Secure, Confidential Blockchains Providing High Throughput and Low Latency

Lefteris Kokoris-Kogias

EPFL

Lausanne, 27-09-2019


LIVE
bitconnect

Blockchain, Blockchain, Blockchain

- Bring Transparency in a Digital World
- Minimise the need for globally trusted third parties
- Cheeper and faster transactions

Talk Outline

- **Introduction**
- Scalable, Strongly-Consistent Consensus for Bitcoin
- OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding

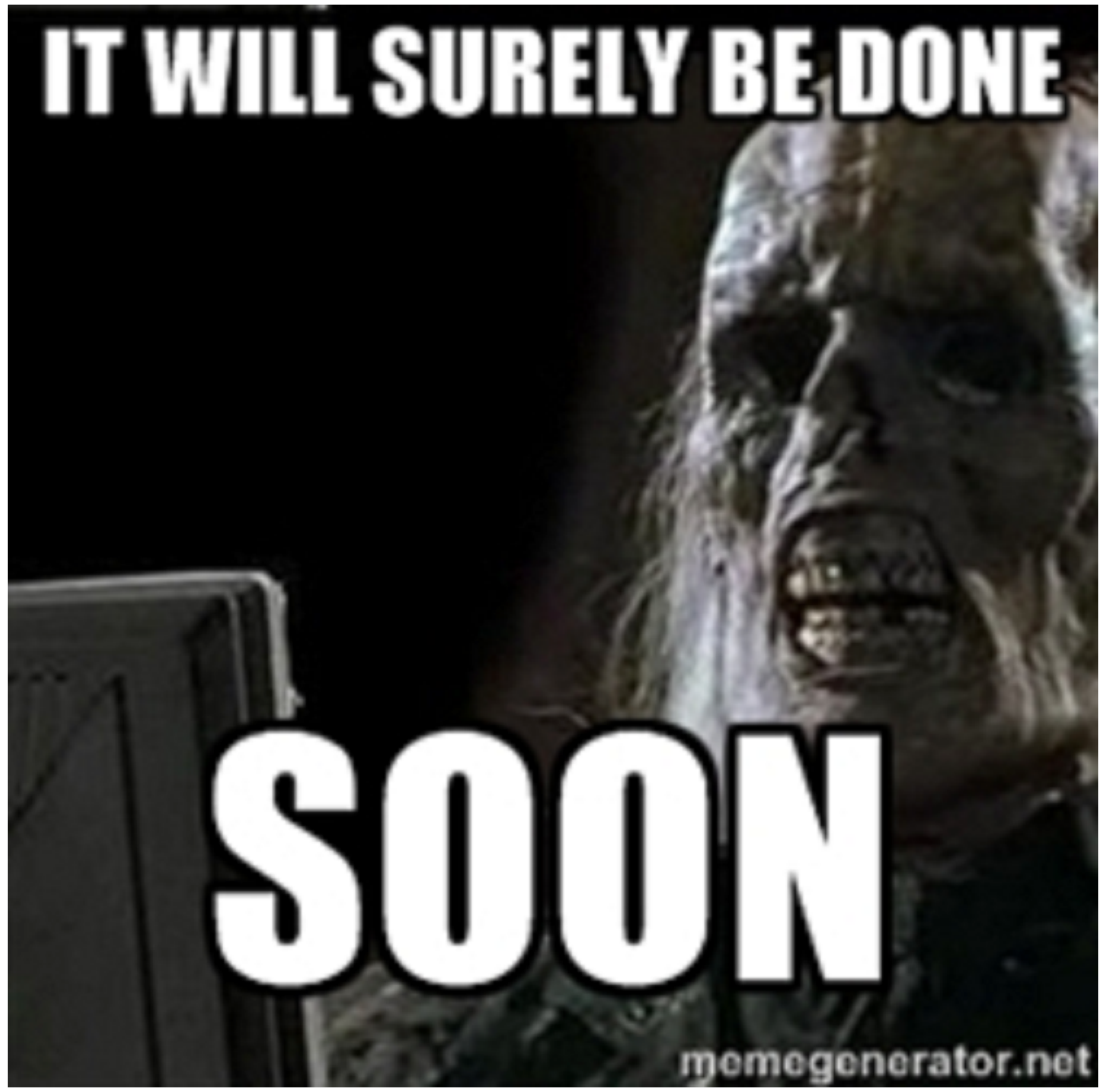
Scaling Blockchains is More Important Than Ever …

CATS RULE THE BLOCKCHAIN, TOO

The ethereum network is getting jammed up because people are rushing to buy cartoon cats on its blockchain

Drawbacks of Bitcoin

- Transaction confirmation delay
  - Bitcoin: Any tx takes >10 mins until being confirmed
- Weak consistency
  - Bitcoin: You are not really certain your tx is committed until you wait >1 hour
- Low throughput
  - Bitcoin: ~7 tx/sec



The Promise of Blockchain

The Potential for Blockchain to Transform Electronic Health Records

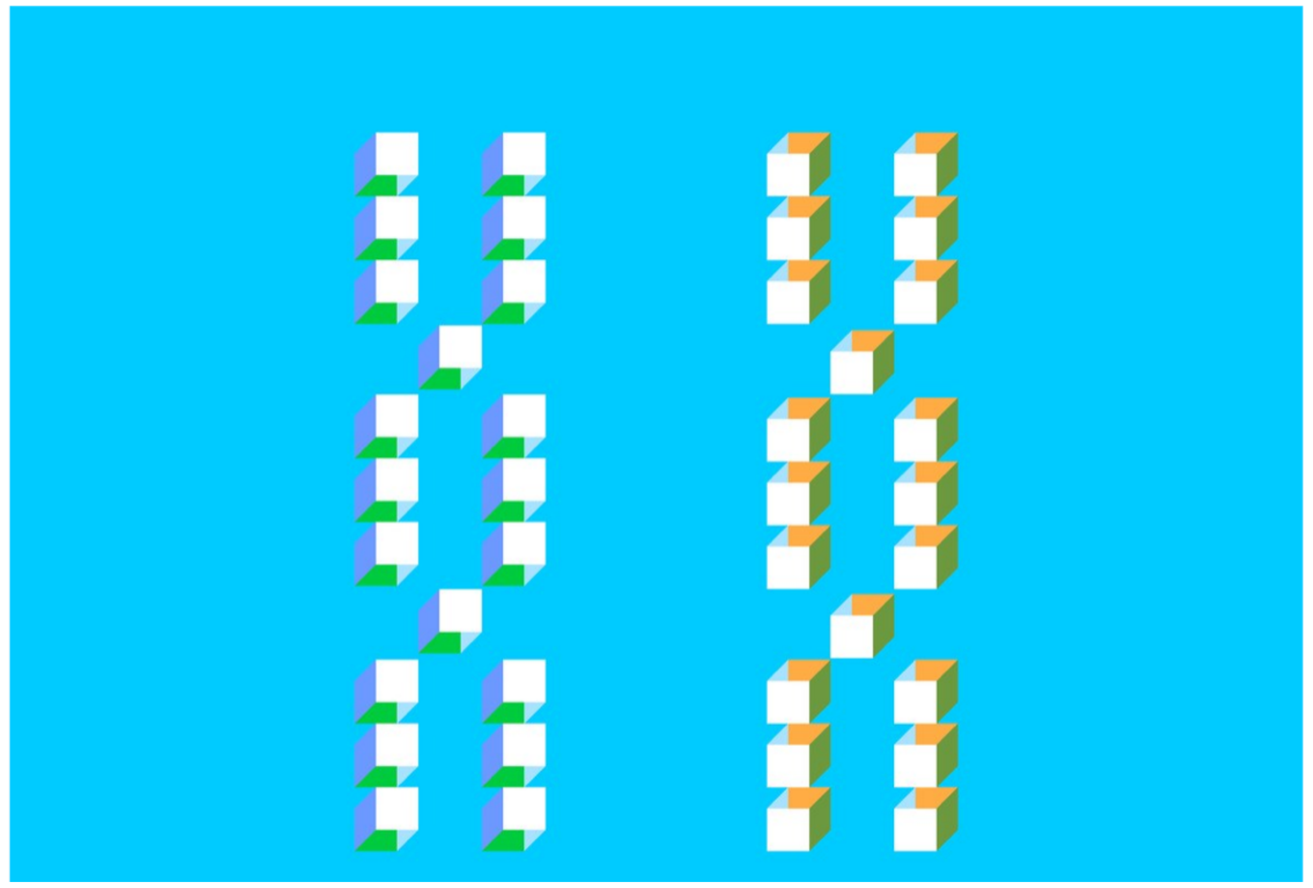
by John D. Halamka, MD, Andrew Lippman, and

MARCH 03, 2017

SAVE SHARE 0 COMMENT TEXT SIZE PRI

ADAM ROGERS SCIENCE 02.21.18 07:00 AM

SOLVE GENOMICS WITH THE BLOCKCHAIN? WHY THE HELL NOT



MEET THE MAN WITH A RADICAL PLAN FOR BLOCKCHAIN VOTING

A new movement says that crypto-voting can purify democracy—and eventually eliminate the need for governments altogether.

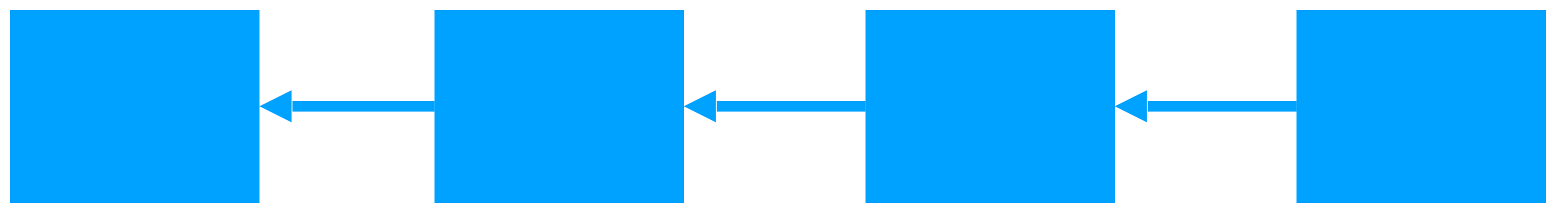
BY ANDREW LEONARD

IN A CAFÉ on the Upper East Side of Manhattan, a one-time videogame developer turned political theorist named Santiago Siri is trying to explain to me how his nonprofit startup world's blockc

Insurance Companies start experimenting with Blockchain technology

August 16, 2018

The Promise of Blockchain



Transparent Decentralized Log

Post encryptions, store keys on cloud

This Thesis

	Scalability	Confidentiality
Open	Oakland ’17,’18 Sec ’16, ’17 HotPETs ‘16	Under Submission
Permissioned	ESORICS ’18	

This Thesis

	Scalability	Confidentiality
Open	Oakland ’17,**’18** Sec **’16**, ’17 HotPETs ‘16	Under Submission
Permissioned	ESORICS ’18	

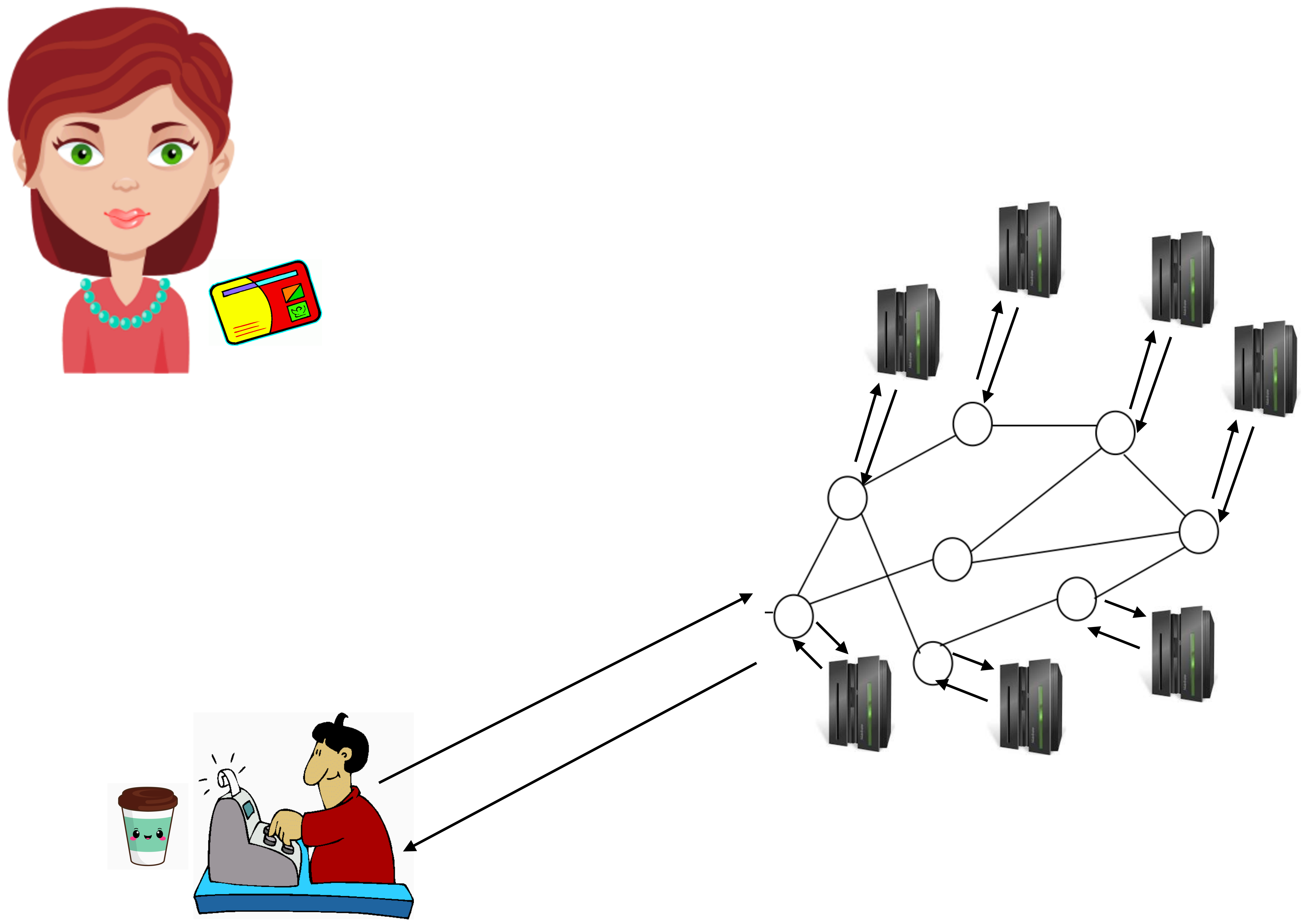
Talk Outline

- Introduction
- **Scalable, Strongly-Consistent Consensus for Bitcoin**
- OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding

