ISSN 2616-5775 Vol. 6, Issue 7: 1-7, DOI: 10.25236/AJCIS.2023.060701

Research on Blockchain Cross-chain Mechanism and Application

Chen Jiaming[1,2,a,*], Zhang Chen[2,b]

[1]*School of Cyber Science and Engineering, Southeast University, Nanjing, 210096, China*
[2]*Purple Mountain Laboratories, Nanjing, 210096, China*
[a]*chenjiaming@seu.edu.cn*, [b]*zhangchen@pmlabs.com.cn*
[*]*Corresponding author*

Abstract: *With the emergence of Ethereum smart contracts, the number of blockchain platforms and decentralized applications has increased rapidly. However, most of the existing blockchain networks operate in an isolated environment, which brings about the scalability and connectivity issues of the blockchain platform and limits its development. Blockchain cross-chain technology has attracted much attention since the birth of Bitcoin. Its purpose is to realize the interconnection between chains and increase the interoperability of blockchains. It is the essential capability of the future blockchain interconnection network. This article systematically analyzes and summarizes the implementation schemes and projects of cross-chain technology. Firstly, it introduces the background and development history of blockchain cross-chain technology and explains the basic scheme of the cross-chain mechanism. Next, it elaborates on the implementation of three cross-chain applications. In the summary section, the advantages and disadvantages of the cross-chain mechanism and multiple cross-chain applications are summarized. Finally, several future research directions of cross-chain technology are listed.*

Keywords: *blockchain, cross-chain mechanism, cross-chain application*

1. Introduction

1.1. Cross-chain background

In the article published in 2008, Satoshi Nakamoto[1] pioneered a new decentralized electronic currency—Bitcoin. The emergence of Bitcoin represents the birth of blockchain technology. Blockchain was initially proposed as a decentralized digital currency that can be transferred to some new or other chains through cross-chain infrastructure[2]. Just like traditional currencies, their value should be consistent throughout the network. Therefore, the original idea of cross-chain is to solve the demand for asset exchange and transfer between different chains. As blockchains continue to improve, so do transaction processing capabilities. From the original Bitcoin to EOS[3], the consensus algorithm from POW[4] to POS[5] to DPoS[6] and the improvement of various Byzantine fault-tolerant algorithms[7], the transaction throughput has changed from the original number of transactions per second The number of confirmations has increased to tens of thousands of transactions per second. Various public chains and consortium chains continue to emerge, and the implementation of blockchain projects carrying different businesses has formed many isolated value systems. The isolation of data and applications dramatically limits the value circulation of the blockchain[8]. The appeal of blockchain interconnection has led to the birth of cross-chain technology.

1.2. Cross-chain development

The lack of interconnection between different ledgers hinders the development of the entire blockchain application and is one of the critical problems to be solved in future blockchain development. Whether a public or private chain, the ledger information stored on each blockchain is independent, and the information is locked on a single blockchain, which cannot exert more excellent value. From the early days of Bitcoin, cross-chain technology has entered the field of vision. From the initial expansion of a single chain to the collaboration of multiple blockchains to the emergence of a unified blockchain cross-chain platform, cross-chain technology has undergone years of development. In 2012, Ripple proposed the Ripple protocol and the Ripple network[9] , aiming to realize a safe, instant, and almost free global

