Hybrid Consensus: Efficient Consensus in the Permissionless Model

Rafael Pass and Elaine Shi

IC3

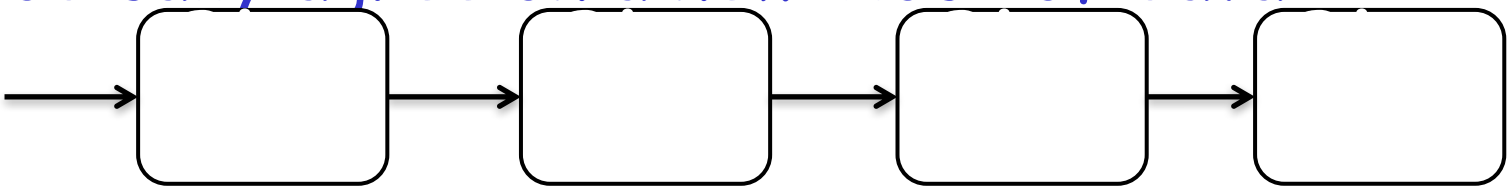
Blockchains

Satoshi Nakamoto, 2009

- Public database
- Shared & maintained between network participants

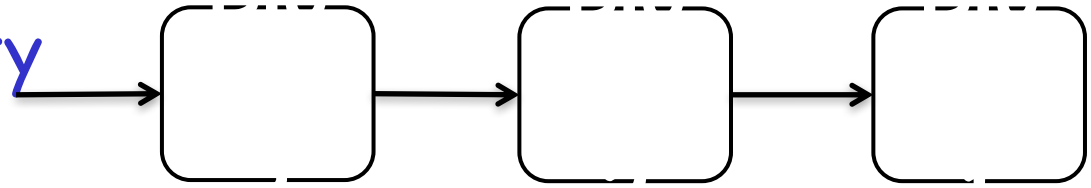
Blockchain agreement protocol

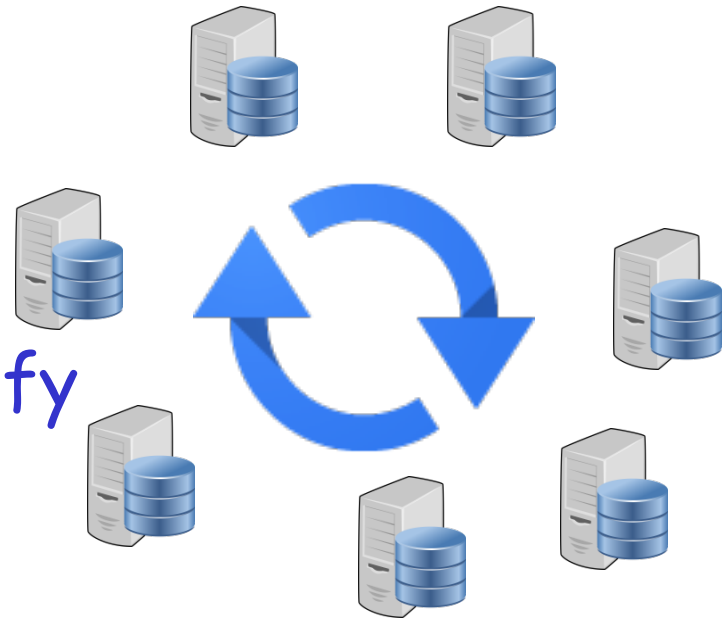
- Periodically agree on a new block of data



The Blockchain Agreement Problem

- Set of N computational nodes
  - No inherent identity
  - No PKI
- Agree on a block
  - Includes a set of new transactions (or data)
- Two properties
  - Agreement
  - Validity: all transactions satisfy some validity conditions