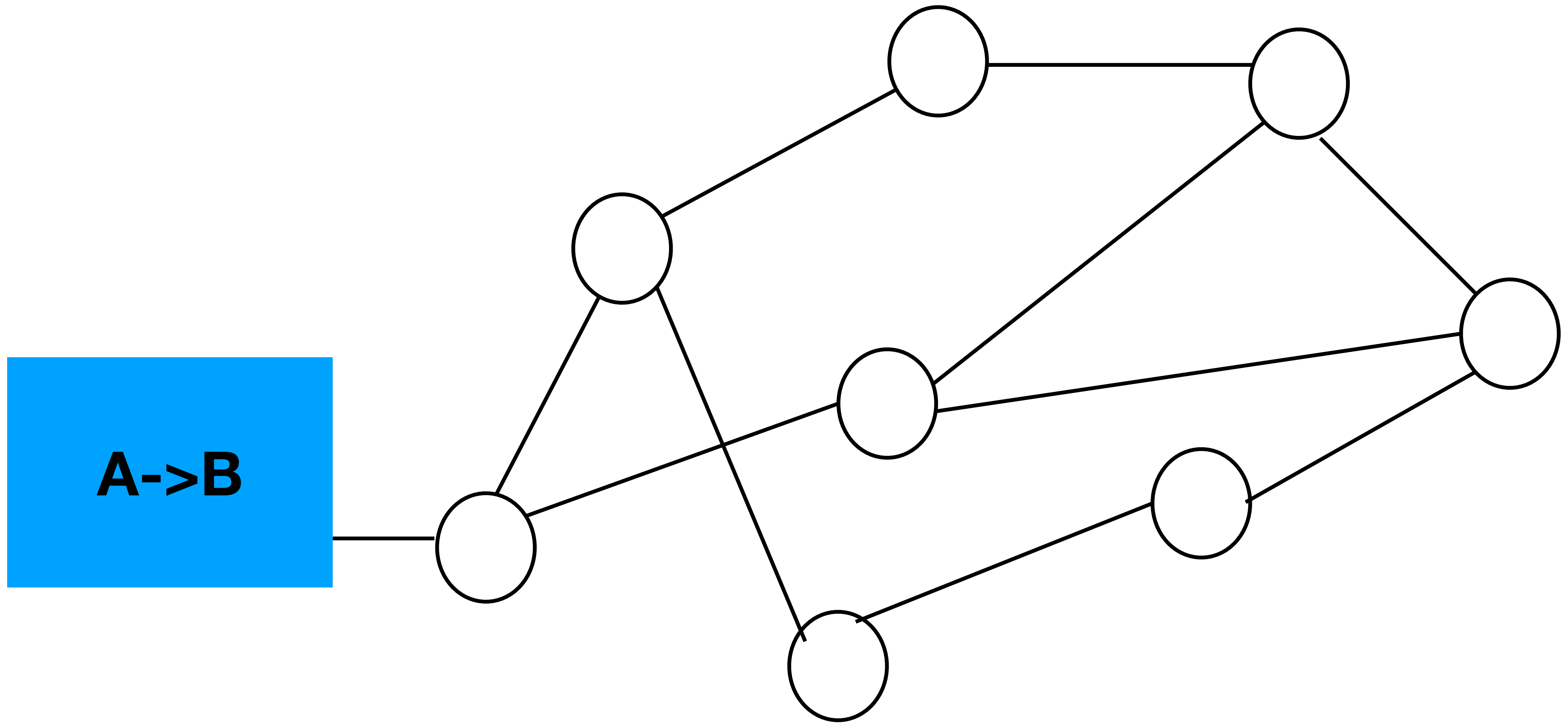
How Bitcoin Works

Traditional Banking

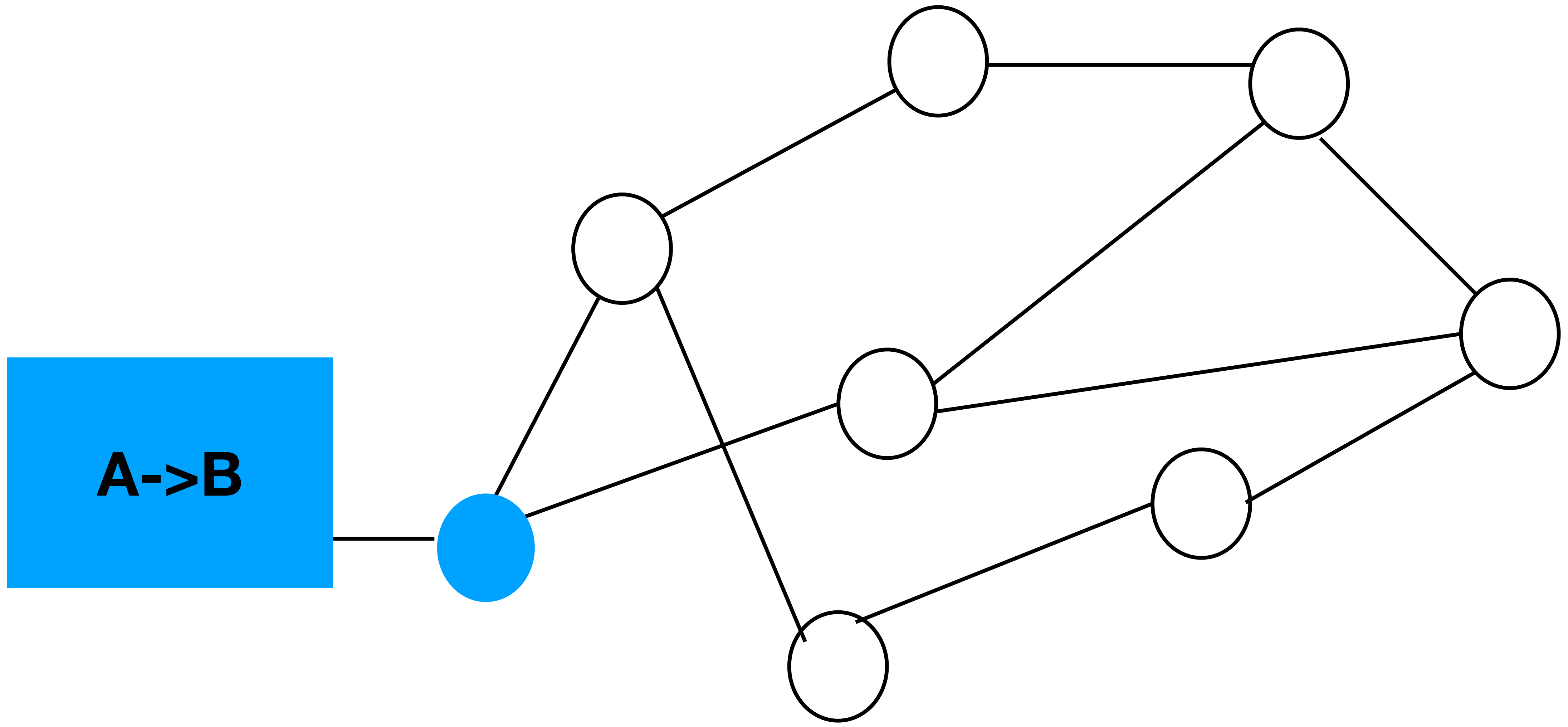
Traditional Banking



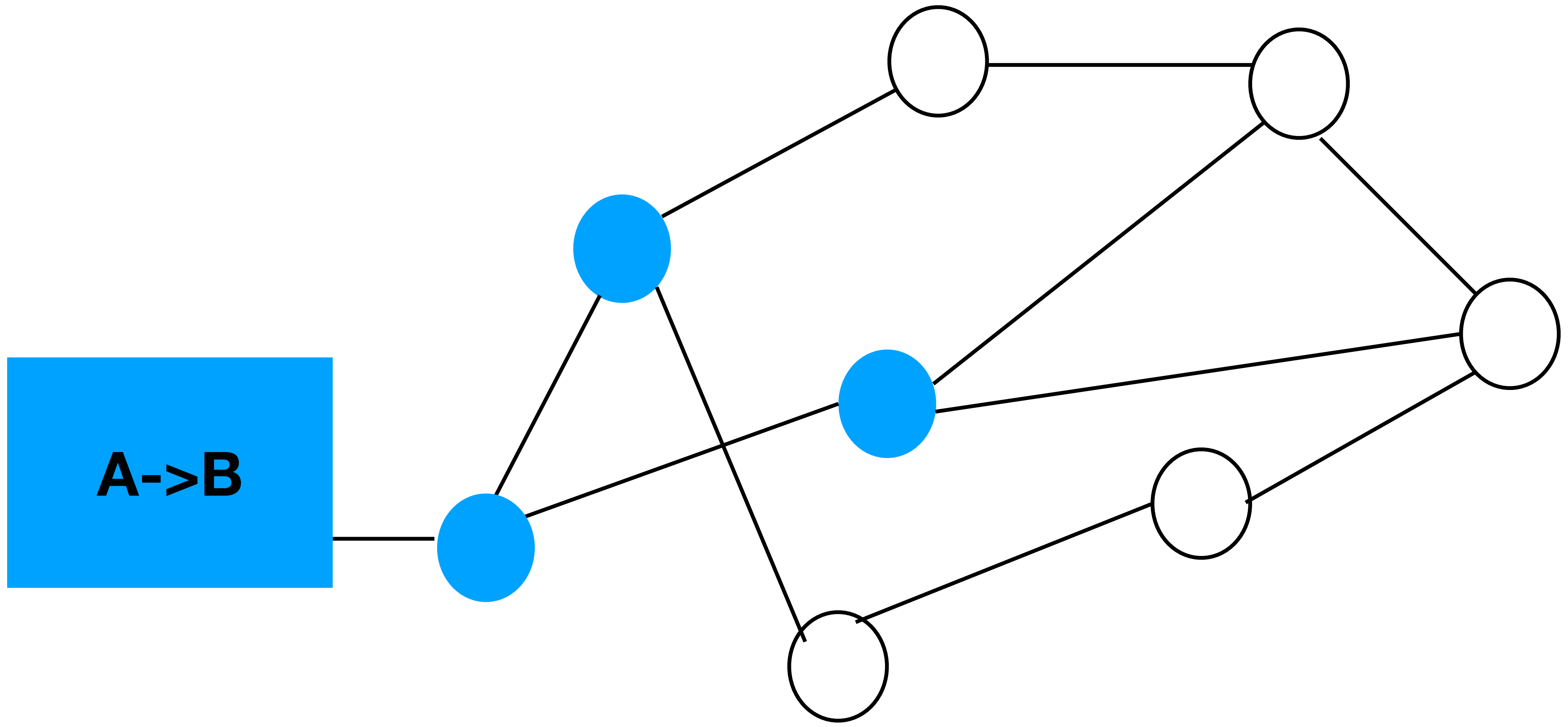
Transaction Verification in Bitcoin



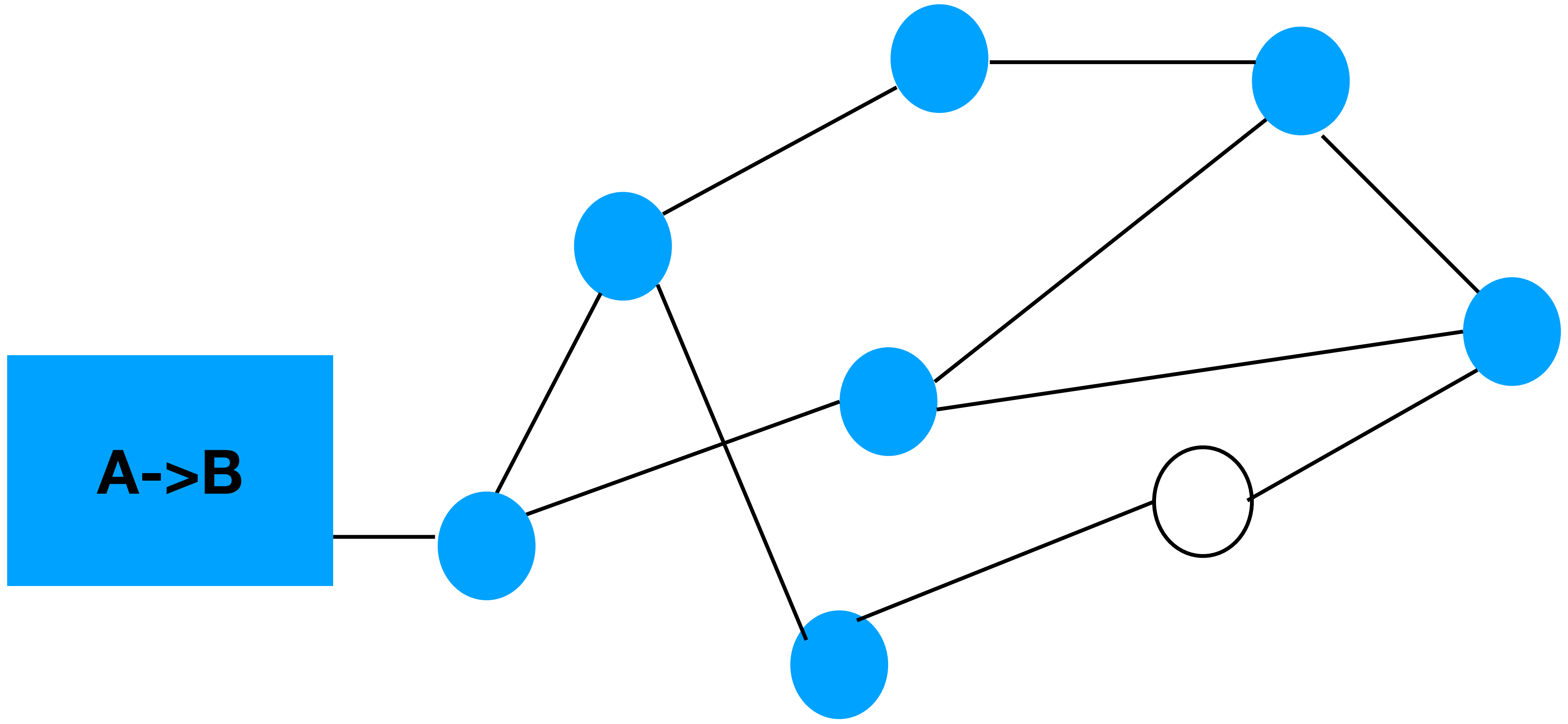
Transaction Verification in Bitcoin



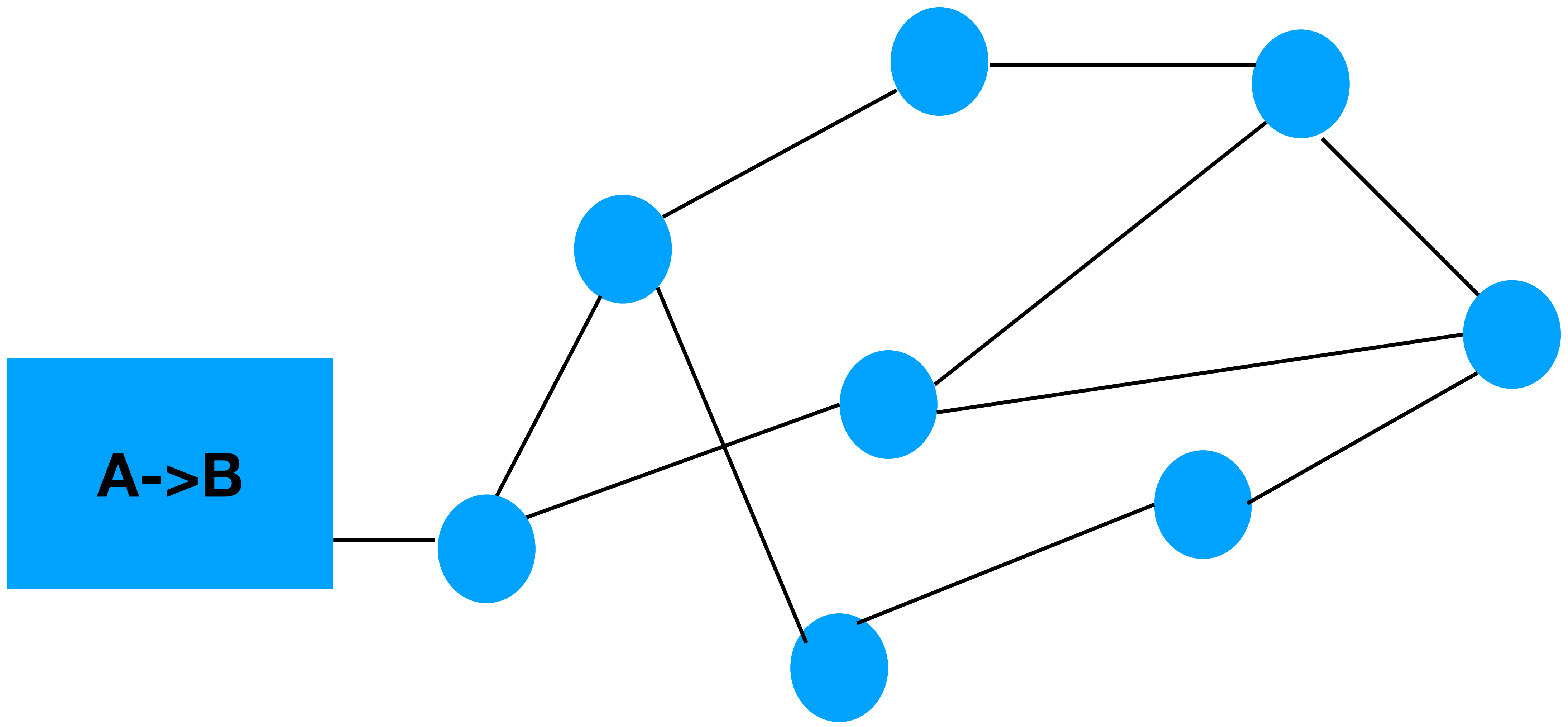
Transaction Verification in Bitcoin



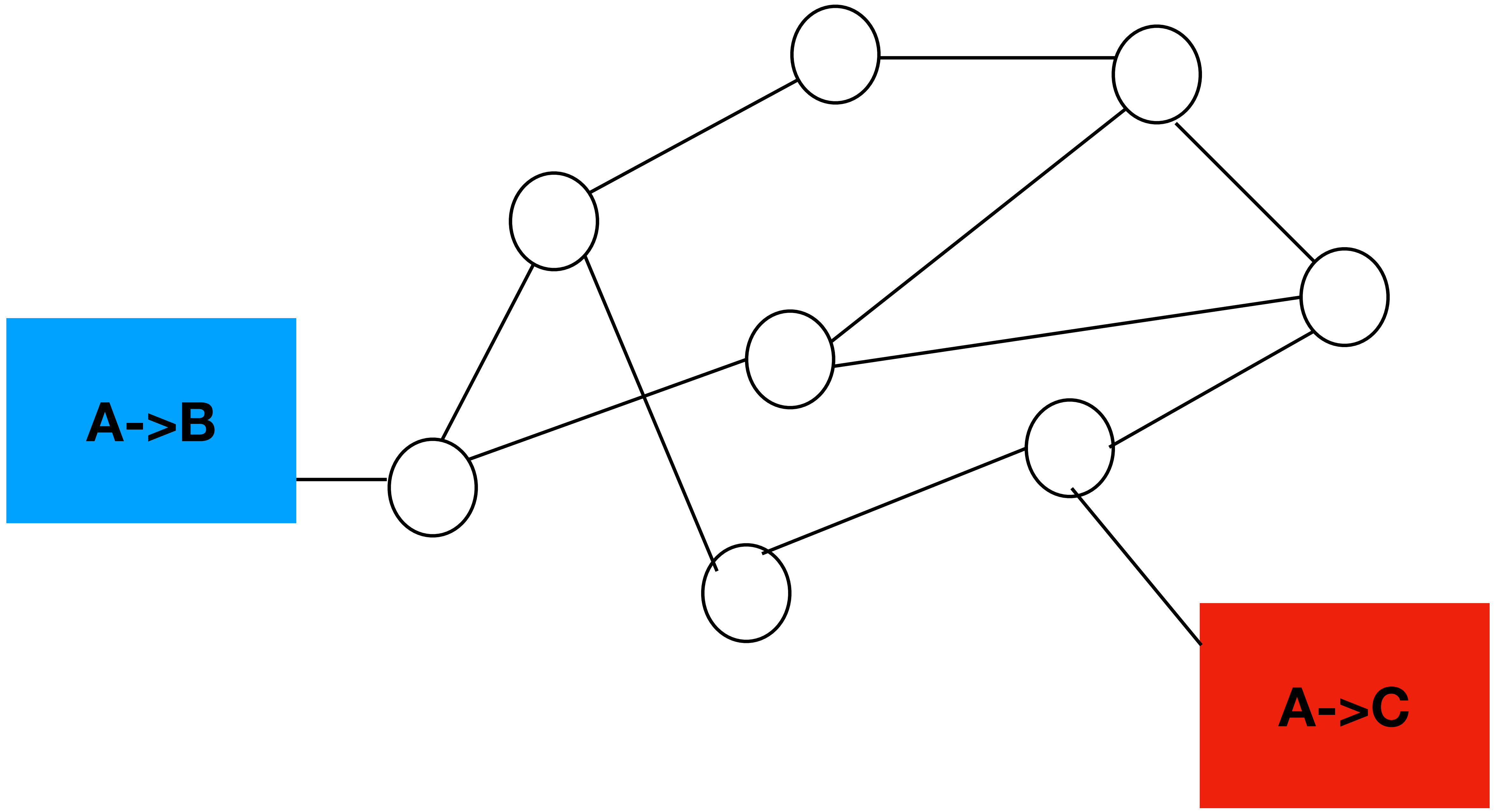
Transaction Verification in Bitcoin



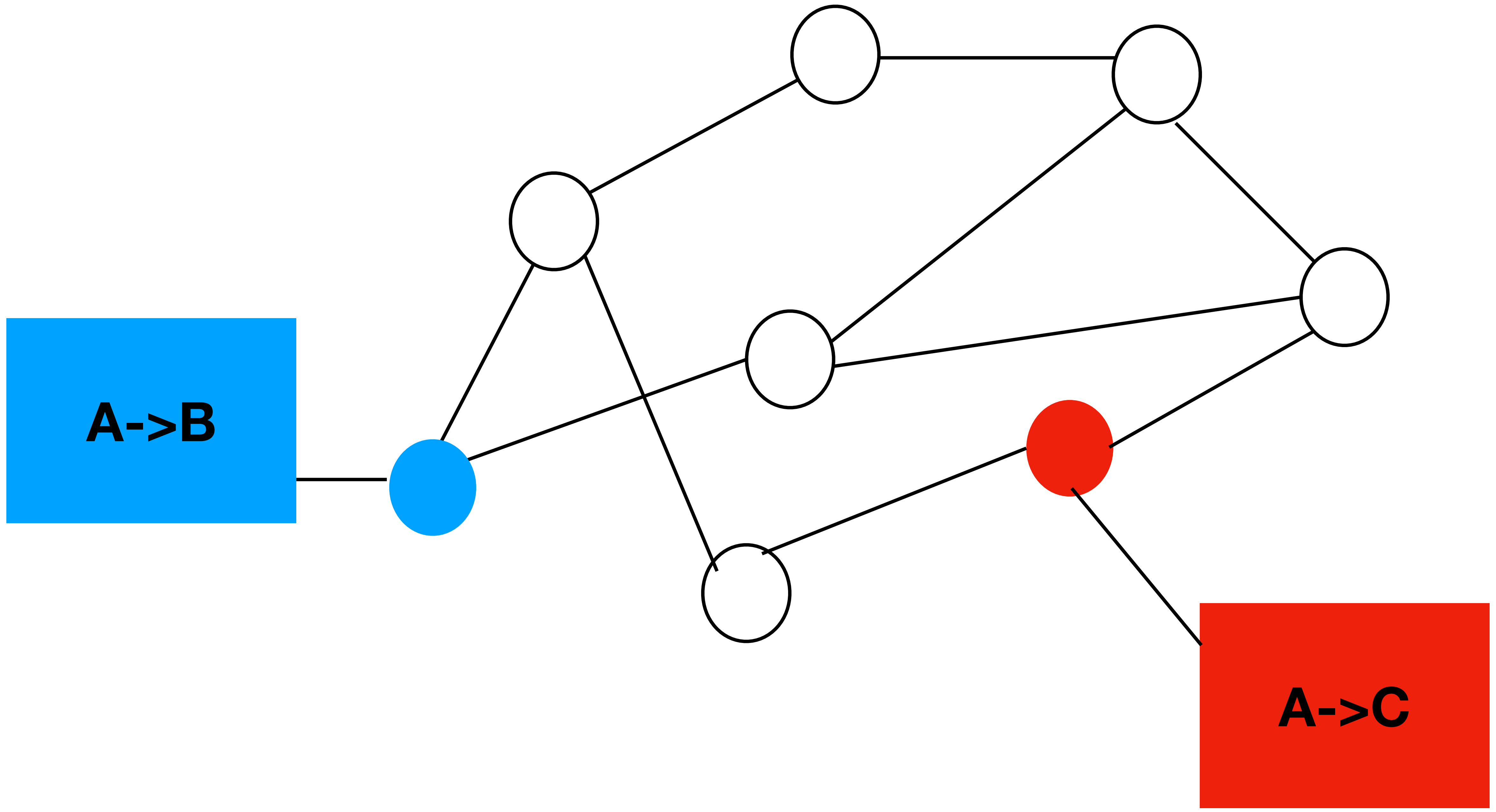
Transaction Verification in Bitcoin



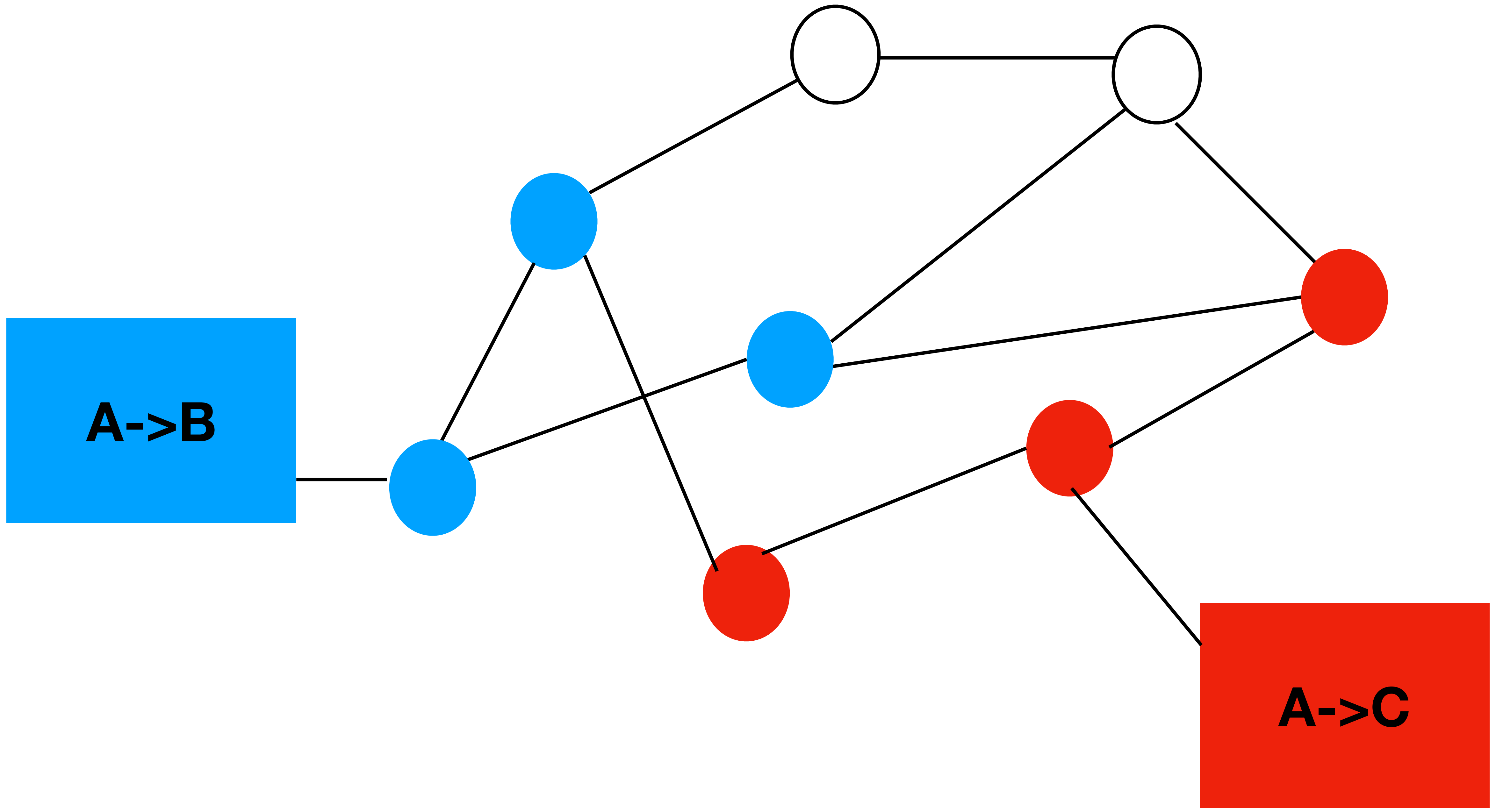
