Advanced Scaling

Bitcoin-NG and Sharding

Leander Jehl

Bitcoin NG

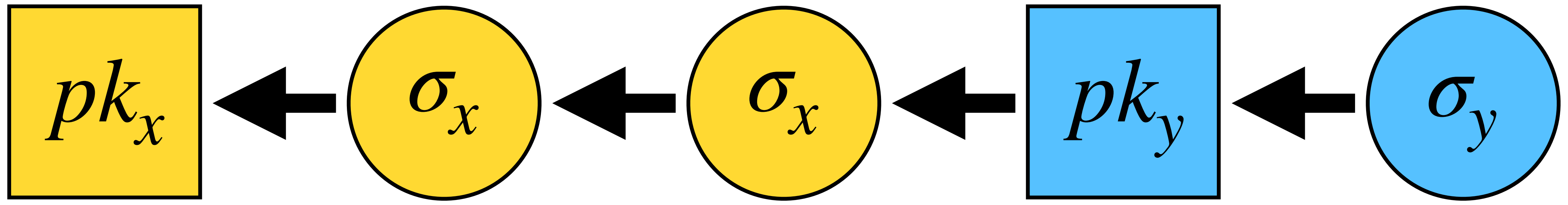
Keyblocks and microblocks

Bitcoin NG

Keyblocks and microblocks

Keyblocks: Include a PoW. *No transactions*, a public key and the hash of the last Key- or Microblock

Microblocks: Include transactions, *no PoW*, and a signature matching the key of the last keyblock.



Longest chain rule: Look only at Keyblocks

Bitcoin NG

Advantages

Can adjust frequency of microblocks and keyblocks independently.

Bitcoin NG

Advantages

Can adjust frequency of microblocks and keyblocks independently.

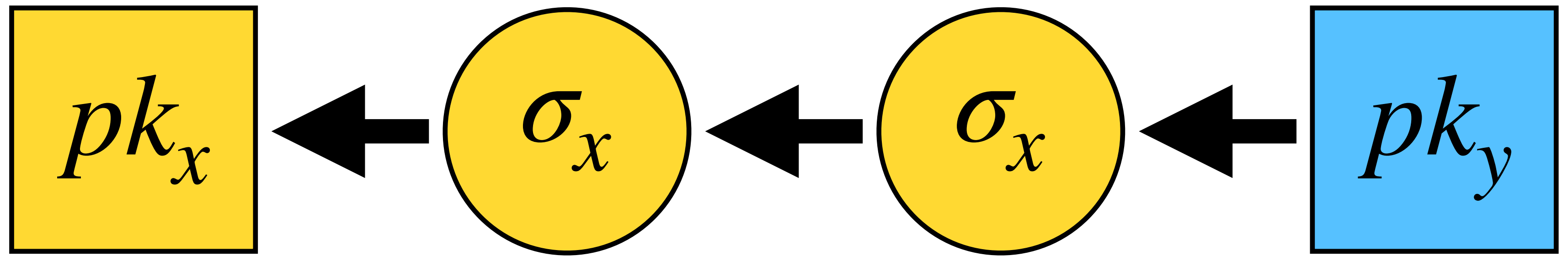
Throughput and latency: Can issue microblocks frequent, which give high throughput.

Security: Slow keyblocks give good security (few forks).

Bitcoin NG

Incentives

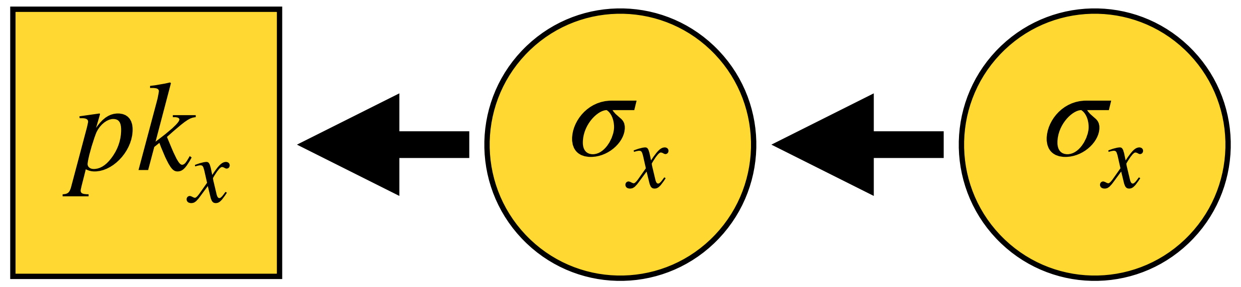
Need to devide block reward (fees) for microblocks between current and next issuer/leader



