Research on Cross-Chain Technology Based on Sidechain and Hash-Locking

Liping Deng[1,2(✉)], Huan Chen[1,2], Jing Zeng[1,2], and Liang-Jie Zhang[1,2]

[1] National Engineering Research Center for Supporting Software of Enterprise Internet Services, Beijing, China

[2] Kingdee Research, Kingdee International Software Group Company Limited, Shenzhen, China

liping_deng@kingdee.com

Abstract. Blockchain is a distributed ledger, which includes public blockchains, private blockchains, and consortium blockchains. How to realize the exchange and transfer of value between different blockchains is an important research topic for the expansion of blockchain technology. This article describes what is cross-chain and elaborates the principles and cases of multi-signature wallet. Then it focuses on analyzing the current significant cross-chain technology and successful cross-chain projects. Finally, this article explores a new cross-chain solution.

Keywords: Cross-chain · Notary schemes · Sidechain · Relays · Hash-locking Distributed private key control

1 Introduction

On October 31, 2008, Satoshi Nakamoto first proposed the concept of bitcoin in *Bitcoin: A Peer-to-Peer Electronic Cash System* [1], which opened up a new era of blockchain. Blockchain is a distributed ledger and a continuously growing list of records [2]. Currently, there are three types of blockchain networks: public blockchains, private blockchains and consortium blockchains. If the consensus mechanism is the soul of the blockchain, cross-chain technology is the key to realizing the value network for the blockchain, especially the consortium chain and the private chain. It is a good medicine to save the consortium chain from scattered and isolated islands. And it is a bridge to expand and connect blockchains [3]. From a business perspective, a blockchain is a value network. The more effective nodes that are connected, the wider the distribution, and the greater the resulting value stack. Blockchain is the core infrastructure of value network space. The application of blockchain cannot be confined to a single network.

In order to solve the trust mechanism between different blockchains and realize the information transmission between different blockchains, a cross-chain protocol is needed. The main contribution of this paper is to propose a cross-chain solution based on sidechain and hash-locking, thus constructing a value network highway.

The reminder of this paper is organized as follows: Sect. 2 introduces the related work about what is the cross-chain technology and multi-signature wallet. In Sect. 3, we present the existing cross-chain technology solutions, including Notary Schemes,

S. Liu et al. (Eds.): EDGE 2018, LNCS 10973, pp. 144–151, 2018.
https://doi.org/10.1007/978-3-319-94340-4_12

Sidechain/Relays, Hash-locking and Distributed Private Key Control. Section 4 introduces the current mature blockchain project on cross-chain technology, including Corda, Polkadot, Cosmos, and Wanchain. For Sect. 5, combined with Sidechain and Hash-locking technology, a solution for cross-chain blockchain technology is proposed.

2 Related Work

2.1 What Is Cross-Chain

The real society includes many industries and different economic fields. It is unrealistic to move the entire real world to a blockchain. Goods in different industries and different economic fields can realize value exchange through the market. Each blockchain is an independent value economic system. The cross-chain blockchain is the hub linking independent blockchains and carries the value exchange function of different value system blockchains. Price is the prerequisite for the exchange of goods. The price is determined by the value of the commodity itself and is influenced by the relationship between supply and demand, and the supply and demand relationship is built on the market. In order to realize the exchange of values on different blockchains, there will be various value transaction markets in the cross-chain blockchain. Each value transaction market in the cross-chain blockchain is a cross-chain contract service.

Cross-chain is a technology that allows value to cross the barrier between different blockchains and direct circulation [4]. Each blockchain is an independent ledger, two different blockchains correspond to two different independent ledgers, and there is no correlation between the two ledgers. In essence, value cannot be transferred between ledgers. However, for a specific user, the value stored in one blockchain can be translated into another blockchain value, which is the circulation of value.

Assuming Alice has 1 BTC and Bob has 12 ETHs, how can they trade? From the ledger point of view, the process of cross-chain operation is as follows (Table 1):

Table 1. Cross-chain operation process.

	Before transaction	Transaction	After transaction
Alice	1 BTC	Alice transfers 1 BTC to Bob	0
	0		12 ETHs
Bob	0	Bob transfers 12 ETH to Alice	1 BTC
	12 ETHs		0

To sum up, the core of cross-chain technology is to help user Alice on the Bitcoin blockchain to find Bob, the user who is willing to swap with the Ethernet blockchain. From a business perspective, cross-chain technology is an exchange that allows users to cross-chain transactions at the exchange.

Since Bitcoin and Ethereum belong to different blockchains, how do users between different blockchains establish trust mechanisms? If Alice transfers Bitcoin to Bob but Bob does not transfer Ethereum to Alice. So what should we do?

