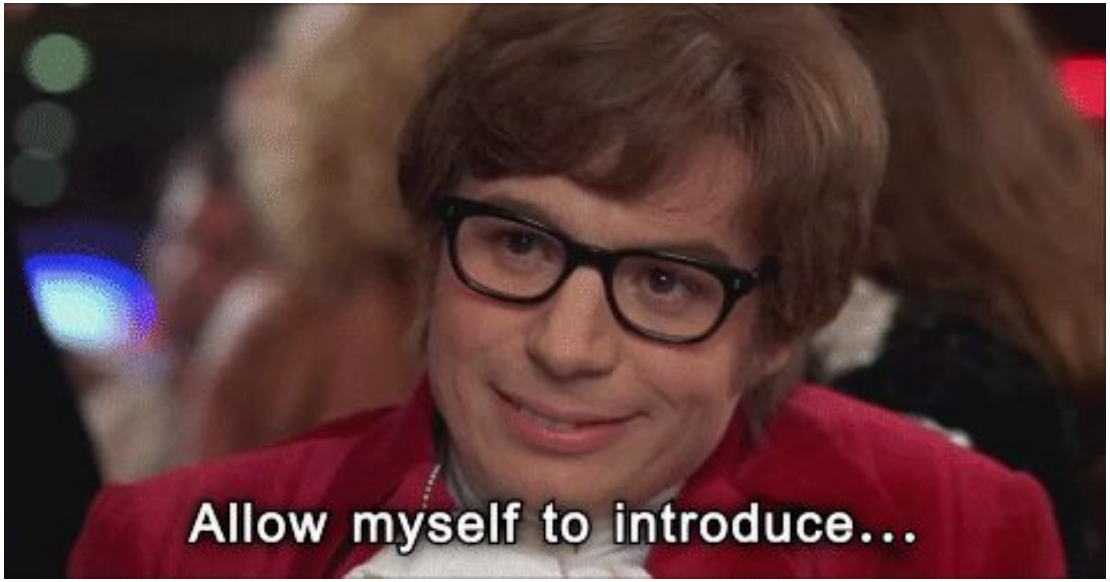
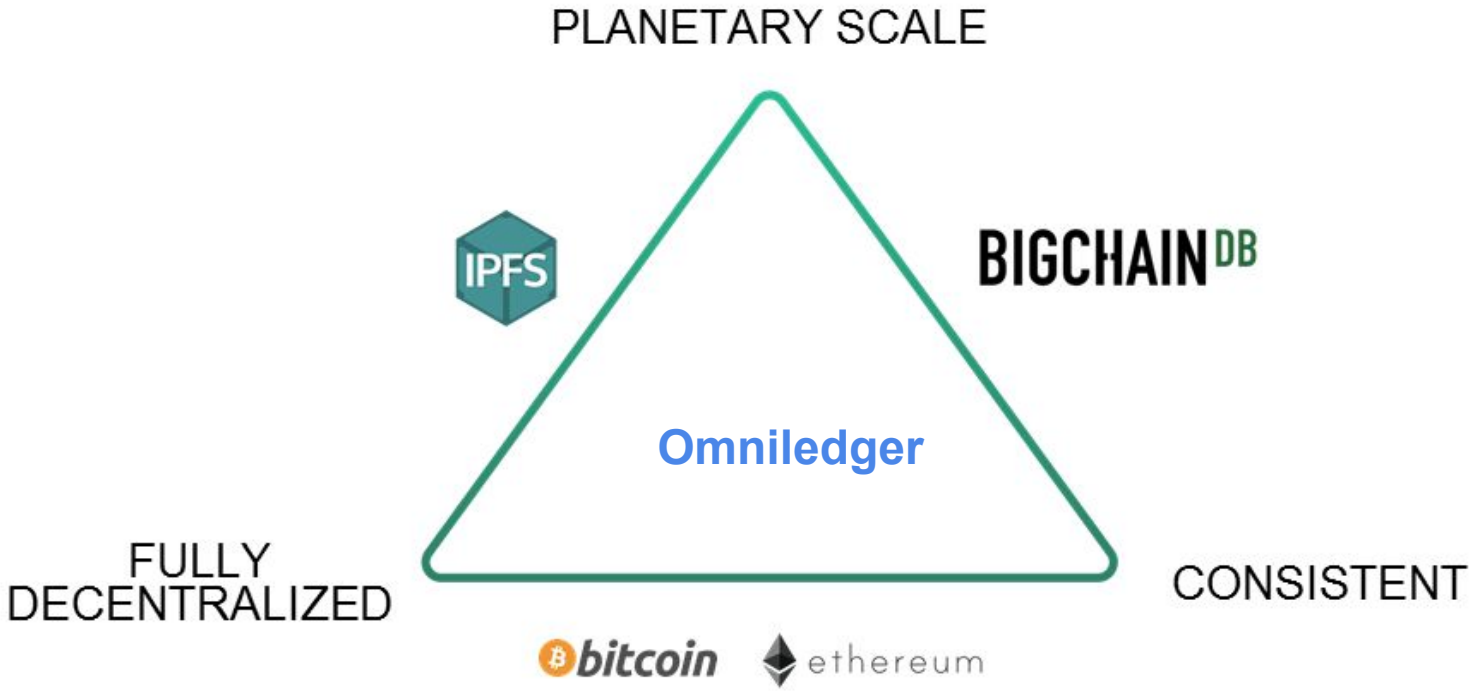
OmniLedger Whitepaper Sharing

