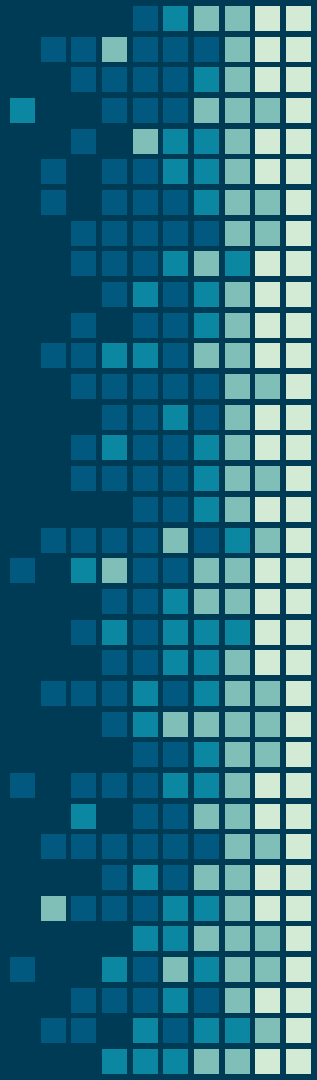
Saito

Proof of Transactions

Why Proof of Transactions?

We cannot scale without paying for bandwidth:

Proof-of-Work:	pays for mining
Proof-of-Stake:	pays for staking
Proof-of-Transactions:	pays for **routing**



Comparable Security to Bitcoin

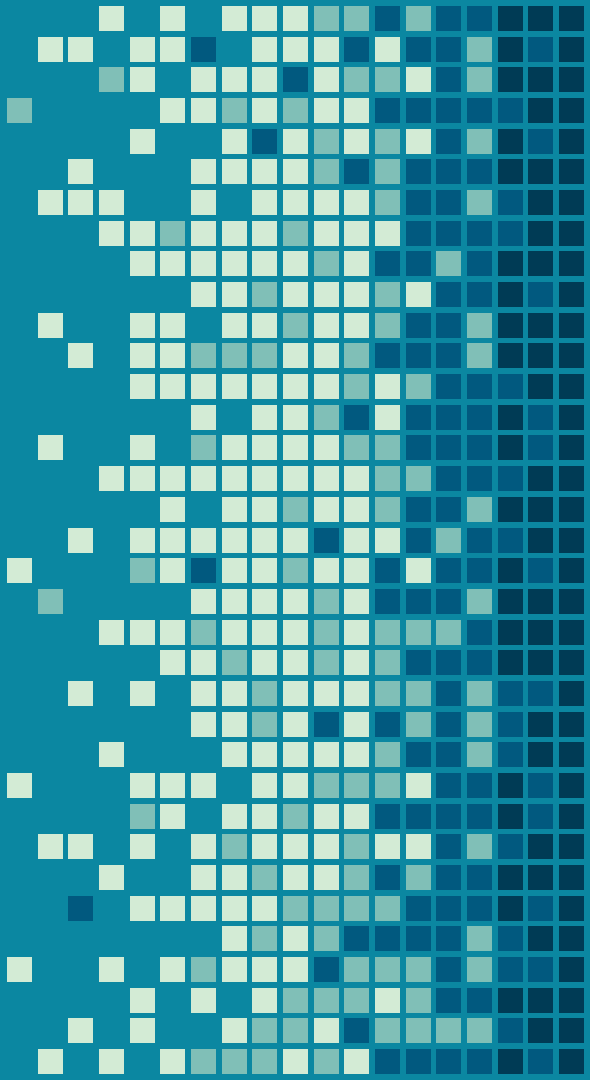
Attack Type	***Solution***	***Bitcoin Method***
Chain-Reorganization	make reorganization attacks expensive and risky	Proof-of-Work
Fee-Recycling	prevent monopolizing revenue	Proof-of-Work
Governance	prevent introduction of vulnerabilities from changes to consensus settings	Proof-of-Work

With a New Consensus Mechanism

Attack Type	***Solution***	***Saito Method***
Chain-Reorganization	make reorganization attacks expensive and risky	Burn Fee
Fee-Recycling	prevent monopolizing revenue	Golden Ticket
Governance	prevent introduction of vulnerabilities from changes to consensus settings	Economics