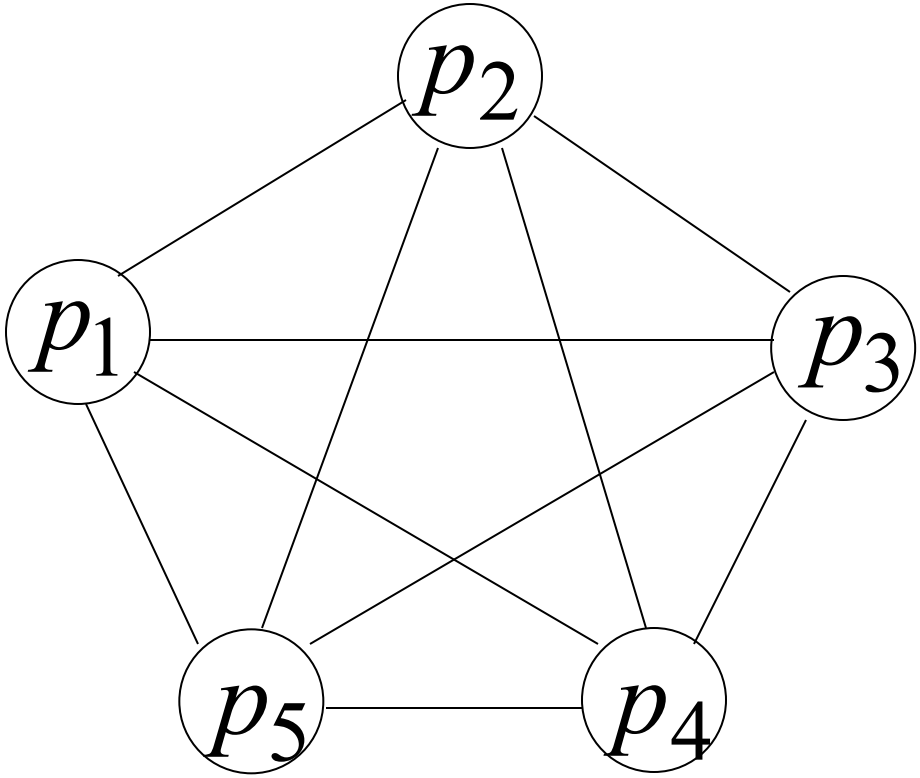
Scalability Issue

1 MB block per 10 mins
3-7 TXs per second

Support limited computations
Several DoS attacks recently

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

Byzantine Agreement

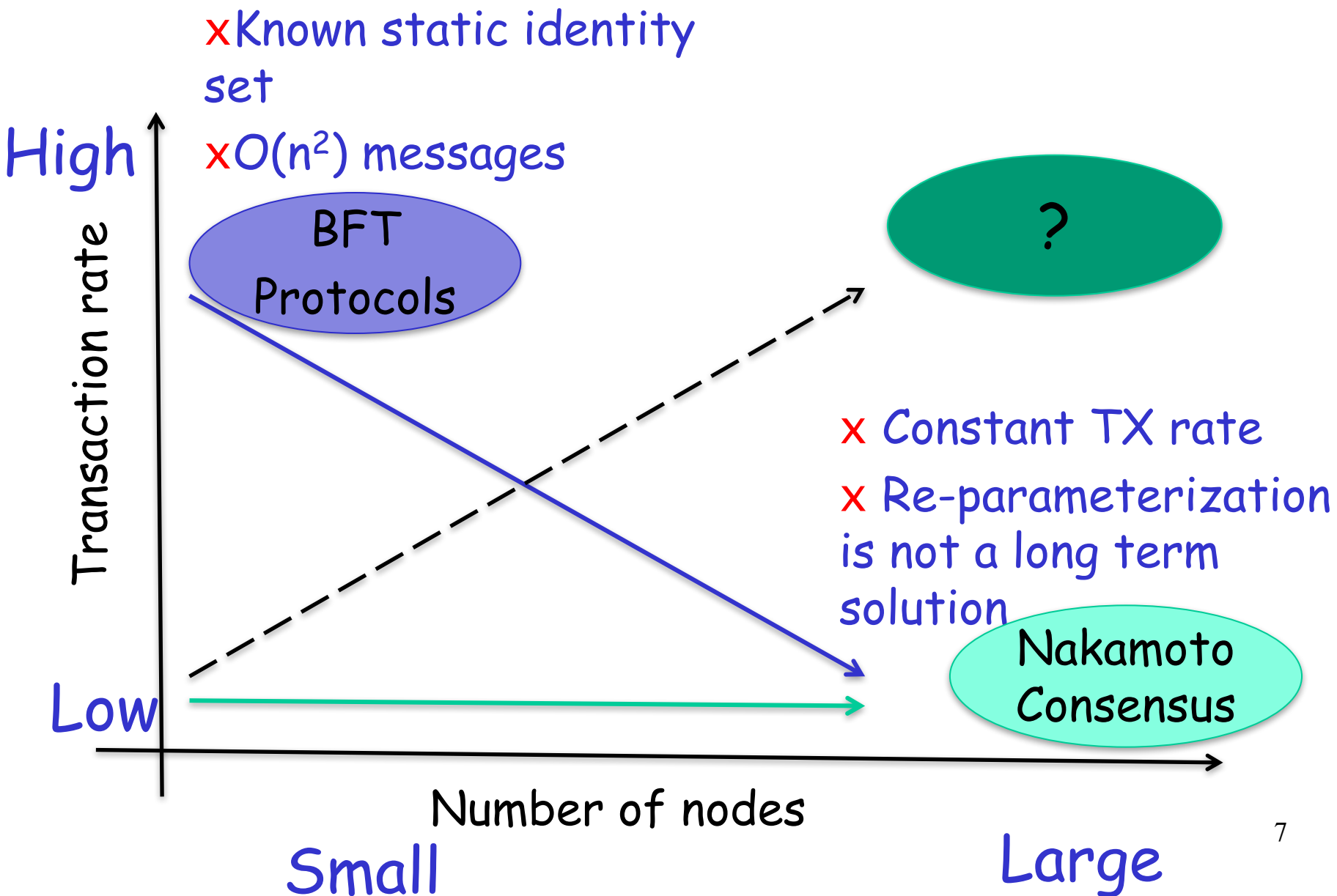


- Complete graph
- permissioned

Agreement:

- Every correct node chooses the same value
- If all the correct nodes have the same input, that input must be the value chosen

Existing protocols are not scalable



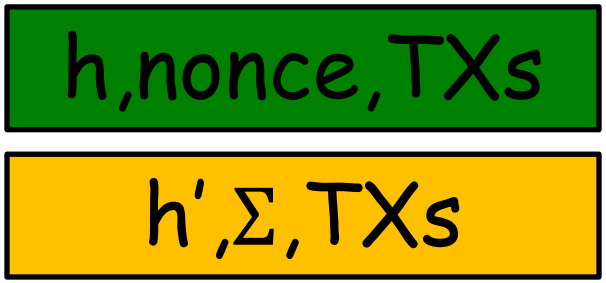
Hybrid Consensus Idea

- Use PoW chain to elect a static committee
  - honest nodes run the blockchain for csize + λ blocks where csize = $\Theta(\lambda)$ denotes the targeted committee size.
  - honest nodes would remove the trailing, unstablized λ blocks from its local chain, and call the miners of the first csize blocks the BFT committee.
- Run BFT to agree on a new block

Blocks

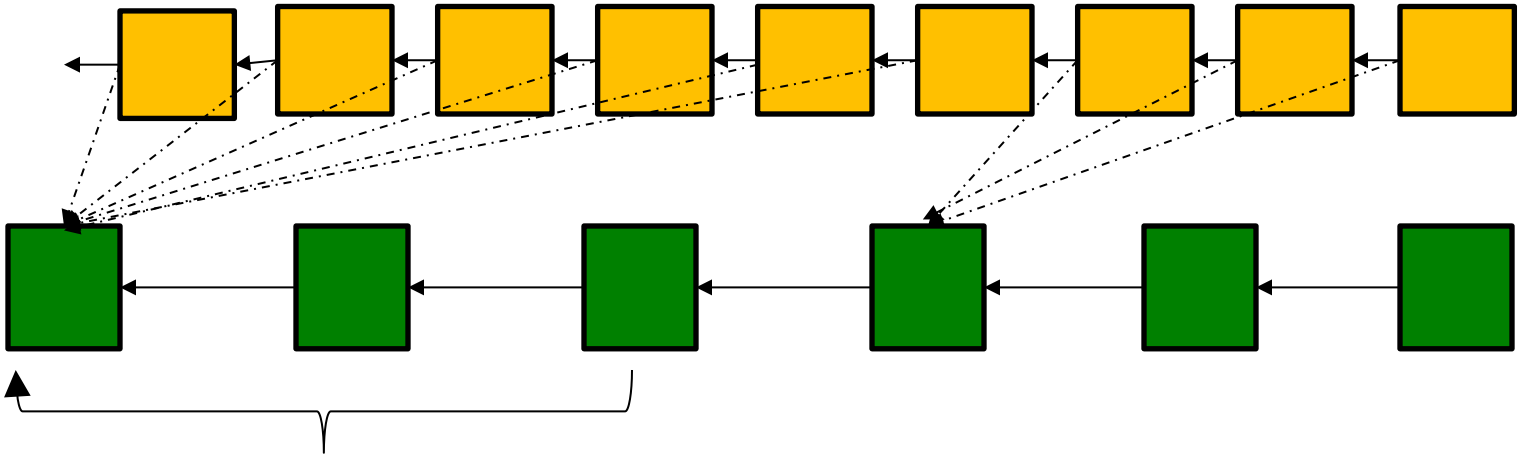
PoW block

BFT block



Σ: a set of signatures

$|\Sigma| \geq csize/3$

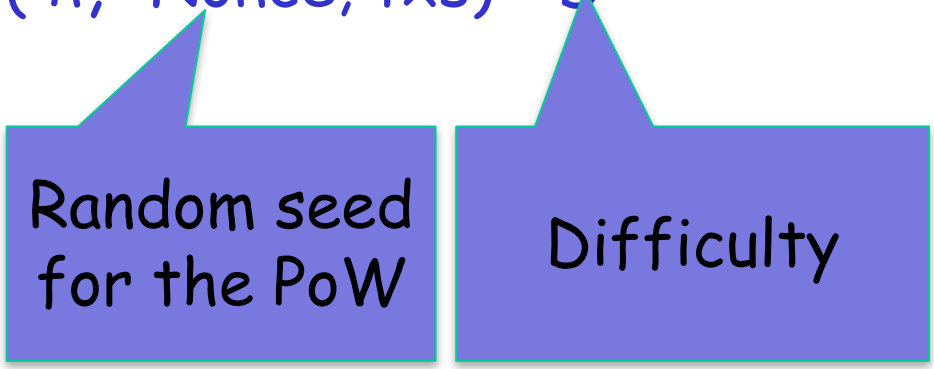


R-th committee

Step 1: Identity establishment

Solve PoW

$$ID = H(h, Nonce, txs) < D$$



The last csize confirmed blocks define members in a committee

