DoS Attacks in the Age of Blockchain

Alberto Sonnino

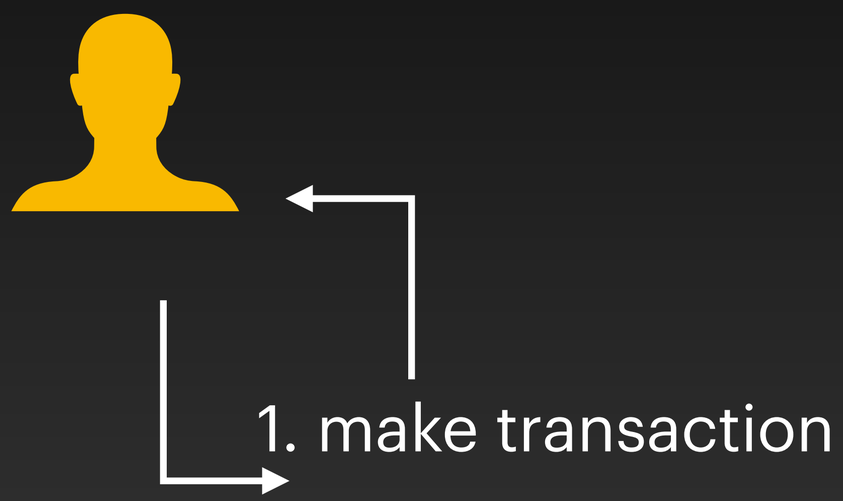
This talk shows the problems

- DoS attacks are vastly ignored in the blockchain community
- A tour of blockchain (consensus) protocols
- Highlights general DoS weaknesses of blockchains
- Not a novelty per se but opportunities to provide DoS protections
- Blockchains present unique DoS challenges
- How SCION-like architecture fit in

