An Electricity Cross-Chain Platform Based on Sidechain Relay

Hongkai Wang¹, Dong He¹, Xiaoyi Wang², Caichao Xu², Weiwei Qiu², Yiyang Yao¹ and Qiang Wang³*

¹State Grid Zhejiang Electric Power Corporation Information & Telecommunication Branch. Room 641, No. 8 Huanglong Road, Hangzhou 310000, China
²Hangzhou Qulian Technology Co., Ltd. 20F, Venture Building 2, No. 399 Danfeng Road, Binjiang District, Hangzhou 310000, China
³College of Computer Science and Technology, Zhejiang University. Hangzhou 310027, China
Email: wangqiang@zju.edu.cn

Abstract. Based on sidechain relay strategy, a cross-chain platform BitXhub-PI is implemented to realize the interoperability between the heterogeneous blockchains for electric power industry. The platform is composed of three roles: relay chain, application chain and cross-chain pier, and it has three core functional characteristics of universal cross-chain transmission protocol, heterogeneous transaction verification engine, and multi-level routing to ensure the security, flexibility and reliability of cross-chain transactions of electricity business. The platform provides a unified cross-chain contract template for homogeneous and heterogeneous electricity application chains, and the relay chain contains a dynamically upgradeable verification engine. The experiments show that the platform guarantees asynchronous distributed electricity business transactions between heterogeneous blockchains, achieving high performance with high throughput, low latency, high scalability, and low overhead.

1. Introduction

In 2015, the World Economic Forum listed blockchain as one of the six major trends. The current popular business areas of startup companies using blockchain technology are smart contracts, securities clearing/transactions, asset management, e-commerce, Internet of Things, social communications, file storage, identity verification, prediction markets, and data APIs. The momentum of the blockchain will start, and leading companies in various industries published blockchain-related research reports. Goldman Sachs Investment Research released a report predicting that blockchain technology can simplify the clearing and settlement of securities, saving US$2 billion annually for the US capital market and US$6 billion for the global capital market, and if blockchain technology is adopted in the payment field, the world can save $550 billion in payment costs every year. A series of research reports indicate that the overall market prospect of blockchain technology is very broad.

The current development of the power industry is also gradually moving towards the stage of cross-border integration, simultaneous development of multiple heads, and accelerated innovation. Introducing blockchain technology into power applications is highly consistent with the guiding ideology of Ubiquitous Power Internet of Things, whose core idea is “holographic perception, ubiquitous connection, open sharing, integration and innovation”.

As a bridge connecting heterogeneous blockchains, cross-chain can provide reliable underlying support for the formation of blockchain interconnection networks and the interconnection of value islands. According to the different interaction content between heterogeneous blockchains, cross-chain transactions can be divided into asset exchange and information exchange. In terms of asset exchange, the current value exchange between heterogeneous blockchains mainly depends on centralized exchanges, and the value of assets on the chain cannot be reasonably evaluated. The information exchange is very complicated because it involves data synchronization between chains and corresponding cross-chain calls. At present, information sharing between heterogeneous blockchains is impossible, and the barriers to business communication are extremely high.

On the other hand, the existing blockchain technology itself has the problem of insufficient performance under the single-chain architecture. Consensus mechanism is time-consuming to reach consensus in a low-trust network. If node evil is considered, the processing complexity is further increased, so in many cases the performance of a single node cannot meet the transaction throughput and transaction delay requirements of commercial application scenarios. At the same time, with the increase of running time, the storage capacity of the blockchain will increase linearly. At present, the local data storage of the chain cannot be expanded in parallel, so the single-chain architecture cannot meet the performance, capacity and other requirements of the application.

Hence, a blockchain platform for power industry BitXHub-PI is designed to meet the requirement of electricity power business.