2.2 Multi-signature Wallet

In order to establish trust between Alice and Bob, trust transfer can be conducted through the trading platform. First, Alice transfers 1 BTC to the platform, and Bob transfers 12 ETHs to the platform. The trading platform then transferred 12 ETHs to Alice and 1 BTC to Bob. By holding a digital currency in the middle of the trading platform, the transfer of trust is realized, ensuring that Alice and Bob can perform cross-chain operations.

However, the trading platform must be credible? If he runs Alice's BTC and Bob's ETH. So what should we do? If the trading platform is operated by multiple entities, or is a public chain, anyone can participate in the operation of the trading platform. the risk of him running can be greatly reduced.

Using a multi-signature wallet allows multiple entities to jointly control an account [5]. In simple terms, multi-signature means that multiple users digitally sign the same message. In principle, A multi-signature address is an address that is associated with more than one ECDSA private key. The simplest type is an m-of-n address that is associated with n private keys, and sending bitcoins from this address requires signatures from at least m keys. A multi-signature transaction is one that sends funds from a multi-signature address.

Taking 2/3 multi-signature as an example, Alice, Bob, and the trading platform all have signing rights. If two of the principals confirm the signature, the transaction can proceed. Bob transfers 12 ETHs to a multi-signature address that is associated with a three-party private key. If the transaction is not going well, both Alice and Bob can arbitrate. After being investigated by the trading platform, they can decide whether to transfer ETH to Alice or return it to Bob through a signature.

3 Cross-Chain Technology

There are natural obstacles to the distribution of value between blockchains. Cross-chain is a complex process. It requires not only a separate verification capability for the nodes in the blockchain, but also a decentralized input, as well as the acquisition and verification of information outside the blockchain. Currently, cross-chain technologies mainly include: Notary schemes, Sidechain/Relays, Hash-locking and Distributed private key control.

3.1 Notary Schemes

The easiest way to interoperate between chains is to use the notary schemes [6]. In the notary mode, a trusted individual or group is used to declare to a blockchain that something has happened on another blockchain, or to make sure that the claim is correct. These groups can both automatically listen to and respond to events and listen and respond to events when they are requested.

Assuming that Alice and Bob can't trust each other, the third party that both Alice and Bob can trust is the intermediary of the notary. This establishes an indirect trust mechanism between Alice and Bob. The representative scheme is Interledger, which is not itself a ledger and does not seek any consensus. It provides a top-level encryption hosting system called "connectors", with the help of this intermediary, allowing funds to flow between ledgers.

3.2 Sidechain/Relays

The sidechain is not specifically referring to a blockchain, but refers to all blockchains that comply with the sidechain protocol and is a concept relative to the main chain of Bitcoin [7]. A sidechain protocol is an agreement that allows bitcoins to be safely transferred from the Bitcoin main chain to other blockchains, and that can be securely transferred back to the Bitcoin main chain from other blockchains [8]. The purpose of the sidechain protocol is to achieve two–way peg so Bitcoin can transit between the main chain and the sidechain. The sidechain protocol means Bitcoin can not only circulate on the Bitcoin blockchain, but also on other blockchains.

The essential feature of the sidechain/relay is to pay attention to the structure and consensus characteristics of the chain. In general, the main chain does not know the existence of the sidechain, but the sidechain must know the existence of the main chain; the double chain does not know the existence of the relay, but the relay must know the existence of the double chain.

3.3 Hash-Locking

Hash locking is a trigger that sets interoperation between different blockchains, usually a hash of the random number to be disclosed. It originated from Bitcoin's Lightning Network [9] and its key technology is the RSMC (Revocable Sequence Maturity Contract) and HTLC (Hashed Time Lock Contract).

Alice and Bob can reach a protocol: The protocol will lock Alice's BTC. Before time T, if Bob can show Alice an appropriate R, make R's hash value equal to the previously agreed value H(R), Bob can get this BTC; if at time T, Bob cannot provide a correct R, then this BTC will automatically thaw and return to Alice.

The use of hash locking can achieve the exchange of cross-chain assets, but can't achieve the transfer of cross-chain assets, but also can't achieve cross-chain contracts, its application scenario is more limited.

3.4 Distributed Private Key Control

The distributed private key control technology is a technology that uses a distributed private key generation and control technology to generate a locked account of the original chain and then maps the corresponding assets to its own blockchain. Wanchain and Fusion use this cross-chain technology. In this trading scheme, the account locking mechanism does not use a two-way peg method. All transaction data is transferred to the original chain node network after being reconstructed and synthesized at the verification node. This completely resolves the specific operations and calculations of the cross-chain transaction. Completed in the new blockchain, no need to modify any mechanism of the original chain, so that no matter existing public blockchains or private blockchains or consortium blockchains can freely access the blockchain, thus reducing cross-chain transactions Cooperative costs, to achieve free mapping of assets between the various chains.