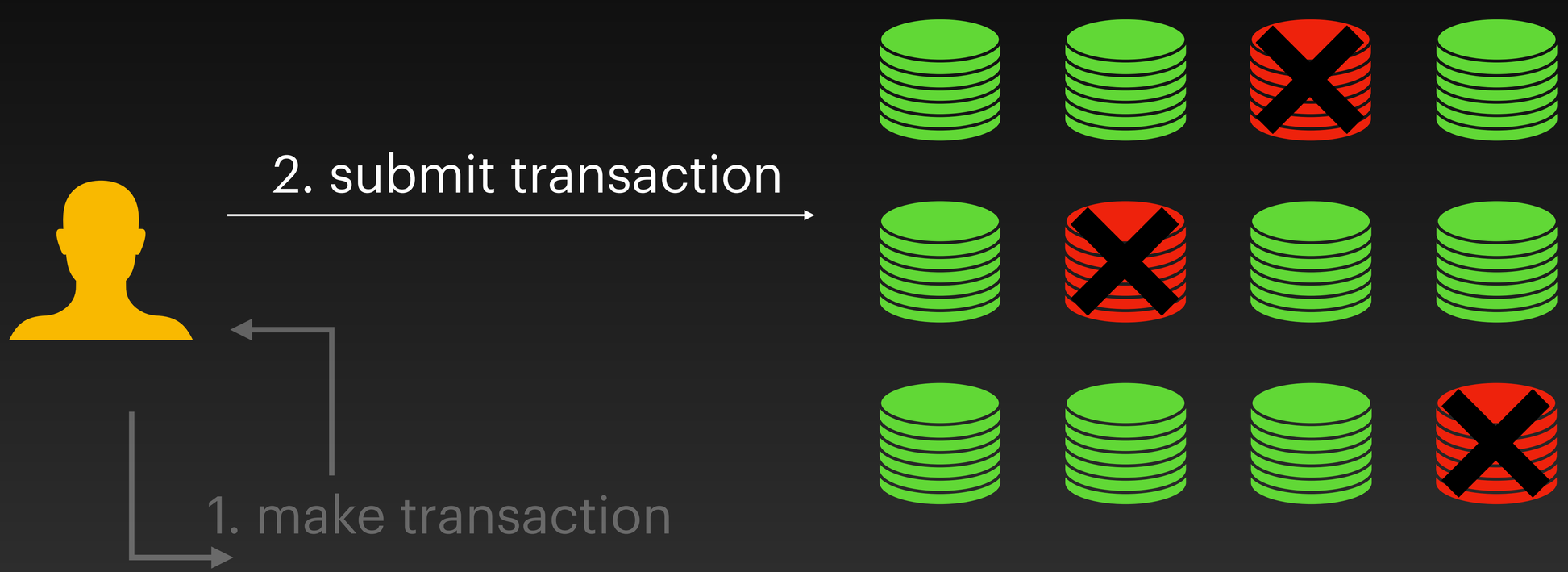
Blockchains

Blockchains

Blockchains

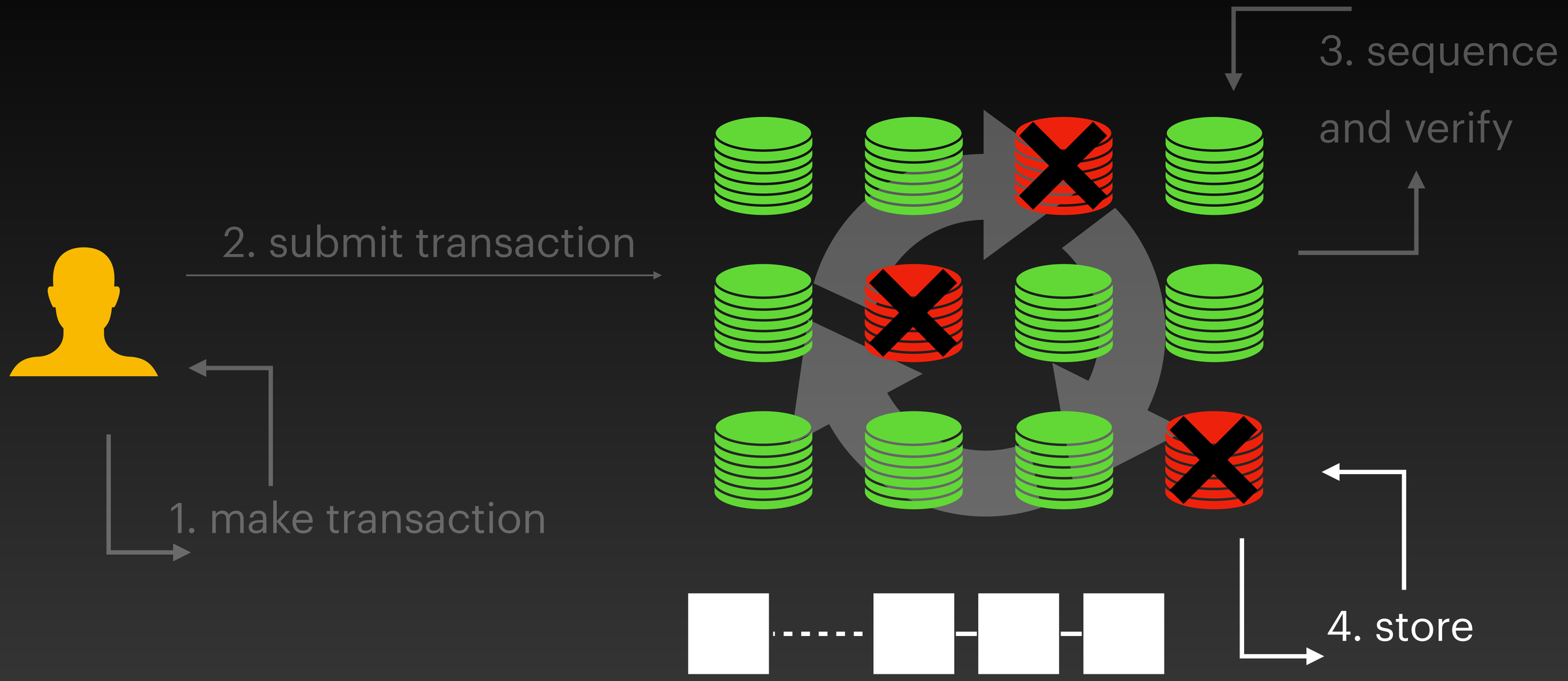


Blockchains

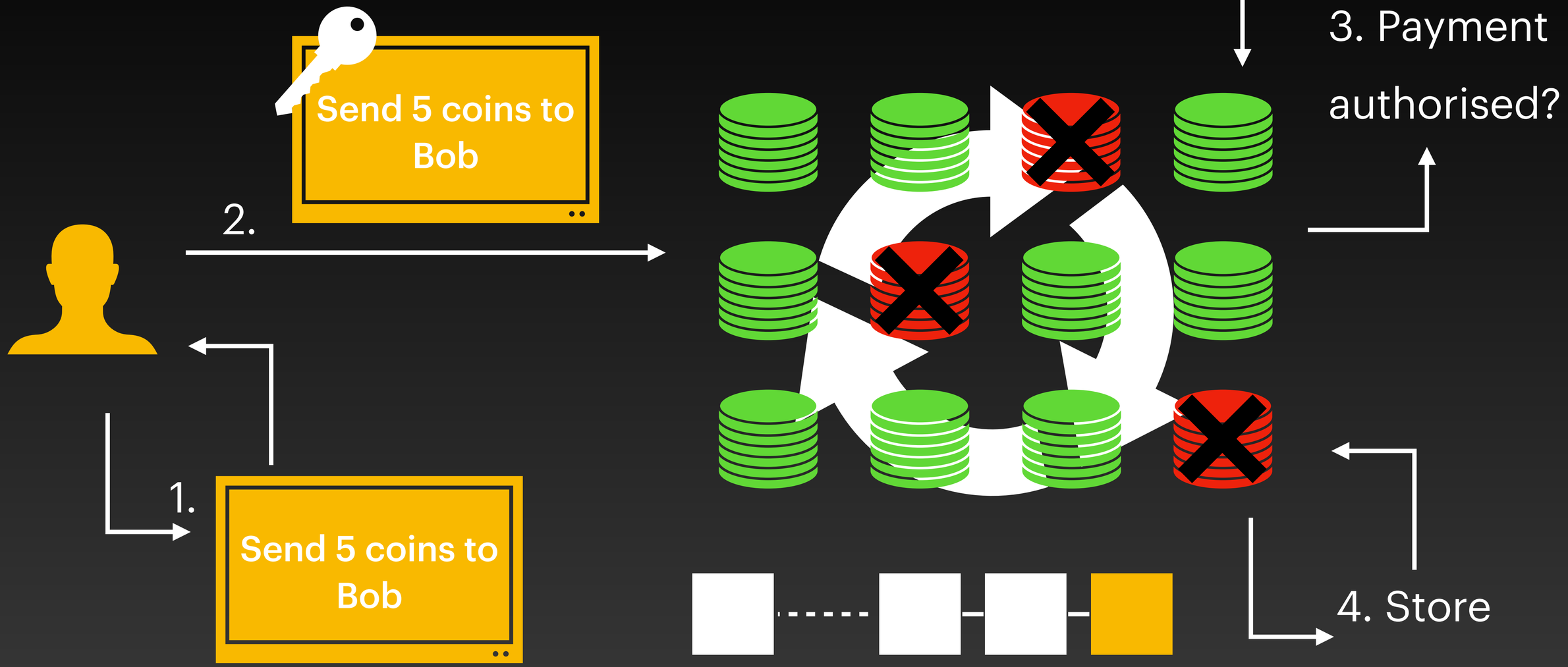


Blockchains

Blockchains