Tianyu Chen
09/21/2018


Allow myself to introduce...

Review: background



Are you kidding me?

- Omniledger can Omniledger up, no can no bb :-P

Bitcoin vs OmniLedger

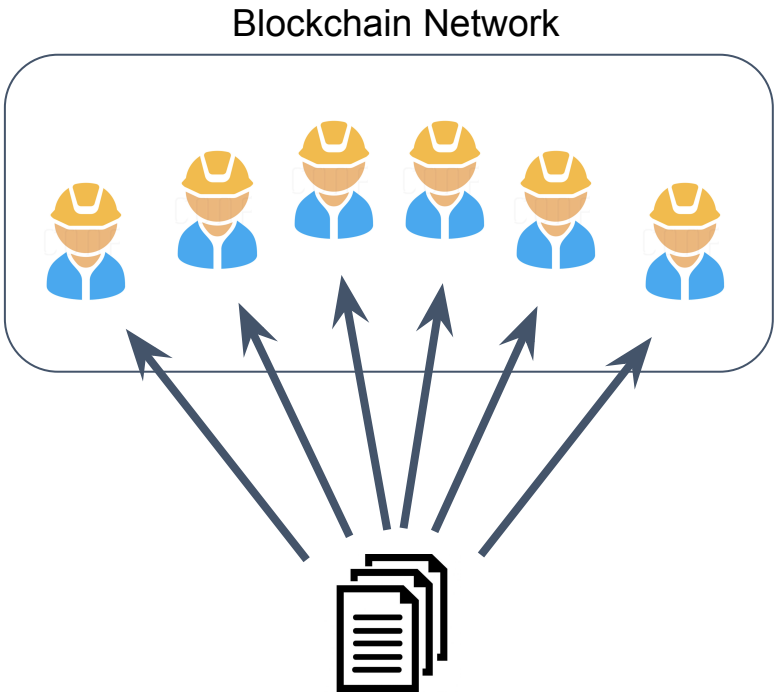
	Bitcoin	OmniLedger*
Throughput	~4 TPS	~20.000 TPS
1-st Confirmation	~10 minutes	~1 second
Full Security	~60 minutes	~42 second
More Available Resources	**No performance Gain**	**Linear Increase in Throughput**

