

Sharding

and other things

About Me

- Early employee at NEAR protocol
- First dev hire for Developer Experience
- Working on sustainable behavior on the side
- Previously...
 - Trying to fix big pharma with data (didn't work)
 - Startups and Stanford
 - Engineer and general misanthrope

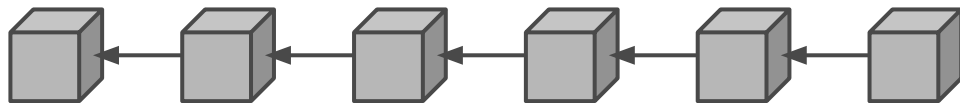
About NEAR Protocol

- Public Sharded Blockchain
- Emphasis on usability,
(specifically Developer Usability)
- A bunch of ex-MemSQL and ex-Google
- A group of ACM ICPC gold medalists
- A grip of previous founders

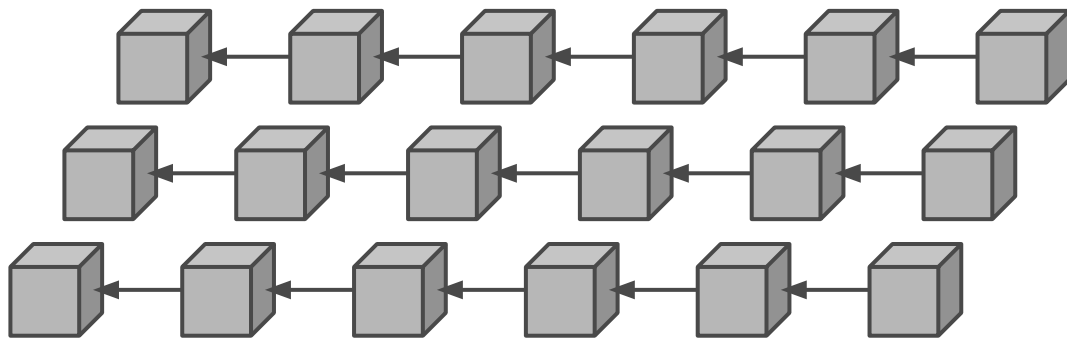
What we're talking about

1. Sharding, (in blockchains)
2. 10,000 ft view of crypto
3. Behavior (it relates to blockchain)

Sharding Overview

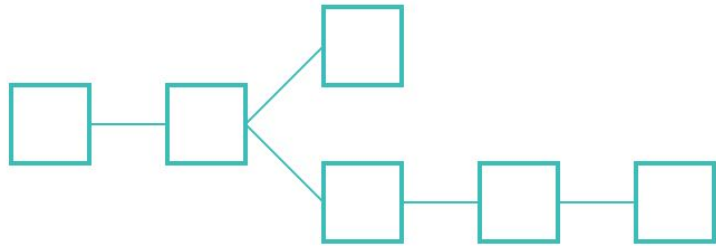


Sharding Overview

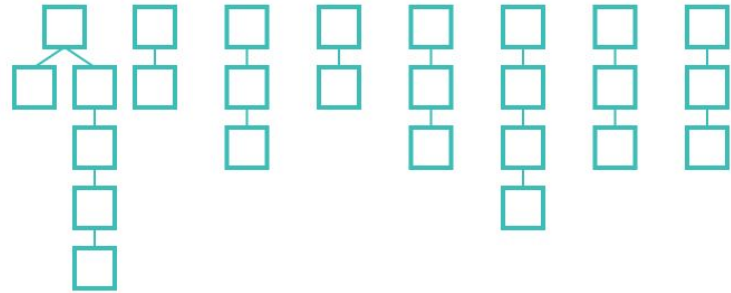


Corrupting Validators

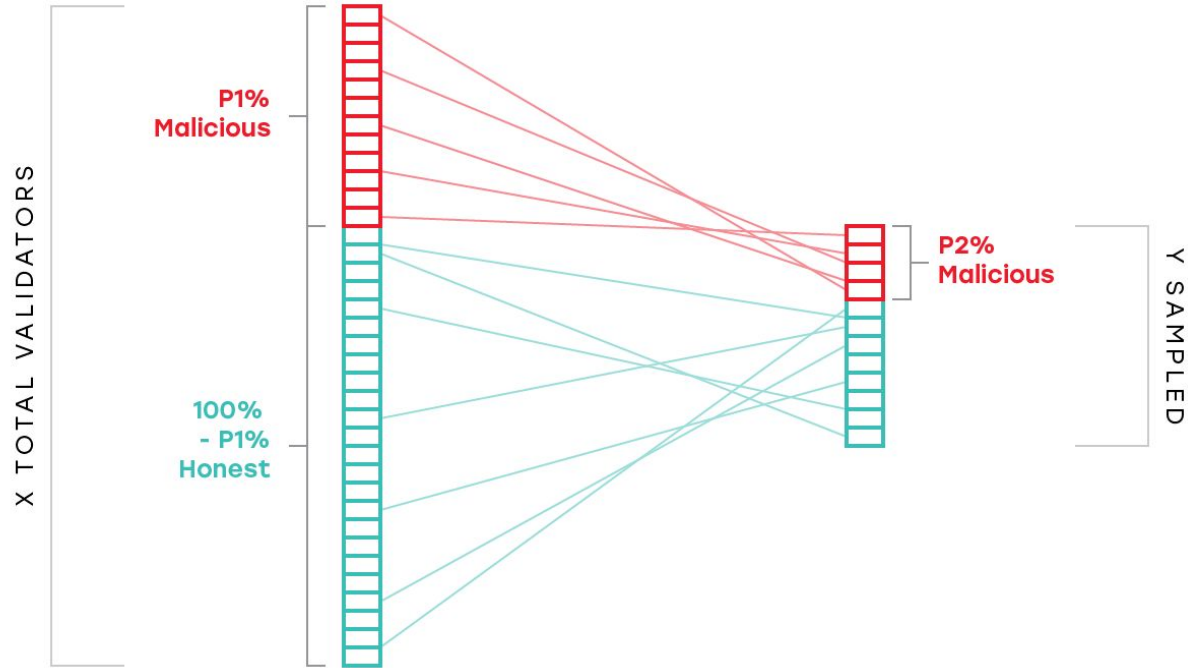
X validators building one chain.
Need to corrupt 0.51x