Transaction Verification in Bitcoin



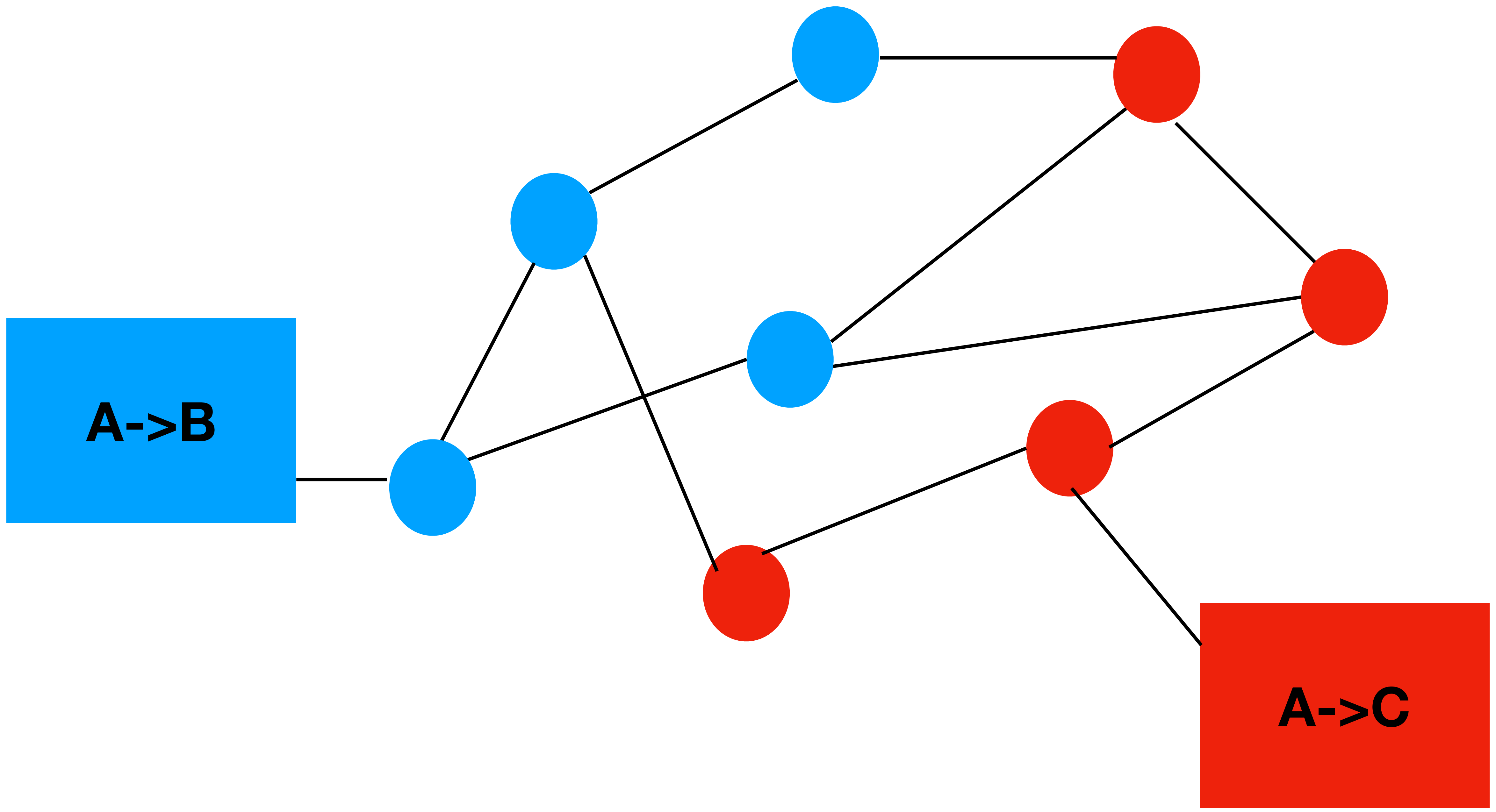
Transaction Verification in Bitcoin



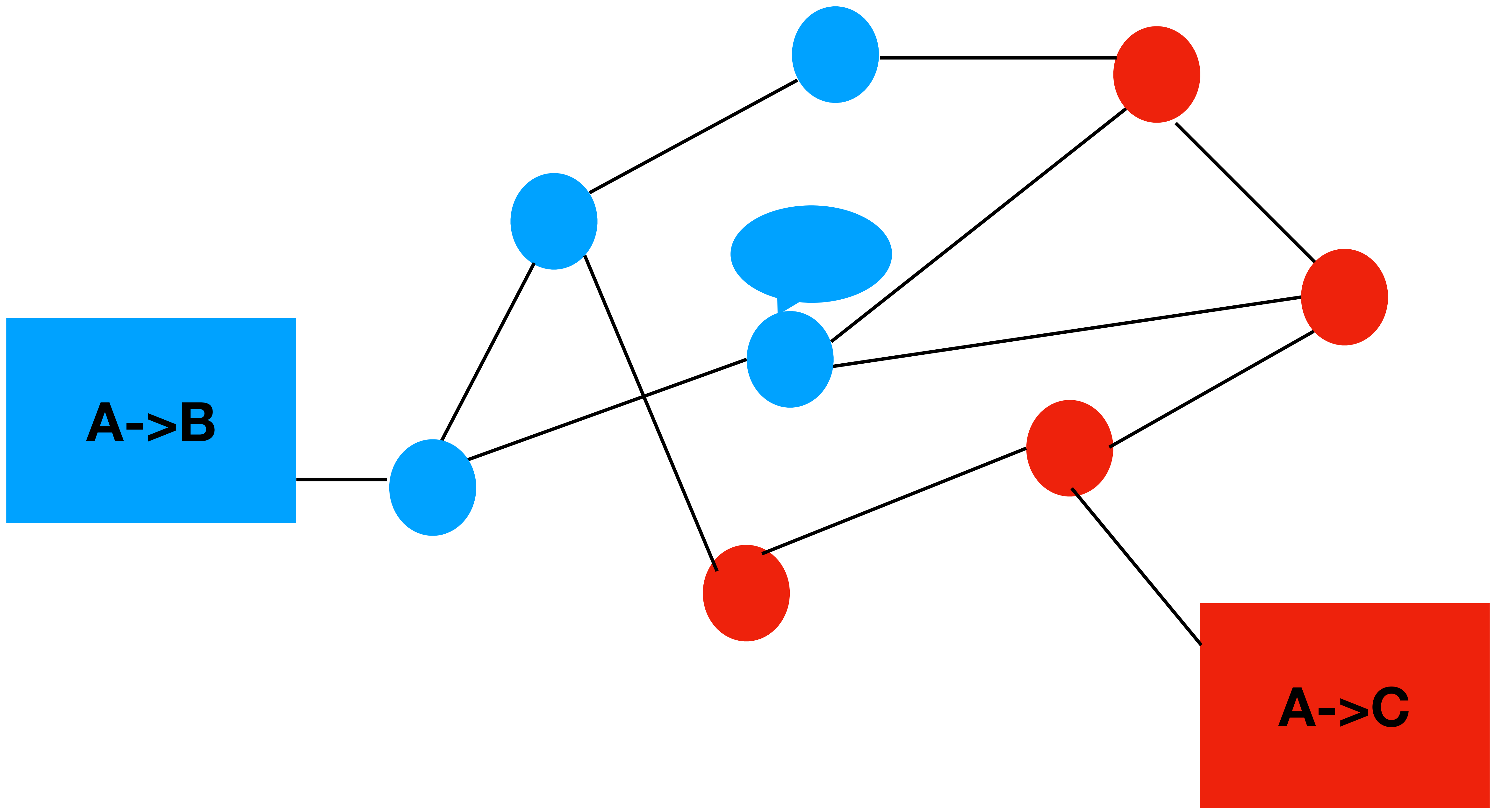
Transaction Verification in Bitcoin



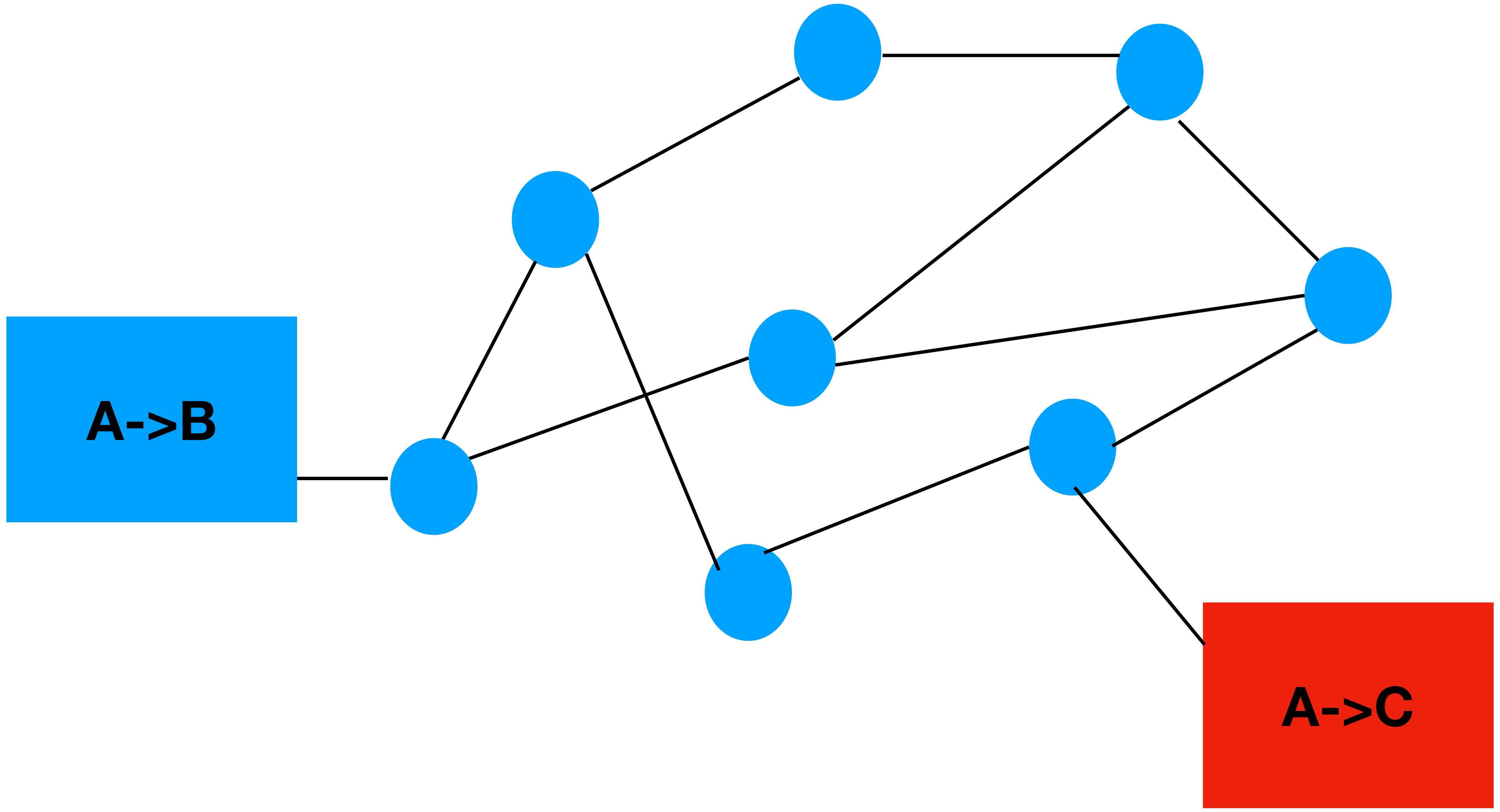
Transaction Verification in Bitcoin



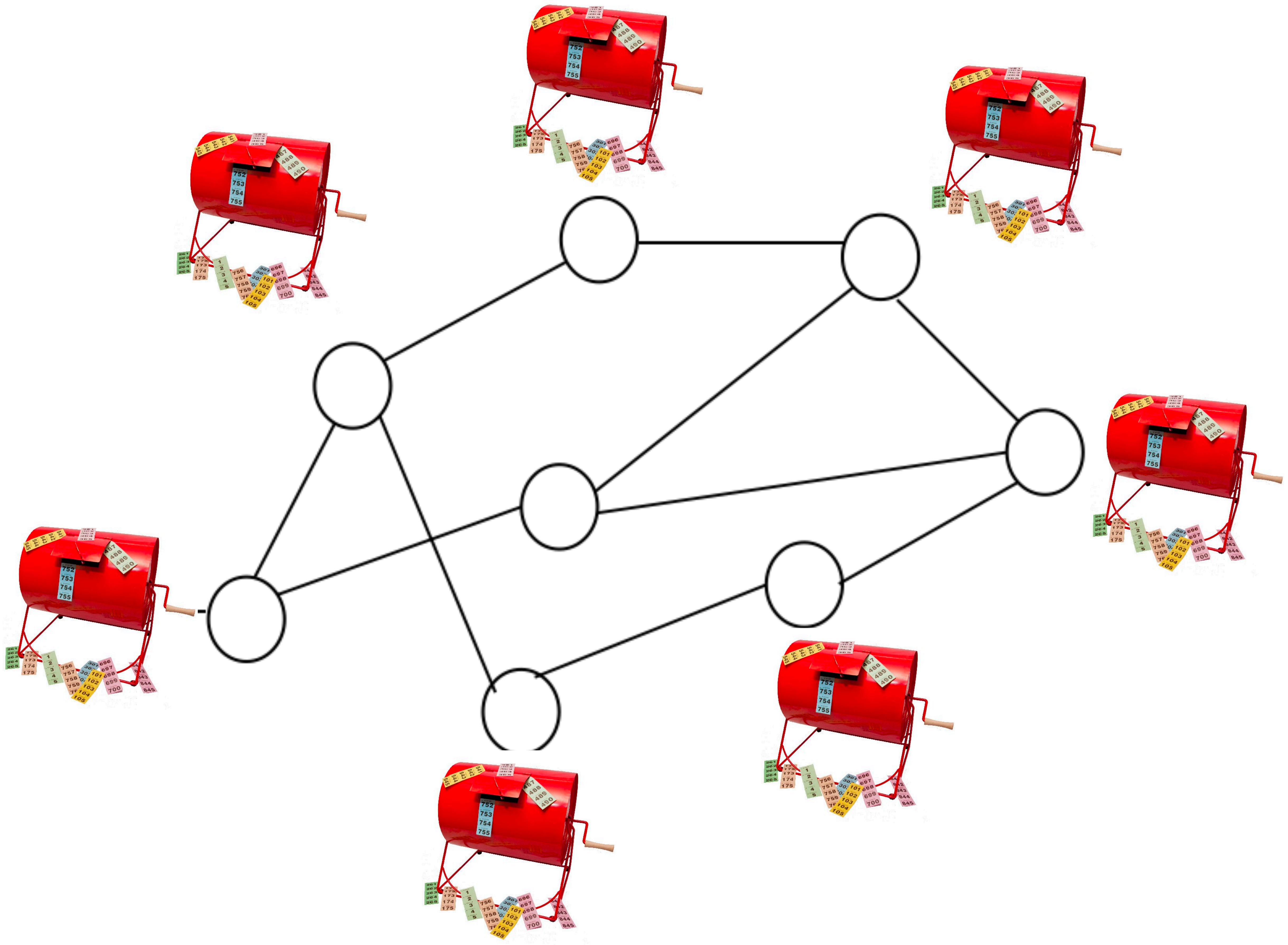
Transaction Verification in Bitcoin



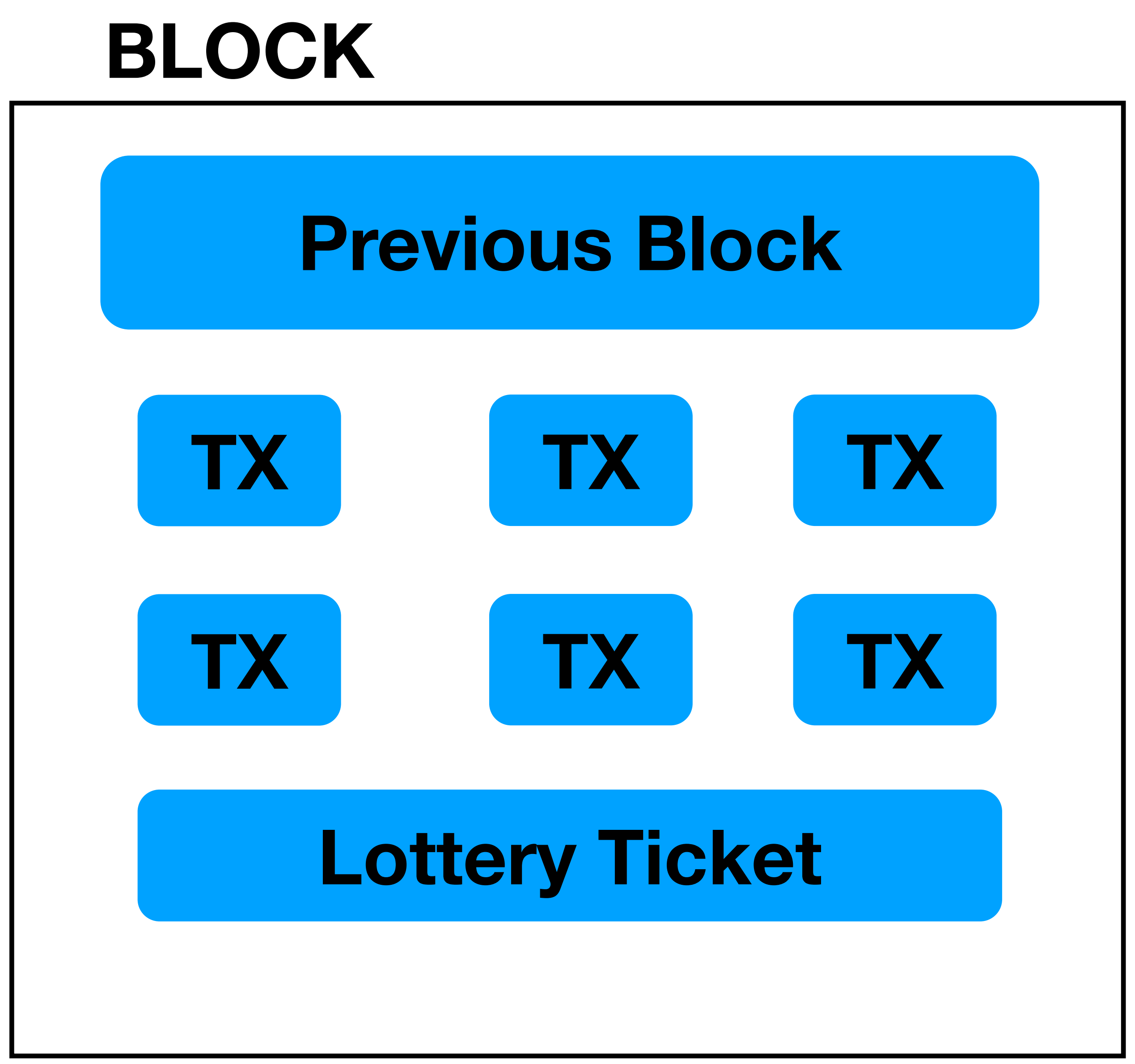
Transaction Verification in Bitcoin



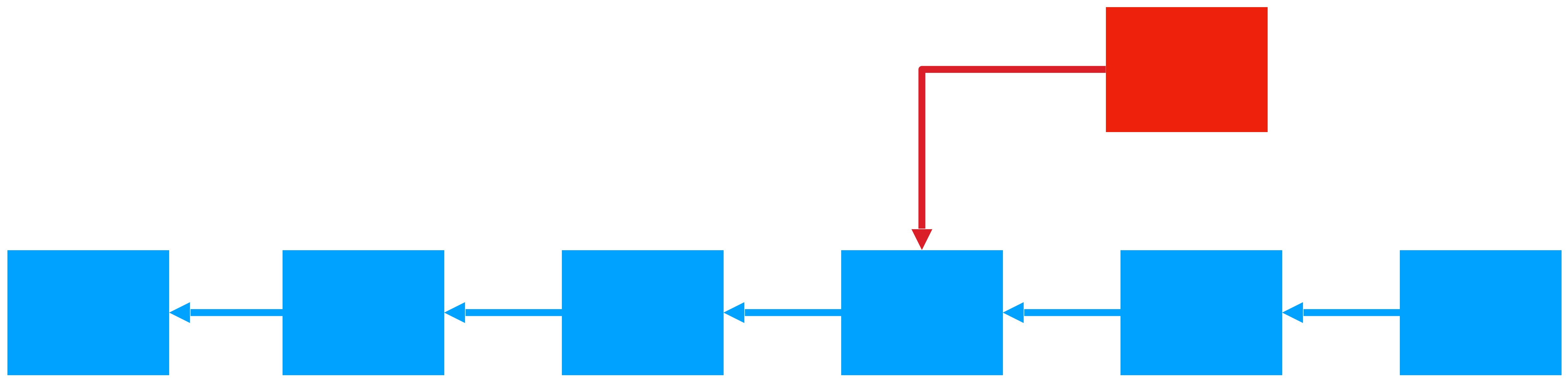
Lottery



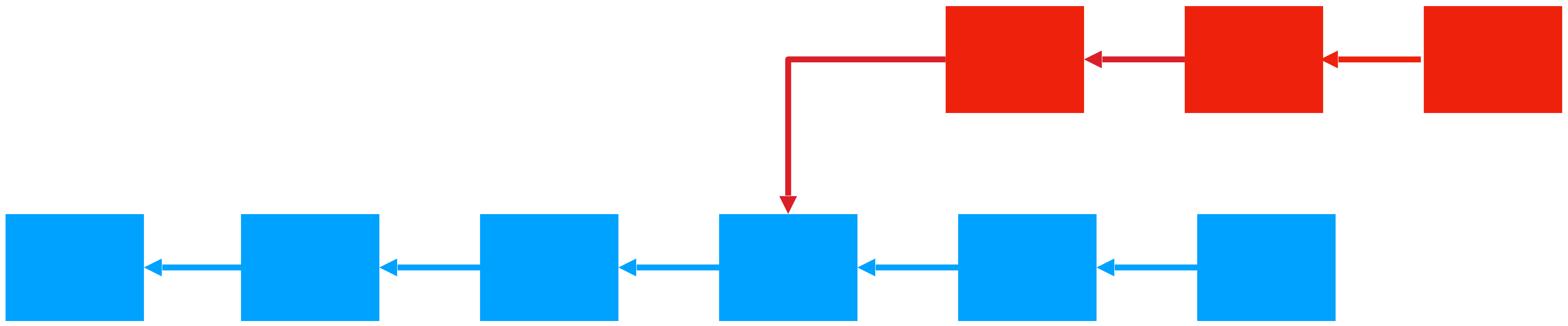
Proof-of-Work



The Blockchain



The Blockchain



Problem Statement