ISSN 2616-5775 Vol. 6, Issue 7: 1-7, DOI: 10.25236/AJCIS.2023.060701

financial transaction method. In 2014, the Blockstream team first proposed the concept of side chains in a white paper[10]. Through the two-way peg (Two-way peg) technology, the verification of asset locking and unlocking by both sides of the cross-chain is realized, and the transfer of cross-chain assets is realized. The side chain provides the technology of cross-chain transactions of valuable assets and, at the same time, expands the functions of the main chain and increases the throughput of transactions. In 2015, the RSK white paper[11] was released. The RSK development team developed the RSK platform as a Bitcoin sidechain based on Bitcoin and realized the asset transfer between RSK and Bitcoin through two-way anchoring technology. In February 2015, Joseph Poon released the draft white paper of the Lightning Network[12], which puts the transaction process under the chain through the micro-payment channel, and uses the hash time lock mechanism to solve the atomicity problem of multi-node asset transfer. In September 2016, Vitalik[13] described three mainstream cross-chain solutions in the literature : notary mechanism, side chain/relay, and hash-locking. In 2017, the Cosmos[14] and Polkadot[15] projects were launched. Starting from the cross-chain infrastructure, they proposed a plan to build a cross-chain primary platform; Realize intercommunication between blockchain applications. In January 2018, Wanchain[16] officially released version 1.0, using a secure multi-party computing method to manage cross-chain accounts and set up cross-chain nodes with different responsibilities to verify and create transactions that occur in cross-chain transactions Cross-chain contracts for asset management. In 2020, BitxHub, a self-developed blockchain cross-chain infrastructure in China, will be officially open-sourced. Based on the IBTP transaction transmission protocol, BitxHub adopts relay chains and cross-chain gateways to allow heterogeneous blockchains to exchange assets, exchange information, and complement services. In March 2022, the Stargate cross-chain bridge will be released. Based on the LayerZero protocol, Stargate transmits cross-chain transaction information through oracles and repeaters, and users obtain assets from a shared liquidity aggregation pool jointly maintained by multiple chains.

This article mainly introduces the relevant cross-chain mechanism and, at the same time, explains the relevant blockchain projects, providing a reference for future research on cross-chain technology and solving existing mechanism problems.

2. Cross-chain mechanism

Currently, there are three mainstream cross-chain mechanism principles.

Notary group based on third-party trusted entities.

Side chain/relay mechanism independent of the original chain.

Hash locking mechanism based on cryptography.

2.1. Notary mechanism

In order to solve the problem of mutual trust in cross-chain difficulties, a trusted third party is introduced to handle cross-chain transaction verification. The central institution accepts the transferred assets from both parties in the cross-chain, and after the central institution confirms the transaction, it sends the corresponding assets to the two parties in the cross-chain. The notary mechanism is easy to implement and supports cross-chain transfers between various heterogeneous chains, making it easy to connect to existing blockchain systems. According to the number of notaries and signature methods in the trusted third party, the notary mechanism is subdivided into three types: single signature, multi-signature, and distributed signature.

2.2. Side chain/relay mechanism

The side chain mechanism realizes asset transfer through two-way peg technology by adding an auxiliary side chain outside the Bitcoin network. The transfer of assets from the main chain to the side chain is not an actual transfer. The principle is that the main chain locks the assets that need to be transferred, and the same amount of assets are unlocked in the side chain. The side chain is an independent system, and security issues on the side chain will not affect the main chain. At the same time, the side chain can expand the main chain's functions and expand the main chain's business by designing smart contracts with different functions in the side chain. Sidechains/relays most often use the SPV model, which is based on the principle of simple payment-proof SPV and does not require an additional third party to verify transactions.

ISSN 2616-5775 Vol. 6, Issue 7: 1-7, DOI: 10.25236/AJCIS.2023.060701

2.3. Hash-Locking mechanism

HTLC(Hash Time Lock Contract) mechanism was first mentioned in the Lightning Network white paper, using cryptography to solve the problem of trustlessness and decentralization in cross-multi-node payment. Hash lock refers to a mechanism for users to guess the original value of the hash value within a specified period to pay. Based on smart contracts, both parties lock assets through hash locks, and if both parties enter the original value of the correct hash value within a limited time, the transaction can be completed.

3. Cross-chain mechanism

3.1. PalletOne

PalletOne uses a multi-signature notary mechanism. In Palletone, the notary is a juror responsible for verifying the smart contract transaction. Each time, a certain number of jurors are randomly selected from the candidate jury to execute the contract transaction. The jury will be dismissed after the execution of the contract is completed. Each candidate juror needs to pledge a deposit in advance and will be given a transaction fee as a bonus. Palletone adopts the notary consensus, which will effectively reduce network congestion compared with the consensus of the whole network. The asset conversion steps between ETH and BTC are shown in Figure 1.

