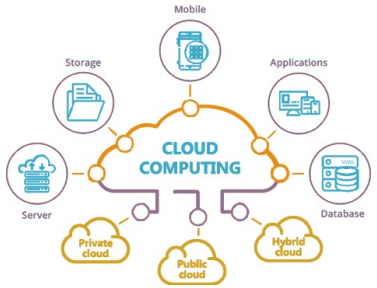
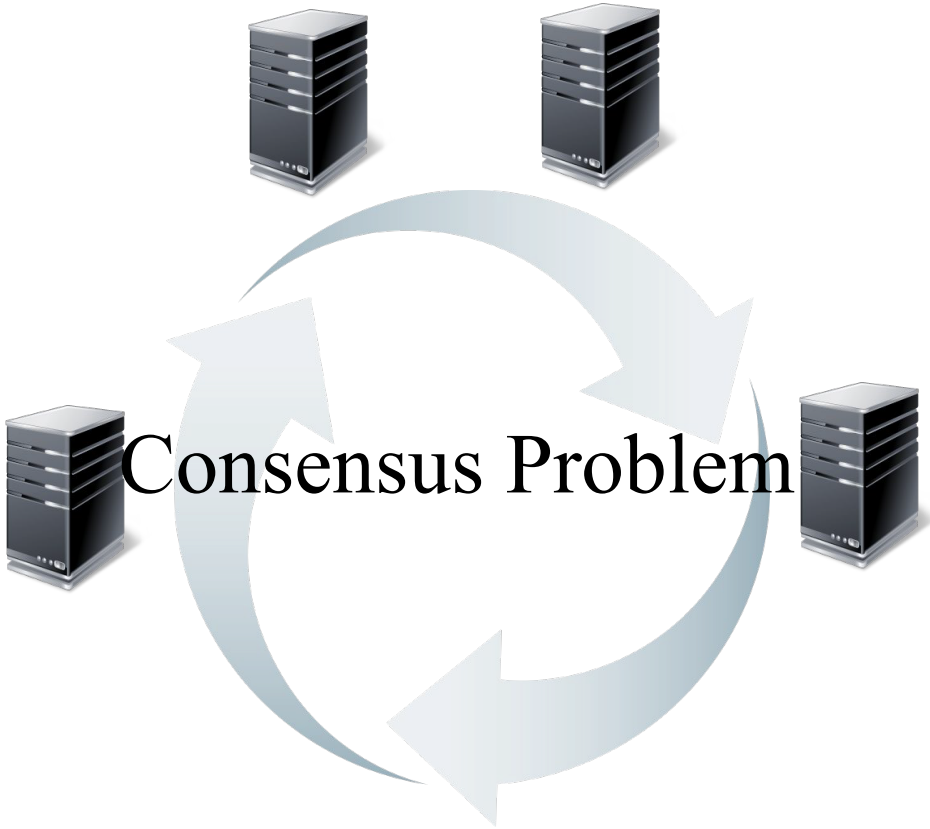
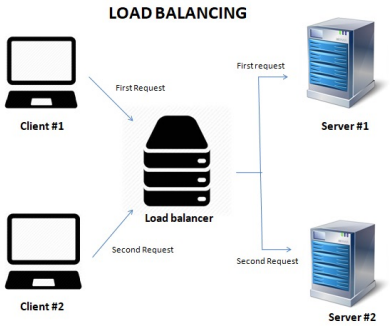
Blockchain Security and Scalability

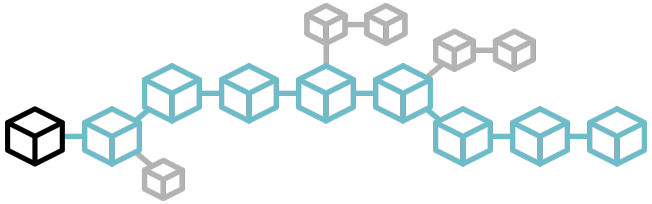
Tuyet Duong





Consensus Problem



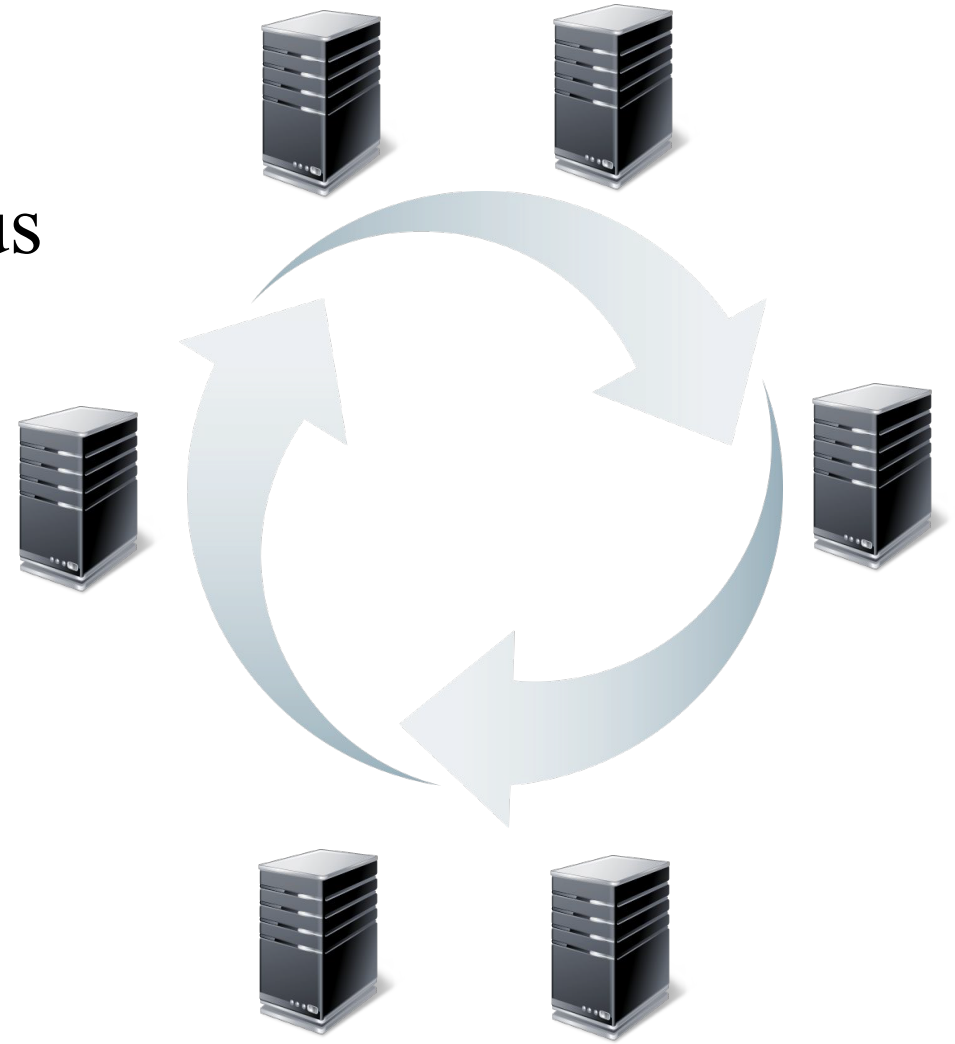


Consensus Problem

Problem

N servers/nodes, f < N are malicious

Propose and agree on one value



Termination : everyone decides

Agreement : all non-malicious agree

Classical Consensus Protocol

Classical Consensus Protocol

- ✗ Assumption of known identity set
- ✗ Bandwidth limited
  - $O(n^2)$ messages (e.g. PBFT)
  - Work for a small network (e.g $n < 100$)

How to Build a Secure and Scalable Consensus Protocol?