Blockchains

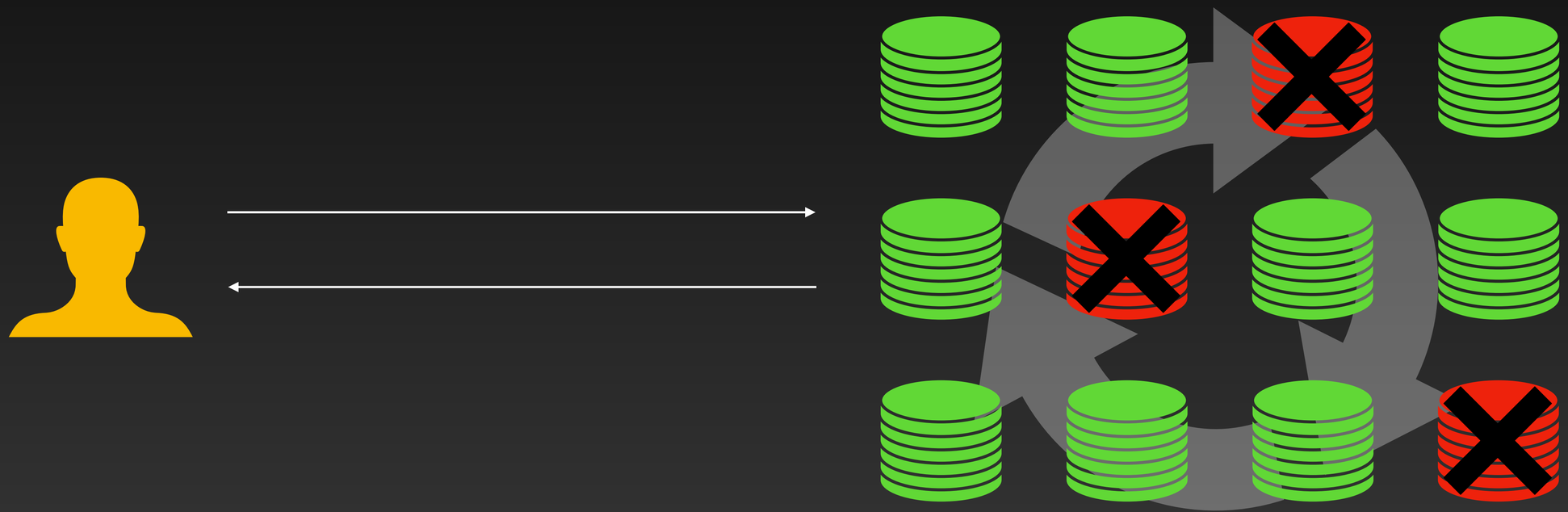


Blockchain
Properties (informal)

- Safety -> No double spend, transactions are totally ordered
- Liveness -> The protocol (eventually) makes progress

