Lecture 8.

Scaling Throughput:

4 modules in this course
* roughly 7 lectures each.

1) Bitcoin ← so far.

2) **Scaling Bitcoin** ← improve Bitcoin performance while still retain basic structure of the longest chain protocol

3) Beyond Bitcoin

4) Designs for real world applications.

Performance: 1) Throughput: tx/s

* Bitcoin → 7 tx/s

Ethereum → 100 inst/s.

1) Why is throughput so small in

Bitcoin?

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

β ← fraction of honest hash power.

λ ← mining rate

B ← block size

forking factor = # of blocks mined in parallel.

β ← no control.

λ ← can be controlled by setting target difficulty easy.

B ← can be controlled by allowing more tx in a block, increasing the block size.

Δ ← network delay is proportional to block size B.

So $\text{Throughput} \propto \frac{(1-\beta)\lambda\Delta}{1+(1-\beta)\lambda\Delta}$

So Throughput limited by $\lambda\Delta$.

Recall: Safety holds when:

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

$\frac{(1-\beta)\lambda}{1+(1-\beta)\lambda\Delta}$: longest chain of honest mining growth rate.

$\beta\lambda$: adversarial private chain growth rate

In summary: throughput is limited due to forking (and security).

In this lecture: we study 3 efforts to improve throughput. The first two are

flawed (to different levels) and the third solves the problem. ↑ only the network limits the throughput.

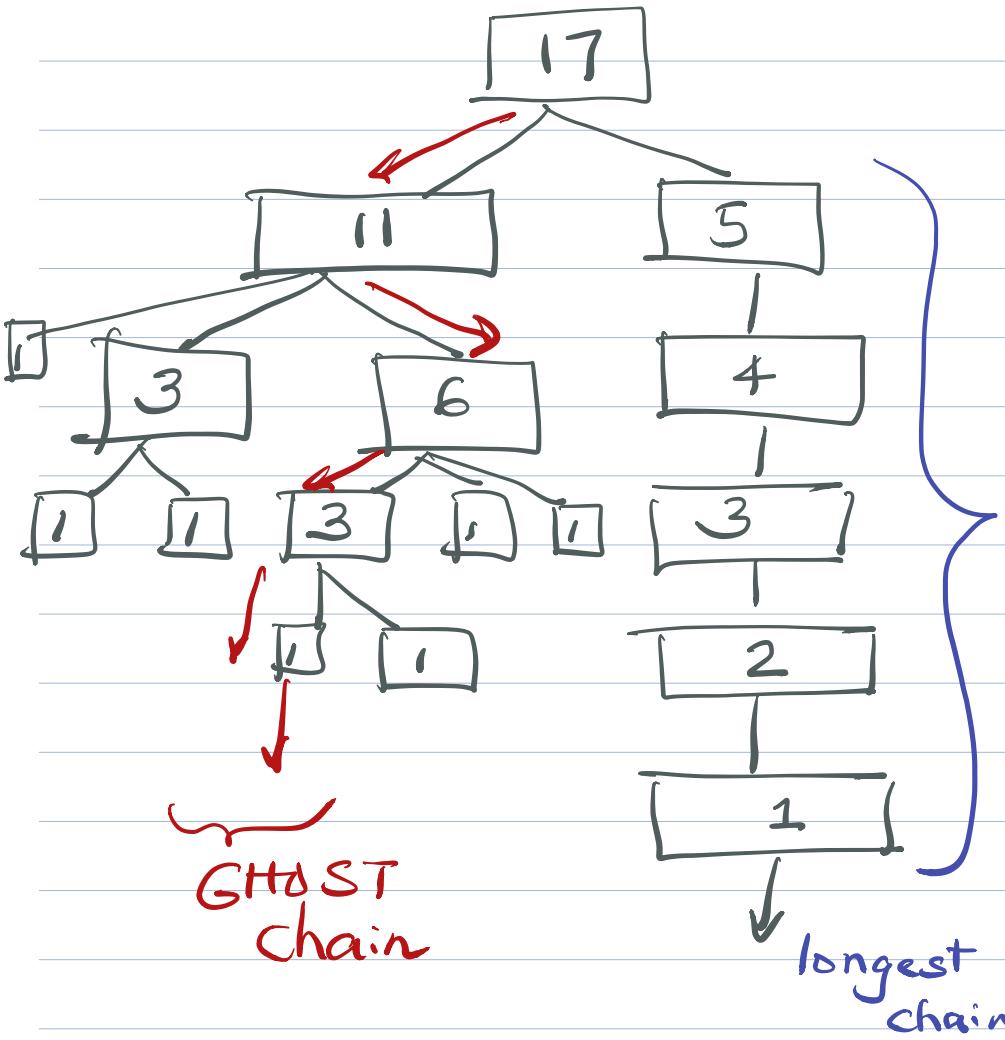
(1) Embrace Forking ← a modification to the mining rule.