Blockchain Consensus Protocol

Bitcoin

- Nakamoto 2008
- Maintained by network participants (miners)


Bitcoin Network

Bitcoin Blockchain Consensus Protocol

How to pick a leader?

Bitcoin Blockchain Consensus Protocol

How to pick a leader?

Proof of Work Puzzle

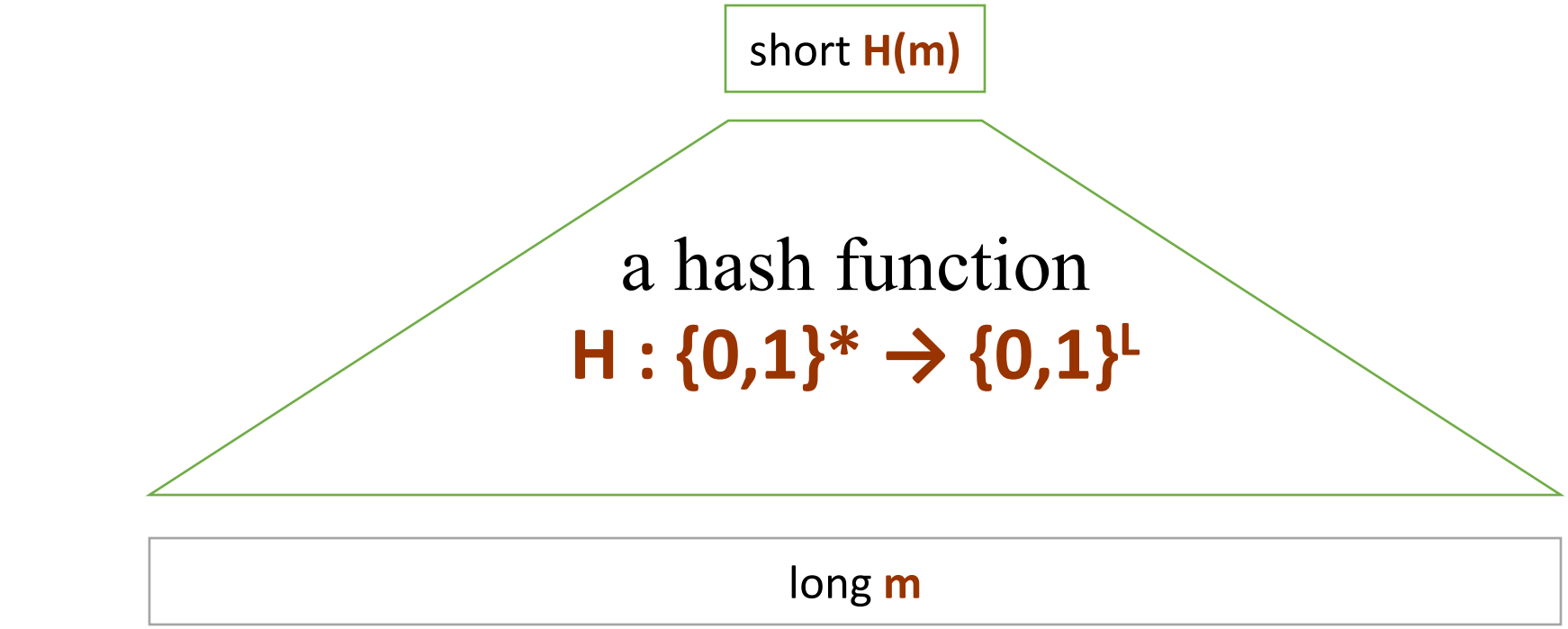
by Cynthia Dwork and Moni Naor in 1993

Recap

- Two different directions to solve the consensus problem
  - Committee-based
  - **Leader-based**

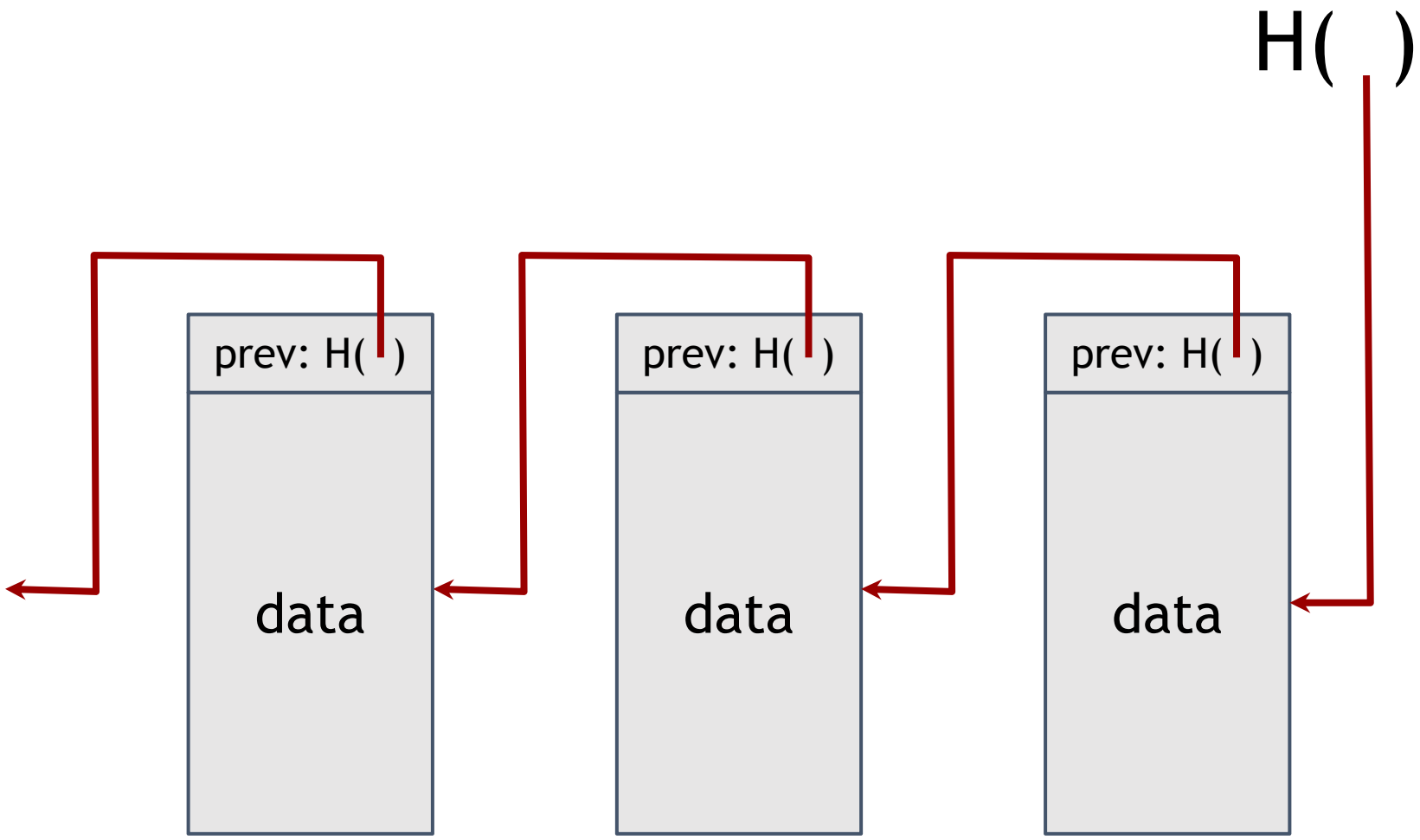
Hash Function and Blockchain Structure

Hash Function



Requirement: it should be hard to find a pair **(m,m')** such that **H(m) =H(m')**

linked list with hash pointers = “block chain”