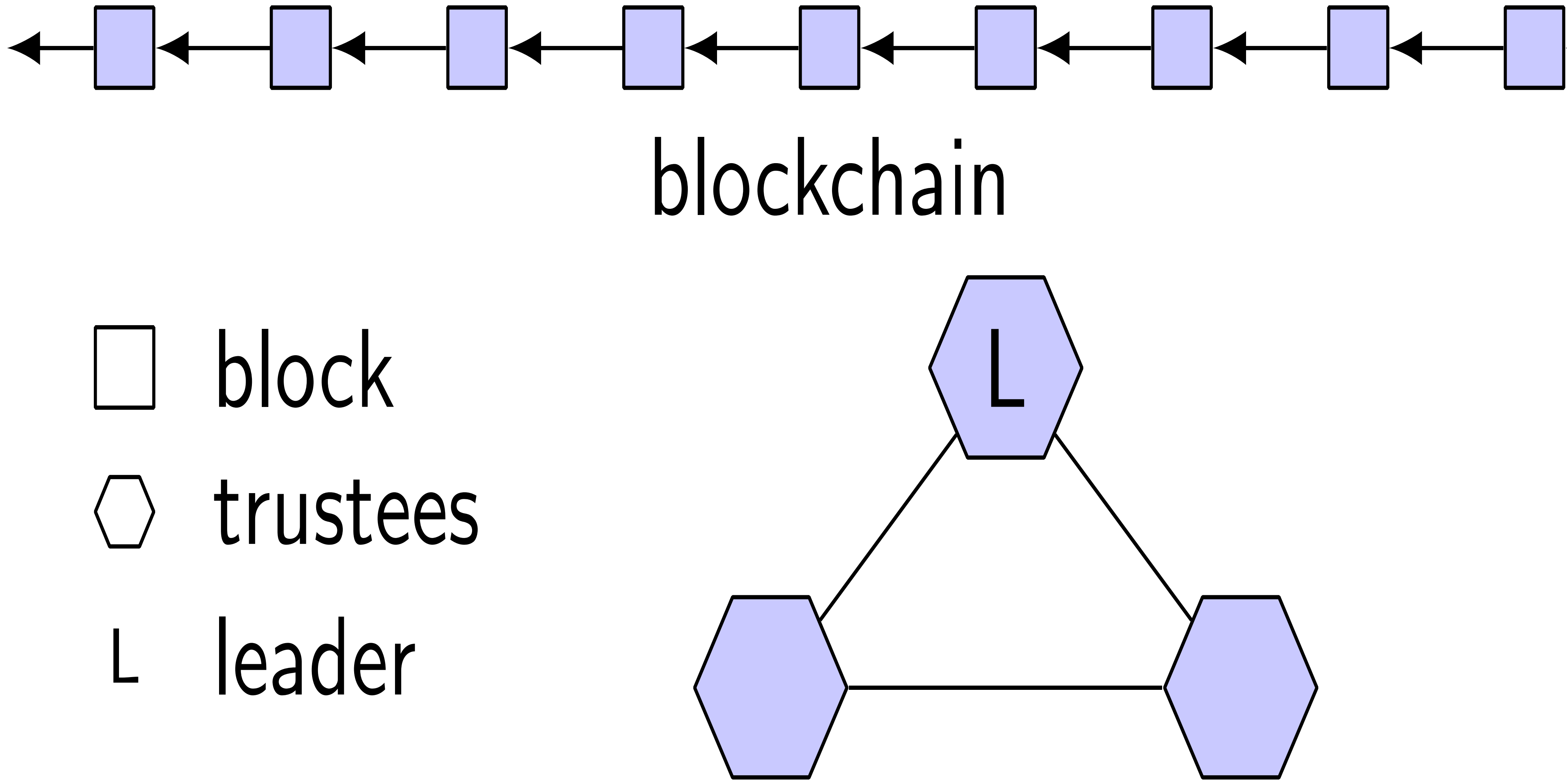
- In Bitcoin there is no verifiable commitment of the system that a block will persist
  - Clients rely on probabilities to gain confidence

Chapter 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

Strawman Design: PBFTCoin

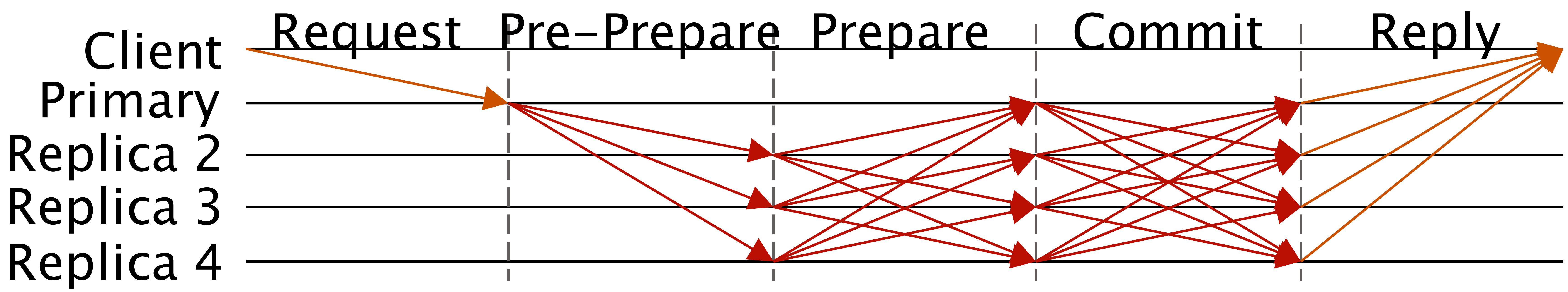
- 3f+1 fixed “trustees” running PBFT* to withstand **f** failures
- Non-probabilistic strong consistency
  - Low latency
- No forks/inconsistencies
  - No double-spending



*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

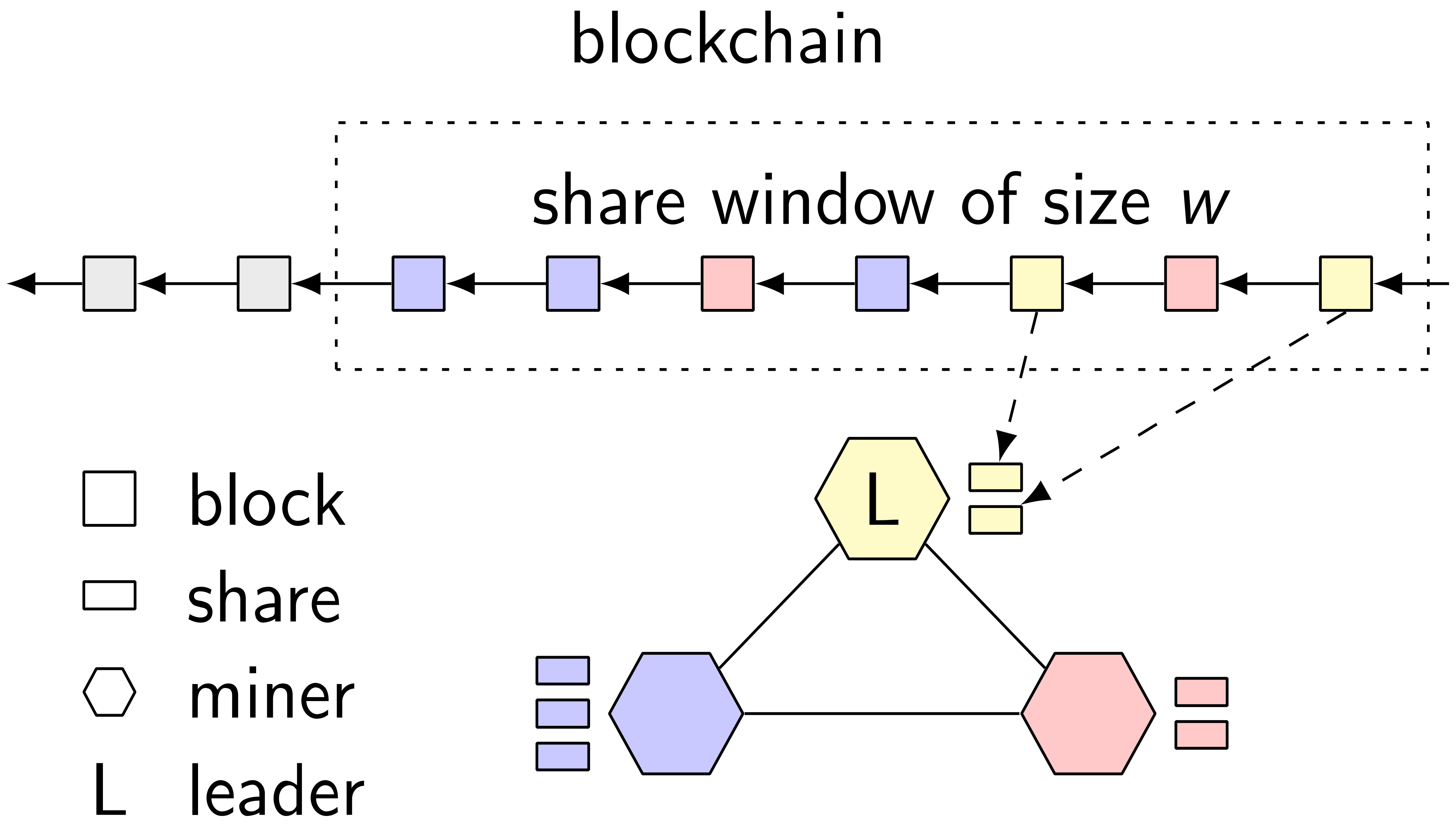


Chapter Outline

