FIBOS INTER-BLOCKCHAIN COMMUNICATION PROTOCOLS WITH OKCHAIN

WALLET.FO

Abstract. —

Speaking of today's blockchain industry, each blockchain project has a unique ecosystem of users, tokens, protocols, consensus algorithms, technical structures. As a result, each blockchain project of different infrastructures often operates isolated, each chain separates from the others. Lack of interoperability has become a considerable hindrance for blockchain adoption. Without this connectivity, it is deeply troublesome to transfer assets from one chain to another one and it is also impossible for smart contracts deployed on different chains to interact with each other.

Therefore, a variety of inter-blockchain communication(IBC) protocols were designed to solve this problem. This article presents a practical heterogeneous IBC protocol to achieve the interoperability between FIBOS and OKChain by implementing an Cosmos-compatible IBC relay plugin on FIBOS. In consider of the fact that OKChain was implemented under Cosmos architecture, the design principles addressed in this article could also apply to all Cosmos Hubs or "Zones" in Cosmos with subtle modifications.

In a future of ever-increasing blockchain platforms, a few might stand the tests of market and time. For those platforms, interoperability will become an important function for survival in the future ecosystem. The ability to integrate and interact with each other appears to be a crucial necessity for global blockchain adoption.

Keywords. — FIBOS, IBC, OKChain, Cosmos.

Table of Content

1. Introduction

At present, a variety of underlying technical architectures of blockchain have emerged in the blockchain industry, which also have various forms : public chains, private chains, permission chains, alliance chains, etc. However, more and more blockchain architectures may adopt different communication protocols, block structures and transaction forms, cryptographic algorithms, consensus protocols, smart contract engines, which make it hard to exchange transactions between blockchains. Inter-Blockchain Communication(IBC) technology could solve this blockchain dilemma, allowing the transactions generated by different technical architecture to communicate within different chains.

What IBC technology wants to solve is the interconnectivity and commutativity between different blockchain systems, that is, to improve their interoperability. In recent years, with the development of blockchain technology, many IBC technical solutions have emerged. Howerever, these solutions usually achieve the value transfer and information exchange in each blockchain system through a centralized system. The blockchain system is mainly characterized by its decentralization. The centralized solutions not only violates the original intention of blockchain's decentralization, but also risks the system security of the blockchain because of the emergence of a centralized role. The security of the blockchain is based on a complete cryptographic engineering rather than a centralized role which has risks at data fraud, doing evil, and inaction. Therefore, it is urgent to discover a truly decentralized and secure IBC protocol in the field of blockchain industry.

At present, the IBC solutions widely used are mainly listed as below :

— **Witness Mechanism :** By introducing a centralized role, witnesses collect data and verify the validity of cross-chain transactions. This will lead to untrustworthy IBC transactions caused by evil witnesses.

— **Hash Locking :** A Hash Time Locked Contract or HTLC is a class of payments that use hashlocks and timelocks to require that the receiver of a payment either acknowledge receiving the payment prior to a deadline by generating cryptographic proof of payment or forfeit the ability to claim the payment, returning it to the payer.

— **Side-chains/Relay chains :** The side-chain itself is a technology and can also be used to describe the relationship between two chains. From the definition of the side-chain, any public chain can become a side chain of Bitcoin, so the value transferring from one chain to another safely is also a cross-chain behavior. And some side-chain protocols are also implemented through relay chains. Among IBC technologies, the relay technology does not rely on a trusted third party to help it perform transaction verification, and can verify itself after receiving the data from

the source chain. Therefore, compared with other IBC technologies, the relay solution is more flexible and easy to scale.

This article presents a novel implemented decentralized IBC protocols between FIBOS and Ethereum. Meanwhile, it also proposes a scheme in design aims to solve the interoperability between FIBOS and OKChain.

The rest sections of this article are structured as below :

— *Section 2* introduces the background knowledge of basic blockchain projects involved in the IBC protocols design, including FIBOS(*Section 3.1*), OKChain(*Section 3.2*) and Cosmos(*Section 3.3*).
— *Section 3* mainly illustrates the detailed design scheme of FIBOS IBC protocols with OKChain.
— *Section 4* will list the benchmarks and performance after the IBC protocols with OKChain has been fully implemented.
— *Section 5* show some of the use cases with the IBC protocols.
— *Section 6* introduces some other blockchain projects which are also dedicated on IBC solutions.