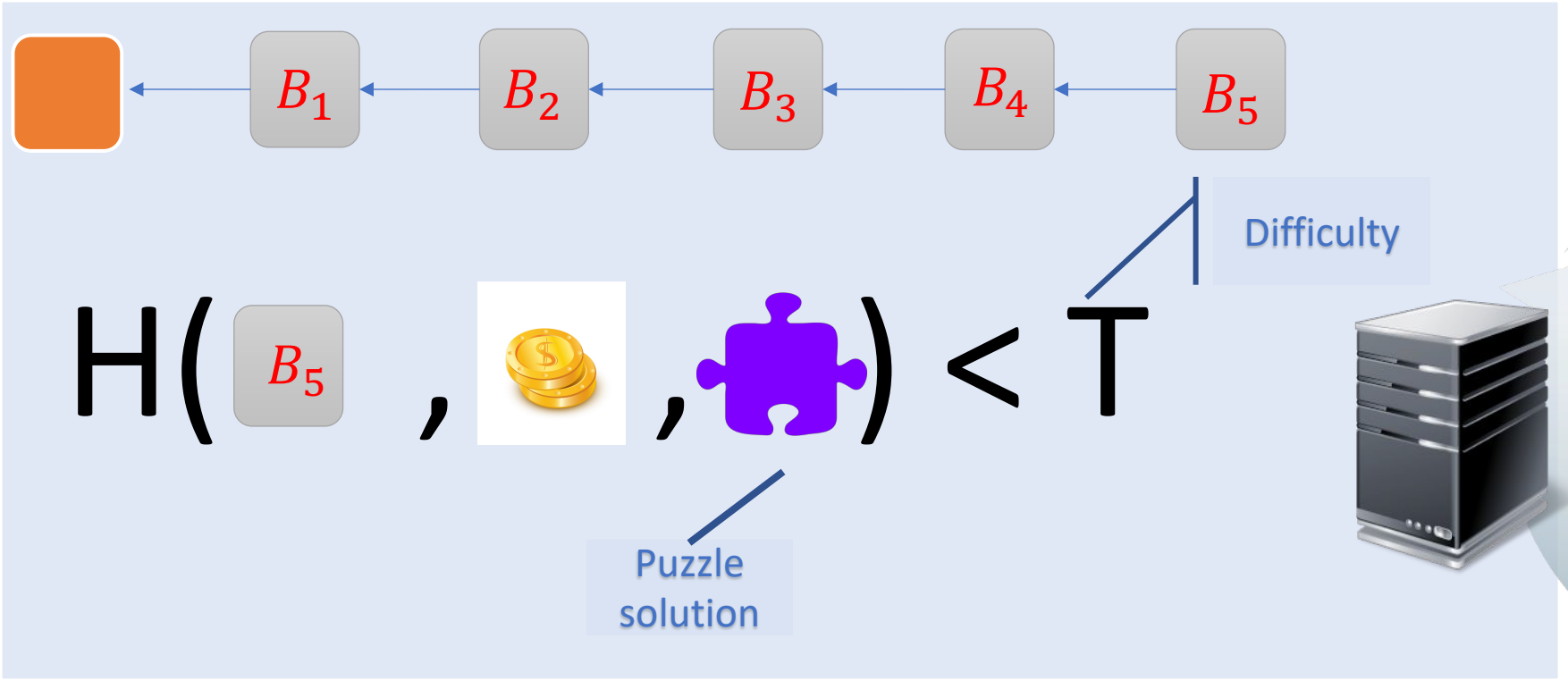


[Nak08]

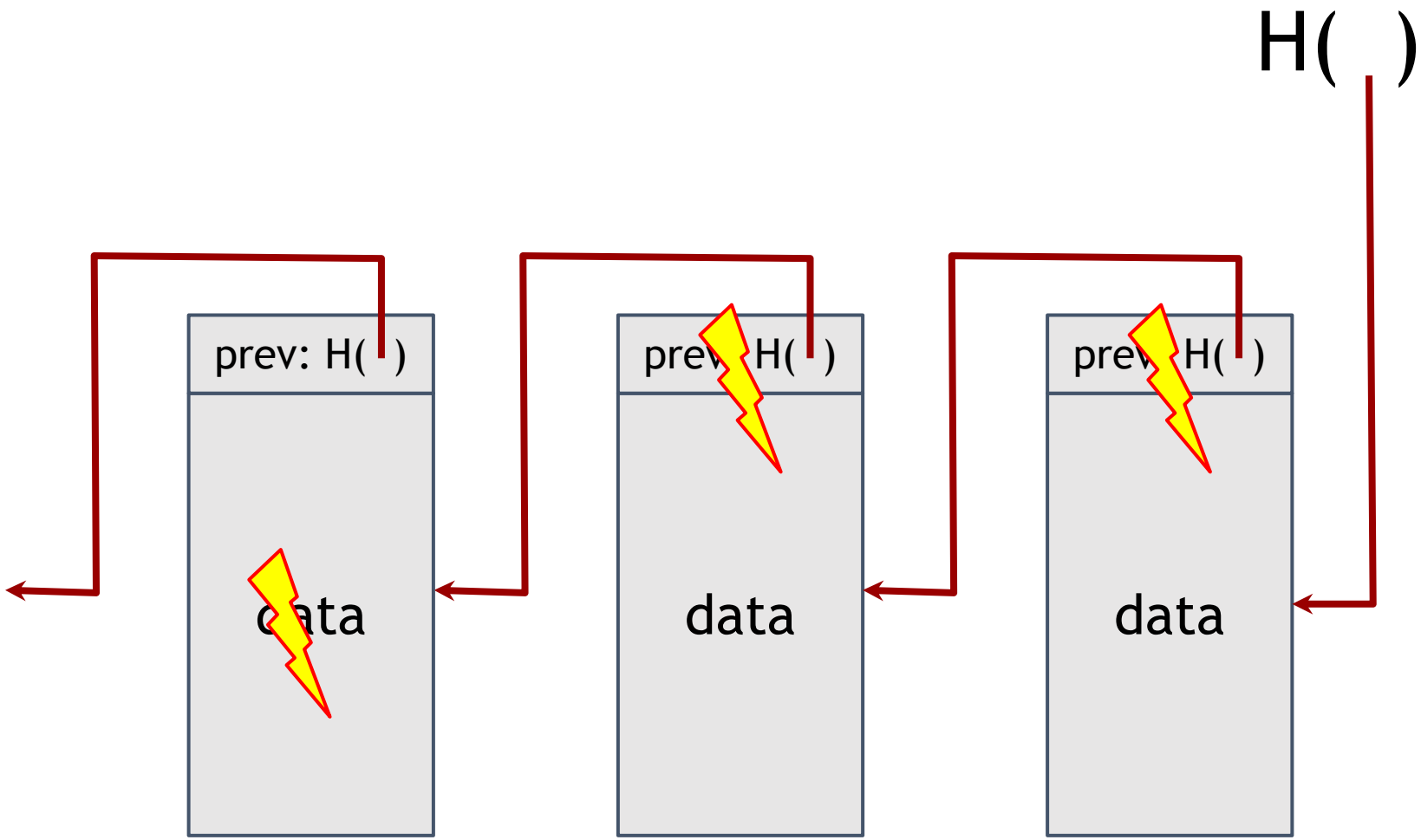
Proof-of-Work Puzzle

Bitcoin Blockchain Consensus Protocol

[Nak08]