1) They create a trading contract and choose four jurors as the jury to execute their trading contract. A and B and the jury establish multi-signature accounts as contract accounts in the Bitcoin and Ethereum networks.

2) A and B need to send their tokens to the corresponding accounts. A sends BTC to the contract account in the Bitcoin network, and B sends ETH to the contract account in the Ethereum network.

3) A initiates an application for receiving ETH and signs it with his private key; B can also initiate an application for receiving BTC and signs it with his private key.

4) After the jury checks the status of the contract account, they will sign to allow A and B to withdraw BTC and ETH from the contract account according to the contract status.

5) BTC and ETH will be sent to the respective accounts of A and B.

Due to multi-signature, Palletone sets a threshold for the number of signatures and does not require all jury members to be online, reducing transaction waiting.

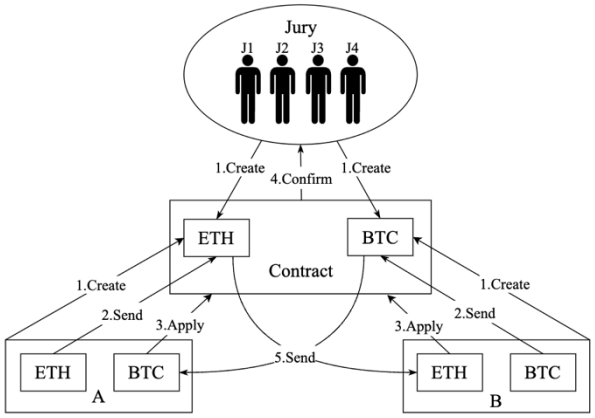

Figure 1: PalletOne Cross-Chain Mode

3.2. Cosmos

Cosmos uses a relay mechanism to achieve cross-chain. It adopts the new blockchain network architecture of Terdermint to create an interconnected blockchain-based development platform.

As shown in Figure 2, Cosmos encapsulates the consensus module and the P2P network module to form Tendermint Core, which separates the blockchain application from the underlying consensus. Cosmos also provides the Cosmos SDK to facilitate developers' modular development. Tendermint Core

ISSN 2616-5775 Vol. 6, Issue 7: 1-7, DOI: 10.25236/AJCIS.2023.060701

interacts with the application layer through the ABCI protocol. Tendermint calls the ACBI interface to send the transaction to be executed to the application layer. The application layer checks the rationality of the transaction and sends it to the designated function module for processing. After the application layer processes and updates the state, it returns the transaction processing result. Each chain runs other chain light clients, and the clients on the chain continuously receive block headers from other chains. When chain A initiates a cross-chain transaction to chain B, chain B verifies the transaction through the received SPV proof. If the verification is passed, chain B will create ten mapped A-Tokens. A-Token carries an A mark, which indicates the source of the Token.

IBC is a communication protocol designed for the Cosmos network and used for message passing between chains. There are two types of blockchains in Cosmos: Hub and Zone. Hub is a relay chain. As the dispatch centre in the Cosmos network, it is a blockchain specially designed to connect Zones together. Zone is an independent blockchain that can perform cross-chain communication, information exchange and asset exchange with the Cosmos major network Hub. When asset conversion is performed with a blockchain that does not adopt the Tendemint consensus, PegZone is used for transfer.

