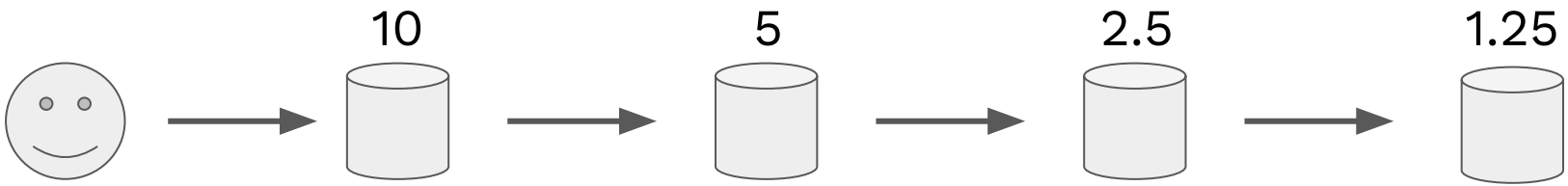
Saito

Routing Work

1. Produce Blocks

Nodes can produce blocks once their mempool has enough “routing work”.

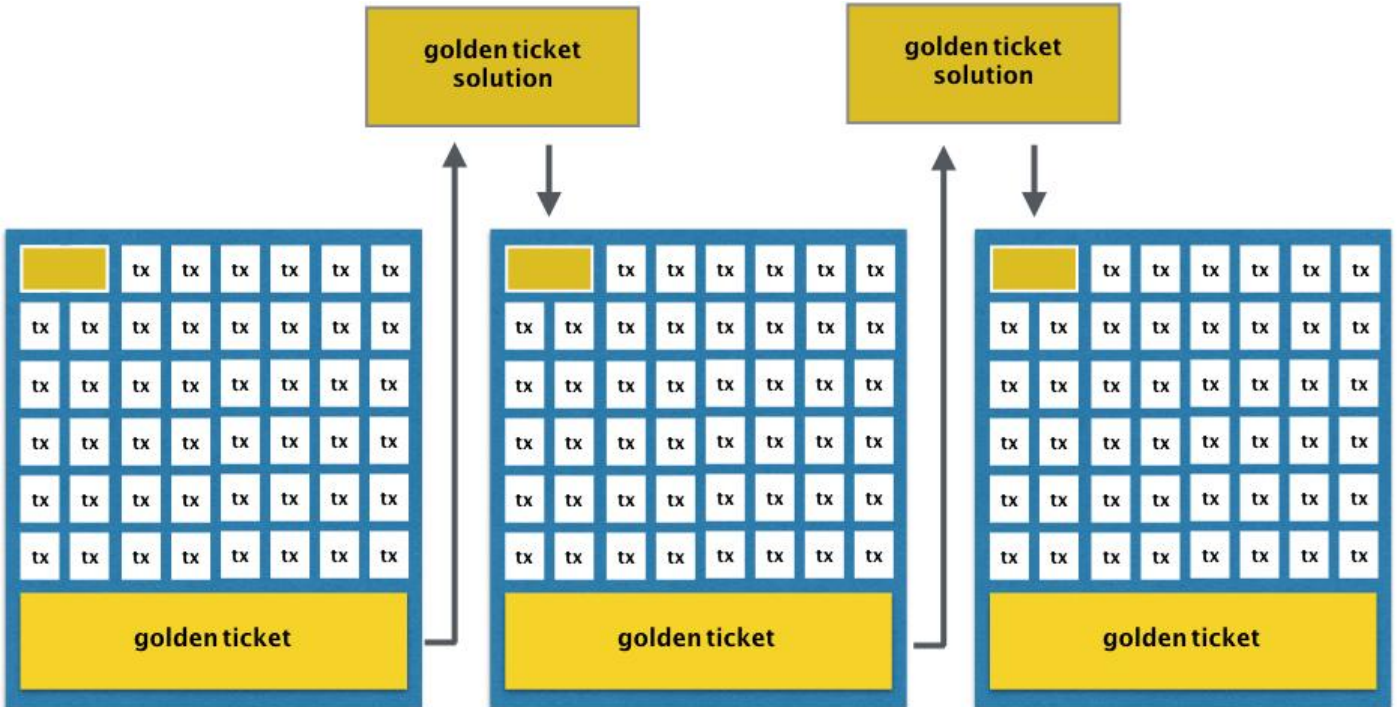
The work each transaction provides drops as it hops into the network.



A 10 SAITO transaction routed 4 hops generating 18.75 units of work.

The last node only gets 1.25 SAITO in routing work.