2. Related Work

Cross-chain technology is the key to realize the value blockchain Internet, and it is the bridge for the scalability and connection of the blockchain. The current research on cross-chain technology has evolved four strategies: notary schemes [1-2], sidechain and relay mechanism [3-5], hash time locking mechanism [6] and distributed private key control technology. The notary mechanism [1-2] is essentially an intermediary mechanism. A trusted third party is used as an intermediary to verify and forward cross-chain messages for both parties [7]. The advantage is that it can flexibly support various blockchains with different structures. The disadvantage is that there is a risk of centralization. Hash lock technology [6] is an asset atomic exchange technology proposed in the Lightning Network. It provides the original value of the hash value to achieve the atomic exchange of assets within the specified time, but this technology can only achieve asset exchange and cannot do transfer of information, so its use scenarios are limited. In the sidechain and relay mechanism, the sidechain refers to another blockchain that fully possesses the function of a chain, which can actively sense the main chain information and take corresponding actions. Relay chain is a combination of sidechain and notary mechanism, with the ability to verify cross-chain messages and forward cross-chain messages. The private key in the distributed private key control technology is jointly managed by the user and the decentralized network, locks the original chain assets when cross-chain, and initiates smart contracts on the destination chain to create new assets.

Cosmos [8] and Polkadot [9] pay more attention to cross-chain infrastructure. Cosmos uses Tendermint [10-11] consensus algorithm, which is a cross-chain network that supports heterogeneous blockchains. Polkadot project is aiming to achieve a scalable heterogeneous multi-chain system. In order to solve the problem of scalability of cross-chain systems [12], it uses an economic incentive mechanism between nodes that do not trust each other.

However, the current cross-chain solution of the public chain cannot solve the cross-chain problem in the alliance chain well, and cannot eliminate the differences caused by the consensus algorithm, account structure, encryption mechanism and other technologies of heterogeneous blockchains. Polkadot takes imperfect token economic governance strategy. People with a certain number of tokens can control the cross-chain network. The verifier role node in the relay chain has an important impact on the change of the world state of any application chain. Despite the monitoring of phishers, the risk exposure is still very large. Cosmos cross-chain network is not compatible with heterogeneous
application chains. The chain of timely confirmation mechanism needs to add IBC protocol, and more complicated operations are needed for the final confirmation chain (PegZone proxy chain).

To meet the requirement of interoperability of heterogeneous blockchains. The following rules should be satisfied:

ACID guarantee for distributed transactions in cross-chain systems. The change between the two ledgers must be atomic, otherwise there will be problems of double payment or loss of value. Internet information transfer is stateless, and network packets can be lost and retransmitted. But the current messaging between blockchains is stateful.

Compatibility guarantee for heterogeneous cross-chain system. This article follows the modular loose-coupling design, proposes a cross-chain pier component, extracts the logic of dealing with heterogeneous blockchains from the relay chain, and puts it into the cross-chain pier to reduce the redundancy calculation and redundancy of each node of the relay chain storage overhead.

Security guarantee for heterogeneous blockchain interoperability. Bundling multiple application chains with different risk preferences, different scalability requirements, and different privacy requirements will affect the overall security of the cross-chain system.

3. Framework of Main-Side Chain for Electricity Business

Aiming at the needs of the power blockchain in different scenarios of value chain and business chain, hierarchical management and flexible business expansion, this paper proposes a hierarchical and scalable multi-chain architecture of the main-side chain. In this system architecture, the blockchain can be divided into a main chain and business sidechains according to functions. The main chain is responsible for the value circulation of the entire platform, the management of the sidechains, data consistency guarantees, core data storage and other key functions, the sidechain is responsible for carrying specific business services, forming a laterally scalable side chain cluster. The main chain and sidechains can be combined in a flexible form of a multi-layered architecture, as shown in figure 1.

Figure 1. The framework of Electricity Main-side chains.

