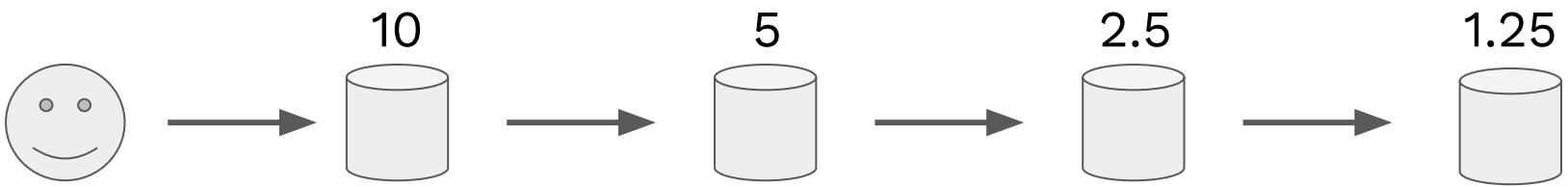
Saito

Blockchain Mechanisms

Part I: Block Production

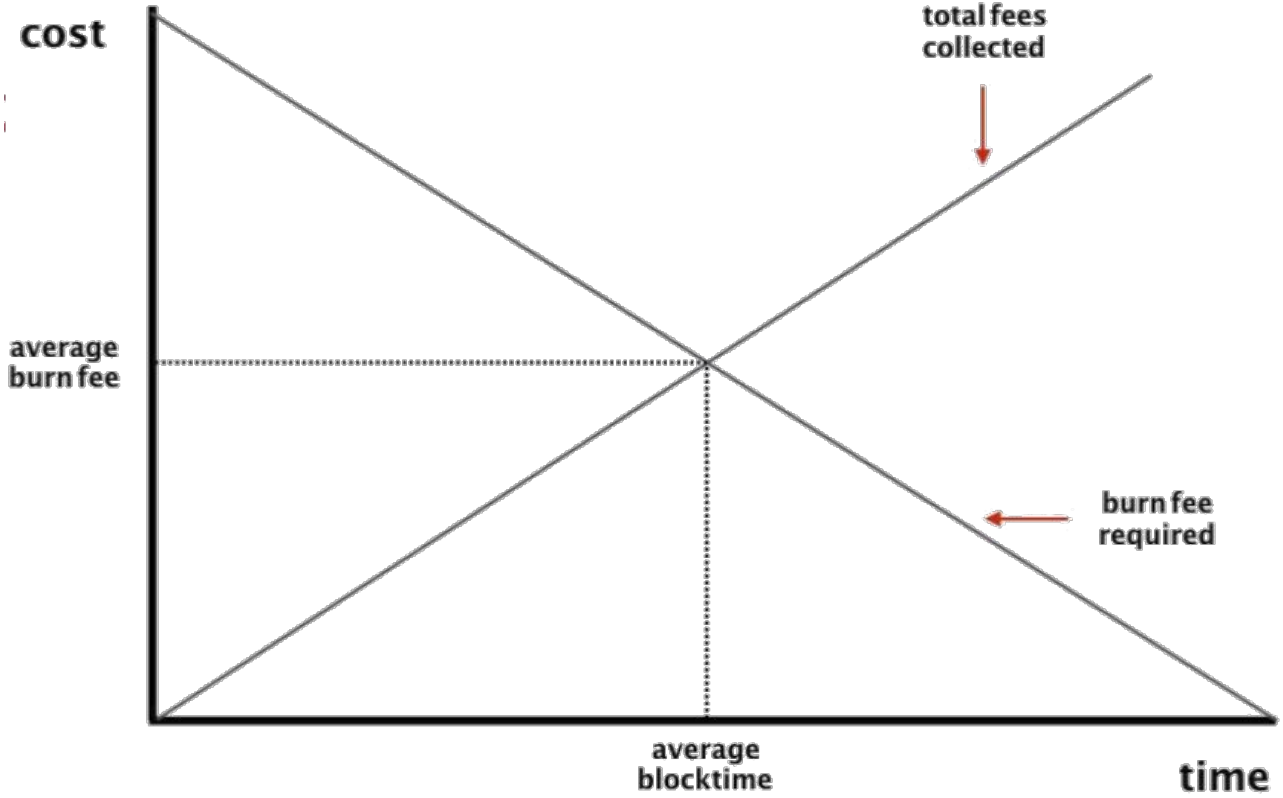
1 - Measure Routing Work

Cryptographic signatures added to the network layer allow us to measure “routing work” (the value of the tx fee, halved by every hop (n > 1) the tx has taken to reach that node:



A 10 SAITO tx-fee routed 4 hops generates 18.75 units of work.