GHOST.

no longer mine on the tip of the longest chain

mine on the tip of the GHOST chain.

GHOST: greedy heaviest observable subtree.



The ghost chain is harder to displace by a private attack

- because all the blocks in the sub-tree count; so forking is not wasted.

and hence the mining rate can

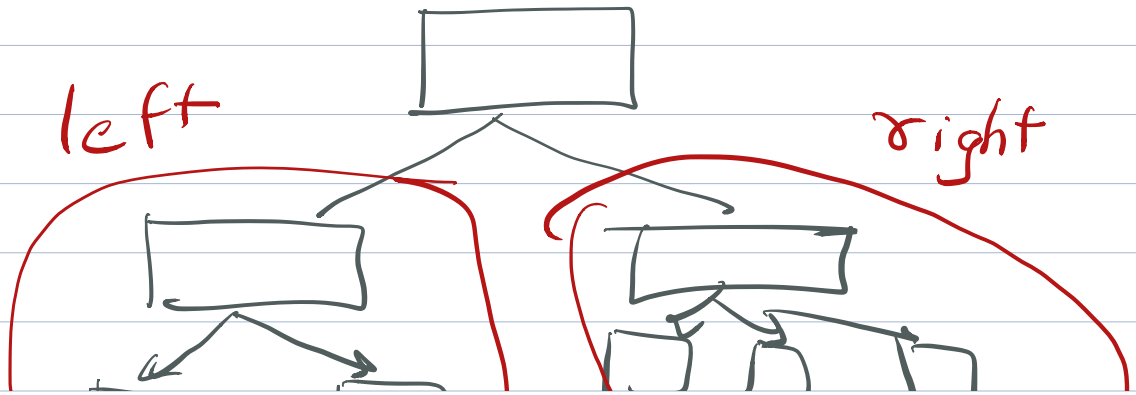
be increased without worrying about forking.

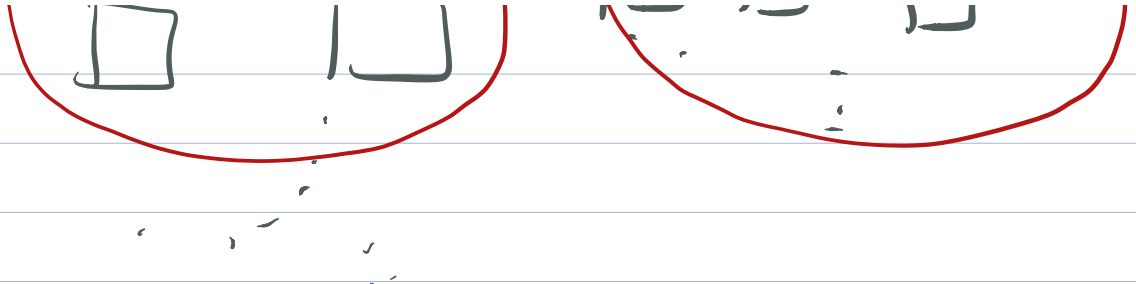
The logic here refers to private attack resistance to

and its also true that the private attack was the worst case attack ← but for the longest chain protocol.

The worst case attack for Ghost rule could be different.