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

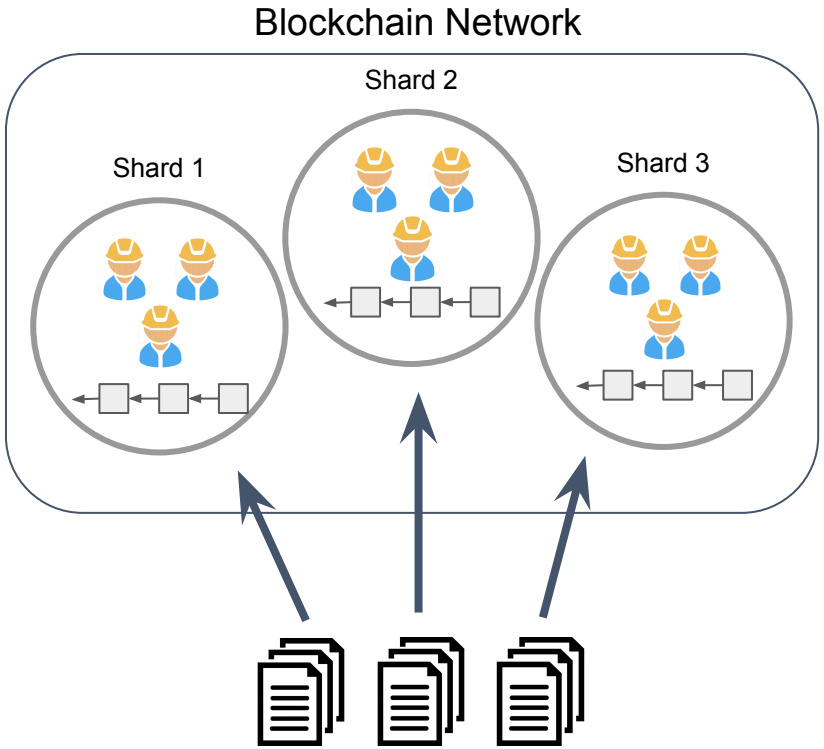
Omniledger System Goals

- Full decentralization
- Shard robustness
- Secure transactions
- Scale-out
- Low storage overhead
- Low latency