Part I: The Burn Fee

Quantify the risk of a block reorganization attack



How it Works

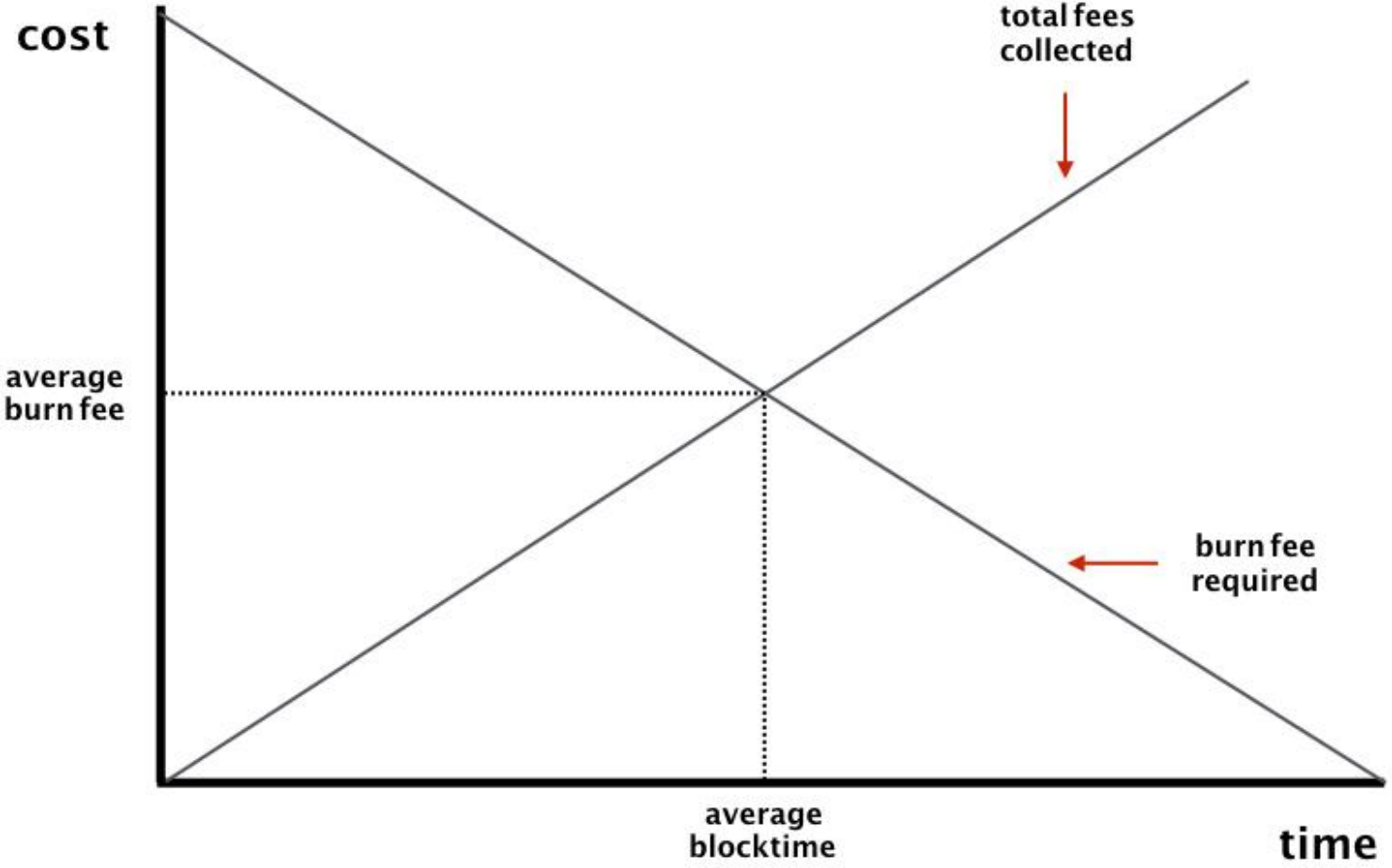
Nodes collect transactions for their fees

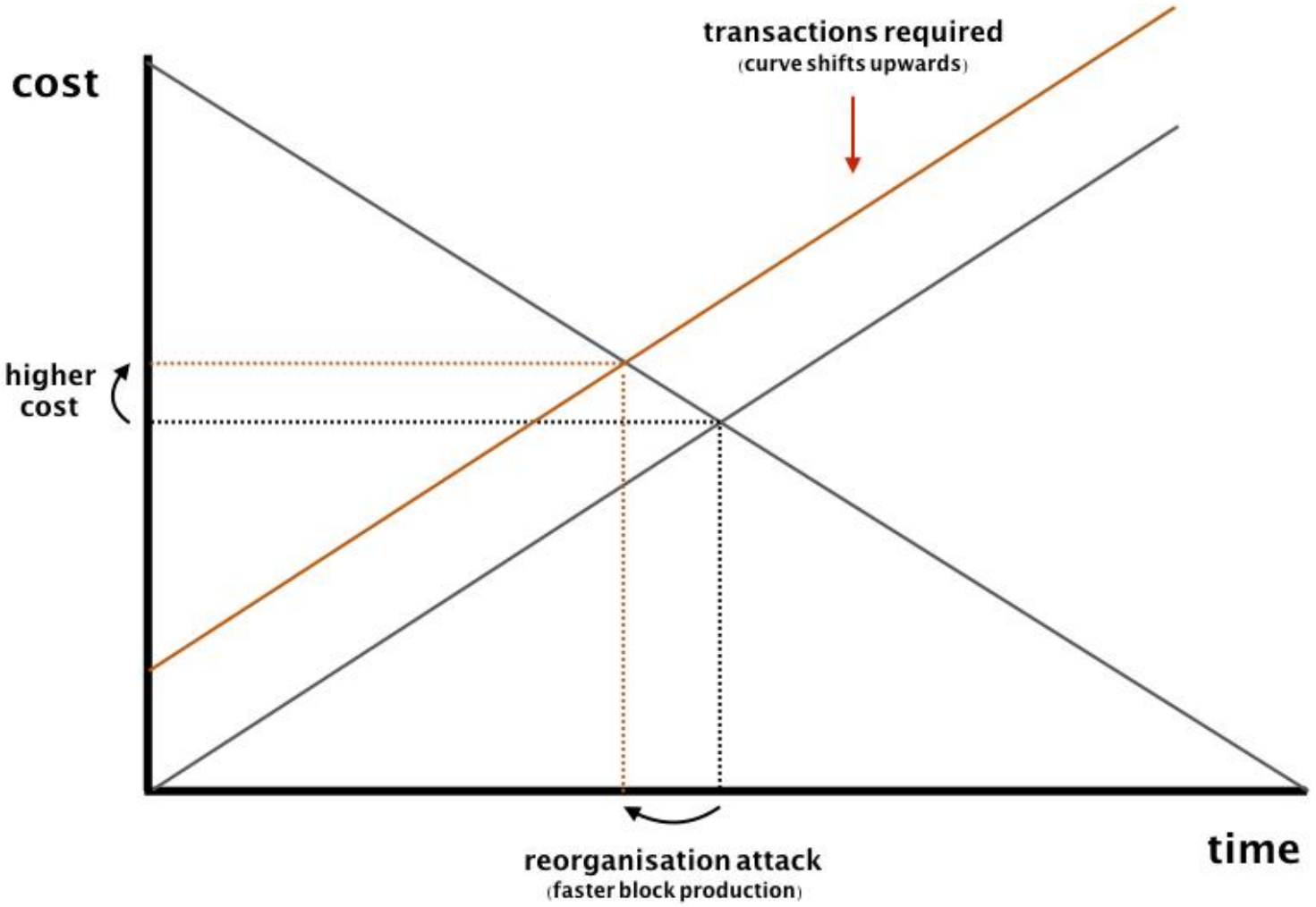
Collect enough fees and you can produce a block !