Balance attack: the idea is to have two chains and honest mining is split between them.





adversary's goal is to split the honest mining : half on the left subtree and other half on the right subtree.

adv. mines & releases blocks so that left & right subtrees have equal weight

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 left & right subtrees.

(2) Have no forking or as little

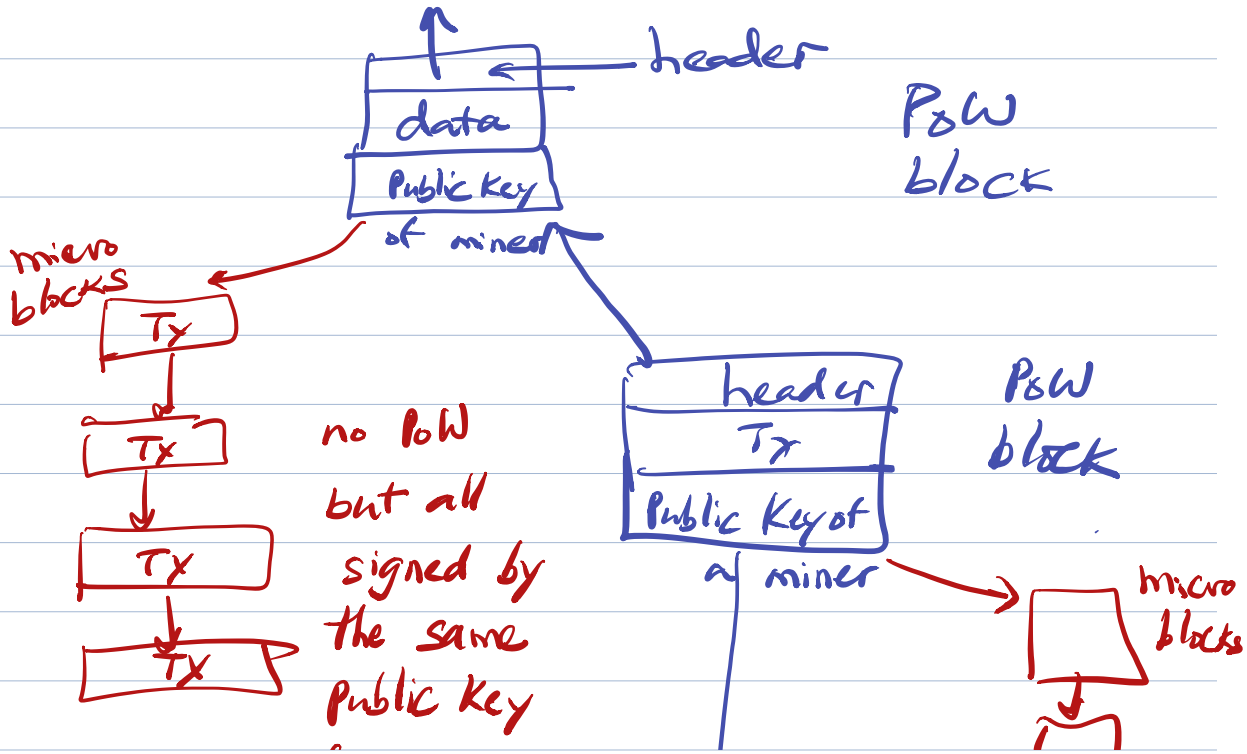
forking as Bitcoin.