Review: Non-sharded Blockchain

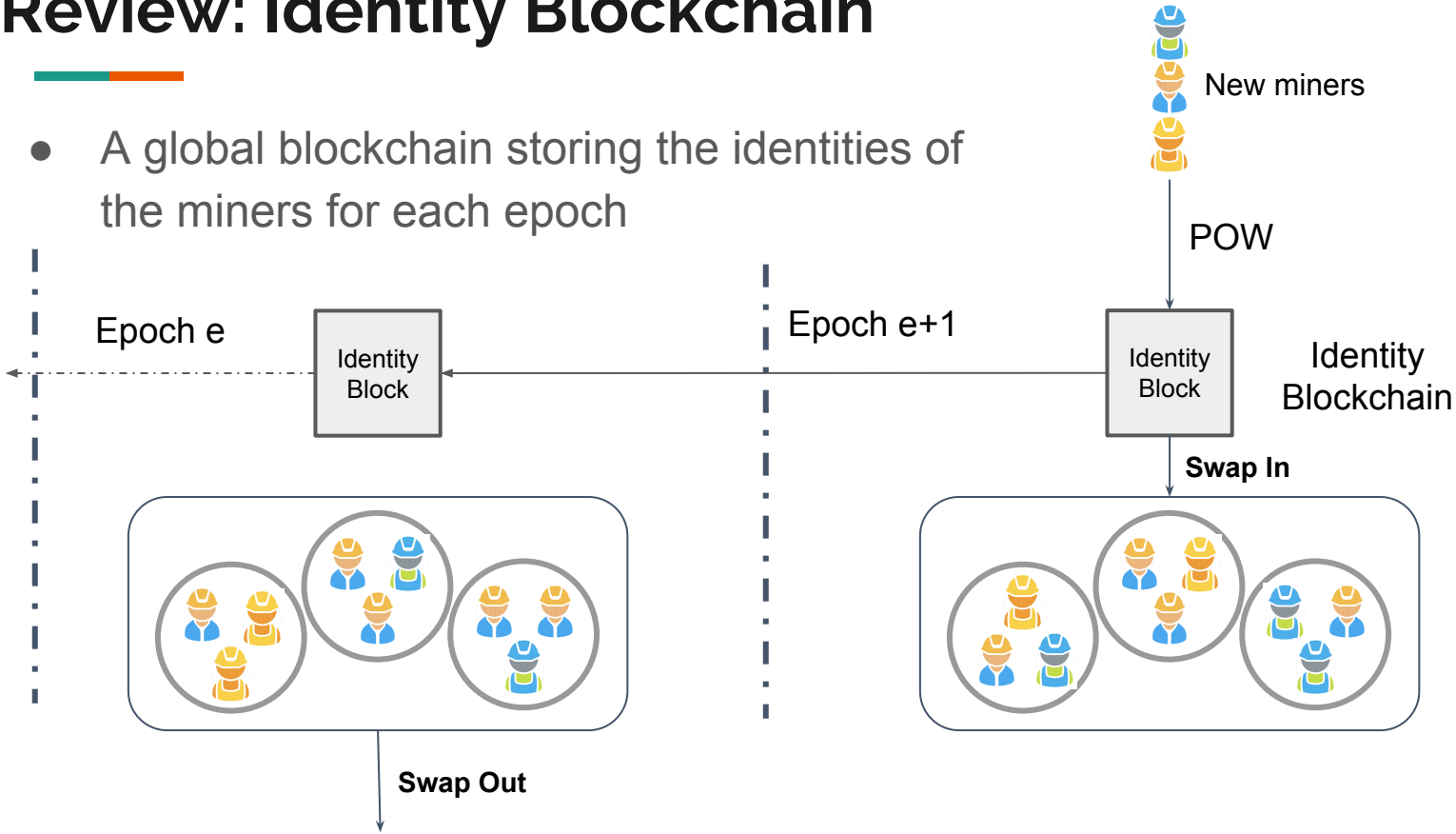


Review: Sharded Blockchain



Review: Identity Blockchain

- A global blockchain storing the identities of the miners for each epoch



Omniledger

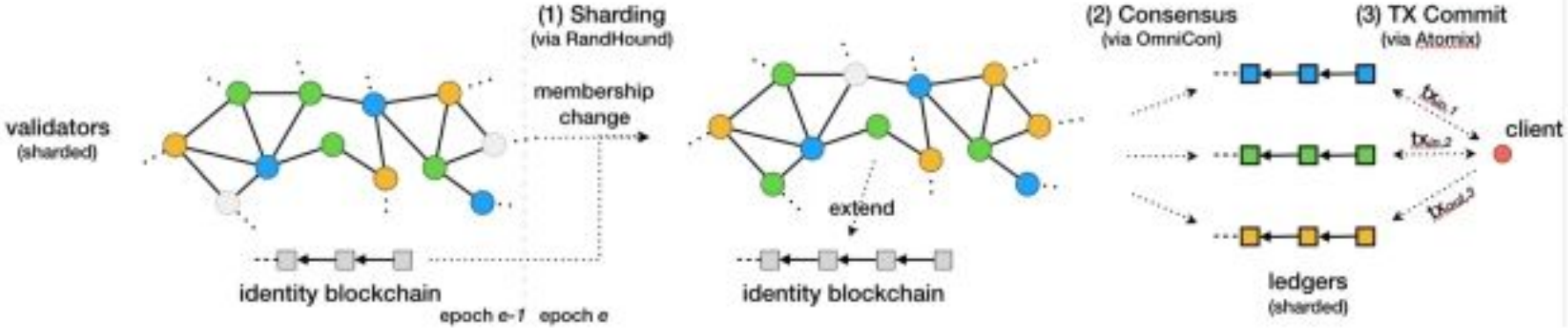
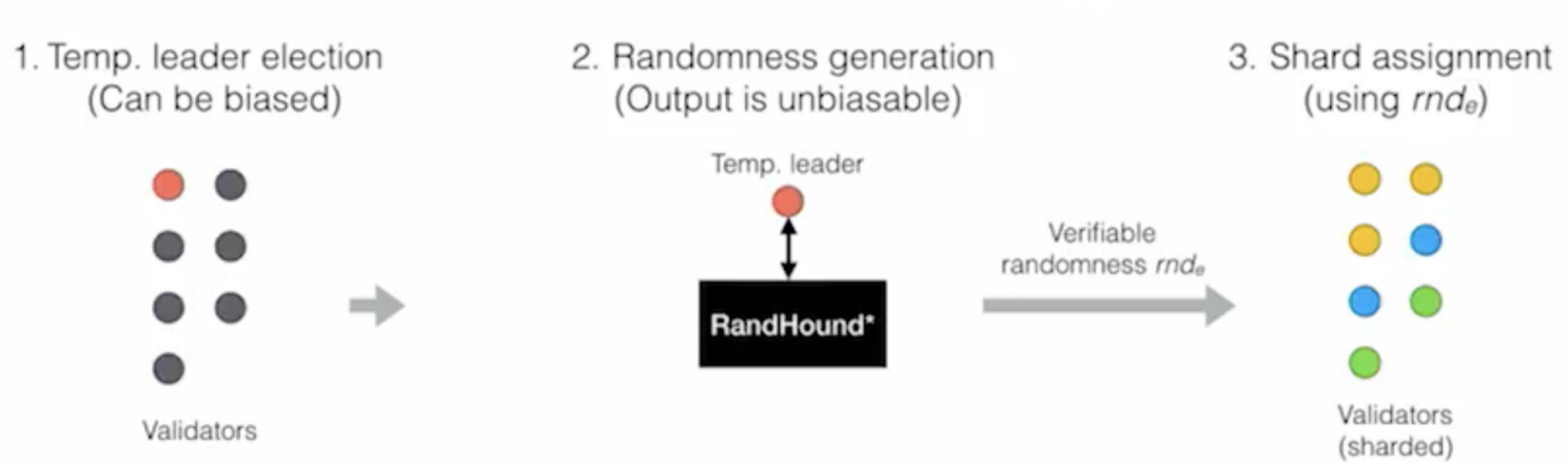


Fig. 2: OmniLedger architecture overview: At the beginning of an epoch e, validators (1) use RandHound to randomly remove old validators from shards and assign new validators who registered to the identity blockchain in epoch $e-1$. Afterwards, validators ensure (2) consistency of the shards' ledgers via Omnicon while clients ensure (3) consistency of their cross-shard transactions via Atomix (here the client spends inputs from shards 1 and 2 and outputs to shard 3).

