Blockchain Principles and Applications

Amir Mahdi Sadeghzadeh, PhD

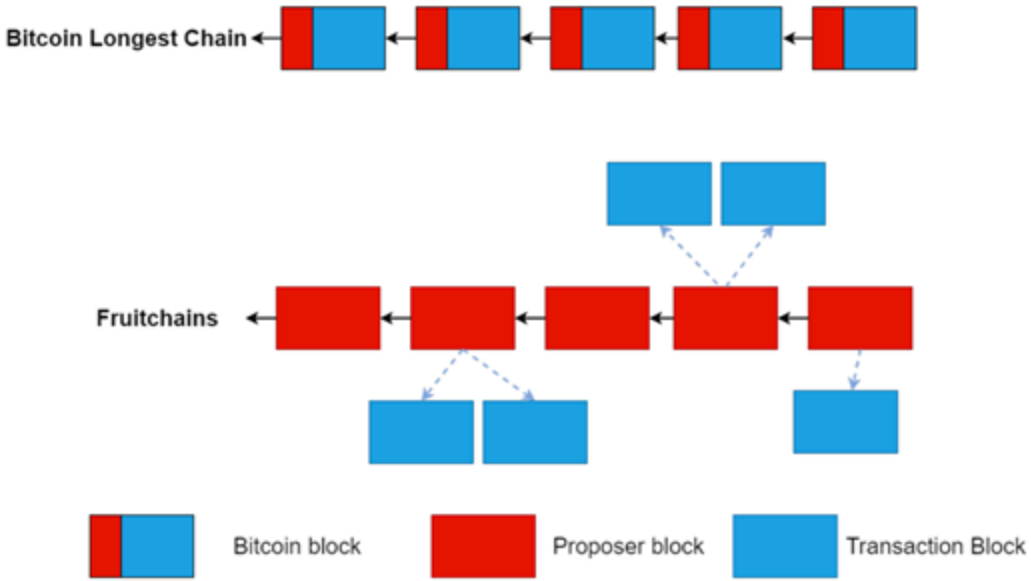
Data and Network Security Lab (DNSL)
Trustworthy and Secure AI Lab (TSAIL)

Most slides have been adapted from ECE/COS 470, Pramod Viswanath, Princeton 2024 and CS251, Dan Boneh, Stanford 2023.

Recap

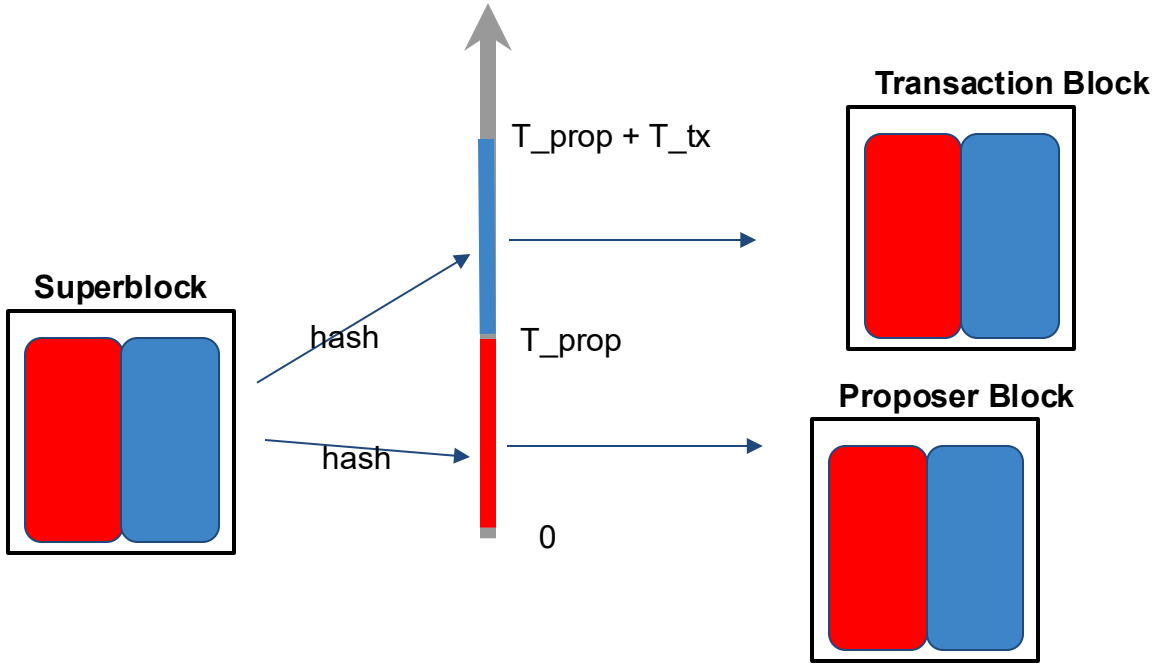
Fruitchains

Main idea: separate transactions (& their rewards) from blocks in the longest chain