Blockchain

Attack Surface: Client <-> Node

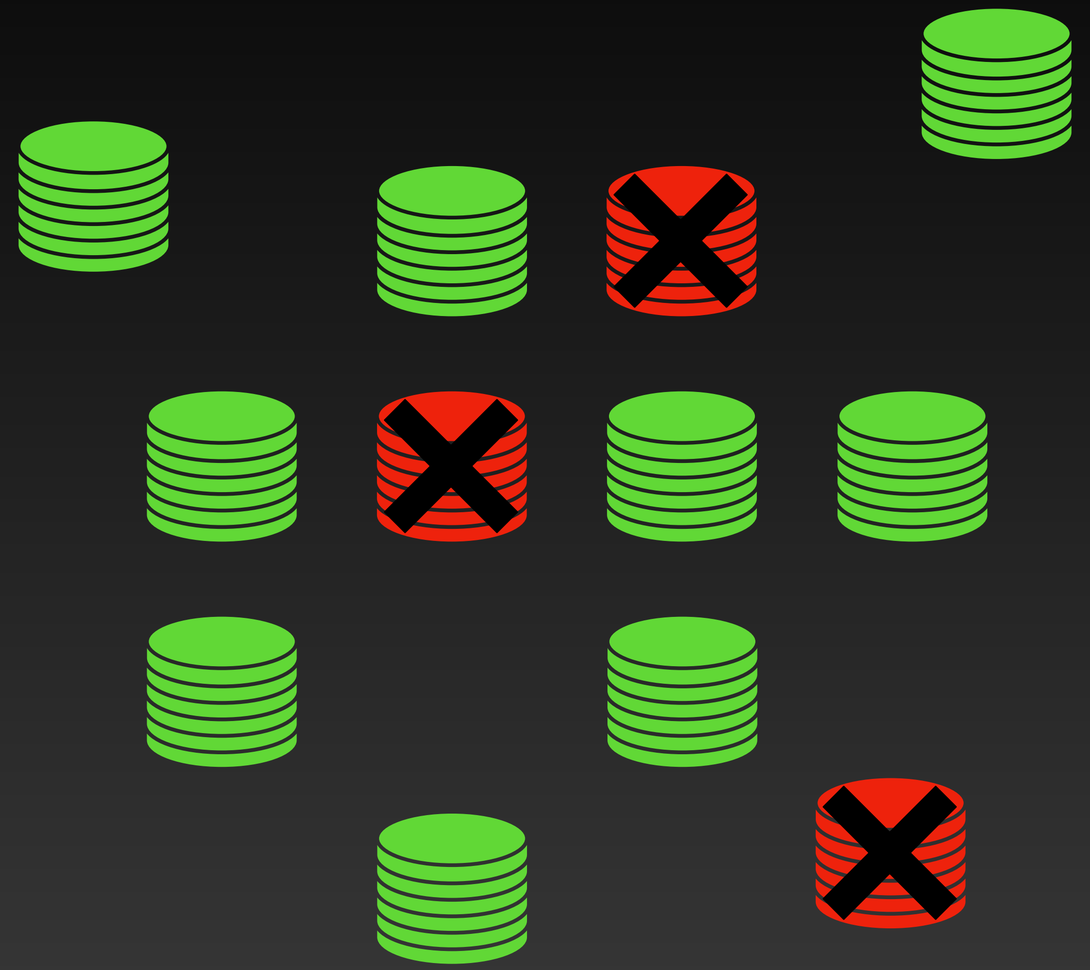


Blockchain

Attack Surface: Node <-> Node

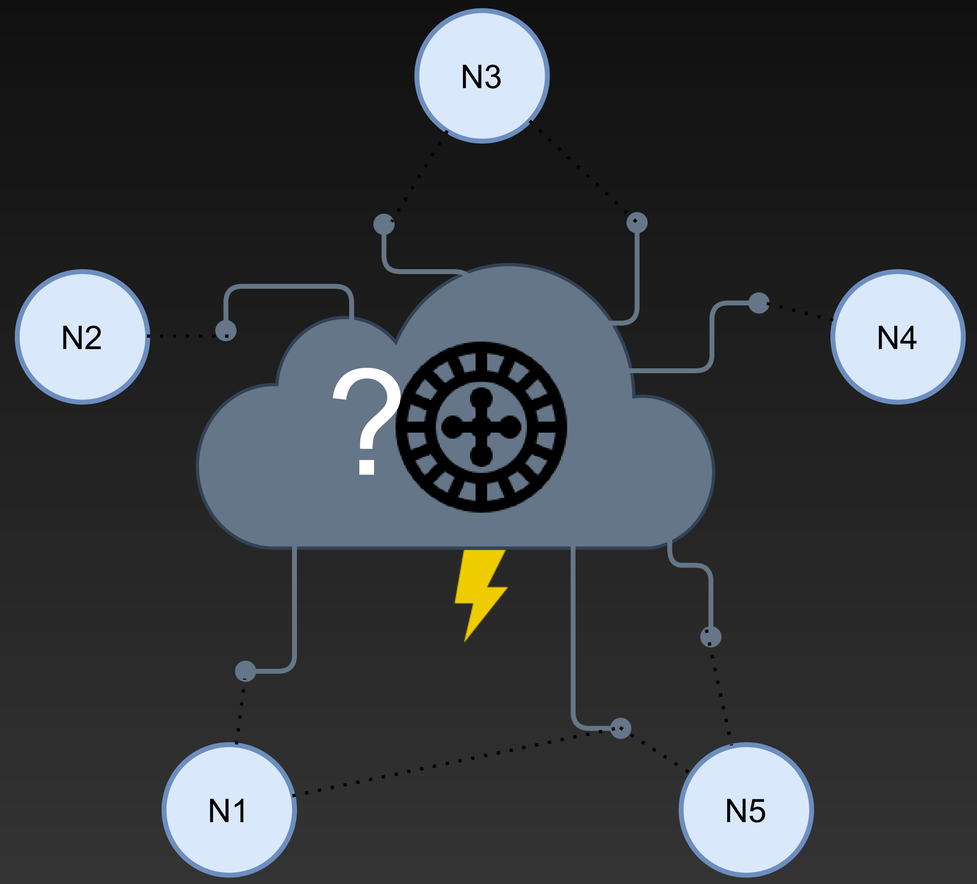
Challenges

- No fixed identity
- Nodes join and leave at will (permissionless) or frequently (quorum-based)
- Run by different entities connected via the internet
- Leased lines / private WAN solutions very costly and inflexible



Challenges

- Neglected threats:
  - DDoS
  - Outages
  - Routing hijacks

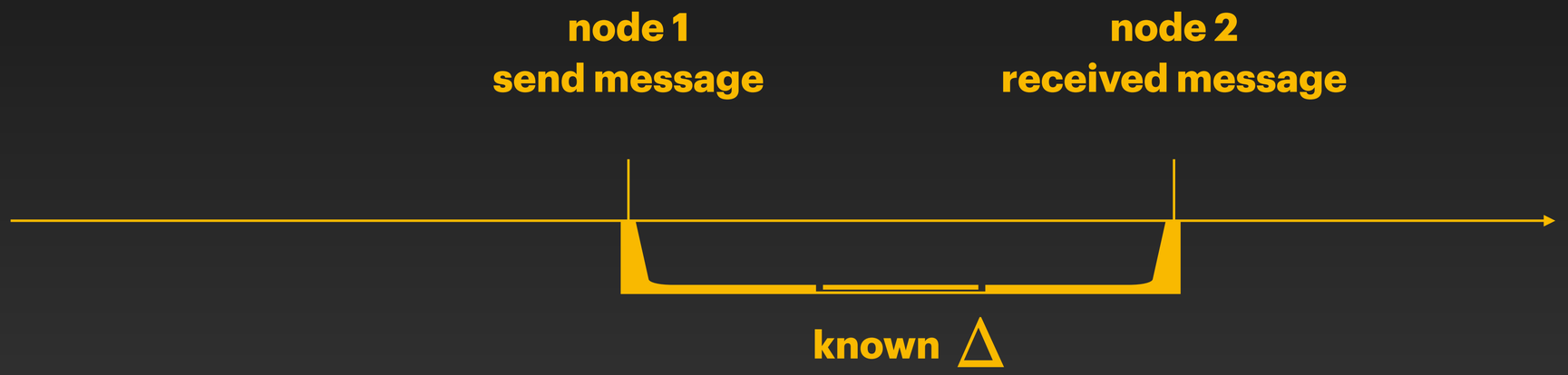


[from ETH Zurich]

