NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty

Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 41: ByzCoin

CONCEPTS COVERED

- Byzcoin: Combining PoW with PBFT
- Scalability: How far can we achieve?

KEYWORDS

- **Byzcoin**
- **Open consensus group**
- **The blockchain performance triangle**

Revisiting the Requirements for Blockchain Consensus

- **Byzantine fault tolerant** – the system should work even in the presence of malicious users while operating across multiple administrative domains

- Should provide **strong consistency guarantee** across replicas

- Should **scale well to increasing workloads** in terms of transactions processed per unit time

- Should **scale well to increasing network size**

Bitcoin-NG: The issue with a Faulty Key Block

- **Problem with Bitcoin-NG:** A faulty key block is verified only after end of the round
- A faulty miner can introduce several correct microblocks following a faulty microblock in the system
  - certainly an overhead for the application - **a fork alleviates the problem further**

Bitcoin-NG: The issue with a Faulty Key Block

- **Problem with Bitcoin-NG:** A faulty key block is verified only

Solve this problem by a set of PBFT verifiers - who will verify a block and then only the block is added in the Blockchain

Issues with PBFT

- PBFT requires a **static consensus group** (because of message passing)

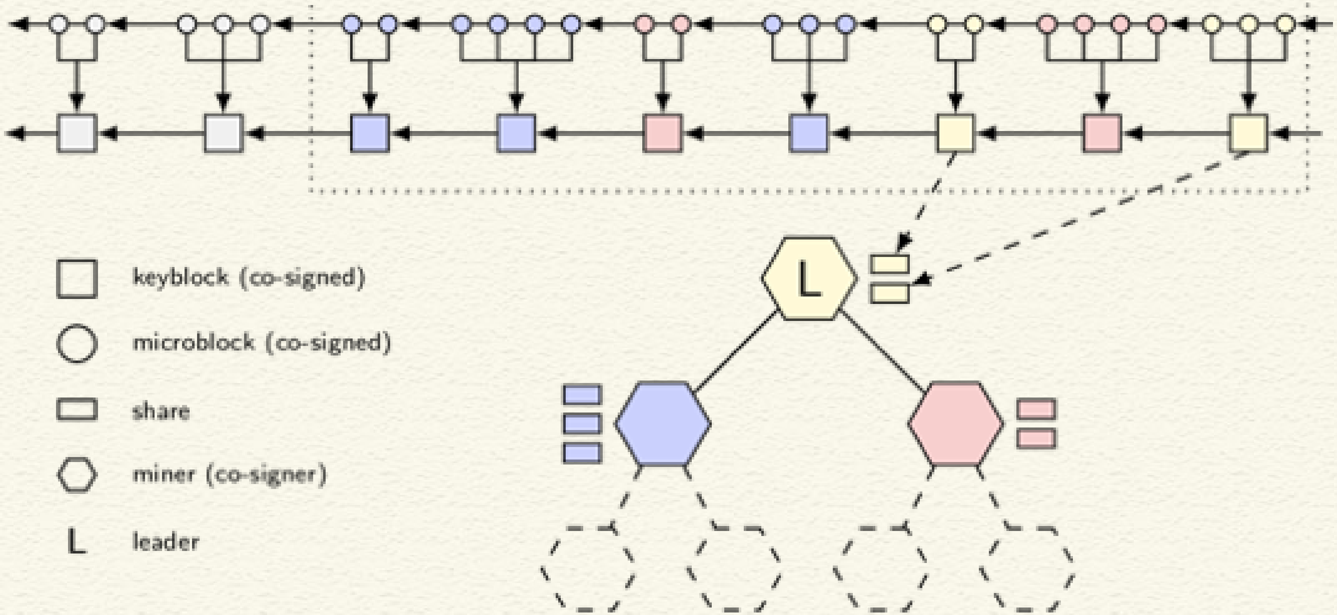
- **Scalability** (in terms of nodes) is a problem for PBFT
  - O(n^2) communication complexity
  - O(n) verification complexity
  - Absence of third-party verifiable proofs (PBFT uses MAC - need to share the keys among the miners)

- **Sybil attack** - create multiple pseudonymous identities to subvert the ***3f+1*** requirements of PBFT

Open the Consensus Group

- Use PoW based system to give a *proof of membership* of a miner as a part of the trustees

