Computer Networks 218 (2022) 109378

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Review article

An overview on cross-chain: Mechanism, platforms, challenges and advances

Wei Ou [a,b], Shiying Huang [c,*], Jingjing Zheng [c], Qionglu Zhang [d], Guang Zeng [e], Wenbao Han [a]

[a] School of Cyberspace Security (School of Cryptology), Hainan University, Haikou 570228, China
[b] Henan Key Laboratory of Network Cryptography Technology, Zhengzhou 450001, China
[c] School of Computer Science and Technology, Hainan University, Haikou 570228, China
[d] State Key Laboratory Of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[e] Information Engineering University, Zhengzhou 450001, China

ARTICLE INFO

Keywords:
Cross-chain
Interoperability
Value transfer
Notary
Sidechain
Hash-locking

ABSTRACT

After years of in-depth development of blockchain, various blockchains with different characteristics and suitable for different application scenarios coexist in large numbers. Due to the isolation of blockchains and the high degree of heterogeneity between chains, value transfer and data communication between existing blockchains are facing unprecedented challenges, and the phenomenon of value isolated island is gradually emerging. The cross-chain technology of blockchain is an important technical means to realize the interconnection of blockchains and improve the interoperability and scalability of blockchains. In this paper, the development and application of blockchain cross-chain technology are studied, the background and significance of cross-chain technology are described, the research status of cross-chain technology is expounded, the current mainstream cross-chain technologies and cross-chain projects are introduced, the mentioned cross-chain technologies and cross-chain projects are analyzed and compared. In addition, this paper also summarizes the difficulties existing in the current cross-chain technology and provides solutions for reference, so as to lead to the discussion of the development trend of cross-chain technology, and finally complete the summary of the research content of the full text and the prospect of cross-chain technology. It is hoped that the relevant summary results can help relevant researchers and practitioners quickly grasp the research progress in the field of blockchain interoperability, and obtain relevant knowledge and application methods in this field.

1. Introduction

Blockchain technology originated from the groundbreaking paper "Bitcoin: A Peer-to-Peer Electronic Cash System" [1] published by a scholar named "Satoshi Nakamoto" on October 31, 2008. In 2009, he established the first open source project for the blockchain, and Bitcoin was born. As the underlying technology of Bitcoin, blockchain is essentially a decentralized distributed database composed of a series of cryptography-based data blocks arranged in chronological order. The data blocks contain transaction information and data verification information, the consistency and integrity of the system are jointly maintained by all nodes in the Bitcoin P2P network. Blockchain technology is not only a simple integration of various technologies, but also a new Internet concept, economic organization form and trade model. With the rapid development of Internet technology and the rise of new finance, blockchain technology shines brightly and gradually attracts the attention of major companies. The increasingly mature blockchain technology has become the new darling of the market. Although the blockchain has achieved great success in just a few years, we need to pay more attention to its shortcomings: from a local perspective, according to the basic principles of the "three problems of scalability" [2], blockchains can only focus on two features among "decentralization", "scalability" and "security" at the expense of the other, so the performance problem of blockchain has always been criticized. From a global perspective, the number of various blockchains in the world is increasing, but due to the natural "independence" of the blockchain system, there is a lack of effective communication channels between blockchains, and they are separated into "isolated islands", it is difficult to achieve value transfer, which to a certain extent violates the original intention of the decentralized interconnection of the blockchain and

* Corresponding author.
E-mail address: huangshiying@hainanu.edu.cn (S. Huang).

https://doi.org/10.1016/j.comnet.2022.109378
Received 4 May 2022; Received in revised form 6 September 2022; Accepted 19 September 2022
Available online 26 September 2022

hinders the development of the blockchain industry. With the vigorous development of the blockchain industry, the emergence of various public chains, private chains and consortium chains creates a problem that is, how to communicate and even exchange value between different blockchains. In order to make these systems communicate with each other and maximize their value, it is necessary to study cross-chain technology to solve the problems existing in the blockchain in terms of scalability, compatibility, etc. Establish channels for data circulation between different parachains to realize information exchange between chains.

The concept of cross-chain was first proposed by the Tendermint team in 2014. On September 9, 2016, Vitalik Buterin, the founder of Ethereum, published an article "Chain Interoperability" at the R3CEV conference, which raised the issue of blockchain interoperability, and made the concept of cross-chain officially enter the researchers' vision [3]. Cross-chain, in a narrow sense, is the process of asset interoperability between two relatively independent blockchain ledgers; in a broad sense, it is the process of data and asset interoperability between two independent blockchain ledgers. The traditional definition of interoperability in the field of information is: "the ability to exchange and use information between different systems or modules" [4]. Vitalik mentioned in "Chain Interoperability" that the interoperability of blockchain mainly refers to the ability of asset transfer, payment or information exchange between two blockchains, which can be achieved by introducing third parties without changing the native chain. A single blockchain network is a relatively closed system that does not actively interact with the outside world. The assets of each chain also exist as an independent value system. If the isolated island between chains can be opened up and the value can be circulated in the wider world, the value of the token assets can be increased from a wider scope, thereby promoting the rapid development of the blockchain industry. Cross-chain technology is committed to building a bridge of trust between chains, breaking the situation of a blockchain is equivalent to an isolated island, and realizing asset interoperability between chains, so as to achieve a real win-win situation.

The current blockchain world is like the stand-alone era in the 1960s. Blockchains are highly heterogeneous and difficult to communicate with each other. All data and services are limited to isolated blockchains. If all blockchain systems can be linked through a standardized cross-chain protocol, many blockchain systems can work together to provide support for more users and more services. The emergence of cross-chain technology can solve the problems of information dissemination and asset transfer between chains, improve the influence of individual chains on the blockchain system, and maximize individual value. The maturity and popularization of cross-chain technology may detonate the prosperity of the blockchain network.

This paper consists of the following 4 sections: Section 1, Background and application. The research status of cross-chain technology is expounded, and the mainstream cross-chain mechanisms and cross-chain projects are introduced and comparatively analyzed; Section 2, Cross-chain technical difficulties and reference solutions. The transaction, interaction, asset management, security and other aspects involved in cross-chain technology are analyzed, the difficulties of current cross-chain technology are studied, and reference solutions are given; Section 3, The development trend of cross-chain technology. The development of cross-chain technology is a process of constantly solving existing difficulties. This section is derived from the previous section, which aims to let us fully understand the changes and iterations of cross-chain technology, so as to gain a more comprehensive understanding of cross-chain technology; Section 4, Summary and outlook. The full text is summarized, the in-depth research content and work focus of cross-chain technology are prospected.

2. Background

Western countries' research on blockchain started early, and governments, enterprises, scholars and related research institutions in Western countries have increased their investment in this technology. Blockchain technology was first proposed by the Bitcoin founder in the form of POWC (Proof of Work Chain) in the Bitcoin white paper [5]. From the perspective of the country's attention to blockchain, the United Kingdom released the blockchain technology report "Distributed ledger technology: beyond blockchain" in January 2016, the EU also dealt with the "European Blockchain Watch Forum" in 2018 and invested a lot of funds to support blockchain research and development. The United States, Japan, South Korea and the Middle East have also responded positively to blockchain technology, supporting and encouraging the research and development of blockchain projects. Because the governments of western countries invested in the research and development of blockchain technology earlier, the blockchain also spread to various fields earlier in the western countries, which made the cross-chain technology born earlier in the western countries. In addition to the great contributions made by Western countries to the development of cross-chain technology, China has also shown great vitality in the cross-chain field. Blockchain technology started relatively late in China, but in recent years, both the central government and local governments have expressed support for the development of blockchain, and local companies have also increased investment in blockchain technology research. In October 2016, Ministry of Industry and Information Technology released the "China Blockchain Technology and Application Development White Paper" [6]; in December, the State Council also proposed the use of blockchain as the focus of the national layout in the "13th Five-Year Plan". In May 2017, the Hangzhou G20 Summit discussed the opportunities and challenges of blockchain development, which is a milestone in the development of blockchain technology in China. In 2018, the Information Center of the Ministry of Industry and Information Technology released the "2018 White Paper on the Development of China's Blockchain Industry" [7]. In 2019, the People's Bank of China stepped up the promotion of blockchain trade financing platforms, and the Supreme Court of the People's Republic of China also applied blockchain technology to judicial evidence for the first time. Guangdong, Guizhou, Shandong, Hebei and other provinces have also proposed their own blockchain development plans since 2016. Since 2015, Baidu, Alibaba, Tencent, JD, 360 and other well-known Internet companies in China have successively launched blockchain-related technical white papers and applications. Because the blockchain started relatively late in China, research in the field of cross-chain technology still has great development potential compared to Western countries.

Blockchain plays a vital role in Bitcoin, Ethereum, and the Metaverse, and all three are also representative blockchain applications. In May 2017, the market value of Bitcoin accounted for less than 50% for the first time; in August of the same year, the transaction volume of Ethereum surpassed that of Bitcoin for the first time. The number of public chains, private chains, and consortium chains is increasing, the application scenarios of blockchain are more abundant, and the industry's demand for cross-chain is more obvious. Since Facebook officially changed its name to Metaverse in Oct. 2021, the metaverse has become a new norm of social networks and three-dimensional (3D) virtual worlds. This paper takes May 2017 and October 2021 as the dividing line, and is divided into three periods: the Bitcoin blockchain era, the post-Bitcoin blockchain era and the metaverse era, and introduces the development background of cross-chain technology respectively.

2.1. The Bitcoin blockchain era

Judging from the research process of cross-chain technology and related projects in the industry, the earliest appearance of cross-chain technology can be traced back to the cross-ledger interoperability protocol "Interledeger Protocol (ILP)" released by Ripple in 2012. It realizes cross-ledger transfer through the notary mechanism, and proposes a cross-ledger interoperability scheme for the first time in the blockchain

field. In May 2013, Schwartz E., Hope-Bailie A. and Thomas S. proposed the idea of atomic swap, which not only realizes cross-chain asset transactions, but also ensures the atomicity of cross-chain transactions [8,9]. The sidechain is the first cross-chain technology that has a great influence. In 2013, Blockstream first proposed a sidechain solution in the original sidechain white paper, which realizes the value circulation between the mainchain and the sidechain through the two-way peg mechanism. In the white paper "Enabling Blockchain Innovations with Pegged Sidechains" [10] in October 2014, the cross-chain protocol was disclosed, and the concept of Pegged Sidechains was proposed at the same time. It aims to implement more technological innovation and financial innovation without affecting the mainchain. In December 2016, Blockstream further proposed the concept of Sidechains with Strong Federations [11], which introduced multi-signature addresses controlled by multiple parties in asset exchanges to reduce latency and improve interoperability. In November 2015, the Ripple team released the white paper of the Interledger project on the basis of the cross-ledger interoperability agreement. This project uses a notary (also called a connector) to transmit cross-chain information, thereby realizing the asset transfer between heterogeneous chain and homogeneous chain [8, 9]. In January 2016, Joseph Poon and Thaddeus Dryja published the Bitcoin Lightning Network [12] white paper, which aims to realize the fast transaction channel off the Bitcoin chain through the Hashed Timelock [13] mechanism. In May 2016, ConsenSys released the BTC Relay project [14], which broke the isolation between the traditional Ethereum platform and the traditional Bitcoin platform, and also realized the data interaction between them. In June 2016, Kwon J. et al. proposed Cosmos, a new network architecture [15], which supports the entry of many different types of blockchains, and heterogeneous blockchains can interoperate through this architecture. In November 2016, Wood G. proposed the Polkadot project and released a white paper, which is a multiple heterogeneous chain architecture that supports decentralized and trustless interactions between different consensus systems [16]. In September of the same year, Vitalik Buterin published "Chain Interoperability" [17], which made a comprehensive and in-depth analysis of blockchain interoperability issues.

2.2. The post-Bitcoin blockchain era

In October 2017, the Cosmos public testnet gaia-1 was launched, where users can send and receive tokens on the Hub. In December of the same year, Joseph Poon and Thaddeus Dryja conducted a series of interoperable test transactions on Bitcoin Core. In January 2018, gaia-2 was released. The test network realized the dynamic node discovery function. From April to August of the same year, some updates were made every month to continuously improve the test network function and start the corresponding new test network. In May 2020, Polkadot launched the first candidate chain and started the first step of the mainnet launch. In July of the same year, the Sudo permission of the Web3 Foundation was canceled, the on-chain governance function was opened, the governance rights of Polkadot were handed over to the community. The mainnet launch was finally completed in August of the same year. In June 2017, Lv Xujun's team released the Wanchain white paper [18], which is a blockchain cross-chain technology based on intermediate chains and one of the earliest blockchain cross-chain projects in China. The cross-chain transaction mechanism is introduced on top of all the mechanisms of Ethereum, which realizes the functions of anonymity and privacy protection of assets on the chain. In August 2017, Buterin V. and Poon J. proposed the Plasma [19] blockchain scaling design pattern, which implements the scaling computation of the blockchain and is expected to scale to 1 billion state updates per second. The concept of the PalletOne project was born in September 2017, and PalletOne released a white paper in March 2018. In September 2018, PalletOne completed the research and development of Bitcoin and Ethereum adapters to realize cross-chain exchange between the two. In November 2017, the Block Collider team released a multiple public chain cross-chain project [20], which achieved consensus through distance and canceled the role of verifier to achieve true power decentralization. In January 2018, Buterin V. proposed a minimum feasible Plasma implementation based on the Plasma blockchain scaling design pattern, which limits the rewards and punishments of nodes [21]. In July of the same year, Herlihy M. proposed an atomic swap cross-chain protocol, which is based on a Hashed Timelock mechanism, and the transfer of cross-chain assets is represented by a directed graph [22]. In November 2018, Zhang Shitong et al. proposed a multi-party cross-chain protocol based on hash-locking [23], which is a cross-chain protocol extended by atomic swap protocol to solve the asset transfer and settlement of users between different blockchains. In March 2019, NULS released white paper V2.0. This project is responsible for connecting with all chains by the NULS main network, realizing inter-chain communication in an open manner. In March 2019, Ilham A. Qasse et al. published a paper titled "Inter Blockchain Communication: A Survey" [24], in which all available solutions for cross-blockchain communication are surveyed and the proposed architectures are compared. In May 2019, Xie Wenlin proposed a peer-to-peer heterogeneous cross-chain mechanism based on the oracle machine [25], which can realize the message exchange between heterogeneous chains without the need for intermediate chains, reducing the dependence of heterogeneous chains on intermediate chains. In November 2019, Zhao Tao et al. proposed a consensus cross-chain exchange model based on cluster centers [26], which divides the nodes in the blockchain into three types of nodes: consensus service nodes, cross-chain exchange nodes and application nodes, and assign each node a different division of labor to realize asset exchange between different blockchains. In 2020, BitXHub [27], the cross-chain technology platform of Hyperchain, and WeCross [28], the cross-chain platform of WeBank, were open sourced, which greatly promoted the development of building China's domestic independent cross-chain technology platform, focusing on the interoperability of ledgers between heterogeneous consortium chains. Solve the core problems of transaction capture, transmission and verification in cross-chain [29]. BitXHub has achieved consortium cross-chain autonomy by the end of 2021, that is, to support services such as unified identity management, cross-chain permission control, node management, and data auditing. In August 2020, the mainnet of Xinghuo blockchain "Xinghuo·ChainNet" was officially launched. It adopts a two-layer structure and builds a network through super nodes and backbone nodes. In December 2020, the Aelf mainnet was officially launched with unlimited scalability, an innovative cross-chain collaboration mechanism and an elegant multi-level mainchain and sidechain structure. It can provide users with a high-performance, good experience, and reliable large-scale commercial blockchain infrastructure.

