XferChain: A Platform Empowering Smart Contracts and Decentralized Applications

Version 1.0

www.XferChain.com

Table of contents

Introduction to the XferChain 3	
Solving the market's biggest problem	3
Vision	3
XferChain's Innovative Performance Breakthrough4	ł
Economic Model	1
XferChain Technical Characteristics	4
Consensus	5
Glossary	5
System contracts	5
Staking	6
Punishment	6
Cross-Chain	7
Compliance and KYC/AML	7
The Genesis Block	8
Interact with Us on Social Media	9
Risk Warning	9

The XferChain Platform is a unified infrastructure platform based on technical, traffic and ecological resources, and will be gradually open to the blockchain industry. It will make the construction of decentralized applications more efficient and cost-effective, and provide comprehensive empowerment in aspects of promotion, traffic, and resources. The XferChain Platform is an EVM compatible blockchain that solves the biggest problem of the Dapp industry. The XferChain Platform will provide global developers with a series of diverse innovative facilities and services.

Solving the market's biggest problem

Decentralized applications (Dapps) running on any blockchain contribute to the biggest use case of the blockchain industry. Many such Dapps face cash flow problems. They have many users and lots of transactions in their smart contracts, but they do not gain anything from those transactions. All the transaction fees paid by the users go to miners (or stakers in PoS blockchain). This creates a scenario of "Rich getting richer and poor getting poorer". We solved this painful industry problem through our innovative technology, where smart contract deployers also gain some percentage of the transaction fee paid by the smart contract user. This will create a huge positive cash flow to the Dapp developers and help them run the Dapp project smoothly and they can carry on their innovative development in the blockchain ecosystem.

Vision

XferChain's vision is not only to be the best public blockchain, but also to focus on the discovery and support of high-potential developers and innovative projects. Relying on the world's largest trading ecosystem, XferChain is committed to becoming the birthplace of innovative technologies and innovative businesses, and building a complete ecological loop of technology development, application promotion, and trading.

XferChain's Innovative Performance Breakthrough

- Potential TPS: 200,000+
- Average block interval: 3s

XferChain 200K+ transaction Approach



As we know, even with the highest speed processor, It is not possible to increase speed after a certain limit due to series processing of instructions. Then to break this processor, the manufacturer started a parallel processing mechanism to get more and more instruction processing per second.

The same thing applies with the Go Ethereum blockchain structures which work on a series processing mechanism. Every block and every transaction is recorded / processed in series Which creates its own limit in terms of number of transactions per second.

Any blockchain which is based on the fork of Go Ethereum source code will generally not be able to get higher transaction throughput due to its structural limit.

XferChain has the possibility of parallel processing with the existing Go Ethereum structures by providing an independent processing for client-side processing.

To achieve this we checked the processing load on EVM. In terms of 'storage writing' and 'processing' we found that even less than 10% instructions are being used as storage writing and more than 90% instructions are actually 'processing' instructions like arithmetic operations, decision making etc.

So our research found an approach of an independent processing engine where for the second part (processing part) which is more than 90% processed in EVM, we decided to make a separate processing engine which will run on the client-side on any device to process those instructions. After processing this, the same engine will put a signature on the processed outcome so that it can be verified by any validator node and on behalf of that signed processed request the validator will update storage on the blockchain. This way we can achieve speeds of more than hundred thousand plus transactions per second.

For this our development team is working to make a independent processing engine which will run on client side on client device, this independent EVM will also process instructions for client and will put a specific signature on those processed data so that it can be validated by validator node to check whatever is processed on client side is is perfectly correct and signed or not and if that passes in validator check then on behalf of that processing instruction validator will update storage in blockchain node in next block this way we reduce the 90% load on core blockchain node. This way the transaction capability of blockchain nodes will also increase and due to independent EVM most of the processing requirements are shifted to client side so not only hundreds of thousands but dramatically it will boost transaction speed more and more as the number of client side processing engines increases.

So The development of our independent EVM processing engine is in progress. We are doing lots of tests from different perspectives like accurate processing, signature, verification and security. Once this engine is ready to serve we can easily achieve 100K+ transactions per second easily even with using the Go Ethereum Fork.

Economic Model

The endogenous token on the chain is Dapo; the transactions consume Dapo as a gas fee.

Miners pledge Dapo to become validator nodes. The reward of nodes is the gas fee, which is distributed according to the mortgage proportion.

XferChain Technical Characteristics

- An open and decentralized network to maintain the security of the network and assets.
- Support the programmability of EVM, the compatibility of smart contracts to reduce development or migration costs.
- Meta-transaction function: gas fee reduction, effectively reducing the cost of developers and users on the chain.
- Support cross-chain asset transfer to optimize users' experience.

Consensus

XferChain adopts a DPoS consensus mechanism with low transaction cost, low transaction latency, high transaction concurrency, and supports up to 21 validators.