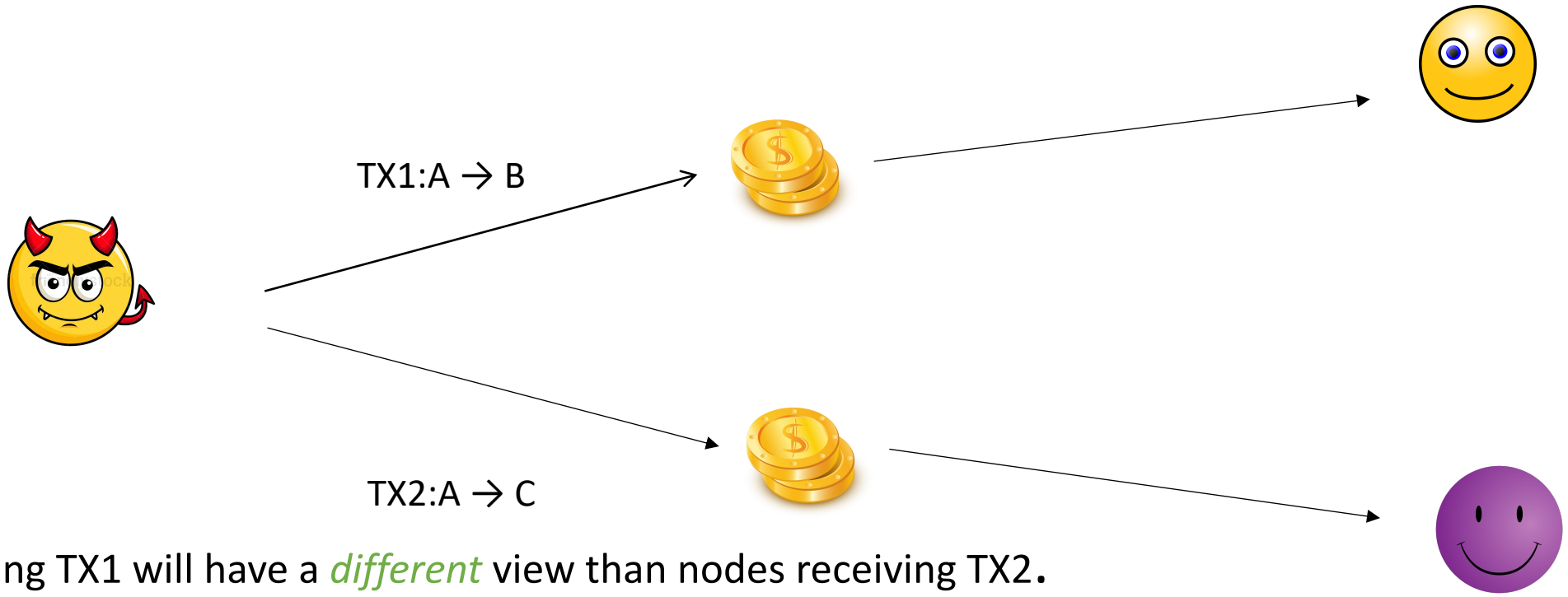
detecting tampering



use case: tamper-evident log

Bitcoin Blockchain Consensus Protocol: Fork

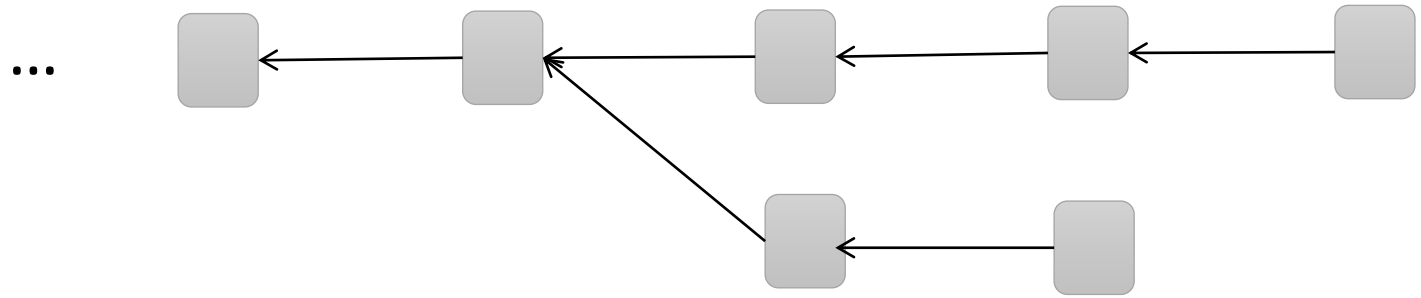
[Nak08]



nodes receiving TX1 will have a *different* view than nodes receiving TX2.

Bitcoin Blockchain Consensus Protocol

[Nak08]



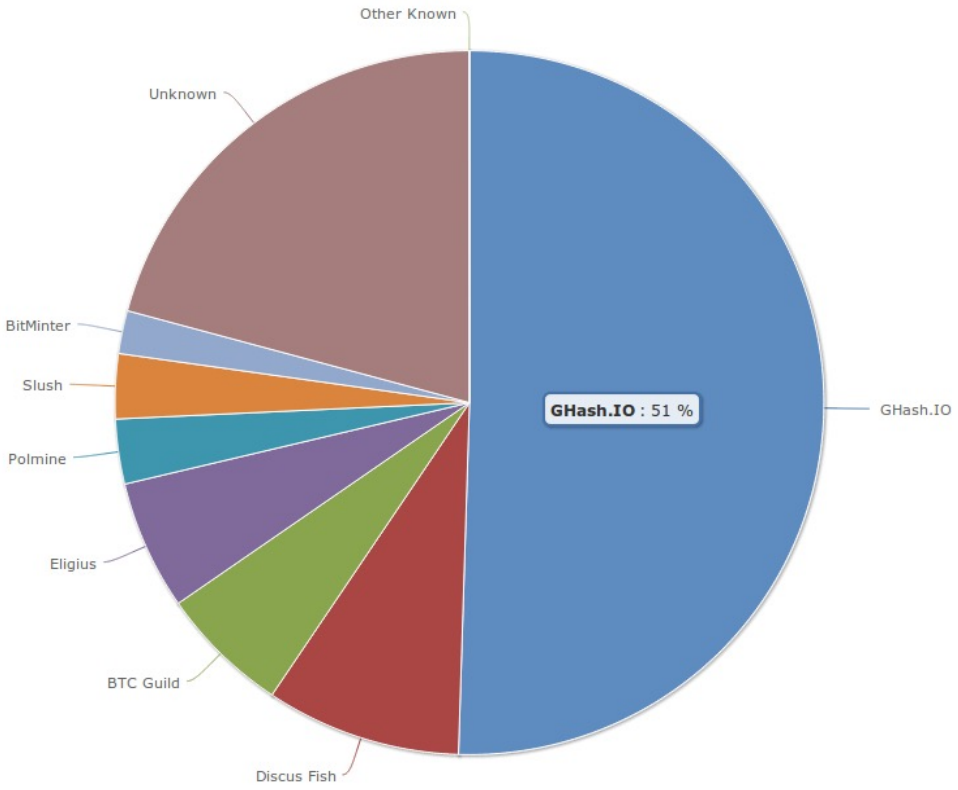
Honest nodes “believe” the longest chain