2.3. The metaverse era

In October 2021, aelf officially launched the node election and provided technical support for global candidates. In July of the same year, aelf completed the design of the cross-chain bridge's pipeline. The bridge, once fully deployed, will enable two-way token transfers between aelf network and EVM compatible blockchains and facilitates transactions between MainChain AELF and SideChains. In October 2021, Wanchain launched the first crosschain Polkadot bridge, bringing EVM smart contracts to Polkadot allowing developers on Ethereum, Wanchain, and more to integrate DOT into their applications using Wanchain's decentralised blockchain interoperability solution. In March 2022, Wanchain released Wanchain Thrust, a special outreach program focused on business development. Its mission is to find and onboard blockchain projects and DApps to deploy on Wanchain's layer 1 blockchain. In December 2021, BitXHub completed the alliance cross-chain autonomy, that is, it supports services such as unified identity management, cross-chain permission control, node control, and data auditing. In November 2021, Rafael Belchior et al. published a paper titled "A Survey on Blockchain Interoperability: Past, Present, and

Future Trends" [30], whose findings show that blockchain interoperability has a much broader spectrum than cryptocurrencies and cross-chain asset transfers. In December 2021, Peter Robinson published a paper titled "Survey of crosschain communications protocols" [31], which surveys crosschain communications protocols, presenting them based on the top-level usage scenarios they are trying to meet: value swapping, crosschain messaging, and blockchain pinning. In February 2022, with over $130 billion in digital assets under management and more than 260 applications and services built into the network, Cosmos has grown into one of the largest blockchain ecosystems today. As DeFi (Decentralized Finance) develops across chains, more and more people understand the need for blockchain interoperability, and Cosmos is currently leading the way. In April 2022, PalletOne completed the establishment of the application layer database of Token cross-chain project, as well as the coding and deployment of Token cross-chain project Ethereum contract. In July 2022, A new Messari report by Nick Garcia, called "State of Polkadot Q2 2022″ [32], has explored the growth of Polkadot, the multichain network and open platform for safe Web 3.0 innovation, and the number of notable adoption milestones reached so far in 2022. In August 2022, Interlay, a decentralized stablecoin network, launched the wrapped Bitcoin token, InterBTC (iBTC) on the Polkadot network to provide users the option to keep BTC in their Polkadot wallet.

3. Cross-chain mechanisms

In the business application scenarios with increasingly complex business forms, there is a lack of a unified interconnection mechanism between chains, which will greatly limit the development space of blockchain technology. To realize a true value blockchain network, it is necessary to connect homogeneous or heterogeneous blockchain networks. For technical difficulties such as data transmission and transaction access between blockchains, there are core technologies such as notary mechanism, sidechain/relay, hash-locking, distributed private key control, notary scheme + sidechains mixing technology, etc. They solve the problem of cross-chain interaction of blockchains to varying degrees, and realize the free circulation of assets between different chains.

3.1. The current cross-chain mechanisms

Notary mechanism is a cross-chain mechanism that is relatively easy to implement. Similar to the working mode of traditional exchanges, the notary mechanism is to verify and forward cross-chain messages by introducing a trusted third party. When assets are exchanged and transferred in different blockchain systems, one or more organizations are elected as notaries to monitor events on different chains automatically or by request, and reach consensus on whether the event occurs through a specific consensus algorithm, and finally respond in a timely manner [33]. At present, the notary mechanism is divided into a single signature notary mechanism, a multi-signature notary mechanism and a distributed signature notary mechanism according to the difference in signature methods in the implementation process.

Single signature notary mechanism: also known as a centralized notary mechanism, it is the simplest cross-chain mechanism in the notary mechanism. Its essence is to designate a single independent node or institution to act as a notary and the notary undertakes the tasks of data collection, verification, and transaction confirmation in the process of cross-chain interaction. It acts as a conflict arbiter, and then replaces the technical reputation guarantee with a trusted third party [1]. The single signature notary mechanism has the characteristics of strong compatibility and fast processing speed, but the scope of application is relatively limited, and most of them are used for cross-chain asset exchange. The asset exchange process between the Ethereum network and the Bitcoin network based on the single signature notary mechanism is shown in Fig. 1.

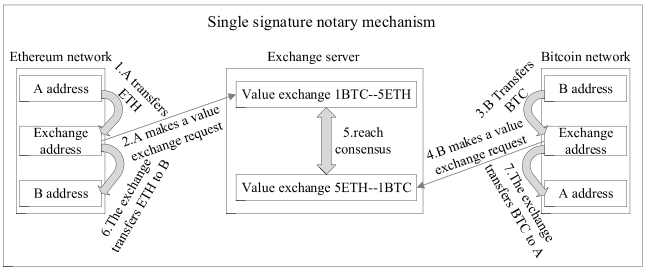


Fig. 1. Flowchart of cross-chain asset exchange between single signature notaries.

User A first transfers the ETH in his wallet address to the account of the exchange address, and then makes a value exchange request to the exchange: 1BTC to 5ETH. Then user B transfers the BTC in his wallet address to the account of the exchange address, and makes a value exchange request to the exchange: 5ETH to 1BTC. As a trusted third party, the exchange transfers the ETH transferred by user A to the wallet address of user B, and at the same time, the exchange transfers the BTC transferred by user B to the wallet address of user A, so that the two parties who match the transaction reach consensus.

Multi-signature notary mechanism: during transaction verification, a part of notaries is randomly selected from the notary group, and then cryptographic technology is used to jointly complete the signature, reducing the degree of dependence on the reliability of notaries. In the multi-signature notary mechanism, the notary is usually a coalition of independent nodes or institutions, each node has a key, only when a certain percentage of notaries jointly sign on their respective ledgers and reach consensus, cross-chain transactions can be confirmed [23,33]. Compared with the single signature notary mechanism, the multi-signature notary mechanism has weakened the risk of centralization and has higher security. When some nodes are maliciously attacked, the operation of the entire cross-chain system will not be affected. The realization process is shown in Fig. 2.

Distributed signature notary mechanism: a notary cross-chain mechanism with higher security and reliability that is continuously optimized on the multi-signature notary mechanism. Compared with the multi-signature notary mechanism, the distributed signature notary mechanism adopts the core idea of MPC (multiparty computation) to ensure the security and privacy of the key [23,34]. The realization process of the distributed signature notary mechanism is to split the unique key generated based on the cryptography into multiple fragments, and distribute the processed fragments randomly to the selected notaries. Even if all notaries piece together the fragments, the key cannot be obtained. Only when a certain percentage of notaries are allowed to complete the signature together can the complete key be pieced together, thereby achieving a more decentralized cross-chain interaction [34]. The realization process is shown in Fig. 3.

In the notary mechanism, the Interledger Protocol [35] (ILP) proposed by Ripple is the most typical notary mechanism technology. The ILP does not need to seek any form of consensus; it provides a top-layer cryptographic escrow system called a "connector". With the help of this intermediary, different blockchain systems can freely transfer digital assets to each other through third-party "validators" [35,36].

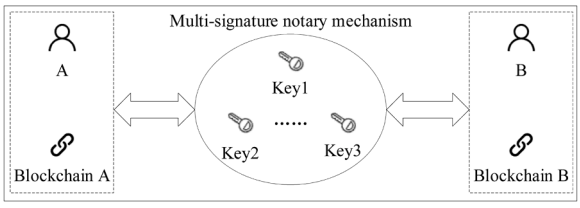


Fig. 2. Flowchart of multi-signature notary mechanism.

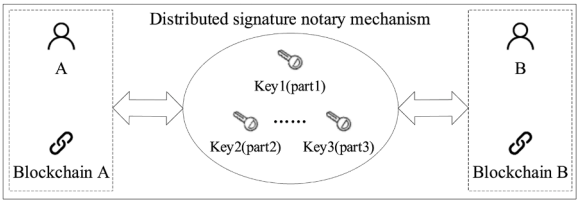


Fig. 3. Flowchart of distributed signature notary mechanism.

Sidechain/relay is a scalable cross-chain technology that can verify transaction data by itself. There is no strict distinction between sidechain and relay. From a formal point of view, sidechain focus on expressing the master-slave relationship between chains, while relay is a technology or solution to realize cross-chain. A sidechain is a concept relative to the mainchain. Compared with the mainchain, there can be multiple sidechains. Assets can be transferred between the sidechain and the mainchain through different two-way peg mechanisms. In this way, digital assets or related transactions can be temporarily transferred to the sidechain when the mainchain is unstable, thereby reducing the pressure on the mainchain and expanding the performance of the mainchain. Relay is a cross-chain operation layer abstractly separated from each mainchain. It provides a unified language. It only collects the data status between the two chains through the middleman for self-verification, which can reduce the security risks of communication between chains and is suitable for linking 2 heterogeneous or homogeneous blockchains [37]. Since the relay cross-chain mechanism needs to wait for the information to be uploaded to the chain, its efficiency is relatively low.

The core technical foundation of sidechain technology is two-way peg. The principle is to temporarily lock the digital assets on the mainchain. After a period of time, the locked transaction is confirmed and sent to the sidechain. The nodes in the sidechain verify locked transactions of the mainchain through the SPV mode, and the equivalent digital assets are released. In the same principle, after the equivalent digital assets are locked on the sidechain and confirmed for a period of time, the digital assets locked by the nodes on the mainchain are released after verification. The incentive mechanism on the mainchain and sidechain determines the security of the two-way peg asset transfer, so that the nodes on the two chains can actively participate in the process of asset transfer and confirm it.

The implementation methods of two-way peg include single hosting mode, alliance mode, drive chain mode, SPV mode, and hybrid mode [11]. The specific implementation principles are as follows.

Single hosting mode: the easiest way to implement two-way peg, the basic principle is the same as the single signature notary mechanism. The transaction participants send the digital assets on the mainchain to a single escrow account address, that is, the address of a fully trusted personal account or exchange. When the custodian receives and confirms the digital assets on the mainchain, the custodian sends the corresponding assets on the sidechain to the sidechain account of the transaction party.

Alliance mode: use the form of a notary union as the asset custodian, and use the multi-signature method to reduce the risk of a single center. Although this method weakens the central form of the single hosting mode, the security still depends on the honesty of all notaries.

Drive chain mode: in the drive chain, the transaction processing node represents the role of the notary group, which is responsible for the custody and unlocking of funds. The transaction processing node submits the information of asset locking on other chains to the block, initiates a proposal, and after voting and confirmation, unlocks the specified asset on the current chain.

SPV mode: SPV (Simplified Payment Verification) is a concept mentioned by Nakamoto in the "Bitcoin White Paper", which means that a light client can verify the existence of a transaction without downloading all block data [38]. An SPV proof consists of two parts: a list of block headers; a cryptographic proof that an output occurs in a block in the list, such as a Merkel proof. To prove that a transaction exists in a block, it is only necessary to use the hash value of this transaction and the hash values of other related transactions to calculate the final Merkle root, and then compare it with the root of the block header. If the calculation result is consistent with the transaction tree root of the block header, it proves that the transaction exists in this block. two-way peg in SPV mode is shown in Fig. 4.

Locking the mainchain assets can be achieved by using a multi-signature account. Waiting for a confirmation period (one or two days) on the mainchain to ensure that enough work is generated to resist denial of service attacks. After the confirmation period of the mainchain ends, the user can generate a generation transaction on the sidechain, and provide the SPV proof of the coin-locking transaction of the mainchain. The generated sidechain assets are in a locked state and need to wait for a competition period. The user waits for a competition period on the sidechain, and the purpose of setting the competition period is to prevent double spending. If during the competition period, the user transfers the coins locked on the mainchain away, and other users can prove this with the latest SPV, the sidechain generation transaction will be invalid, and this proof is called the reorganization proof. After the competition period ends (about 1–2 days), the sidechain tokens are generated and can be circulated on the sidechain. The sidechain tokens are returned to the mainchain and the previous process is repeated.

Hybrid mode: the above methods are all symmetrical, that is, the principle of asset transfer from the mainchain to the sidechain and from the sidechain to the mainchain is the same. In the hybrid mode, the method of two-way peg to solve digital assets can be different. For example, the mainchain to the sidechain uses the drive chain mode, and the sidechain to the mainchain uses the SPV mode.

Hash-locking, whose full name is hash timelock contract, is a cross-chain technical solution to complete inter-chain asset exchange through hash-locks and time-locks without the need for trusted notaries. In the implementation process, the initiator first randomly selects the secret value as the key for hash decryption, then hashes the secret value and sends the obtained hash value as the hash-locked public key to the responder; the initiator and the responder lock their digital assets in the smart contract through the hash value, and set their own time-locks (usually the initiator's time-lock is longer than the responder's time-lock), If both parties provide the secret value within the specified time, the assets locked in the contract will be successfully exchanged, otherwise, as long as any party fails to provide the secret value (the key for hash decryption) within the specified time, the assets locked in the contract will be recovered by the other party. The hash-locked atomic swap protocol ensures that the total amount of assets in the same chain remains unchanged, but the scope of use of hash-locking is relatively limited, and it can usually only be used for cross-chain asset exchange, and cannot realize cross-chain transfer of assets. The most typical application is to use hash-locking to realize the atomic exchange of ETH to BTC. The realization process is shown in Fig. 5.

Specific steps: chain A generates a random number S, calculates the corresponding hash value h at the same time, and transmits h to chain B through the network. Set a time-lock on chain A, and lock BTC in the smart contract of chain A through the hash value h. Chain B sets a time-lock, while using h passed from chain A to lock ETH in the smart contract

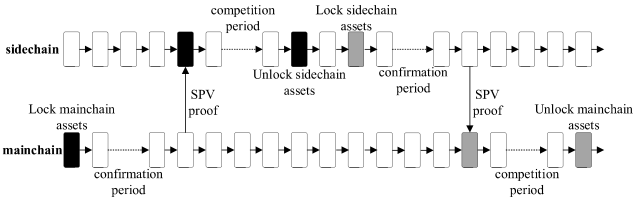


Fig. 4. two-way peg in SPV mode.

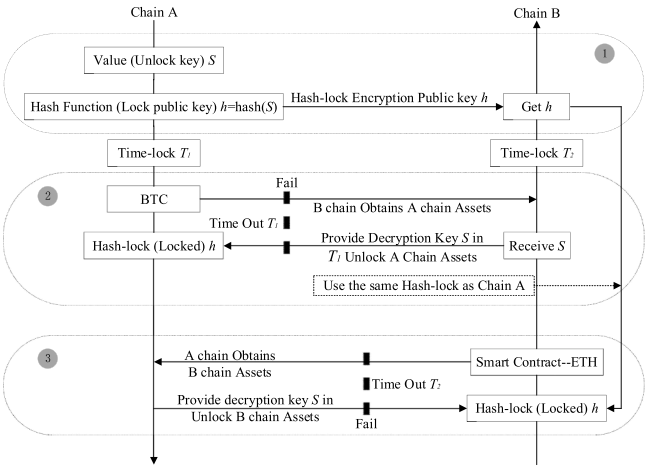


Fig. 5. Flowchart of cross-chain interaction of hash-locking.

of chain B. Chain A provides S (the secret value for unlocking) to chain B within time T_2, chain B transfers the locked ETH to chain A, and chain B obtains S at the same time. If the time expires, the cross-chain fails, and both parties retrieve the assets in the smart contract. Chain B provides S (the secret value for unlocking) to chain A within time T_1, and chain A transfers the locked BTC to chain B. If the time expires, the cross-chain fails, and both parties retrieve the assets in the smart contract. If any chain fails to provide S within the time frame specified by the other party's time-lock, the consequence will be the failure of the entire cross-chain asset exchange.