As a result of ongoing development of Cosmos IBC protocol[**1**], all detailed IBC implementation with OKChain described in this article may change in the final version. Some of the design principals illustrated in this article are still in draft version.

2. Background

2.1. FIBOS

FIBOS[**2**] is a public chain project launched by developers and industry members of blockchain, is also a platform cultivating blockchain applications. FIBOS has the largest community of blockchain developers, which is focus on business applications and cutting-edge technology explorations of blockchain area. FO, which is fundamental circulation token of FIBOS blockchain, is also the gas of the on-chain resource model of FIBOS.

Including heterogeneous decentralized IBC protocol[**3**], DEX decentralized asset exchange protocol[**4**], many original DeFi fundamental facilities have been launched on FIBOS. Many underlying digital currencies issued on Ethereum, such as ETH[**5**], USDT, DAI[**6**], have also been circulated on FIBOS which is benefited from the robust IBC protocols. FIBOS DEX is a basic protocol for decentralized exchange with the characteristics of providing depth and liquidity with combined algorithmic trading and manual limit order, without KYC, supporting any trading pair transactions between various tokens on FIBOS.

2.1.1. *FIBOS IBC Infrastructure*

The fundamental architecture of FIBOS IBC consists of :

— **Prover :** It should be part of sender chain of IBC transactions. The prover need to generate verifiable cryptographic IBC transaction prove.
— **Verifier :** Verifier need to verify the IBC transaction proves generated by provers from other chains. The verification result determines whether the IBC transactions could be executed or not.
— **Messenger :** Messenger is a decentralized, untrusted role of the protocol. It is responsible for passing information between sender chain and receiver chain. The messages which messengers need to deliver are always the IBC transaction proves generated by provers and the destinations are always the verifiers of the receiver chain. Messengers could be fraud, misrepresent the proves, but the IBC protocols need to be strong enough to defend against all this kind of attacks by well-designed cryptographic implementation.

2.1.2. *FIBOS IBC Case with Ethereum*

FIBOS has already implemented the IBC protocols with Ethereum called cross.fo whose detailed information listed on the website http ://cross.fo.

In the design schema of FIBOS IBC protocols with Ethereum, we developed a smart contract on FIBOS to implement the functionality of the prover and verifier. In the prover part, it will generated an unsigned IBC transaction when a user would like to make an IBC transaction. The block producers will sign the transaction using its producing private key and pack the signed transaction as a proof. Then, the proof will be deliver to the verifier on Ethereum.

There is another kind of proof generated by prover. As mentioned above, the consensus algorithm of FIBOS is based on DPoS whose network of blockchain nodes are consists of block producers. The block producers (addr. BPs) are voted by the token holder of the whole network. So, the BPs are always changing and switching. When the BP list of FIBOS is changing, the smart contract will generate a proof contains the changed BP data. The proof will be delivered to verifier of Ethereum to maintain the latest BP list version of FIBOS chain.

At Ethereum side, we also deploy a smart contract as the verifier of the protocol. There is no need to implement a prover on Ethereum by smart contract because the block header, the merkle tree structure of the transaction and the transaction itself are the perfect cryptographic proofs. The verifier is responsible for validate the proofs by verify the signatures in the proof through the maintained keys of BP list stored in smart contract on the Ethereum side.

More details about the FIBOS IBC protocols with Ethereum are shown in Figure.1.