How are validator assigned to different shards?

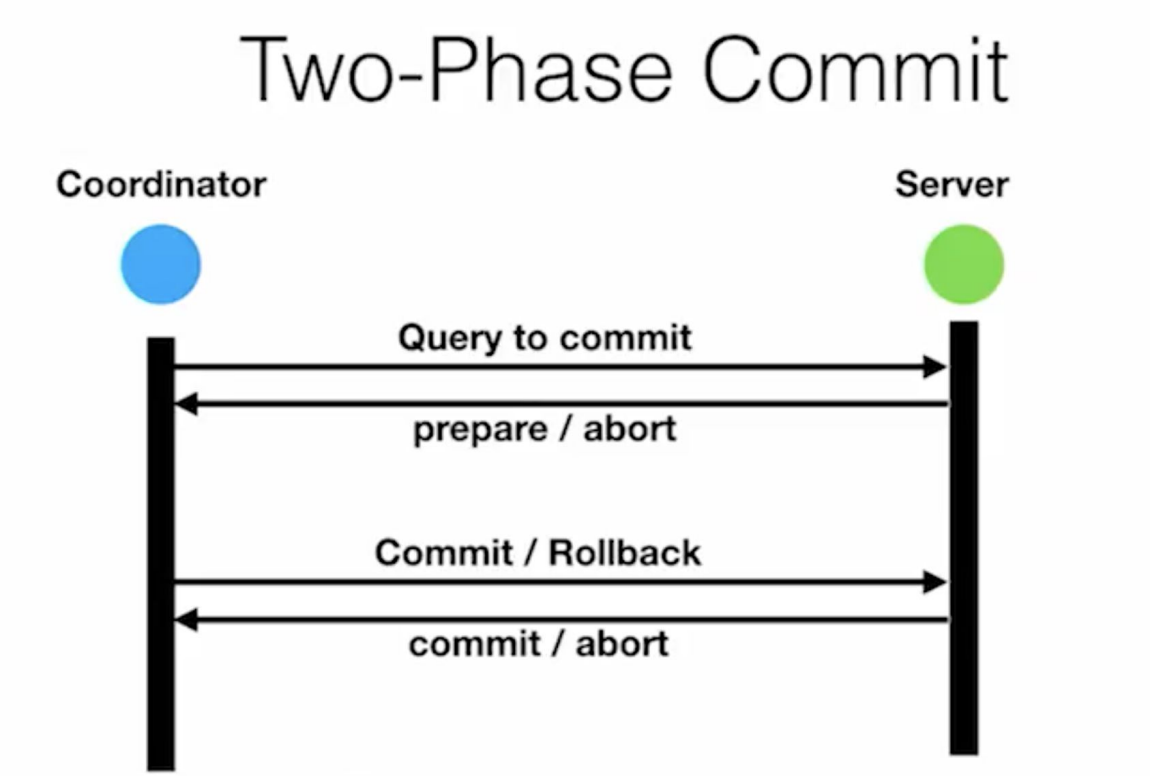
- Randomly!
- But hmm… purely random?
- Randomness on 1 machine is based on seed, which is risky
- Can we leverage the whole network?

Shard Validator Assignment



How about cross-shards transactions?

Review


Two-Phase Commit
Coordinator
Server
Query to commit
prepare / abort
Commit / Rollback
commit / abort