2. Hold a Lottery

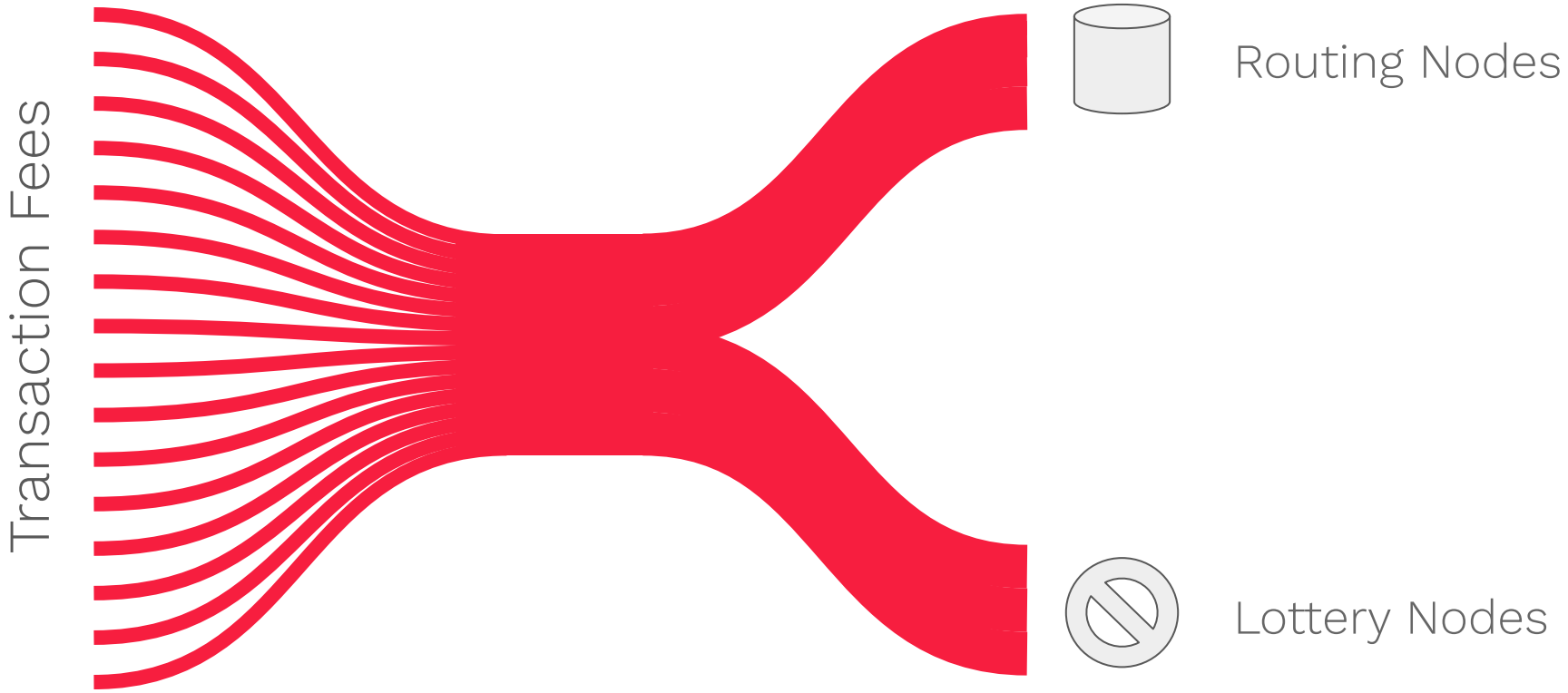


Each block contains a hashing puzzle. Saito calls this the golden ticket.

If a solution is found and included in the very next block, a random number in the solution is used to pick which nodes in the network get paid.

If no solution is found or included, no-one is paid.

3. Split Fees



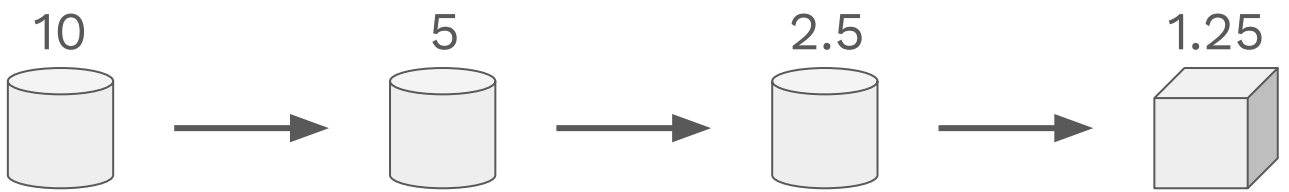
Miners Earn

$$\frac{\text{their hashpower}}{\text{sum of all hashpower in network}}$$

Routing Nodes Earn

$$\frac{\text{their routing work in block}}{\text{sum of all routing work in block}}$$

Saito Pays for Network Infrastructure!



