Saito

Bitcoin in Disguise

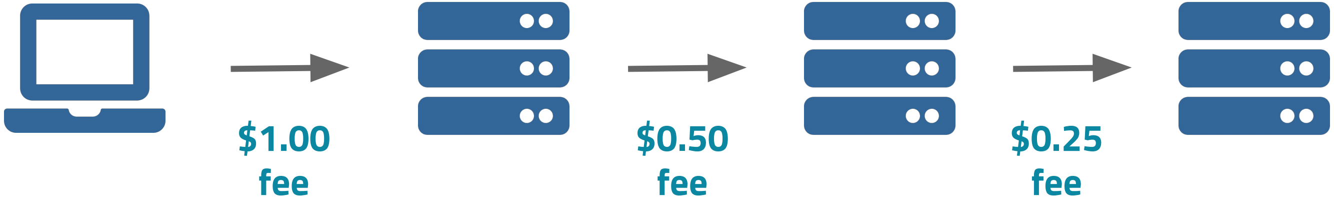
Part I: Saito is Bitcoin

We make it expensive to produce blocks …

How it Works

Full-nodes collect transactions.

Once they have enough usable fees, they can produce a block....



Quick aside: notice how our "usable fees" halve with each hop across the network? This makes Saito impervious to sibylling and ensures that transactions are only valuable to honest nodes that participate in active routing.

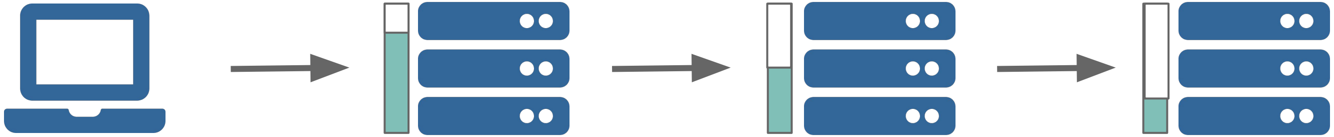
Blocks Cost Money

Nodes pay for blocks by proving they routed enough transactions.

For complicated reasons, no-one can steal transactions.

So honest nodes route data and produce blocks for free.

Attackers need to spend their own money to attack the network.



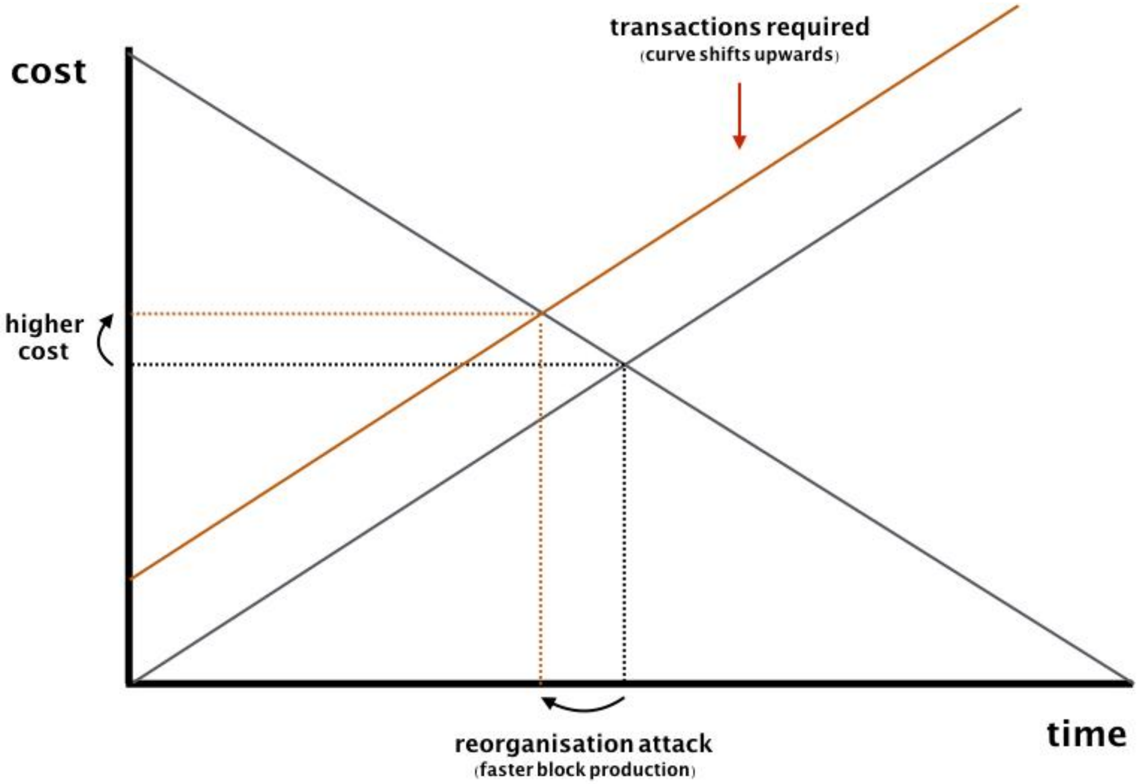
Saito/Bitcoin is Hard to Rewrite

number of confirmations x cost per block = cost to attack

10 x 100k USD = 1 million USD

Just like Bitcoin! If you need more security, wait for more confirmations!

Security Guaranteed by Economics



Our technical presentation has graphs like this.

It takes about 40 minutes to learn exactly how our system works.

And it is worth it. In the future POT will be an important consensus mechanism.

