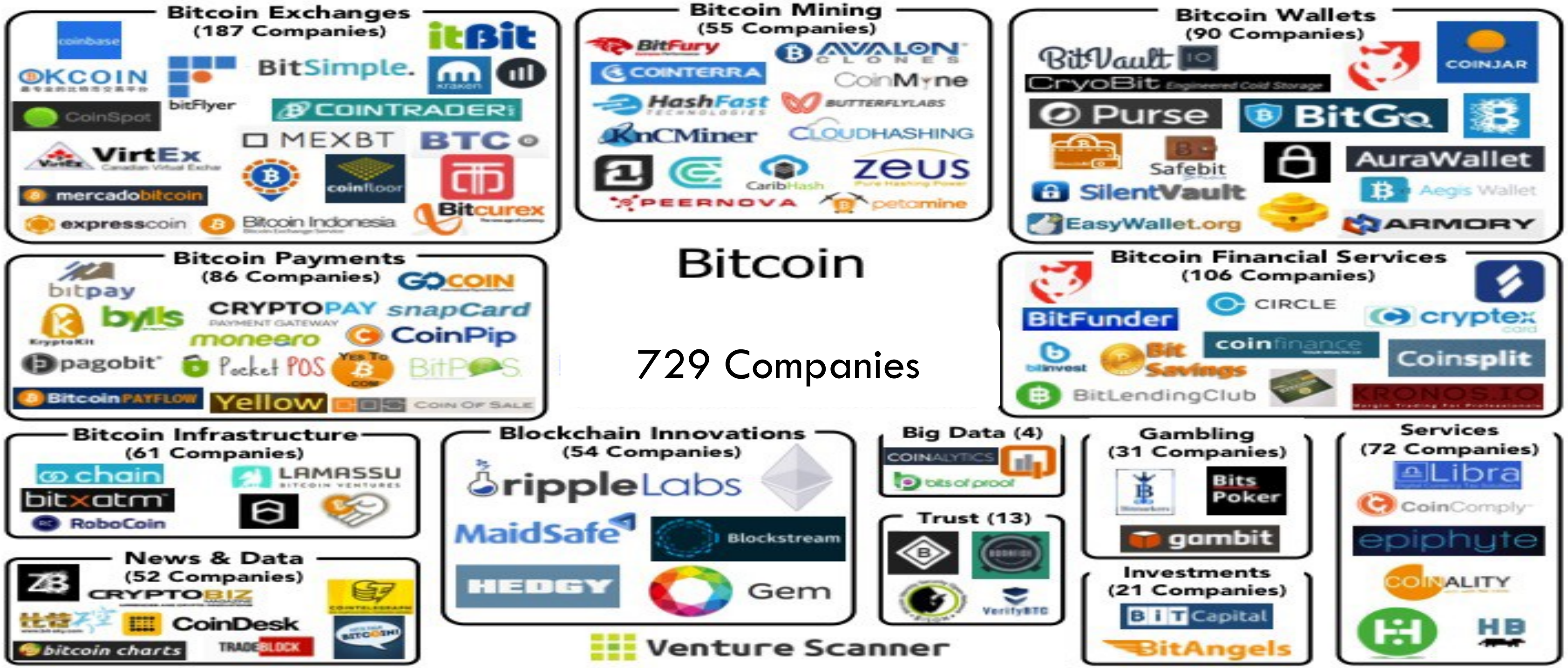
25th USENIX Security Symposium – Austin, TX, August 10th, 2016

ENHANCING BITCOIN SECURITY AND PERFORMANCE WITH STRONG CONSISTENCY VIA COLLECTIVE SIGNING

Lefteris Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser and Bryan Ford
EPFL

@LefKok

Cryptocurrency Ecosystem



Distributed Ledger (Blockchain)

- Cheaper transaction management
- M2M payments (IoT)

Distributed Ledger (Blockchain)