4 Cross-Chain Project

At present, the research on cross-chain technology of blockchain is still in the exploratory stage. There are also some outstanding projects being tested. Below, we will focus on four cross-chain blockchain projects.

4.1 Corda

Corda is a blockchain platform created for the business world [10]. It eliminates the barriers between business transactions by achieving a direct exchange of business. Corda implements a collaborative, open network that gives companies greater ability to collaborate with each other and exchange value directly with one another.

Corda uses transactions to form a ledger, and its distributed ledger is an electronic record stored on all parties involved in a financial or commercial contract [11]. This information is stored in Corda Vault. At the same time, Corda will also store all trading histories, trace the history of a recorded matter and verify it independently.

Transactions in Corda are only spread between participants and notaries. The notary is chosen jointly by the parties to the transaction and is highly credible. The notary is responsible for verifying the validity of the data and verifying the uniqueness of the data. You can safely verify cross-billing messages by simply selecting cross-notices for different ledgers or forcing them to point to the same authenticator and synchronizing their ledgers.

4.2 Polkadot

Polkadot is a heterogeneous multi-chain technology [12]. It consists of many parachains with potentially differing characteristics which can make it easier to achieve anonymity or formal verification. Transactions can be spread out across the chains, allowing many more to be processed in the same period of time. Polkadot ensures that each of these blockchains remains secure and that any dealings between them are faithfully executed. Specialised parachains called bridges can be created to link independent chains.

Polkadot is a protocol that allows independent blockchains to exchange information. Polkadot is an inter-chain blockchain protocol which unlike internet messaging protocols (e.g. TCP/IP) also enforces the order and the validity of the messages between the chains. This interoperability also allows the additional benefit of scalability by creating a general environment for multiple state machines.

4.3 Cosmos

Cosmos is a decentralized network of independent parallel blockchains, each powered by classical BFT consensus algorithms like Tendermint [13]. The first blockchain in the Cosmos Network is the Cosmos Hub, whose native token is the Atom. Cosmos is a permissionless network, meaning that anybody can build a blockchain on it.

The Cosmos Center connects (or calls it space) many other blockchains through a new blockchain communication protocol. The center can track numerous token types and record the total number of tokens in each connected space. Tokens can be safely and quickly transferred from one space to another without the need to reflect exchange liquidity between the two, because the token transmission between all spaces passes through the Cosmos Center.

Cosmos is not just a single distributed ledger, but the Cosmos Center is not a closed garden or a cosmic center. We are designing a protocol for the open network of distributed ledgers. This protocol will become a new foundation for the future financial system based on the principles of encryption, robust economics, consensus theory, transparency, and accountability.

4.4 Wanchain

Wanchain is not merely a universal cross-chain protocol, it is a distributed ledger that records cross-chain and intra-chain transactions [14]. Wanchain connects and exchanges value between different blockchain ledgers in a distributed manner. It uses the latest cryptographic theories to build a non-proprietary cross-chain protocol and a distributed ledger that records both cross-chain and intra-chain transactions. Any blockchain network, whether a public, private or consortium chain, can integrate with Wanchain to establish connections between different ledgers and perform low cost inter-ledger asset transfers. The Wanchain ledger supports not only smart contracts, but also token exchange privacy protection.

When an unregistered asset is transferred from the original chain to Wanchain, Wanchain will create a new asset using a built-in asset template to deploy a new smart contract based on the cross-chain transaction information. When a registered asset is transferred from the original chain to Wanchain, Wanchain will issue the corresponding equivalent tokens in the existing contracts to ensure that the original chain assets can still be traded on Wanchain.

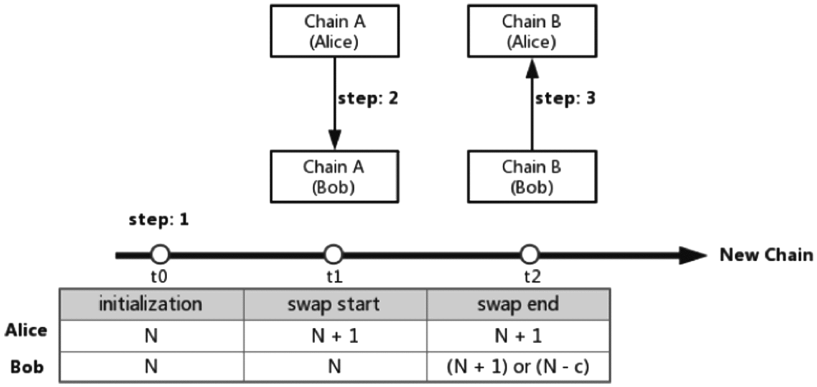
5 The Cross-Chain Solution

In the many problems faced by the blockchain, the network isolation hinders the cooperative operation between different blockchains, and limits the playing space of the blockchain to a great extent. In order to realize the information interaction between different blockchains, we explored a feasible scheme. The program combines side-chain technology and hash-locking technology to establish a new blockchain as a third-party trading platform, thus ensuring the transmission of trust between different blockchains.