DPoS is a combination of PoA and Pos. To become a validator, you need to submit a proposal first and wait for other active validators to vote on it. After more than half of them pass, you will be eligible to become a validator. Any address can stake to an address that qualifies to become a validator, and after the validator's staking volume ranks in the top 21, it will become an active validator in the next epoch.

All active verifiers are ordered according to predefined rules and take turns to pack out blocks. If a validator fails to pack out a block in time in its own round, the active validators who have not been involved in the past n/2 (n is the number of active validators) blocks will randomly perform the block-out. At least n/2+1 active validators work properly to ensure the proper operation of the blockchain.

The difficulty value of a block is 2 when the block is generated normally and 1 when the block is not generated in a predefined order. When a fork of the block chain occurs, the block chain selects the corresponding fork according to the cumulative maximum difficulty.

Glossary

- validator. Responsible for packaging out blocks for on-chain transactions.
- active validator. The current set of validators is responsible for packing out blocks, with a maximum of 21.
- epoch. Time interval in blocks, currently 1epoch = 200block on XferChain.
 At the end of each epoch, the blockchain interacts with the system contracts to update active validators.

System contracts

XferChain-System-Contracts

The management of the current validators are all done by the system contracts.

- Proposal: Responsible for managing access to validators and managing validator proposals and votes.
- Validators: Responsible for ranking, management of validators, staking and unstaking operations, distribution of block rewards, etc..
- Punish: Responsible for punishing operations against active validators who are not working properly.

Blockchain call system contracts:

- At the end of each block, the Validators contract is called and the fees for all transactions in the block are distributed to active validators.
- The Punish contract is called to punish the validator when the validator is not working properly.
- At the end of each epoch, the Validators contract is called to update active validators, based on the ranking.

Staking

For any account, any number of coins can be staked to the validator, and the minimum staking amount for each validator is 32Dapo (To be confirmed). If you want to unstake, you need to do the following:

- 1. Send an unstaking transaction for a validator to the Validators contract;
- 2. Waiting for 86400 blocks before sending a transaction to Validators contract to withdraw all staking coins on this validator;

Punishment

Whenever a validator is found not to pack a block as predefined, the Punish contract is automatically called at the end of this block and the validator is counted. When the count reaches 24, all income of the validator is punished. When the count reaches 48, the validator is removed from the list of active validators, and the validator is disqualified.

Cross-Chain

Assets such as ETH and stable coins can be mapped to XferChain by an asset bridge. The realization method is to lock a certain number of tokens on the original chain then generate a corresponding number of tokens on XferChain.

XferChain encourages developers to provide more decentralized cross-chain solutions.

Compliance and KYC/AML

The blockchain platform integrates a robust KYC/AML (Know Your Customer/Anti-Money Laundering) framework to ensure compliance with regulatory standards while maintaining the integrity of user interactions. The system verifies the identity of users through secure, decentralized processes, utilizing blockchain's transparency and immutability to create tamper-proof records. Automated checks against global watchlists, coupled with advanced risk assessment tools, help detect and prevent fraudulent activities.

The KYC is enforced at the Cross-chain bridge level, as that is the entry point for the ecosystem. People only get the mainnet coins from the bridge initially and hence KYC enforcement creates a regulatory compliance ecosystem entry point.

We will be using <u>sumsub.com</u> for the automated KYC verification, which will allow users to quickly verify themselves and have seamless user experience.

The Genesis Block

Both the mainnet and testnet genesis information of XferChain chain have been hardcoded in blockchain, and the corresponding genesis files are listed below for verification.

- chainId The unique identification of the chain.
- homesteadBlockeip150Blockeip150Hasheip155Block

eip158Block byzantiumBlock constantinopleBlock petersburgBlock istanbulBlock muirGlacierBlock Hard fork height configuration.

- congress Consensus parameters period is time interval of blocks. epoch is set for a period in block, and at the end of each epoch, the validators are adjusted accordingly.
- number gasUsed parentHash nonce timestamp extraData gasLimit difficulty are all parameters for genesis block.
- extraData The initial validators is set up here.
- alloc Configured initial account information that can be used for asset pre-allocation and pre-initialization of system contracts.
 - 0xdaf88b74fca1246c6144bc846aaa3441ed095191 //Genesis account for Dapo
- System contract repo: <u>XferChain-System-Contracts</u>

Risk Warning

- All users and developers can participate in the current test environment and subsequent stages of XferChain for free, and there is no charging scenario.
- All users must distinguish the test environment from the Mainnet. The assets generated in the test environment have no value. Be aware of counterfeit currency fraud.
- XferChain announces authorization, promotion and other collaborations only through the official social media platform. Developers and users should check carefully to avoid losses.
- Do not misread the official website (XferChain.org), and be cautious with private key phishing.