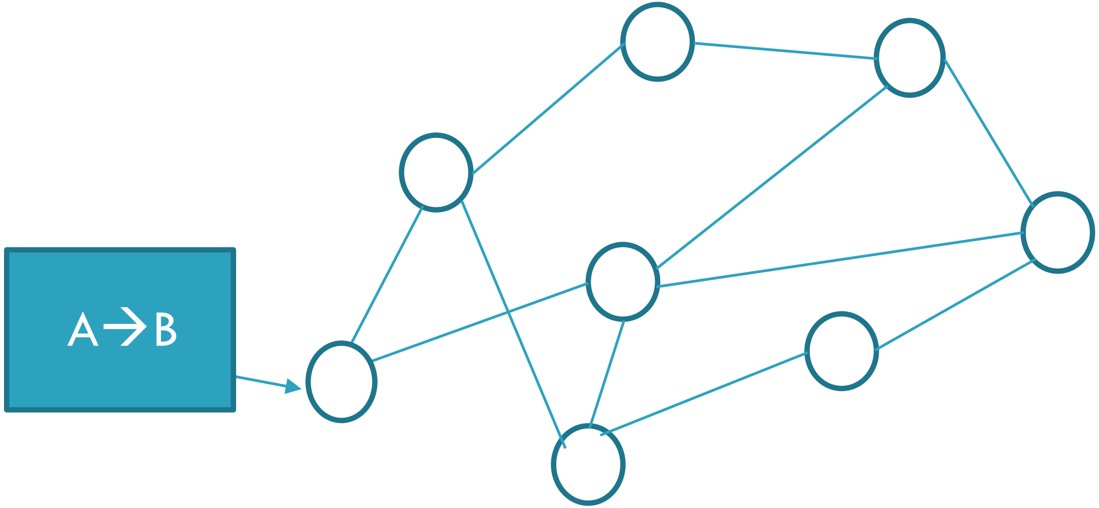
- ○ Real-time verification is not safe (need 1 hour of delay)
- ○ Throughput is low (7 tx/sec)

accenture
High performance. Delivered.
intel
JPMorgan Chase & Co.
IBM
NEC
SAMSUNG
Credit Suisse
Bank of England
vmware
cisco
UBS
Bank of America
Morgan Stanley

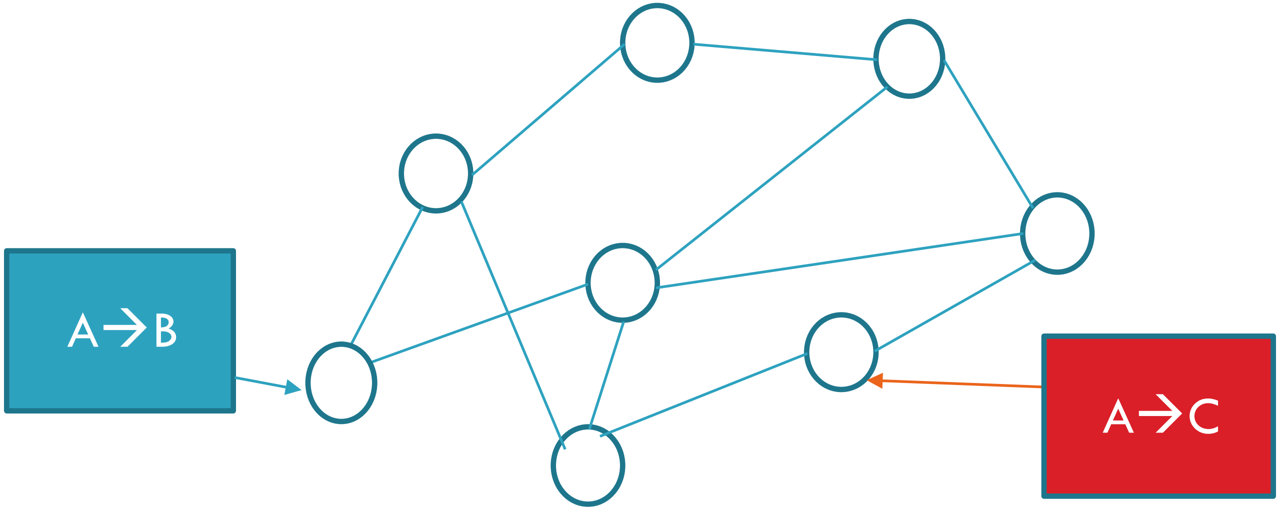
Talk Outline

- **Bitcoin and its limitations**
- Strawman design: PBFTCoin
- Opening the consensus group
- From MACs to Collective Signing
- Decoupling transaction verification from leader election
- Performance Evaluation
- Future work and conclusions