Cross-shards transactions

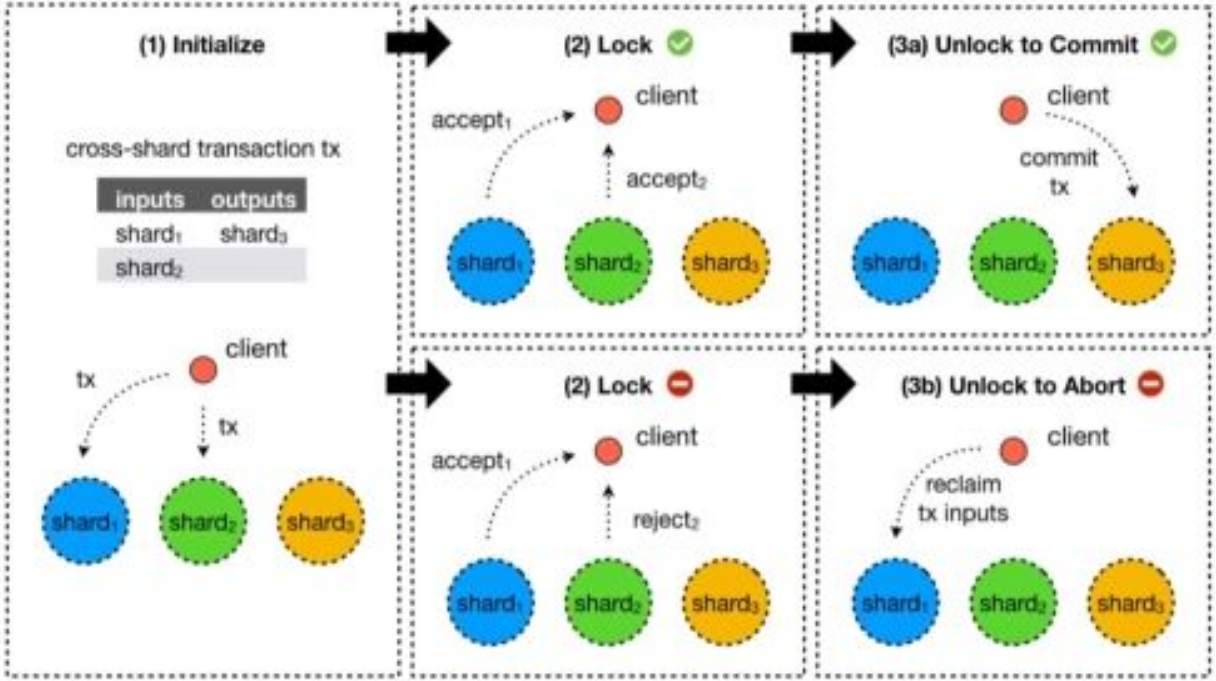


Fig. 3: Atomix protocol in OmniLedger.

Latency vs. Throughput trade-off

- Larger block size -> more throughput, but more latency too! :-(
- Smaller block size -> less latency, but less throughput as well! X-(

Introducing the HACK:

Trust-but-Verify Transaction Validation

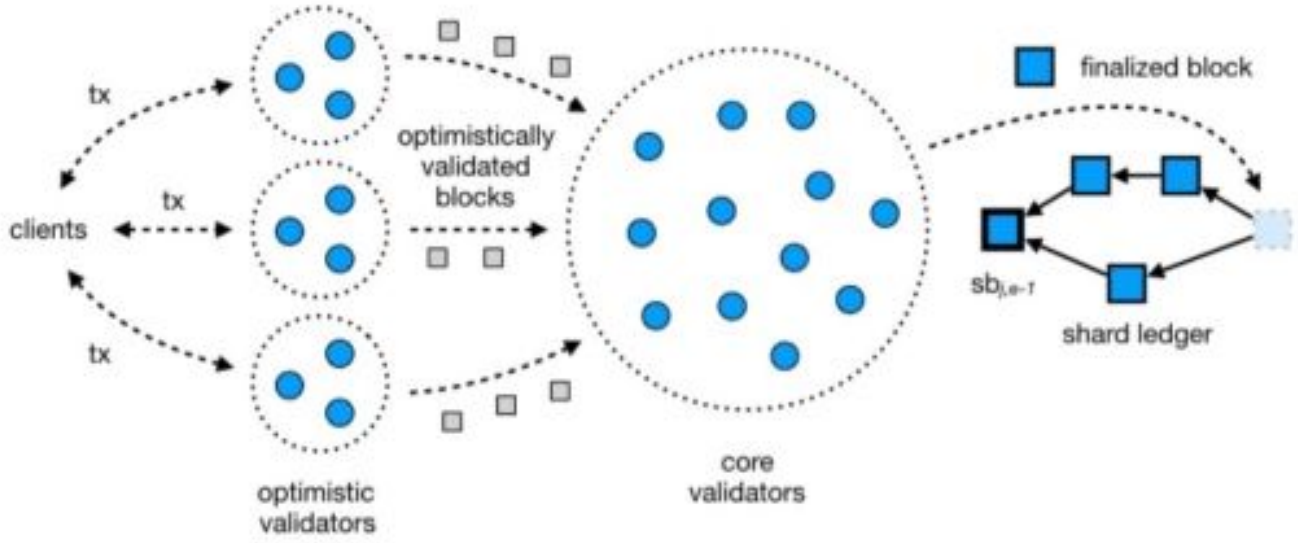


Fig. 4: Trust-but-Verify Validation Architecture

Trust-but-Verify Transaction Validation

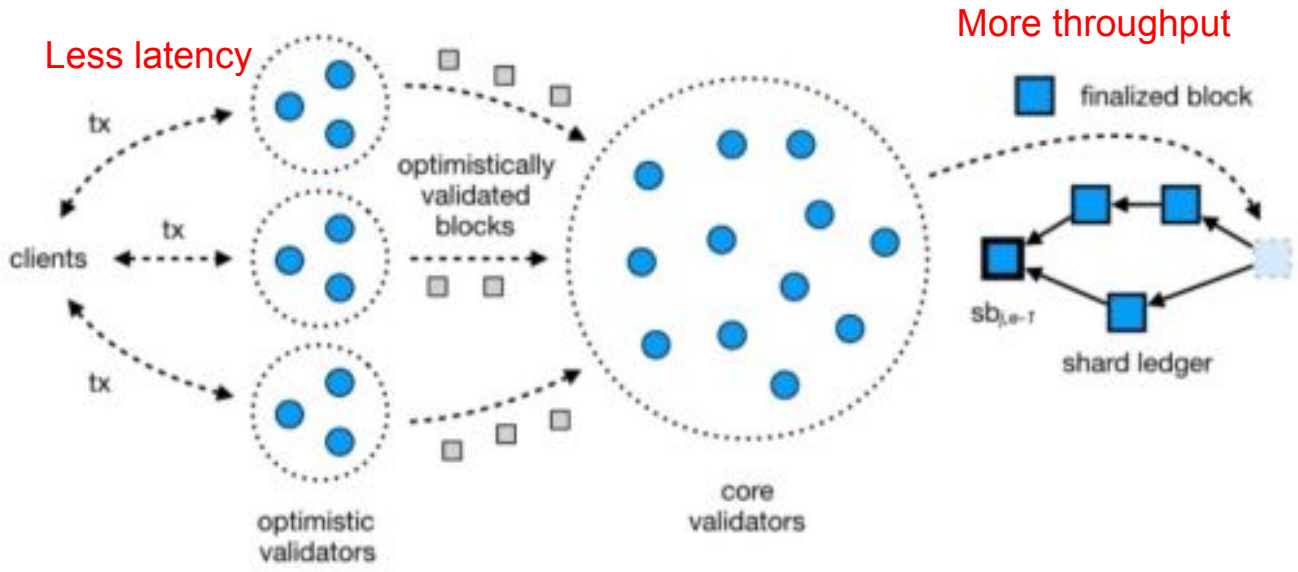
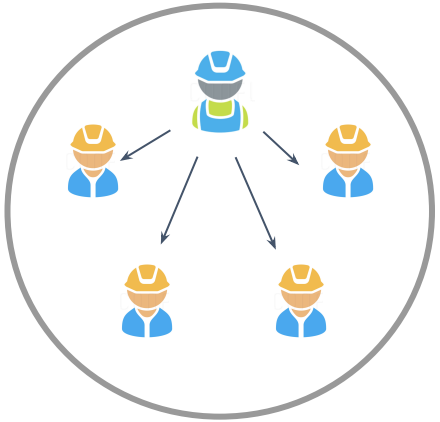
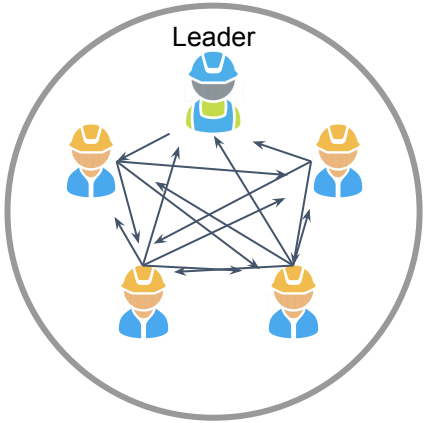


Fig. 4: Trust-but-Verify Validation Architecture

Consensus 101: PBFT

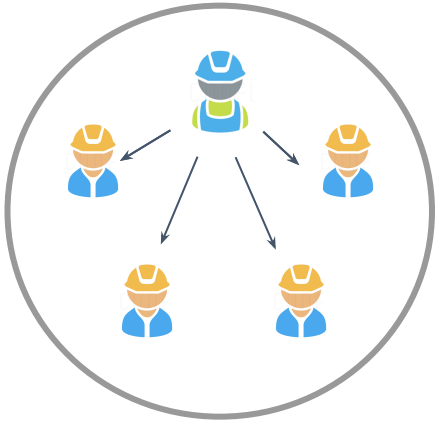
- Practical Byzantine Fault Tolerance
- Voting-based consensus: consensus reached with 2/3 majority votes
- Instant Finality (vs. probabilistic finality in POW)
- Assumes <1/3 of malicious nodes (vs. <1/2 in POW)
- Requires a leader to initiate the consensus process (similar to block proposer in POW)
- O(n^2) Network Complexity
- Only scale to 10-20 nodes