The user develops a new blockchain as a trading platform. It can be either a public chain or a private chain for recording transaction credentials. The transaction credentials should appear in pairs, for which we have agreed on a trading interval, which is also the difference in the hash-locking interval. At the same time, the new blockchain can realize the quantification of value by issuing coins.

The specific implementation plan mainly includes three steps:

Step1: Both sides of the information exchange are registered as users on the new blockchain, and the corresponding wallet is opened. At the same time, it is necessary to deposit a sufficient amount of margin in personal accounts, which is a prerequisite for achieving cross-chain value transmission. Margin can be the new blockchain currency or other widely recognized and accepted cryptocurrencies such as BTC and ETH. As shown in Fig. 1, at t0, Alice and Bob each have an asset with a value of N as collateral. If Alice transfers assets to the Bob account on the chain A, there is no need to worry about Bob running away with the assets in the account.



	initialization	swap start	swap end
Alice	N	N + 1	N + 1
Bob	N	N	(N + 1) or (N - c)

Fig. 1. A feasible cross-chain solution.

Step2: In order to encourage cross-chain transactions, all active parties based on the new blockchain will be rewarded. At t1, Alice and Bob make a transaction on block-chain A. The transaction initiator actively submits transaction credentials to the new blockchain. The blockchain records the transaction in real-time and issues a 1 unit bonus to Alice. After the record is complete, Alice's asset in the new blockchain account is N + 1 and Bob's asset is N.

Step3: In the case that the transaction is completed normally, at t2, on blockchain B, Bob will pay Alice's account the same amount of assets c as required by the prior agreement. After the transaction is complete, Bob submits the transaction credentials to the new blockchain, and Bob will also receive a bonus for 1 unit of assets. The cross-chain transaction was successfully implemented. If, after a given time interval, Bob still does not pay Alice the same amount of assets, or if the paid assets are less than the agreed value c. Bob will not be able to submit transaction credentials to the new blockchain normally. When the waiting time exceeds the hash-lock interval, Bob will deduct the same amount of assets c in the new blockchain account, meanwhile, the deducted assets c will pay for Alice as transaction compensation.

With the deepening of blockchain applications, cross-chain collaboration and interworking between future blockchain systems is an inevitable trend. Cross-chain technology is the key to the realization of value networks in blockchain, and the interconnection and interoperability of blockchains will become more and more important issues.

Acknowledgement. This work is partially supported by the technical projects No. 2016YFB1000803, No. 2017YFB0802703, No. 2017YFB1400604, No. 2012FU125Q09, No. 2015B010131008 and No. JSGG20160331101809920.

References

1. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Consulted **1**, 28 (2008)
2. https://en.wikipedia.org/wiki/Blockchain. Accessed 8 May 2018
3. Gao, Z.: Blockchain cross-chain technology introduction. JKGC Mag. **11**, 46–51 (2016)
4. https://en.bitcoin.it/wiki/Atomic_cross-chain_trading. Accessed 10 May 2018
5. Yang, B., Chen, C.: The Principle, Design and Application of Blockchain, pp. 58–60. China Machine Press (2018)
6. https://www.jianshu.com/p/7dd5305d71b6. Accessed 10 May 2018
7. Chang, J., Han, F.: Blockchain from Digital Currency to Credit Society, pp. 84–87. China CITIC Press (2016)
8. Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., Wuille, P.: Enabling blockchain innovations with pegged sidechains. https://blockstream.com/sidechains.pdf
9. Poon, J., Dryja, T.: The bitcoin lightning network: scalable off-chain instant payments. https://lightning.network/lightning-network-paper.pdf
10. http://cncorda.com/. Accessed 10 May 2018
11. Hearn, M.: Corda: a distributed ledger. https://docs.corda.net/_static/corda-technical-whitepaper.pdf
12. Wood, G.: Pounder. Polkadot: Vision for a Heterogeneous Multi-chain Framework. https://block.academy/researches/PolkaDotPaper.pdf
13. Kwon, J., Buchman, E.: Cosmos: a network of distributed ledgers. https://cosmos.network/resources/whitepaper
14. Wanchain: Building Super Financial Markets for the New Digital Economy. https://www.wanchain.org/files/Wanchain-Whitepaper-EN-version.pdf