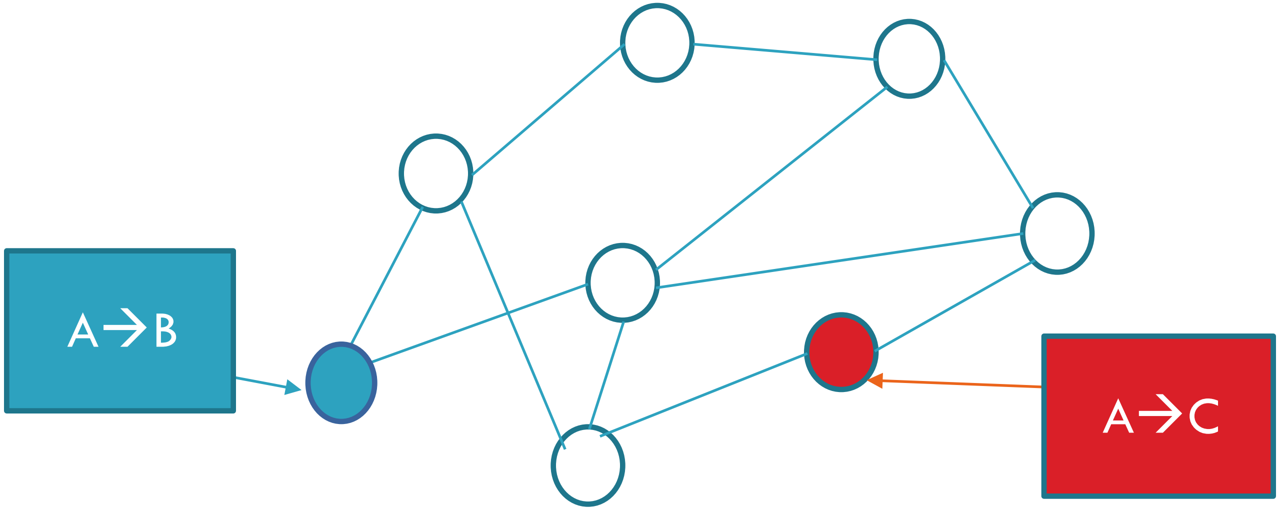
Transaction Verification in Bitcoin



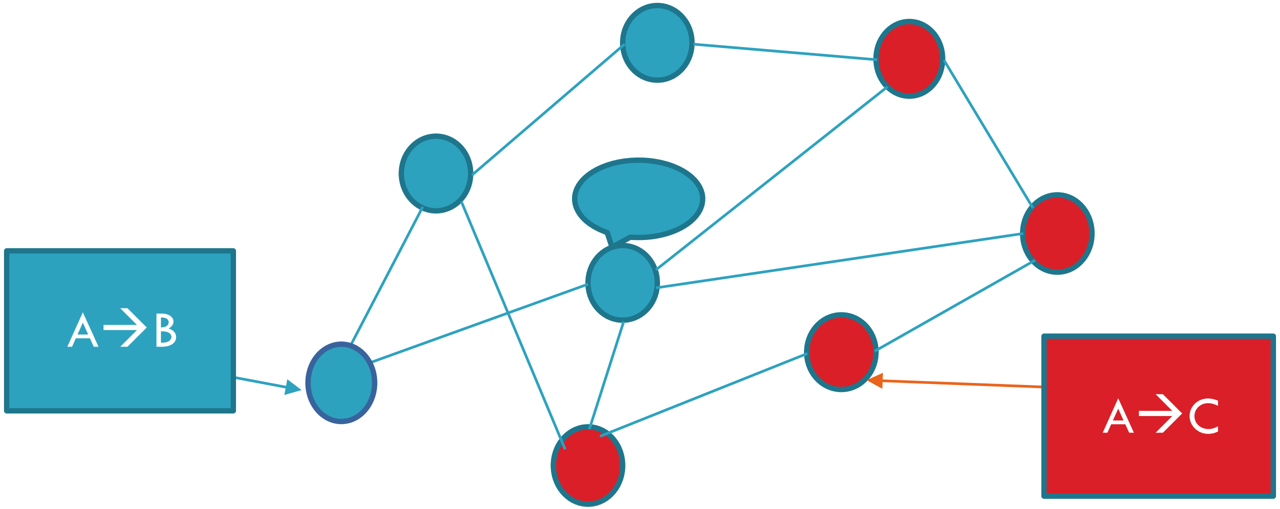
Transaction Conflicts



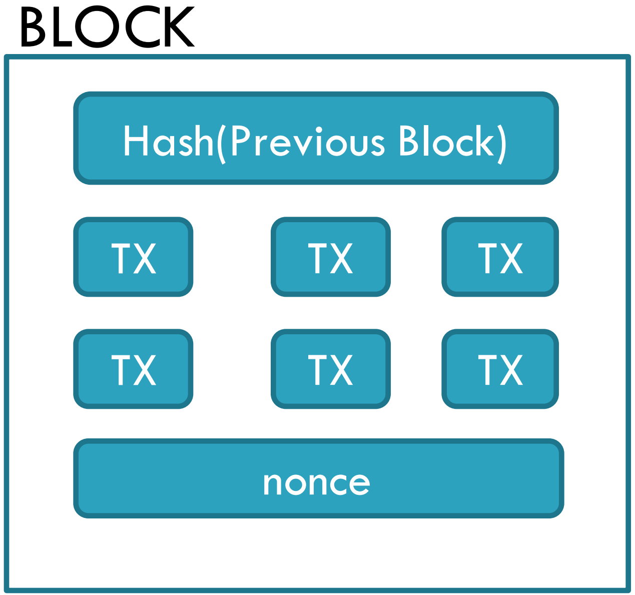
Transaction Conflicts



Resolving Conflicts



Proof-of-Work



H(Block, nonce=0) =abc3426fe31233

H(Block, nonce=1) =fe541200abc229

H(Block, nonce=2) =0bc3429831233

.

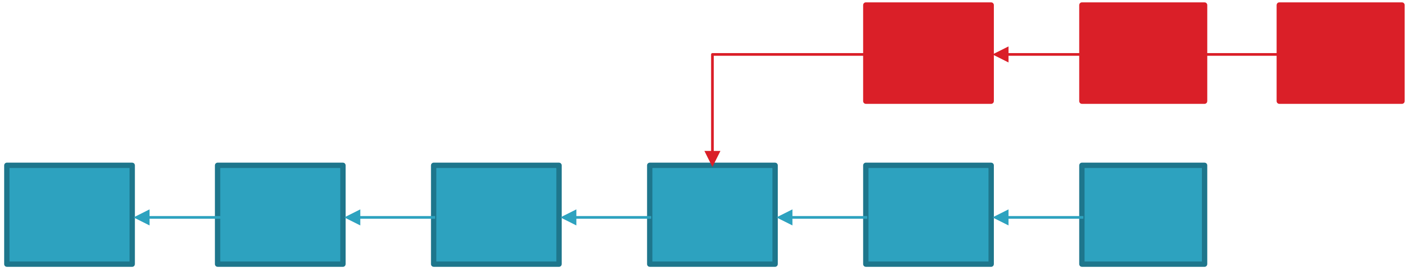
.

.

.

H(Block, nonce=2^9) =0000fed98312

The Blockchain



Problem Statement