Distributed private key control, as the name implies, is to use distributed nodes to control the private keys of various assets in the blockchain system, separate the right to use and ownership of digital assets, so that the decentralized system can safely receive the control of the assets on the chain. At the same time, the assets on the original chain are mapped to the cross-chain, so as to realize the asset circulation and value transfer between different blockchain systems [39]. The implementation process of distributed private key control is to use a built-in asset template based on the blockchain protocol, and then deploy new smart contracts based on cross-chain transaction information to create new cryptocurrency assets [26]. When the original chain transfers a registered asset to the cross-chain, the cross-chain node will issue the corresponding equivalent tokens for the user in the existing contract, ensuring that the assets of original chain can still be traded and circulated on the cross-chain.

Notary scheme + sidechains mixing technology is a special cross-chain mechanism. It is known that the notary mechanism has the advantages of simple implementation, easy operation, two-way cross-chain, etc., and the sidechain has the characteristics of independence, speed and efficiency.

Therefore, on the basis of the existing four mainstream cross-chain technologies, the researchers combined the notary mechanism and the sidechain, and proposed this cross-chain mechanism to improve the cross-chain interaction performance, which has been applied in practical scenarios. The notary scheme + sidechains mixing technology gives full play to the advantages of the two mechanisms. Improve the efficiency of efficient communication between blockchain systems through sidechain technology. Use the notary mechanism to realize the cross-chain of assets, and then support the interaction of cross-chain assets, cross-chain contracts and asset mortgages. It achieves the goal of using distributed nodes as the public, avoids centralized control, and is the easiest way to achieve interoperation between chains. While improving the efficiency of cross-chain interaction, the distributed nodes of mutual trust between the blockchains act as notaries to complete asset exchange and realize cross-chain interaction. At present, Ether Universe is the world's first cross-chain service platform based on the third-generation blockchain platform EOS.IO using the notary scheme + sidechains mixing technology. It is a set of completely innovative cross-chain interaction technology solutions [40].

3.2. Comparative analysis

At present, the existing 5 mainstream cross-chain mechanisms have solved various problems of cross-chain to varying degrees, they have also achieved certain performance improvements in some technical bottlenecks. However, due to their different implementation principles and application scenarios, the existing cross-chain technologies have great limitations. In order to understand the differences between the 5 mainstream cross-chains more comprehensively and intuitively, this paper analyzes and compares the interoperability, trust model, number of participating chains, transaction processing, multi-currency smart contracts, security and performance. As shown in Table 1.

The conclusions that can be drawn from the comparison results: in terms of interoperability, hash-locking is a cross-dependence relationship, which is applied to the interaction of locked assets between two chains. Hash-lock and time-lock are used to ensure the atomicity of cross-chain transactions, that is, the transaction can be completed only if certain time conditions and hash conditions are met, which has obvious shortcomings compared to other cross-chain mechanisms; in terms of trust model, the notary mechanism requires multiple trusted third parties as notaries. The algorithm has the risk of centralization, that is, a group of elected notaries still have the potential to do evil, while other cross-chain mechanisms do not have this problem; in terms of the number of participating chains, sidechain/relay technology is a completely decentralized cross-chain solution, but this technology will have the disadvantage of soft forks on the mainchain or sidechain. With the increase of cross-chain transactions, it will have a greater impact on the blockchain system; in terms of cross-chain transaction processing, the limitation of hash-locking is relatively large. In most cases, it can support cross-chain asset mortgage, but it does not directly support cross-chain primitive operations, nor does it support cross-chain asset transfer, that is, the total amount of assets on each chain remains unchanged, and the holders of assets change, while other cross-chain mechanisms can better support related operations of cross-chain transactions. For cross-chain asset transfer, we also need to note that cross-chain asset transfer (one-way) and cross-chain asset exchange (two-way) are two different concepts, and there is no special relationship between the two in terms of support. As mentioned in this section when introducing the specific cross-chain mechanism. Hash-locking can usually only be used for cross-chain asset exchange, and cannot realize cross-chain asset transfer. Not all notary mechanisms support cross-chain asset transfer, it is known that according to the difference in the signature method in the implementation process, the notary mechanism is divided into a single signature notary mechanism, a multi-signature notary mechanism and a distributed signature notary mechanism, and the single-signature notary mechanism only supports cross-chain asset exchange; in terms of multi-currency smart contracts, only the distributed private key control technology can be effectively supported, and other cross-chain mechanisms still need to be optimized and improved; in terms of technical security and performance, the security of notary mechanism and sidechain/relay mechanism is relatively low, and the transaction speed needs to be improved. The notary scheme + sidechains mixing technology are better in terms of security and transaction speed, but it is difficult to achieve. At the application level, the limitations of the cross-chain mechanism should be the main consideration. More importantly, the application of the cross-chain mechanism is not single, and the first consideration for users is how to combine multiple mechanisms skillfully, and maximize the advantages of different mechanisms to achieve complementary purposes. All in all, there is currently no complete set of cross-chain standards and systems applicable to any scenario. In different application scenarios, only by considering the factors and existing problems of the cross-chain

Table 1
Comparative analysis of cross-chain mechanisms.

Projects for comparison	The mainstream cross-chain mechanism of blockchain				
	Notary mechanism	Sidechain/relay	Hash-locking	Distributed private key control	Notary scheme + sidechains mixing technology
Principle of realization	Trust a group of notaries	Collect the information of the original chain and verify it	Validate hash-locks and time-locks	Separation of ownership and use rights of assets	Use notaries for transaction authentication, and use sidechain for Token locking
Interoperability	All	All	Cross-dependence	All	All
Trust model	Most notaries are honest	The chain will not fail	The chain will not fail	The chain will not fail	Mixed model
Number of participating chains	Multi-chain	Double-chain/ multi-chain	Double-chain	Multi-chain	Double-chain/ multi-chain
Cross-chain asset transfer	Support	Support	Not support	Support	Support
Cross-chain asset mortgage	Support	Support	Most support	Support	Support
Applicable cross-chain primitives	Support	Support	Do not directly support	Support	Support
Multi-currency smart contracts	Difficult	Difficult	Not support	Support	Difficult
Cost ratio	Medium	High	Medium	Medium	Low
Security	Low	Low	Medium	Medium	High
Transaction speed	Slow	Slow	Medium	Medium	Fast
Difficulty to achieve	Medium	Difficulty	Easy	Medium	Difficult
Limitation	Relying on a third-party notary	Adapt to many scenarios, absolute consistency of access chain	The scene is single, the initiator has the initiative	The scope of application is small, and the smart contract needs to be improved	Difficult to implement multi-currency smart contracts
Typical case	Ripple	RootStock/Cosmos	Lighting Network	Fusion/Wanchain	Ether Universe

technology in an all-round way, can a suitable cross-chain mechanism be selected and the corresponding practical problems be solved.

4. Cross-chain projects

This chapter classifies cross-chain projects according to the cross-chain mechanism they are based on, and exemplifies representative cross-chain projects in each classification. Since hash-locking is mostly used as a means of implementation, among the cross-chain mechanisms mentioned in the previous chapter, only the notary mechanism, side-chain/relay, distributed private key control, and notary scheme + sidechains mixing technology participate in the classification of cross-chain projects. In addition, cross-chain projects that use other special mechanisms are classified as others.

4.1. Cross-chain project based on notary mechanism

4.1.1. Interledger

Interledger [8] is the most important project based on the notary mechanism, which is implemented by hash-locking. In this project, Interledger focuses on the problem of cross-ledger transactions, creating a system that can interconnect the two parties of the transaction, so that two different systems can exchange currencies without trust through a third-party connector. Interledger uses cryptographic algorithms. Asymmetric encryption is used to provide escrow for the funds created by these two accounting systems and connectors. The realization of mutual transactions requires that all participants reach a consensus on the amount of funds. While providing escrow for the funds created by the two accounting systems and connectors, the ledger will hide the funds that need to be escrow. When a public key that satisfies the pre-defined or a valid signature provided by the hash appears, the ledger verifies its correctness, secures it, and transfers the funds. When the algorithm is correct, all parties involved can conduct transactions without trust. When the two parties of the transaction reach a transaction consensus, cross-ledger funds flow occurs immediately and atomically [41]. A prerequisite for implementing Interledger is escrow Escrow is an operation in which the sender creates an escrow transaction so that its own assets are escrow, but the assets are not transferred at this time; the escrow transaction will be attached with a conditional preimage, and anyone who knows the conditional preimage can confirm or reject the escrow transaction; the sender can attach a time value to the escrow transaction. Within a unit time, the escrow transaction cannot be modified or deleted, but if this time value passes, the escrow transaction will automatically become invalid.

Here we take the cross-chain transaction of A using currency X and B using currency Y as an example to illustrate the specific operation process of Interledger cross-chain transaction, as shown in Fig. 6.

A and B first agree on a shared password, and this password is only known to A and B. B will tell A the unique address of B in its own system. Subsequently, A learns the currency exchange rate through the connecting party C and pays a part of the handling fee to C. A generates an escrow package according to the message format specified in the Interledger protocol, and generates a conditional preimage based on the password agreed by A and B. The preimage is hashed to get the conditions of the transaction. Then, attach this condition and a specified time to the escrow package, and the destination address of this escrow package should be set to C. C detects an operation involving itself on the escrow package and calculates the assets that should be transferred to B. C changes the address in the escrow package to B's address, and sets another time in the escrow package in the Ripper ledger, which should be before the time set by A. B detects an operation involving itself in the Ripper protocol and parses the escrow package, and then verifies the secret corresponding to the conditional preimage to determine whether the transaction asset is real. If B successfully resolves the escrow package, B can accept or reject the transaction. If B accepts the transaction

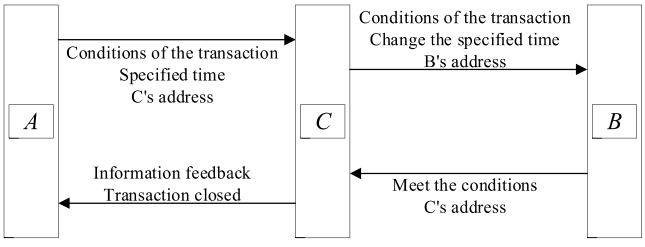


Fig. 6. Implementation of Interledger.

before the specified time, then B will set up a new escrow operation involving C in the Ripper ledger. C confirms the authenticity of the transaction by parsing the escrow package, and then confirms the transaction to get the handling fee.

Therefore, Interledger does not create a unified ledger, nor does it require mutual trust between the participating parties, but proposes a new method of cross-chain asset transfer by determining a protocol. The core of the protocol is to determine the address rules of each account and define the cross-chain messaging format. A transaction can be completed if and only if all actors involved in the transaction reach consensus. The role of the connector does not need to be trusted, and any individual with more than two ledgers can act as a connector, thus ensuring the security of transactions.

4.1.2. PalletOne

PalletOne (Protocol for Abstract-Level Ledger Ecosystem) [42] propose an efficient way to simultaneously solve a few problems related to scalability, interoperability, user-friendliness, and platform lock-in. PalletOne adopts jury consensus as its consensus mechanism, and smart contracts only need a set of validators for verification and execution, these validators are called jurors, and they form a jury. Through the jury consensus protocol, PalletOne completely decouples the smart contract from the underlying blockchain to realize cross-chain value exchange. Mediator is the core component of PalletOne and is responsible for the security of the PalletOne network. The working mechanism of PalletOne is divided into the following stages:

Template Deployment: In PalletOne, smart contracts are used to create all types of services. The creation of contracts is based on contract templates. For ease of use, PalletOne provides users with contract templates for common scenarios. Users can also create new contract templates according to their own needs and deploy them to PalletOne. The deployment of the contract template requires a mediator to complete. Mediator is responsible for checking the syntax, specifications and other factors of the contract template, and only the contract template that meets the requirements can be deployed successfully. The successfully deployed contract template will be saved in Distributed Storage for future use when deploying the contract.

Contract Deployment: If the contract template is not deployed in PalletOne, the user needs to create the corresponding template first. Once a contract issuer attempts to deploy the contract, PalletOne will follow the steps shown in Fig. 7 to deploy.

- Step 1: contract issuer sends the hash value of the contract template code and the initial parameters of the contract to mediator.
- Step 2: mediator will randomly select a specified number of jurors from the candidate jurors according to the contract parameters to form a jury.
- Step 3: juror list of this jury form the contract's jury. At the same time, mediator sends the initial parameters to the jury, and the jury extracts the corresponding contract template code from Distributed Storage.
- Step 4: after receiving the initial parameters and contract template code, the jury members form a new contract, which is independently verified and executed. After verification and execution, the state data, contract ID, and assigned juror list will be saved in Distributed Storage.

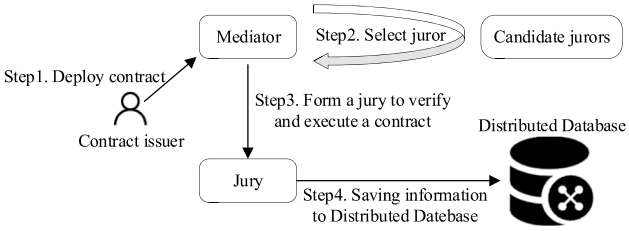


Fig. 7. PalletOne contract deployment diagram.

Contract execution is divided into two jury modes: lock juror mode and unlock juror mode. User can select different kind of jury when creating a contract template according to different application scenarios.

Contract Invocation: after the contract has been deployed, other participants are able to invoke it. The contract invocation process is shown in Fig. 8.

- Step 1: the contract invoker makes a query in the Distributed Storage based on the contract ID. Distributed Storage returns the contract program. In lock juror mode, the list of jurors responsible for contract execution will be returned at the same time; in unlock juror mode, mediator selects a new jury. After obtaining necessary data, the contract will be packaged into the request object along with the parameters and sent to the jury.
- Step 2: jurors will independently execute the contract according to the latest state of the contract and the invocation parameters after receiving the request. If everything works as expected, then the results executed by the jurors will be the same, and the contract state will be shifted to the next one.
- Step 3: if a cross-chain transaction is triggered, jury members will sign a multi-signature transaction on the corresponding blockchain.

Contract Query: after the contract is deployed, the query interface in the contract can be called by the user to query various state data of the contract. The Distributed Storage of PalletOne will not be changed by the query of the contract, so the consensus of the jury is not involved.

Contract Termination: after the contract is executed, or the conditions for termination are met, the contract issuer can apply for contract termination. The contract termination process in PalletOne is shown in Fig. 9.

- Step 1: the contract issuer applies to mediator to terminate the contract.
- Step 2: in lock juror mode, mediator queries and obtains a list of jury members from the Distributed Storage according to the contract ID. In unlock juror mode, mediator re-selects the jury.
- Step 3: mediator sends the contract jury an order to terminate the contract.
- Step 4: jury obtains contract program, state data and other information from the Distributed Storage according to the contract ID.
- Step 5: jury checks the termination conditions of the contract, and if the conditions are met, executes the termination logic defined in the contract.
- Step 6: jury records the contract termination state to Distributed Storage, while returning a termination message to the mediator.
- Step 7: mediator verifies the contract termination state, and the corresponding jury is dismissed after the verification is passed.