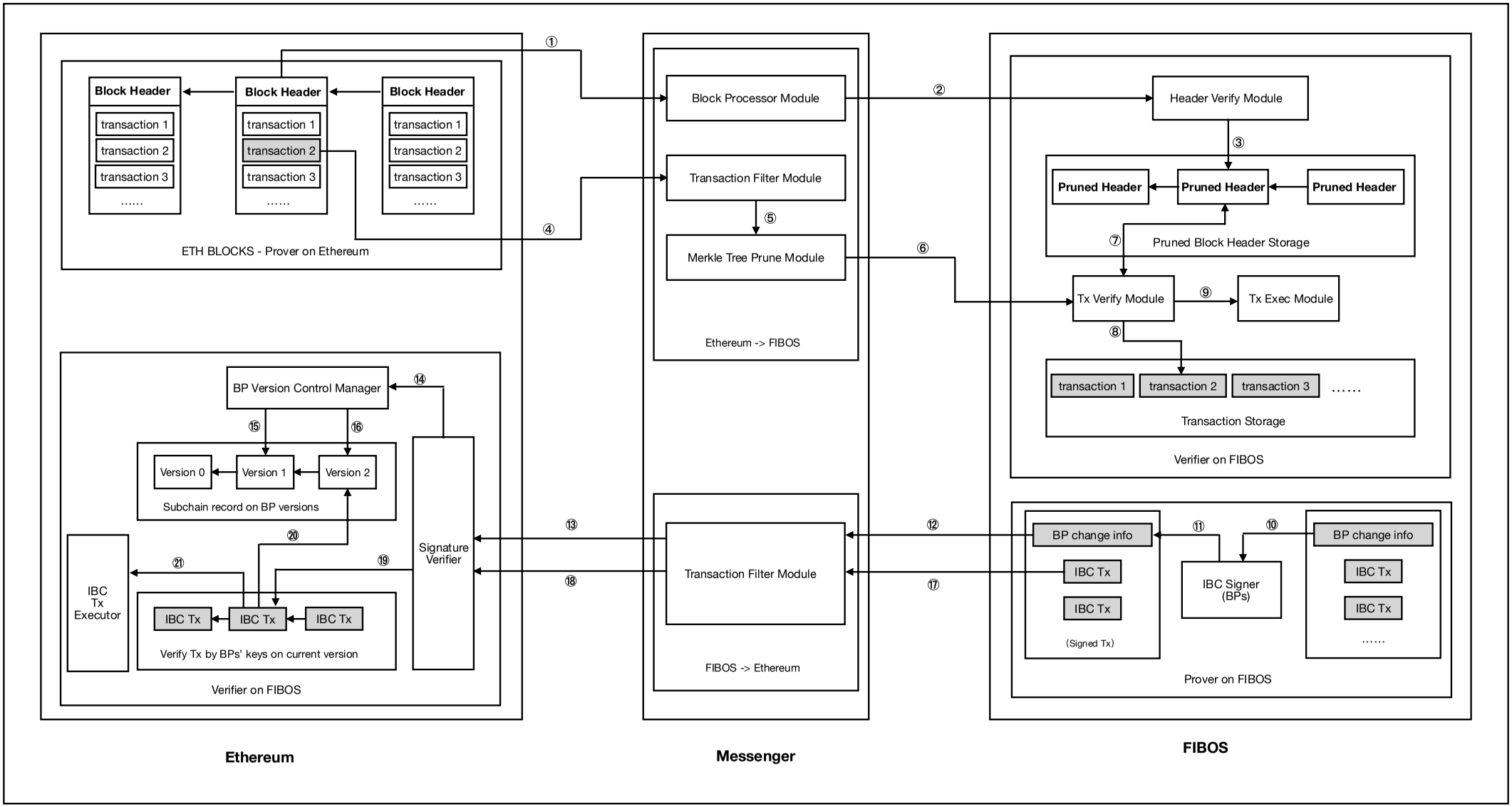

Figure 1.FIBOS x Ethereum IBC Infrastructure

2.2. OKChain

OKChain[**7**] is a set of open-source blockchain projects based on Cosmos developed by OKEx, aiming to promote the landing of large-scale commercial applications based on blockchain technology. It gives each participating node the same rights, allowing users to launch a variety of decentralized applications smoothly, issue their digital assets, create their own digital asset trading pairs, and trade freely. The cross-chain technology is the key to achieving the landing. Through the cross-chain module, the value interconnectivity, user interconnectivity, and scenario application interconnectivity of blockchain can be realized simply and efficiently, so that we can co-construct the ecosystem and the value-added system.

As a vital part of the blockchain industry, OKChain Ecosystem has attracted widespread attention since it has its code open-sourced. FIBOS community also conducted a full-scale investigation and analysis of OKChain. OKChain Ecosystem draws a broad vision of "decentralization", "the rights and governance of community" and "DeFi", which is sync with the belief which FIBOS holds – communalization, frictionless value flow and “discover value everywhere”.