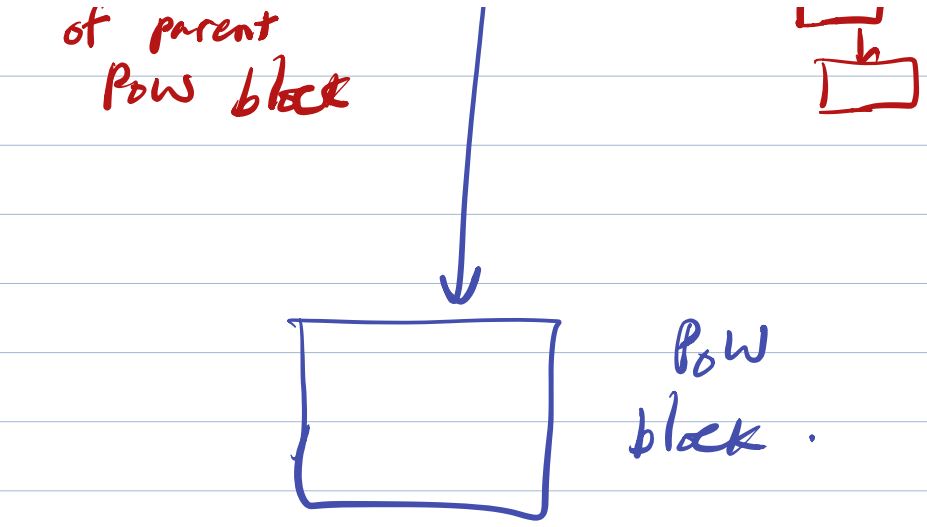
Bitcoin-NG:

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 value of B, block size?





* K-deep rule : PoW blocks

* PoW difficulty level same as Bitcoin ← security same.

* micro blocks contain payload.

* ledger creation: pull in all micro blocks into parent PoW block.

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

Negative: Bitcoin-NG is permissionless but doesn't have all the security of longest chain protocol.

Predictability

In longest chain protocol, there

(1) is utter unpredictability on who successfully mines.

(2) second, after mining, the block is sealed by the nonce and cannot be altered.

Putting (1) & (2) together: Bitcoin is very resistant to bribing attacks.

But in Bitcoin-NG (1) & (2) are true only for PoW blocks

(1) & (2) are NOT true for micro blocks.

So Micro-blocks are vulnerable to bribing attacks.

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

(3) Prism. (1.0)

* Similar to Bitcoin-NG
  Two types of blocks

  (Porposer blocks & Tx blocks)

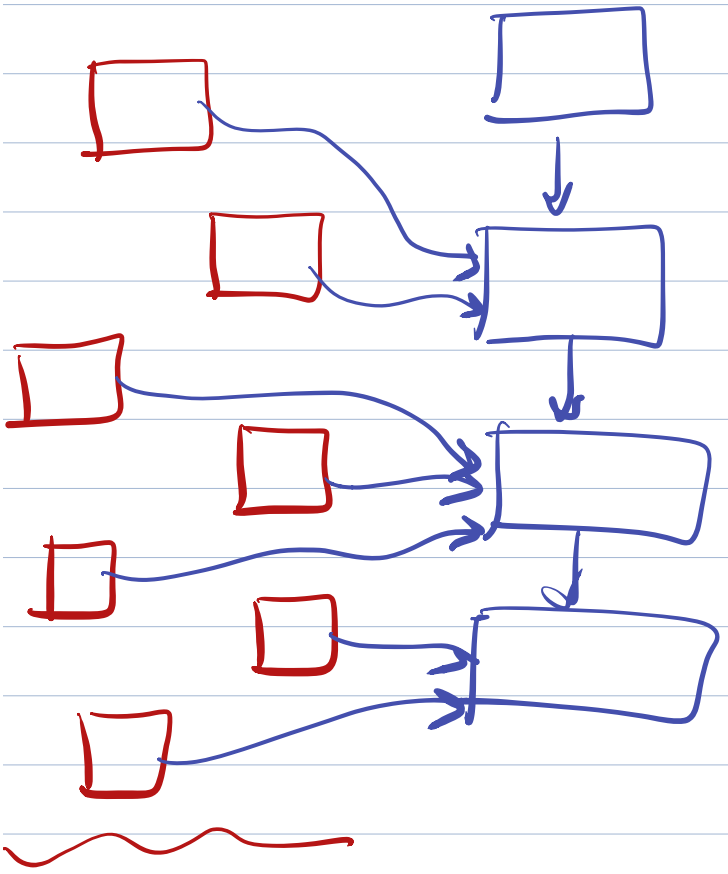
  Porposer blocks ↑ similar to PoW blocks.

  Tx blocks ↑ similar to micro blocks

* But both blocks go through common PoW frame work.

no chaining

Tx blocks



Poopasa blocks

(chained)

mined slowly for security

mined fast as fast as n/w supports.