4.2. Cross-chain project based on sidechain/relay

4.2.1. Polkadot

Gavin Wood proposed Polkadot [43] in 2016. In the white paper, he

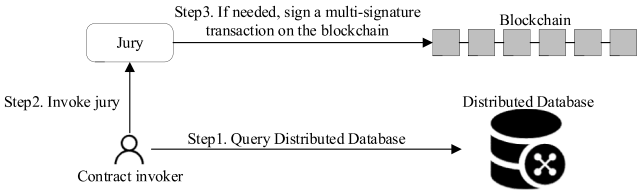


Fig. 8. Flowchart of PalletOne contract invocation.

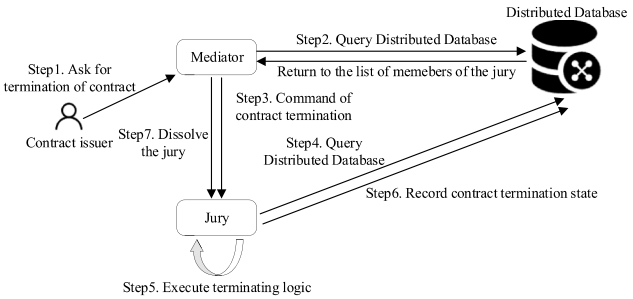


Fig. 9. Flowchart of PalletOne contract termination.

proposed a heterogeneous multi-chain cross-chain platform that supports multi-chain structures, realizing decentralized and trustless cross-chain interaction. The overall architecture of Polkadot is shown in Fig. 10. Unlike the previous implementations that focused on the implementation of different application functions on a single blockchain, Polkadot does not actually provide any inherent functional applications, but provides a large number of relay chains to connect the current independent blockchains. Its purpose is to provide cross-chain communication between different chains, so Polkadot is just a protocol that allows different independent chains to exchange information.

Blockchain has played a lot of roles in all walks of life, but the consistency and effectiveness of the consensus structure are too closely linked, and there are still flaws in many aspects. Five key flaws of existing technologies: scalability, isolation, development, governance, and applicability. Polkadot mainly improves scalability and isolation. As a collection of independent chains, Polkadot has two characteristics: collection guarantees, the blockchain does not need to establish a mining system to protect the security of the network, and existing certifiers and nominees are responsible for the security of the entire network; trustless inter-chain tradability, which is why Polkadot is scalable.

Plokadot can join many parallel blockchains, so this system can scale out to a great extent, which overcomes the disadvantages of poor scalability of blockchains. Although the management model and even the transaction method are different for each chain, through this system, all elements can be processed.

In order to maintain the operation of Polkadot, the participation of the following four roles is required: validators (responsible for verifying the data of the parachain), collators (responsible for collecting the data of the parachain and submitting it to validators), fishermen (responsible for reporting and proving malicious behavior), and nominators (provide deposits and credit endorsements for validators). The cross-chain architecture is shown in Fig. 11.

Validators: validate and finalize parachain candidate blocks, add them to blocks on the relay chain, and receive token rewards. On each block, validators must be ready to accept a new candidate block at any time. This process includes receiving, validating, and republishing candidate blocks. However, it cannot have fully synchronized data for

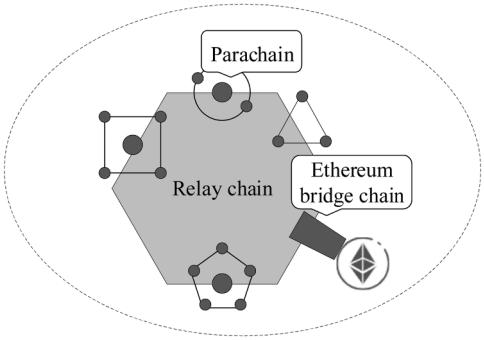


Fig. 10. Overall framework of Polkadot.

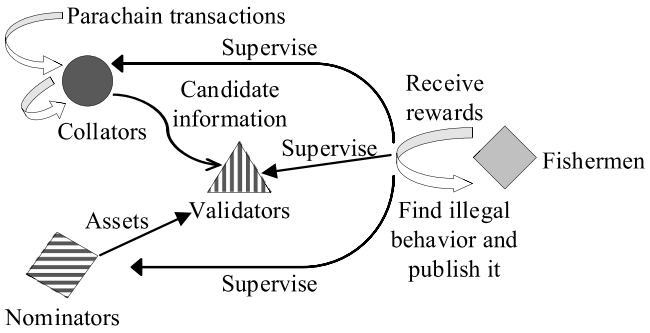


Fig. 11. Participating roles of Polkadot.

all parachains, at which point the collator is required to provide candidates to propose work on new blocks for the parachains.

Collators: verify valid parallel blocks, collect parachain transactions into candidate blocks for validity proof, charge transaction fees, provide candidate blocks to validators, and they will maintain all the information.

Fishermen: they do not directly participate in the interaction and operation between blocks, but independently act as the supervisory police. fishermen who find illegal behavior, such as validators approving invalid blocks or signing two invalid blocks with the same parent block, will receive a large one-time reward.

Nominators: nominators have the right to vote on who is the validator, and no more roles than that. They delegate their security deposit to a validator they trust, who maintains the network; according to the deposit ratio, the deposits they contribute will also increase or decrease proportionally [44].

4.2.2. BitXhub

The overall architecture of BitXHub is shown in Fig. 12, which consists of three roles: application chain, relay chain, and cross-chain gateway.

Application chain: responsible for specific business logic, which can be divided into two types. (1) Homogeneous application chain: a blockchain that supports the BitXHub cross-chain protocol structure. Homogeneous application chains have similar block and transaction data storage formats, and have the same consensus algorithm and security algorithm. (2) Heterogeneous application chains: blockchains that do not necessarily satisfy the block data storage structure, security algorithm and consensus logic directly supported by BitXHub, such as Fabric [45], Hyperchain, etc.

Relay chain: the core of the BitXHub system. As a sidechain of heterogeneous blockchains that have been connected to BitXHub, the relay chain is mainly responsible for the verification, persistence and routing of cross-chain IBTP messages between application chains. The relay chain and multiple application chains form a consortium, so each node of the relay chain is jointly maintained by each application chain, which is a consortium chain. The relay chain adopts plug-in consensus, and uses Hyperchain's RBFT, POS [46], Polkadot's GRANDPA, AVA [47], Algorand [48], Cosmos' Ten-dermint and other consensus algorithms as

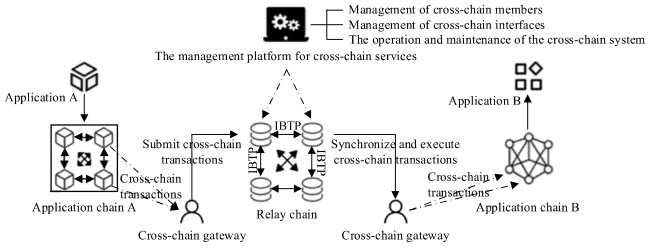


Fig. 12. Architecture of BitXHub.

plug-ins, and dynamically switch according to application chain requirements.

Cross-chain gateway: an independent system between the application chain and the relay chain, which is mainly responsible for the collection of cross-chain transactions and the forwarding of cross-chain transactions. The cross-chain gateway cannot only be used between the application chain and the relay chain, but also realize the routing of cross-chain transactions between the relay chains through the DHT (Distributed Hash Table) [49] P2P ad hoc network.

The management platform for cross-chain services mainly provides the following functions: management of cross-chain members, that is, reviewing the application chain; management of cross-chain interfaces, that is, querying the status of a transaction, querying whether the target blockchain is online, providing relevant template interfaces for cross-chain contracts connected to BitXHub, etc.; the operation and maintenance of the cross-chain system, that is, using monitoring tools to monitor the system situation in real time, and display the heat map of cross-chain transactions in real time.

In order to further improve the scalability of BitXHub, a multi-level overall architecture of BitXHub is proposed, as shown in Fig. 13. The relay chain and multiple application chains form a consortium. The consortiums use the IBTP general cross-chain protocol to route and verify cross-chain transactions. The relay chain can also forward transactions through the IBTP protocol and through the cross-chain gateway of the P2P ad hoc network to achieve highly scalable cross-chain relay. Between the application chain and the relay chain, and between the relay chains, the messages conforming to the IBTP protocol are forwarded through the cross-chain gateway.

Taking the cross-chain transaction of application chain A, a relay chain, and application chain B as an example, to illustrate the simple cross-chain transaction processing flow of BitXHub, as shown in Fig. 14.

The specific steps of cross-chain transaction are as follows:

- Step 1: a cross-chain user on application chain A sends a transaction instruction (the execution function of the instruction contains cross-chain call) to application chain A;
- Step 2: the cross-chain gateway A receives the cross-chain transaction information through the event thrown by the application chain A, and packages it and sends it to the relay chain after collecting enough transaction signatures and transactions;
- Step 3: after the relay chain receives the cross-chain request, the reliability of the transaction is verified. After the verification is passed, it is sent to the consensus module to participate in the relay chain consensus. Finally, the cross-chain transaction is stored from the transaction source queue to the transaction arrival queue, that is, the transaction routing;
- Step 4: cross-chain gateway B synchronizes block headers and cross-chain transactions from the relay chain and submits them to application chain B;
- Step 5: application chain B executes the corresponding cross-chain transaction. If there is a receipt for the cross-chain transaction, the second to fourth steps are executed in reverse.

4.2.3. Aelf

Aelf [50] consists of a mainchain and multiple sidechains attached to the mainchain (Fig. 15). The biggest difference between Aelf and the traditional single-chain system is that it is a "branch ecosystem", and the

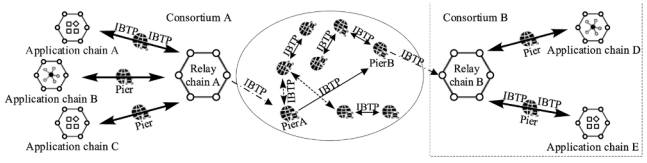


Fig. 13. Architecture diagram of multi-level full topology BitXHub.

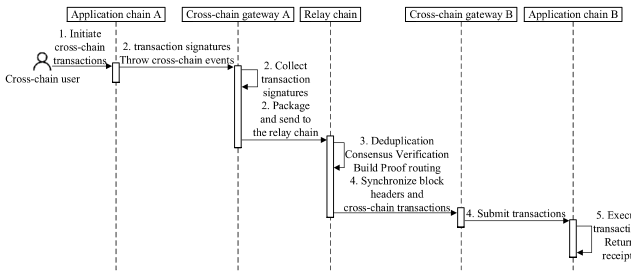


Fig. 14. The simple cross-chain transaction processing flowchart of BitXHub.

mainchain acts as the backbone of the entire system to connect multiple sidechains (may even contain multi-level sidechains).

Aelf can be connected with Bitcoin, Ethereum and some other blockchain systems through adapters, so as to be compatible with existing mainstream ecosystems. aelf sidechains include the system built-in aelf sidechains and other chains generated based on the aelf operating system or aelf kernel. The mainchain interacts with the sidechains by sidechain dynamic indexing. Aelf has the following characteristics:

One Chain One Contract: different from the traditional "one chain to any type of contracts" shown in Fig. 16(a), Aelf proposes a "one chain to one type of contract" structure. As shown in Fig. 16(b), each chain specializes in handling one type of transaction and solving one type of business problem. This makes the entire architecture and data simpler and more in line with business needs. Aelf expands more functionality by adding new sidechains, while maintaining an "easy to manage" structure.

Sidechain Dynamic Indexing: aelf is a dynamic system where all sidechains are attached to the mainchain. The mainchain contains the index of the system boundaries (records to attached sidechains). The interaction between the chains is carried out through the Merkle Tree of the mainchain and the input verification of external messages, rather than direct interaction, so that sidechains can be easily added or deleted in the Aelf system.

"Tree branch" Sidechain Extension: as shown in Fig. 17, Aelf defines a "mainchain and sidechain structure". Theoretically speaking, any sidechain can also be connected with a few sub-chains underneath, and then act as the "mainchain" for that part. This creates a branch structure in the system, giving Aelf the ability to scale both horizontally and vertically. This idea is similar to sharding and partitioning in database architecture. Each shard can perform specific functions, and when a single shard is too large to manage, it is further divided into multiple shards. In Aelf, this corresponds to sidechains.

4.3. Cross-chain project based on distributed private key control

Wanchain [51] provides an infrastructure for cross-chain transfers between different blockchain networks. Wanchain is a distributed ledger, which is characterized by interconnection with different blockchain networks through cross-chain protocols; complete recording of cross-chain transactions, and maintenance of cross-chain transaction details.

Wanchain supports cross-chain transactions between mainstream public chains, cross-chain transactions between consortium chains, and cross-chain transactions between public chains and consortium chains. The Wanchain model is shown in Fig. 18.

The overall architecture of Wanchain can be divided into the following aspects:

Distributed Ledger and Smart Contract Virtual Machine: Wanchain is a general ledger developed based on Ethereum. It can run applications independently, retain account models and smart contracts, and fully realize the original functions of Ethereum. On top of this, a cross-chain transaction mechanism is added, and the privacy protection of smart

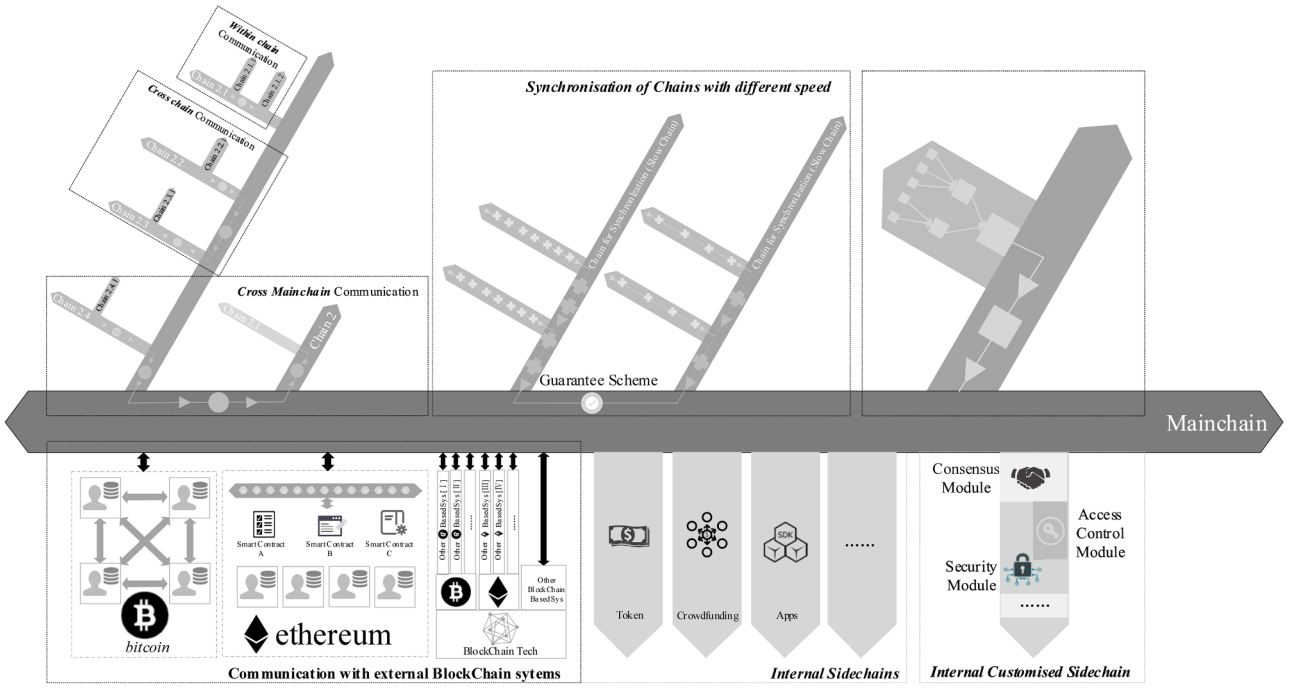


Fig. 15. Aelf Architecture Overview.