Fees drop with each hop through the network

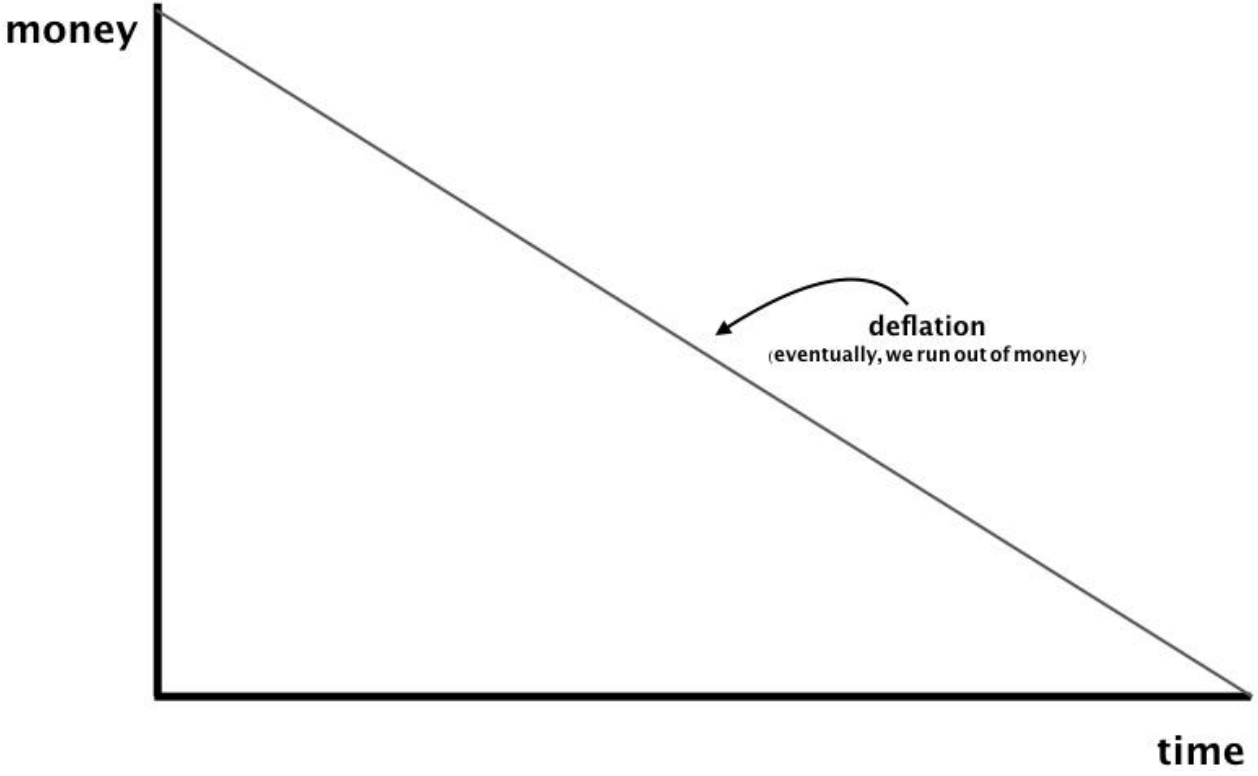
Economic forces secure the blockchain / prevent sibylling

BONUS: nodes can deny fees to censors / attackers !


cost
total fees
collected
average
burn fee
burn fee
required
average
blocktime
time


transactions required
(curve shifts upwards)
cost
higher
cost
time
reorganisation attack
(faster block production)