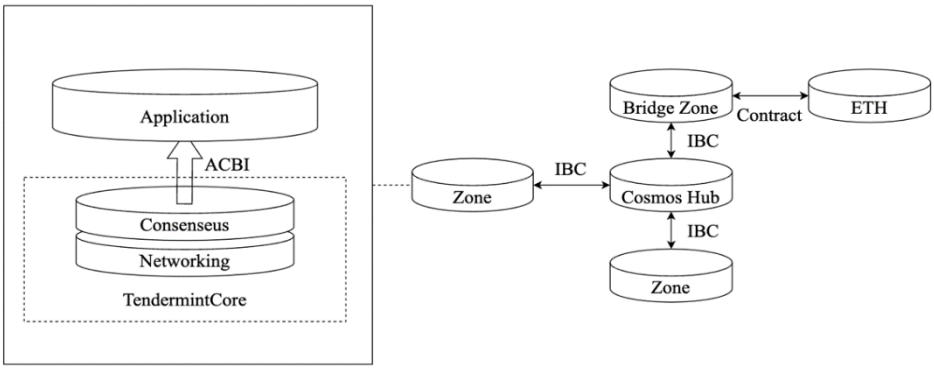

Figure 2: Cosmos Cross-Chain Mode

3.3. Wanchain

WanChain's cross-chain principle includes a hash-locking mechanism and a notary mechanism. Compared with other cross-chain applications, WanChain has added innovations in cryptography. WanChain uses secure multi-party computing and threshold keys to realize asset control and transaction confirmation of distributed nodes.Taking the asset conversion from ETH to WanChain as an example to explain the cross-chain principle. The asset conversion steps from ETH to Wanchain are shown in Figure 3.

1) First, set the Storeman node responsible for managing locked accounts on ETH. The Storeman node will jointly participate in the generation of the locked account, which will accept the transfer funds sent from ETH. The user's wallet will construct a transaction to transfer assets, send the funds to the account managed by the Storeman node, and the hash time lock will lock the transaction.

2) The Voucher node provides proof of asset transfer transactions on ETH. The Storeman node will wait for the Voucher node to send the transaction proof.

3) After receiving the transaction proof, the Storeman node will initiate a transfer contract on the WanChain account, and the payee is the user's account on WanChain.

4) The user wallet will monitor the cross-chain contract transactions on WanChain.

5) When the user's wallet finds a transaction, it will fragment the previously locked secret key to the Storeman node.

6) The Storeman node obtains control over the corresponding ETC in the locked account through the password,

7) The user obtains the Wan transferred from the contract on WanChain. The hash time lock ensures that during the transaction execution process, if the user does not send the password, the ETC control on the original chain will return to the user, and the cross-chain contract transaction will be invalid.

The generation and custody of locked accounts are combined with the notary model. Storeman nodes participating in cross-chain transactions jointly create locked accounts and distribute private key

ISSN 2616-5775 Vol. 6, Issue 7: 1-7, DOI: 10.25236/AJCIS.2023.060701

fragments to each node through threshold key-sharing technology. When it is necessary to transfer funds from a locked account, the account signature is generated by a Storeman node that partially holds the private key fragment through secure multi-party computation. N verification nodes only need to exceed a certain threshold, such as K nodes participating in the transaction, and the signature of the locked account can be generated typically. Therefore, when individual verification nodes are offline or node failures occur, the regular operation of the system will not be affected. This scheme ensures that when the majority of Storeman nodes do evil, the wrong transfer of the locked account will occur.

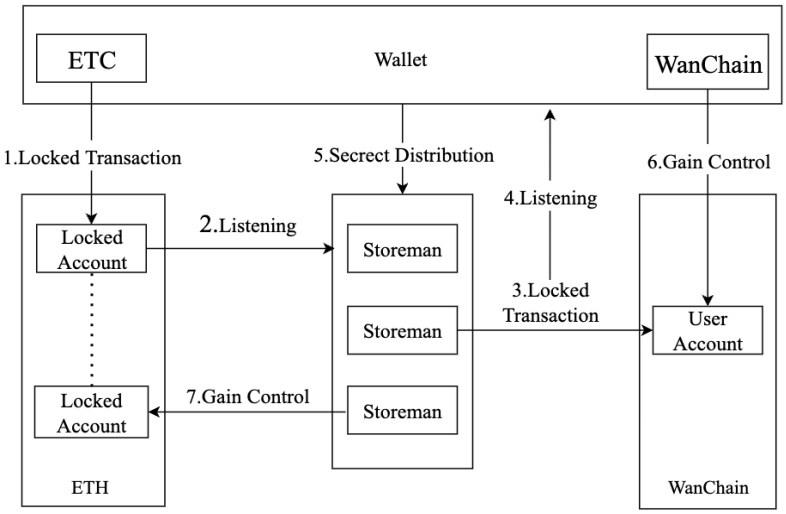

Figure 3: Wanchain Cross-Chain Mode

4. Conclution

Currently, the existing three mainstream cross-chain mechanisms have solved various problems in cross-chain to varying degrees. However, the existing cross-chain technologies have relatively large limitations due to their different implementation principles and application scenarios. In order to understand the differences between the three cross-chain mechanisms more comprehensively and intuitively, this article compares the three cross-chain mechanisms in terms of advantages and disadvantages. The three mechanisms are summarized as follows.