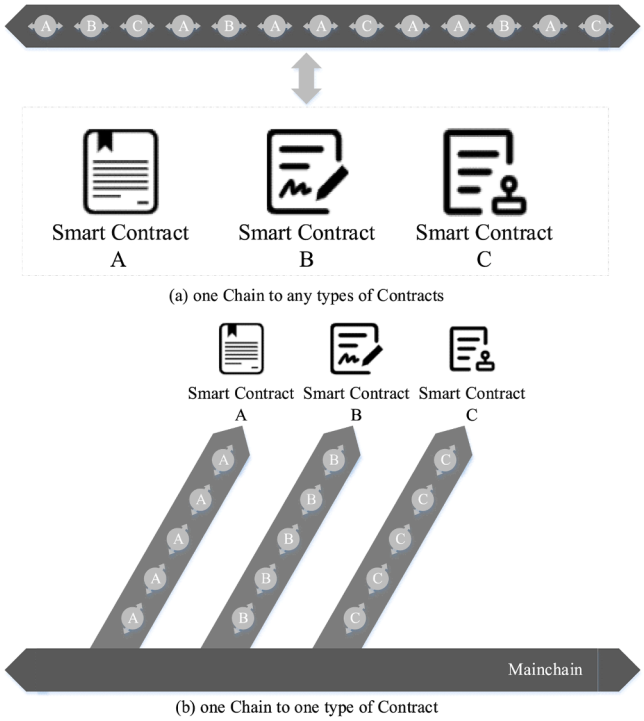


Fig. 16. Complex data structure of blockchain.

contract token transactions is realized.

Native Coin: the native coin of Wanchain is Wancoin. Both ordinary transactions within the chain and cross-chain transactions will consume a certain amount of Wancoin. And Wancoin will also be used as security deposit for verification nodes of cross-chain transactions.

Consensus Mechanism: for the consensus mechanism of ordinary transactions on Wanchain, Proof of Stake (POS) is adopted. At the same time, based on the traditional POS, a consensus and incentive mechanism for cross-chain transactions is introduced.

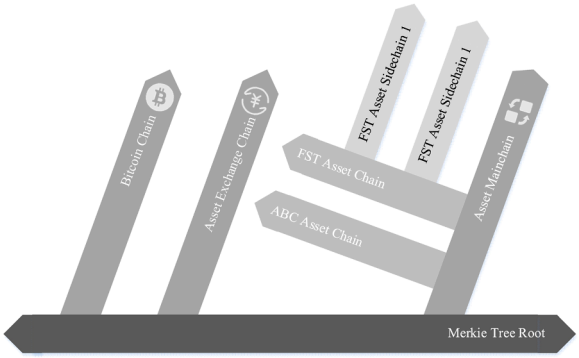


Fig. 17. Multi-level sidechain structure.

Intra-Chain Transactions: ordinary transactions on Wanchain are the same as on Ethereum, but with the addition of a privacy protection mechanism for smart contract token transactions, which is implemented through a one-time account mechanism and a ring signature scheme.

Cross-Chain Integration: both blockchains and assets that integrate with Wanchain first need to complete the registration on Wanchain to ensure that Wanchain can uniquely identify them. These functions are completed via chain and asset registration protocols.

For cross-chain transactions, secure multi-party computing and threshold secret-sharing are used for alliance mode, and minimum-cost access is achieved through cross-chain communication protocol without changing the original chain mechanism. Wanchain is a complete development platform. The public chains, consortium chains and private chains developed by Wanchain have the privacy protection function of smart contract token transactions. Therefore, Wanchain is suitable for a wide range of financial application scenarios. More importantly, other blockchains developed on Wanchain are equivalent to the homogeneous blockchains of Wanchain, have the same cross-chain mechanism as Wanchain, and can seamless connect with Wanchain.

Cross-Chain Transactions: when the original chain transfers an unregistered asset to Wanchain, Wanchain nodes will use a protocol-based built-in asset template to create a new asset, thereby deploying a new

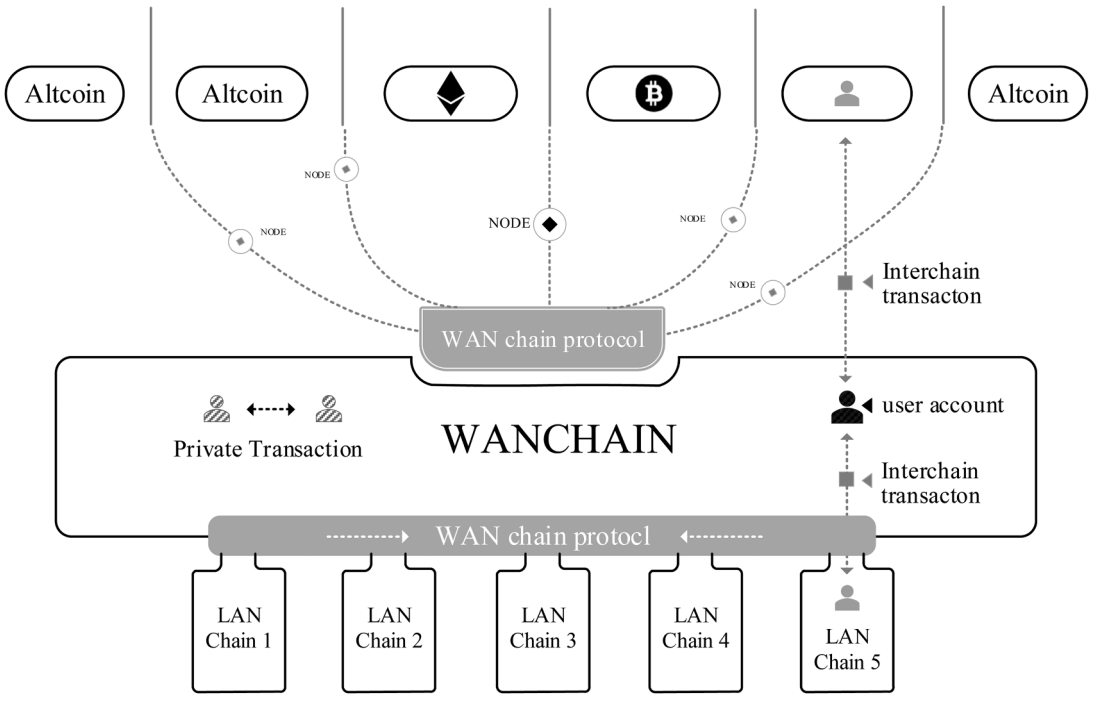


Fig. 18. Wanchain model diagram.

smart contract based on cross-chain transaction information. When the original chain transfers a registered asset to Wanchain, Wanchain nodes will issue corresponding tokens for users in existing contracts, ensuring that the original chain assets can still be traded with each other on Wanchain.

In order to further understand Wanchain, take Ethereum as an example to describe in detail the transfer of assets between the public chain and Wanchain:

Transfer-In Process is shown in Fig. 19: Alice and Bob have accounts on Ethereum and Wanchain respectively, and a transaction to transfer 10 ETH to Bob needs to be completed by Alice. Alice uses Wanchain wallet to send a cross-chain transaction request, and initiates a transfer to Ethereum, and the recipient is Wanchain's cross-chain locked account on Ethereum. The cross-chain transaction request is received by the validator node of Wanchain. The validator node needs to verify that the transaction has been recorded on Ethereum and create a new smart contract token ETH′ (the representative of the ETH on the Wanchain that Alice needs to transfer across the chain) on Wanchain, which corresponds to the ETH that needs to be transferred to Bob on Wanchain.

Transfer-Back Process is shown in Fig. 20: Bob transfers the 10 ETH received from Alice to Cris. Bob uses the Wanchain wallet to initiate a cross-chain transaction to the ETH' asset contract. After the verification node receives the transaction, the value of Bob's asset corresponding to 10 ETH' is turned into a locked state; after the locking is completed, the verification node uses the threshold secret-sharing mechanism to create an Ethereum transaction. The transfer-out party of the transaction is the Locked Account that previously locked Alice's assets, and the transfer-in party is Cris's account on Ethereum; after the verification node verifies the transaction confirmation on Ethereum, it clears the 10 ETH' locked under Bob's account, which means that the assets of the same value have returned to the original chain.

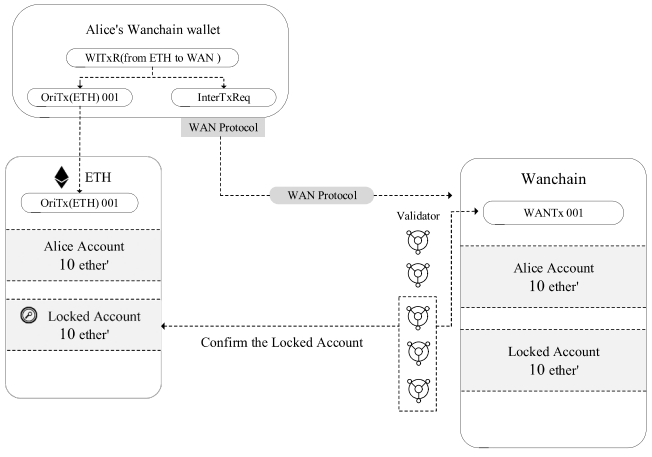


Fig. 19. Cross-chain transaction from Ethereum to Wanchain.

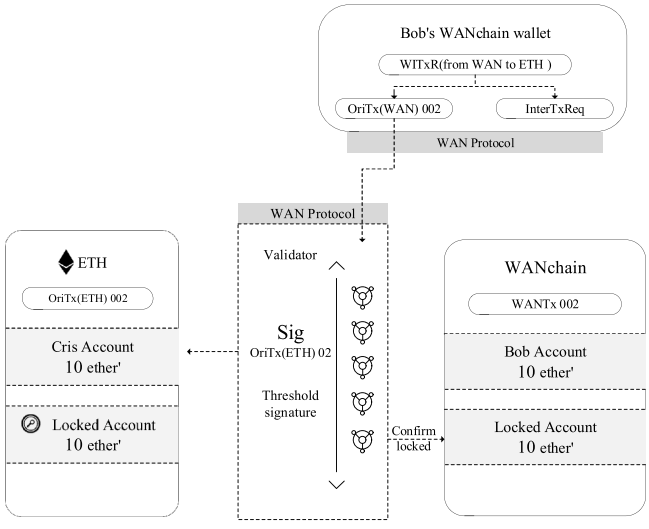


Fig. 20. Cross-chain transaction from Wanchain to Ethereum.

4.4. Cross-chain project based on notary scheme + sidechains mixing technology

The Xinghuo blockchain [52] adopts the master-sub chain architecture, that is, the 1+N architecture of "master chain + sub-chain". The master chain is a permissioned public blockchain based on relay chain technology. Permissioned public blockchain is a blockchain technology system that is compatible with scalability, flexibility, and open access of public blockchains, and integrates the features of consortium blockchains such as ease of supervision, high performance, security and controllability. The master chain supports the entry of homogeneous and heterogeneous sub-chains. After the sub-chain is registered, it can realize cross-chain through the relay chain, which can ensure the safety and reliability of data while decentralizing.

In the Xinghuo blockchain, the master chain ensures the efficient operation of the chain group, and is responsible for chain group management and value anchoring; the sub-chain adopts a self-governance model and is independently designed for different business scenarios to realize the security isolation of data and ensure different requirements for privacy and effectiveness in different scenarios.

As shown in Fig. 21, three types of nodes are set up in the Xinghuo blockchain, namely super nodes, backbone nodes and business nodes. Different types of nodes work together to ensure the stable operation of the chain network.

The super node is mainly responsible for executing the consensus of the master chain, and has functions such as data hosting, qualification review, and chain group management. All nodes in the chain group can apply to become super node candidates and have the right to be elected as super nodes.

The backbone nodes have the functions of anchoring the master chain, sub-chain consensus, sub-chain supervision, smart contract deployment, etc. The sub-chain performs the cross-chain interaction process with the master chain through the backbone nodes, and at the same time assumes the responsibility of the cross-chain gateway. It is the bridge between the master chain and the sub-chain, and realizes the cross-chain communication between the master chains and sub-chains. Xinghuo cross-chain technology is a cross-chain network structure with a high-performance consensus master chain as the core and a sub-chain dynamic access mechanism. The backbone node acts as a cross-chain bridge to ensure the efficiency, scalability and security of the cross-chain technology.

The business node cooperates with the backbone node to execute consensus and execute business activities, and its authority is managed by the backbone node.

In the master-sub chain architecture of Xinghuo blockchain, the master chain is the core of Xinghuo blockchain and consists of multiple super nodes. The super node is responsible for maintaining the stable and safe operation of the entire blockchain, maintaining the registration application and information maintenance of each sub-chain, linking the cross-chain transaction and transaction verification process of each blockchain, ensuring the efficient operation of the chain group and escorting the healthy development of the entire chain group. Sub-chains

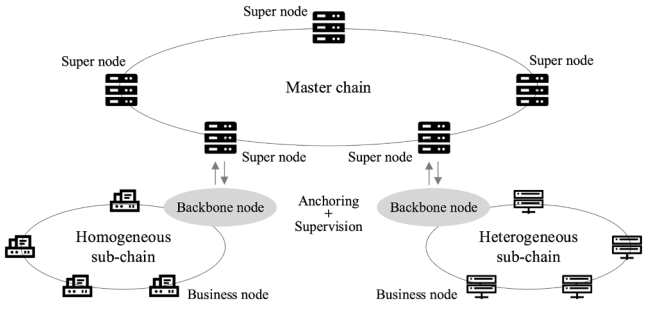


Fig. 21. Xinghuo Blockchain architecture.

are all heterogeneous or homogeneous blockchains participating in the cross-chain ecosystem, which can be various public chains, consortium chains, private chains, etc. It will not affect the normal cross-chain process of other sub-chains, even if an exception occurs, so it can be seen that it has strong independence.

As shown in Fig. 22, a typical cross-chain transaction between master chains and sub-chains is mainly divided into transaction initiation stage, transaction routing stage, transaction verification stage, and transaction confirmation stage.

Transaction initiation stage: mainly by the backbone nodes to monitor the transactions initiated by users and submit them to the cross-chain message queue. In Xinghuo blockchain, the backbone node will monitor and obtain the cross-chain request in the network. When the user invokes the cross-chain contract to initiate a cross-chain request from sub-chain A to sub-chain B, the request will be obtained by the backbone node, and the backbone node will verify the request, confirm the permission of the request originator, cross-chain content and cross-chain serial number, etc. After the verification is correct, the cross-chain request information is formed into data in a specific format and submitted to the cross-chain message queue. If there is a problem with the verification, the transaction is aborted and an error message is returned.