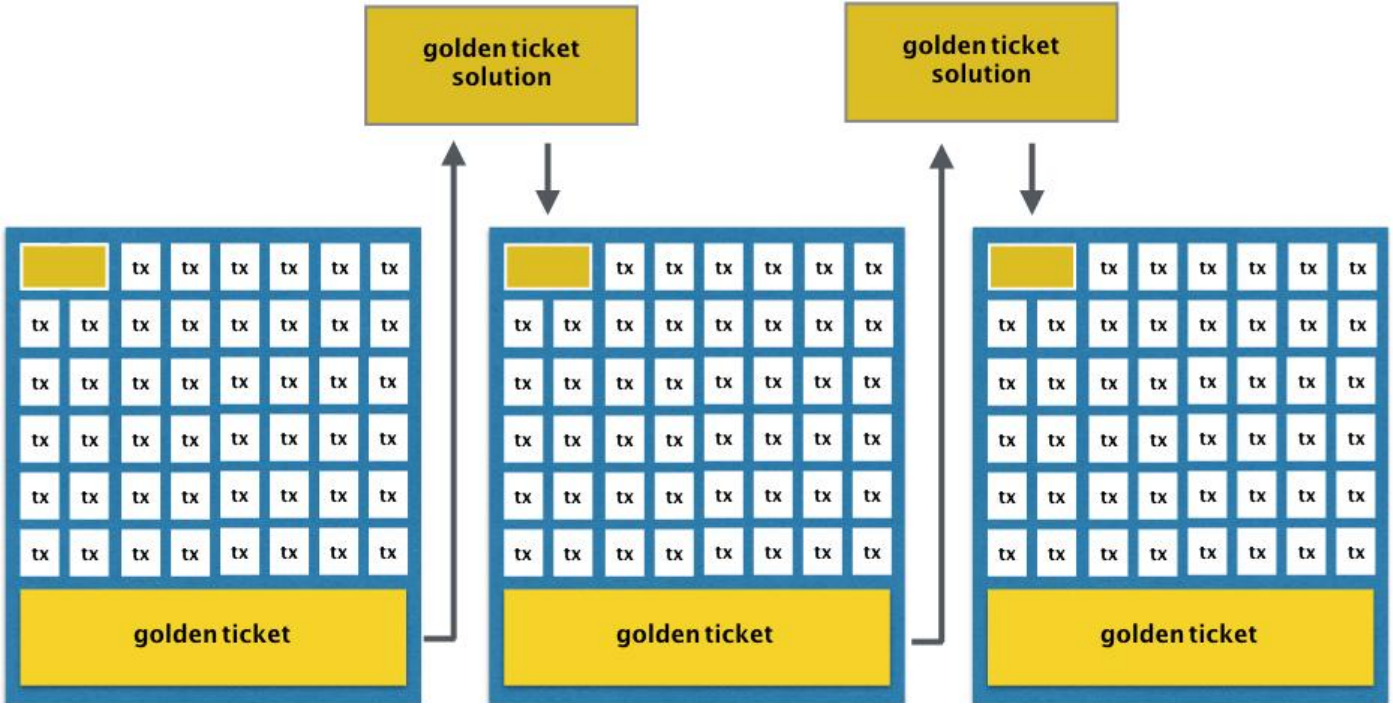
2 - Use Routing Work to Produce Blocks



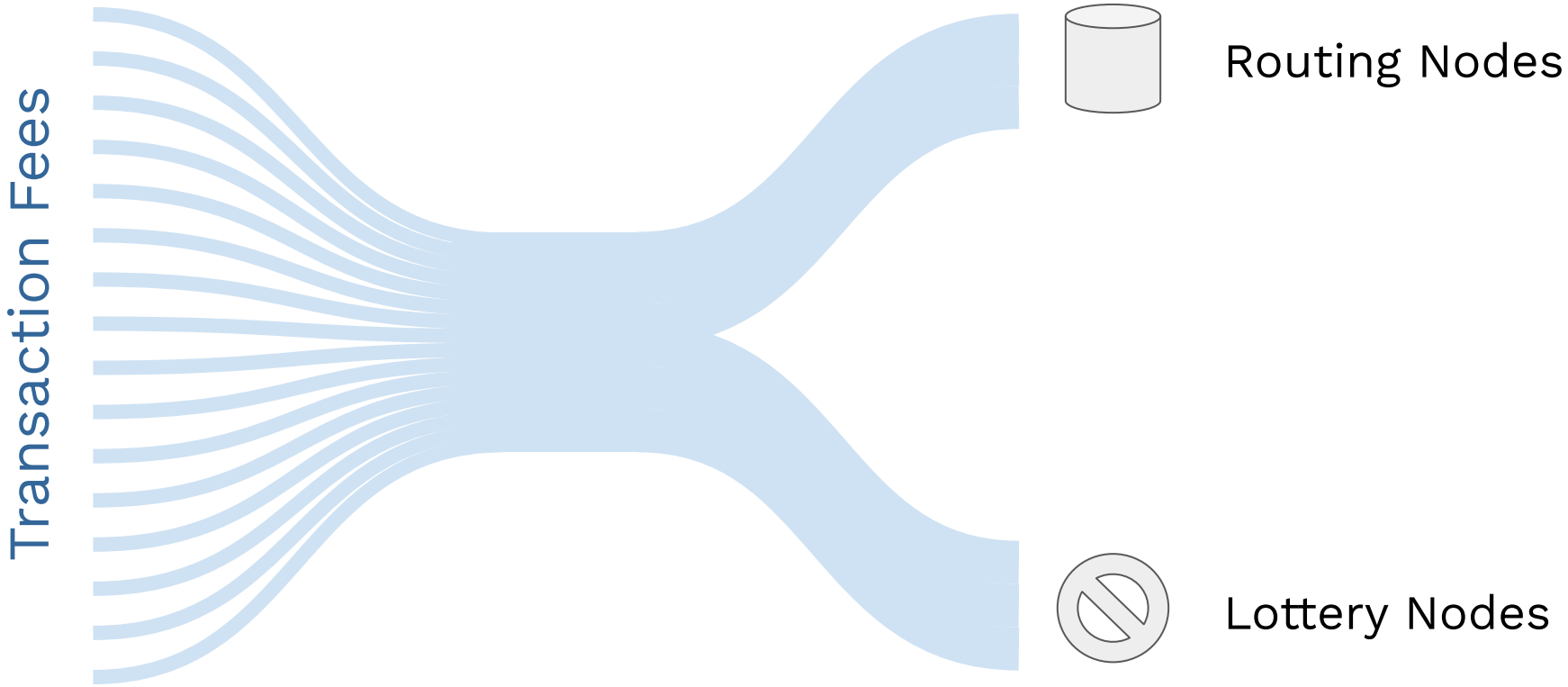
Honest nodes route transactions and eventually produce blocks for free.

Attackers must spend their own money to attack the network.

3 - Hold a Proof-of-Work Lottery



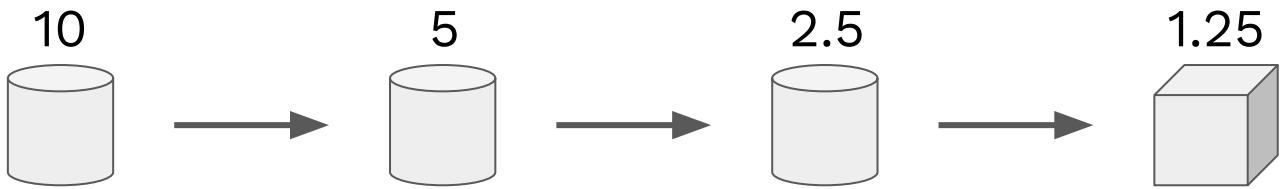
4 - And split up the block reward



5. Random Solution picks Winning Router...

$$\text{CHANCE OF WINNING} = \frac{\text{your routing work}}{\text{sum of all routing work in block}}$$

... so pay is proportional to work



CHANCE OF WINNING

$$\frac{10}{18.75} \qquad \frac{5}{18.75} \qquad \frac{2.5}{18.75} \qquad \frac{1.25}{18.75}$$

Paying routing nodes incentivizes:

Data Throughput

while the lottery eliminates economic attacks...

Secure Against 51% Attacks:

