Saito: Mainnet Structure and Launch Strategy

David Lancashire

September 15, 2019
v. 1.0.0

Abstract

Saito is a blockchain designed to process terabytes of data every day. It differs from other networks in not requiring volunteers to serve, and in its design that guarantees that attackers will always lose money attacking the blockchain. For implications and usability, please see the project website (https://saito.tech). This document explains actual network structure.

This document is divided into three parts. The first discusses the Saito pruning mechanism that permits the network to process terabytes of data each day without collapsing. The second explains how the consensus mechanism works. The third explains the technical choices for the network at MAINNET launch, and discuss launch strategy.

1. THE DATA PRUNING MECHANISM

All Saito-class blockchains are divided into "genesis periods" of a length specified in the consensus rules. If the "genesis period" is 100,000 blocks and the latest block is number 500,000, the current genesis period stretches from block 400,001 to block 500,000.

Once a block is no longer in the current genesis period, its unspent transaction outputs (UTXO) are no longer spendable and must be considered for reinclusion in the very next block. Only UTXO that contain enough tokens to pay the rebroadcasting fee (double the average network fee over the last genesis period) are eligible for rebroadcast.

These UTXO are formatted in special "automatic transaction rebroadcasting" (ATR) transactions produced by the block producer. All ATR transactions must include all data contained in the original transaction. And the rebroadcasting fee is deducted from the transaction. All of these criteria are enforced by the consensus rules of the blockchain - any blocks that do not follow these rules are considered invalid according to consensus criteria.

Spent transaction outputs and unspent transaction outputs that cannot pay the ATR fee are permitted to fall off the chain. Any "dust" in those outputs are collected into the "treasury" of the blockchain, the value of which is maintained under consensus rules, from which they are redistributed to the network as part of the block reward.

This system requires block producers to maintain data for the last two genesis periods. After that point it is safe to delete everything except the 32-byte header-hash (i.e. the block-data hash that is combined with the previous block hash to generate the block hash) which needed to demonstrate the connection between.

2. THE CONSENSUS MECHANISM

Saito adds cryptographic signatures to the network layer. This gives each transaction an unforgeable record of the path it has taken into the network from its originator to the block producer.

The consensus rules of the blockchain set a "difficulty" for block production. This difficulty is a "cost" that can only be paid by collecting the "routing work" embedded in these routing paths. The amount of "work" in any transaction is the value of the transaction free halved repeatedly with each additional hop taken into the network.

Transactions that do not contain a cryptographically verifiable routing-path to a node do not provide any "routing work" that can be used to pay the "difficulty cost" of block production.

If the amount of "routing work" included in a block is greater than the "difficulty" required to produce that block, the block producer may take the difference in immediate payment for the work of block production. The rest of the block reward (transaction fees from the block plus any tokens recycled from the transient chain) is then distributed to the network via the payment lottery.

2. THE PAYMENT LOTTERY

Once a block is broadcast to the network, a provably-fair lottery divides the money, with each routing node having a chance of winning proportional the amount of routing work that it has done, relative to its peers in the network.[1]

The lottery works as a proof-of-work challenge. Each block contains an implicit computational puzzle in the form of its block hash. If a miner finds a solution to this puzzle, it broadcasts this solution to the network as part of a normal Saito transaction. We call this solution the "golden ticket".

If this "golden ticket" is included in the very next block, the block reward is divided between the miner that found the golden ticket and a random routing node. If a golden ticket is not found, the block reward is allowed to fall off the chain where it is eventually captured by the .

The system is impossible to cheat. Block producers cannot predict the outcome of the mining lottery, and thus cannot game the block to control the routing subsidy. Miners cannot

The difficulty of the mining puzzle is automatically adjusted to keep the

[1] If a transaction paying a 10 SAITO fee passes through two relay nodes before its inclusion in a block, the first relay node is deemed to have done 10 / 17.5 percent (57%), the second node is deemed to have done 5 / 17.5 percent (29%), and the block producer is deemed to have done 2.5 / 17.5 percent (14%) of the routing work. The chance each node has of winning the lottery is normalized by the percentage that the transaction fee has relative to the total fees in the block.

3. HOW THIS SOLVES THE 51% ATTACK

All non-Saito POW and POS blockchains suffer from 51

4. MODIFYING THE LOTTERY TO IMPROVE SECURITY

3. IMPROVEMENT SECURITY BEYOND 100%

As an aside, it can be seen that this system is fully sybil-resistant. Sybils broadcast Elementary mathematics illustrate that this system is fully sybil resistant. Routing paths with sybils are less profitable for all participants. Knowledge of network paths also

3. MAINNET TECHNICAL CRITERIA

Saito is launching with a "genesis period" of 30 days, and a blocksize cap of 1 BB.

The slope of the "difficulty curve" for block production will be set at - - -