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

Opening the Consensus Group

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



Chapter 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

From MACs to Signing

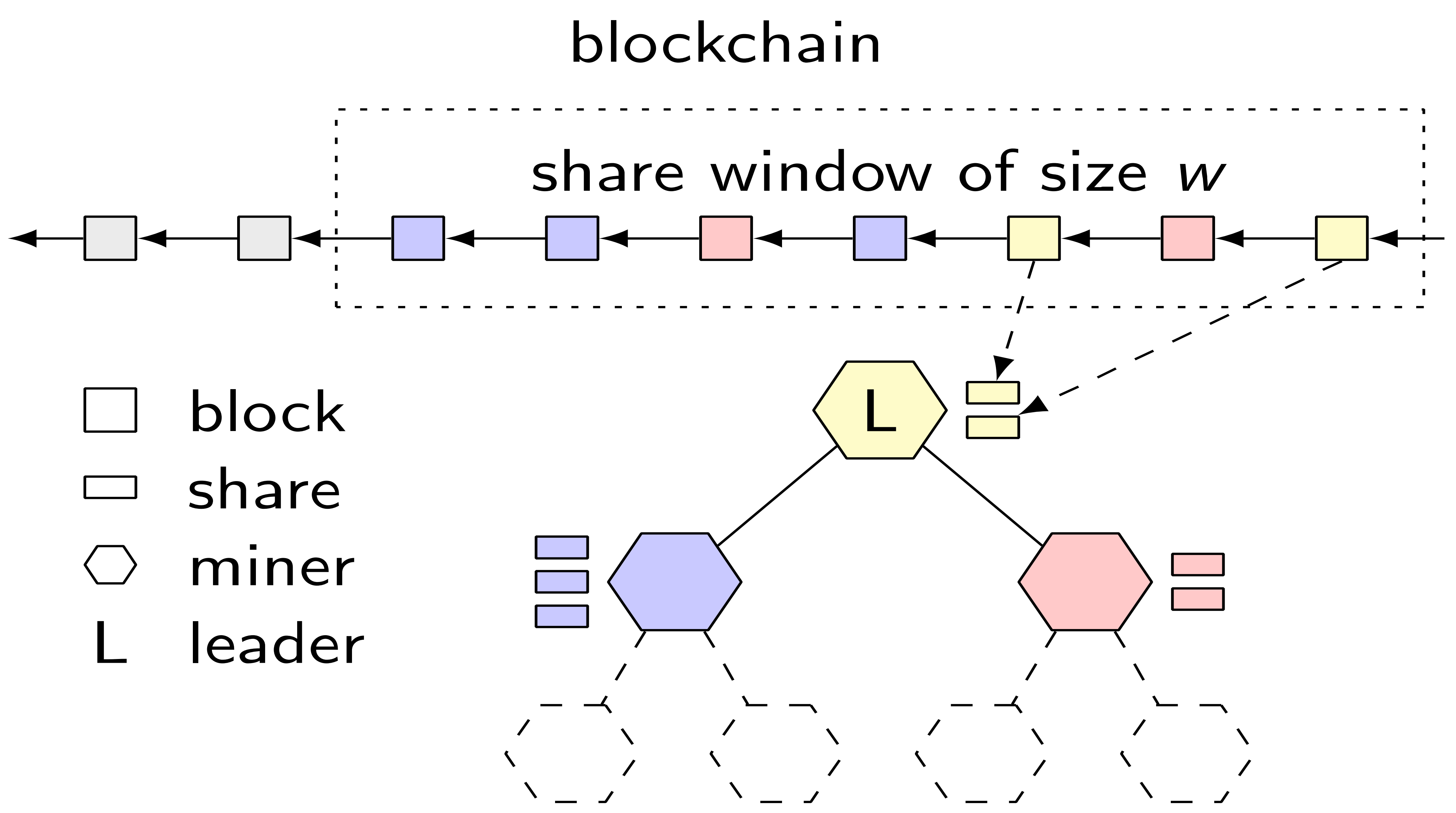
- Substitute MACs with public-key cryptography
  - Third-party verifiable
  - Enables sparser communication patterns (ring or star topologies)

From MACs to Collective Signing

- Can we do better than O(n) communication complexity?
  - Multicast protocols transmit information in O(log n) steps
  - 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]