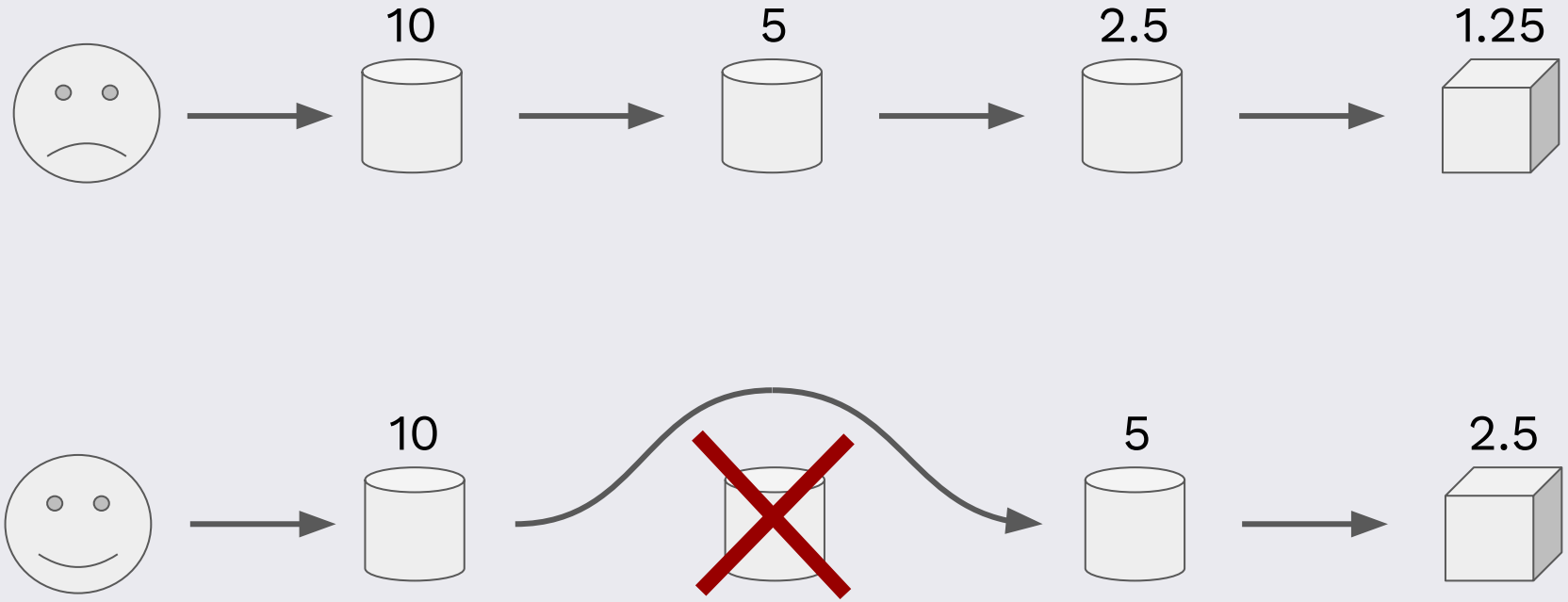
Producing a viable fork requires attackers to:

- match all outstanding routing work collected by honest nodes in the network (by locking up their own money to generate comparable routing work).

- more than double the mining done by the honest network to attack the payment lottery and get a portion of their money back.

Attackers are guaranteed to lose money in all situations. For an intuitive understanding of how this dynamic works, check out the “poker video” listed on our page about Saito Economics.

Secure against Sybil Attacks:



Secure Against Spam Attacks:

Consensus rules and cryptographic signatures on the network layer defend against “block flooding” and other forms of network spam attacks.

Other Remarkable Properties

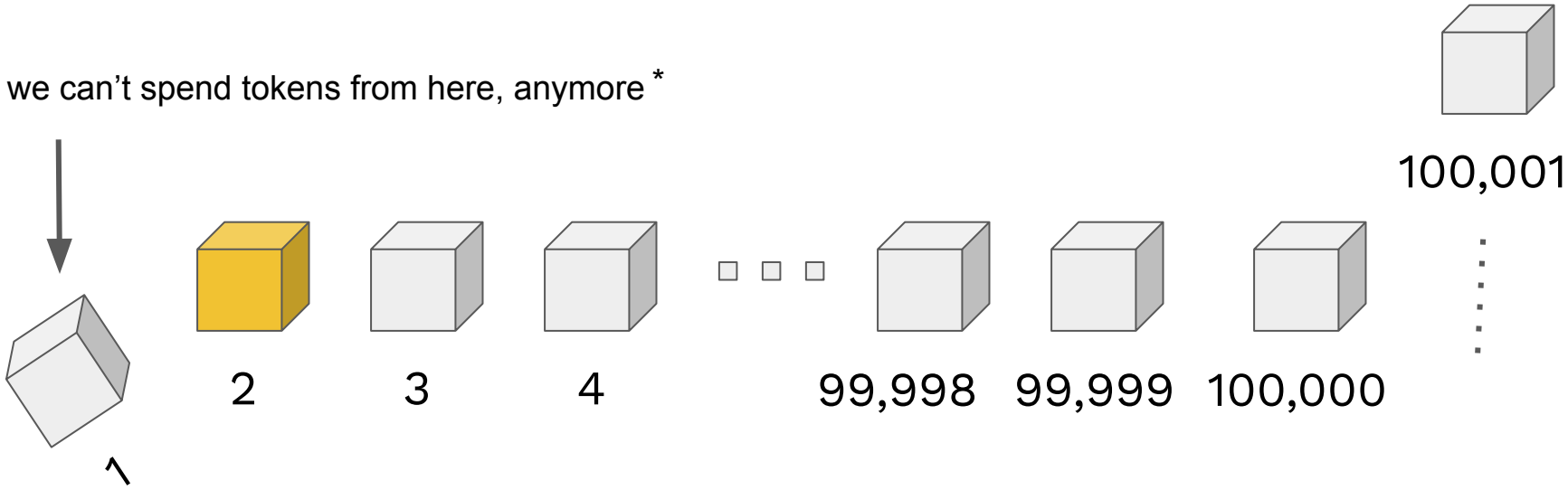
Servicing network users is the Saito equivalent of mining