4.1. Notary

Advantages: Compared with other mechanisms, the notary is simple to implement. It supports the access of heterogeneous chains and does not need to add additional program scripts. It only requires the notary to be able to access the information on both chains.

Defects: In order to maintain the trust model, notaries usually mortgage assets to obtain verification rights. Mortgage brings the capital cost to the witness, and the capital cost of the notary will be converted into high cross-chain fees. At the same time, the notary mechanism is contrary to the idea of blockchain decentralization, and the security mainly depends on the honesty of the third party. A single point of failure occurs if a trusted entity is compromised or shut down[17].

4.2. Side-chain/relay

Advantages: Compared with the notary mechanism, the two-way peg technology based on SPV does not require the central node to participate in the verification, eliminating the idea of centralization. At the same time, the side chain mechanism allows users to access various other functions and features provided on the side chain by using the assets of the main chain. Furthermore, sidechains are isolated from the main blockchain, and damage is entirely confined to the sidechain itself.

Defects: The sidechain/relay mechanism can be attacked by 51% computing power[18]. The sender can forge the SPV certificate, especially when the computing power of the sidechain is small. Although the relay chain is currently a commonly used cross-chain mechanism, it is challenging to develop.

ISSN 2616-5775 Vol. 6, Issue 7: 1-7, DOI: 10.25236/AJCIS.2023.060701

4.3. Hash-locking

Advantages: This mechanism does not require trust assumptions and eliminates the dependence on central institutions. HTLC guarantee the atomicity of transaction practices.

Defects: the blockchain must be compatible with HTLC functions. If the hash-locking mechanism wants to conduct cross-chain transactions, it must wait for an online transaction party. Waiting too long will affect the efficiency of the transaction. The hash-locking mechanism in Bitcoin is implemented through two transactions. Both transactions will be uploaded to the chain, increasing the handling fees for both parties.

4.4. Summary of cross-chain application

This article counts the mechanism principles, blockchain platforms, consensus mechanisms, and implementation languages used in some blockchain cross-chain applications, as shown in the following Table 1.

Table 1: Cross-chain Application.

Cross-chain application	Cross-chain mechanism	Blockchain platform	Transaction type	Consensus mechanism	Implementation language
Rsk	Side chain	BTC	Based on transfer	Improved Pow Consensus	Java
PolletOne	Notary	Own chain	Support smart contracts	Notary consensus	Golang
Cosmos	Relay	Own chain	Support smart contracts	Improved Pos Consensus	Golang
Lighting Network	Hash locking	BTC	Based on transfer	Hash algorithm	Golang
Wanchain	Notary Hash locking	ETC	Based on transfer	Improved Pos Consensus	Golang
Polkadot	Relay	Own chain	Support smart contracts	Improved Pos Consensus	Rust

5. Summary And Outlook

This article introduces the development of blockchain cross-chain, analyzes and compares the different types of mainstream cross-chain technologies, introduces related blockchain projects, analyzes the advantages and disadvantages of different cross-chain mechanisms, and finally counts the Characteristics of different cross-chain mechanisms.

Future research directions in blockchain interoperability will depend on addressing the current challenges of available systems. For current industrial solutions, there needs to be a complete interoperable architecture that meets the needs of the industry ecosystem. If interoperability between blockchain platforms can be achieved, blockchain will play a substantial economic value. Blockchain will be more widely used in international finance, data storage and other fields[19].