Discussion

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



Problem Statement

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

Chapter Outline

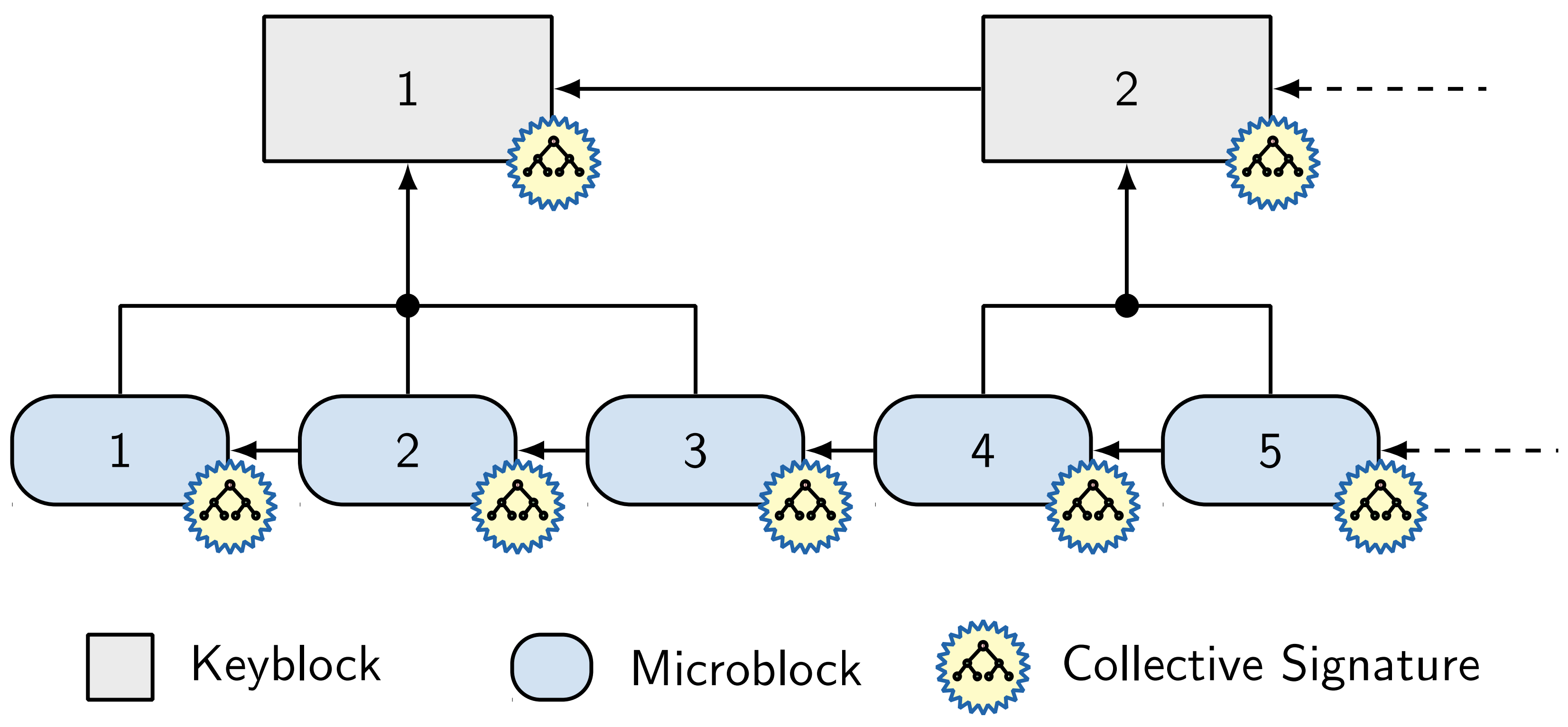
- Bitcoin and its limitations
- Strawman design: PBFTCoin
- Opening the consensus group
- From MACs to Collective Signing
- **Decoupling transaction verification from leader election**
- Performance Evaluation

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



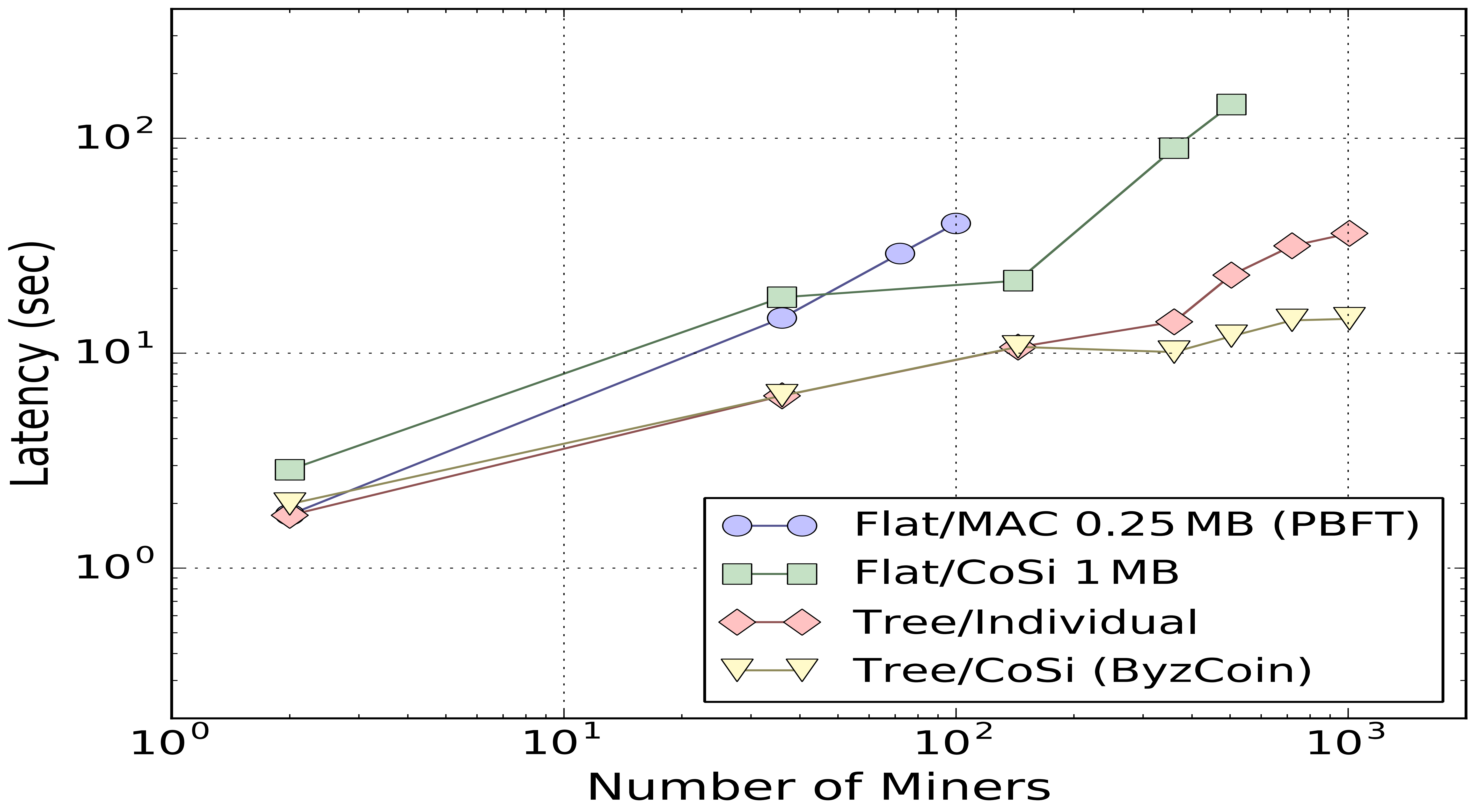
Chapter Outline

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

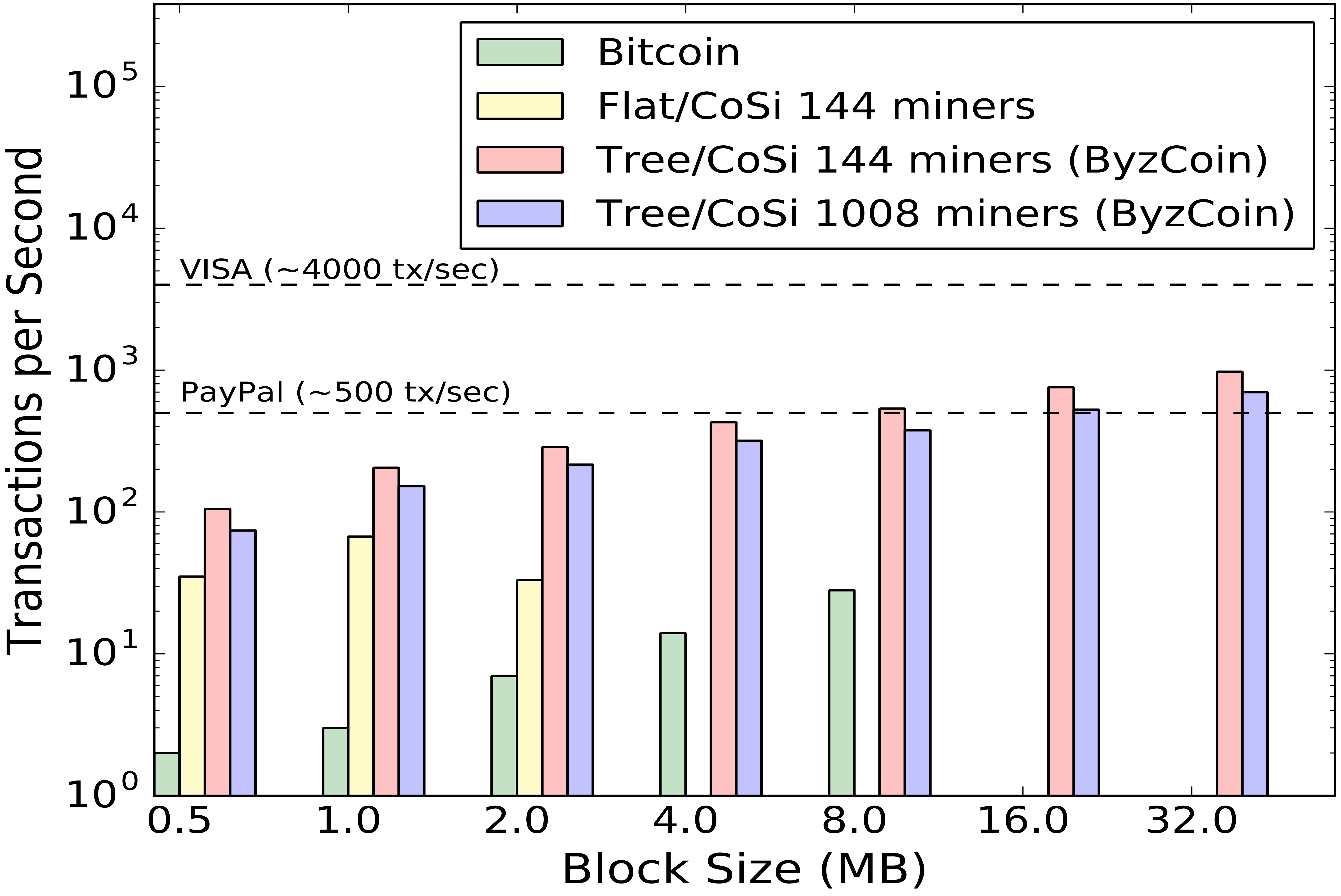
Performance Evaluation

- 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

- Introduction
- Scalable, Strongly-Consistent Consensus for Bitcoin
- **OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding**

Bitcoin vs OmniLedger

	Bitcoin	OmniLedger*
Throughput	~7 TPS	~20.000 TPS
1-st Confirmation	~10 minutes	~1 second
Full Security	~60 minutes	~42 second
More Available Resources	No performance Gain	Linear Increase in Throughput

** Configuration with 1120 validators against a 12.5% adversary*

Bitcoin vs OmniLedger

	Bitcoin	OmniLedger*
Throughput	~7 TPS	~20.000 TPS
1-st Confirmation	~10 minutes	~1 second
Full Security	~60 minutes	~42 second
More Available Resources	**No performance Gain**	**Linear Increase in Throughput**

