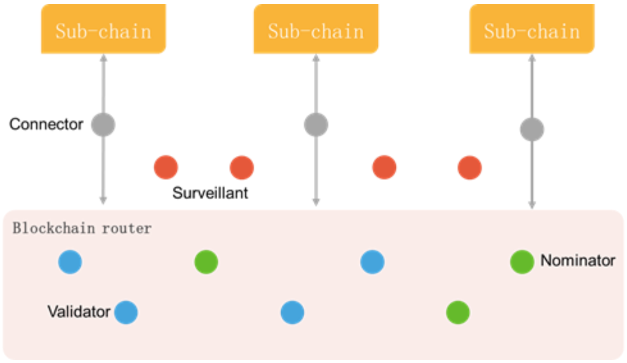

Figure 1. Architecture Overview of Blockchain Routers.

4. ECONOMIC MODEL

In this section, we present the economic model of blockchain router network, in which the participants are in dynamic equilibrium state. Here we assume that all participants are rational.

4.1 Token Issuance

Blockchain Router issues its own token ZAC through Proof-of-Stake (PoS). In order to encourage ZAC holders to participate in the consensus mechanism, the issue pattern of ZAC is in inflation mode. Since no one wish their money devaluate through time, he/she will try to participate in the consensus process.

Let $*$ be a particular kind of participant where v, c, n represent validator, connector and nominator, R_*be the reward of token issuance, ARR_* be the average reward rate, S be the ZAC in the fund, then the reward of token issuance can be expressed as follows.

$$R_* = ARR_* \times S$$

Three different kinds of participants could benefit from the token issuance: validator, connector and nominator. Each participant has an average different reward rate

$$ARR_v > ARR_c > ARR_n,$$

which means

$$ARR_v \times S > ARR_c \times S > ARR_n \times S$$

that is

$$R_v > R_c > R_n.$$

In this way, for the same amount of ZAC, different kinds of participants get different reward. So ZAC holders will be prioritized as validator, and successively as connector and nominator.

The number of validators and connectors is limited. Let the maximum number of validators and connectors be N_v and N_c.

Before the number of validator reached N_v, every ZAC owner can apply to be a validator. When the maximum is reached, one owner must mortgage more ZAC than the least owner of current validator to take the place of that validator. After the number of validator reached N_v, the ZAC owner will apply to become a connector. Those nodes which do not have enough ZAC can delegate his stake to a validator, and the reward to this validator should be further allocated to its consignors. In this way, the nodes having few ZAC can also contribute to the network consensus and avoid his loss caused by annual inflation.

4.2 Punishment mechanism

We prevent the participants from doing evil through mortgage funds. Participant needs to put some ZAC into the fund before sending a potentially risky transaction. When malicious actions are detected, part of the mortgaged ZAC will be transferred to the reward pool. Putting ZAC into the reward pool will result in a decrease in the total amount of ZAC in circulation, so the currency in the reward pool will be used as additional currency in the currency issuance and be distributed proportionally to the participants.

4.2.1 Validators and nominators

Validator can raise a proposal and it can be approved when more than $2/3$ total stake commit to agree. There are 5 types of commitment, includes agreement, intensive agreement, disagreement, intensive disagreement, and abstention. If over $1/3$ total stake commit intensive disagreement, the proposal will be rejected and the validators who commit agreement and intensive disagreement will be punished. As the result, the validators' ZAC in the fund will reduce and the same amount of ZAC will be added to the reward pool. Those proposals approved will be executed in two weeks.

Double-signing and unable to commit is two typical cases need to be punished. Double-signing means the validator sign for two different blocks on the same height in the same commit round. Such action will affect the DS-PBFT algorithm. Once double-signing is found, the validator will lose some ZAC and reputation as a punishment. When the reputation of some validator is negative, it will be removed out of the validator list. Validator may offline a long time because of network failure or machine damage and consequently absent too many committing rounds. As a result, this validator will be punished.

The actions above can be easily detected. For those kinds of violations, which are difficult to be found, a two week duration of time is set to unbind the mortgage ZAC from the fund so as to extend the time of violation detection.

When illegal actions have been found, the nominators are subjected to the same degree of punishment as validator. In this way, nominators should choose a trustworthy validator.

4.2.2 Connectors

Since connector is the only data source for the validator, connector plays a very important role in the blockchain router network. Therefore the security of the connectors must be adequately safeguarded.