Transaction routing stage: It mainly includes relaying and routing of cross-chain messages. The relay contract in the master chain is responsible for relaying and routing cross-chain requests in the cross-chain message queue, coordinating routing allocation, and transmitting cross-chain transaction information to the corresponding sub-chains. After the cross-chain request from sub-chain A to sub-chain B is sent to the message queue, the relay contract monitors and queries and verifies the corresponding request information, and then forwards the request to the corresponding sub-chain B according to the routing information. The master chain starts the message timing program at the same time. If the feedback information from the corresponding sub-chain is not received within the specified time, it will be treated as a timeout failure. The backbone node of the corresponding sub-chain will monitor all cross-chain transaction requests, and after receiving the cross-chain transaction request forwarded by the relay contract, the transaction will be submitted to the cross-chain contract of the sub-chain for processing; the cross-chain contract of sub-chain B verifies the transactions submitted by the backbone nodes, submits candidate blocks after voting by node signatures, synchronizes the relevant information to the master chain, and submits cross-chain feedback. At the same time, start the timing program and wait to receive the feedback information from the master chain within the specified time.

Transaction verification stage: mainly the verification and synchronization of transaction data. After the master chain receives the cross-chain information fed back by sub-chain B, it first performs SPV verification on the cross-chain transaction, that is, simple verification through the transaction hash value and Merkle tree. After the verification is passed, it is forwarded to the cross-chain initiator sub-chain A. After the backbone node of the cross-chain initiator sub-chain A monitors the cross-chain confirmation information sent by the master chain, it submits the cross-chain feedback to the sub-chain A, and sub-chain A will confirm the cross-chain transaction and submit the confirmed cross-chain transaction to the cross-chain contract; the cross-chain contract of sub-chain A verifies the submitted confirmed transaction information, verifies that the cross-chain transaction really comes from the master chain, and then performs voting verification to ensure the execution of the transaction, and returns the corresponding receipt information at the same time.

Transaction confirmation stage: the master chain completes the final confirmation and generates a cross-chain deposit certificate. After the master chain receives the feedback information, it will perform SPV verification, synchronize the corresponding sub-chain data information, update the block header data, submit the candidate block, wait for the sub-chain to confirm the cross-chain information, and the candidate block will become the formal block; at the same time, a cross-chain

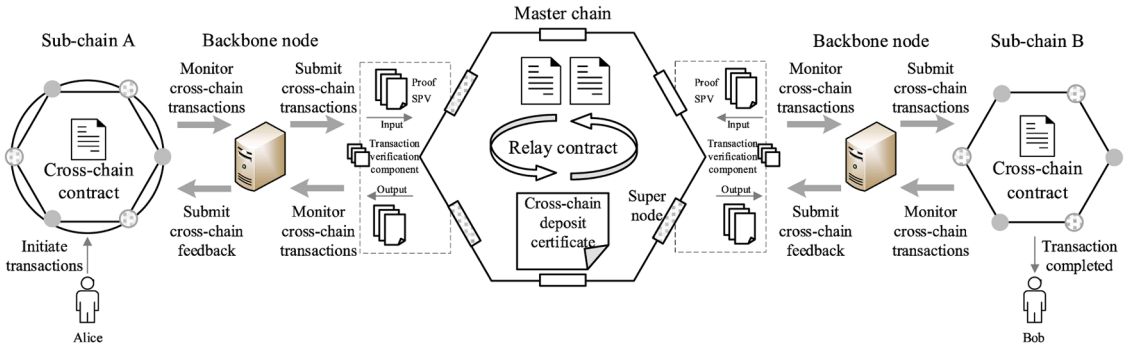


Fig. 22. Cross-chain process of Xinghuo blockchain.

deposit certificate is generated to ensure that cross-chain transactions are authentic and effective. After the cross-chain deposit certificate is generated, it indicates that the cross-chain transaction process has ended normally.

4.5. Others

4.5.1. Commos

Cosmos is a cross-chain project developed by the Berkeley Tendermint team as the core team, and launched on the mainnet in March 2019. Cosmos is a decentralized independent parallel blockchain network [53]. The goal of the project is to create a network that allows all other blockchains to communicate with each other, improve interoperability between blockchains, and communicate in the most efficient and fastest way possible.

The Cosmos network consists of three layers: the application layer, the consensus layer, and the network layer. The application layer is mainly used to design specific business logic, process transactions and update network status. The consensus layer is mainly responsible for the design of the consensus mechanism and helps nodes reach consensus based on the current status of the system.The network layer is used for communication between transactions and blockchains, and is responsible for the design of communication protocols and underlying data structures.

Cosmos Hub is the first blockchain launched on the Cosmos network. The blockchain connected to the Hub through a cross-chain protocol is called a Zone. The Hub acts as an intermediary between all independent blockchain Zones in the Cosmos network. In Cosmos, each Zone can perform its own basic functions, including verifying accounts and transactions, creating and assigning new tokens, etc. The mission of the Cosmos Hub is to facilitate interoperability among all Zones in the network by tracking its state.

Different Zones are connected to the Cosmos Hub through Inter-Blockchain Communication (IBC), which enables information to travel freely and securely between each connected Zone. The implementation of Cosmos is shown in Fig. 23. Once a Zone is connected to the Cosmos Hub, it can interoperate with other Zones connected to that Hub, allowing data to be exchanged between blockchains with different consensus and verification mechanisms. For example, a smart contract on chain A wants to determine if an event has occurred on chain B. For this, the smart contract on chain B needs to obtain the block header of chain A, verify whether it satisfies the consensus and reach the final result [54].

Fig. 23. Implementation of Cosmos.

IBC defines the communication standard between chains and is responsible for routing data packets to a target blockchain, which can process any specific ordered data packet from another blockchain. Each blockchain connected to the Hub keeps track of the block headers of other blockchains. When chain A transfers a fund to chain B, the assets on chain A will be locked first through the IBC protocol, and then a certificate will be sent to the target blockchain B, so the target blockchain will create an asset equivalent to the locked asset accordingly. A similar mechanism is used when restoring assets on the original chain A. For other types of blockchains that do not use the IBC protocol, a proxy chain that complies with both the original chain communication standard and the IBC standard will be developed for the original chain, and cross-chain will be realized through the proxy chain.

4.5.2. WeCross

WeCross's cross-chain system architecture design fully considers the multi-blockchain interconnection across industries, institutions and regions. Whether it is a newly deployed blockchain platform or an existing blockchain platform, based on WeCross' abstraction of the blockchain system, it can seamlessly access the WeCross platform without changing the underlying layer of the original blockchain platform.

The WeCross system architecture includes the following components:

Cross-chain Zone refers to a collection of blockchains running the same type of business. WeCross can name and address the blockchain collection itself and internal blockchain resources. For example, in Fig. 24, the namespace of the deposit certificate service is "deposit certificate zone", and the namespace of the settlement service is "settlement zone".There are two deposit certificate chains in the deposit certificate zone, namely deposit certificate chain A and deposit certificate chain B. An asset deposit certificate resource is deployed on deposit certificate chain A, and the fees and related assets may require deposit certificate. Therefore, according to business needs, cross-chain operations will generate between zones and between chains within a zone.

Cross-chain Router refers to the service process used to bridge the business system and the blockchain. Multiple cross-chain routers can be connected to each other and forward request to each other. Users access resources in cross-chain zones by initiating requests to cross-chain routers.

Cross-chain Stub refers to interface implementation that connects to a blockchain and can be loaded by a cross-chain router. A cross-chain router can configure multiple blockchain stubs to achieve the effect of connecting multiple blockchains. The configuration information of the blockchain stub is automatically synchronized between the cross-chain routers, thereby helping users to address resources located on other blockchains.

Cross-chain Resources refer to data objects accessible to users such as smart contracts and digital assets on the blockchain. Similar to the configuration information of the blockchain stub, the meta information

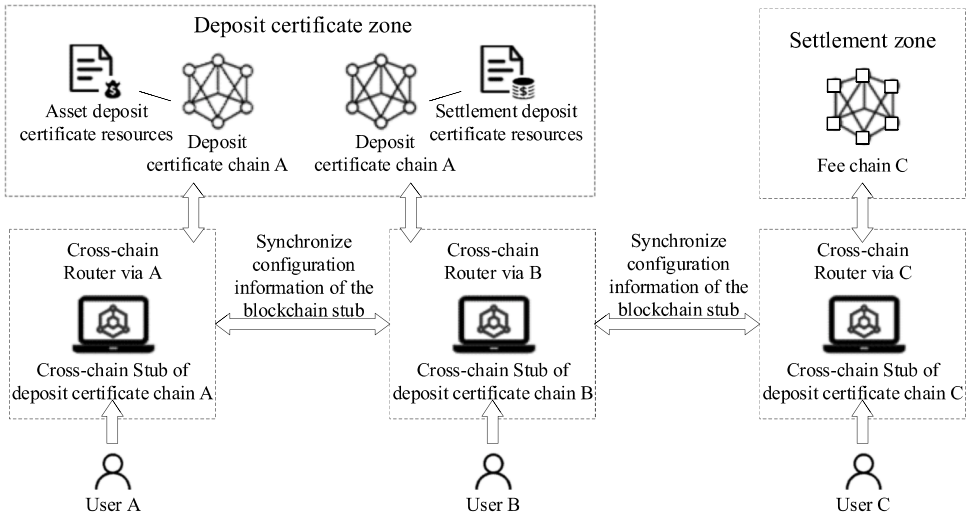


Fig. 24. Cross-chain partition diagram.

of the cross-chain resources is also synchronized between the cross-chain routers. Users address and call resources in cross-chain zones through unified interfaces.

When WeCross processes cross-chain interactions, in addition to transmitting blockchain transaction information, it also transmits relevant proof data of blockchain transactions, and use this information to prove the existence of transactions and receipts (transaction execution results), thereby proving the authenticity and reliability of the information on the chain.

Taking the cross-chain interaction shown in Fig. 25 as an example, institution 1 and institution 2 have deployed blockchain A and blockchain B respectively. Now users of institution 1 want to access blockchain B of institution 2, and the result of the access is required to be authentic and credible, and the sequence of cross-chain interaction is shown in Fig. 26.

Compared with the processing flow of traditional blockchain transactions, WeCross cross-chain router not only transmits the information of transactions and receipts, but also additionally transmits Merkel proofs of transactions and receipts. The sender of the transaction uses these proofs to perform credible verification of cross-chain data access, so that the sender of the transaction can confirm that the transaction has actually occurred on the target blockchain and obtained the result, so as to ensure the authenticity of the transaction and receipt.

WeCross follows the principle that all cross-chain interactive data can be self-certified, and requires interactive response messages to carry both data and proof. This rule is generally applicable to various cross-chain scenarios and can be used to ensure the authenticity and

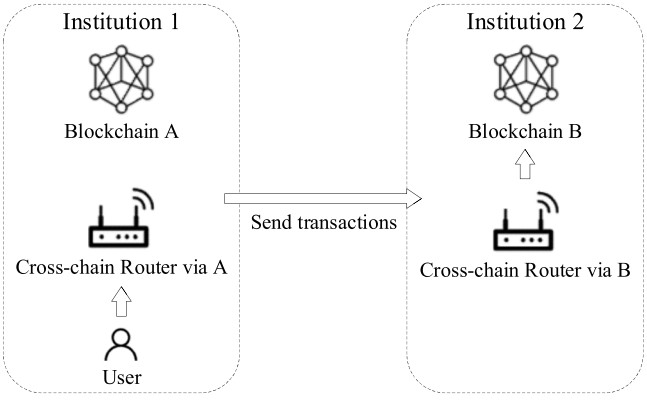


Fig. 25. Example diagram of cross-chain interaction.

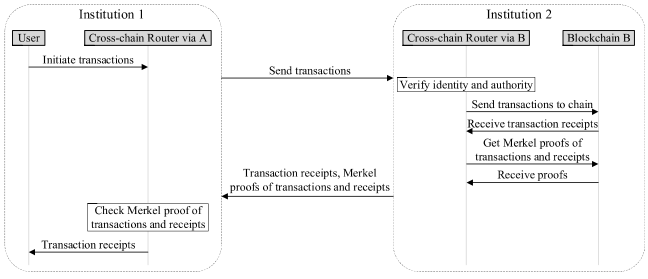


Fig. 26. Sequence diagram of cross-chain interaction.

credibility of the entire transaction process.

4.6. Comparative analysis

This chapter introduces 9 representative cross-chain projects. The cross-chain mechanisms adopted by these cross-chain projects are different, so the characteristics of each cross-chain project are also different. The cross-chain mechanism adopted by the cross-chain project involves its underlying principles and is the basis for the realization of the project. Whether to support atomic transaction, asset pledge, cross-chain authentication, and cross-chain contract are the basic attributes of cross-chain projects. Interoperability and trust model are the core attributes of cross-chain projects.Transaction efficiency and implementation difficulty are the most intuitive performance parameters for the realization of cross-chain projects. Therefore, this paper selects the above aspects to analyze and compare cross-chain projects, as shown in Table 2.

The conclusions that can be drawn from the comparison results: In terms of the applied cross-chain mechanism, a single cross-chain project may involve the integrated application of multiple cross-chain mechanisms mentioned in Section 3. For example, Interledger adopts notary mechanism and hash-locking. Its unique principle design causes its trust model to be different, which is chain failure or 1/3 malicious nodes. In addition, some projects use the communication protocol suite as the cross-chain mechanism. For example, Cosmos will lock the assets on the blockchain through the IBC protocol during the cross-chain process, and then send the certificate to the target blockchain, so the target blockchain will create an asset equivalent to the locked asset accordingly, the application of the communication protocol suite makes the cross-chain process more flexible, but it also increases the difficulty of implementation; in terms of basic attributes, the cross-chain projects

Table 2
Comparison and analysis of cross-chain projects.

Cross-chain project	Cross-chain mechanism	Atomic transaction	Asset pledge	Cross-chain authentication	Cross-chain contract	Interoperability	trust model	transaction efficiency	Difficulty to achieve
Interledger	Notary, hash-locking	Support	Support	Support	Difficult	All	Chain failure or 1/3 malicious nodes	Low	Medium
PalletOne	Notary	Support	Support	Support	Support	All	Most notaries are honest	Medium	Medium
Polkadot	Sidechains/ Relays	Support	Support	Support	Difficult	Chain with relay	Chain failure or 51% attack	Low	Great
BitXHub	Sidechains/ Relays	Support	Support	Support	Difficult	Chain with relay	Chain failure or 51% attack	High	Great
Aelf	Sidechains/ Relays	Support	Support	Support	Difficult	Chain with relay	Chain failure or 51% attack	Medium	Great
Wanchain	Distributed private key control	Support	Support	Support	Support	All	Chain failure or 51% attack	High	Medium
Xinghuo blockchain	Notary scheme + sidechains mixing technology	Support	Support	Support	Difficult	All	Mixed model	High	Great
Cosmos	Relay, communication protocol suite	Support	Support	Support	Difficult	Chain with relay	Chain failure or 51% attack	Low	Great
WeCross	Communication protocol suite	Support	Support	Support	Difficult	All	Chain failure or 51% attack	Medium	Medium

mentioned in this paper all support atomic transaction, asset pledge, and cross-chain authentication. The only difference lies in the difficulty of supporting cross-chain contracts. The main reference conditions are the implementation and storage methods of cross-chain contracts in cross-chain projects. For example, distributed ledger and smart contract virtual machine in the overall architecture of Wanchain make the realization of cross-chain contracts less difficult than other cross-chain projects; in terms of core attributes, there is usually a certain connection between the core attributes and the adopted cross-chain mechanism. For example, the interoperability of cross-chain projects using sidechains/ relays is generally only applicable to chains with relays, and the trust model of cross-chain projects that only use notary mechanisms is that most notaries are honest, and the trust model of cross-chain projects using Notary scheme + sidechains mixing technology is Mixed model; transaction efficiency and implementation difficulty are an overall assessment of a cross-chain project, involving various factors such as the cross-chain project architecture, the design of the cross-chain process, and security assurance.