Step 2: Propose BFT blocks

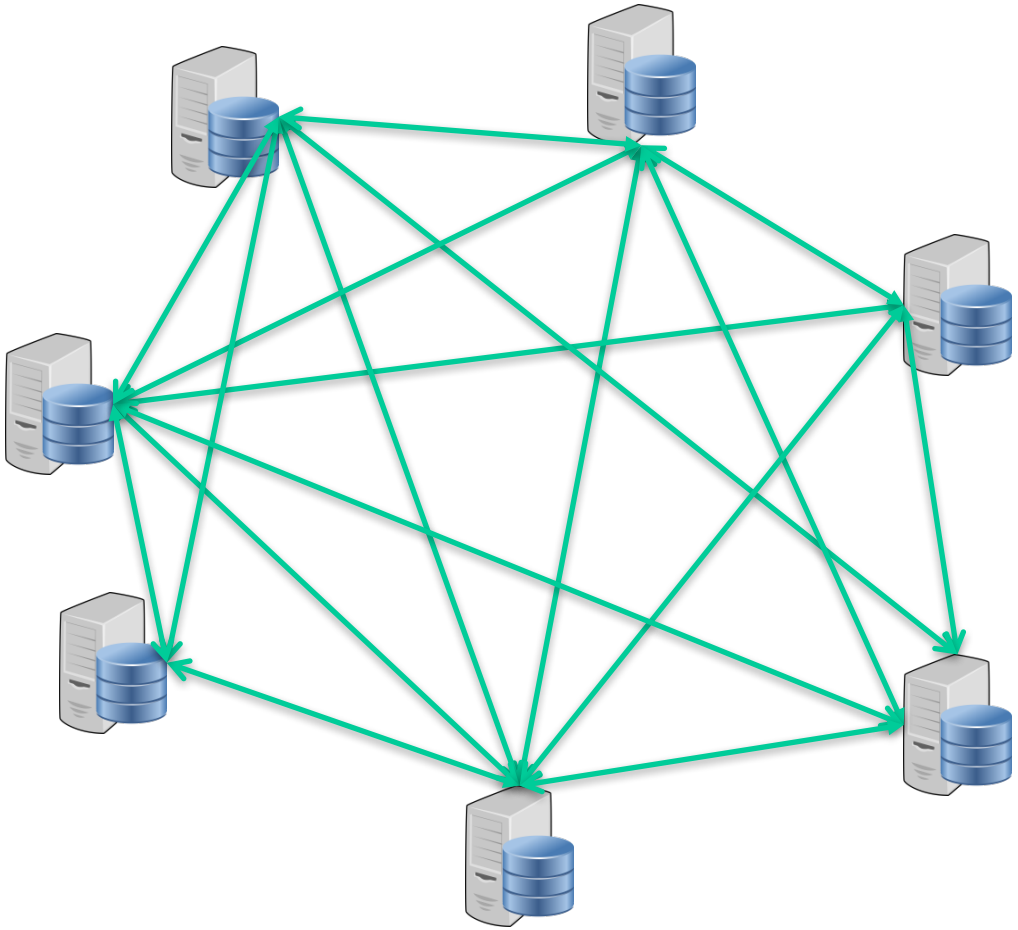
Run a classical Byzantine agreement protocol

- -Members agree & sign on one valid BFT block
- -Each committee serves for a period of time to generate csize PoW blocks, e.g. 1 day.
- - Broadcast the block to the network

When each committee has at least C members?

Each committee has $O(\lambda)$

- $O(\lambda^2)$ messages
- =>scalable



Security guarantees

Due to the consistency property of PoW chain, all honest nodes agree on the same BFT committee.

Due to the chain quality property of PoW chain, with appropriate overall parameters, we can ensure that more than 2/3 of the committee members are honest which is sufficient to ensure the security of the permissioned BFT protocol.

Security guarantees

- Due to the chain growth property of the pow chain, it will not take too long for the BFT committee to form

THANK YOU