** Configuration with 1120 validators against a 12.5% adversary*

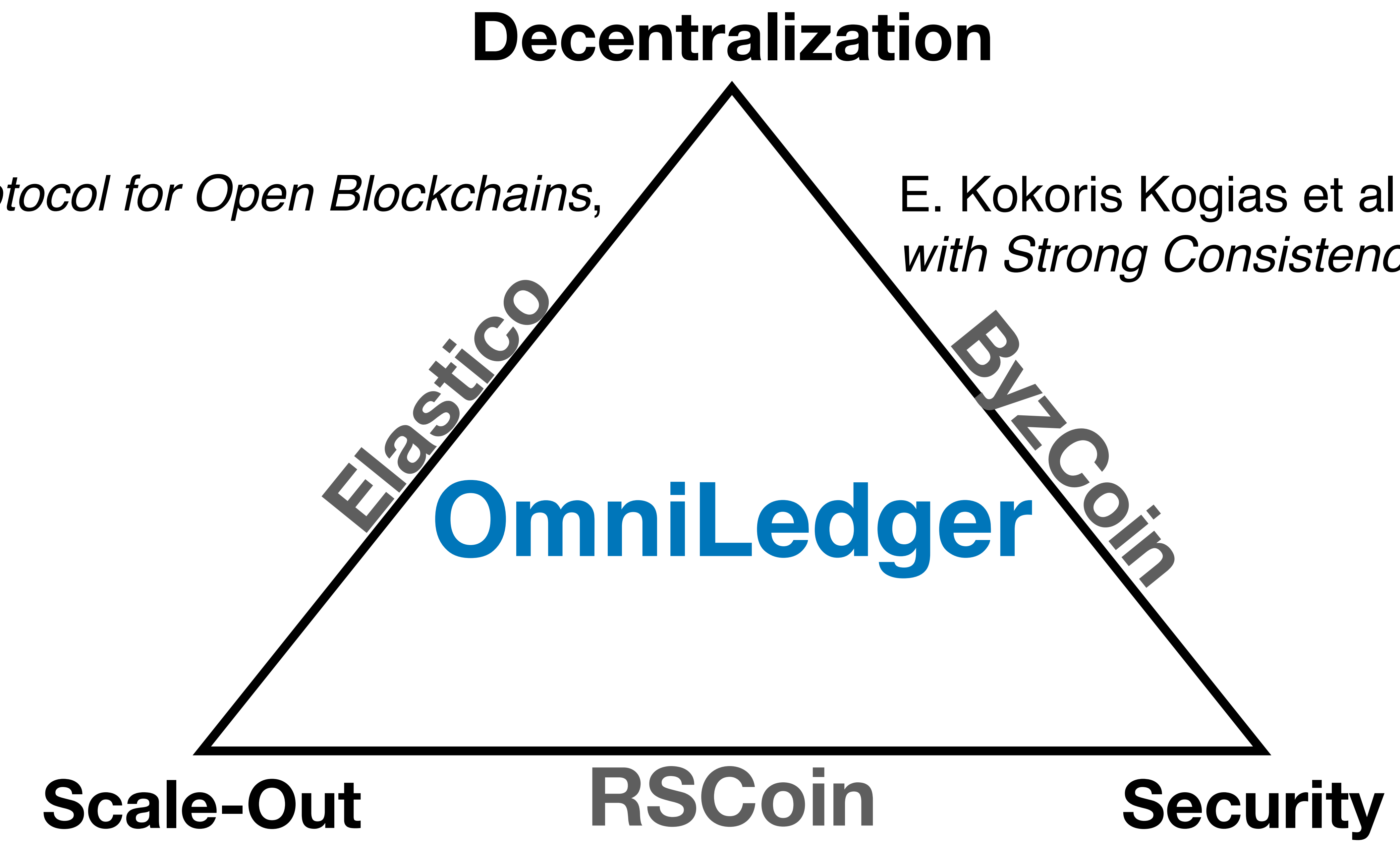
Scale-Out

… But Scaling Blockchains is Not Easy

Distributed Ledger Landscape

L. Luu et al., *A Secure Sharding Protocol for Open Blockchains*, CCS 2016

E. Kokoris Kogias et al., *Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing*, Security 2016

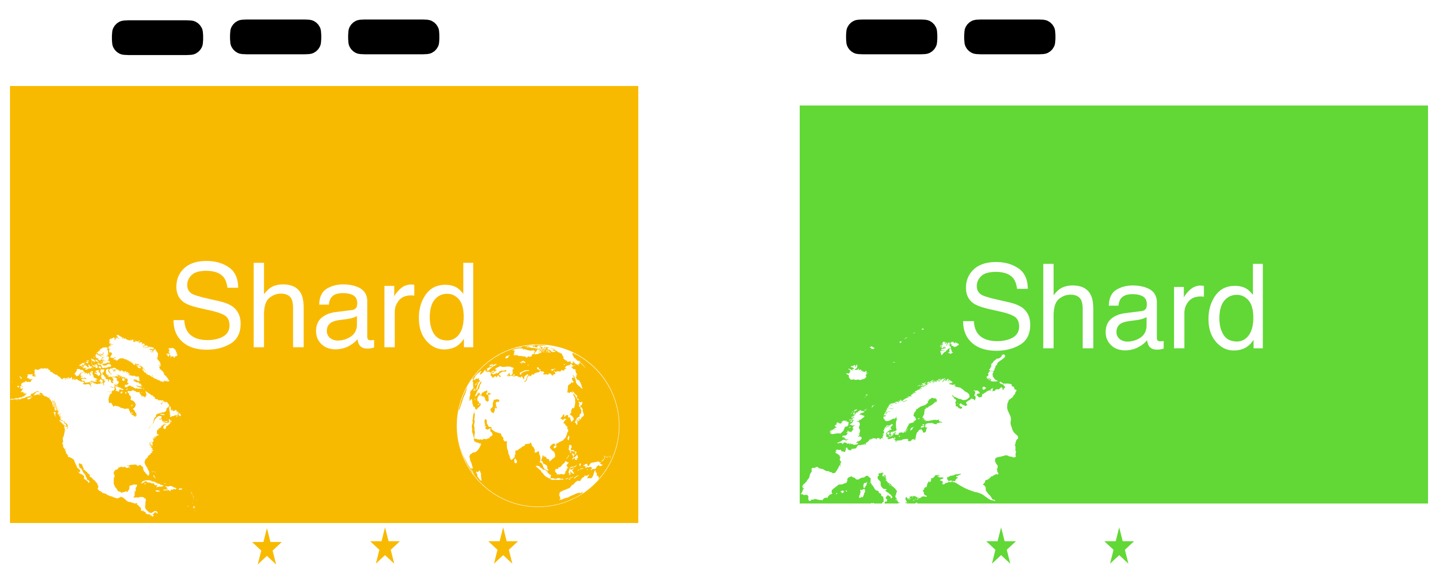


G. Danezis and S. Meiklejohn, *Centrally Banked Cryptocurrencies*, NDSS 2016

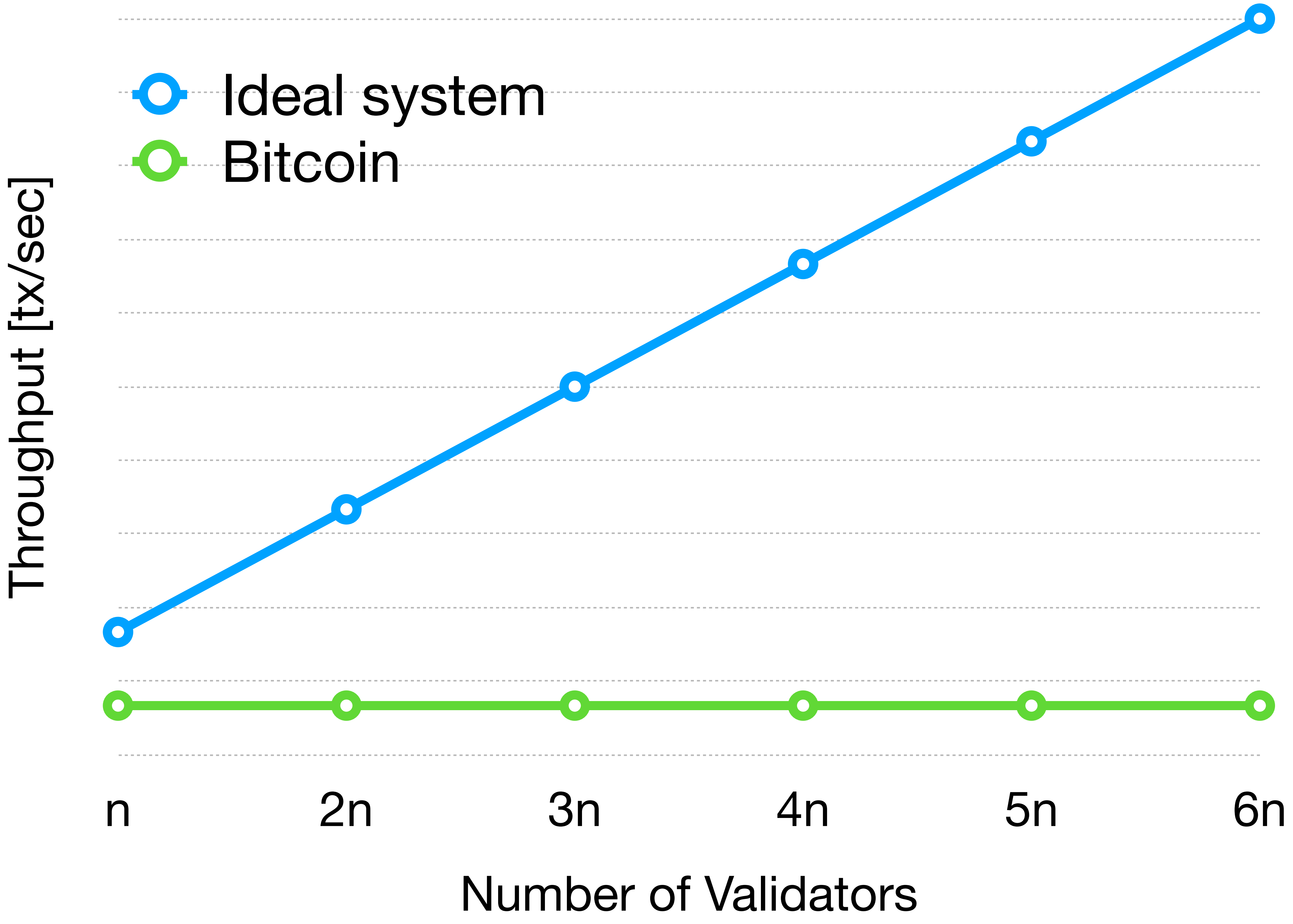
No Scale-Out (Bitcoin)

Scale-Out (OmniLedger)

- How do validators choose which blockchain to work on?
- How can I pay a yellow vendor with greencoins?

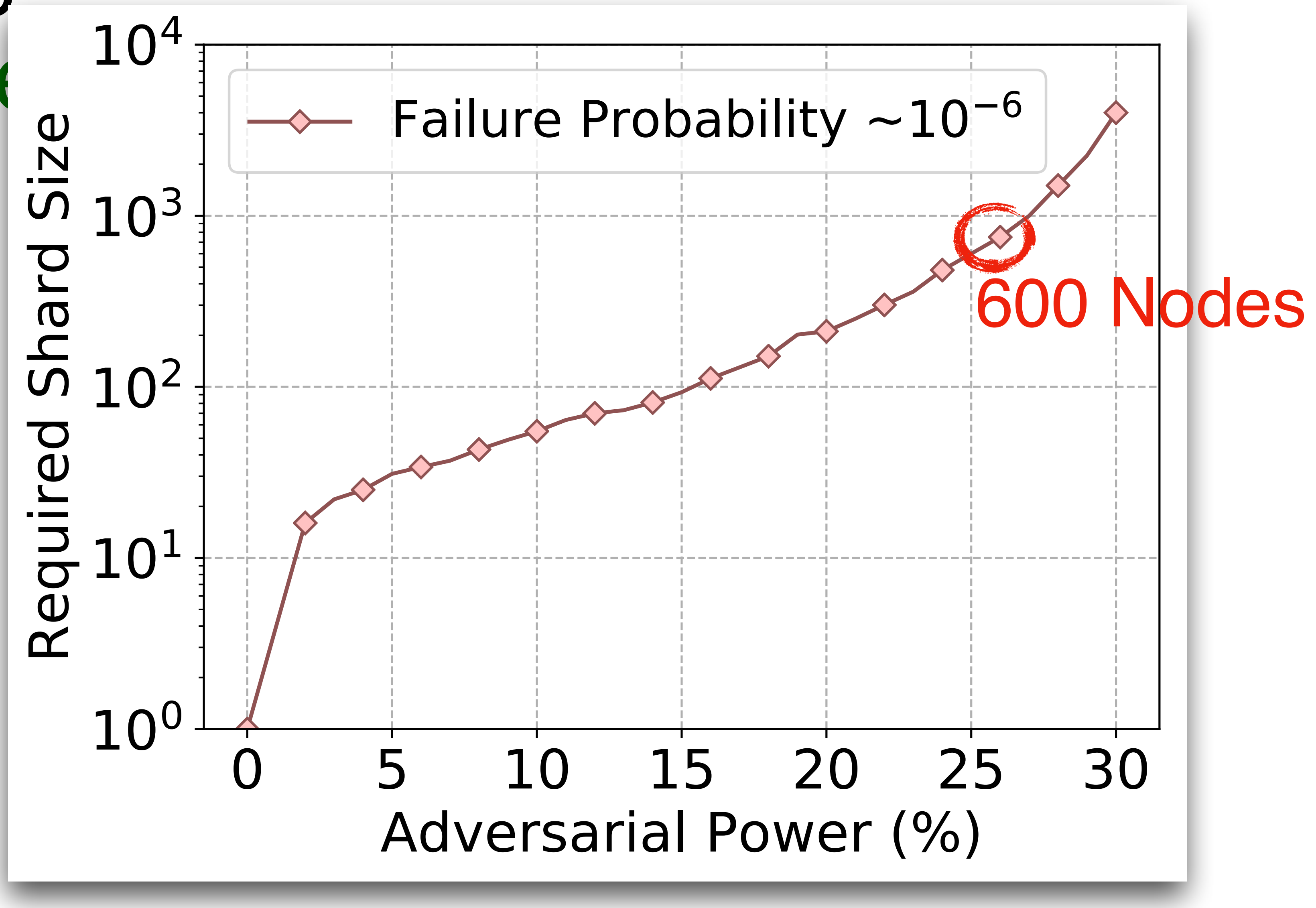


Double Throughput



Random Validator Assignment

- Let validators choose? —> All malicious validators can choose the same chain
- Randomly assign validators? —> Preserve security for adequately larg



Public Randomness is Hard

	Availability	Unpredictability	Unbiasability	Verifiability	Scalability
Strawman I	⛔	⛔	⛔	⛔	✅
Strawman II	⛔	✅	⛔	⛔	✅

Strawman I

- **Idea:** Combine random inputs of all participants.
- **Problem:** Last node controls output.

Strawman II

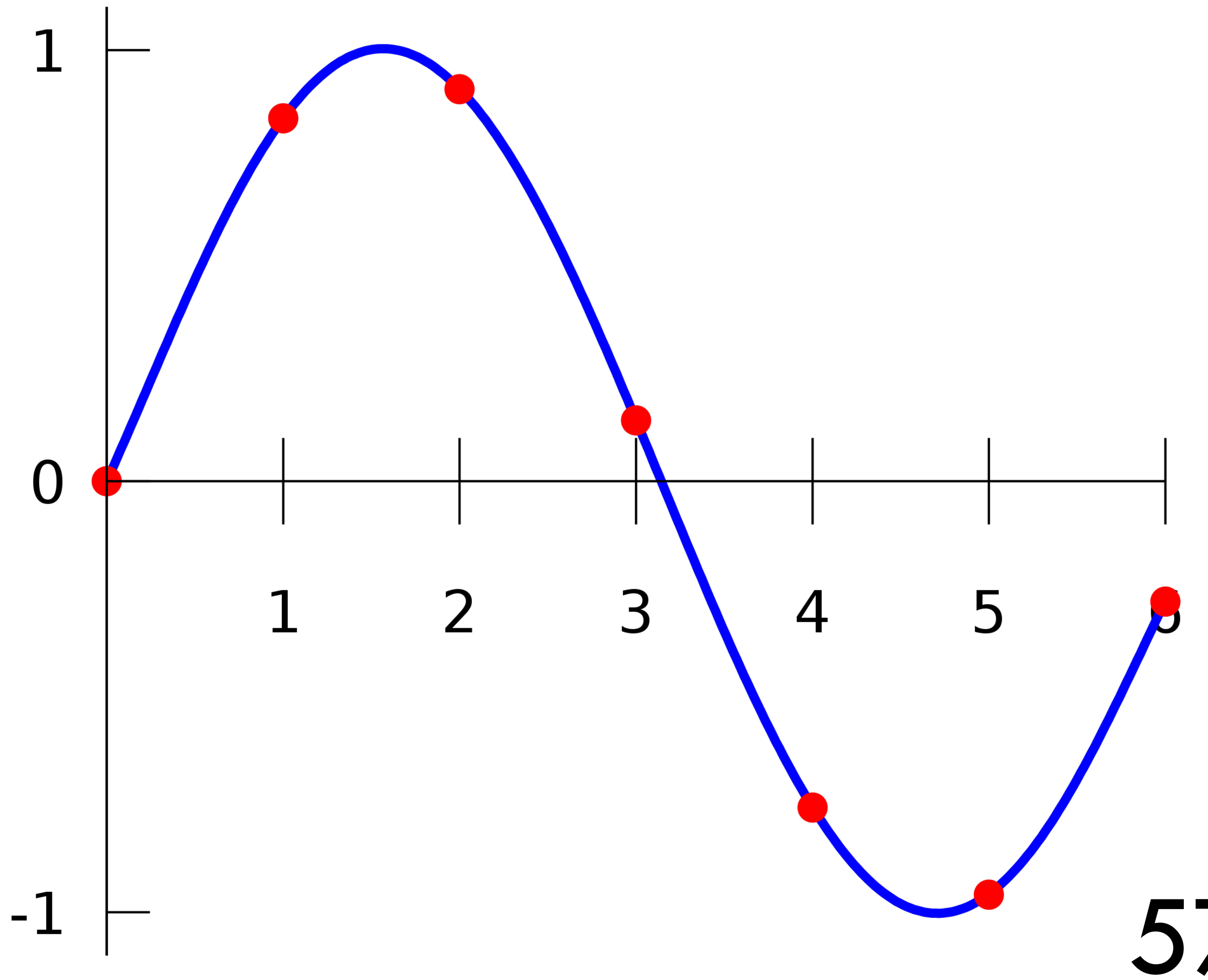
- **Idea:** Commit-then-reveal random inputs.
- **Problem:** Dishonest nodes can choose not to reveal.

Public Randomness is Hard

	Availability	Unpredictability	Unbiasability	Verifiability	Scalability
Strawman I	✗	✗	✗	✗	✓
Strawman II	✗	✓	✗	✗	✓
RandShare	✓	✓	✓	✗	✗

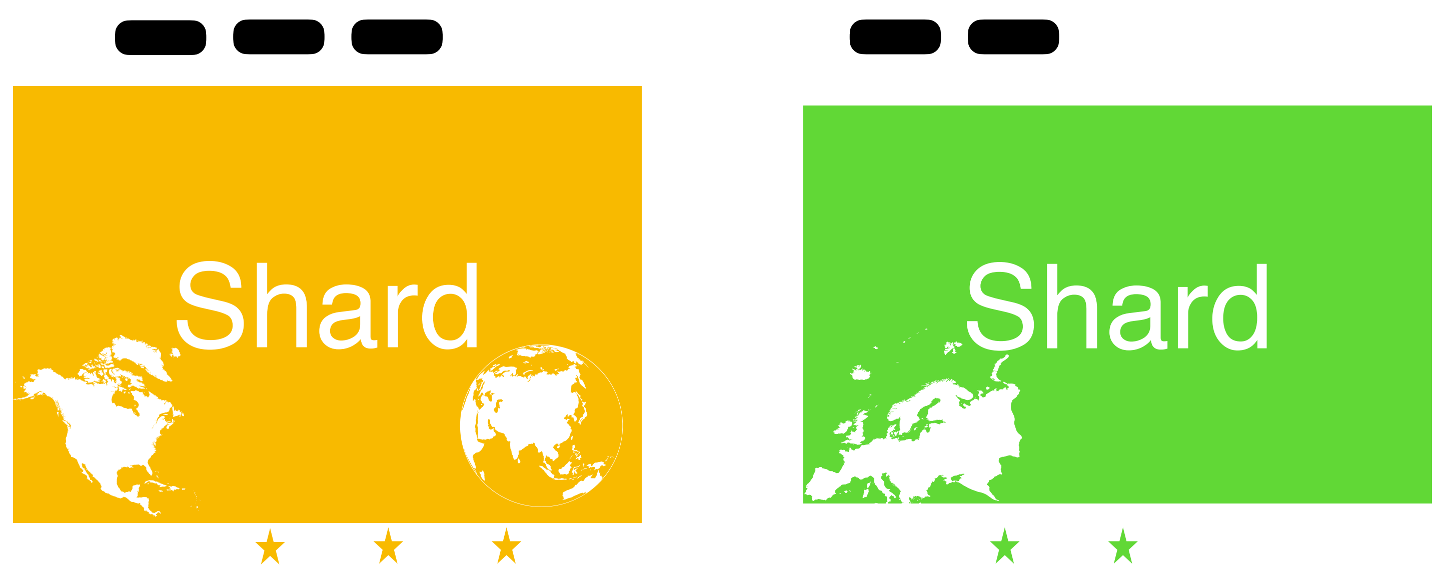
RandShare

- **Idea:** *Verifiable secret sharing* (Feldman, 1987)
- **Problems:**
  - Not publicly verifiable
  - Not scalable: $O(n^3)$ communication / computation complexity