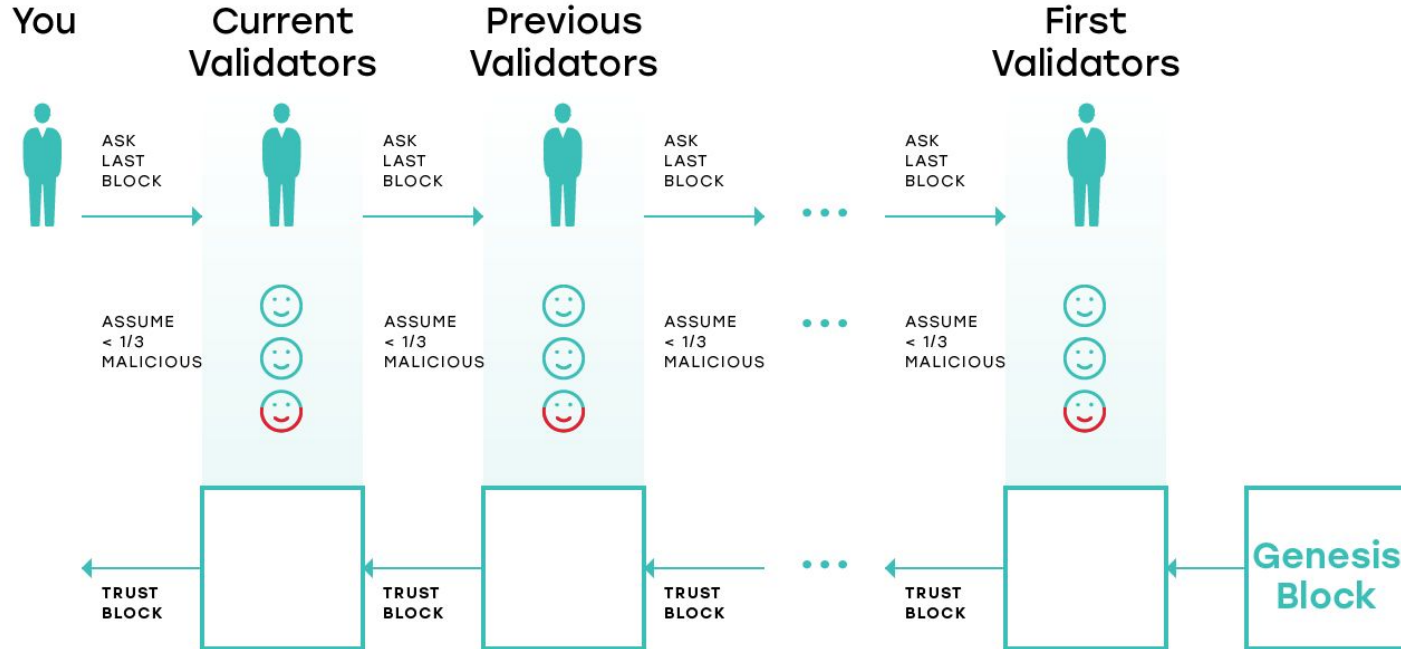
X validators building 10 chains
Need to corrupt 0.051x



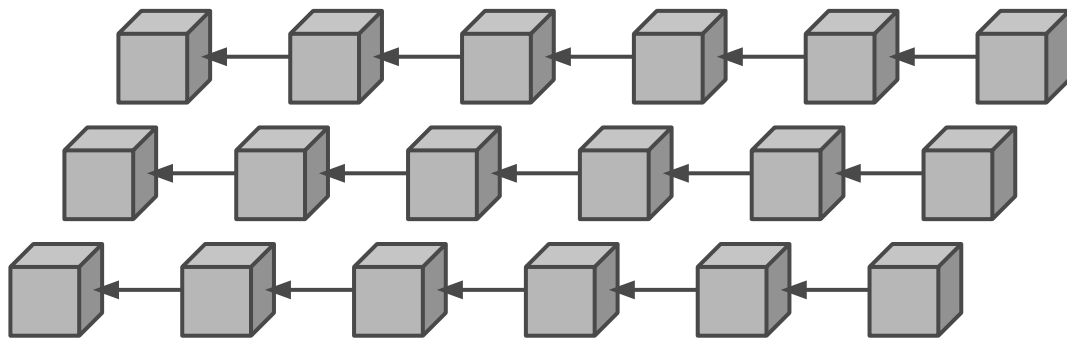
Sampling Validators



Sampling Validators



Sharding Overview



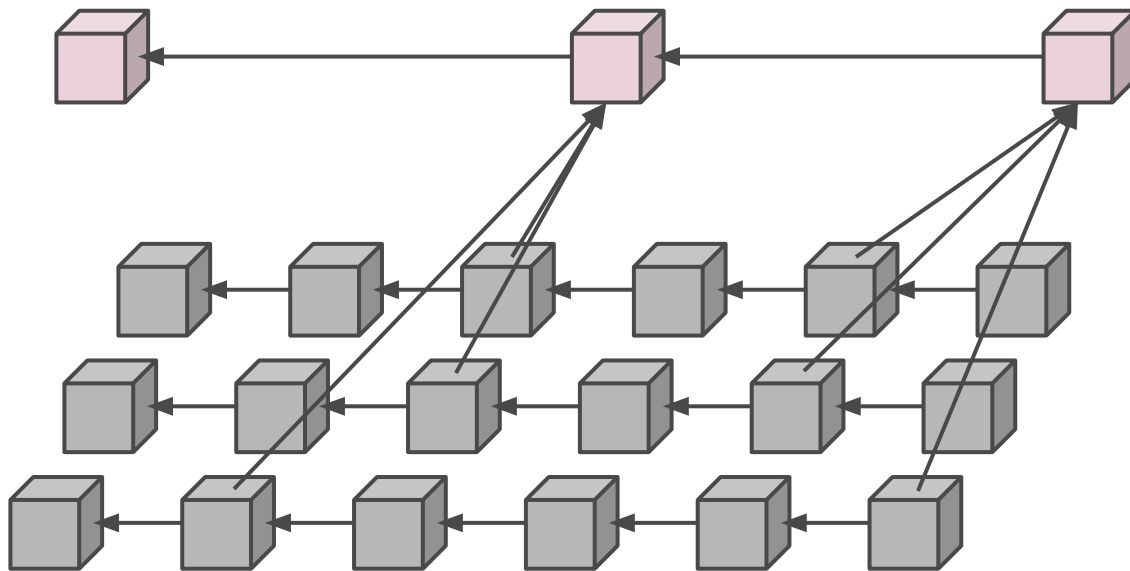
Sharding Overview

Main Chain

a.k.a.
Beacon Chain
Relay Chain
Hub

Shard Chains

a.k.a.
Parachains
Zones



Malicious Behavior

Forking

Invalid State Transitions

Invalid State Transition

Transaction X

From: **Alice**
To: **Bob**
Amt: **10**

Block A (Valid)

State Before: **Alice: 10, Bob: 0**
Transactions: **X**
State After: **Alice: 0, Bob: 10**

Block A' (Invalid)

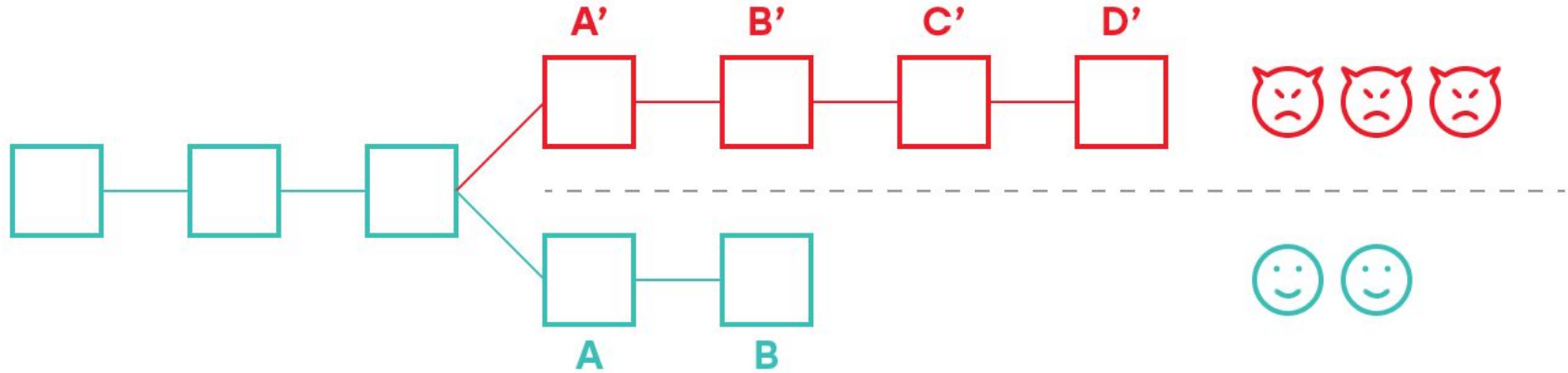
State Before: **Alice: 10, Bob: 0**
Transactions: **X**
State After: **Alice: 0, Bob: 1000**