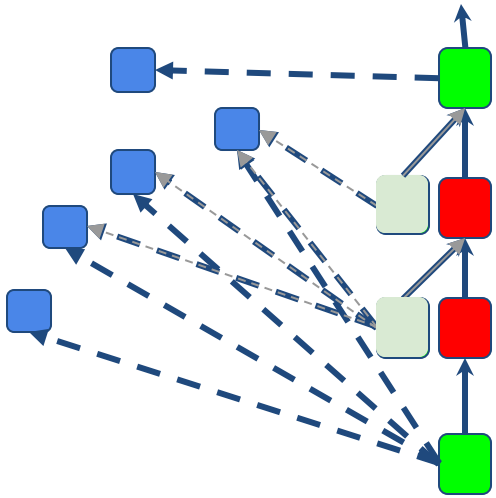


Cryptographic Sortition

How to do PoW for both types of blocks simultaneously?



Optimal chain quality



Transaction block

Displaced proposer block

Honest proposer block

Adversarial proposer block

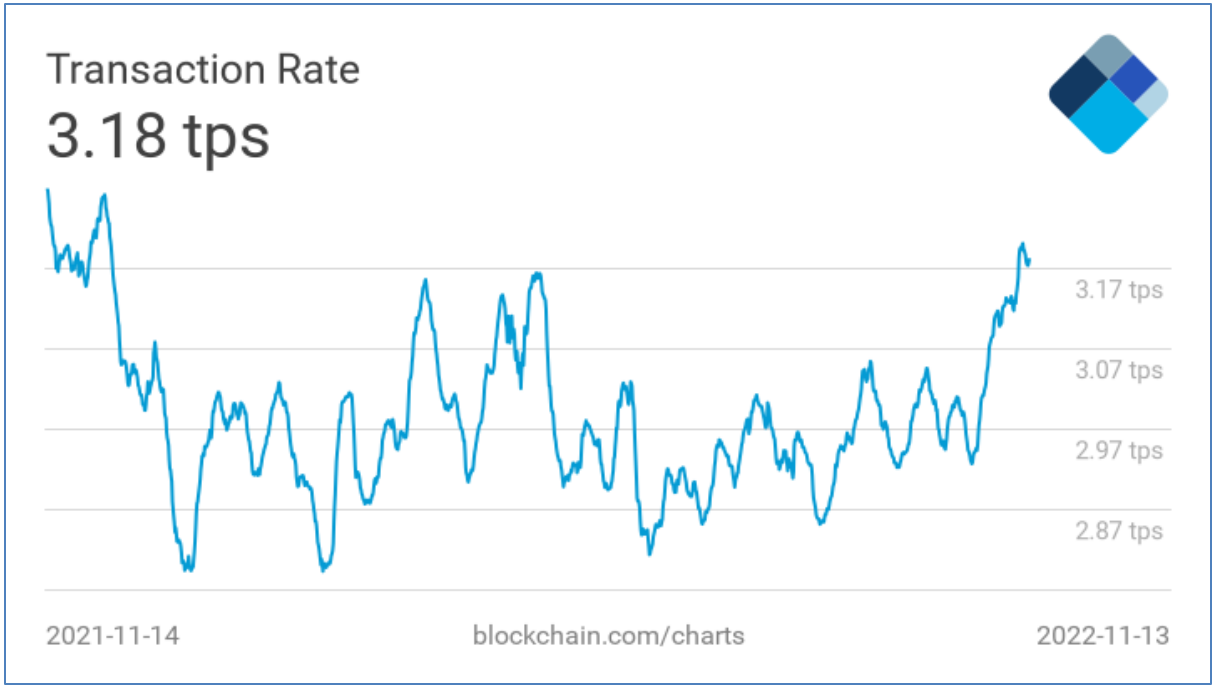
Fraction of honest transaction blocks **in the longest chain**