Network Model

Sync | Partial-Sync | Async

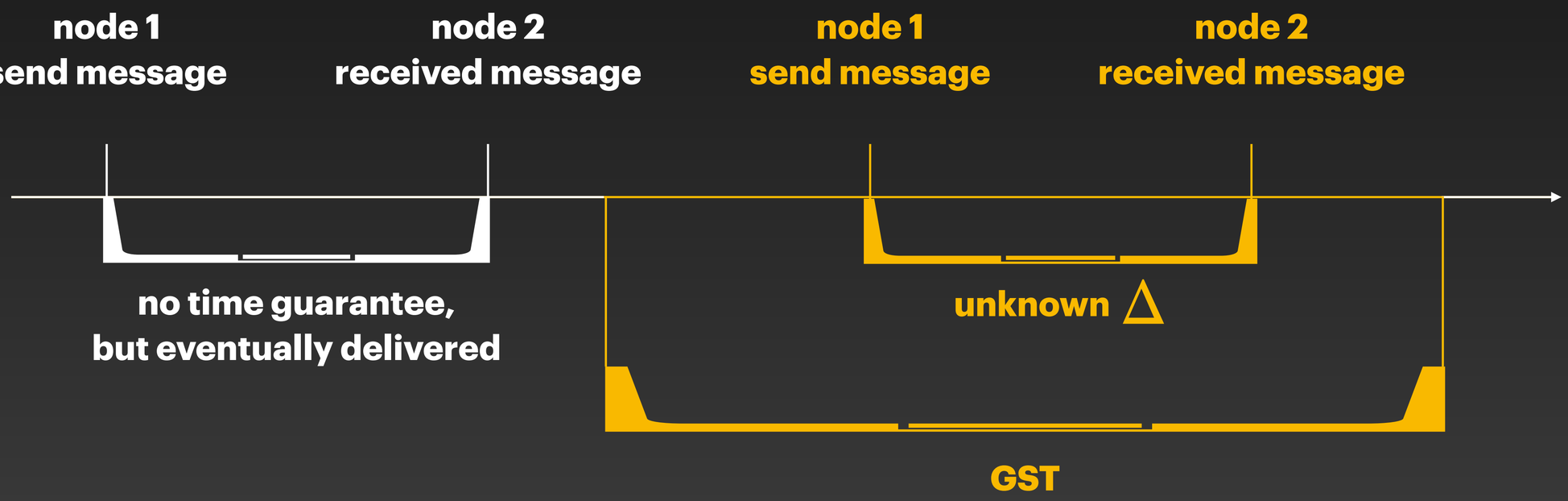
- Synchronous



Network Model

Sync | Partial-Sync | Async

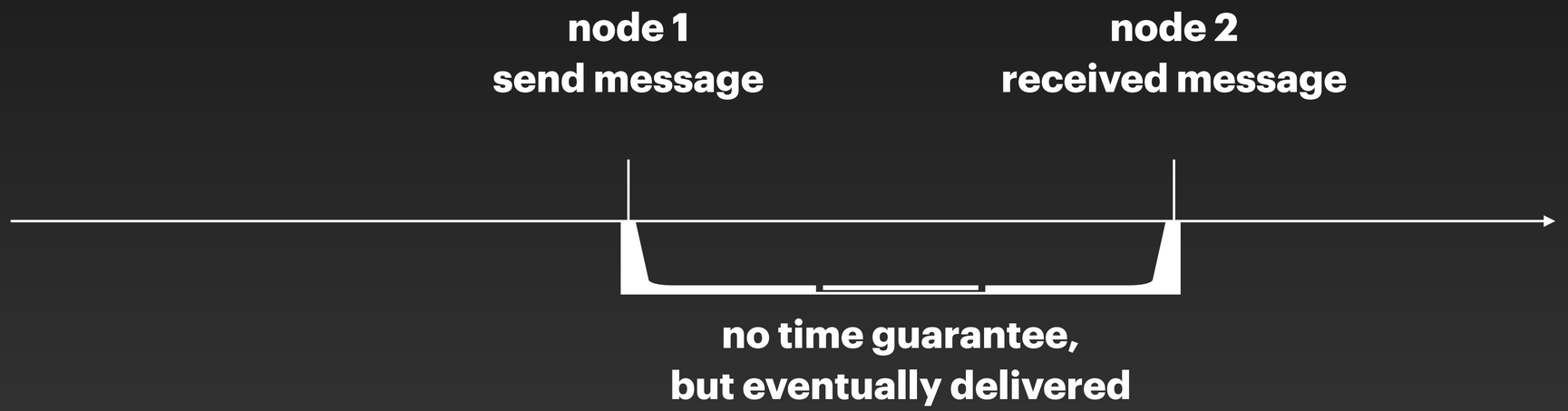
- Partially Synchronous



Network Model

Sync | Partial-Sync | Async

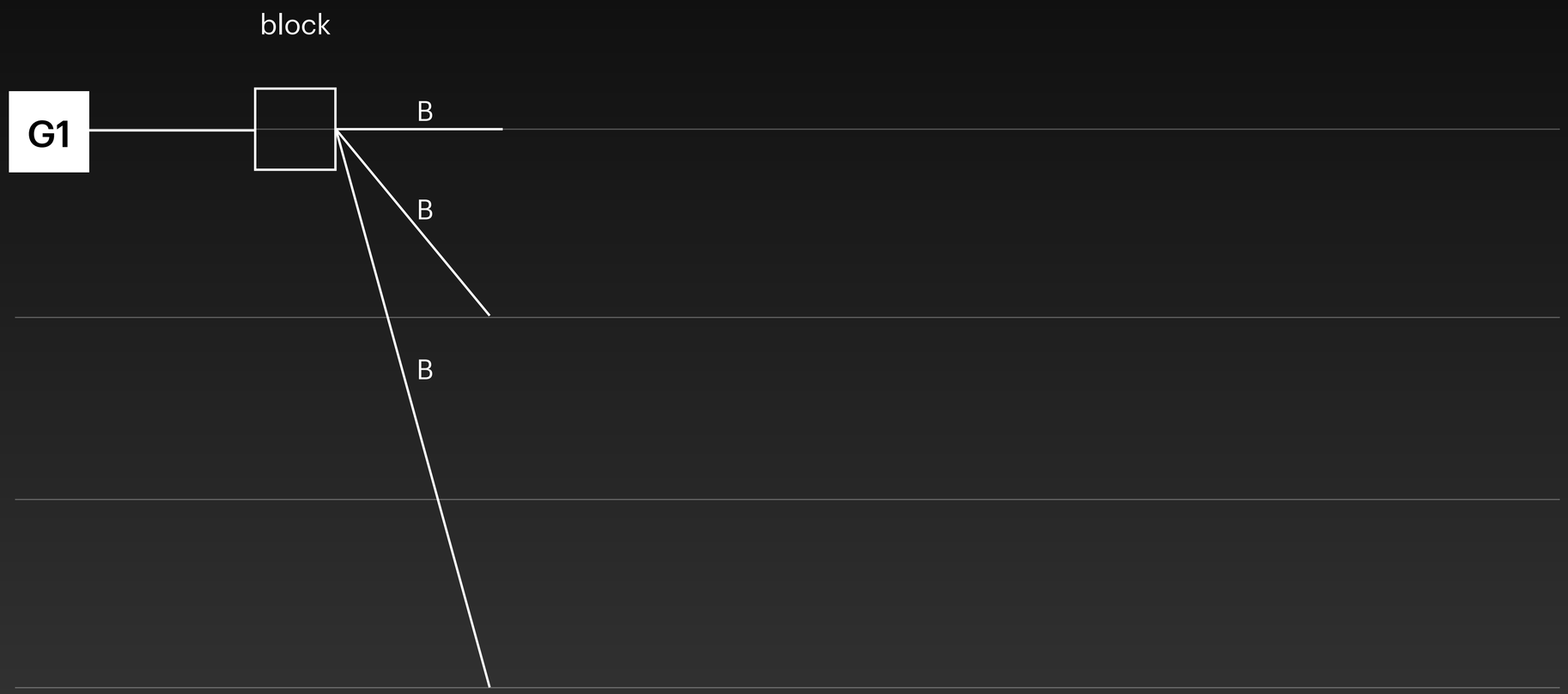
- Asynchronous



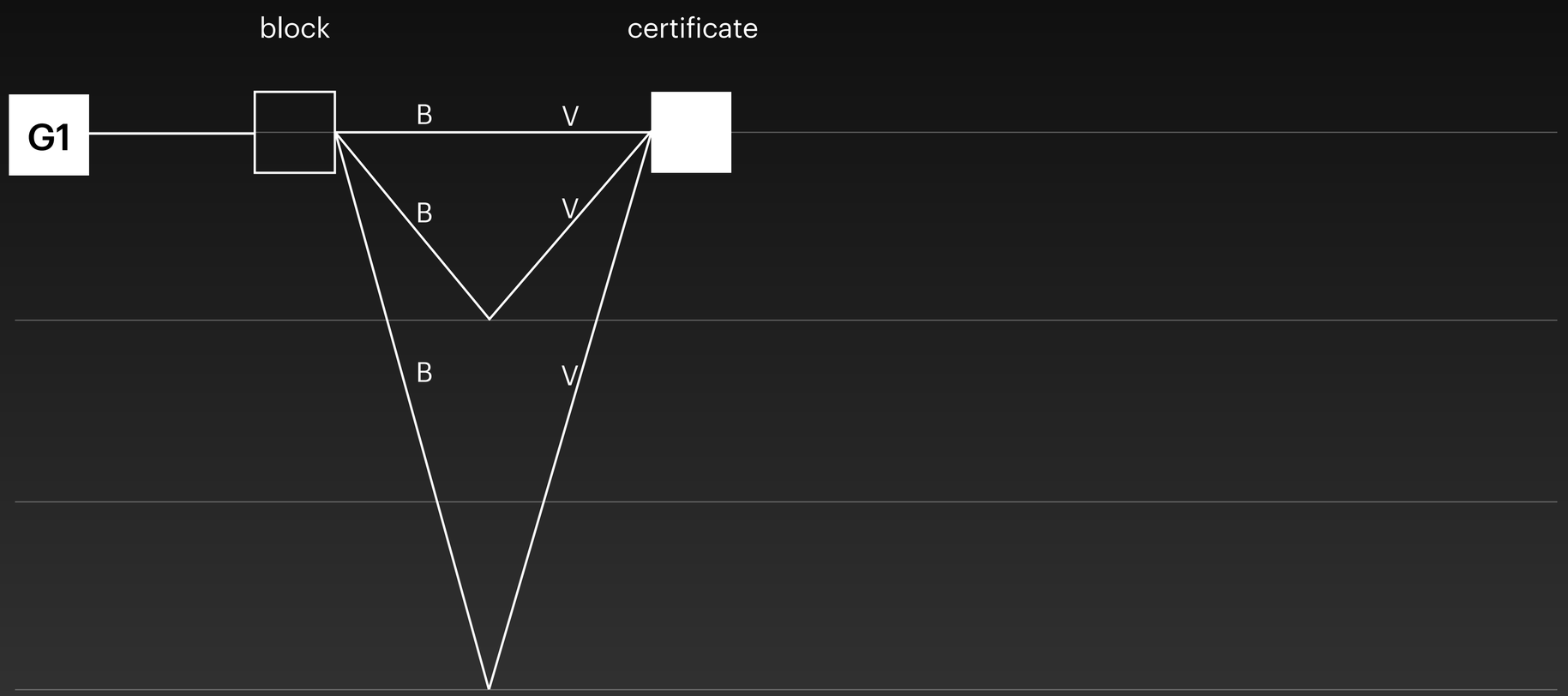
Leader-Based Protocols

- LibraBFT / DiemBFT
- Tendermint
- PBFT