5. Existing problems

Since the concept of sidechain was proposed, cross-chain has always been the key research direction of blockchain technology. Due to the rapid development of blockchain, the demand for cross-chain has also increased, and related cross-chain technologies are also constantly breaking through. The current difficulties of cross-chain technology and its reference solutions are mainly concentrated in 4 aspects, which are performance and verification of cross-chain transactions, adaptation of multi-chain protocols and connection and interaction, cross-chain transaction and locked asset management, and cross-chain information synchronization and security assurance.

5.1. Performance and verification of cross-chain transactions

The first is the performance of cross-chain transactions. Blockchain is a decentralized ledger technology that needs to ensure openness, autonomy, and non-tampering. Decentraliz ation refers to the use of distributed accounting and storage. There is no centralized management organization or hardware. The obligations and rights of any node are equal. The nodes with maintenance function in the whole system jointly maintain the data blocks in the system. That is to say, any node in the system needs to perform full calculation and storage of transaction data. Therefore, the blockchain is not scalable, that is, the overall performance of the system is limited by the upper limit of the performance of a single node. Even if a large number of nodes are added, the overall performance of the system cannot be improved. The main factors affecting the performance of blockchain transactions include consensus mechanism, transaction verification, broadcast communication, information encryption and other links, but the optimization of these links has not solved the fundamental problem, and its performance improvement is still limited by stand-alone performance. The Lightning Network and State Channel are solutions executed off-chain. They use a centralized system to improve the performance of the blockchain, which is contrary to the concept of blockchain centralization, and is complicated to use and has poor user experience. Both sharding and multi-chain solutions allow each shard or chain to process and store some transaction data. Each shard and chain can process different transaction data in parallel. In this way, the greater the number of shards or chains, the higher the overall performance of the system, for example, the sharding scheme of Ethereum and the multi-chain scheme of Cosmos. The second is the verification of cross-chain transactions. To realize the interconnection between blockchains, and make the transactions of one blockchain can be received and verified by another blockchain, the first thing to do is to design the trust mechanism between blockchain systems. Confirmation and verification of transactions involve two issues, one is to confirm that the transaction has occurred and written into the

blockchain ledger, and the other is to verify that the transaction has been confirmed by enough blocks in the system. At present, the common cross-chain transaction verification mechanisms include the notary mechanism and the "block header + SPV" [35] mode. The notary mechanism is to verify the reliability of the cross-chain message through an external notary (alliance). The notary needs to sign the cross-chain message after the verification is passed. The "block header + SPV" mode saves the block header data of the external blockchain system provided by the notary (alliance) in its own network, and verifies the transaction according to the SPV mechanism.

5.2. Adaptation of multi-chain protocols and connection and interaction

With the development of blockchain technology and the continuous implementation of applications, the future blockchain ecosystem must be a multi-chain coexisting and interconnected ecosystem. Multi-chain interconnection contains two meanings, one is how to realize interconnection of existing blockchain systems; the other is how to pave the way and prepare for the interconnection of blockchains to be developed. Therefore, multi-chain and cross-chain schemes can be divided into active compatible schemes and passive compatible schemes. The active compatible scheme is carried out from top to bottom, mainly for the existing blockchain system. First, there are different upper-layer blockchain application systems, and then the underlying cross-chain mechanism is developed. Usually, the existing blockchain systems are heterogeneous chains, which need to be connected one by one. The passive compatible scheme is designed from the bottom up, mainly for the blockchain system that has not yet been developed. First build the underlying cross-chain platform, then develop a new blockchain system based on the cross-chain platform, or connect the existing blockchain system to the platform in a simple, convenient and safe way to share the convenience of the cross-chain platform system. A single blockchain system is designed without considering the coexistence of multiple chains. A single parachain is a closed and independent system. Different systems are unknown and incompatible with each other. No communication methods were considered in the design, and they developed vertically. Therefore, in order to realize the connection between chains, a specific role must be added to act as the connecting party to undertake the information exchange between the two parties. The form of the connecting party may be various, and it may be through a third party, allowing one or a group of notaries to assume this role; it may also only operate on two parachain participants that need to interact, in the form of a separate module or even an independent chain; It's even just adding a function to the smart contract of one chain that can read the other chain. No matter what form it evolves, the role of the connecting party is irreplaceable. Since different blockchain systems are not designed with the existence of other chains in mind, it is even less likely that a common protocol exists to manage these chain systems. Therefore, it is a great difficulty to realize cross-chain if the connecting party wants to realize the common use of different chains, or be trusted by two different systems, so that two systems that are unknown to each other can conduct secure trade [22]. In the notary mechanism, individuals or groups can be selected through the on-chain or off-chain governance mechanism to play the role of a notary, and play the role of an internal neutral party. The elected notary has the functions of monitoring, viewing, verifying, auditing, etc. In the sidechain mechanism, there are two modes that can act as the connecting party, namely the hosting mode and the SPV mode.

5.3. Cross-chain transaction and locked asset management

A complete cross-chain transaction can be split into several sub-transactions, and each sub-transaction is processed in its own blockchain system. These sub-transactions constitute a transaction, which requires cross-chain transaction management to ensure consistency and atomicity of transaction [55]. Cross-chain transaction management is further divided into two sub-problems, namely the final certainty of transactions and the atomicity of transactions. In cross-chain transaction management, in order to ensure the final certainty of transactions, there are usually three schemes: waiting for enough confirmations, block entanglement, and using consensus algorithms such as DPoS [56]/xBFT. Waiting for enough confirmations is the simplest and crudest method, and the disadvantage is that the transaction processing time will be longer. The principle of block entanglement is to make blocks between two chains have a dependency relationship. When a block on one chain is revoked, related blocks on other chains are automatically revoked. Compared with PoW consensus algorithms, consensus algorithms such as DPoS or xBFT are easier to achieve final certainty, and blockchain systems using such consensus algorithms can realize cross-chain transactions more efficiently. The atomicity of transactions is the basic requirement for realizing cross-chain transactions, and it is also a difficulty that must be solved in cross-chain transactions. Two-way peg is the process of two-way transfer of assets on the mainchain and the sidechain according to a 1:1 exchange ratio. The key issue in two-way peg is who manages the locked account and performs operations such as locking and unlocking, and how to ensure that the locked assets are released safely without causing double-spending [26]. In addition, how to ensure that the total amount of assets in the two chains remains unchanged is equally important. Regarding the management of locked assets, there are currently single hosting model, alliance mode and smart contract mode. The single hosting mode is that a custodian is responsible for managing the locked assets, executing and supervising the unlocking operations of the locked assets. Although the single hosting mode is simple and easy to implement, it relies too much on centralized custodians. The more decentralized mode is the alliance mode. When receiving a cross-chain unlocking request, N notaries in the alliance independently verify the transaction and vote. When the number of votes reaches the threshold M, the locked assets can be disposed of. The smart contract mode is for further decentralization. The premise of this solution is that the blockchain system can support smart contracts and can store the block headers of external blockchains to verify external transaction data.

5.4. Cross-chain information synchronization and security assurance

Cross-chain information synchronization means that after the connection, both parties keep consistent information records to avoid double-spending and assets disappearing out of thin air. First, there are two levels of confirmation of transactions, the first level is that the transaction is verified and considered reliable on the sending chain, and the second level is that the confirmed transaction is confirmed by sufficient chains on the receiving chain. There are two scenarios for asset transactions involved. The first scenario is to change the holder of the asset, but the total amount of assets remains unchanged. This implementation is relatively easy, as long as the respective systems themselves are safe and reliable. The second scenario is to realize the actual transfer of assets. In this case, the actual assets of each chain are changing, so the precise synchronization of information must be ensured. Only when the ledgers of the two chains are completely consistent can the synchronization of information be realized, that is, the atomicity of the transaction is guaranteed. In addition, the crux of the question is whether the total amount of assets in the two chains can still be maintained when a chain is restructured. Since the chains cannot read each other, it is very difficult to achieve complete synchronization of messages. In the strong coupling mode, the communication method of the two chains has been constructed at the time of design. The specific implementation method is as follows: when two interoperable chains are constructed, part of each other's block information is added to their own chain, such as the block header information of the other chain. Therefore, after the construction is completed, the two parties can realize the exchange of information as expected. When the two chains trade, they only need to find each other's information in their own storage space. It can be seen that the strong coupling mode is a good solution to the problem of information

synchronization. When two systems interact, it will inevitably affect each other. If the security between chains cannot be isolated, then if one chain is attacked, the entire cross-chain network will be affected. How to ensure the security of one's own system and the other party's system in the process of cross-chain transactions is a question worth thinking about. In general, it can be considered from the following three aspects: moderate isolation, detection of security incidents, and guarantee of correctness of cross-chain transactions. The chains should maintain their independence, and try to handle cross-chain transactions through third-party nodes or independent modules, so that when problems occur in cross-chain transactions, the processing of transactions on the chain itself will not be affected. If third-party nodes or independent modules have the ability to detect and respond to security incidents, then the isolation of the system architecture is further advanced, so that the cross-chain protocol or system has functions similar to firewalls. Different cross-chain mechanisms also have their own security issues. The first is the trust issue of the notary mechanism. Due to the participation of third-party institutions or organizations, although there are mature election strategies, value transfer or information exchange mainly depends on the honesty of notaries, so the degree of centralization is high. The notary's multi-signature enhances the security to a certain extent through random selection, but does not completely eliminate the relevant dependencies, and there is still a risk of collusion. Some cross-chain projects based on the notary mechanism are also seeking to combine with other technologies, such as Interledger, which incorporates hash-locking mechanism in the protocol to provide more complete security. The second is the security issue of hash-locking. Its technical security is mainly related to the fund locking mechanism and the timeout of the locking time. For example, the Lightning Network based on hash-locking foresees three security risks when the system is designed. The first risk is that malicious actors create a large number of transaction channels and cause all channels to time out at the same time, causing spam transaction information to be broadcast in the network and cause blockages, thereby affecting normal transactions. The second risk is that a certain amount of funds must be locked in the opening phase of the transaction channel, that is, users need to use "hot wallet" to stay connected to the blockchain network for a long time to be able to sign transactions, rather than "cold wallet" or offline storage and other more secure methods, which will increase the risk of hackers stealing users' private keys. The third risk is that if one party to the transaction loses data or does not broadcast the transaction at the correct time, there may be a risk of funds being stolen by the other party. In addition, cross-chain technology also has security issues such as orphan block, long range attack, eclipse attack, cross-chain replay attacks, and compatibility issues after upgrade. It can be seen that in the design process of the cross-chain system, it is necessary to adopt the protection mechanism in time, and at the same time fully understand the security issues that the blockchain technology needs to solve in an all-round way, in order to promote its development in a more diverse direction.

6. Development trend

Cross-chain technology should meet the requirements of low access threshold, good user experience, high transaction efficiency, safe and reliable transactions, and full traceability; at the same time, cross-chain should also support the cross-chain of accounts and data other than the value of digital currencies to meet the integration of multi-chain value.

The development trend of cross-chain technology can be analyzed from the following aspects:

Architecture: research new cross-chain architecture, support data (assets) circulation and contract invocation between multiple heterogeneous (homogeneous) blockchains; for cross-chain communication between homogeneous blockchains, cross-chain communication between blockchains with the same underlying architecture is relatively simple compared to heterogeneous cross-chains. For the cross-chain communication of heterogeneous blockchains, Bitcoin and Ethereum are the two most influential blockchains at present. The former is the earliest blockchain with the highest market value, while the latter has integrated thousands of applications provided by developers around the world. If a cross-chain solution wants to gain global recognition, it must be compatible with these two different types of blockchains. Therefore, after the implementation of homogeneous cross-chain, more research has been invested in heterogeneous cross-chain, thus opening up different value circulation systems and better serving the economic society. As an important computer network technology, virtual networks can ensure the stability and security of the cross-chain process, and can also improve the efficiency of data transmission and network interaction. In addition, compared with the notary mechanism, the virtual networks have a wider range of usage scenarios, including but not limited to the adaptation of multi-chain protocols, the operation of cross-chain transactions, and the management of locked assets. Therefore, integrating virtual networks into the cross-chain architecture is also an advanced development trend.

Interoperability at three levels: study application-layer interoperability, inter-chain interoperability, and off-chain data interoperability; the application-layer interoperability refers to the ability to exchange information between the upper-layer application system instance and the underlying blockchain system instance, and to use the exchanged information. It contains two meanings: data circulation and value sharing between different applications through the underlying chain; docking and interaction between the upper-layer application system instance and the underlying blockchain system instance. This paper focuses on describing the latter, that is, focusing on interface standardization, promoting the compatibility of interfaces of different blockchain systems, and simplifying the adaptation and docking work between upper-layer applications and underlying blockchains. Inter-chain interoperability refers to the ability to exchange information between instances of different blockchain systems and use the exchanged information, that is, cross-chain in the traditional sense. It is mainly manifested in the process of information interaction between different blockchain system instances, including homogeneous blockchain interoperability and heterogeneous blockchain interoperability. Off-chain data interoperability refers to the ability to exchange information between blockchain system instances and off-chain data systems, and to use the exchanged information. It is mainly manifested in the process of secure interaction between the blockchain system and the external data system.

Uniform standards: design cross-chain architecture programming interfaces, shield the technical details of the underlying blockchains, and support developers to quickly build cross-chain applications; in the design and implementation process of the interface layer, it usually involves hierarchical division, interface design, data structure, coding method, communication protocol, etc. A well-designed interface layer can significantly reduce the use threshold of the underlying chain, while providing better security and scalability. Research the safe and efficient cross-chain data transmission and verification mechanism, define the format specification of cross-chain data, and ensure the trusted transmission of data between blockchains; as the carrier of cross-chain messages, communication routing is extremely critical in its versatility and flexibility. At present, different inter-chain interoperability solutions have each implemented their own routing protocols, which solves the interconnection problem between heterogeneous underlying blockchains to a certain extent. However, there are problems of incompatibility between different cross-chain networks in terms of message formats and communication protocols, which hinders the interconnection of different cross-chain networks. In order to improve the versatility and flexibility of communication routing protocols, in the future, multiple manufacturers and standardization organizations will need to build consensus and jointly launch a basic blockchain protocol similar to TCP/IP to promote the development of interoperability.