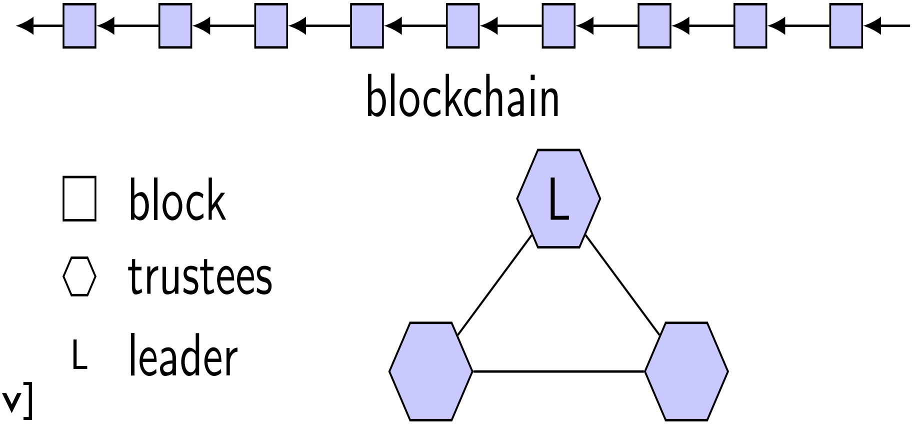
1. In Bitcoin there is no verifiable commitment of the system that a block will persist
   - Clients rely on probabilities to gain confidence.
   - Probability of successful fork-attack decreases exponentially

Talk Outline

- Bitcoin and its limitations
- **Strawman design: PBFTCoin**
- Opening the consensus group
- From MACs to Collective Signing
- Decoupling transaction verification from leader election
- Performance Evaluation
- Future work and conclusions