Malicious Behavior **without** Sharding

✓ Forking

✗ Invalid State Transitions

Malicious Behavior **without** Sharding



Malicious Behavior **with** Cross-Shard Transactions

✓ Forking

✓ Invalid State Transitions

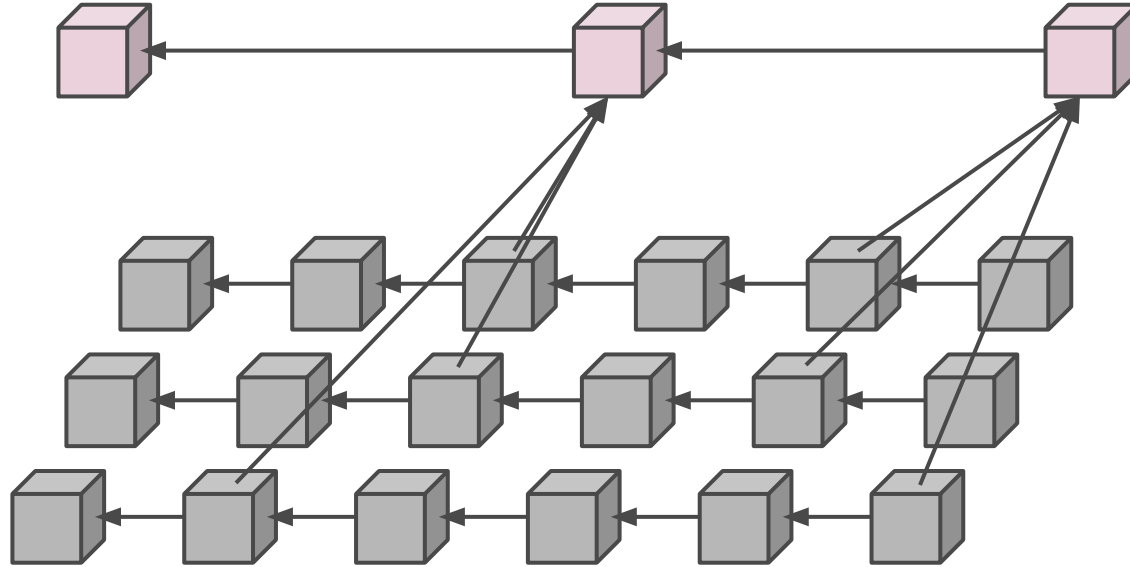
Cross-shard Communication

Main Chain

a.k.a.
Beacon Chain
Relay Chain
Hub

Shard Chains

a.k.a.
Parachains
Zones



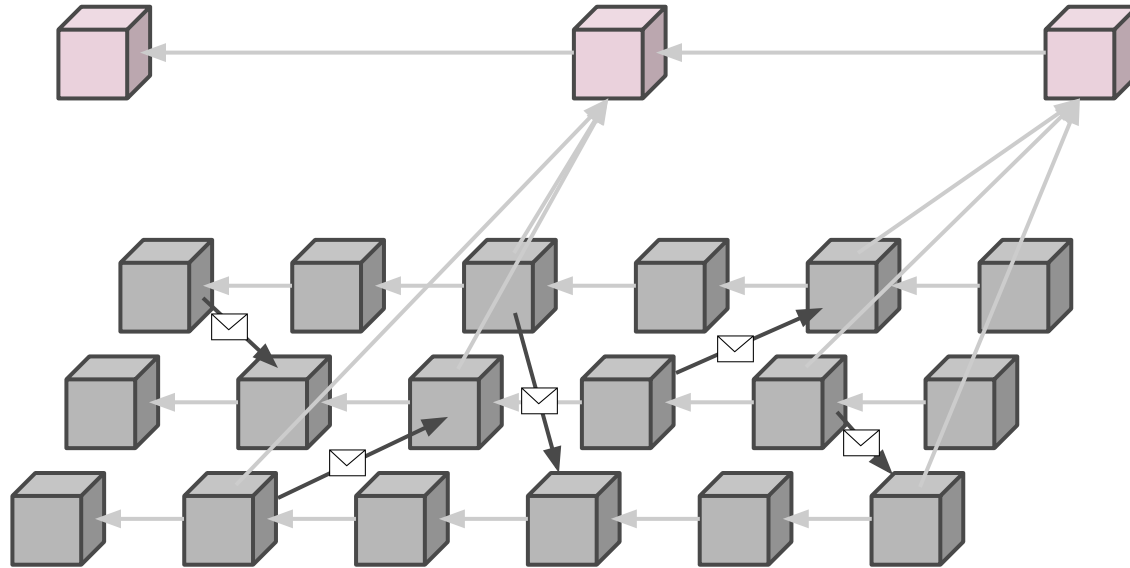
Cross-shard Communication

Main Chain

a.k.a.
Beacon Chain
Relay Chain
Hub

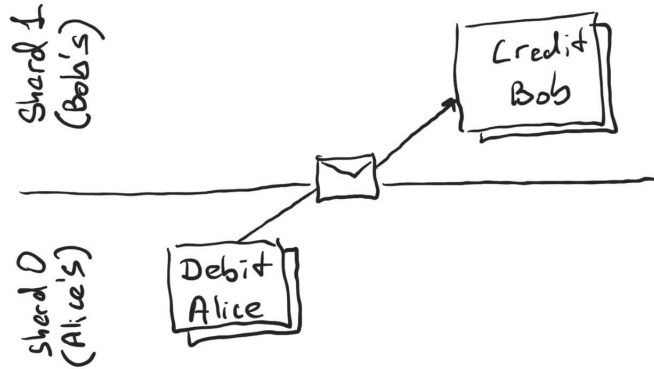
Shard Chains

a.k.a.
Parachains
Zones

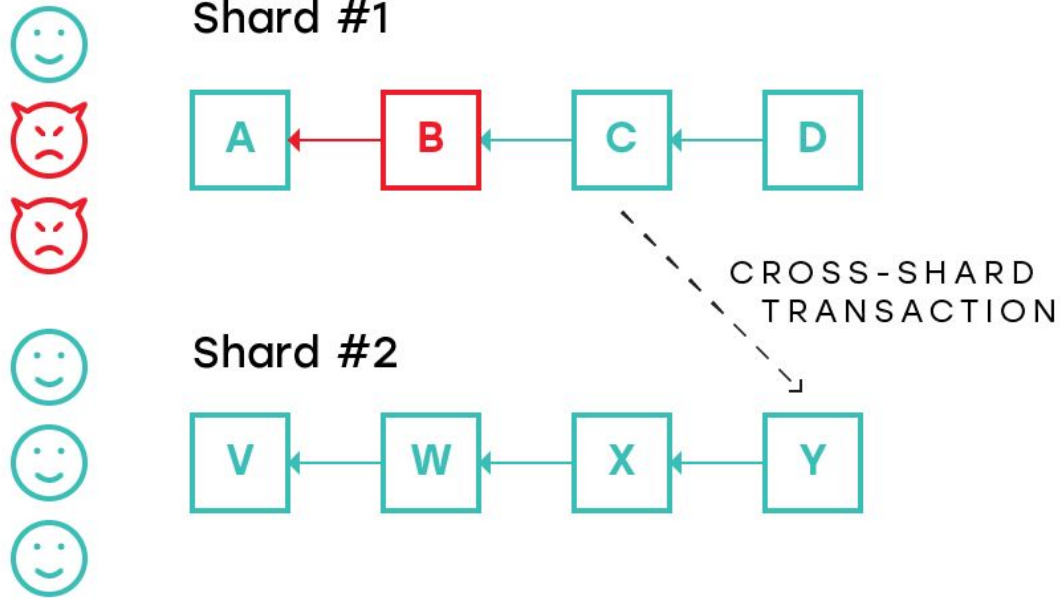


Cross-shard Communication: Receipts

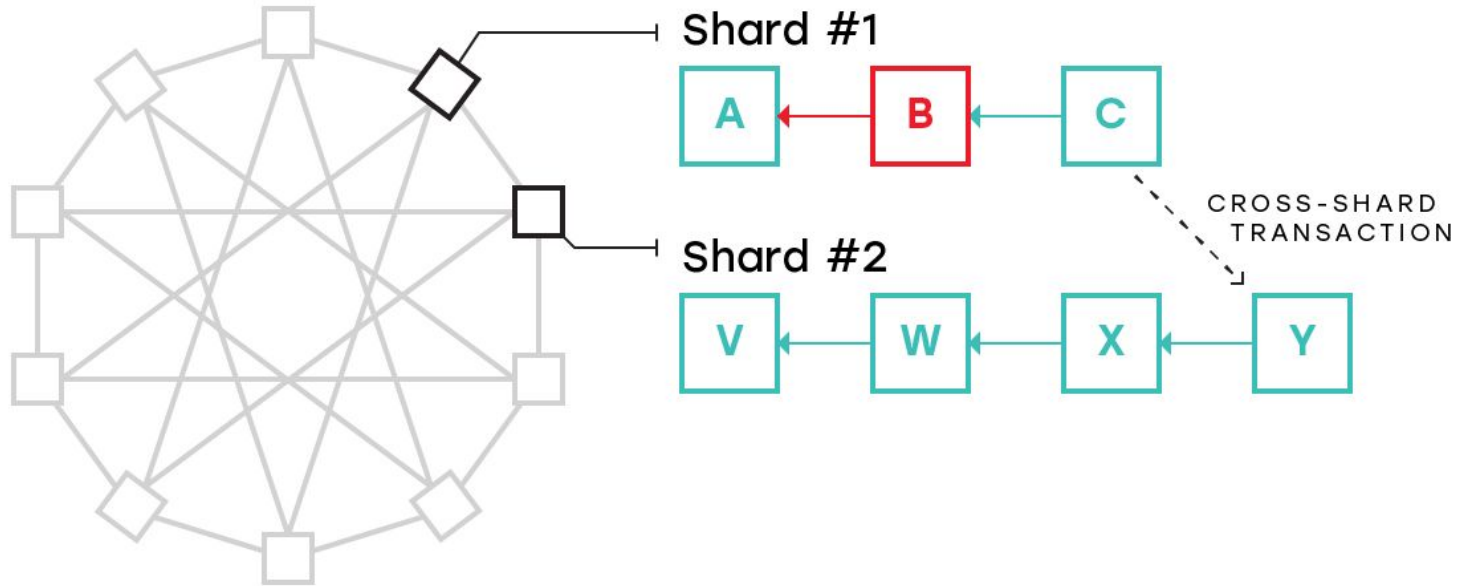
- Alice from Shard#1 sends money to Bob on Shard#2;
- A tx that debits Alice's account is executed on Shard#1;
- A proof of execution (Receipt) is created and sent to Shard#2;
- A tx that credits Bob's account is executed on Shard#2.