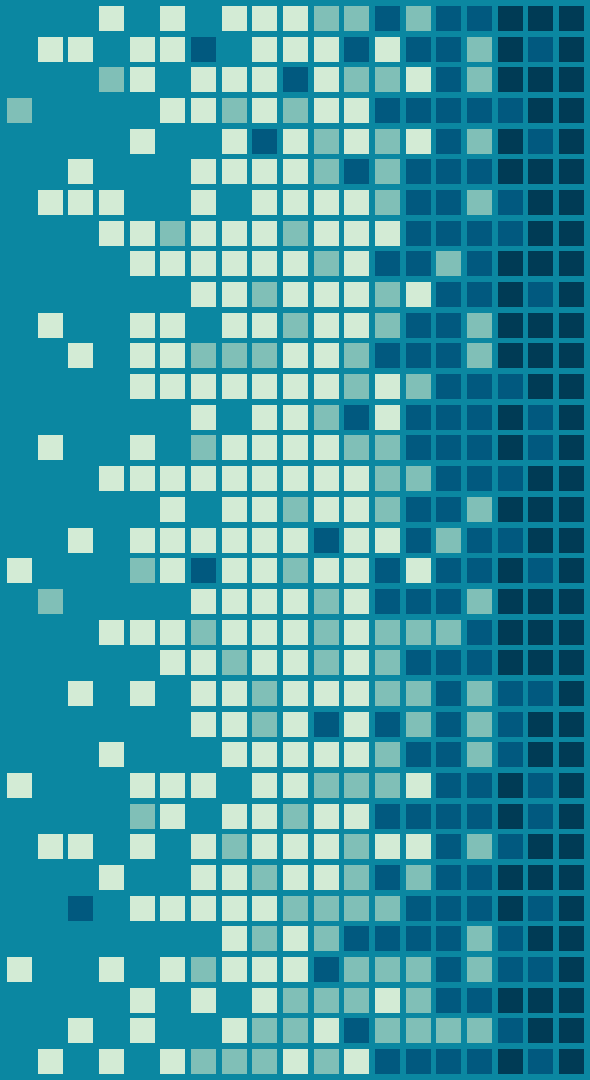
Problem: Monetary Issues



Part II: The Golden Ticket

Re-inject Money into our Blockchain

And Prevent Fee-Recycling Attacks

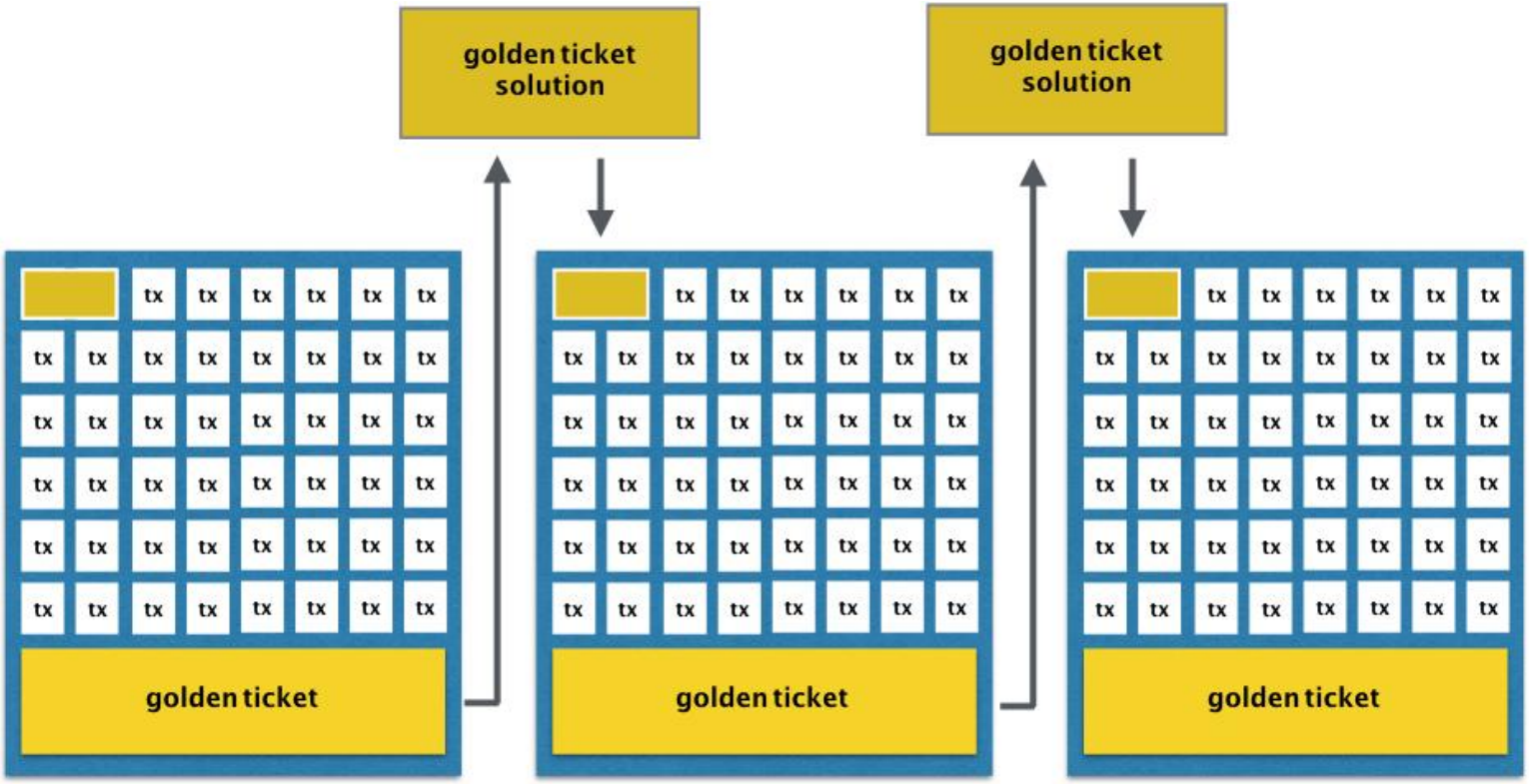


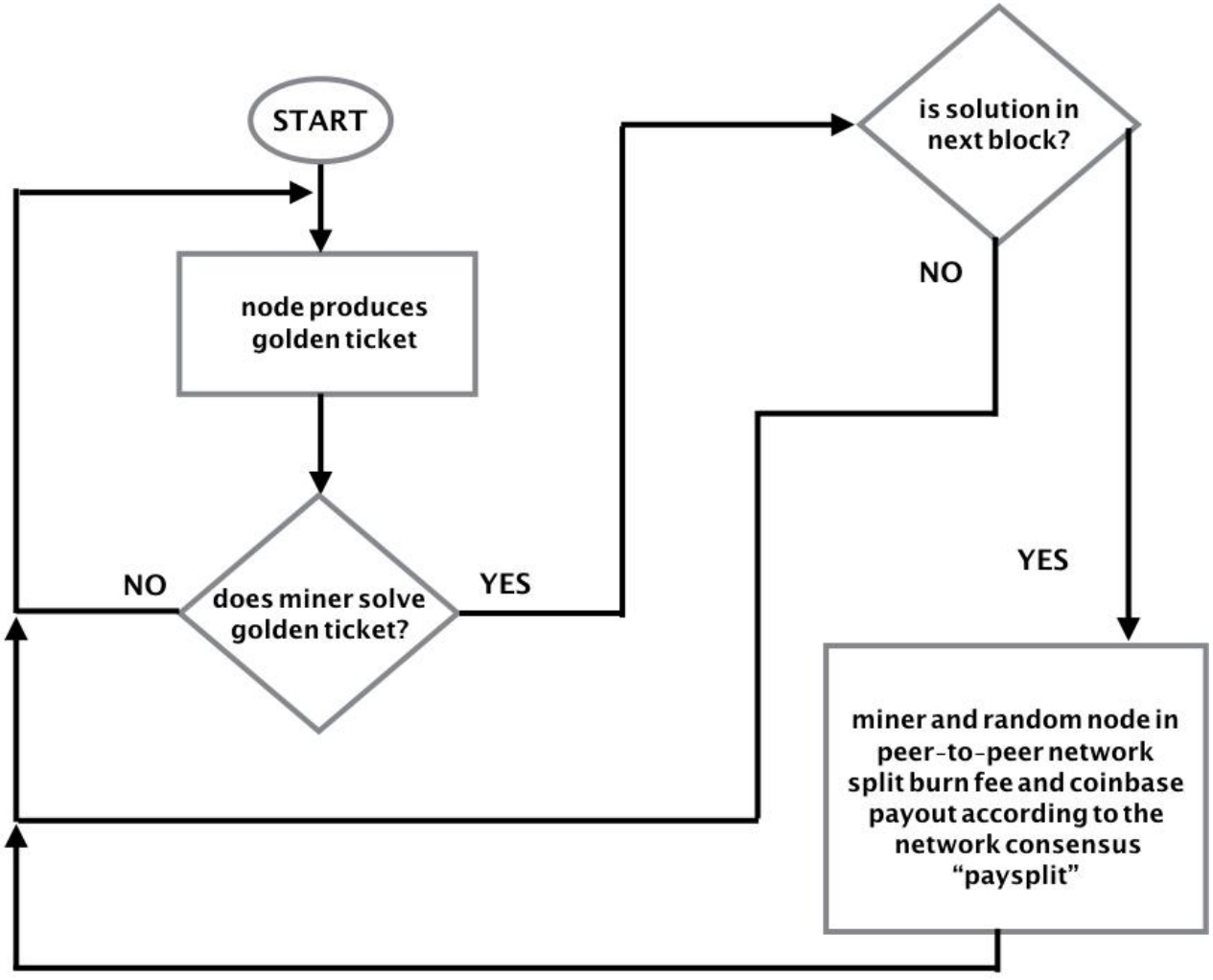
The Golden Ticket System

Nodes that produce blocks no longer "receive tokens"

In fact, no-one can predict who will get paid

But long-term distribution reflects contribution to network


golden ticket solution
golden ticket solution
tx
golden ticket
golden ticket
golden ticket


START
node produces golden ticket
does miner solve golden ticket?
NO
YES
is solution in next block?
NO
YES
miner and random node in peer-to-peer network split burn fee and coinbase payout according to the network consensus "paysplit"

Why is this fair?

neither full-nodes nor miners can predict the winners:

- the full-node provides the puzzle
- the miner provides the solution
- winning full-node selected using miner solution

cheating is impractical

but what should the paysplit, between miner and node, be:

0.5? 0.25?