Governance and Supervision: research the cross-chain transaction processing mechanism, design a cross-chain data (asset) circulation and

contract invocation protocol without single point dependence, and ensure the atomicity of data (asset) circulation and contract invocation under abnormal conditions; research the cross-chain governance mechanism, design the cross-chain system access mechanism, authority mechanism, reward and punishment mechanism, supervision and audit mechanism; cross-chain governance specifically includes the underlying chain authority control mechanism, illegal transaction rollback mechanism, network exception handling mechanism, supervision and audit mechanism, and network upgrade governance mechanism. Currently, the inter-chain interoperability solution is still in the early stage of exploration in terms of cross-chain governance. Take Polkadot as an example in the public chain field. Polkadot manages, routes, and verifies consensus on cross-chain messages through the relay chain. Collators, validators, nominators, fishermen and other different roles cooperate and restrict each other, and combine the reward and punishment mechanism and the mode of council governance to ensure the stable and safe operation of the cross-chain network. Take WeCross as an example in the consortium chain field. WeCross supervision nodes realize penetrating supervision of pre-blocking, in-process supervision, and post-event accountability for key operations, and combine reward and punishment governance mechanism to achieve multilateral governance of cross-chain networks.

Security guarantee: conduct security analysis on the cross-chain system, study various attacks against the system and their corresponding preventive measures, and carry out experimental tests in scenarios such as confrontation in cyberspace. The cross-chain technology is proposed for the cross-chain interaction requirements of the blockchain, so the robustness of the cross-chain technology is bound to be closely related to the various security issues faced by the blockchain in practical applications. The development of cross-chain technology will also be inseparable from the application mode of blockchain technology. The development of the diversity of blockchain technology will put forward higher requirements for cross-chain technology. However, most of the various cross-chain protocols that support cross-chain data communication are currently in the state of research and development, and have not yet received widespread recognition and consensus. Therefore, the analysis of the common security problems of the blockchain is conducive to improving the security loopholes in the cross-chain technology.

7. Summary and outlook

Cross-chain technology has become the core technology for realizing Internet of Blockchains and building value network highways, and it is the technological engine that promotes the cross-scenario integration and development of the blockchain industry. With the continuous exploration of blockchain technology, a blockchain ecosystem will be formed in the future, in which the interconnection and coexistence of multiple chains can be realized. The diversity of blockchains will inevitably lead to increasing requirements for cross-chain technology changes, and the demand for cross-chains will no longer be limited to transactions. In the future, with the continuous popularization of the application of blockchain technology, it is the development trend of cross-chain technology to focus on the research and development of communication technology for data interface similar to the standardization in the Internet, to build Internet of Blockchains, and to realize cross-chain interaction between various blockchains. The biggest problem of current various blockchain systems is the lack of interoperability. Therefore, cross-chain technology should focus on how to adapt to various blockchains and ensure the high efficiency and high security of cross-chain operations. The implementation of cross-chain technology is relatively difficult, and it is still in the development stage, and a completely unified cross-chain standard and stable cross-chain system have not yet been formed. In the future development process, various challenges will inevitably be encountered. In order to realize the real value interconnection, so that the blockchain system can be applied on a large scale like the current operating system supports the TCP/IP protocol, there are still a lot of problems to be solved urgently. For example, security and connection robustness between cross-chain networks, early warning and suppression of malicious behavior between cross-chain networks, the optimization of the incentive system for cross-chain networks, infinite loop of the destination chain in cross-chain transactions, etc. These are all challenges that cross-chain technology has to face in the development process.

In recent years, the popularity of blockchain technology has remained high. Many countries in the world have raised the blockchain to the national strategic level, scrambling to seize the commanding heights of blockchain innovation and development. With the current surge in demand for blockchain application scenarios and strong support from the government, countries around the world have taken blockchain as an important part of the country's new information infrastructure. Cross-chain technology will also be continuously innovated and developed with the in-depth exploration of blockchain technology. At present, cross-chain technology is ushering in a new round of research upsurge. In the future, extensive and in-depth research and exploration will be carried out on the multi-chain protocol interoperability of cross-chain architecture, the security and reliability of cross-chain data transfer and verification, the consistency of cross-chain transactions and contract execution, and the efficiency of access and governance of cross-chain systems, etc. It will break through the technological bottleneck of a new generation of interconnection, credibility and efficiency step by step, support cross-scenario and cross-regional applications, realize cross-chain interoperability and collaboration, create a more dynamic and promising business model, and open an era of multi-chain interconnection.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

No data was used for the research described in the article.

Funding

This work was supported in part by the Hainan Provincial Natural Science Foundation of China (621RC508), Henan Key Laboratory of Network Cryptography Technology (Grant/Award Number: LNCT2021-A16), the Science Project of Hainan University (KYQD(ZR)-21075).

Supplementary materials

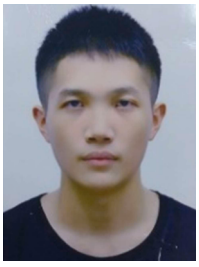
Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.comnet.2022.109378.

References

[1] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, Decent. Bus. Rev. (2008) 21260.
[2] A. Hafid, A.S. Hafid, M. Samih, Scaling blockchains: a comprehensive survey, IEEE Access 8 (2020) 125244–125262.
[3] M. Swan, Blockchain: blueprint for a new economy, " O'Reilly Media, Inc.", 2015.
[4] M. Noura, M. Atiquzzaman, M. Gaedke, Interoperability in internet of things: taxonomies and open challenges, Mobile Netw. Applic. 24 (3) (2019) 796–809.
[5] B. Zhang, The application of foreign blockchain technology and related enlightenment, Financ. Technol. Time 24 (5) (2016) 35–38.
[6] Y. Liu, Blockchain Technology and Its Influence on the Development of Internet Finance Industry, Gansu Financ. 39 (10) (2019) 16–20.
[7] H. Su, The Ministry of Industry and Information Technology released the "2018 white paper on the development of China's blockchain industry, China Auto Parts Market 17 (02) (2018) 15.

[8] A. Hope-Bailie, S. Thomas, Interledger: creating a standard for payments, in: Proceedings of the 25th International Conference Companion on World Wide Web, 2016, pp. 281–282.
[9] E. Schwartz, A payment protocol of the web, for the web: or, finally enabling web micropayments with the interledger protocol, in: Proceedings of the 25th International Conference Companion on World Wide Web, 2016, pp. 279–280.
[10] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, P. Wuille, Enabling blockchain innovations with pegged sidechains [online], 2014, URL http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains.
[11] J. Dilley, A. Poelstra, J. Wilkins, M. Piekarska, B. Gorlick, M. Friedenbach, Strong federations: an interoperable blockchain solution to centralized third-party risks, 2016, arXiv preprint.
[12] J. Poon, T. Dryja, The Bitcoin lightning network. Scalable o-chain instant payments, 2016.
[13] R. Russell, Lightning networks part ii: hashed timelock contracts (htlcs) [online], 2015, URL https://rusty.ozlabs.org.
[14] D. Li, J. Liu, Z. Tang, Q. Wu, Z. Guan, Agentchain: a decentralized cross-chain exchange system, in: 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (Trustcom/BigdataSE), IEEE, 2019, pp. 491–498.
[15] Z. Liu, Y. Xiang, J. Shi, P. Gao, H. Wang, X. Xiao, B. Wen, Y. Hu, Hyperservice: interoperability and programmability across heterogeneous blockchains, in: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019, pp. 549–566.
[16] P. Gaži, A. Kiayias, D. Zindros, Proof-of-stake sidechains, in: 2019 IEEE Symposium on Security and Privacy (SP), IEEE, 2019, pp. 139–156.
[17] V. Buterin, Chain interoperability, R3 Res. Paper (2016) 9.
[18] X. Lv, Wanchain: blockchain cross-chain technology and application ecology, Hangzhou 6 (18) (2018) 32–33.
[19] F. Li, Z. Li, H. Zhao, Research on the progress of blockchain cross-chain technology, J.Softw. 30 (6) (2019) 1649–1660.
[20] I.A. Qasse, M. Abu Talib, Q. Nasir, Inter blockchain communication: a survey, in: Proceedings of the ArabWIC 6th Annual International Conference Research Track, 2019, pp. 1–6.
[21] V.A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, G. Polyzos, Interledger Approaches, 7, IEEE Access, 2019, pp. 89948–89966.
[22] M. Herlihy, Atomic cross-chain swaps, in: Proceedings of the 2018 ACM symposium on principles of distributed computing, 2018, pp. 245–254.
[23] S. Zhang, B. Qin, H. Zhang, Research on the protocol of multiple cross-chains based on the hash-locking, Cyberspace Secur. 9 (11) (2018) 57–62.
[24] I.A. Qasse, T.M. Abu, Q. Nasir, Inter blockchain communication: a survey, in: Proceedings of the ArabWIC 6th Annual International Conference Research Track, 2019, pp. 1–6.
[25] W. Xie, Research On Efficient Consensus and Cross-chain Mechanism of Permissioned Blockchain, Shandong University, Shandong, 2019.
[26] T. Zhao, L. Zhang, Q. Zhao, H. Wang, Across block chain consensus transation model based on cluster center, PeerJ Comput. Sci. 46 (S2) (2019) 557–561.
[27] S. Ye, X. Wang, C. Xu, J. Sun, BitXHub:side-relay chain based heterogeneous blockchain interoperable platform, PeerJ Comput. Sci. 47 (6) (2020) 294–302.
[28] WeCross Technical White Paper Blockchain cross-chain collaboration platform [online], 2020, URL http://www.d-long.com/eWebEditor/uploadfile/20200416165616557031.pdf.
[29] V. Buterin, Minimum viable plasma [online], 2018, URL https://ethresear.ch/t/minimal-viable-plasma/426.
[30] R. Belchior, A. Vasconcelos, S. Guerreiro, M. Correia, A survey on blockchain interoperability: past, present, and future trends, ACM Comput. Surv. (CSUR) 54 (8) (2021) 1–41.
[31] P. Robinson, Survey of crosschain communications protocols, Comput. Networks Chem. Lab., Symp. 200 (2021), 108488.
[32] State of Polkadot Q2 2022 [online], 2022, URL https://messari.io/report/state-of-polkadot-q2-2022.
[33] X. Gu, Current research progress and development prospects of blockchain technology, Inf. Comput. 16 (2018) 106–107 (Theoretical Edition).
[34] F. Mark, Compact SPV proofs via block headercommitments [online], 2019, URL http://sourceforge.net/p/bitcoin/mailman/message/32111357/.
[35] Q. Shao, C. Jin, Z. Zhang, W. Qian, A. Zhou, Blockchain: architecture and Research Progress, Jisuanji Xuebao 41 (05) (2018) 969–988.
[36] J. Mendling, I. Weber, W.V.D. Aalst, et al., Blockchains for business process management-challenges and opportunities, ACM Trans. Manag. Inf. Syst. 9 (1) (2018) 1–16.
[37] W. Chen, Z. Zheng, Blockchain data analysis: current situation, trends and challenges, Comput. Res. Dev. 55 (9) (2018) 1853–1870.
[38] L. Baird, The swirlds hashgraph consensus algorithm: fair, fast, byzantine fault tolerance. Swirlds Tech Reports SWIRLDS-TR-2016-01, Tech. Rep, 2016, p. 34.
[39] H. Wang, X. Song, J. Ke, Q. Xu, Blockchain in digital currency and its privacy protection mechanism, Inf. Netw. Secur. 17 (7) (2017) 32–39.
[40] H. Kim, M. Laskowski, Toward an ontology-driven blockchain design for supply-chain provenance, Intelligent Systems in Accounting, Financ. Manag. 25 (1) (2018) 18–27.
[41] S. Thomas, E. Schwartz, A protocol for interledger payments [online], 2015, URL https://interledger.org/interledger.pdf.
[42] Protocol for abstract-level ledger ecosystem distributed interchain protocol - IP protocol of blockchains [online], 2018, URL https://www.allcryptowhitepapers.com/wp-content/uploads/2018/11/PalletOne_whitepaper_en.pdf.
[43] G. Wood, Polkadot: vision for a heterogeneous multi-chain framework, White Paper 21 (2016) 2327–4662.
[44] Z. Gao, The introduction of cross-chain technology, Cards World 11 (2016) 46–51.
[45] E. Androulaki, A. Barger, V. Bortnikov, et al., Hyperledger fabric: a distributed operating system for permissioned blockchains, in: Proceedings of the thirteenth EuroSys conference, 2018, pp. 1–15.
[46] A. Kiayias, A. Russell, B. David, R. Oliynykov, Ouroboros: a provably secure proof-of-stake blockchain protocol, in: Annual international cryptology conference, Springer, Cham, 2017, pp. 357–388.
[47] T. Rocket, Snowflake to avalanche: a novel metastable consensus protocol family for cryptocurrencies, 2018.
[48] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, N. Zeldovech, Algorand: scaling byzantine agreements for cryptocurrencies, in: Proceedings of the 26th symposium on operating systems principles, 2017, pp. 51–68.
[49] P. Maymounkov, D. Mazieres, Kademlia: a peer-to-peer information system based on the xor metric. International Workshop on Peer-to-Peer Systems, Springer, Berlin, Heidelberg, 2002, pp. 53–65.
[50] aelf - A Multi-chain parallel computing blockchain framework [online], 2018, URL https://aelf.com/gridcn/aelf_whitepaper_EN. pdf? v=1.
[51] Wanchain - Building Super financial markets for the new digital economy [online], 2017, URL https://www.wanchain.org/_files/ugd/9296c5_0d623032c67b4e2380e14452ec02a9e4.pdf.
[52] J. Xie, Z. Li, J. Jin, Cross-chain mechanism based on Spark blockchain, J. Comput. Applic. 42 (2) (2022) 519–527.
[53] Y. Yuan, F. Wang, Parallel blockchain: concept, methods and issues, Acta Autom. Sin. 43 (10) (2017) 1703–1712.
[54] Y. Sun, L. Fan, X. Hong, Technology development and application of blockchain: current status and challenges, Strateg. Study Chin. Acad. Eng. 20 (2) (2018) 27–32.
[55] S. Tan, C. Yang, Research and improvement of blockchain DPoS consensus mechanism. Modern Computer (Professional Edition), 2019.
[56] G.O. Karame, E. Androulaki, S. Capkun, Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin, Cryptol. EPrint Archive (2012).

Wei Ou received his Ph.D. in cryptography from National University of Defense Technology in 2013. He is currently an associate professor at the School of Cyberspace Security (School of Cryptology), Hainan University. His research field is cryptography. His research interests include cryptanalysis, IoT security, and brain-like computing applications.



Shiying Huang is currently an undergraduate student at the School of Computer Science and Technology, Hainan University. His research interests include blockchain and AI security.

Jingjing Zheng is currently an undergraduate student at the School of Computer Science and Technology, Hainan University. Her research interests include blockchain and image encryption.

Qionglu Zhang received his Ph.D. degree in Communication and Information Systems from the University of Chinese Academy of Sciences in 2021. She is currently a senior engineer at the Institute of Information Engineering, Chinese Academy of Sciences. Her research interests include data security and cryptographic applications. Her research interests include IoT security and blockchain.

Guang Zeng received his Ph.D. in cryptography from Information Engineering University in 2013. He is currently an associate professor at the School of Cyberspace Security, Information Engineering University. His research field is cryptography. His research interests include IoT security and protocol security.

Wenbao Han received his Ph.D. in Applied Mathematics from Sichuan University in 1994. He is currently a professor at the School of Cyberspace Security (School of Cryptology), Hainan University. His research field is cryptography. His research interests include cryptanalysis, cryptographic engineering, and brain-like computing.