XT Smart Chain Technical

Whitepaper

Table of contents

1. Introduction

XT Smart Chain is a decentralized, energy-efficient public chain. It is compatible with smart contracts and supports high-performance transactions. The endogenous token of the XT smart chain is XT, which adopts the HPoS consensus mechanism, which has low transaction costs, Features such as low transaction latency and high transaction concurrency.

The mission of XT Smart Chain is not only a public chain, but also focuses on discovering and supporting high-potential developers and innovative projects. Relying on the world's largest trading ecosystem, XSC is committed to becoming the birthplace of innovative technologies and innovative businesses. To build a complete ecological cycle of technology development, application promotion, and trading.

2. XT Smart Chain Features

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

3. XT Smart Chain Other Features

- [GitHub - xt-smartchain/xsc-chain: XT Smart Chain, a chain based on the go-ethereum fork] Anyone can access all the open-source code and compile and run their own nodes.
- The rules for participation in validation are publicly available in the form of code.
- Anyone can audit the code to verify the system's security.

- Anyone can verify whether the system's rules are being followed by checking local and on-chain data.

4. Concept

4.1 Consensus

- The consensus mechanism of XT Smart Chain is based on the HPoA consensus mechanism.
- HPoS is a proof-of-stake-based consensus mechanism, which is a hybrid of DPoS and PoA.
- PoS can effectively defend against 51% attacks but is not decentralized enough. HPoS involves token holders voting and electing a set of validators, increasing decentralization and benefiting community governance.

XSC adopts HPOS consensus mechanism of low transaction cost, low transaction delay, and high transaction concurrency, and supports up to 21 active validators. The administrator can designate any address to become a common validator, and the 21 validators with the largest number of pledges the node is an active validator, responsible for the packaging of the block producing node. After each epoch, the pledge amount ranks among the top 21 validators, and it will become the active validator for the next epoch.

All active validators are sorted according to predefined rules and packed into blocks in turn. If a validator fails to pack blocks in time in its own round, n/2 (n is active) The number of validators) Active validators who have not participated in the block will randomly perform block generation. At least n/2+1 active validators are working normally to ensure the normal operation of the blockchain.

The difficulty value of the block is 2 when it is generated normally, and 1 when it is not generated in a predetermined order. When the blockchain forks, the blockchain selects the corresponding fork based on the cumulative maximum difficulty.

4.2 Working Mechanism of HPoS

- Blocks are generated by a limited set of validators.

- Validators take turns generating blocks in a PoS manner, similar to Ethereum's Clique consensus engine.
- The set of validators is selected based on stake-based governance on the XT Smart Chain, with a certain probability and randomness.
- Changes to the validator set are relayed through a cross-chain communication mechanism.
- The Parlia consensus engine interacts with a set of system contracts to enable slashing, revenue distribution, and validator set updates.

Based on the fundamental principles of blockchain design, if this consensus mechanism is not followed, non-compliant nodes will be forked out, while compliant nodes can always verify whether the consensus mechanism is being followed. This is the foundation of blockchain security and decentralization.

4.3 Description

- Validator

There is no limit in theory, anyone can become a validator, which can be set by the administrator (validatorV1Admin).

- Active validator

Currently the validator set responsible for packaging blocks, up to 21.

- epoch

The time interval in blocks. The current 1epoch = 200block. At the end of each period, the blockchain interacts with the system contract to update the active validator.

4.4 Punishment

Whenever it is found that the verifier has not packaged a block according to the predefined, the `Punish` contract will be automatically called at the end of the block, and the verifier will be counted. When the count reaches 24, all the verifier's income will be punished. When the count reaches 48, the validator will be removed from the list of active validators and disqualified.

4.5 Reward

XT Smart Chain's mining rewards are only commissions. The distribution rules are as follows:

- **10%** to backups (10% is evenly distributed to ordinary validator nodes)
- **40%** validators share by vote (40% is distributed to active validator nodes in proportion to the pledge weight)
- **50%** validators share (50% is evenly distributed to active validator nodes)

For any account, you can pledge any number of coins to the validator, If you want to cancel the mortgage, you need to do the following:

1. Send unstaking transaction to validator management contract;

2. Wait for 86400 blocks and then send a withdrawal transfer to the validator management contract.

Each validator node can individually set the percentage of the current block reward to be distributed to users. Staking users get rewards based on the percentage. Ordinary validator nodes can also be distributed to staking users.

4.6 Creation Archives

What is a Creation Document

The genesis File is a JSON file that defines the initial state of the blockchain. It can be regarded as the height of the `0` blockchain. The first block located in height, `1`, will refer to the creation World file as its parent file.

The state defined in the genesis file contains all necessary information, such as initial token allocation, creation time, default parameters, etc. Let's break down this information.

Description

- chainId

The unique identifier of the chain. The main net is 520, the test net is 530, and the network id of test-net should be different from main-net.

- period

Block time interval

- epoch

The time interval in blocks, the current lepoch = 200block At the end of each period, the blockchain interacts with the system contract to update the active validator

- nonce

The random number is a cryptographically secure proof of mining workload, which undoubtedly proves that a certain amount of calculation has been spent in determining the value of this token.