Strawman Design: PBFTCoin

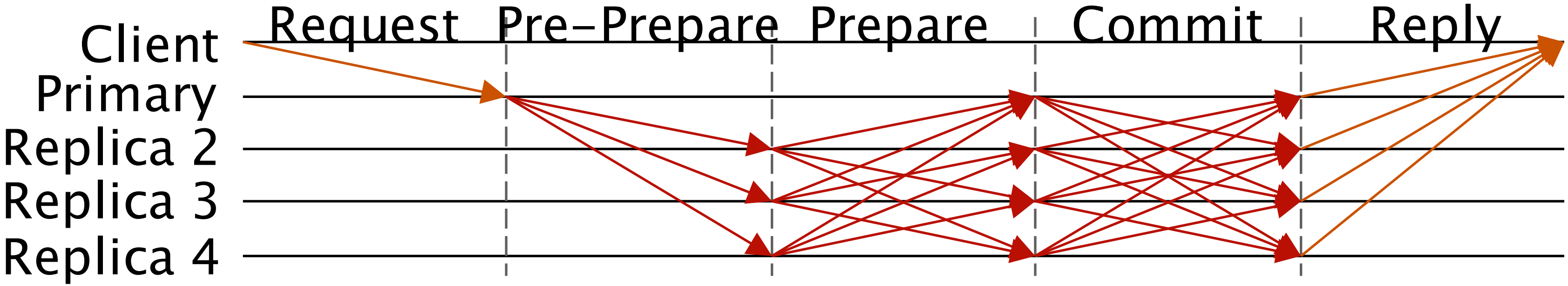
- **3f+1** fixed “trustees” running PBFT* to withstand **f** failures
- Non-probabilistic strong consistency
  - Low latency
- No forks/inconsistencies
  - No double-spending



*Practical Byzantine Fault Tolerance [Castro/Liskov]

Strawman Design: PBFTCoin

- Problem: Needs a static consensus group
- Problem: Scalability
  - $O(n^2)$ communication complexity
  - $O(n)$ verification complexity
  - Absence of third-party verifiable proofs (due to MACs)

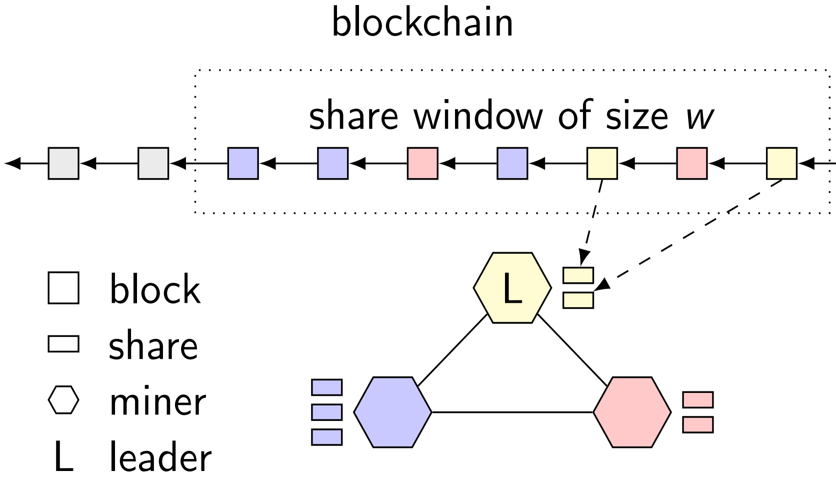


Talk Outline

- Bitcoin and its limitations
- Strawman design: PBFTCoin
- **Opening the consensus group**
- From MACs to Collective Signing
- Decoupling transaction verification from leader election
- Performance Evaluation
- Future work and conclusions

Opening the Consensus Group

- PoW against Sybil attacks
- One share per block
  - % of shares ∝ hash-power
- Window mechanism
  - Protect from inactive miners



Talk Outline

- Bitcoin and its limitations
- Strawman design: PBFTCoin
- Opening the consensus group
- **From MACs to Collective Signing**
- Decoupling transaction verification from leader election
- Performance Evaluation
- Future work and conclusions