- Maintains a “balance of power” within the BFT consensus group
  - Use a fixed-size sliding window
  - Each time a miner finds a new block, it receives a *consensus group share*
  - The share proves the miner’s membership in the trustee group



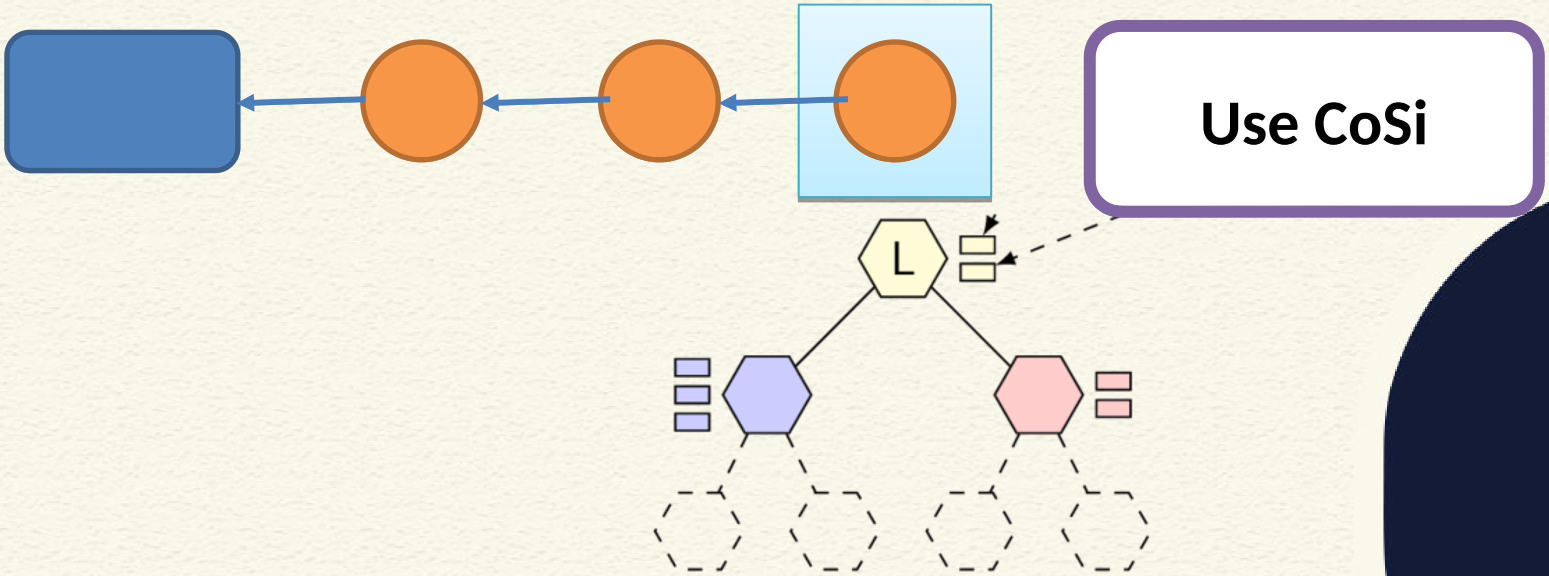
Kogias, E. K., Jovanovic, P., Gailly, N., Khoffi, I., Gasser, L., & Ford, B. (2016, August). **Enhancing bitcoin security and performance with strong consistency via collective signing**. In *25th USENIX Security Symposium 2016*

