Blockchain Sharding Intro

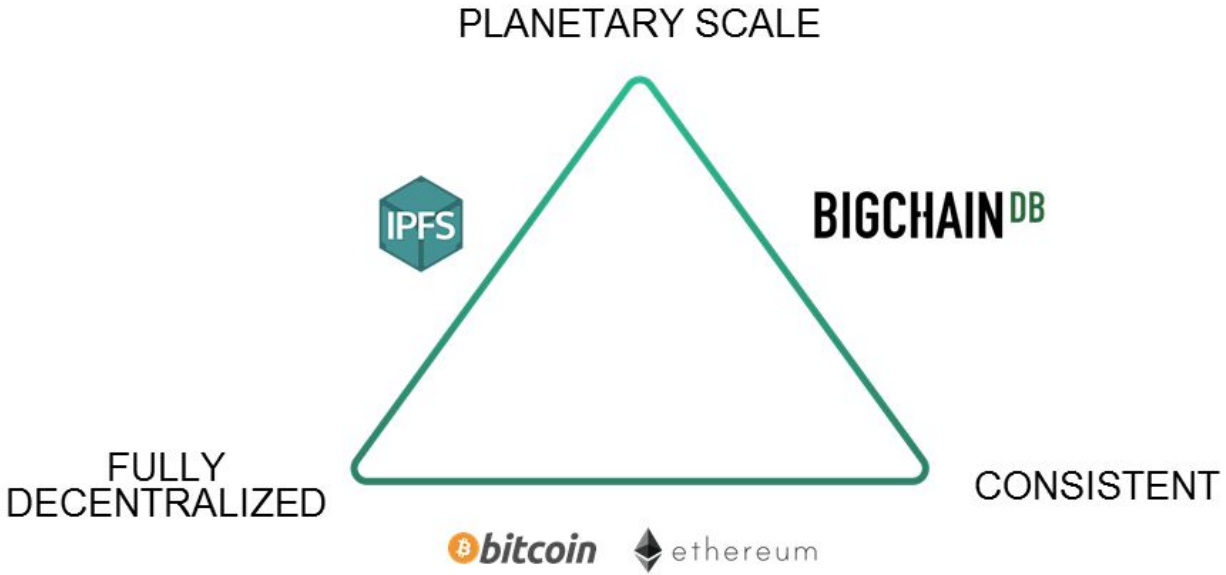
What's wrong with current blockchain?

Scalability

Bitcoin and Ethereum ~7-10 TX/s V.S. 8000 TX/s

Reason: Every Node has to verify every TX

What's wrong with current blockchain?

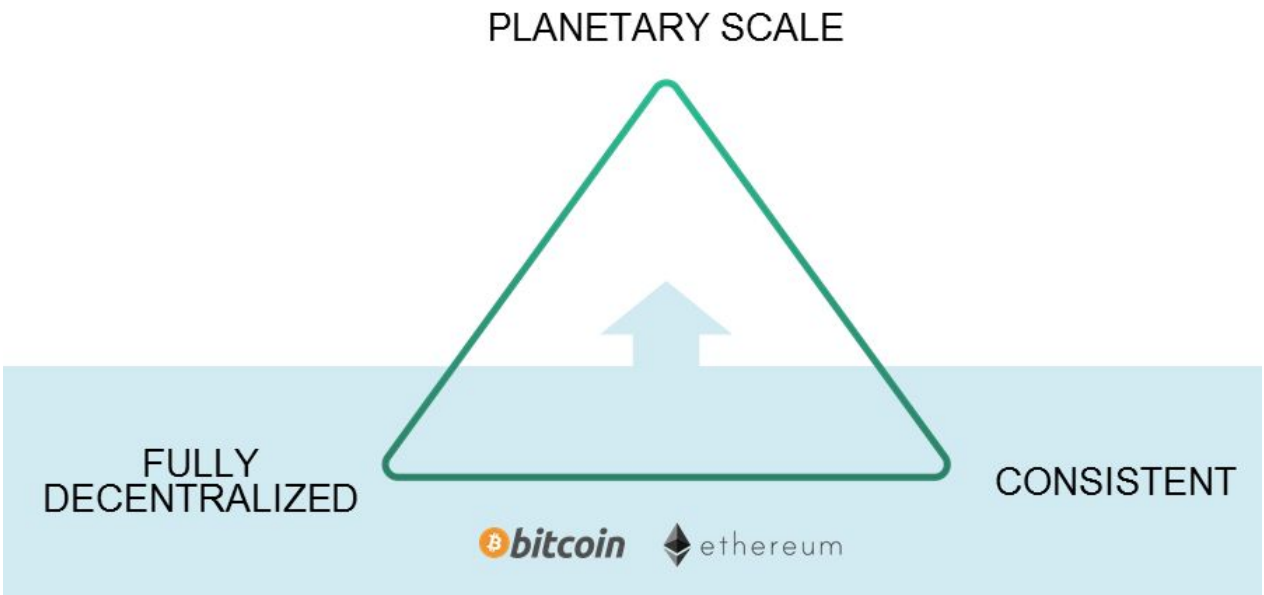


What's wrong with current blockchain?