Fraction of honest transaction blocks **overall**

$$\mathrm{CQ} \geq \frac{(1-\beta)\lambda_{\mathrm{tx}}}{(1-\beta)\lambda_{\mathrm{tx}} + \beta\lambda_{\mathrm{tx}}} = 1-\beta.$$

Scaling Throughput

Bitcoin Tx per second



≈4200 Tx/block
1 block / 10 mins

⇒ max: 7 Tx/sec

Ethereum Tx per second

Ethereum avg Tx per second:

≈ 15 Tx/sec

Simple Tx: 21k Gas
max 30M Gas per block
⇒ max 1428 tx/block

1 Block/12s
⇒ max 119 tx/s

In comparison …

Visa: up to 24,000 Tx/sec (regularly 2,000 Tx/sec)

PayPal: 200 Tx/sec

Ethereum: 15 Tx/sec

Bitcoin: 7 Tx/sec

Goal: scale up blockchain Tx speed

Performance

Throughput: transaction per second (tx/s)

- **Bitcoin: 7 tx/s**
- **Ethereum: 100 tx/s**

Why is throughput so small in Bitcoin?

Throughput

Throughput = $\frac{(1-\beta)\lambda}{1+(1-\beta)\lambda\Delta} \cdot B$ tx/s

- β: fraction of adversarial hash power; no control
- λ: mining rate; can be controlled by setting mining target easy
- B: block size; can be controlled by allowing more transaction in a block
- Δ: network delay; proportional to block size B

So throughput $\propto \frac{(1-\beta)\lambda}{1+(1-\beta)\lambda\Delta}$, limited by $\lambda\Delta$

Recap: security

Security holds when longest chain mining growth rate > adversarial private chain growth rate, i.e.,

$$\frac{(1-\beta)\lambda}{1+(1-\beta)\lambda\Delta} > \beta\lambda$$

So throughput is limited due to forking (and security)

Scaling throughput

We study 3 efforts to improve throughput

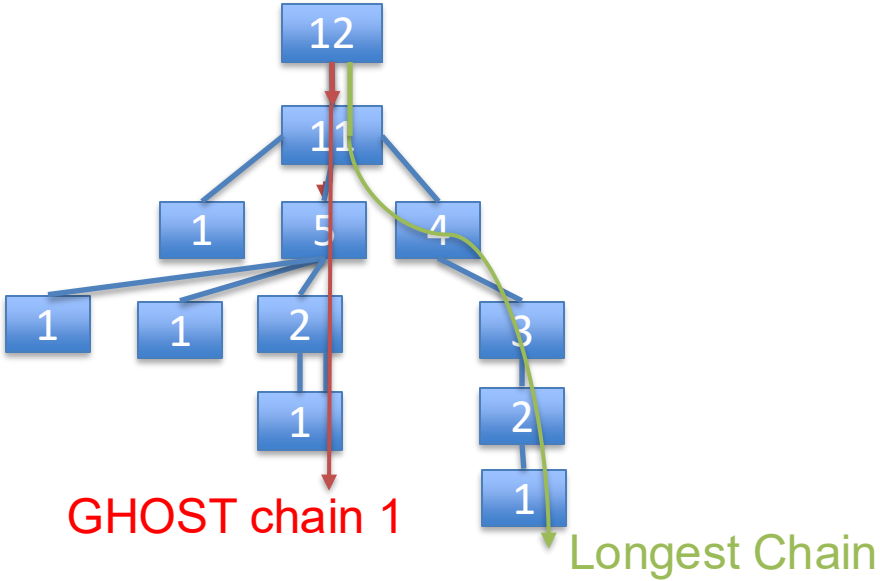
The first two are flawed to different levels

And the third scales throughput optimally, where only the network limits the throughput