From MACs to Signing

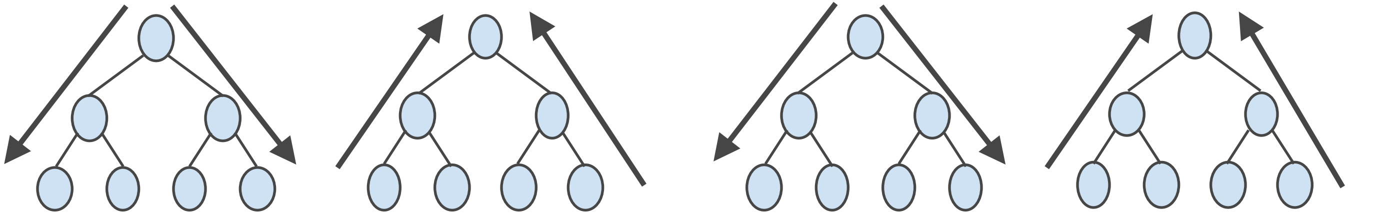
- Substitute MACs with public-key cryptography
  - ECDSA provides more efficiency
  - Third-party verifiable
  - PoW Blockchain as PKI
  - Enables sparser communication patterns (ring or star topologies)

From MACs to Collective Signing

- Can we do better than O(n) communication complexity?
  - Multicast protocols transmit information in O(log n)
  - Use trees!!
- Can we do better than O(n) complexity to verify?
  - Schnorr multisignatures could be verified in O(1)
  - Use aggregation!!
- Schnorr multisignatures + communication trees
  = Collective Signing [Syta et all, IEEE S&P '16]

CoSi

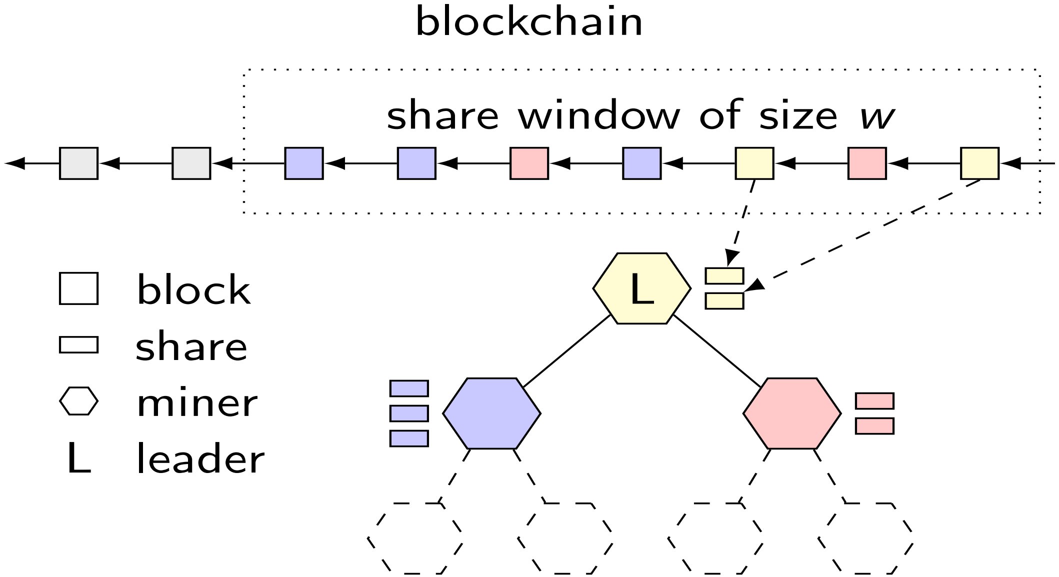
- Efficient collective signature, verifiable as a simple signature
  - 80 bytes instead of 9KB for 144* co-signers (Ed25519)



* Number of ~10-minute blocks in 1-day time window

Discussion

- CoSi is not a BFT protocol
- PBFT can be implemented over two subsequent CoSi rounds
  - Prepare round
  - Commit round



Problem Statement

1. In ~~Bitcoin~~ ByzCoin there is ~~no~~ a verifiable commitment of the system that a block will persist
2. Throughput is limited by forks
   - Increasing block size increases fork probability
   - Liveness exacerbation