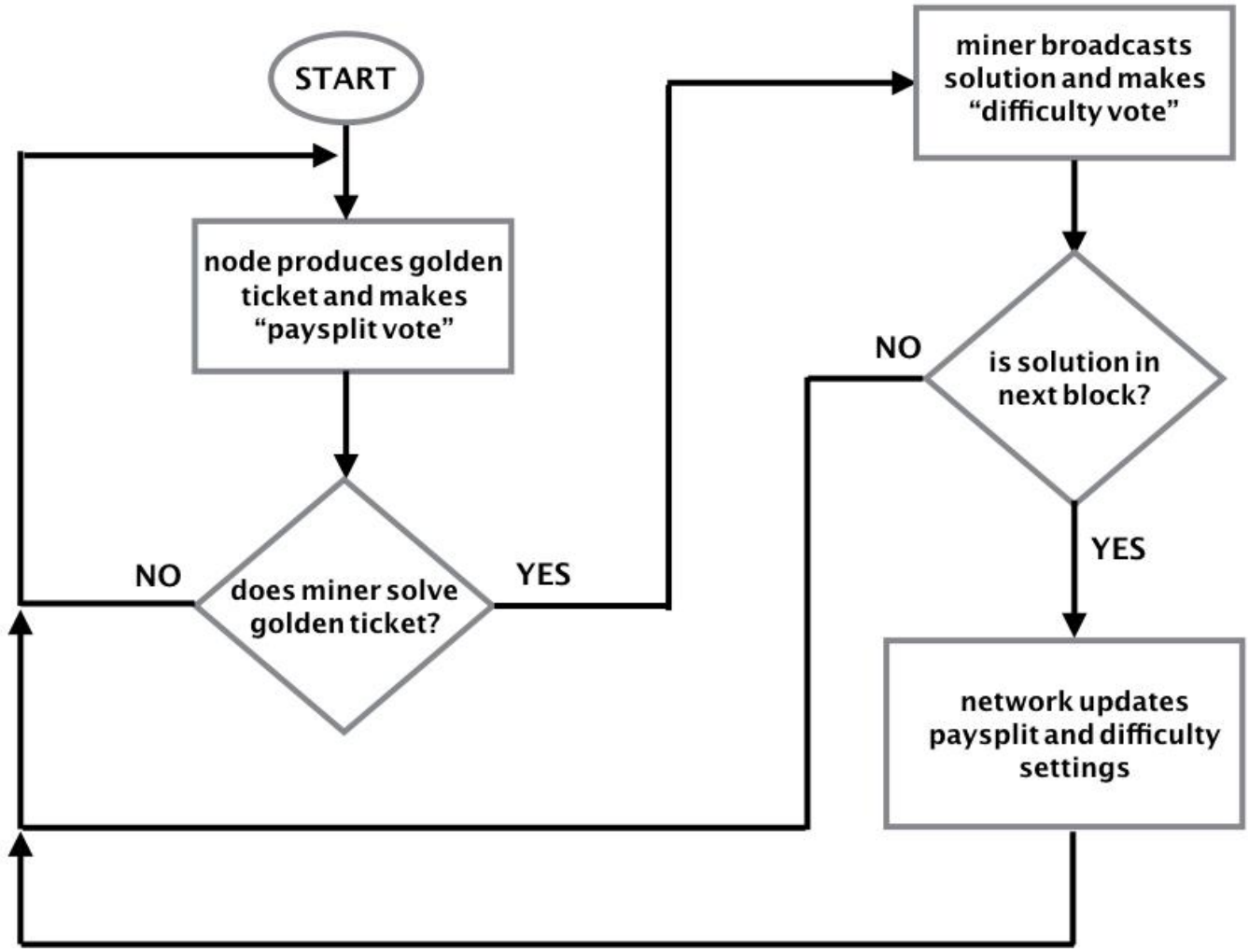
Part III: Voting Mechanism

Allows paysplit to optimize, yet:

Defends against Governance Attacks

nodes vote on paysplit

miners vote on difficulty


START
node produces golden ticket and makes "paysplit vote"
does miner solve golden ticket?
NO
YES
miner broadcasts solution and makes "difficulty vote"
is solution in next block?
NO
YES
network updates paysplit and difficulty settings

Why don't nodes take all the money?

security concerns

economic incentives

Security Concerns

1. All votes require node and miner approval

otherwise no-one gets paid

2. Nodes want miner support for security reasons

less mining == fewer solutions == smaller transaction fees

more mining == more solutions == bigger transaction fees

Paying miners more speeds up block production and secures the network

3. Nodes also need to ward off orphaning attacks....

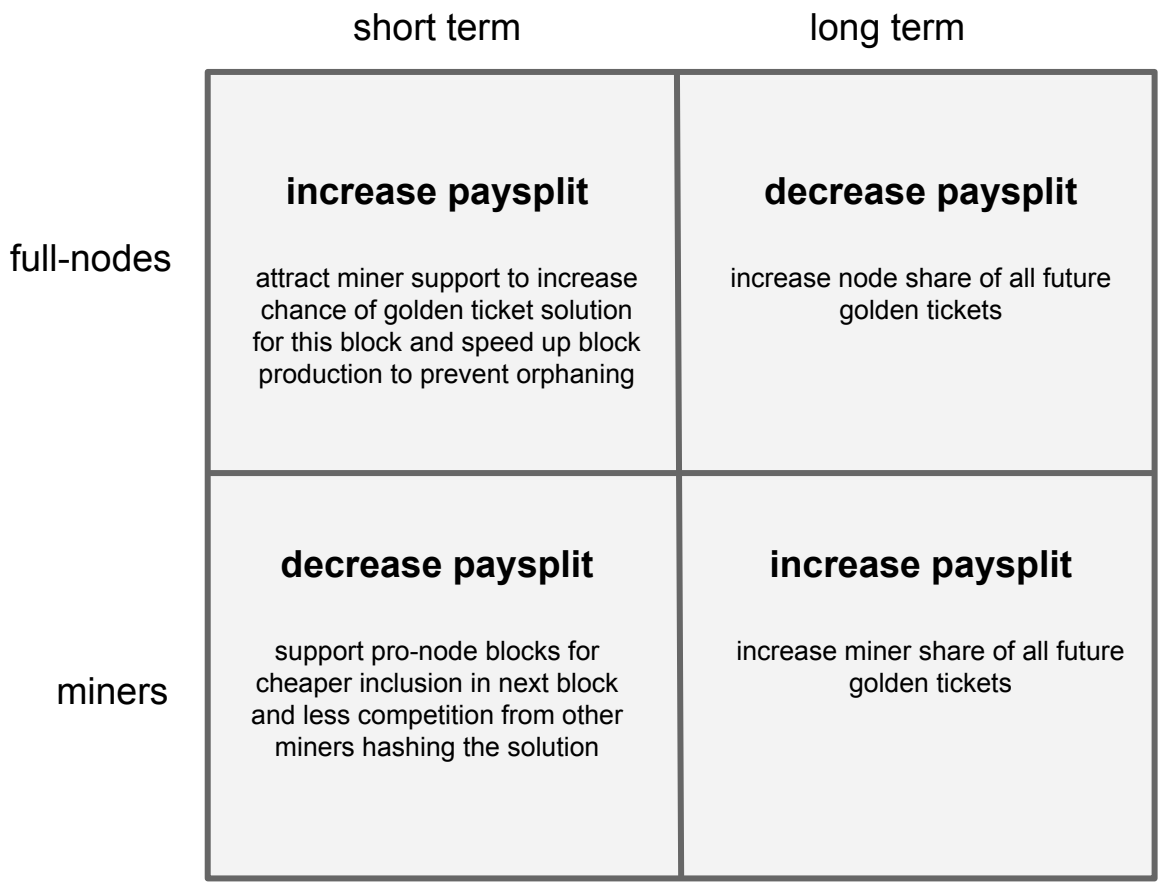
because miners can pump-out pro-miner blocks too