EXPECTED INCOME	10 / 18.75	5 / 18.75	2.5 / 18.75	1.25 / 18.75

* nodes get paid for servicing users and collecting transactions:
  1-CPU-1-VOTE but for network operations.

Saito fully eliminates:

Economic Attacks

while preserving the cost-of-attack and anti-spam properties of classic POW

Example: 51% Attacks

Producing a viable fork requires attackers to:

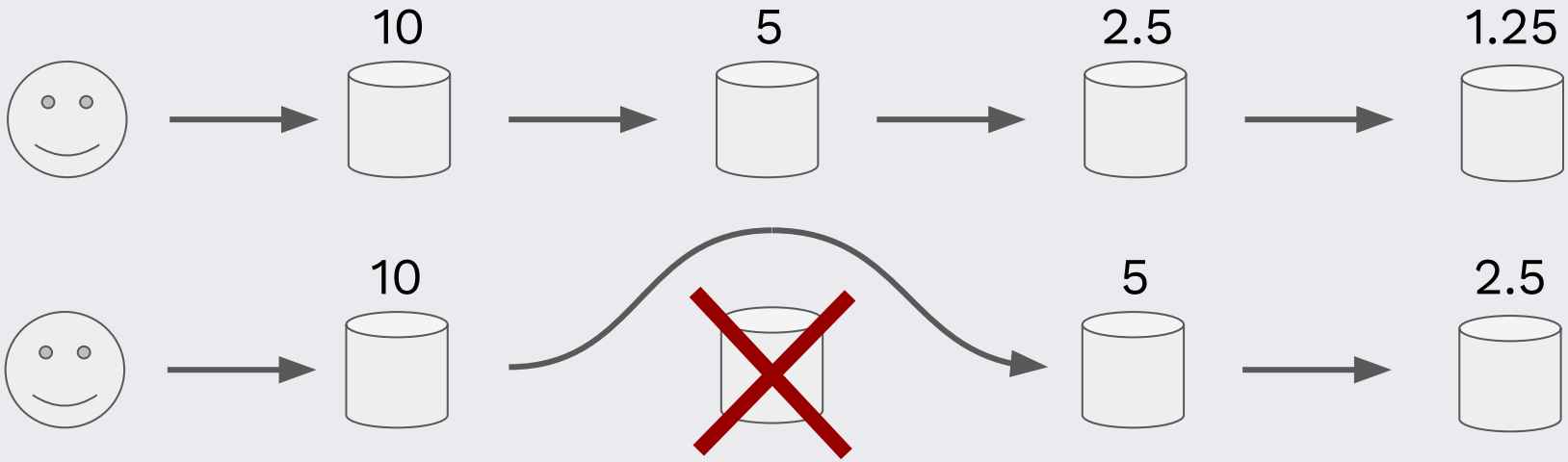
- Match 100% of honest routing work (by spending their own UTXO) to produce blocks faster than the main chain.

- More than double the mining done by the honest network to prevent the fees they are hemorrhaging from flowing into the hands of honest nodes.

There is no situation in which attackers can make money attacking the chain. Economic attacks in external markets and majoritarian attacks are fully eliminated. Cost-of-attack is a conservative 2x that in all POW and POS mechanisms.

Example: Sybil Attacks

Sybils are unnecessary hops in routing paths.
In Saito sybils lower the profitability of every other node.



Nodes that get sybilled go bankrupt.

Example: Spam Attacks

Producing blocks without the support of the honest nodes and users in the network is extremely expensive. Additional steps also protect the network from attackers willing to burn money.

- Cryptographic signatures added to block routing allow nodes to identify when multiple blocks are produced by the same node at the same block depth. Subsequent blocks are not routed.
- The golden ticket system can require valid chains to have a certain number of hash-solutions. This prevents attackers from burning money to create a fake chain without support from a reasonable percent of network hashpower.

And so much more....

POW and POS swap out the criteria they use to produce blocks. They remain trapped in a world of “technical tradeoffs” caused by their economic design.

Saito elegantly solves the underlying economic problems.

https://saito.io

Learn more about how Saito works as well as the technical details behind the network implementation and the applications that it enables on our website.

Saito

info@saito.tech

https://saito.io