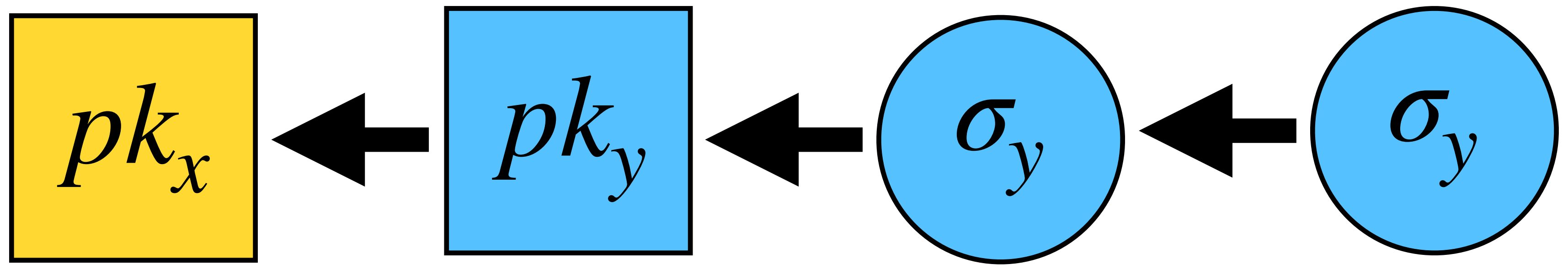
Solution: 40% to pk_x and 60% to pk_y

Bitcoin NG

Incentives - possible attacks

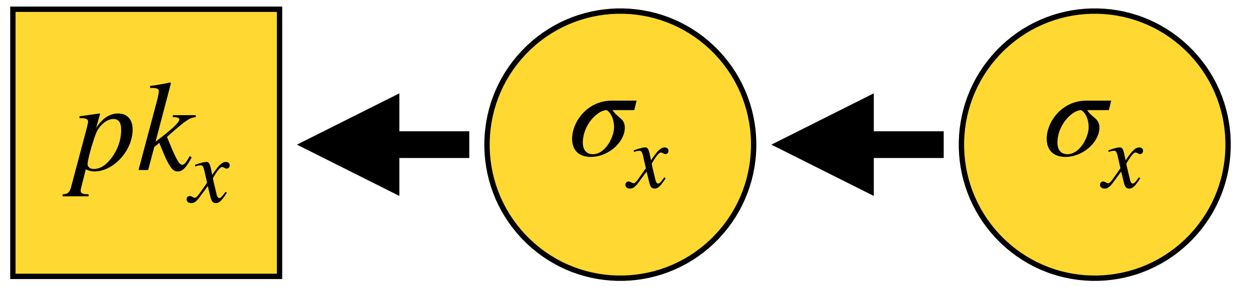


- Steal microblocks:

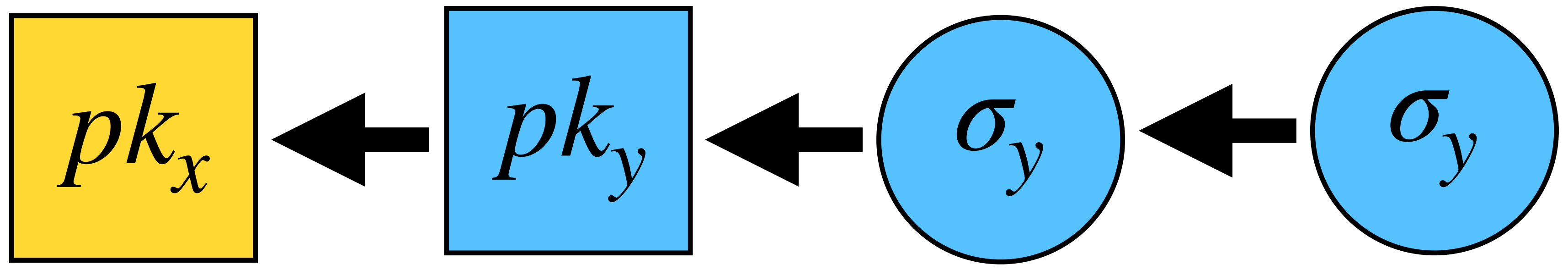


Bitcoin NG

Incentives - possible attacks



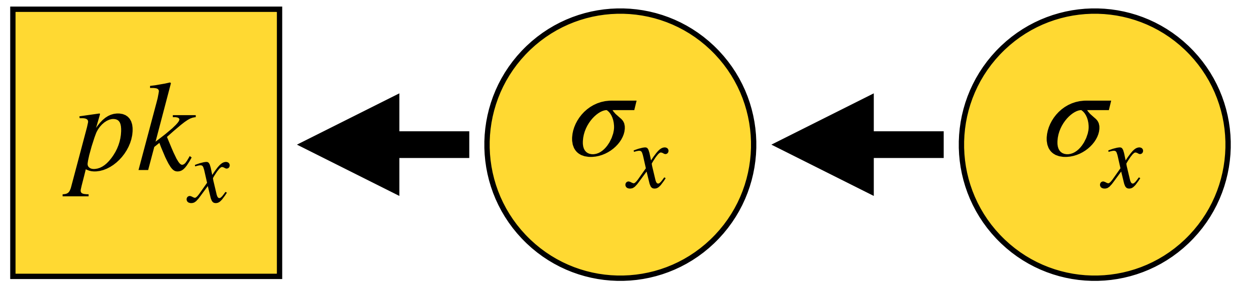
- Steal microblocks:



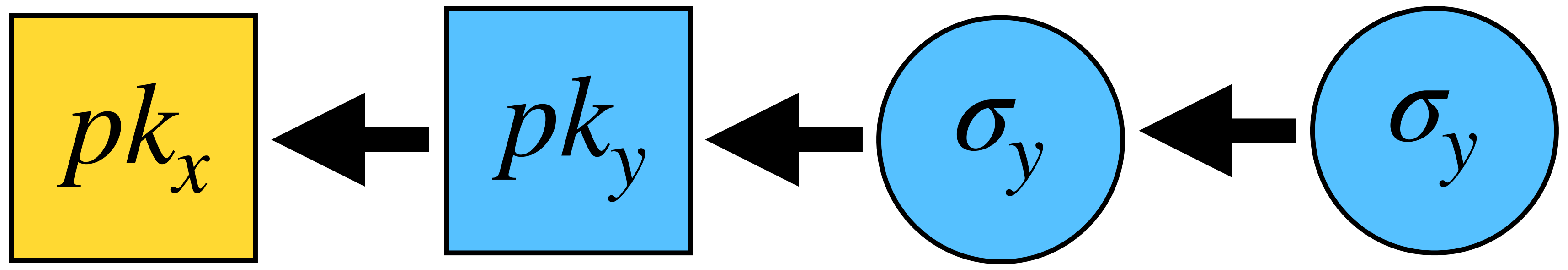
Big enough reward for next leader!

Bitcoin NG

Incentives - possible attacks

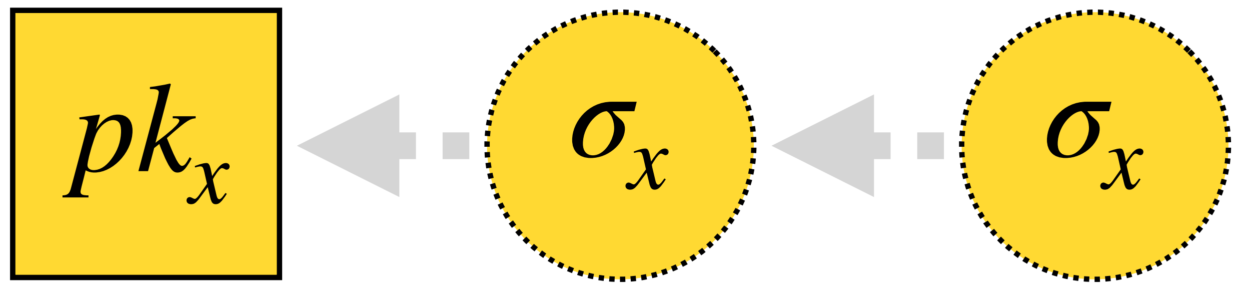


- Steal microblocks:



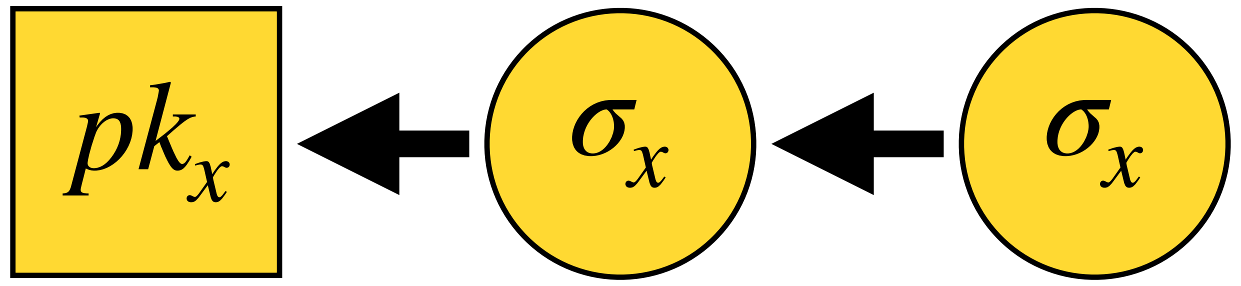
Big enough reward for next leader!

- Selfish mining: Secret microblocks

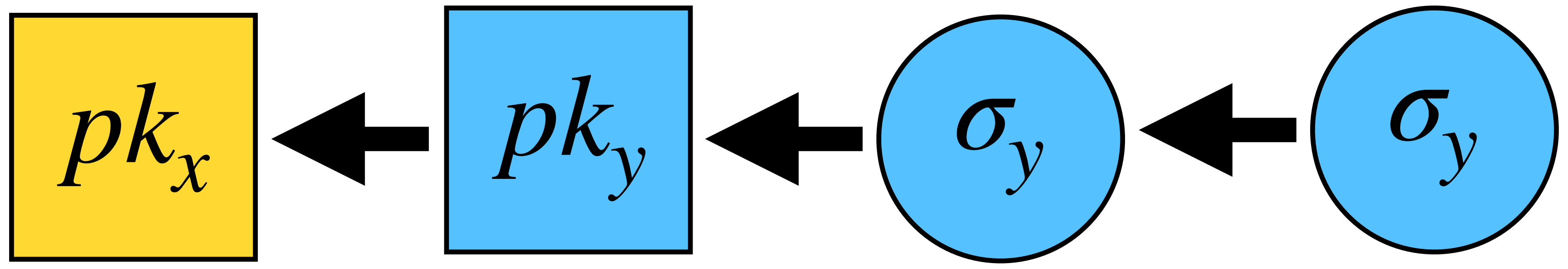


Bitcoin NG

Incentives - possible attacks

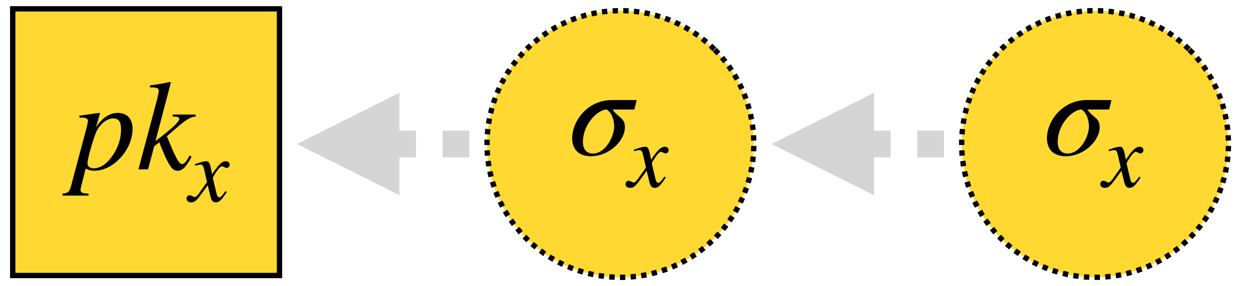


- Steal microblocks:



Big enough reward for next leader!

- Selfish mining: Secret microblocks



Big enough reward for previous leader!

Bitcoin NG

Problems

Bitcoin NG

Problems

If leader fails, no transactions.

Allow DDOS attacks on leader.

Sharding

Sharding

Ideas and potential

Shard:

Potential:

Sharding

Ideas and potential

Shard: Subsystem with a fraction of the state, processing transactions on this part of the state.

Potential: Scale throughput linearly with the number of shards.

Sharding

Problems

Sharding

Problems

A. **How to distribute state?**

B. **How to process transactions across shards?**

C. **How to avoid mining power dillusion?**
Easier to attack a single shard than the complete system.

Sharding

Solutions

A. **How to distribute state?**

- Consistent hashing.