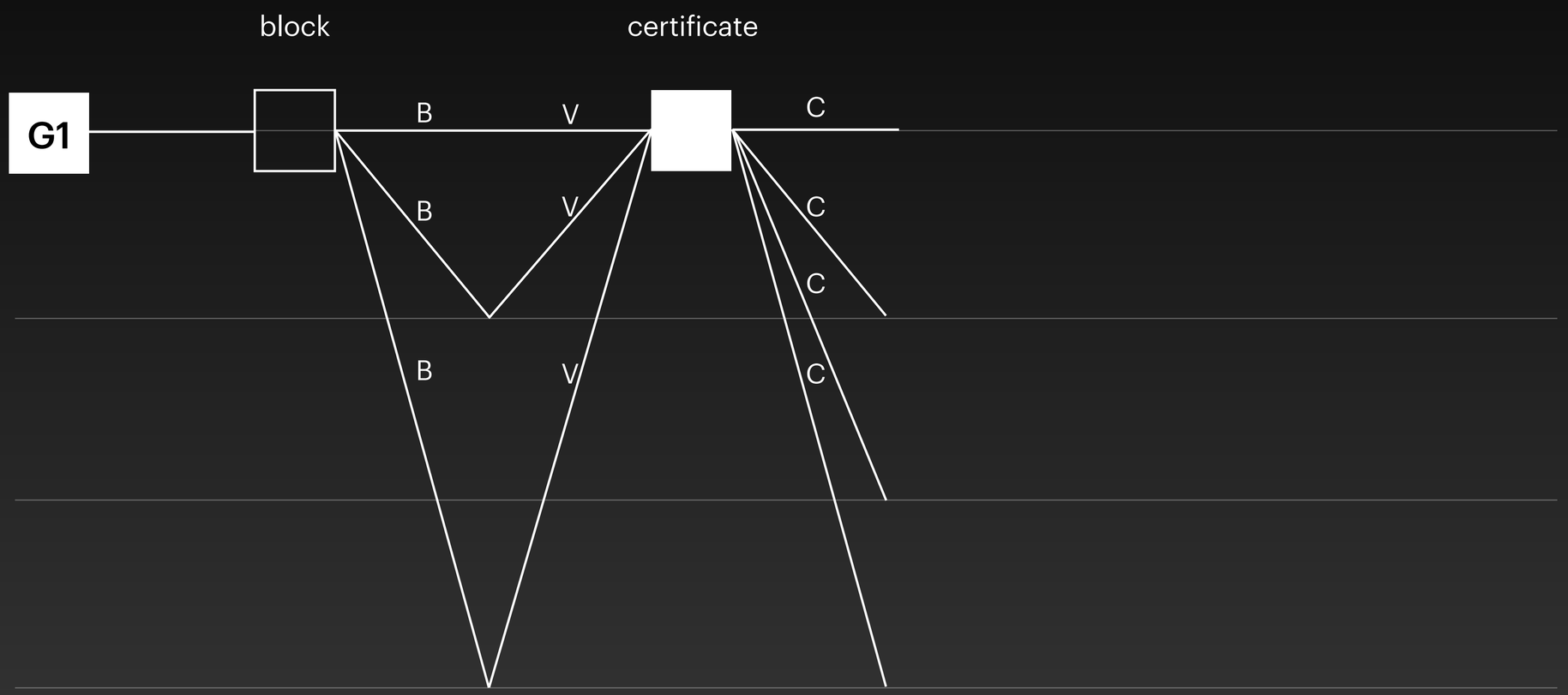
Leader-Based Protocols



Leader-Based Protocols

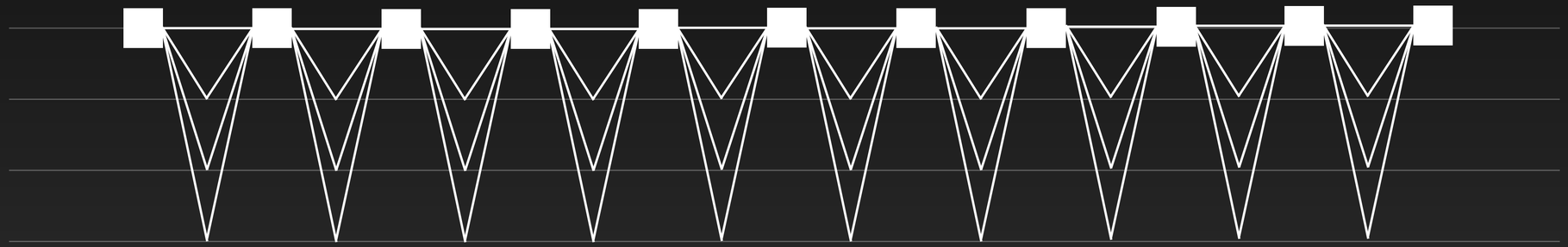


Leader-Based Protocols



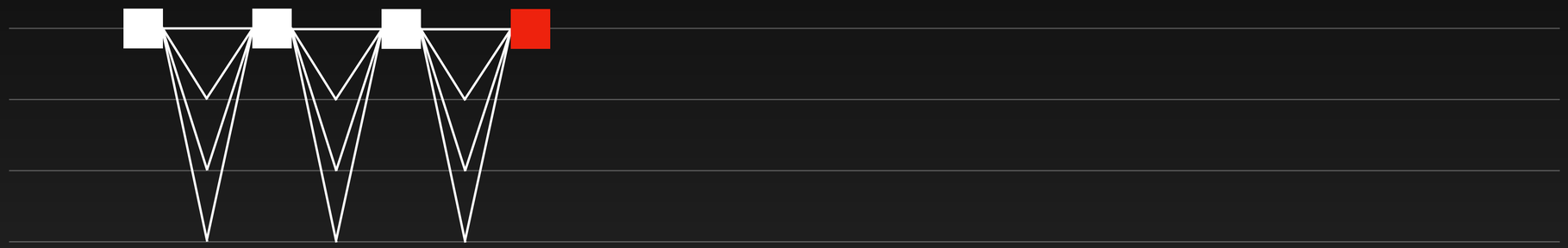
Leader-Based Protocols

Typical pattern



Leader-Based Protocols

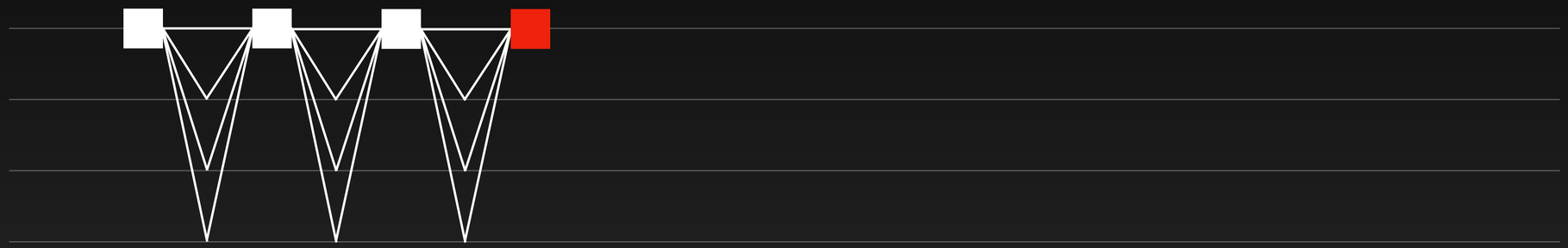
If the leader fail?



- Wait for a timer (5 - 30 sec)
- Complex view-change protocol
- Start over with a new leader