Only one problem with this method...

We have to tweak the Bitcoin Coinbase

We can't give **all** the money to the node that makes the block

... or they can recycle their fees into the next block.

This is the only new vulnerability with Saito.*

We call it the "fee-recycling attack".

** ok, we lied. The bitcoin version of this attack occurs when miners collude to gain advantage over non-colluding peers and pour the profits into buying more hashpower (i.e. the FIBRE network). There are sophisticated trade-offs involved in how Bitcoin and Saito address these attack vectors and how crippling these attacks are when they happen.*

Part II: Tweaking Coinbase

We pay for routing, not mining...

Saito moves the Coinbase:

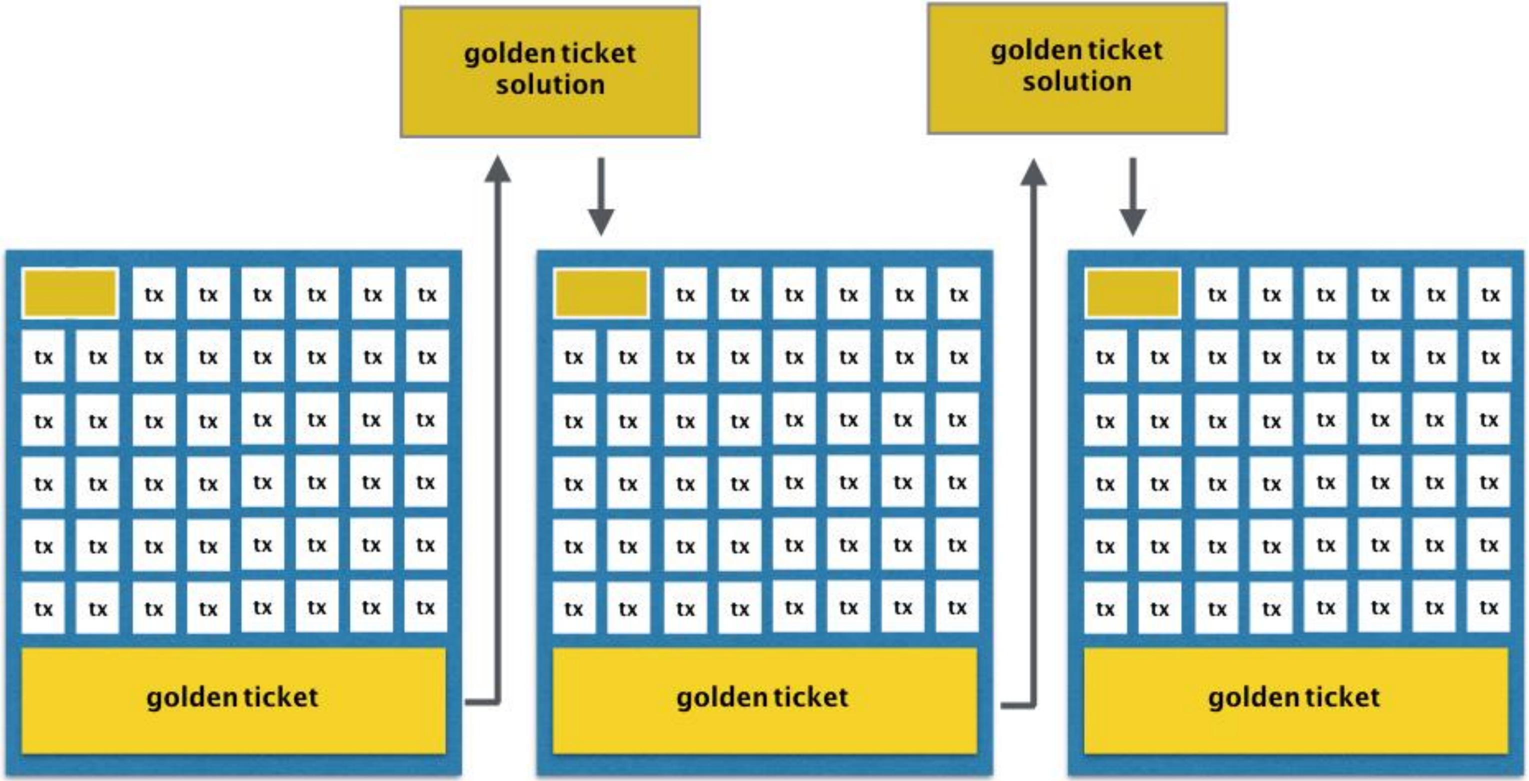
Every block we play a game to see who gets paid.

Nodes get a ticket for each transaction they route.

Miners conduct a provably-fair lottery.

One lucky node and one lucky miner split the fees!

Golden Ticket = Bitcoin Coinbase



Saito is Bitcoin… for routing

Keeping the network secure means preventing someone from collecting 100% of the fees/coinbase on demand. But we still need to pay them for their expenses. This requires that:

1. no-one can determine exactly when they get paid

2. but our overall payout reflects long-term workload

The difference?

Saito pays nodes for routing transactions.

Saito creates a viable, high bandwidth blockchain.

And it gets better....

Sometimes we want more mining, or cheaper bandwidth.

Wouldn't it be nice to change the paysplit sometimes?

But how?

Users / Applications

Users can change the paysplit of the lottery tickets….

… if you can get them to mostly agree

… and they have the support of either nodes or miners

Economic Equilibrium:

USERS
NODES
MINERS