Talk Outline

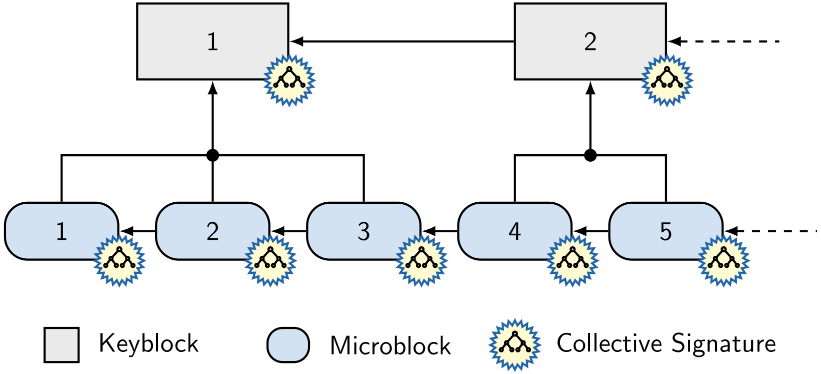
- Bitcoin and its limitations
- Strawman design: PBFTCoin
- Opening the consensus group
- From MACs to Collective Signing
- **Decoupling transaction verification from leader election**
- Performance Evaluation
- Future work and conclusions

Bitcoin-NG [Eyal et all, NSDI ’16]

- Makes the observation that block mining implement two distinct functionalities
  - Transaction verification
  - Leader election
- But, Bitcoin-NG inherits many of Bitcoin’s problems
  - Double-spending
  - Leader is checked after his epoch ends

Decoupling Transaction Verification from Leader Election

- Key blocks:
  - PoW & share value
  - Leader election
- Microblocks:
  - Validating client transactions
  - Issued by the leader



Talk Outline

- Bitcoin and its limitations
- Strawman design: PBFTCoin
- Opening the consensus group
- From MACs to Collective Signing
- Decoupling transaction verification from leader election
- **Performance Evaluation**
- Future work and conclusions

Performance Evaluation

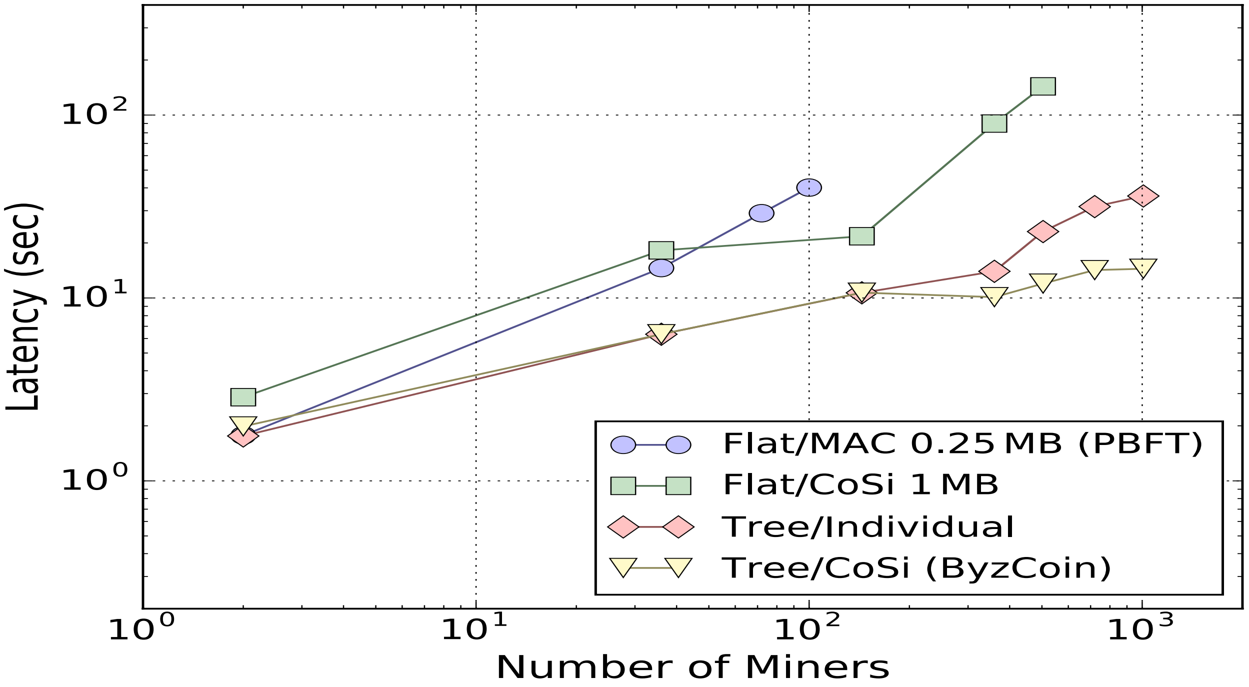
- Experiments run on DeterLab network testbed
  - Up to 1,008* miners multiplexed atop 36 machines
  - Impose 200 ms roundtrip latencies between all servers
  - Impose 35 Mbps bandwidth per miner