Is Lightening (Payment Channel) a solution to this?

- Probably to retailer level payment system
- Probably not to a enterprise level system (transparency, auditability, storage, etc.,)

What's wrong with current blockchain?



What and Why is Sharding?

- Network would be divided into different shards
- Each shard comprises different nodes
- Each Node only possesses and processes a fraction of TXs.

What and Why is Sharding?

- Dramatically improve the rate at which traffic can progress.
- Improving transaction throughput will bring more and more users and applications to decentralized systems.
- Bring blockchain mass adoption down to earth.
- Make mining more profitable and attract more nodes to public networks because of lower fee.

Sharding Strategies

- Network Sharding
- Transaction Sharding
- State Sharding
- Computionaly Sharding

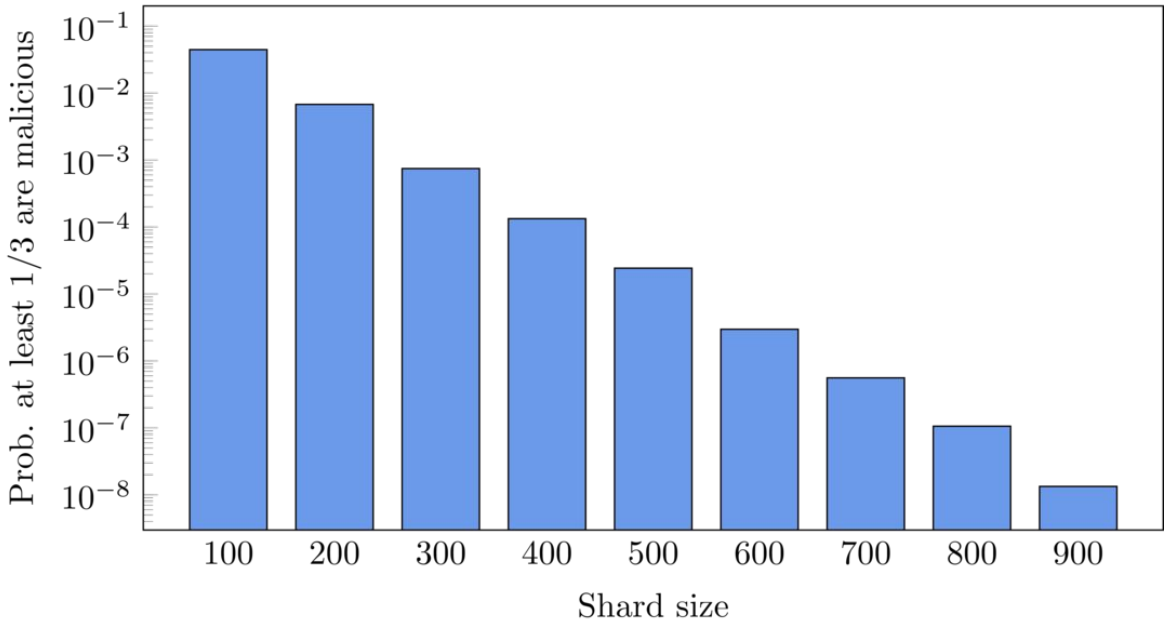
Network Sharding

- Network is divided into smaller groups of nodes each referred to as a shard.
- These shards can process transactions in parallel.
- Throughput linearly increases with the size of the network.

Network Sharding - Issues

- Open to malicious nodes (PoW, PoS, PoX)
- Shards creating (Committee, Pow, Randomness, etc.,)
- Shard size (Pow, Hash, Sampling)

