Attacks

Saito is secure against classes of attack which have no defense mechanisms in other chains. This document explains how these defense mechanisms work, since they can be non-obvious to those new to way Saito works.

1. SYBIL ATTACKS

Saito is secure against sybil attacks.

It is possible to identify sybils in Saito by examining the transaction-embedded routing paths. This ability to recognize sybils (who occupy intermediate positions in the routing network and consume more in value than they contribute to their peers) and makes Saito distinct from other blockchains, which lack the information to identify which nodes in their routing network are providing real value.

As every hop in a routing path lowers the profitability of every single node on that path, there is a strong incentive for all nodes to purge sybils from their routing paths. This is particularly the case for nodes on the inside of a sybil which experience an immediate fifty-percent drop in profitability. Nodes which fail to monitor local routing conditions and get sybilled will be less profitable than their peers, unable to compete effectively, and forced off the network through organic economic competition.

Nodes may easily route around sybils by connecting to their remote peers, using the blockchain to communicate with distant peers as necessary.

2. TRANSACTION HOARDING

All blockchains which give 100 percent of the block reward to the nodes that produce blocks are vulnerable to transaction-hoarding attacks.

In these attacks, block producers who pay to collect transactions refuse to share those transactions with their peers lest those peers "free-ride" on their work and gain market share at their expanse. This problem emerges slowly as blockchains scale and the block reward falls. Hoarding is an issue for many reasons, not least that users looking for fast confirmations will direct their transactions to the largest and more profitable block producers, unleashing self-fullfiling centralization pressures.

Saito is secure against transaction hoarding attacks. It achieves this by paying the nodes which collect transactions from users the largest share of the routing payment. Access nodes are incentivized to form at user-facing portions of the network - ensuring there will always be nodes willing to offer routing services offering competitive and efficient routing into the network.

Once transactions are in the network, the profitability of routing nodes depends on their forwarding received transactions as quickly and efficiently as possible. Any nodes which hoard transactions risk losing the value of their work completely. But those who do forward will earn revenue from routing work even if they are not able to produce a block. Simultaneously, the transaction-embedded routing paths allows users and nodes to monitor the behavior of their peers and negotiate reasonable terms of service given local economic conditions.

3. BLOCK-FLOODING ATTACKS

Proof-of-Work networks require block producers to burn money to produce viable blocks. All peers are expected to forward all blocks by default, under the understanding that the costs needed to create a block prevent block-flooding (DOS) attacks on the network.

Saito imposes the same block-flooding protections by stipulating that peers only forward blocks once they have been convinced those blocks form part of the longest-chain. While nodes may thus forward the first block they receive from attackers, they will not forward subsequent blocks at the same block depth. The fact that every additional block produced imposes a cost on attackers ensures that this approach provides the same guarantee: attackers cannot flood the network with data without paying the cost of block production.

It should be noted that the cost of producing the longest chain is higher in Saito than Bitcoin, providing double the effective security against DOS attacks. Additionally, the economic structure of the routing network incentivizes nodes to monitor their peers and maintain efficient network connections. While nodes on the edge of the network may offer attackers an access point for data-flooding attacks, high-throughput nodes towards the center have strong economic incentives to penalizes peers which impose undue costs on them. Malicious nodes must necessarily start their attacks from positions on the edge of the network, where their attacks can be easily overcome by the honest network and face higher costs for success.

4. GRINDING ATTACKS

Proof-of-Stake networks without an explicit cost to block production are susceptible to grinding attacks. These occur when it is possible for nodes to create a large number of variant blocks in order to find one that benefits them.

This is not possible in Saito as block producers have no control over the block reward. Nodes which delay producing blocks for any reason also risk losing the entire value of their routing work, lowering their profitability and alienating the routing nodes with whom they are cooperating in sourcing transaction flow. Miners who find a golden ticket and fail to submit it promptly will not find another in time to collect any payment.

5. 51% ATTACKS

Saito is the only blockchain that is fully secure against 51 percent attacks. To understand how Saito accomplishes this, note that attackers who wish to attack the blockchain must necessary produce the same amount of routing work as the honest nodes as a prerequisite for issuing the longest-chain. Once that is done they must then match the amount of honest mining in the network in order to produce the golden tickets which allow them to get their money back from these blocks.

Security reaches the 100 percent level as attackers who do not include the "routing work" of honest nodes in their attack blocks face a non-stop increase in attack costs. Not only are they forced to match ALL CUMULATIVE OUTSTANDING ROUTING WORK when producing blocks (requiring a limitless increase in tokens) but the increased pace of block production traps miners in a situation where their mining costs must also rise as less time is available between blocks to find valid solutions.

The only way attackers can escape this trap is by "defusing" the accumulation of "routing work" outside their fork by including other people's transactions in their blocks. But in this case attackers must necessarily double their mining costs as it now takes two golden tickets on average to find a solution that will pay them (rather than an honest routing node) the block revenue. The security of the network is guaranteed by 100 percent of fee volume rather than merely 51 percent.

6. THE DEATH OF MOORE'S LAW

Blockchains secured by proof-of-work collapse once the supply curve of hashpower becomes reasonably elastic. This is why the death of Moore's Law is an existential threat all proof-of-work chains: commodity hardware production makes the slope of the supply curve for hashpower fully elastic. This problem is also why the shrinking block reward is a major issue for Bitcoin, as reduced miner revenue slows the pace of improvements in mining technology and makes 51 percent attacks feasible as well as profitable.

Saito remains secure beyond the death of Moore's Law. The reason for this is that the golden ticket system ensures that collecting 100 percent of the routing reward always costs 100 percet of network fees. The addition of proof-of-stake component adds a deadweight loss *on top of this* that imposes costs on attackers that are proportional to the percentage of the stake that is not controlled by the attacker multiplied by the proportion of total network revenue that is allocated to the staking pool.

As a result, the only situation in which attackers can theoretically avoid losing money attacking the network is if they control 100 percent of network hashpower, control 100 percent of the outstanding network stake, and are able to match 100 percent of the network stake. But even in this situation, the rational response for users facing an attack (an increase in the pace of block production) is to expand their own stake in the network. Economic forces move the network back to security even from extremes of centralized control. This is different from existing proof-of-stake implementations, in which stakers have an incentive to liquidate their stake when the network comes under attack.

7. I-HAVE-ALL-THIS-MONEY-WHY-DEAR-GOD-WILL-NO-ONE-SELL-ME-A-PEPSI ATTACKS

Occasionally people new to Saito think their way into circular critiques where there is some hypothetical attack on a Saito node that consists of an attacker maneuvering itself into being someone's only point of access to the network and leveraging that to censor transaction flows, extract supra-market rents or produce a dummy blockchain at a much slower rate than the chain produced by the honest network. We call these I-HAVE-ALL-THIS-MONEY-WHY-DEAR-GOD-WILL-NO-ONE-SELL-ME-A-PEPSI attacks.

All consensus systems fail in situations where one's view of the longest chain (i.e. consensus) is dictated by an attacker. Saito is no different than other blockchains in this regard. For those concerned about these issues, the important thing to note is that only Saito provides explicit economic incentives that prevent these issues. While proof-of-work and proof-of-stake variant networks typically suffer from an underprovision of unpaid access nodes, in Saito access to the network is easy: any scarcity in access points is an immediate and profitable commercial opportunity.

8. OTHER ATTACKS

Concerned about other attacks? Contact us at info@saito.tech and we will expand this document to clarify any outstanding issues.