Idea 1: embrace forking

GHOST: Greedy Heaviest-Observed Sub-Tree

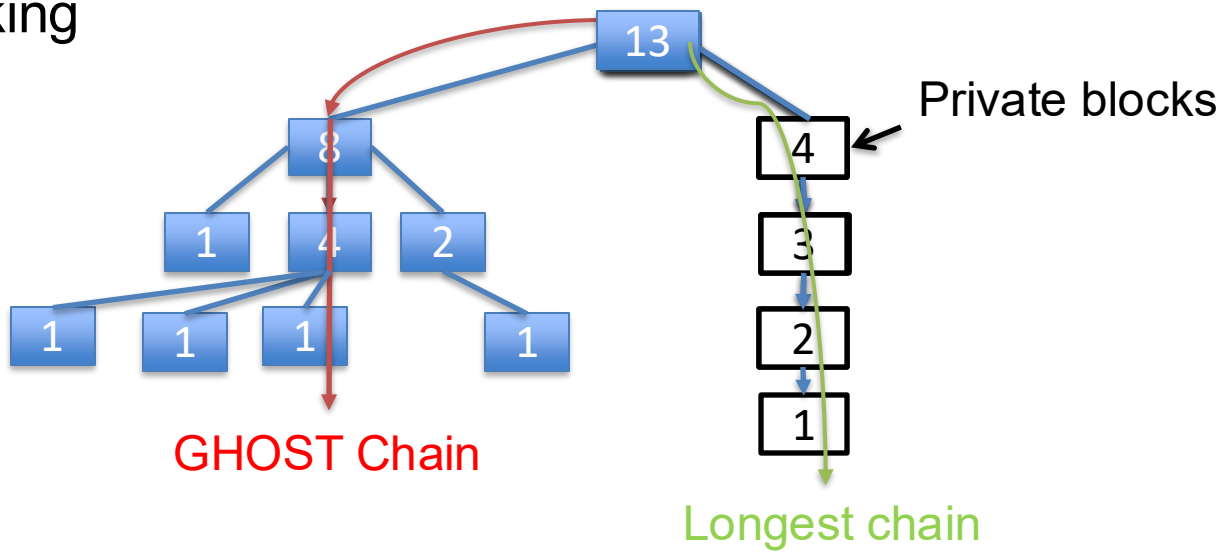
- A modification to the mining rule: no longer mine on the tip of the longest chain; mine on the tip of the GHOST chain



Private attack on GHOST

The GHOST chain is harder to displace by a private attack

- Because all the blocks in the sub-tree count; forking is not wasted
- Hence the mining rate can be increased without worrying about forking



GHOST is secure?

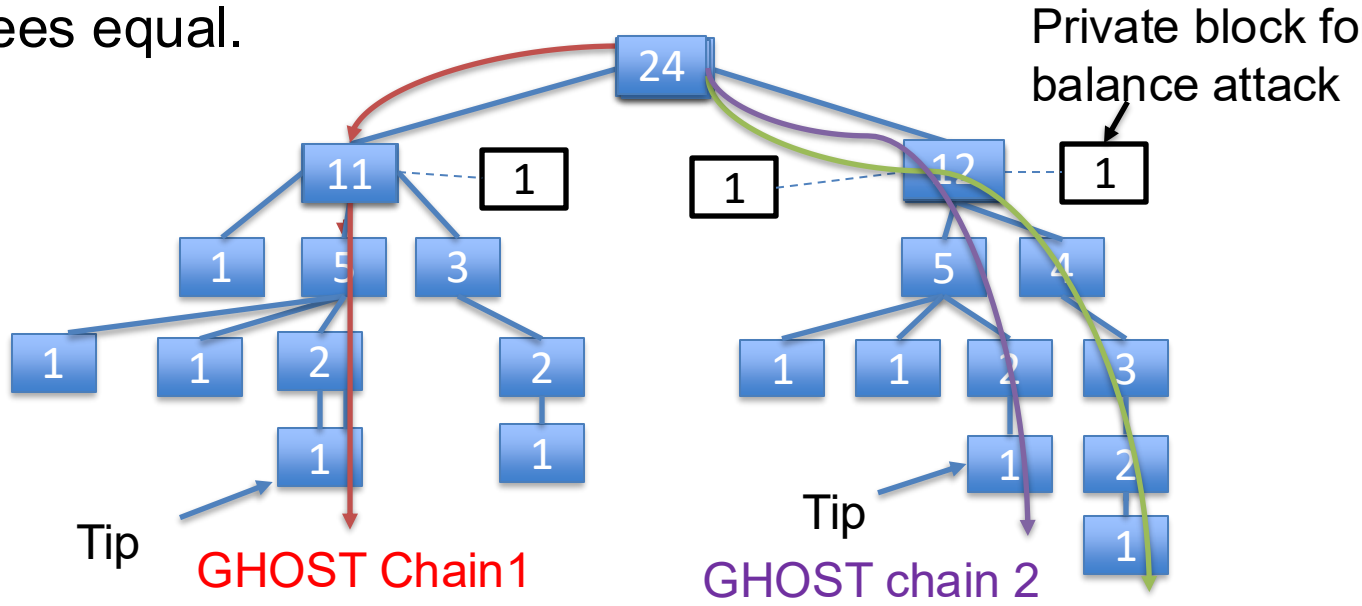
The intuition behind GHOST refers to resistance to the private attack