Assumption: ***honest nodes control the majority of computing power***

Security and Scalability Problems and my Contributions

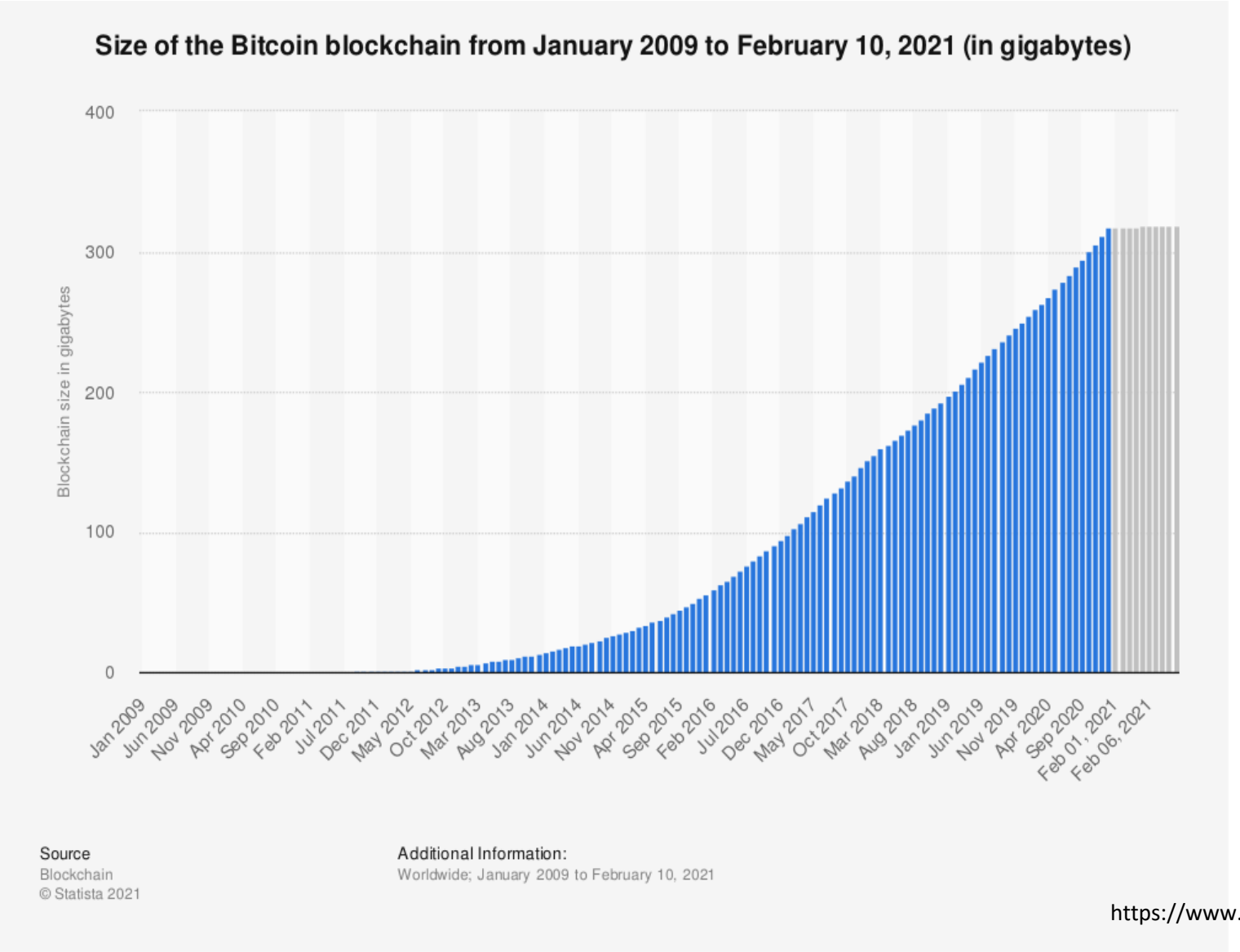
Problem 1 : Security

51% Honest Mining Power Assumption could be challenged



June 12, 2014
GHash.IO large mining pool crisis
https://blockchain.info/pools

Problem 2: Storage Scalability



https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

Problem 2: Throughput Scalability

3-7 TXs per second

Demand from Practice: 1,200 - 50,000 TXs/s

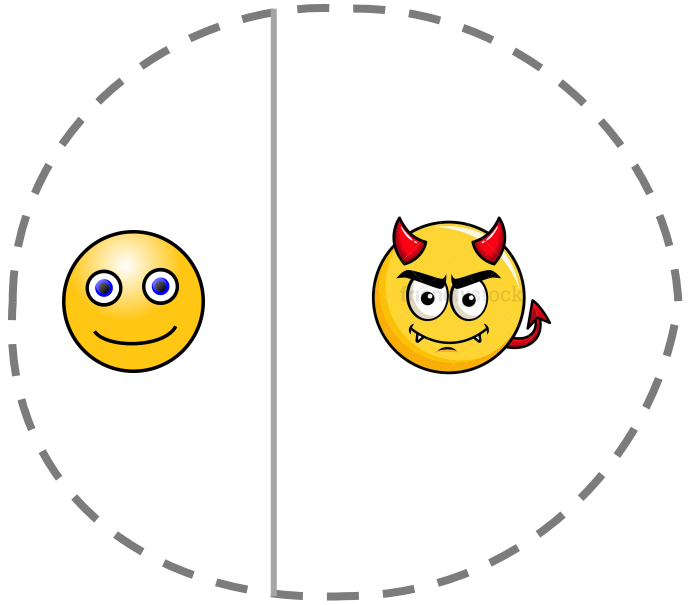