2.3. Cosmos

Strictly speaking, Cosmos is a decentralized network of independent parallel blockchains, each powered by BFT consensus algorithms like Tendermint consensus.

In other words, Cosmos is an ecosystem of blockchains that can scale and interoperate with each other. Before Cosmos, blockchains were siloed and unable to communicate with each other. They were hard to build and could only handle a small amount of transactions per second. Cosmos solves these problems with a new technical vision. In order to understand this vision we need to go back to the fundamentals of blockchain technology.

The vision of Cosmos is to make it easy for developers to build blockchains and break the barriers between blockchains by allowing them to transact with each other. The end goal is to create an Internet of Blockchains, a network of blockchains able to communicate with each other in a decentralized way. With Cosmos, blockchains can maintain sovereignty, process transactions quickly and communicate with other blockchains in the ecosystem, making it optimal for a variety of use cases.

More than anything, Cosmos is not a product but an ecosystem built on a set of modular, adaptable and interchangeable tools. Developers are encouraged to join the effort to improve existing tools and create new ones in order to make the promise of blockchain technology a reality. These tools are the foundation

needed to create the decentralized internet and global financial system of tomorrow.

3. Design of IBC Protocols with OKChain

Implemented based on Cosmos-sdk, OKChain follows the heterogeneous IBC strategy presented by Cosmos which is basically structured as a "federal architecture". This kind of IBC formula is essentially implemented by collecting the voting from relay chain verifiers, which leads to more trust issues. The validation of IBC transactions is strongly depending on the degrees of the verifiers.

Its strategy takes a detour to avoid technical challenge by implementing community governance mechanism instead of cryptographic engineering. This brings the next problem ; the system risk will be increased with the growing IBC asset.

FIBOS believes that current solution is not perfect and safe for the promising OKChain Ecosystem, which will lay hidden dangers for the future development of the public chain ecology.

Problems :

— Current solution causes problems in assets security and system stability.
— Low efficiency and high cost.
— Complex architecture leads to poor risk tolerance.

In order to solve these problems, FIBOS presents a reliable design principal of IBC protocols with precise and simplicity.

Plenty of investigations and verifications prove that it is feasible to use a fusion strategy – for non-predominant public chain (except for Bitcoin, Ethereum, EOS, etc.), OKChain could use federal IBC solution ; for Ethereum or EOS, OKChain could use FIBOS as a trusted relay chain.

The IBC solution currently implemented by FIBOS does not rely on any individual verifier or any group of verifiers. Instead, it ensures IBC security and asset transferring through public chains by cryptographic engineering.

FIBOS's scheme has a simple and straightforward architecture. It is currently the most secure and robust strategy in terms of operation, asset cross-chain cost and cross-chain transaction transmission. The only problem is that it is not a universal protocol and cannot be quickly and cost-effectively compatible with other public chain. But it can be solved by the relay chain solution of Cosmos architecture.

FIBOS have already built a decentralized heterogeneous IBC protocol through FIBOS and Ethereum. After cooperating with OKChain Ecosystem, FIBOS will design heterogeneous decentralized IBC architecture with OKChain and EOS and will become a general IBC parallel relay chain for OKChain, Ethereum, and EOS.

At the same time, the OKChain Ecosystem can also become a block producer of FIBOS chain, just like HelloPool, EosAsia, Starteos, EOS Gravity, Slowmist and other EOS block producer, would be responsible for witnessing OKChain IBC assets and attracting developers of FIBOS and EOS community to OKChain Ecosystem.

3.1. More Specific Design

TBD.

4. Performance

TBD.

5. Use Cases

5.1. Eco-assets IBC Transferring with OKChain

Ethereum is currently the largest market for DeFi application. It will continue to become the most valuable public chain aggregating considerable amount of developers, users, and assets for the foreseeable future. Nevertheless, markets on DPoS chains such as FIBOS or EOS - due to its weak decentralized property - needs "strong" assets from the Ethereum urgently.