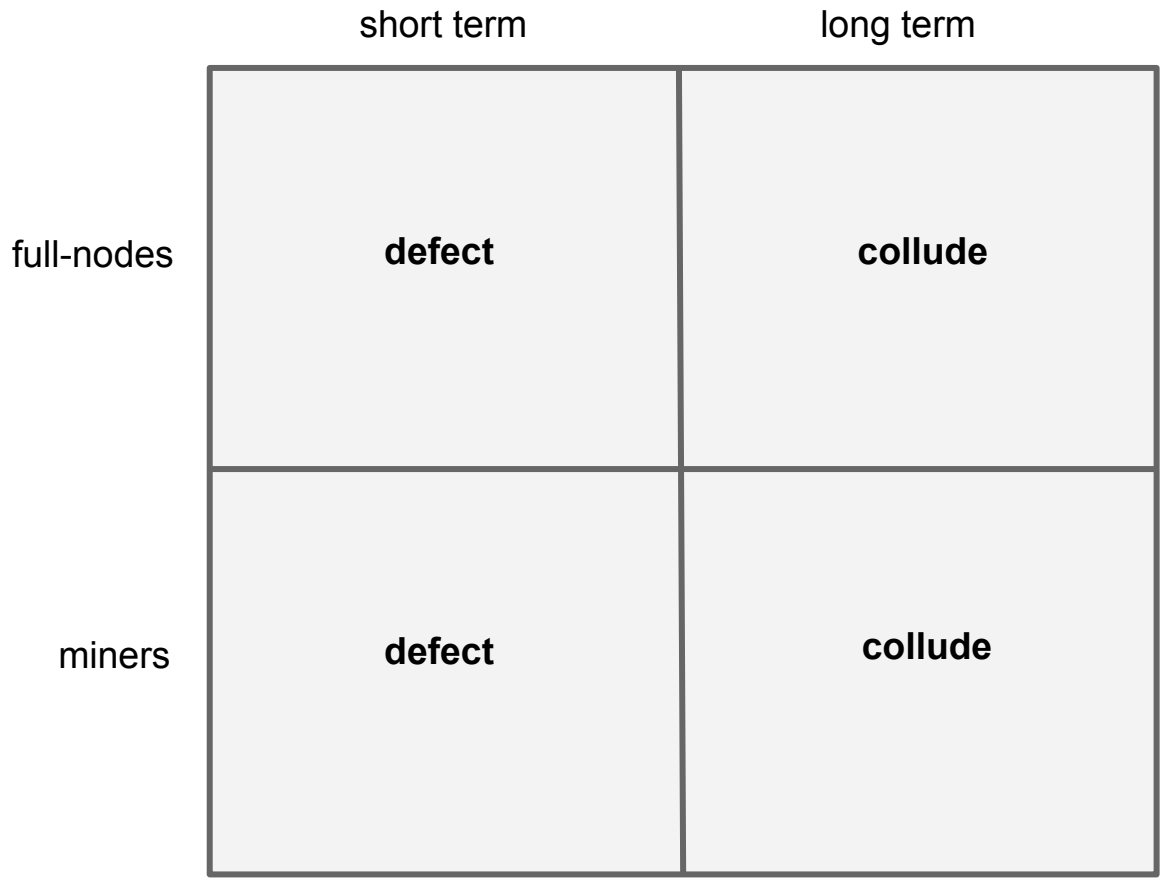
Economic Incentives

Collusion leads to Profits

Profits lead to Competition

Competition leads to Defection


short term
long term
full-nodes
miners
increase paysplit
attract miner support to increase chance of golden ticket solution for this block and speed up block production to prevent orphaning
decrease paysplit
increase node share of all future golden tickets
decrease paysplit
support pro-node blocks for cheaper inclusion in next block and less competition from other miners hashing the solution
increase paysplit
increase miner share of all future golden tickets


short term
long term
full-nodes
miners
defect
collude
defect
collude

When does the short-term dominate?