Recap

- Problems:
  - Security Assumption
  - Storage and Throughput Scalability

Solving Problem 1 : Security in the presence of the 51% Attack

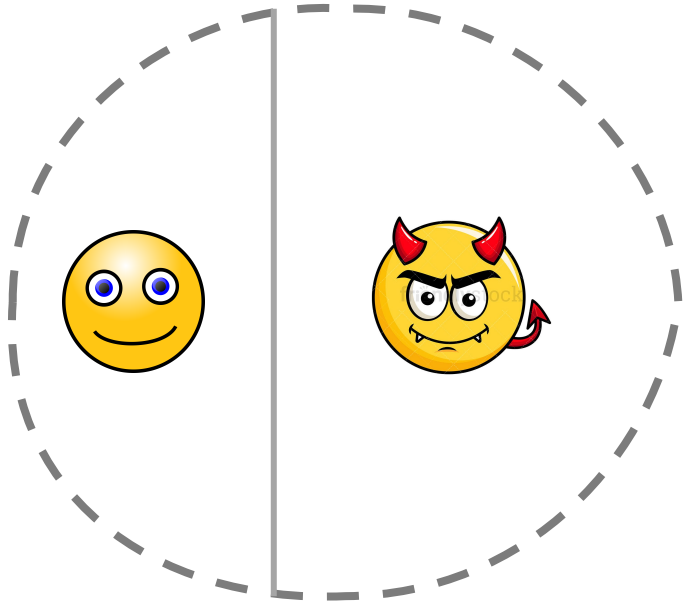
2-hop Protocol: Idea

Computing power

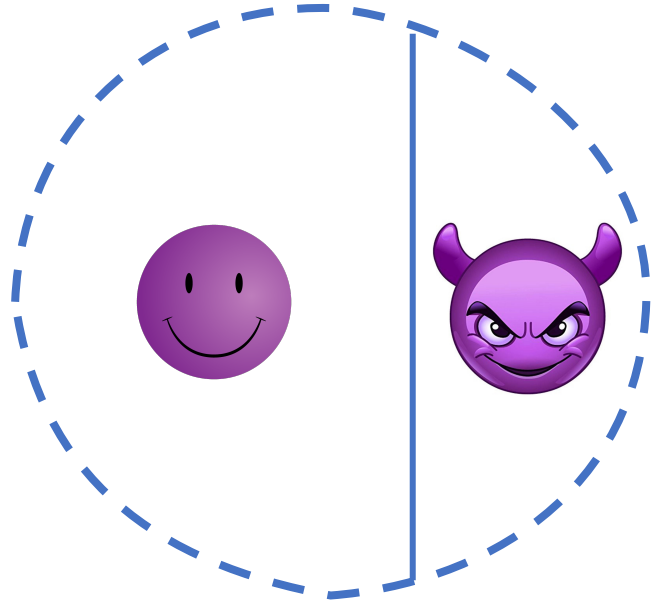


2-hop Protocol: Idea

Computing power

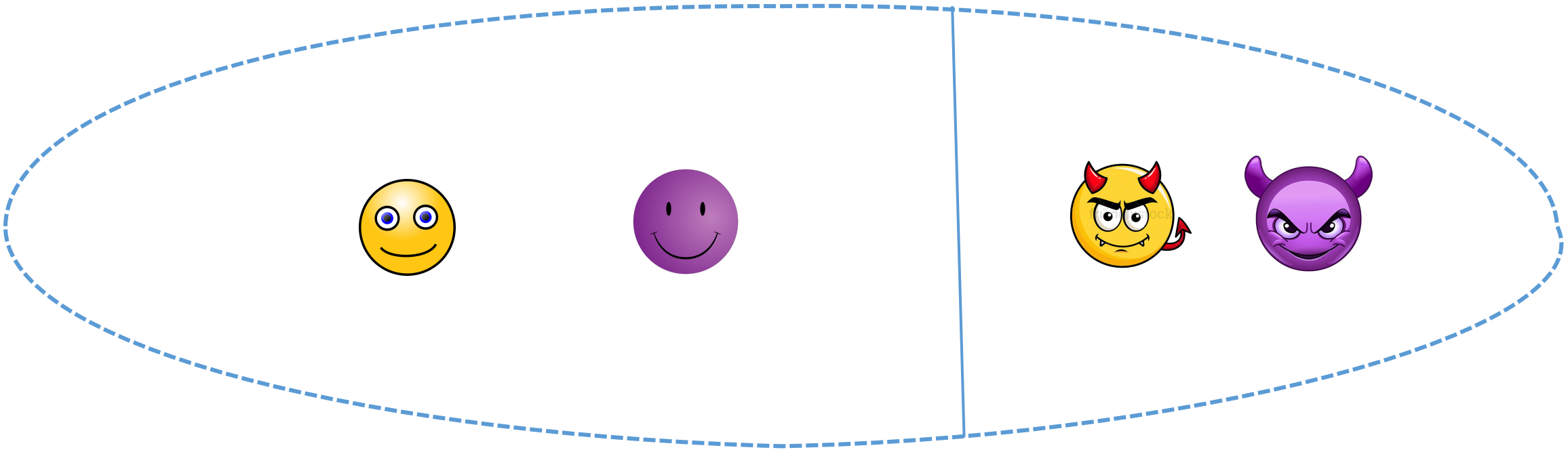


Stake



2-hop Protocol: Idea

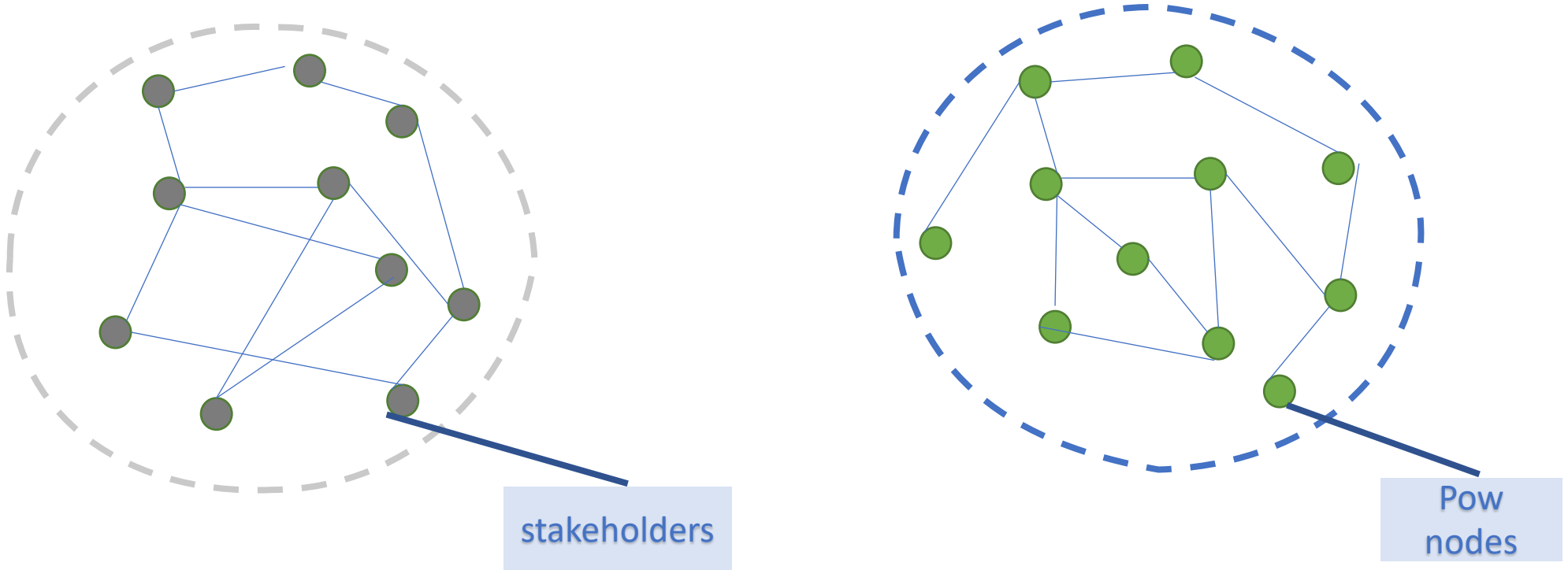
Computing power and Stake



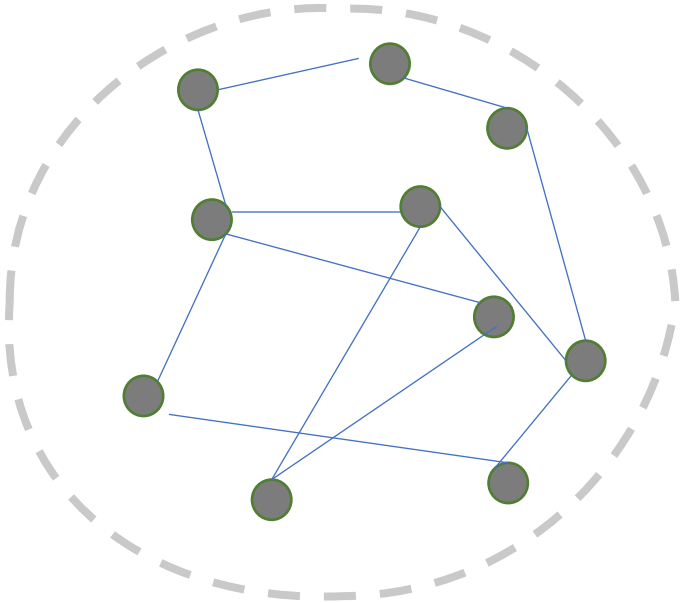
2-hop Protocol: Challenge

How to design a Proof-of-Stake Puzzle?