There are two different illegal actions of connectors:

1. sending the fake block to the validator.

2. without verifying sub-chain blocks.

Obviously, the first one is of the most serious impact. Therefore, in the consensus system of connectors for each sub-chain, there is no Byzantine fault-tolerant mechanism. Specifically, a sub-chain block could be considered legitimate only if it has been verified by all connectors. In other words, an attacker must control all the connectors of one particular sub-chain to be able to send a fake block.

To further prevent this kind of attack, the target sub-chain is randomly assigned by the cryptographic method in the application of Connector. The assignment of sub-chains to different connectors is based on data combined from previous blocks of each sub-chain under a cryptographically secure hash.

Let CAbe the average stack of all connectors, and c be the number of sub-chain, k be the number of connectors on each sub-chain, n be the number of connector controlled by an attacker. Thus, the cost for the attacker is about

$$CA * n.$$

According to [13] the probability that the attacker control all connectors of a single sub-chain to lunch a successful attack is approximately

$$p \approx 1 - exp(n^k e^{-n/c}(\tfrac{n}{c(k+1)} - 1)^{-1} c^{1-k} (k!)^{-1}),$$

which is small when $c * k >> n$.

This raises another problem, if a connector of the sub-chain does not participate in the consensus for non-malicious reasons, the communication of this sub-chain will be delayed. Therefore, in practice, one can allow a small number of connectors that does not return signature. But the proportion of this kind of connectors must be strictly limited.

4.2.3 Surveillants

Unlike connectors and validators, surveillants do not participate in block verification, but are rewarded by detecting illegal actions. The surveillants is rewarded by proving that one party acted illegally. Illegal actions include double signing, approving invalid blocks, and so on.

In order to prevent evil connectors or validators from acting as surveillants to take away deposit, surveillants receive fines that are only part of the deposit, such as 30%. The rest will be put into reward pool. So that the evil connectors or validators will never share fines with the supervisor, as they will lose most of the deposit.

Surveillant must deposit a small bond as it broadcasting some illegal action. This bond prevents sybil attacks from wasting validators' time and computing resources. It is immediately withdrawable, probably no more than the equivalent of a few dollars but may lead to reaping a hefty reward from spotting a misbehaving validator.

5. CONCLUSION

After detailed market research and case studies, we believe blockchain will become a key technology in many industries and further drive innovation, changing the industry infrastructures. Currently, there isn’t any complete blockchain architecture that can meet the requirements of high-traffic, regulation, privacy and scalability at the market. Meanwhile, various application cases have different product requirements on the blockchain architecture.

The blockchain router network is the application of the concept similar to the internet router in information transmission. Blockchain Router Network can break down the current isolation between different chains, maximally advancing blockchain’s potentiality and realizing interconnection, interoperability and mutual trust cross chains.

6. REFERENCES

[1] Wood, D.G., "Polkadot: Vision For A Heterogeneous Multi-Chain Framework".

[2] Ethan Buchman and Jae Kwon. Cosmos: A network of distributed ledgers. https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md, 2016.

[3] Thomas, S. and Schwartz, E., 2015. A protocol for interledger payments. URL https://interledger.org/interledger.pdf.

[4] Economist Staff. "Blockchains: The great chain of being sure about things". The Economist, 18 June 2016.

[5] Morris, David Z. "Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting". Fortune (magazine), 2016-05-23.

[6] Popper, Nathan (2016-05-21). "A Venture Fund With Plenty of Virtual Capital, but No Capitalist". New York Times, 2016-05-23.

[7] Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". https://bitcoin.org/bitcoin.pdf, 2008.

[8] Buterin et al. "A Next-Generation Smart Contract and Decentralized Application Platform". https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper, 2014.

[9] Juan Benet. "IPFS - Content Addressed, Versioned, P2P File System". https://arxiv.org/abs/1407.3561, 2014.

[10] Lamport, Leslie et al. "The Byzantine generals problem". ACM Transactions on Programming Languages and Systems (TOPLAS) 4.3 (1982): 382-401.

[11] Szabo, Nick. "Formalizing and Securing Relationships on Public Networks". First Monday, 6 March 2014.

[12] Goldreich, Oded. "Secure multi-party computation". Manuscript. Preliminary version (1998): 86-97.

[13] Arnold, M., & Glaß, W. (2013). Simple Approximation Formulas for the Birthday Problem. American Mathematical Monthly, 120(7), 645-648.