The formulation of cross-chain communication protocols is an important research direction for the future interaction of heterogeneous blockchain platforms. A successful cross-blockchain communication protocol may become the new backbone of the cross-chain Internet and a standard communication protocol in the blockchain network. There are also research gaps in using smart contracts to create interoperable protocols between homogeneous blockchains. For example, expanding chains through multiple single-chain ledgers requires information communication between ledgers. In addition, the current blockchain projects are widely used in transferring assets or exchanging tokens. The ability to share applications and smart contracts between different blockchain networks can also serve as a future cross-chain research direction.

Cross-chain technology is a critical technology in the blockchain 3.0 era[20]. It builds a bridge between blockchains and realizes the interconnection between chains. Cross-chain technology still needs improvement, and scholars must continue innovating and researching to realise blockchain's interconnection.

ISSN 2616-5775 Vol. 6, Issue 7: 1-7, DOI: 10.25236/AJCIS.2023.060701

References

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Decentralized Business Review, 2008: 21260.
[2] Williams I. Cross-chain blockchain networks, compatibility standards, and interoperability standards: The case of european blockchain services infrastructure[M]//Cross-Industry Use of Blockchain Technology and Opportunities for the Future. IGI global, 2020: 150-165.
[3] Xu B, Luthra D, Cole Z, et al. EOS: An architectural, performance, and economic analysis[J]. Retrieved June, 2018, 11: 2019.
[4] Nair P R, Dorai D R. Evaluation of performance and security of proof of work and proof of stake using blockchain[C]//2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). Tirunelveli, India: IEEE, 2021: 279-283.
[5] Saleh F. Blockchain without waste: Proof-of-stake[J]. The Review of financial studies, 2021, 34(3): 1156-1190.
[6] Yang F, Zhou W, Wu Q, et al. Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism[J]. IEEE Access, 2019, 7: 118541-118555.
[7] Bach L M, Mihaljevic B, Zagar M. Comparative analysis of blockchain consensus algorithms[C]//2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). Opatija, Croatia: Ieee, 2018: 1545-1550.
[8] Pillai B, Biswas K, Muthukkumarasamy V. Cross-chain interoperability among blockchain-based systems using transactions[J]. The Knowledge Engineering Review, 2020, 35: e23.
[9] Jani S. An overview of ripple technology & its comparison with bitcoin technology[J]. 2018.
[10] Back A, Corallo M, Dashjr L, et al. Enabling blockchain innovations with pegged sidechains[J]. URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains, 2014, 72: 201-224.
[11] Rahman A, Hossain M S, Rahman Z, et al. Performance enhancement of the internet of things with the integrated blockchain technology using RSK sidechain[J]. International Journal of Advanced Technology and Engineering Exploration, 2019, 6(61): 257-266.
[12] Lin J H, Primicerio K, Squartini T, et al. Lightning network: a second path towards centralisation of the bitcoin economy[J]. New Journal of Physics, 2020, 22(8): 083022.
[13] Buterin V. Chain interoperability[J]. R3 Research Paper, 2016, 9.
[14] Kwon J, Buchman E. Cosmos whitepaper[J]. A Netw. Distrib. Ledgers, 2019.
[15] Wood G. Polkadot: Vision for a heterogeneous multi-chain framework[J]. White Paper, 2016, 21: 2327-4662.
[16] Lu J, Yang B, Liang Z, et al. Wanchain: Building super financial markets for the new digital economy[R]. Technical report, 2017.
[17] Ou W, Huang S, Zheng J, et al. An overview on cross-chain: Mechanism, platforms, challenges and advances[J]. Computer Networks, 2022: 109378.
[18] Lin S, Kong Y, Nie S, et al. Research on cross-chain technology of blockchain[C]//2021 6th International Conference on Smart Grid and Electrical Automation (ICSGEA). IEEE, 2021: 405-408.
[19] Qasse I A, Abu Talib M, Nasir Q. Inter blockchain communication: A survey[C]//Proceedings of the ArabWIC 6th Annual International Conference Research Track. Rabat Morocco, 2019: 1-6.
[20] Zhong C, Liang Z, Huang Y, et al. Research on Cross-chain Technology of Blockchain: Challenges and Prospects[C]//2022 IEEE 2nd International Conference on Power, Electronics and Computer Applications (ICPECA). Shenyang, China: IEEE, 2022: 422-428.