Network Sharding



State Sharding

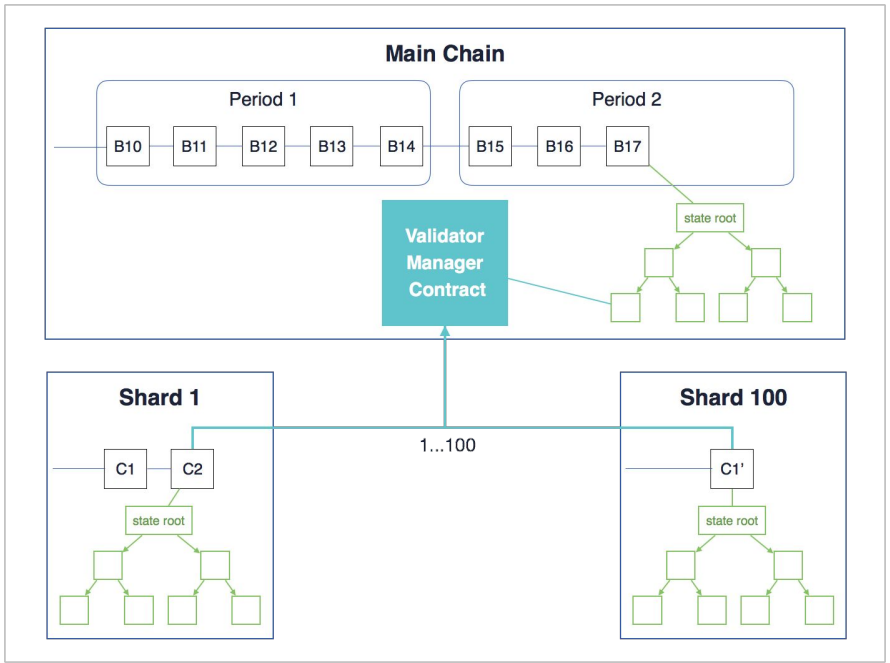
- Sharding the nodes into smaller subsets.
- Each shard processes specific sets of transactions.
- Simultaneously update the state of the entire network.

State Sharding - Ethereum

Transaction groups are assigned to each shard

- Header
  - The shard ID of the transaction group
  - Assignment of validators through random sampling (verify the transactions in the shard)
  - State Root
- Body
  - All of the transactions that belong to the transaction group that are part of the specific shard.

State Sharding - Ethereum



State Sharding - Cross-Shard Communication

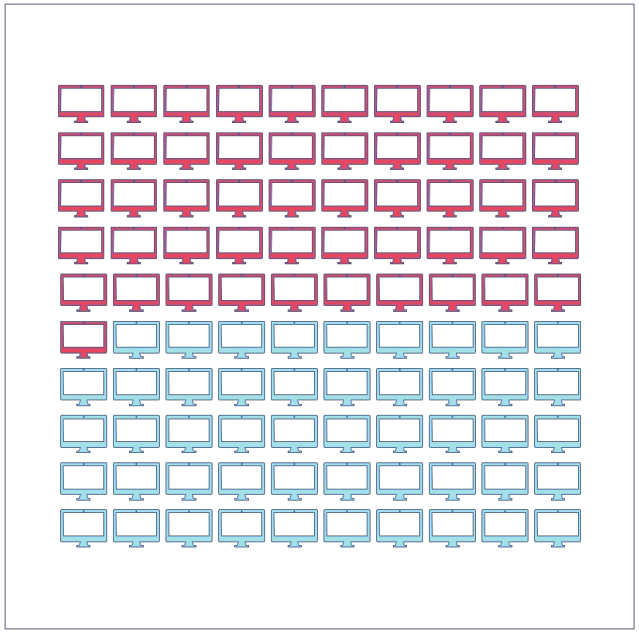
- Transaction receipts (UTXO)
- Receipt for a transaction is stored in a merkle root
- Receiving shard ensure that the receipt has not been spent
- Shared memory

Ethereum 2.0

Casper (PoS) + Sharding

(Slated for 2019 while sharding will follow in 2020 or 2021)

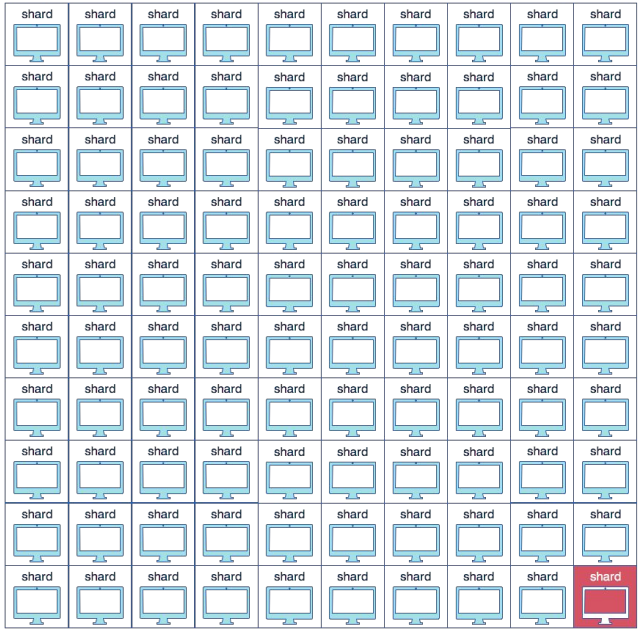
Trade-Off



Majority Attack, 51% Attack

> “Attacker controls a majority of network hash rate to revise transaction history.”

Trade-Off



1% Attack

> In 100 shards system, it takes only 1% of network hash rate to dominate the shard.

Other Solutions

- Zilliqa
- QuarkChain
- Raiden Network
- Loom Network
- ……

References

Provisioning Sharding for Smart Contracts: A Design for Zilliqa

Sharding FAQs

How to Scale Ethereum: Sharding Explained