B. **How to process transactions across shards?**

- Atomic commit?

C. **How to avoid mining power dillusion?**

- Disallow choosing, e.g. consistent hashing (difficult).
- Allow multiple shards as in Monoxide (will there be sharding?)

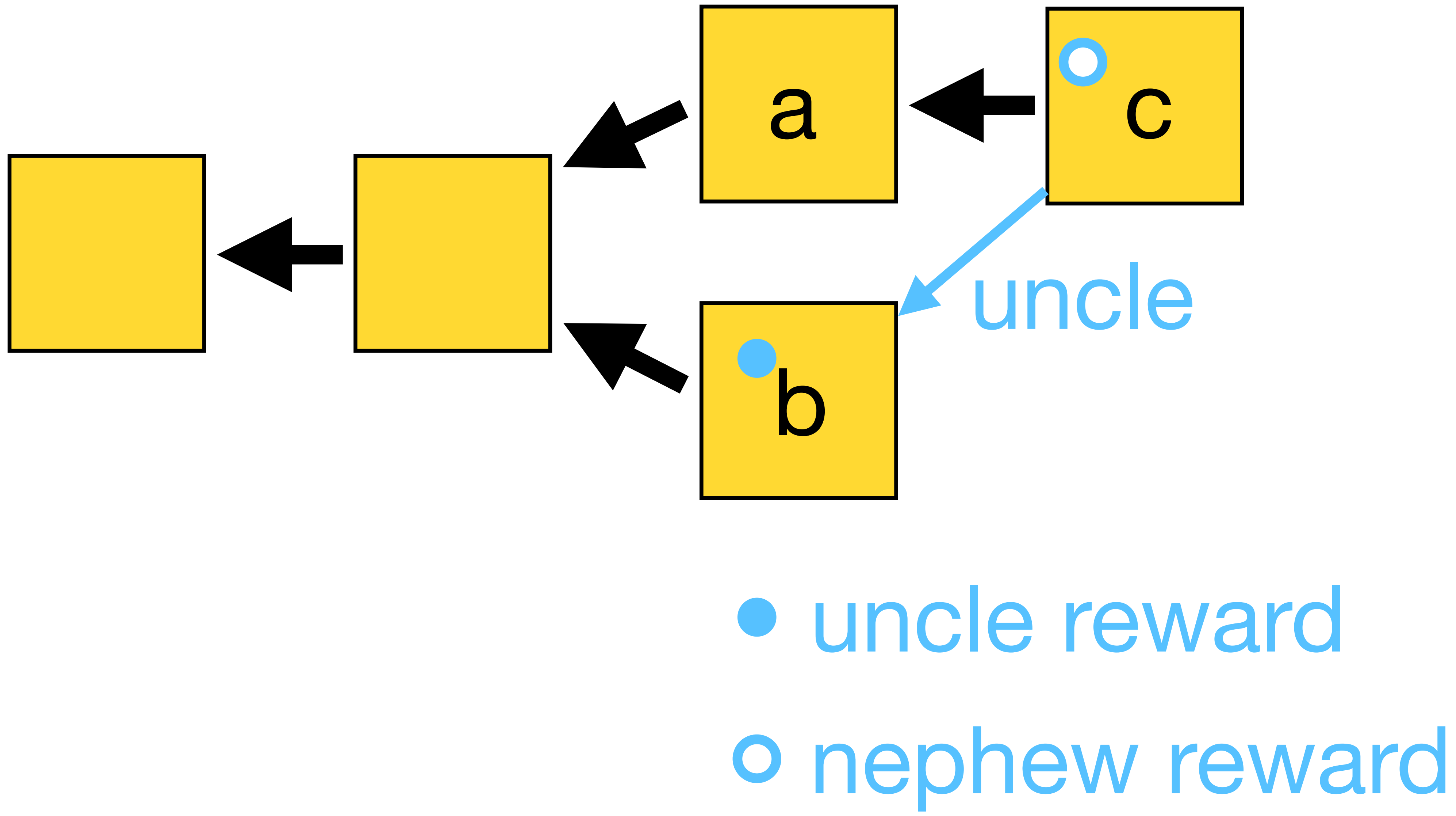
Sharding

Uncles and sharding

Can executed transactions from uncles:

- Transactions in b, that are not in a, can be executed together with block c.

Not done in Ethereum!


a
c
uncle
b
● uncle reward
○ nephew reward