Transferring ecological assets including USDK / OKB to FIBOS is simple and efficient by utilizing FIBOS decentralized IBC protocols. USDK / OKB on FIBOS could be used in FIBOS DEX and DeFi applications and could also be made use of community developers and DApps. After the official launch of the OKChain Mainnet, it will provide USDK / OKT with OKChain / Ethereum / EOS / FIBOS multi-chain circulation and enable developers adopt USDK / OKB / OKT as a basic value medium on their own DApps.

5.2. DEX Protocol

FIBOS DEX is a protocolized solution, that is, as a fundamental infrastructure, is fully open and integratable. For users or traders, anyone could complete the initiation of a trading pair of any of two tokens on FIBOS, make a transaction on any trading pairs with no KYC regulations. For developers, integrating display of front-end page with data of the on-chain transactions of DEX is also simple and flexible.

The OpenDEX program of OKChain shares the same idea with the DEX protocol of FIBOS, both of which are aiming at minimizing transaction friction and promoting circulation efficiency.

FIBOS could also provide DEX solutions for OKChain with standardized integration of front-end UI and API, exchange trading algorithms, etc.

Uniswap / Bancor is currently the most mainstream Automated Market Maker (abbr. AMM) algorithm, which can provide users with no-counterparty transactions and excellent performance in depth and liquidity of exchange.

However, the AMM protocol of Uniswap / Bancor has defects in transaction slippage, loss on exchange transactions, K-line display, readability, poor user experience.

For this purpose, FIBOS DEX adopts a fusion solution, combining Uniswap trading algorithm with the traditional order book transactions, so that DEX protocol could serve users and assets with different needs simultaneously. Through order integration, non-specific transaction direction and other solutions, DEX protocol is taking automated market making and user experience into account, which could contribute to a better formula of the OKChain DEX protocol.

6. Related Work

6.1. Polkadot

Polkadot is an inter-blockchain protocol that aims to allow independent blockchains to seamlessly transact and exchange information in a "trust-free" manner via multiple chains. The multiple chains provide a sort of a pooled security for each member of the network, regardless of the blockchain in which they operate.

The Polkadot protocol envisions itself as a complex multi-blockchain technology, with three key components : relay chains, parachains, and bridges.

The coordinated efforts of these three chains aim to allow for the protocol to process several transactions in parallel, making it easy to attain anonymity or formal verification.

Each of these blockchains will seek to ensure that the Polkadot system remains secure, while adding the benefit of scalability through a common ecosystem for multiple blockchains.

6.2. Wanchain

Wanchain is a cross-blockchain platform that seeks to create a "distributed bank" by connecting and exchanging value between different ledgers, to establish a decentralized financial infrastructure.

The protocol provides a framework for financial applications based on digital assets and cryptocurrencies. It's also an independent blockchain network complete with support for its native coin, smart contracts, and dApps.

Wanchain's goal is to provide financial services to all blockchain clients through their financial platform, through which any individual, firm, or institution can set up a business window to provide services. These services could include asset exchanges, credit payments, and transaction settlements.

Wanchain intends to interlink blockchains, with low transaction costs, and provide banking services to the unbanked. They also help others run their ledgers, smart contracts, and wallets through the Wanchain system.

6.3. Komodo

Komodo is an open source platform that offers support for fungible, transparent, and private transactions. In 2018, the platform developed UTXO-based smart contracts, which can be implemented on the Bitcoin blockchain.

Komodo's vision is to create a healthy, multi-blockchain ecosystem that enhances easy access and understanding of the technology. In addition to UTXO-based smart contracts, the platform boasts atomic swaps, scalability solutions, and interoperability solutions.

References

[1] Cosmos Inter-blockchain Communication Protocol (IBC). — *https ://github.com/cosmos/ics/tree/master/ibc*

[2] FIBOS Website. — *https ://fibos.io*

[3] Website on FIBOS IBC with Ethereum. — *https ://cross.fo*

[4] Website on FIBOS Decentralized Exchange protocol. — *https ://dex.fo*

[5] Ethereum. — *https ://ethereum.org/*

[6] DAI - a stablecoin on Ethereum. — *https ://makerdao.com/*

[7] OKChain. — *https ://www.okex.com/okchain*