* 1008 = # of ~10-minute key-blocks in 1-week time window

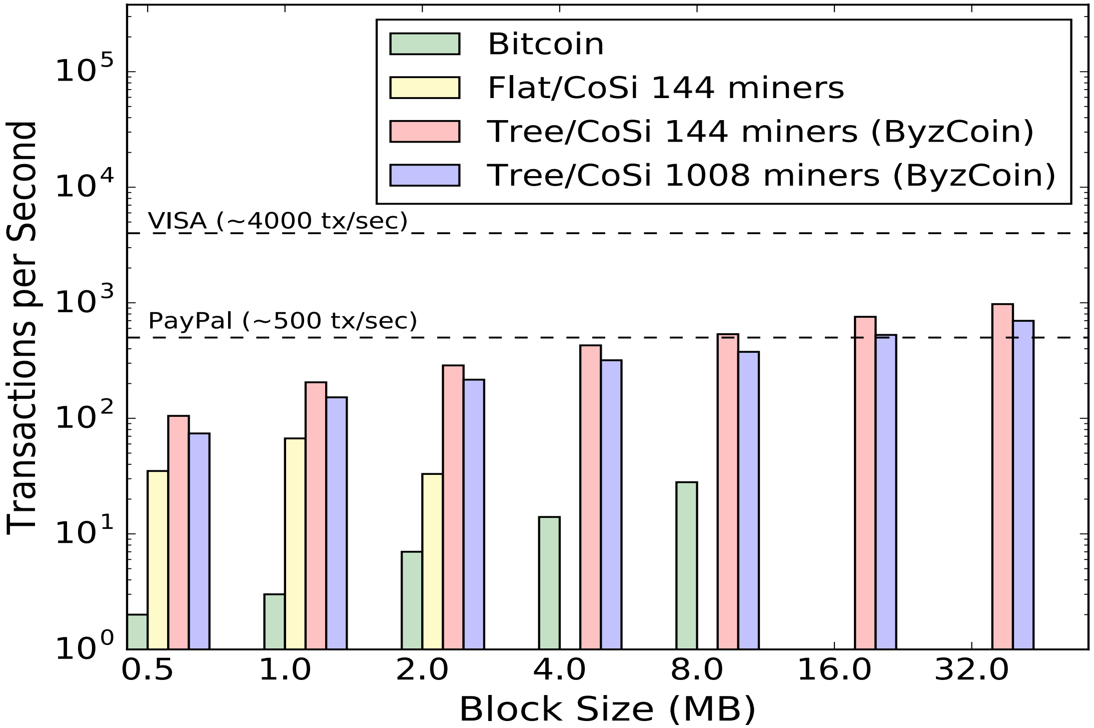
Performance Evaluation

- Key questions to evaluate:
  - What size consensus groups can ByzCoin scale to?
  - What transaction throughput can it handle?

Consensus Latency



Throughput


Bitcoin
Flat/CoSi 144 miners
Tree/CoSi 144 miners (ByzCoin)
Tree/CoSi 1008 miners (ByzCoin)
VISA (~4000 tx/sec)
PayPal (~500 tx/sec)
Transactions per Second
10^0
10^1
10^2
10^3
10^4
10^5
0.5
1.0
2.0
4.0
8.0
16.0
32.0
Block Size (MB)

Talk Outline

- Bitcoin and its limitations
- Strawman design: PBFTCoin
- Opening the consensus group
- From MACs to Collective Signing
- Decoupling transaction verification from leader election
- Performance Evaluation
- **Future work and conclusions**

Limitations

- Attacker with >= 1/3 of the shares
  - Can trivially censor transactions / DoS the system
  - Can double-spend if he splits the network
- Can currently only scale-up not scale-out
- Leader can exclude miners from the consensus

Future Work

- Alternatives to PoW
- Sharding to enable scaling-out
- Incremental deployment to existing cryptocurrencies
- Fail more gracefully under 33% attacks

Conclusion

- Use Collective Signing to scale BFT protocols
- Use PoW to create hybrid permissionless BFT
- Combine the above with Bitcoin-NG to create ByzCoin
- Demonstrate experimentally its practicality
- ByzCoin increases the security and performance of cryptocurrencies.

Thank you

eleftherios.kokoriskogias@epfl.ch

people.epfl.ch/eleftherios.kokoriskogias

@LefKok