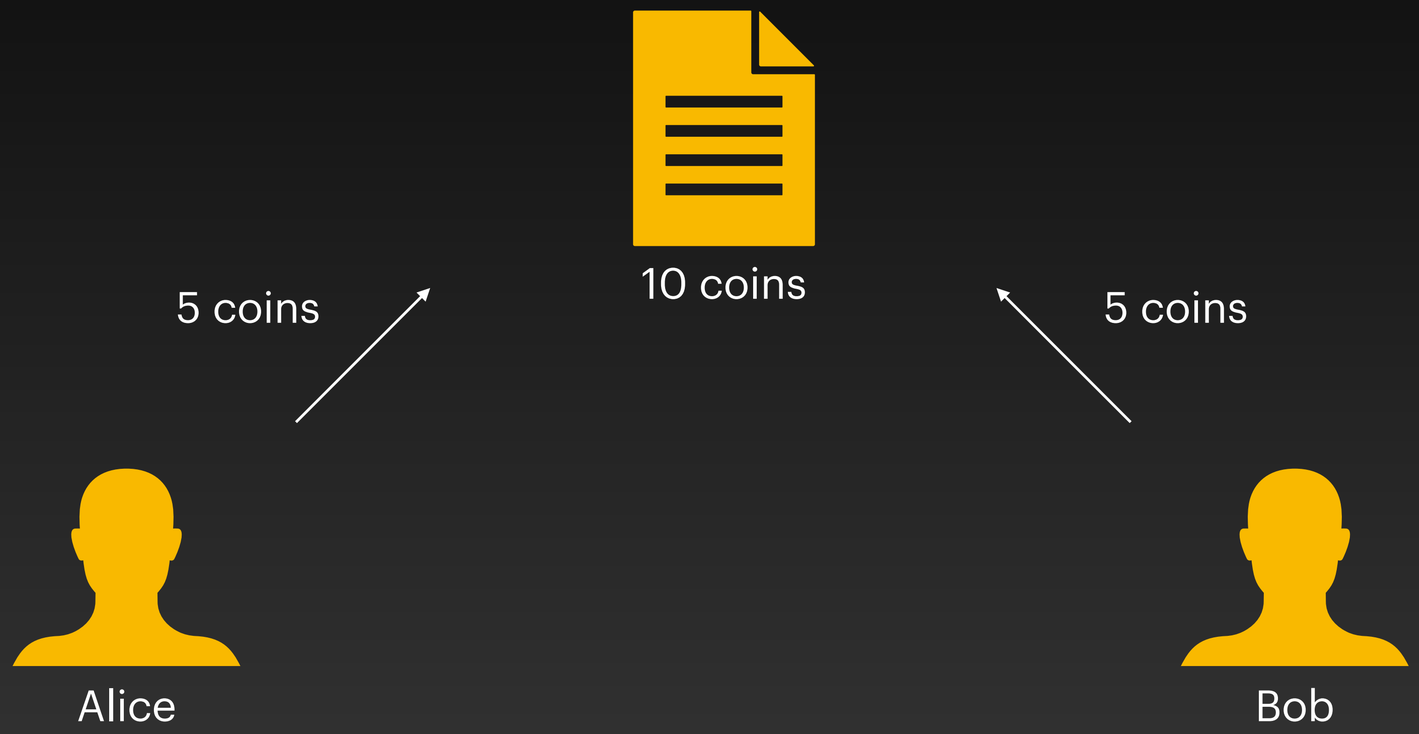
Leader-Based Protocols

If the leader fail?



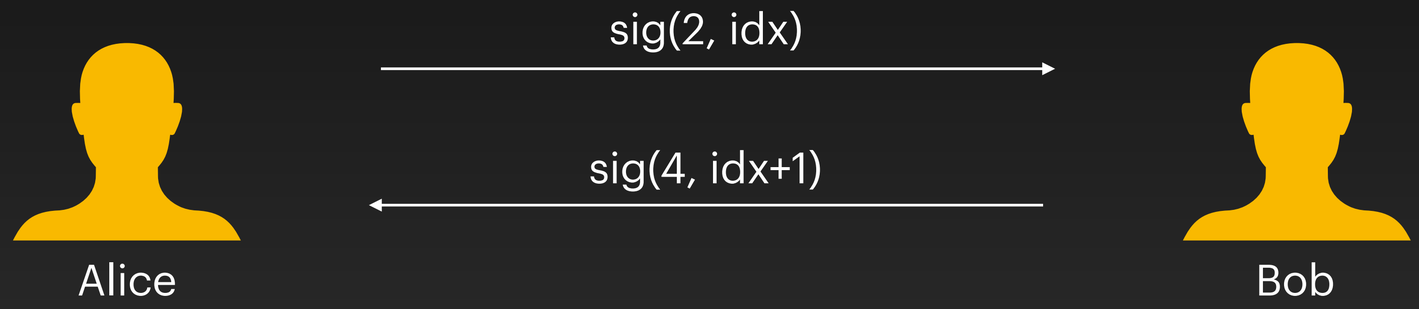
- Problem: DoS on node <-> node links
- Safety attack (double-spend) if synchronous protocol
- Liveness attack (never commit) if partially-synchronous protocol