The power blockchain main-side chain architecture is divided into three layers. The first layer is the main chain. The main chain is mainly responsible for the value circulation of the entire platform, the interaction between the auxiliary sidechains (value exchange or data transfer), and the supervision of the entire system. The value data in the main chain is a collection of sidechain business data analysis. The data in the sidechain can be transferred between different sidechains through the main chain, or cross-chain interaction can be directly performed in the sidechains. The main chain needs to detect the
power settlement data uploaded by the sidechains. For the performance consideration of the entire main sidechain system, the main chain only needs to regularly detect the settlement data uploaded by the sidechains. If the data is problematic, that is, it fails the regulatory review, the main chain is eligible to prohibit the cross-chain operation of the sidechain, or the sidechain is removed from the cross-chain system, or the value of the sidechain pledge is deducted from the main chain as punishment. In addition, in order to further verify the authenticity of the electricity business data of the sidechain, the main chain can request the sidechain to upload specific data of a specific block regularly, say, one day or half a day, and then settle the detailed power data through smart contracts.

The second layer is a cross-link network composed of cross-chain piers. When each sidechain joins the main sidechain system, it is necessary to deploy a dedicated cross-chain pier, then different cross-chain piers are connected together to form a cross-link network, which is mainly responsible for transmitting cross-chain transactions of the main-side chain and electricity business data flow between the sidechains.

The third layer is the sidechain layer. As long as each sidechain implements the cross-chain pier according to the interface specified by the main-side chain system, and then successfully registered with the main chain, it can be added to the main side chain network. In order to cooperate with the main chain to supervise the electricity business data, the sidechain needs to upload two kinds of electricity business data regularly: one is to upload the settlement results of the electricity business data in the block every other block; the second is to upload the detailed electricity business data of a specific block once every interval (say, half a day or one day).

The main-side chain for electricity power application model research deploys value data and business data between the main chain and the sidechain. The main chain is responsible for the registration of the main-side chain participants on the main chain blockchain, key generation, digital identity, signature, verification and other operations related to the account management and cross-chain asset authorization of various parties, as well as the data exchange process between the side chains, including cross-chain data, data authorization and other information are regarded as value data. The sidechain deploys the business data of the power in different sidechains. The data in different sidechains can be exchanged after being authorized, identified, source-verified through the main chain. Data transmission and synchronization between sidechains are implemented through cross-chain piers.

4. Cross-Chain Procedure

Under the main-side chain architecture, the main chain uniformly manages the data identity information, data authorization information, and cross-chain sharing process information of sidechain users in the main-side chain architecture network. The sidechain interacts with other sidechains through cross-chain piers, verify the digital identity and authorization information of the side chain through the main chain, and verify the sidechain for cross-chain data authorization, confirmation signature and other operations.

The cross-chain process is shown in figure 2. The steps of cross-chain transactions between sidechain A and sidechain B include:

1. The user/device (including the initiator and the receiver) generates a public and private key on the sidechain A, passes a digital identity cross-chain contract, and throws a cross-chain event after in-chain consensus.

2. After the cross-chain event is listened by the cross-chain pier of the sidechain, it is converted into a cross-chain transaction of the IBTP structure, and the transaction is routed to the cross-chain pier of the main chain blockchain.

3. The main chain cross-chain pier parses the received cross-chain transaction and verifies it according to the verification rules of the side chain blockchain. After the verification, the transaction is converted into the transaction format corresponding to the main chain blockchain.

4. The main chain registers users/devices of the sidechain according to the request information in the cross-chain transaction, and binds the public key to the authenticated identity information. The sidechain forms unique identity through the main chain.
(5) The initiator executes the instruction operation (synchronizes the data of side chain A to the side chain B through the cross-chain pier), the initiator performs the signature confirmation operation of the cross-chain data, and signs the identity of the side chain via the main chain.

(6) After the main chain verification is successful, the verification result is returned to the sidechain A, and the sidechain A can synchronize the cross-chain data to the sidechain B through the cross-chain pier.