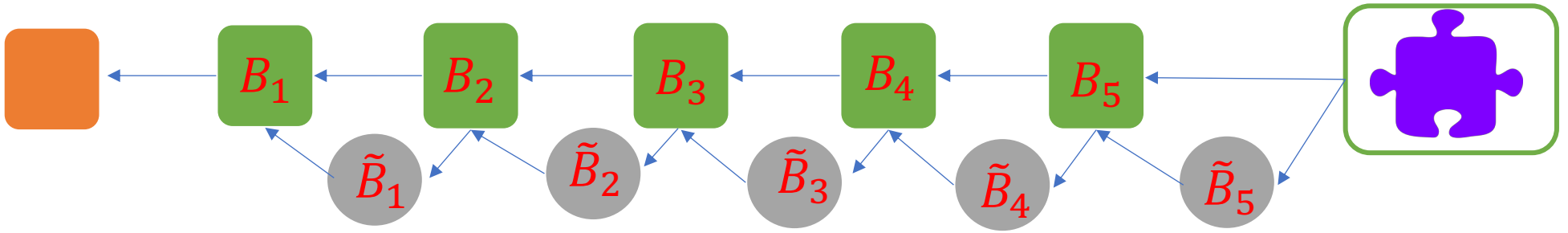
2-hop Protocol: Challenge



2-hop Protocol: Challenge



2-hop Protocol: Blockchain extension

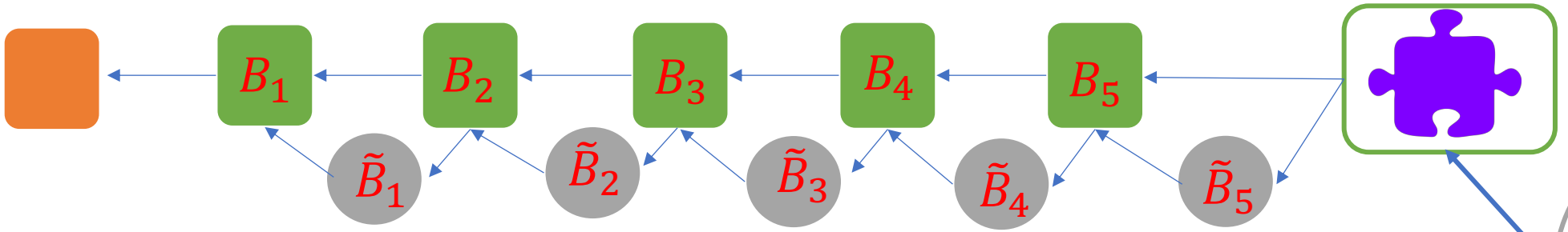


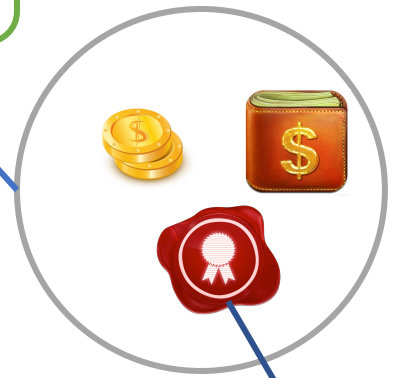
$$\tilde{H}(\ ,\ ,\ ) < \tilde{T}$$

PoW as a biased random beacon

Stakeholder identity

2-hop Protocol: Blockchain Extension

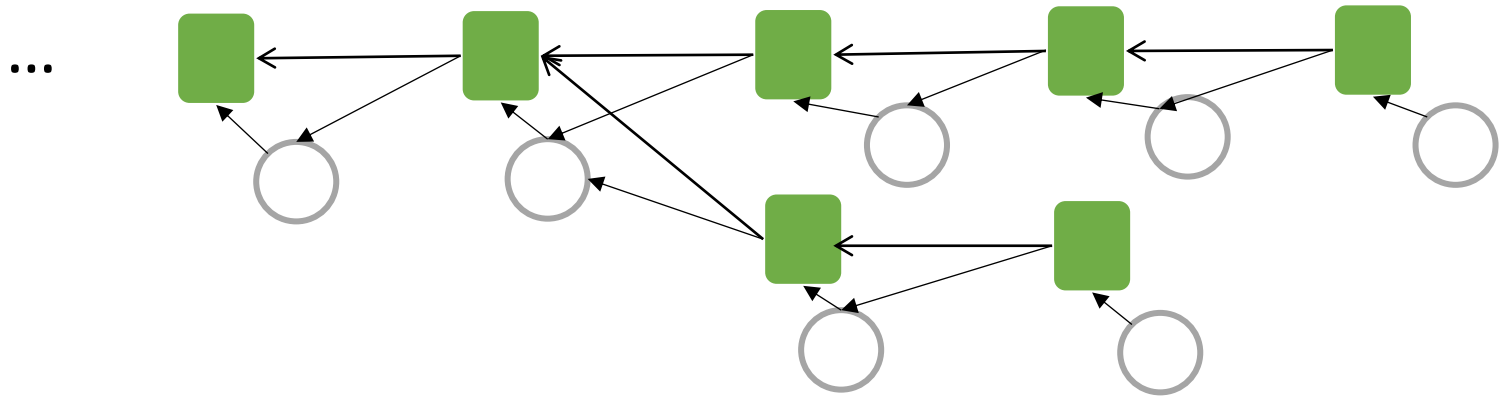




$$\tilde{H}(\ ,\ ,\ ) < \tilde{T}$$

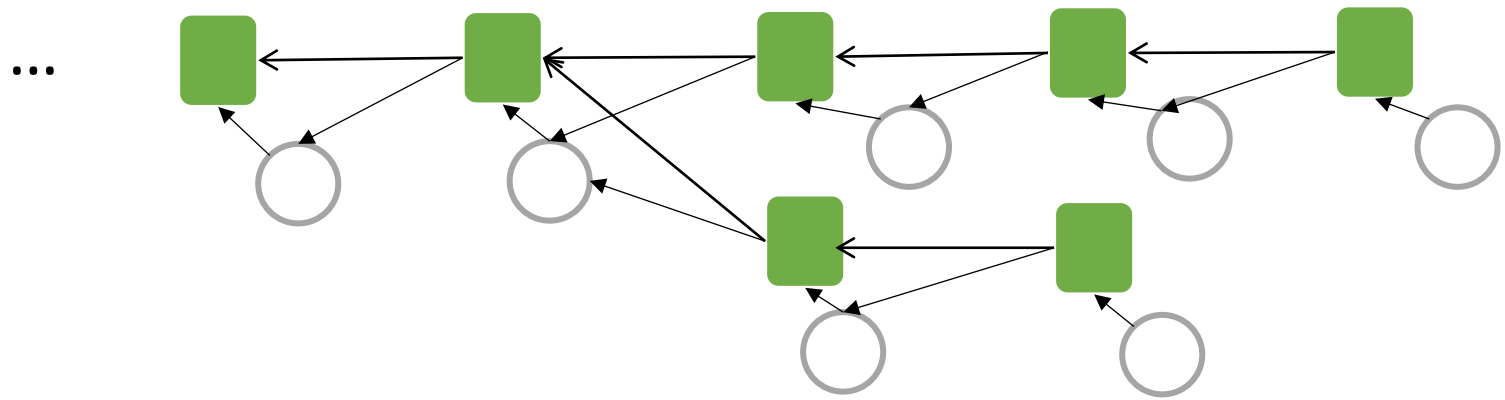
Unique Signature

2-hop Protocol: Blockchain Extension



Honest nodes “believe” the chain-pair with the longest PoW chain

2-hop Protocol: Blockchain Extension

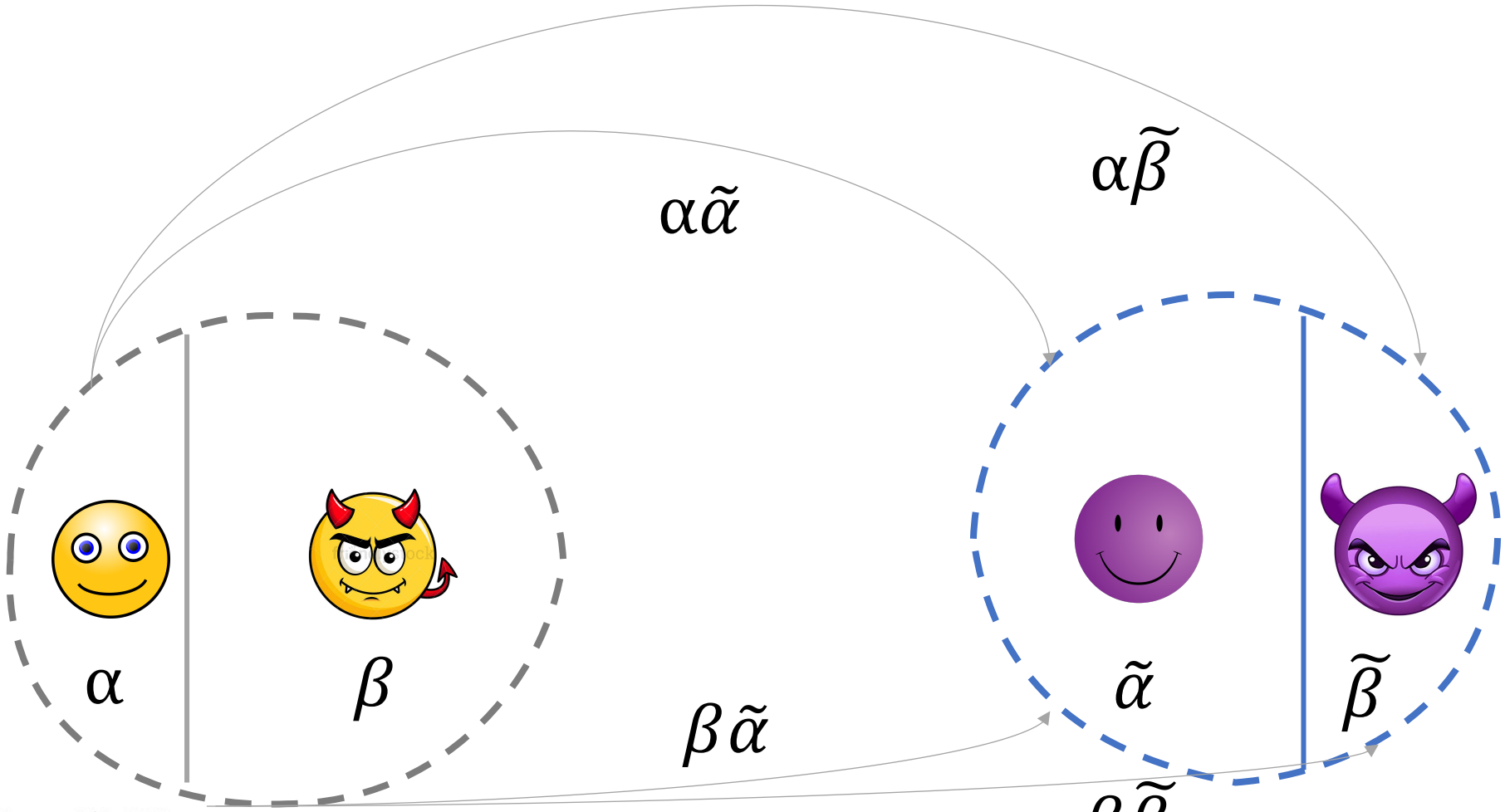


Assumption: ***honest nodes control the majority of collective resources***

Security Analysis

$$\alpha = 1-(1-p)^{(1-\rho)n}$$

$$\beta = \rho n p$$

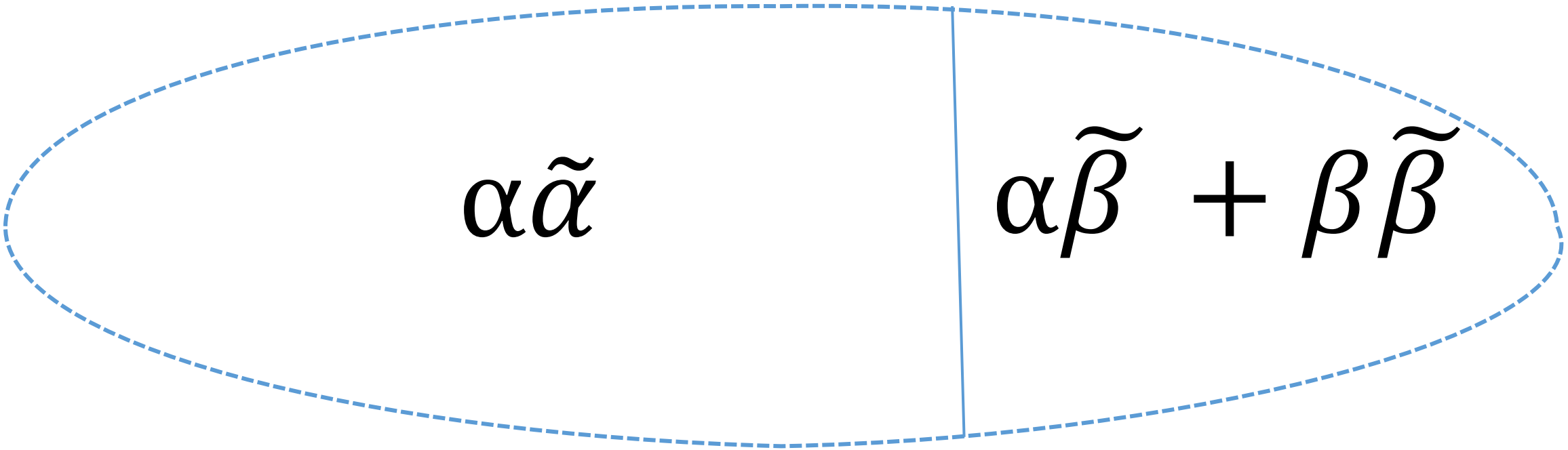


$$\tilde{\alpha} = 1-(1-\tilde{p})^{(1-\tilde{\rho})\tilde{n}} \approx (1-\tilde{\rho})\tilde{n}\tilde{p}$$