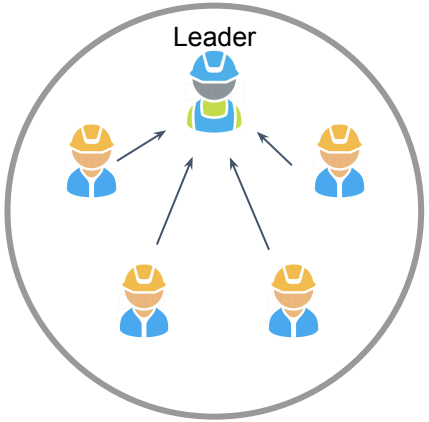




Consensus 101: Scalable BFT

- Rely on Schnorr Multi-Signature
- Aggregate O(n) votes (signatures) into a O(1)-sized multi-signature proof
- Miners check the multi-signature proof instead of directly receiving votes from each other
- Scales to hundreds of nodes:
- O(n) complexity instead of O(n^2) in traditional PBFT

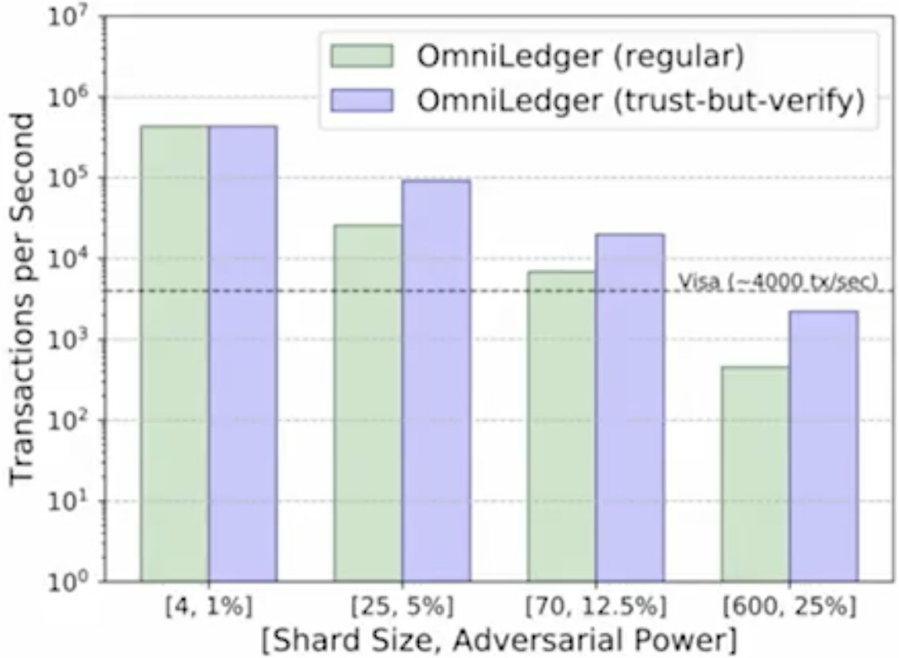




Consensus

- ByzCoin -> ByzCoinX
- Demo

Evaluation: **Throughput**



Results for 1800 validators

Evaluation: **Latency**

Transaction confirmation latency in seconds for regular and mutli-level validation

#shards, adversary	4, 1%	25, 5%	70, 12.5%	600, 25%	
regular validation	1.38	5.99	8.04	14.52	1 MB blocks
1st lvl. validation	1.38	1.38	1.38	4.48	500 KB blocks
2nd lvl. validation	1.38	55.89	41.89	62.96	16 MB blocks
Bitcoin	600	600	600	600	

latency increase since optimistically validated blocks are batched into larger blocks for final validation to get better throughput

Omniledger Limitations

- The cost of epoch bootstrap is significant
  - Extra overhead
- The actual throughput is dependent on the workload.
  - E.g. If all transactions touch all the shards before committing, then the system is better off with only one shard.

References

OmniLedger: a secure, scale-out decentralized ledger via sharding

OmniLedger's talk on 2018 IEEE Symposium on Security & Privacy

Philipp Jovanovich introduces OmniLedger

Thanks to Rongjian’s sharding talk

Q & A


全国优秀畅销书
Omniledger
从入门到出家
程序员转行指南
Bitnauts ®
ビットノーツ
Yoshitaka Jingu 著
ほりかわ けんいち 訳
weibo.com/natsumi136