(7) The receiver on the sidechain B receives the data of the initiator on the sidechain A through the cross-chain pier, and the receiver synchronizes the data identity and authorization signature information of the hashed data on the sidechain B through the cross-chain pier to the main chain. The main chain verifies the cross-chain data authorization signature of the sidechain to verify the authenticity of the cross-chain identity, data identity, data authorization willingness, and data source of side chain A;

(8) The main chain verifies the data identity of sidechain A, verifies the data authorization signature of sidechain A, and returns the verification result to the receiver of sidechain B through the cross-chain pier.

(9) The receiver sidechain B receives the successful verification of the main chain and sidechain A, and the result of successful data identity verification, confirms that the source of the cross-chain data is authentic, and that the cross-chain data has not been tampered with, receives the receipt of the verification, and confirms the data reception and verification.

5. Experiments
We tested the scalability of BitXHub-PI. Its scalability is manifested by changes in its throughput and latency as the number of access application chains increases. Only one relay chain is used in the experiment, continuously increasing the number of electricity power business application chain clusters, which are heterogeneous chains, e.g. hyperchain and fabric chains. When testing the peak throughput of a certain number of application chain clusters, the peak throughput is measured by continuously increasing the rate of sending simple cross-chain transactions between multiple chains.

The experimental results are shown in figure 3. When the number of BitXHub-PI access application chains is less than 18, the peak performance will gradually increase from 4710TPS to 5957TPS. It has gradually decreased when 18 or more application chains enter, which is due to the network overhead of BFT [13] in the relay chain.

Figure 2. Cross-chain process.
Figure 3. Changes in peak throughput as the number of application chains increases.

6. Conclusion
BitXHub-PI is designed based on the side chain relay strategy. Compared with Polkadot and Cosmos, BitXHub-PI defines a common cross-chain protocol IBTP, which realizes stateless cross-chain message forwarding. Based on the cross-chain pier, multi-level cross-chain message routing is realized, thereby building a highly scalable and compatible blockchain value network. Experiments show that BitXHub-PI can ensure asynchronous distributed transactions between heterogeneous blockchains, and maintain high throughput, low latency, high scalability, low overhead, stable and safe performance.

References
[1] Adrian H B and Stefan T 2016 Interledger: Creating a standard for payments Proc. of the 25th International World Wide Web Conferences Steering Committee (Switzerland: International World Wide Web Conferences Steering Committee) pp 281-2.
[2] Koen T and Poll E 2019 Assessing interoperability solutions for distributed ledgers Pervasive and Mobile Computing 59 101079.
[3] BTC Relay 2017 BTC Relay https://github.com/ethereum/btcrelay.
[4] Chow J 2020 A Bridge between the Bitcoin Blockchain & Ethereum Smart Contracts http://btcrelay.org/.
[5] Adam B, Matt C, Luke D, Mark F, Gregory M, Andrew M, Andrew P, Jorge T and Pieter W 2014 Enabling Blockchain Innovations with Pegged Sidechains https://www.blockstream.com/sidechains.pdf.
[6] Buterin V 2016 Chain Interoperability https://allquantor.at/blockchainbib/pdf/vitalik2016chain.pdf.
[7] Herlihy M 2018 Atomic cross-chain swaps Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing (New York: Association for Computing Machinery) pp 245-54.
[8] Kwon J and Buchman E 2020 A Network of Distributed Ledgers Cosmos https://static.coinpaper.io/files/whitepapers/atomcosmos_whitepaper.pdf.
[9] Wood G 2017 Polkadot: Vision for a Heterogeneous Multi-chain Framework https://polkadot.network/PolkaDotPaper.pdf.
[10] Kwon J 2014 Tendermint: Consensus without Mining https://cdn.relayto.com/media/files/LPgoWO18TCeMlVgJvkt_tendermint.pdf
[11] Buchman E, Kwon J and Milosevic Z 2018 The latest gossip on BFT consensus Preprint arXiv: 1807.04938.
[12] Teutsch J and Reitwießner C 2019 A scalable verification solution for blockchains Preprint arXiv: 1908.04756.
[13] Vukolić M 2015 The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication International Workshop on Open Problems in Network Security (Cham: Springer) pp 112-25.