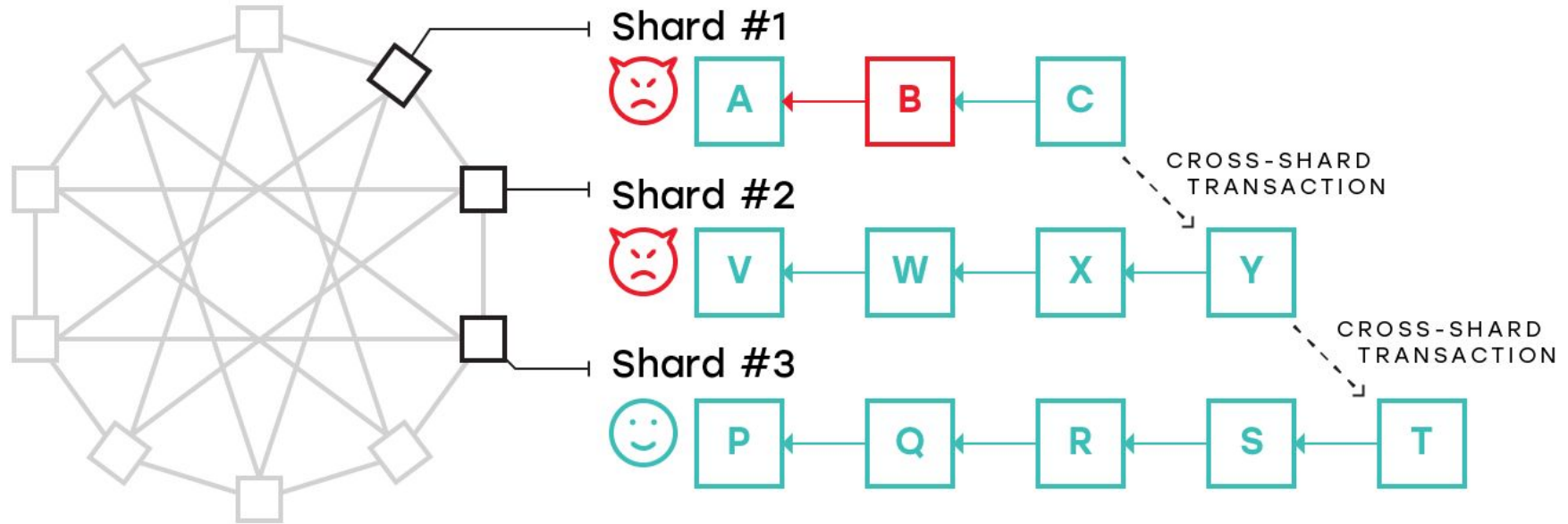
State Validity



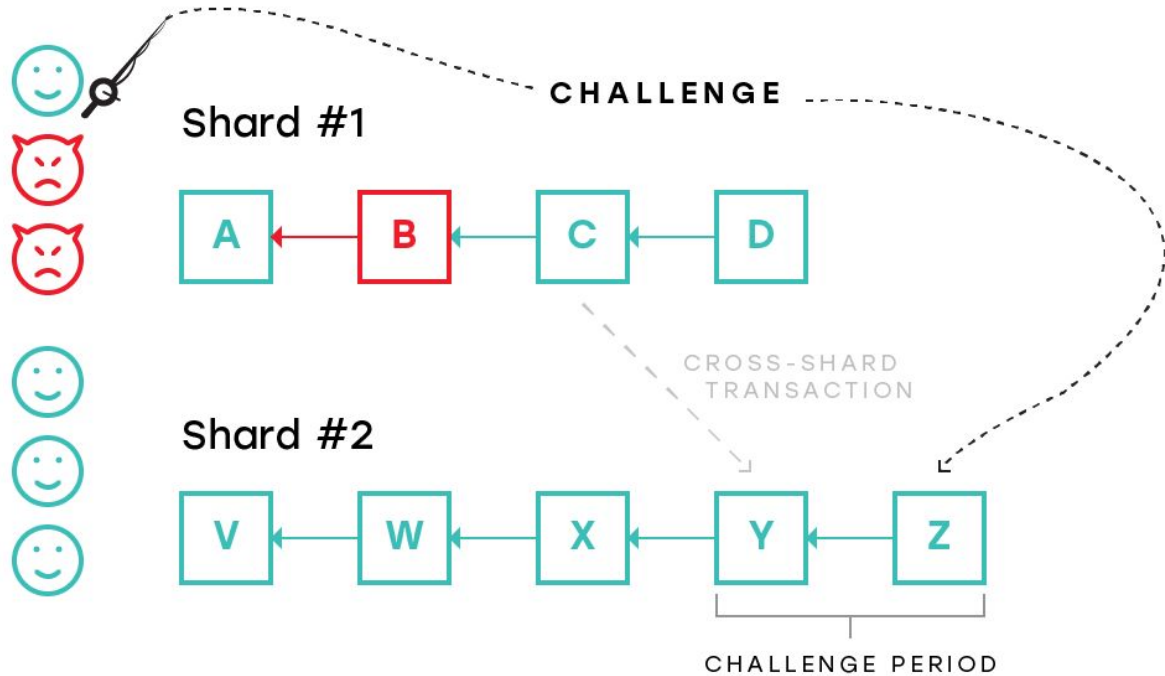
State Validity



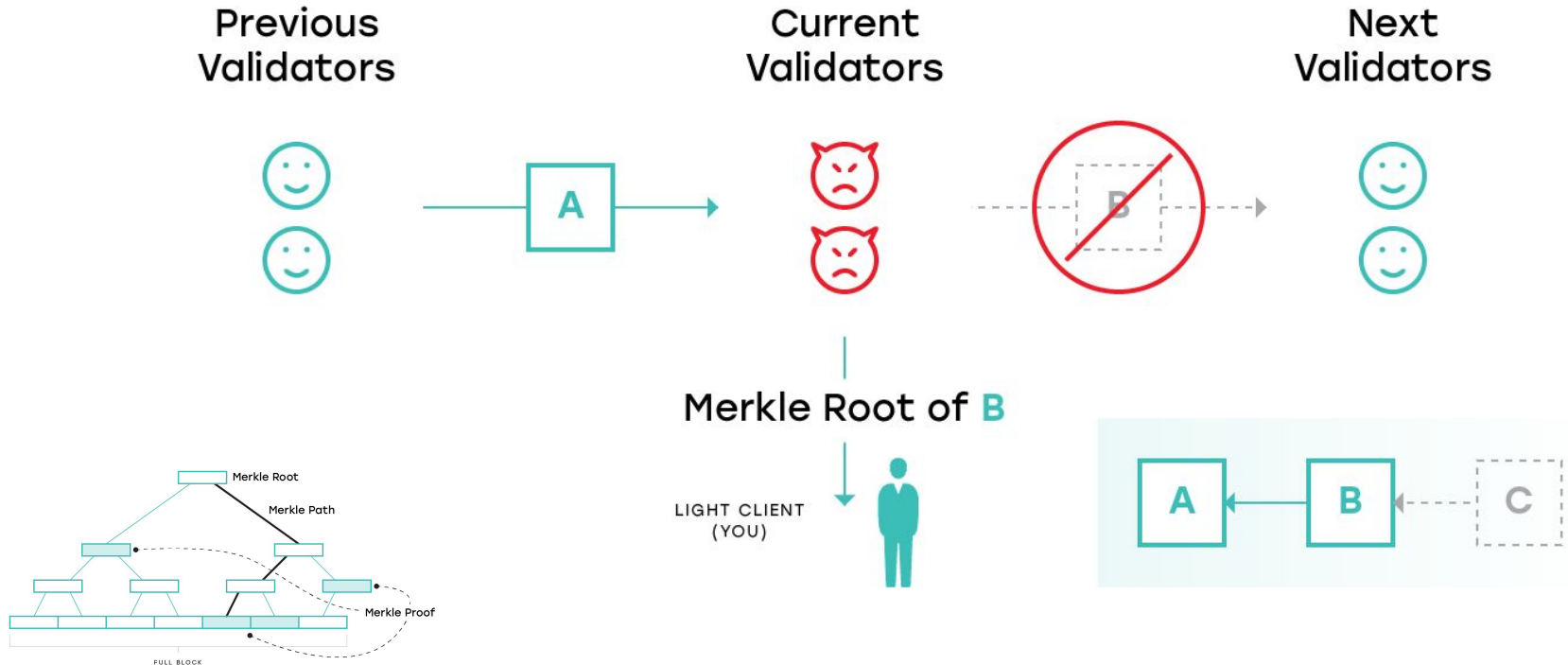
State Validity



Fisherman



