CoinEx Smart Chain

White Paper

CoinEx Smart Chain

Contents

Motivation

Since Vitalik Buterin first proposed Ethereum in 2013, smart contracts have entered the spotlight. In the eight years since the birth of Ethereum, smart contracts started from scratch, got developed, and later prospered, drawing a lot of attention. Ethereum is the most successful and widely used smart contract platform in current society.

In the rapid succession of various DApps, especially DeFi applications, Ethereum’s drawbacks become obvious than ever before such as low throughput, a small number of transactions and high transaction fees.

In general, it is “high cost with low efficiency”. Many platforms developed proposals to ensure high throughput and accelerate transactions in response, but compromise decentralization more or less.

Committed to building an infrastructure for blockchain and the principle of decentralization and permissionless block generation, CoinEx launches CoinEx Smart Chain (or CSC). Serving as a support for high-performance transactions, CSC is completely compatible with EVM, and applies the PoS model so that all users can become a node by staking tokens without any permission.

CSC Contract

CoinEx Smart Chain (CSC) , it is a decentralized and high-efficiency public chain with high efficiency, created by the CoinEx public chain team for decentralized

finance. It can provide developers with an efficient and low-cost on-chain environment to run decentralized smart contract applications (DApps) and store digital assets. CSC has the following features:

(1) Perfect compatibility with the Ethereum ecosystem. Developers can easily migrate Dapp to CSC, which is based on the Ethereum Virtual Machine (EVM), using mature development tools, and users can also quickly access the CSC network;

(2) Extremely high efficiency and low transaction fees. With the POS consensus protocol, CSC generates a block in seconds, supports extremely high TPS, and keeps transaction fees at a low level in the meantime;

(3) No permission required for block proposers. CSC supports up to 101 block proposers, which are sorted and determined according to the number of CET stakes. It does not require the review of centralized institutions, making the network more decentralized;

Design Principles

The design of CSC follows the following principles:

1. Compatibility with the Ethereum ecosystem:
Ethereum is the first practical and widely used smart contract platform. With the regard to smart contracts, the first thing that comes to mind is Ethereum. Ethereum already has relatively mature applications, communities and toolchains, which constitute a complete ecosystem. CSC's compatibility with Ethereum means that

almost all DApps, ecosystem components and tools on Ethereum can be migrated to CSC directly or with only minor changes.

2. PoS-based consensus:
The consensus based on the Proof of Stake (PoS) is more environmentally friendly, and outruns PoW-based consensus in the respect of performance (with less block generation time and higher transaction capacity). PoS-based consensus can be flexibly managed by the community, without compromising decentralization.

Consensus and Validators

Based on the above design principles, the consensus protocol of CSC aims to achieve the following objectives:

1. Compared with Ethereum, the block generation time by about around 3 seconds.
2. To be compatible with the Ethereum ecosystem as much as possible
3. Staking-based on-chain governance mechanism
4. Up to 101 block proposers without permission

Proof of Stake

Although Proof of Work (PoW) has proven to be a practical solution for decentralized networks, it is not environmentally friendly and requires a large number of participants to maintain network security.

Ethereum and some other networks use Proof of Authority (PoA) or its variants in

different scenarios, including testnets and mainnets. PoA defends against 51% ofattacks, and more effectively prevents Byzantine nodes from arbitrary behaviors. However, the PoA protocol has been criticized for not being as decentralized as PoW because its validators have great power, which could lead to corruption and security attacks. Other blockchains, such as EOS and Cosmos, have introduced different types of Delegated Proof of Stake (DPoS) that allow token holders to vote for validators, which makes the network more decentralized and is conducive to community management.

Integrating the features of PoS and PoA, CSC adopts PoS as the underlying consensus mechanism with the block generation mechanism of PoA. The adopted scheme as below:

1. Blocks are generated by a limited number of validators
2. Validators generate blocks in PoA in turn. In other words, they share the same probability of generating blocks, which is similar to the Clique consensus engine of Ethereum
3. The set of validators is selected and eliminated by on-chain governance based on staked tokens without any permission
4. Anyone can delegate tokens to the node he or she trusts

Validators

In the genesis block stage of the network, some trusted nodes will operate as the initial set of validators. For the management of privileges and stakes, a validator management system contract will be deployed after the network is launched.

After the block is generated, anyone can participate in the election of validators by

calling the system contract to stake CET. The top 101 nodes that by the number of staked tokens, will constitute the next set of validators. Such election and elimination go every 200 blocks. Given the block generation time of 3 seconds, the set of validators will be updated every 10 minutes.

Security

Under the block generation mechanism of PoA, more than half of the N/2+1 validators in the network are reliable and trustworthy, and in most cases the network can run safely and normally.

The availability of CSC relies on each node in the set of validators in the PoS consensus that they can generate blocks in time. However, a validator may fail to generate blocks due to some reasons, such as hardware, software, configuration, or network issues. Those unstable operations will jeopardize the performance of the network and bring more uncertainty to the system.

In order to ensure the stability of the network, CSC introduces the penalty mechanism and internally maintains a penalty contract to record the blocks missed by each validator. Once the number goes beyond the predefined threshold, the validator will have part of its staked tokens confiscated.

Yields

Yields of validators generally come from two aspects: mining rewards and the transaction fees in each block. The yields are distributed according to the percentage of tokens staked by validators in the total stake.

Since the validators generate blocks in turn with the same probability (in the case

that they are always online), their yields are determined by the proportion of their CET staked.

Token Economics

Native Token

CoinEx Token (CET), as a value-added service and privilege scheme based on CoinEx ecosystem, is the native token of CoinEx Smart Chain. Born in January 2018, CET used to base on the Ethereum ERC20 protocol, and will be migrated to CSC after the mainnet is live.

CET on CSC runs the same way as ETH runs on Ethereum, and its main functions are:

1. As block reward for validators
2. To pay for the gas for transfers and contract calls on CSC
3. To pay for the transaction fees for deploying smart contracts on CSC
4. To be delegated to the selected validators

Other Tokens

Since CSC is compatible with the Ethereum ecosystem, the ERC20 contract supported on CSC is called "CRC20" contract. CRC20 "enhances" existing protocols by introducing more settings, which can disclose more information, such as token units and precision.

Prospect

It’ s hard to forecast the future of CoinEx Smart Chain for the moment because it is constantly evolving. CSC is just a small part of the development prospect. In fact, CoinEx is committed to product development and service improvement, and contributes its share to the infrastructure of the blockchain world.

While ensuring the compatibility between Ethereum and its future upgraded versions, CSC will constantly improve the throughput of the blockchain, make the blockchain client easier to use, enhance the security of the custody services, and provide more versatile token cross-chain services. Meanwhile, enriching decentralized applications will be one of the developing directions of CoinEx in the future.