$$\tilde{\beta} = 1-(1-\tilde{p})^{\tilde{\rho}\tilde{n}} \approx \tilde{\rho}\tilde{n}\tilde{p}$$

Security Analysis

Computing power and Stake



Security Analysis

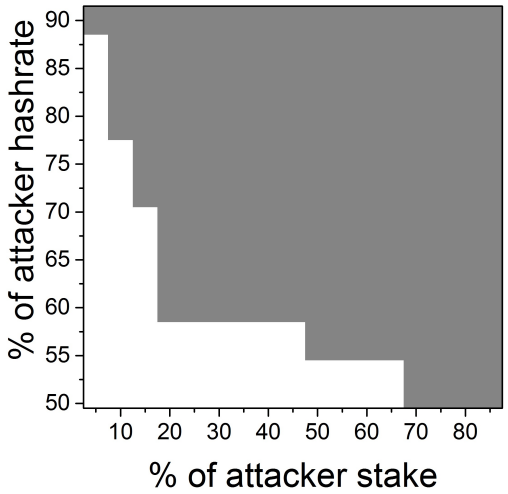
1. Define events of interest, i.e., # honest vs malicious blocks
2. Derive expectations for the events of interest
3. Deploy concentration theory, e.g., Chernoff bound. In *t* rounds

$$\Pr[Y < (1-\delta''')\alpha\tilde{\alpha}t] < e^{-\Omega(t)} \qquad \Pr[Z > (1+\delta')(\alpha+\beta)\tilde{\beta}t] < e^{-\Omega(t)}$$

Y> Z with probability at least $1 - e^{-\Omega(t)}$ under the constrain that $\alpha\tilde{\alpha} > \alpha\tilde{\beta} + \beta\tilde{\beta}$

Experiments

Use Scorex framework (https://github.com/input-output-hk/Scorex)
https://bitbucket.org/twinscoin/twinschain



- 70% of total mining power an adversary also needs for about 20% of total stake to generate a better chain than honest party's.
- 20% of stake is about $2.3 billion.

Thank you!