Data Availability



Data Availability

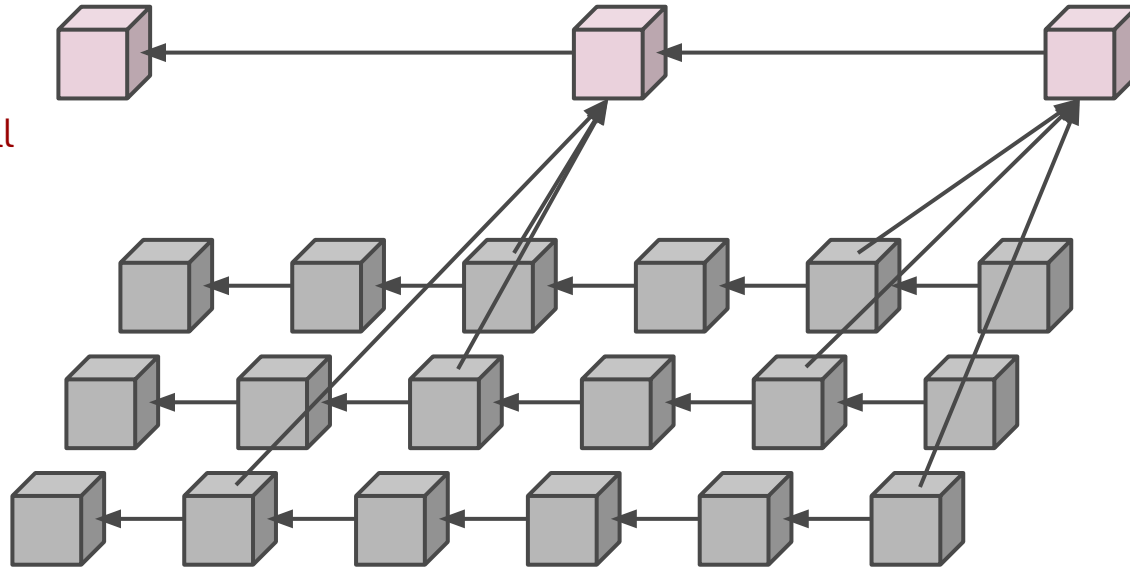
Main Chain

Light Client

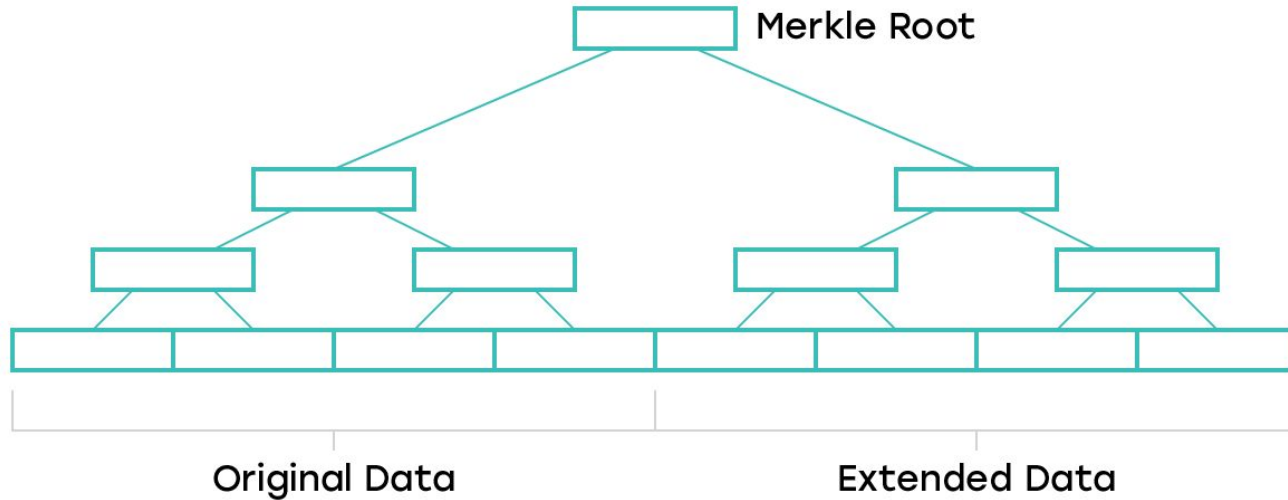
Can't download all
the blocks from
shard chains