We already know that the private attack was the worst case attack for **the longest chain protocol**

However, the worst case attack for GHOST could be different

Balance attack on GHOST

- The idea is to have two chains and honest mining is split between them
- The adversary reveals private blocks to keep the weights of two sub-trees equal.



Balance attack on GHOST

- Balance attack is a bit more subtle than private attack in the sense that more network control is needed
- **Safety attack:** because the ledger swings wildly between two sub-trees
- Security threshold: essentially back to the Bitcoin level
  - This limits throughput

Idea2: reduce forking

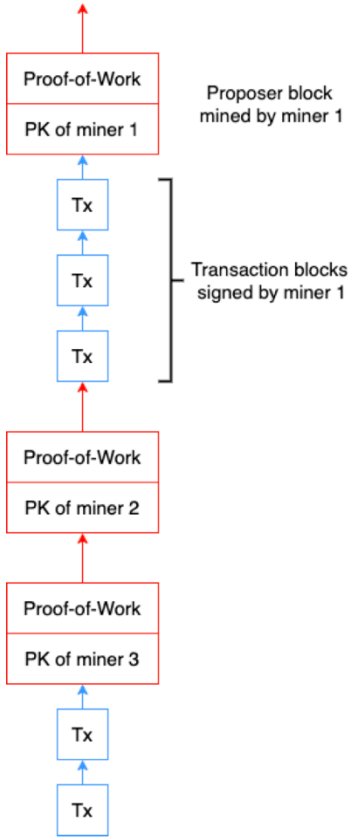
Longest chain rule: miner proposes only one block for a successful nonce

Idea: why not do many blocks for one mining?

How is this different from a large block size?

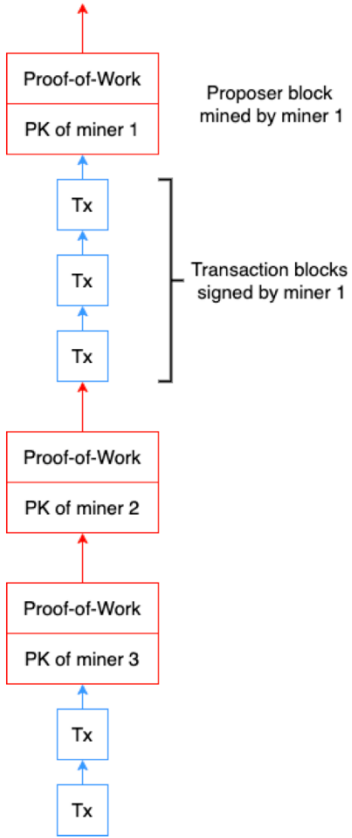
Bitcoin-NG

- Consist of proposer blocks and transaction blocks
- Only mine the proposer block at the tip of the longest chain
- The same proposer signs transaction blocks



Bitcoin-NG

- K-deep rule: PoW blocks
- PoW difficulty level same as Bitcoin: same security
- Tx blocks contain payload; generation rate is not limited by PoW (security)
- Ledger creation: pull in all Tx blocks into parent PoW block



Remuneration and Fork Prevention

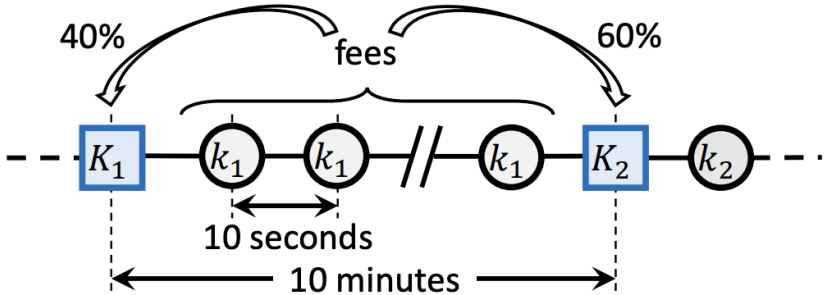


Figure 1: Structure of the Bitcoin-NG chain. Microblocks (circles) are signed with the private key matching the public key in the last key block (squares). Fee is distributed 40% to the leader and 60% to the next one.