Merging BFT Consensus with PoW

- Validate each microblock by a set of witness consigners

Merging BFT Consensus with PoW

- Validate each microblock by a set of witness consigners



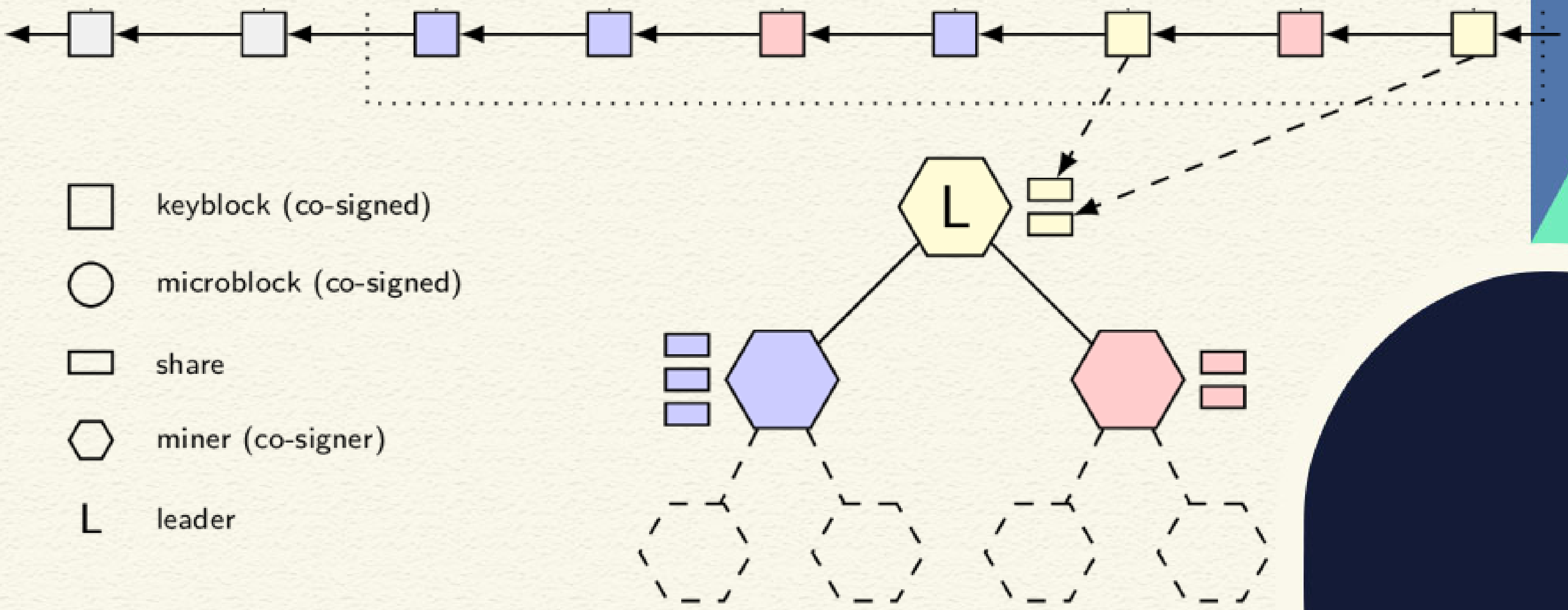
Use CoSi

Merging BFT Consensus with PoW

- Validate each microblock by a set of witness consigners

- **How do we select the witness cosigners?**

Selecting a Consensus Group



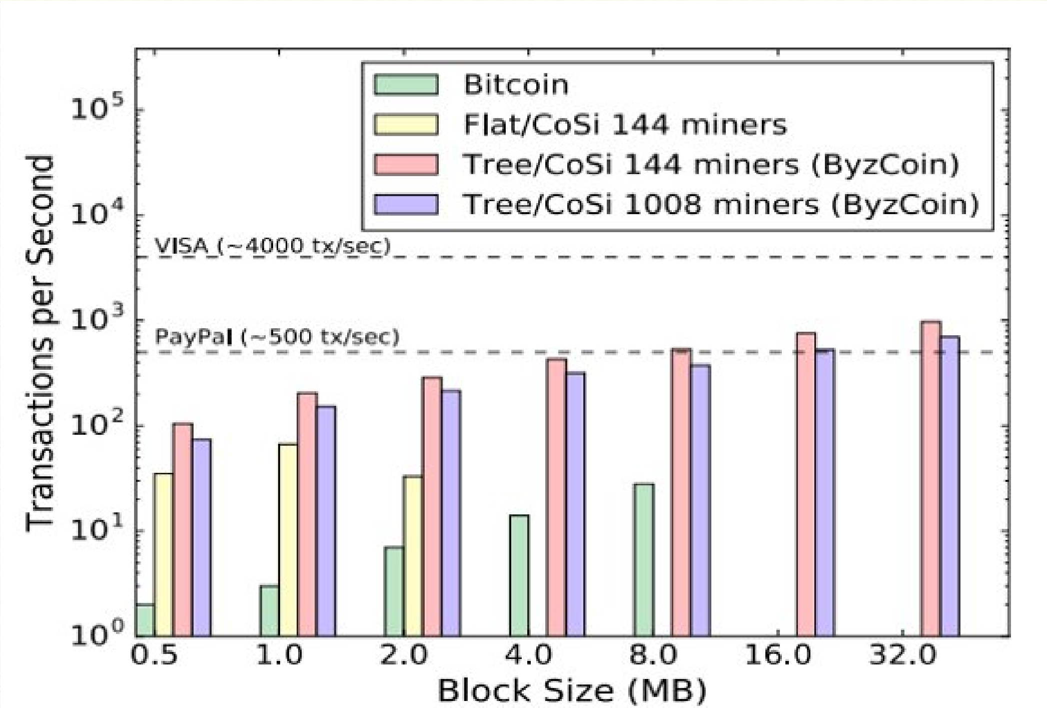
Improving Efficiency of BFT Consensus

- **Improve O(n) communication complexity**
  - Use tree-based multicast protocol - share information with O(log n)

- **Improve O(n) complexity for verification**
  - Use Schnorr multi-signatures
  - Verification can be done in O(1) through signature aggregation

- Multi-signatures + Communication trees = **CoSi**

ByzCoin Performance



ByzCoin Summary

- ByzCoin solves the problem of introducing a faulty microblocks in Bitcoin-NG
- Combine PoW with PBFT
    - Open the consensus group with the help of CoSi

ByzCoin Summary