Shard Chains

Full Nodes



Data Availability



Any n out of $2n$ are sufficient to reconstruct

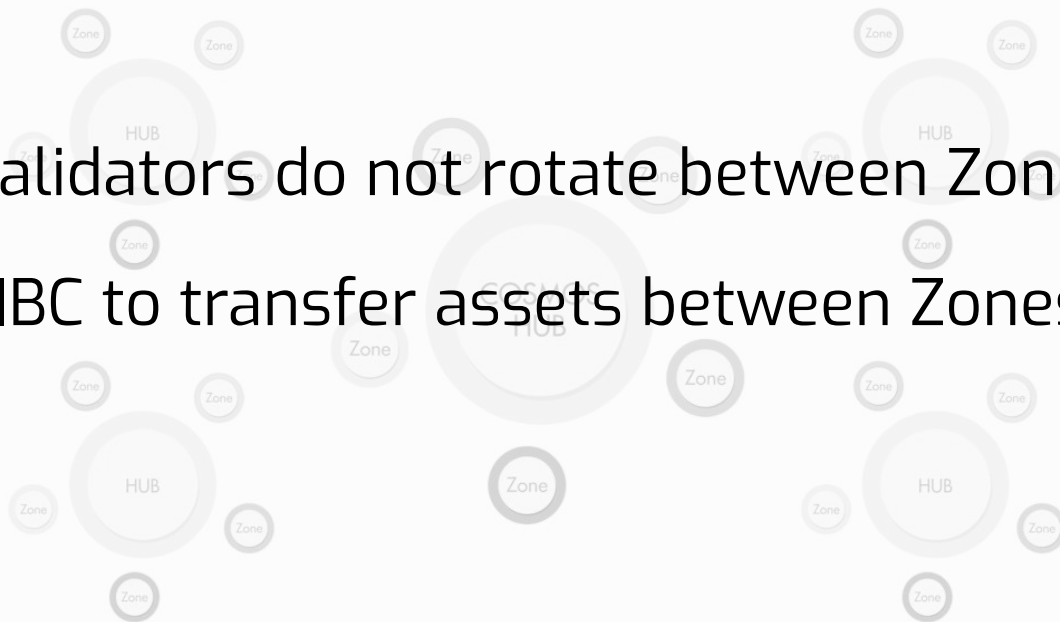
Proposed Protocols

Cosmos

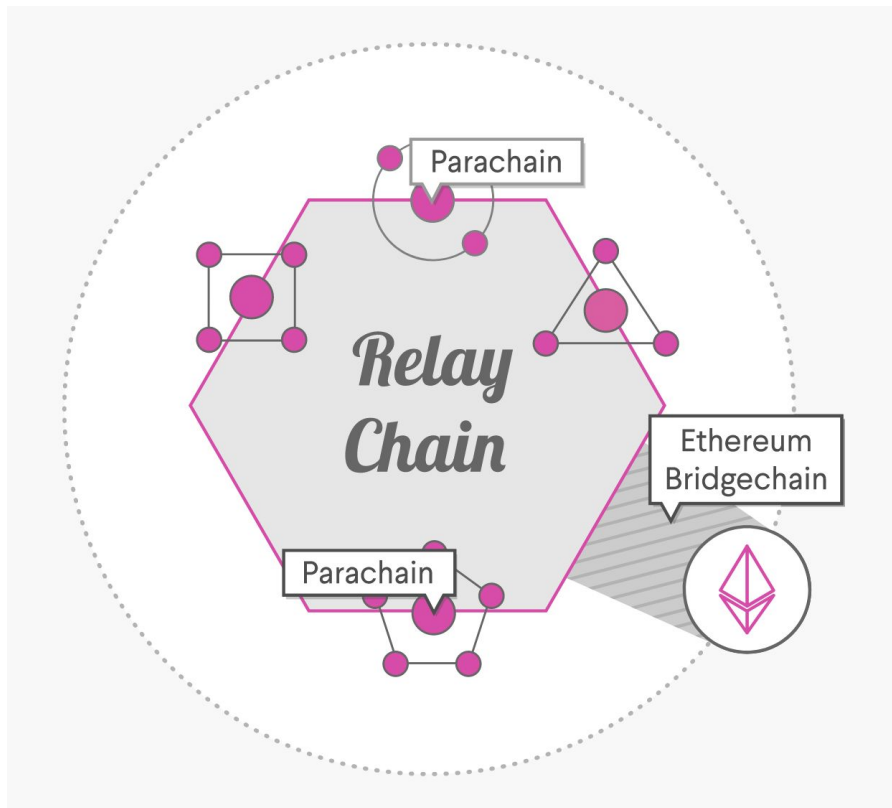


Cosmos

Validators do not rotate between Zones
IBC to transfer assets between Zones



Polkadot

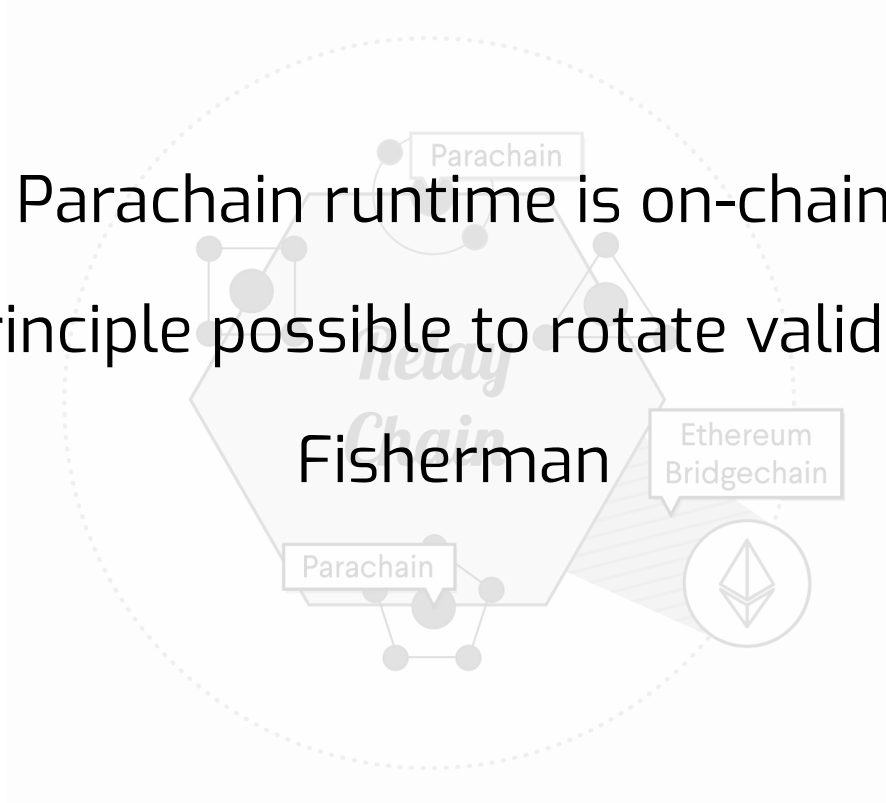


Polkadot

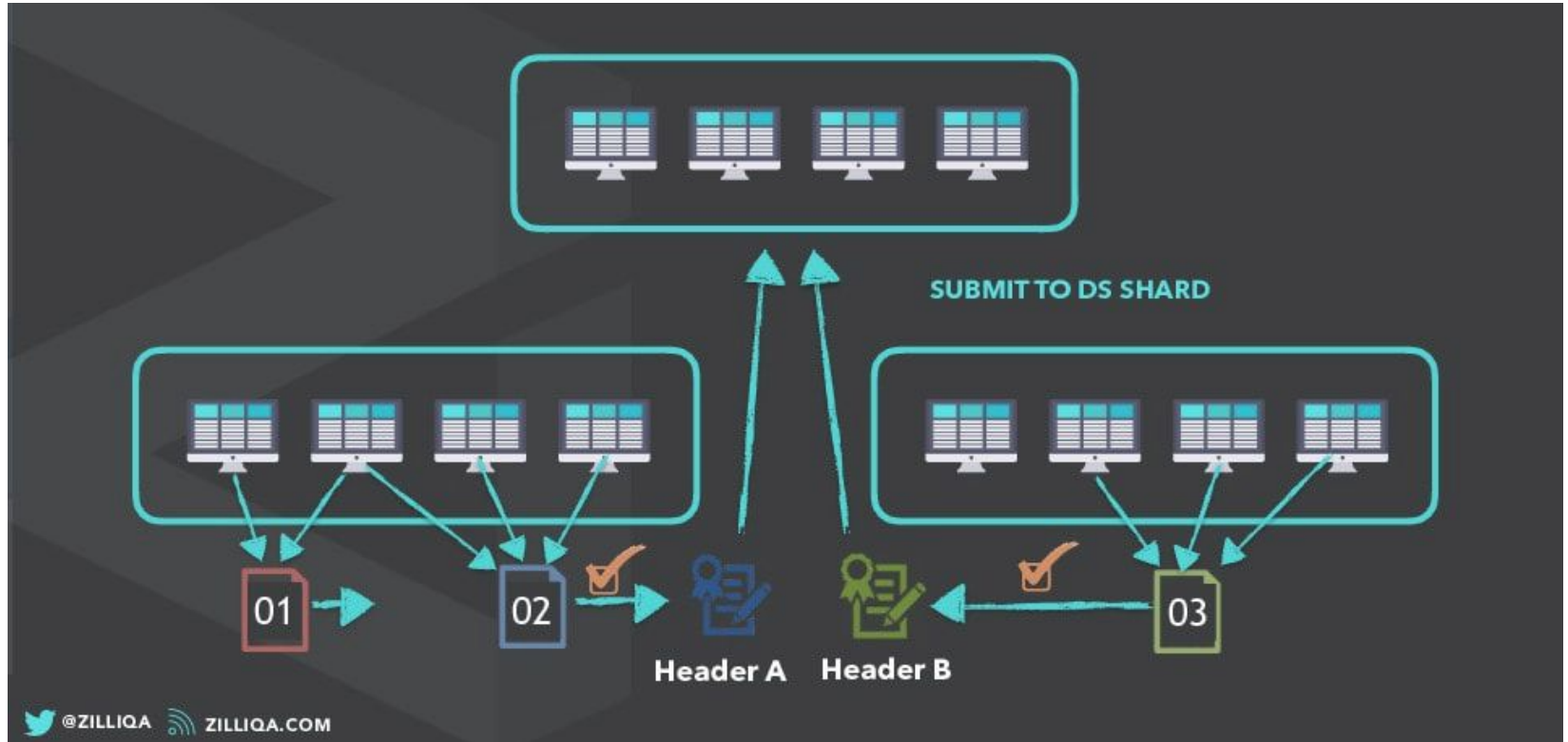
Parachain runtime is on-chain

In principle possible to rotate validators

Fisherman



Zilliqa

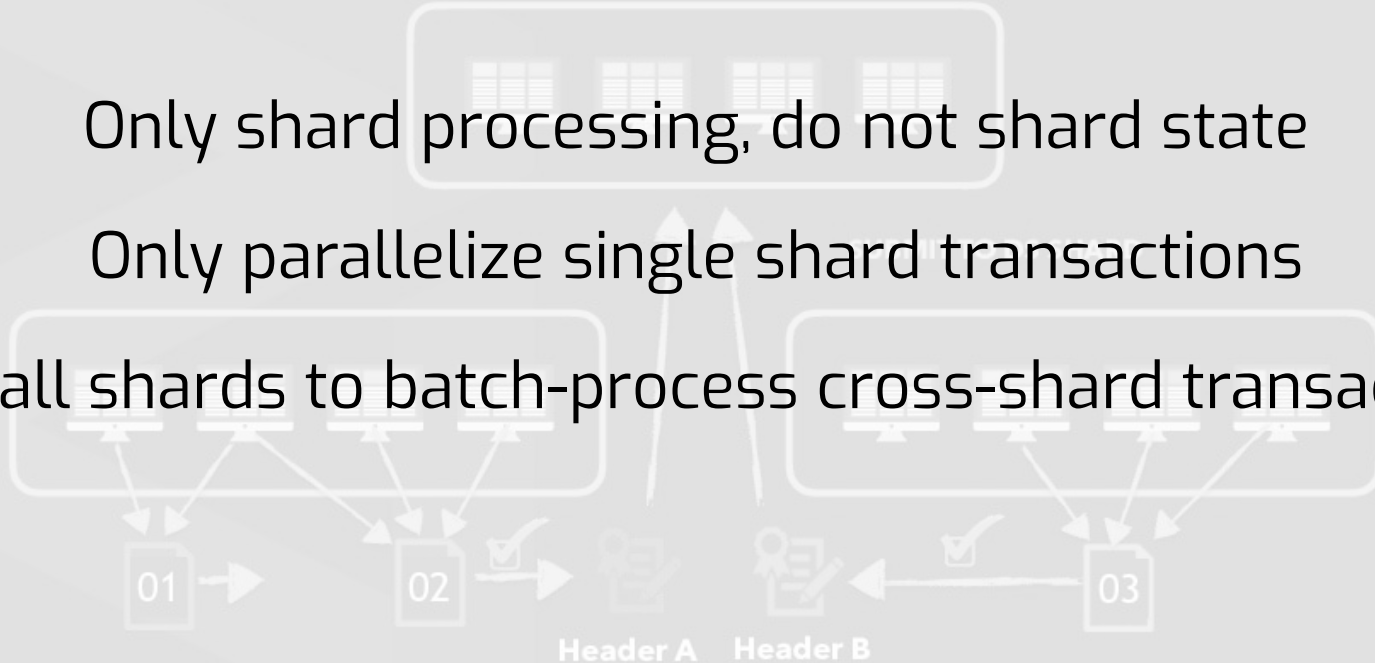


Zilliqa