- timestamp

Must be at least the parent's timestamp + BLOCK_PERIOD.

- extraData

The initial validator is set here

- gasLimit

A scalar value equal to the current full chain limit of Gas spending for each block. In our case, it is high to avoid being restricted by this threshold during the test. Note: This does not mean that we needn't pay attention to the gas consumption of our contract.

- difficulty

Scalar value corresponding to the difficulty level applied during the discovery of the random number of this block. The testnet recommends using 0x1

- coinbase

The address of the system used to collect block rewards

- alloc

Allows to define a list of pre-installed wallets.

Contract Name	Address
Genesis account	0x58b1E31682C95417be998b27db00731b54b7E5EC
validators contract address	0000000000000000000000000000000000000C000
punish contract address	0000000000000000000000000000000000000C001
proposal contract address	0000000000000000000000000000000000000C002

- number

The height of the block in the chain, where the creation height is block 0

- parentHash

The Keccak 256-bit hash value of the entire parentHash (including its nonce and mixhash). A pointer to the parent block, thereby effectively establishing the blockchain. In the case of the Genesis block, and only in this case, it is 0.

5. Investors

The currency holding and lock-up status of the main investment team and investors:

Holder	Address	Lock Amount
1 round of Airdrop	0x7b600783cE0e5a4253a5Fbd30845C75d1DF1e934	40,000,000
2 round of Airdrop	0x2BC4687Bf2B986Ce9bAC11D9628269e8c1334961	40,000,000
3 round of Airdrop	0xAD0c5dE43D02F3dcC21Bb79d40162B44cF88d22d	40,000,000
4 round of Airdrop	0x01182db4ff68718c94B10b7620F6F03D1e985337	40,000,000
5 round of Airdrop	0xf500191F55Ae33B4b696b2D607c55728823214D3	40,000,000
6 round of Airdrop	0x19f6125150A2A12FB3e1f2871bb59974f76cf204	40,000,000
7 round of Airdrop	0x565dfa07F1A11eBFe103745630b1511542514d88	40,000,000
8 round of Airdrop	0xe44888a2847C5675E1597c9c0ac5DEf4661A002A	40,000,000
9 round of Airdrop	0x5861FB5459b7Eb076462f56f0A6a435f1FCE6B74	40,000,000
Development Team	0xE7c1056D187d863F06164621B29cfD2afDC9ED3b	140,000,000
1 round of investors	0x6FBC5C93E96eee97463CADd41D8Be377ebFF6c3a	30,000,000
2 round of investors	0x35B6df0d9a39dc5E8D212B74bb7fFfc14256ef3A	30,000,000
3 round of investors	0x5Af395cc3DB5185BF2F3e06D1260550A265edd54	40,000,000

Foundation	0xD472f62184Cd293C76653a13a158eF9Cdd911011	140,000,000
Ecological Fund	0x8e5548BFFBA7b1A1F48B1289f0329Ad384efb8fb	260,000,000

Lock-up mechanism:

1. **Airdrop:** 50% will be unlocked during airdrop, and the remaining will be released in 6 months
2. **Development Team:** Unlocked after 18 months, released in 42 months
3. **Investors:** Unlocked after 12 months, released in 36 months
4. **Ecological Fund:** 20% will be unlocked with the airdrop event,and the rest will be released over 48 months
5. **Foundation:** Unlocked after 18 months, released in 42 months

6. Roadmap

- 2021/11

XSC Mainnet is online, More information at here: https://www.xsc.pub

- 2022/01

XSC scan v1.0.0 is online, more information at here: https://xscscan.pub

- 2022/02

XSC NFT market opensky is online, more information at here: https://opensky.xsc.pub/home

- 2022/03

XSC takerdao(it's a stable currency system) is online, more information at here: https://takerdao.xsc.pub/

- 2022/04

XSC XSwap system is online(It's forked from Uniswap V2), more information at here: https://swap.xsc.pub/exchange

- 2022/05

XT wallet app v1.0.0 is online(it support XSC chain), more information at here: https://www.xsc.pub/download?lang=en

- 2022/06

XSC bridge v1.0.0 is online(it support XSC and ETH chain), more information at here: https://bridge.xsc.pub/

- 2022/07

XSC sky ticket is online, more information at here: https://www.skyticket.pub/

- 2023/02

XSC scan v1.2.0 is online, more information at here: https://xscscan.pub and new features:

- support verify solidity contract

- 2023/10

XT wallet app v1.2.0 is online, more information at here: https://www.xsc.pub/download?lang=en and new features:

- support ETH chain

- support Polygon chain

- 2024/03

Plan to upgrade XSC bridge(https://bridge.xsc.pub/) to v1.2.0, and support following features:

- support Polygon chain

- support BSC chain

- 2024/06

Plan to upgrade XSwap to V3 version(it's same with Uniswap V3), more information at here: https://swap.xsc.pub/exchange

- 2024/11

Plan to upgrade XT wallet(https://www.xsc.pub/download?lang=en) to 2.0.0 version, and support following features:

- support XSwap feature within DAPP

- support XSC bridge feature within DAPP

- 2025

Plan to upgrade XSC mainnet and takerdao system, develop some new production base one XT smart chain.