- ByzCoin solves the problem of introducing a faulty microblocks in Bitcoin-NG

- Combine PoW with PBFT
  - Open the consensus group with the help of CoSi

- **How can we achieve Internet-scale scalability?**
  - **Both performance and network size**

Bitcoin Recap

- **Key Idea**:
  - Consensus through proof-of-work (PoW)
- **Communication**:
  - Gossip protocol
- **Key Assumption**:
  - Honest majority of mining computation power

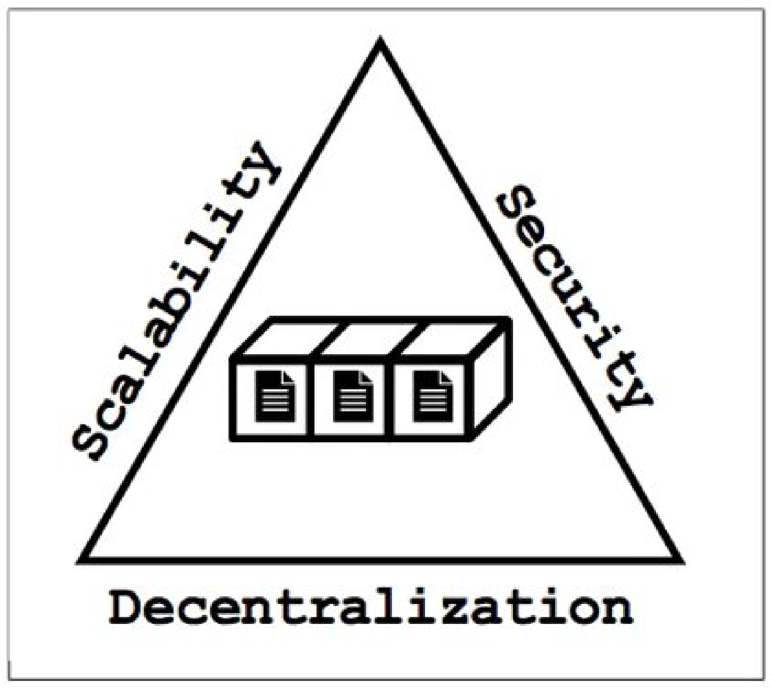
Bitcoin Limitations

- **Resource wastage**:
  - high computational, electricity cost
- **Concentration of power**
  - only ~5 mining pools control the entire system
- **Vulnerable**
  - easy to track miners, concentrated to a few mining pools - https://www.blockchain.com/btc/blocks?page=1

Bitcoin Limitations

- **Scalability**
  - number of users not clear (1M, 10M, 100M??), high latency(~10minutes)
- **Ambiguity**
  - fork in blockchain

Conclusion: The Blockchain Performance Triangle



Is it ever possible to achieve all three simultaneously?

Thank you