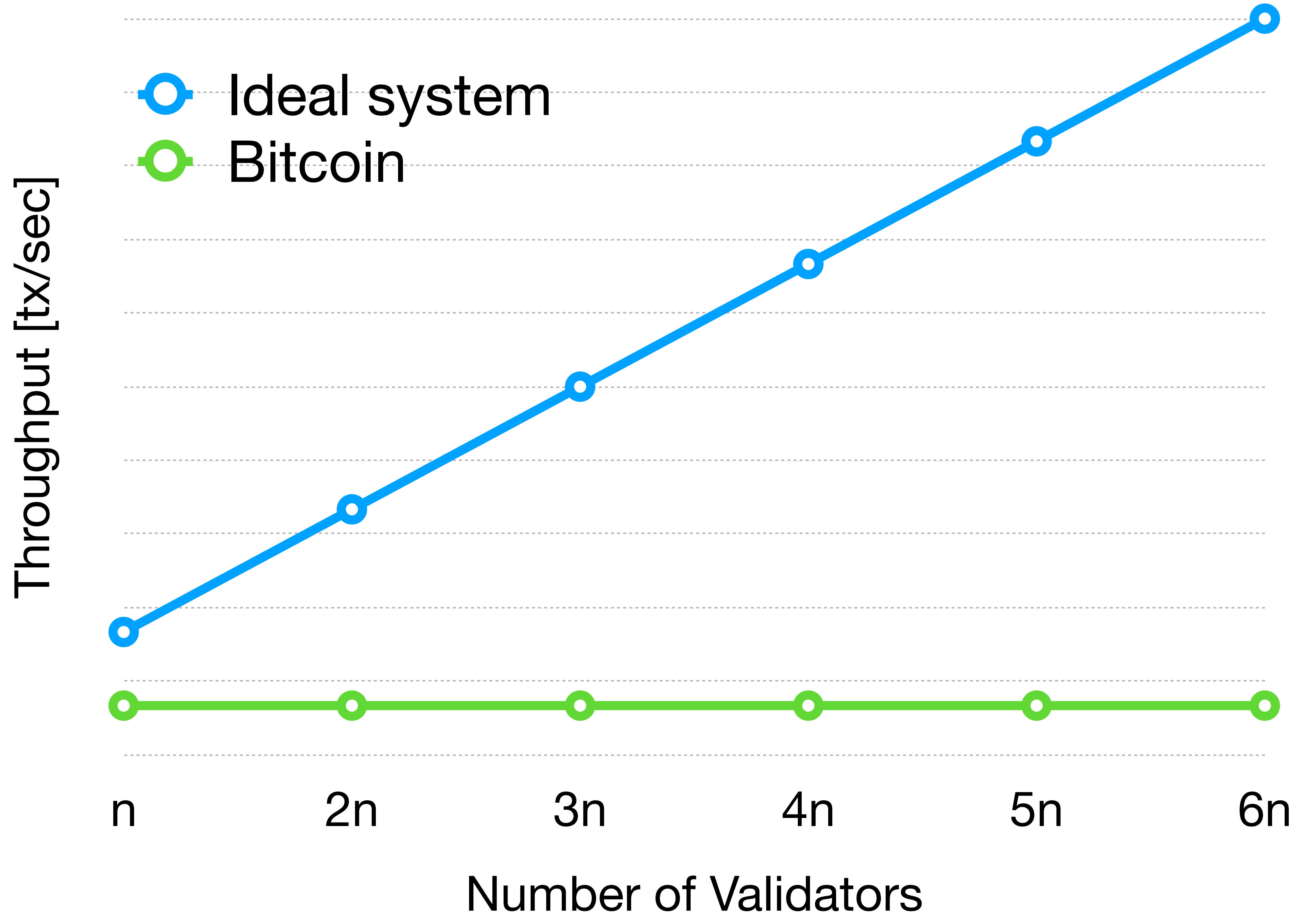


Scale-Out (OmniLedger)

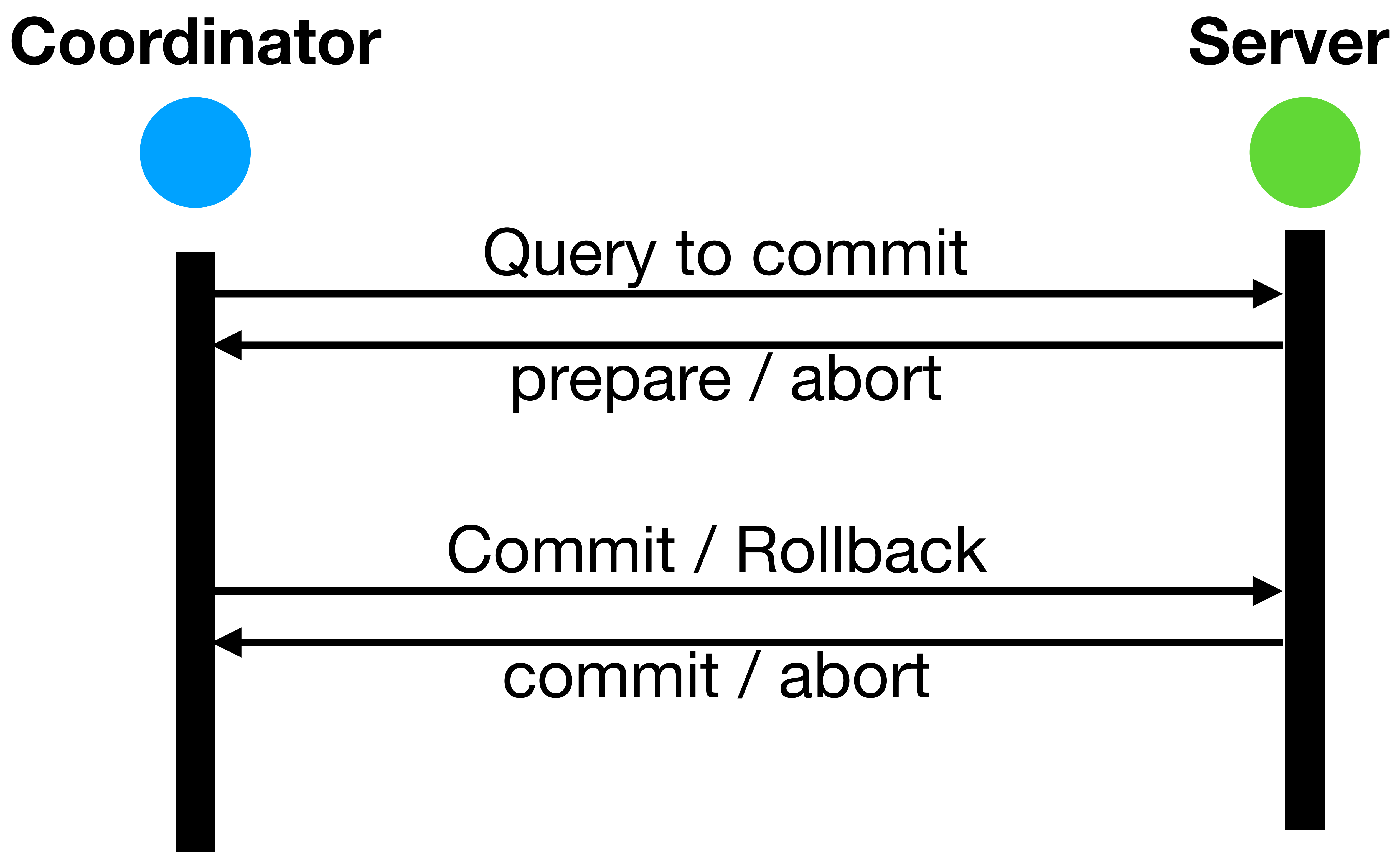
- How do validators choose which blockchain to work on?
- How can I pay a yellow vendor with greencoins?



Double Throughput



Two-Phase Commit



Atomix: Cross-Shard Transactions

Challenge:

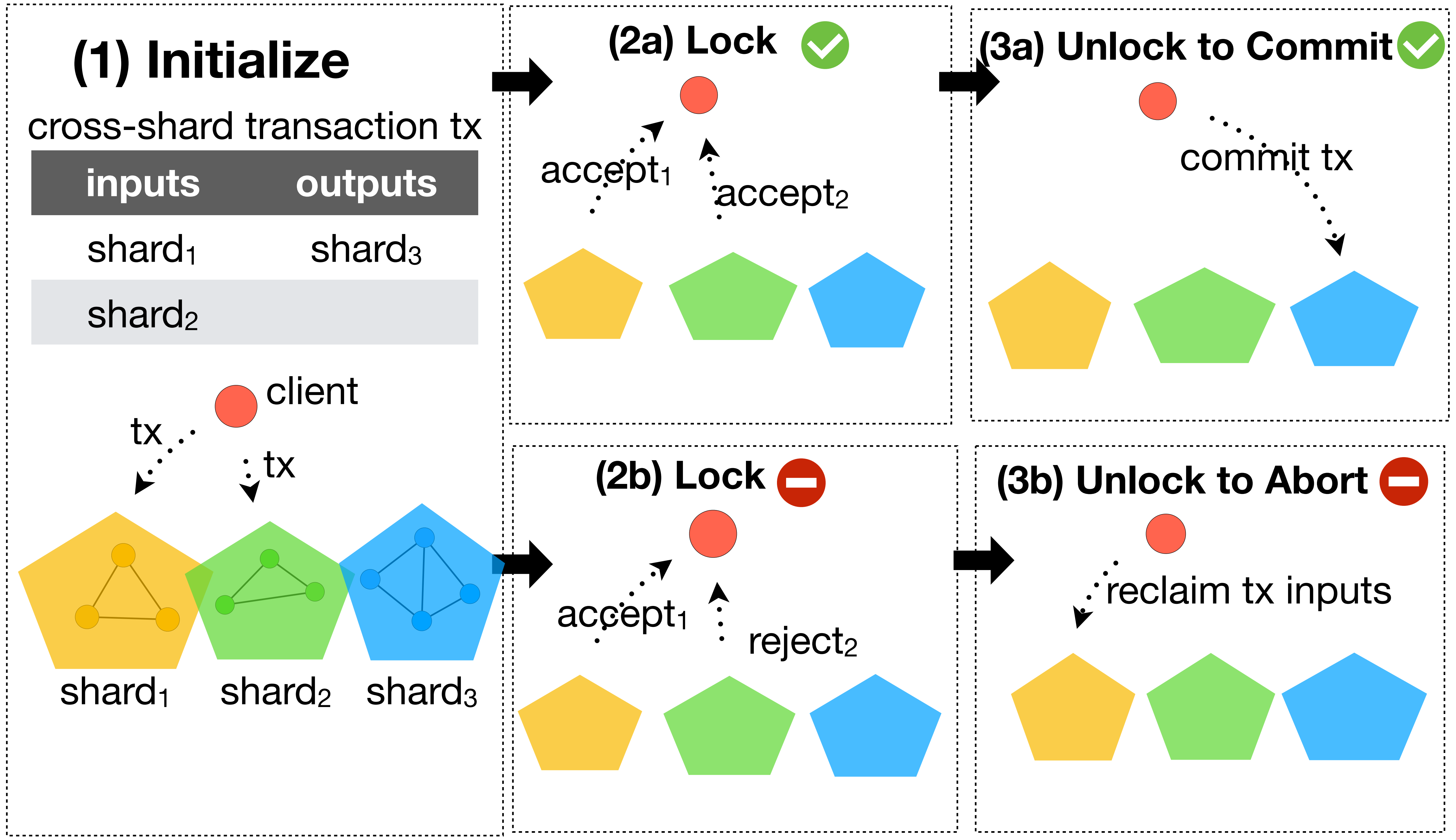
- Cross-shard tx commit atomically or abort eventually

Solution: Atomix

- Client-managed protocol
    1. Client sends cross-shard tx to input shards
    2. Collect ACK/ERR proofs from input shards

(a) If all input shards accept, commit to output shard, otherwise

(b) abort and reclaim input funds



Chapter Outline

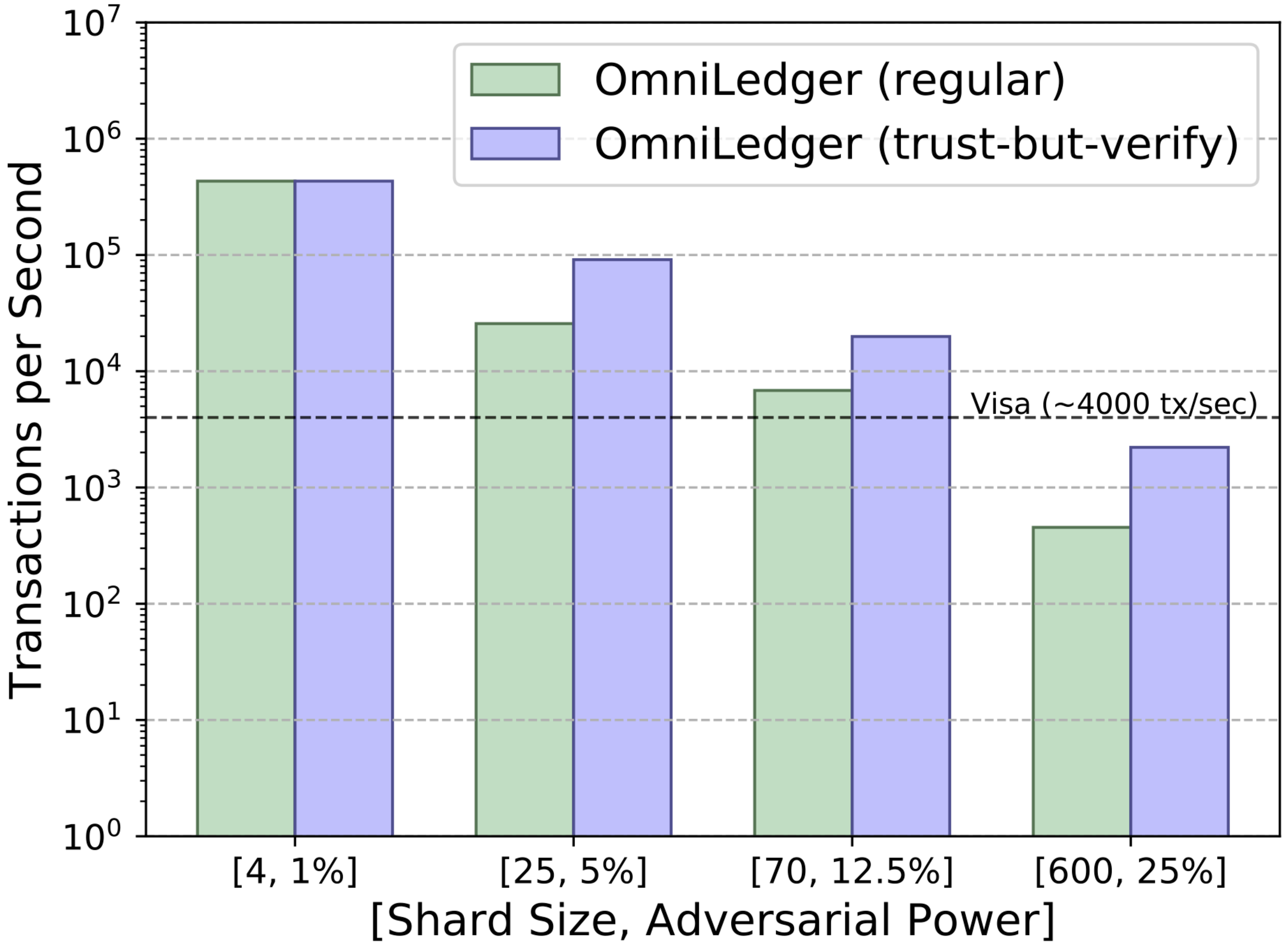
- Motivation
- OmniLedger
- **Evaluation**

Evaluation: **Scale-Out**

#validators	**70**	**140**	**280**	**560**	**1120**
OmniLedger (tx/sec)	439	869	1674	3240	5850
Bitcoin (tx/sec)	~7	~7	~7	~7	~7

Scale-out throughput for 12.5%-adversary and **shard size 70** and 1200 validators

Evaluation: **Throughput**



Results for 1800 validators

Thank you!!

- Questions?