Side Chains
Lock Fundings



Side Chains

Off-chain Transfers



Side Chains

Settle

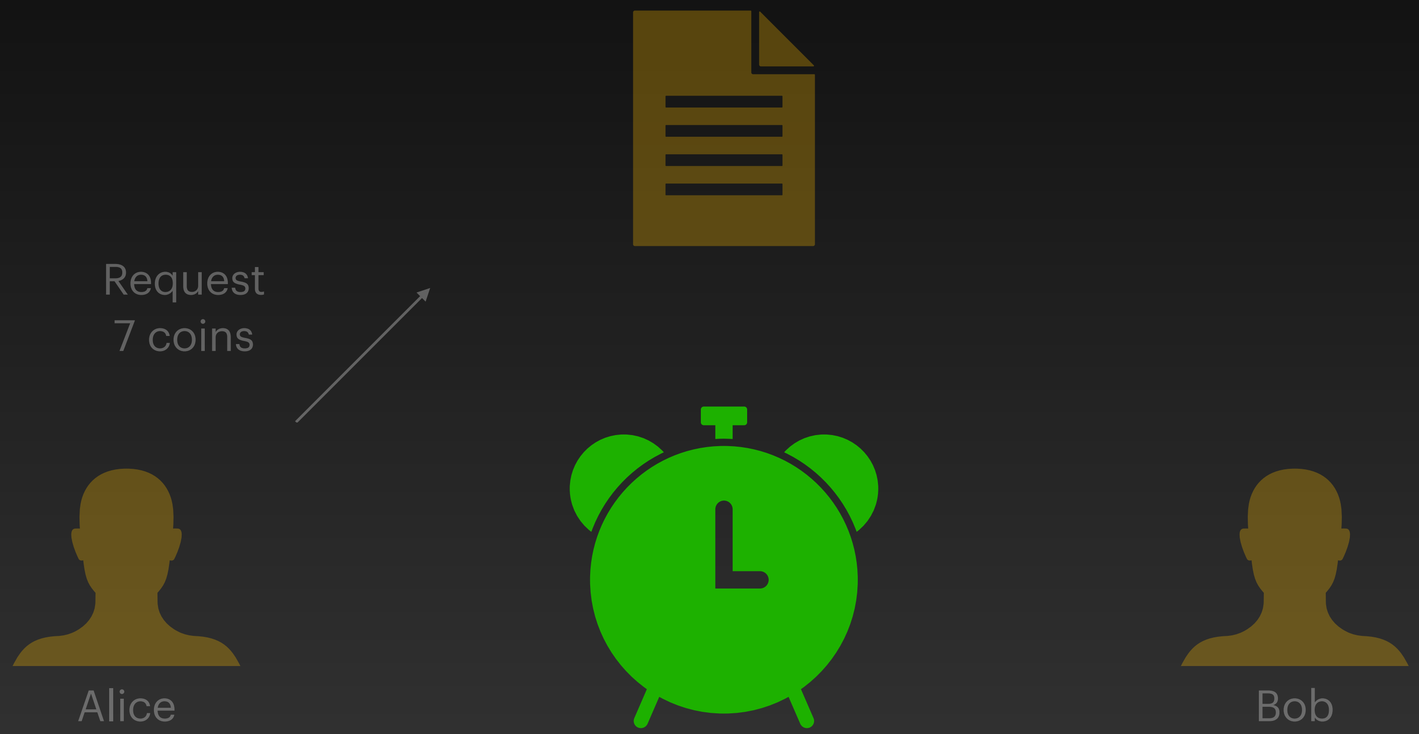
Request
7 coins

Alice

Bob

Side Chains

Settle



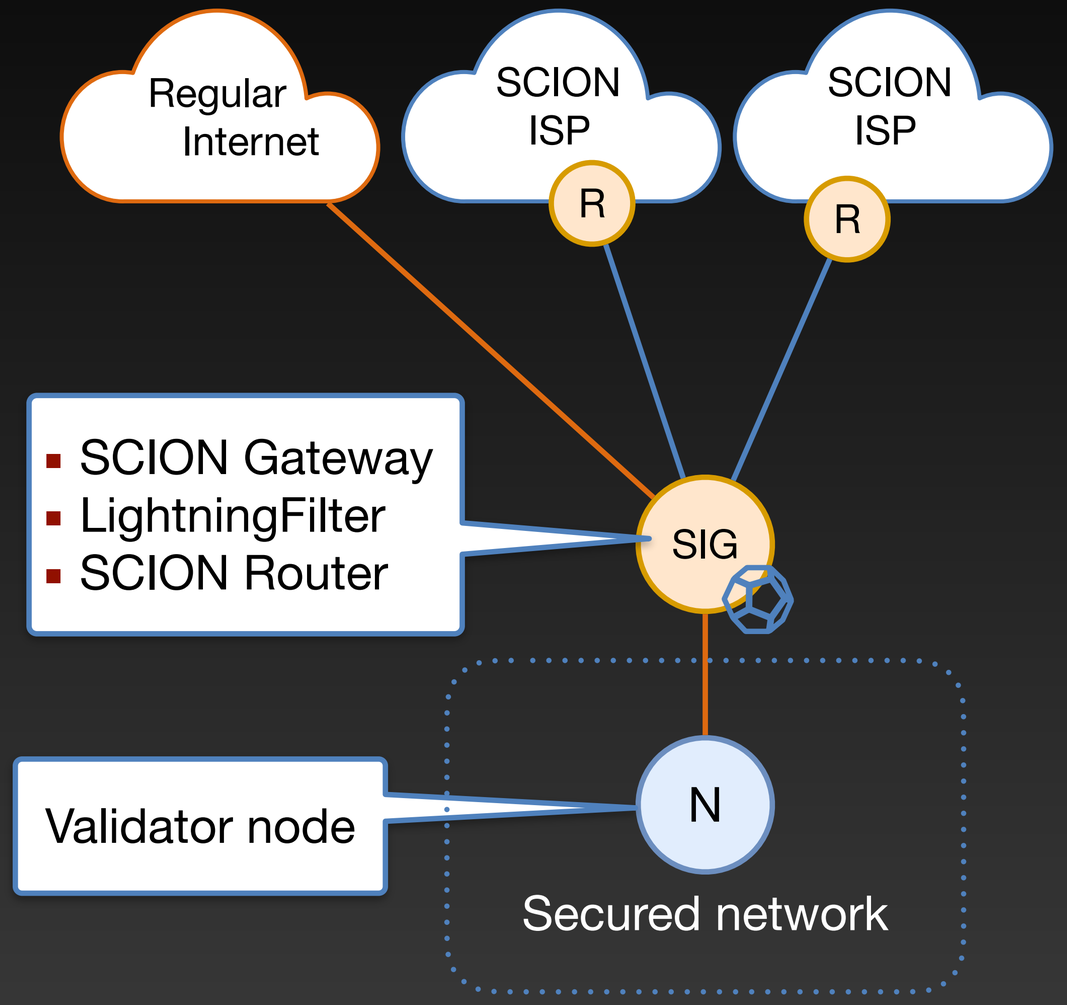
Side Chains

- Problem: DoS on client <-> node
- Synchronous protocols
- If Bob is under DoS and misses the deadline, Alice can lies and steal coins
- Only in Lightning Network: 140,000,000 USD

SCION

Improve Security

- Nodes communicate over IP & SCION
- Communication between SCION nodes with strong guarantees
  - Packet authentication
  - DDoS resilience
  - Internet fault-independence
- No upgrades to the consensus protocol

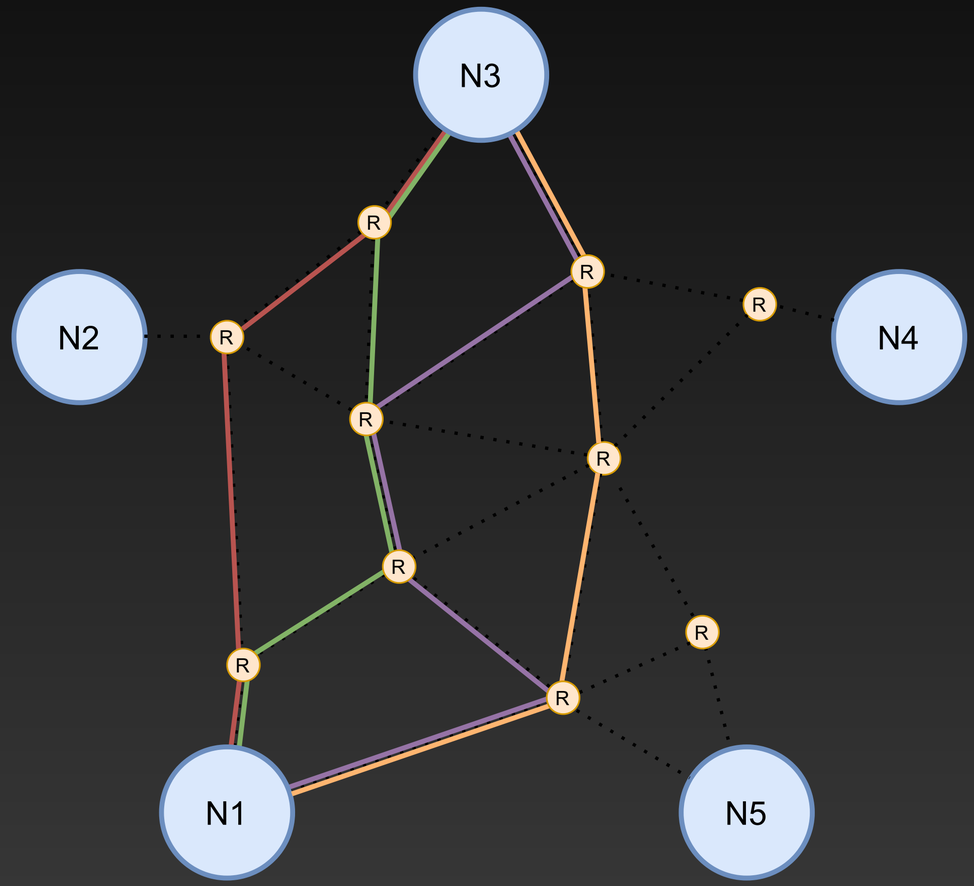


[from ETH Zurich]

SCION

Improve Performance under Attack

- High availability, secure against DDoS and routing attacks
- Fast failover & multipath
- High efficiency through path optimization
- Works in distributed scenarios
- Fault-independent from today’s Internet



[from ETH Zurich]

Lightning Filter

Guarantee Network performance and availability

- Filtering service that is deployed upstream of protected end server
- Performs:
  - Packet authentication (DRKey)
    → authentic source AS
  - Duplicate suppression (using Bloom Filter)
    → no duplicates
  - Per-AS history collection (using Cuckoo hash table)
  - History-based resource allocation and filtering during DoS
    → fair resource allocation based on previous usage
- Result: collateral damage only for hosts within attacker-controlled AS

[from ETH Zurich]

Conclusion

- A lot of money is involved and many things can go wrong
- An emerging field with many opportunities
- DoS attacks against blockchains are vastly ignored