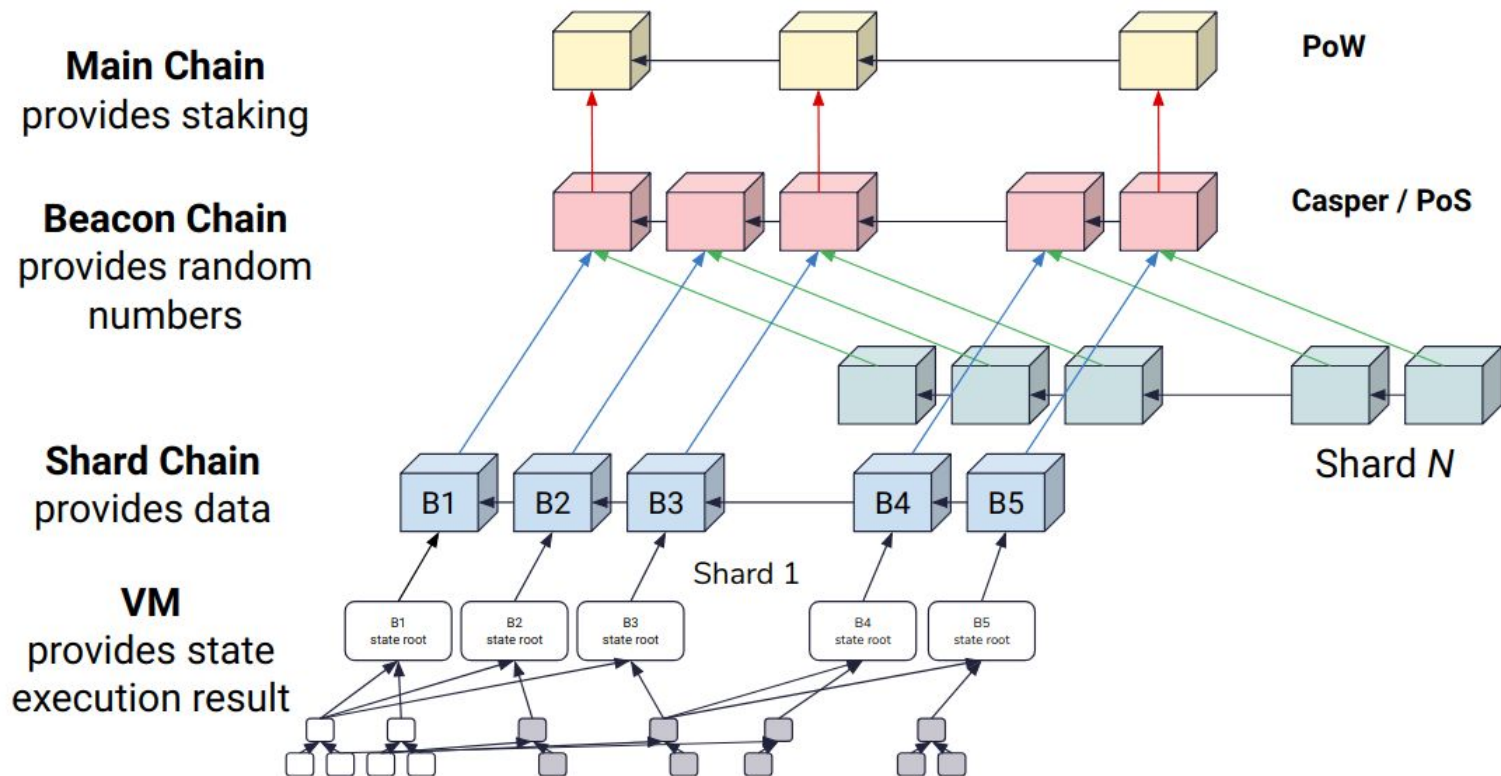
Only shard processing, do not shard state

Only parallelize single shard transactions

Stop all shards to batch-process cross-shard transactions

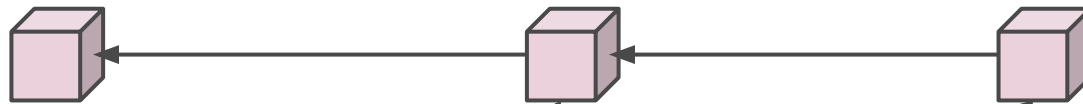


Ethereum Serenity

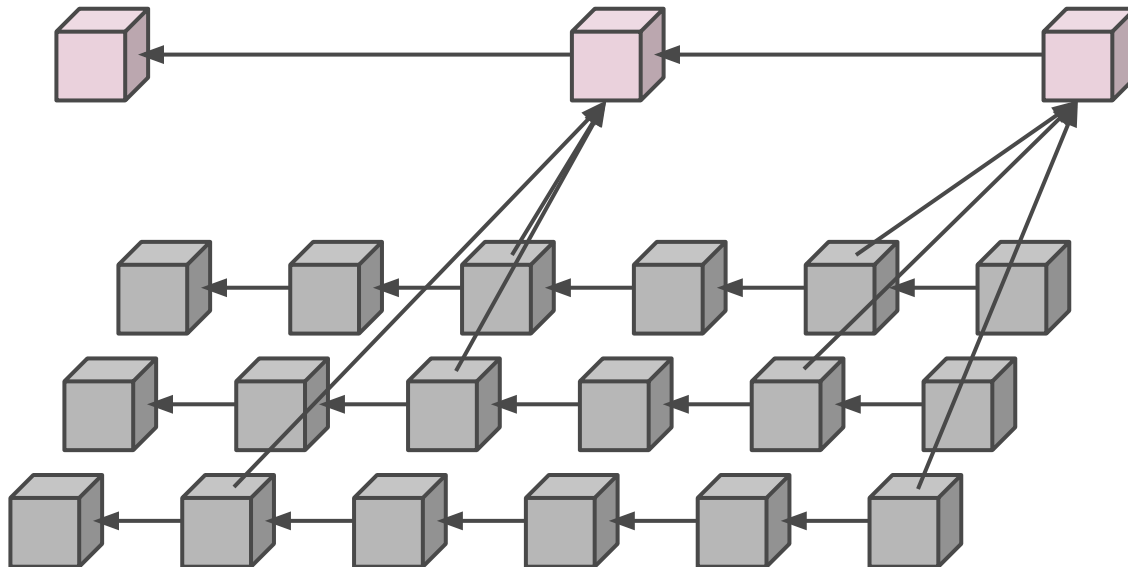


Near Protocol

Main Chain

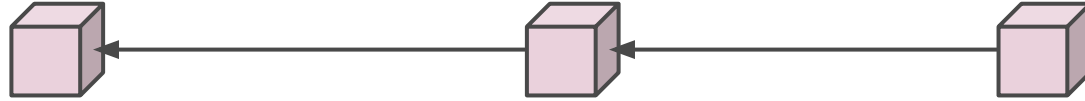


Shard Chains



Near Protocol vs Ethereum Serenity

Main Chain



Ethereum: **GHOST** + Casper FFG among **all validators**

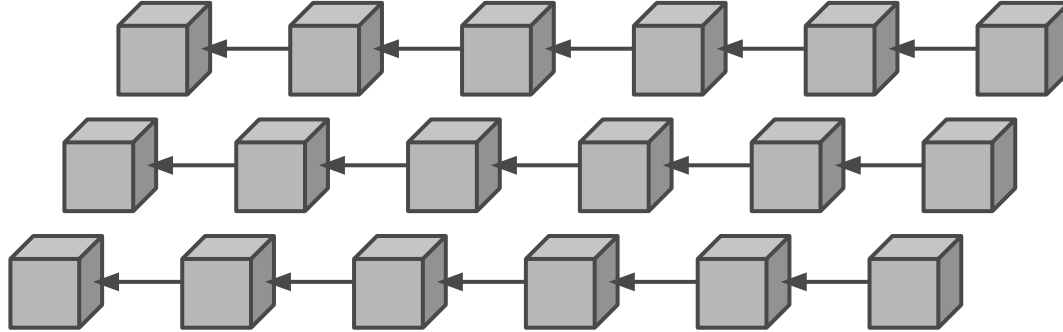
Near: **BFT** per block, validators rotate within one day

Near Protocol vs Ethereum Serenity

Ethereum: Proposers + Attesters + Cross-linking

Near: BFT per block

Shard Chains



Crypto/business

Behavior

As it relates to crypto

Behavior

As it doesn't relate to crypto

Thank You

Check out code

- <http://near.dev> -- example apps
- <http://github.com/nearcore> -- core chain code

Whiteboard Series (Cosmos, Solana, Ontology, more to come...)

- <http://near.ai/youtube>

Code is open, all the discussions are public

- <http://near.chat>

Nightshade: <https://near.org/papers/nightshade/> and