When the expected future value (EFV) of in-group collusion is worth less than the profits from defecting. This is guaranteed at some point because:

profit = revenue - expenses

EFV is discounted because:

(1) time-value of money

(2) high profits will attract competition

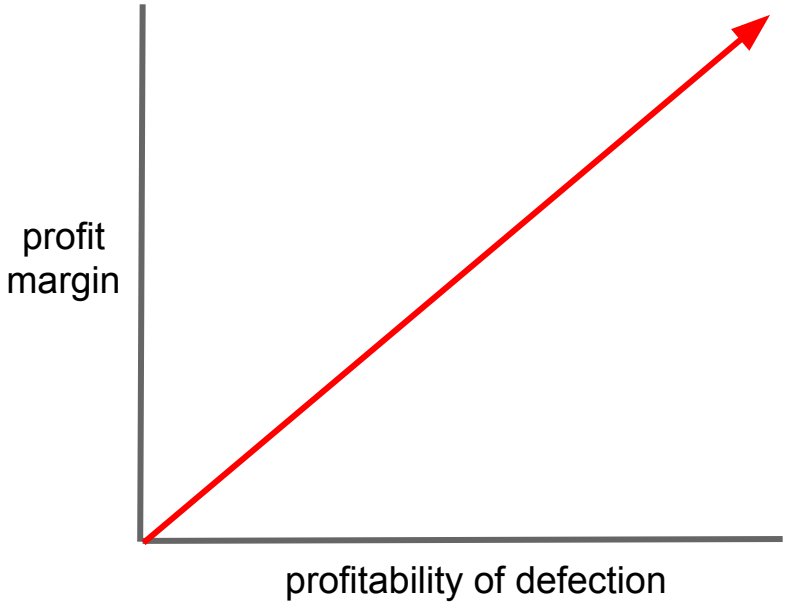
(3) competition increases difficulty of collusion

(4) competition lowers return on investment

The Long-Term is in Equilibrium

Our two-player equilibrium lies at the point where nodes and miners have equal incentives to collude and defect.

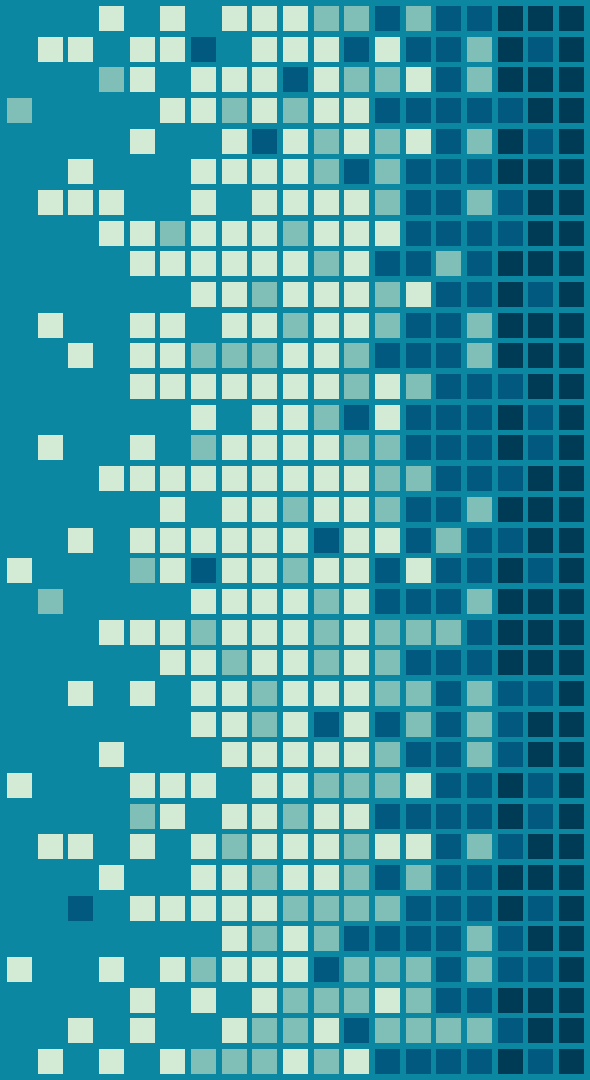
The only way to improve profitability at this point is to become more efficient at routing or mining: exactly what we want to incentivize.



Improving our Equilibrium

A two-player equilibrium reflects the trade-offs that nodes and miners make to maximize their own interests.

We want paysplit to reflect the market preference for bandwidth versus security, and thus we add....



USERS

NODES

MINERS

A Three Player Game:

Every transaction gets an optional paysplit vote

Transactions cannot be included in blocks which vote against their paysplit preference

This subtly adjusts the resources available to full-nodes and miners in their battle over paysplit, shifting the equilibrium gradually towards cheaper bandwidth or higher difficulty.

No Group Can Dominate

USERS

NODES

MINERS

What have we accomplished?

consensus variables float... securely

centralization in routing / mining non-threatening

economic pressures secure the network

any two groups can safeguard the network from a malevolent third

Proof-of-Transactions is Bitcoin-Class

Attack Type	***Solution***	***Method***
Chain-Reorganization	make reorganisation attacks expensive and risky	Burn Fee
Fee-Recycling	prevent any user from monopolizing revenue	Golden Ticket
Governance	prevent introduction of vulnerabilities from changes to consensus settings	Economics