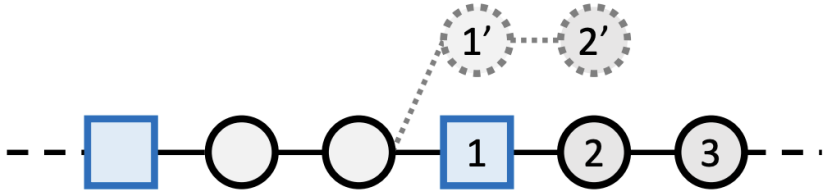


Figure 2: When microblocks are frequent, short forks occur on almost every leader switch.

Bitcoin-NG

- Positive: Throughput is high because Tx blocks are many in number and only limited by network capacity

- Negative: Bitcoin-NG is permissionless but does not have the full security of longest chain protocol
  - **Predictability**

Bribing attack on Bitcoin-NG

On longest chain protocol:

a) There is unpredictability on who successfully mines
b) After mining, the block is sealed by the nonce and cannot be altered

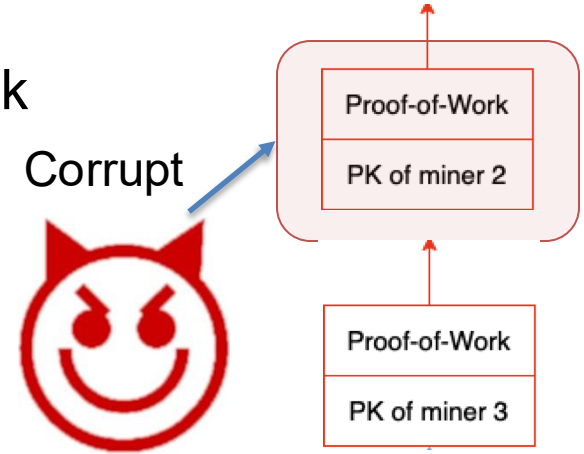
Putting a) & b), Bitcoin is very resistant to bribing attacks

But in Bitcoin-NG, a) & b) are true only for PoW blocks, but not true for Tx blocks

Bribing attack on Bitcoin-NG

- But in Bitcoin-NG, a) & b) are true only for PoW blocks, but not true for Tx blocks

- So Tx blocks are vulnerable to bribing attacks
  - Slow-down attack
  - Not a security attack



Slow-down attack

- A miner publishes a **new key block** → becomes the leader.
  - Their **public key is visible** in the key block.
- An attacker (adaptive adversary) sees the new leader and **immediately targets them**:
  - **DDoS them**
  - Or **physically attack their infrastructure**
  - Or **corrupt them** if possible
- The leader **can't send transaction blocks anymore**.
- No transactions are included until the **next key block is mined**, which could take minutes.

Idea 3: Prism 1.0 or Fruitchains

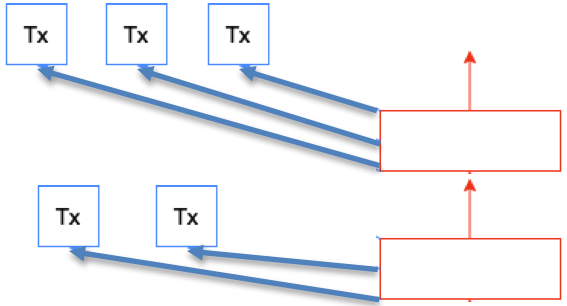
Bitcoin-NG is a good idea: it separated security from payload/data

Prism 1.0 is similar to Bitcoin-NG

- Consist of proposer blocks and transaction blocks

But

- Transaction blocks are not linked but referred by proposer blocks
- The PoW for transaction blocks is easy for throughput
- The PoW for proposer blocks is hard for security



Conclusion

- Bitcoin throughput is limited by mining rate which is limited by security
- GHOST is a different fork choice rule
  - More secure against private attack but vulnerable to balance attacks
- Fruitchains achieves optimal throughput
  - Other graph based schemes, each vulnerable to security attacks

Resources

- ECE/COS 470, Pramod Viswanath, Princeton 2024