Eliminating 51 percent attacks doubles the security of POW and POS mechanisms, and halves cost since additional fees are not needed to pay for network infrastructure.

The full consensus mechanism, including PAYSPLIT / POWSPLIT modifications which increase security above 100 percent of network fee volume, can be found in the Saito Whitepaper or in the Github docs directory of the main distribution.

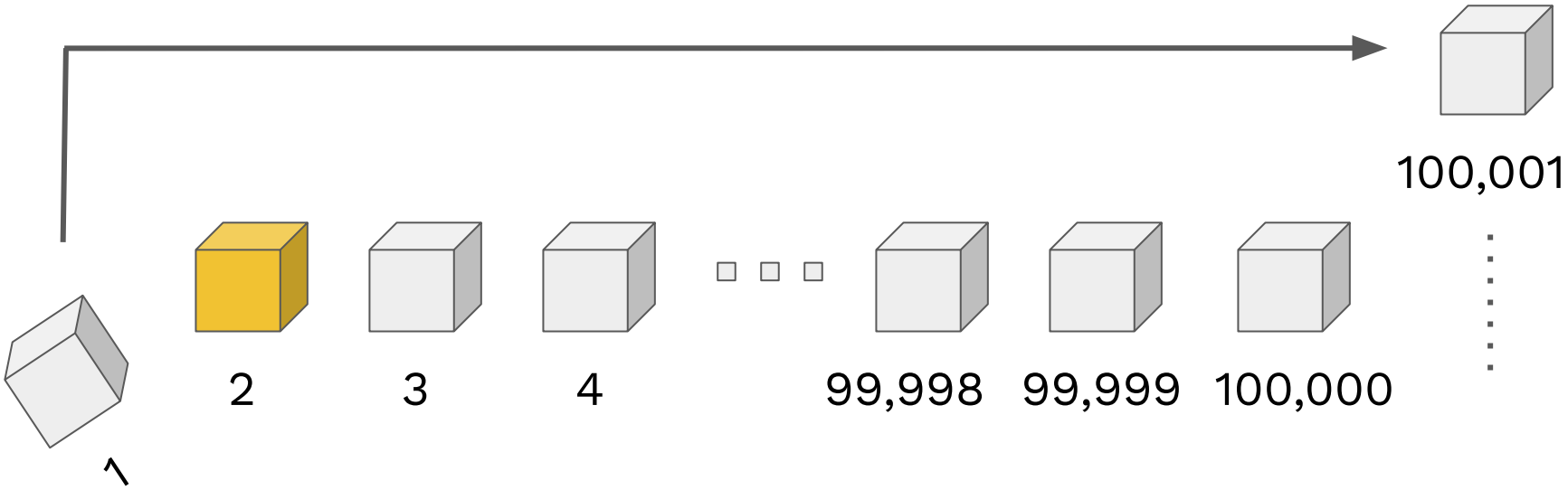
Part II: Blocksize Economics

#1 - Genesis Block updates (like a checkpoint)



* 32-byte header retained to prove original genesis block

#2 - Transactions Automatically Rebroadcast



- UTXO and data from block #1 must be re-included in block #100,001
- ATR transactions are charged a fee for data rebroadcasting
- UTXO that are spent or unable to pay this fee are removed

Block Producers:

1. accept fewer new transactions
2. increase fees paid by old transactions
3. profit-motive regulates blocksize

Market Solution:

1. users pay market rates
2. no-one can pass costs into the future
3. keep data on-chain forever (if you want)
4. or remove it (spend the UTXO)