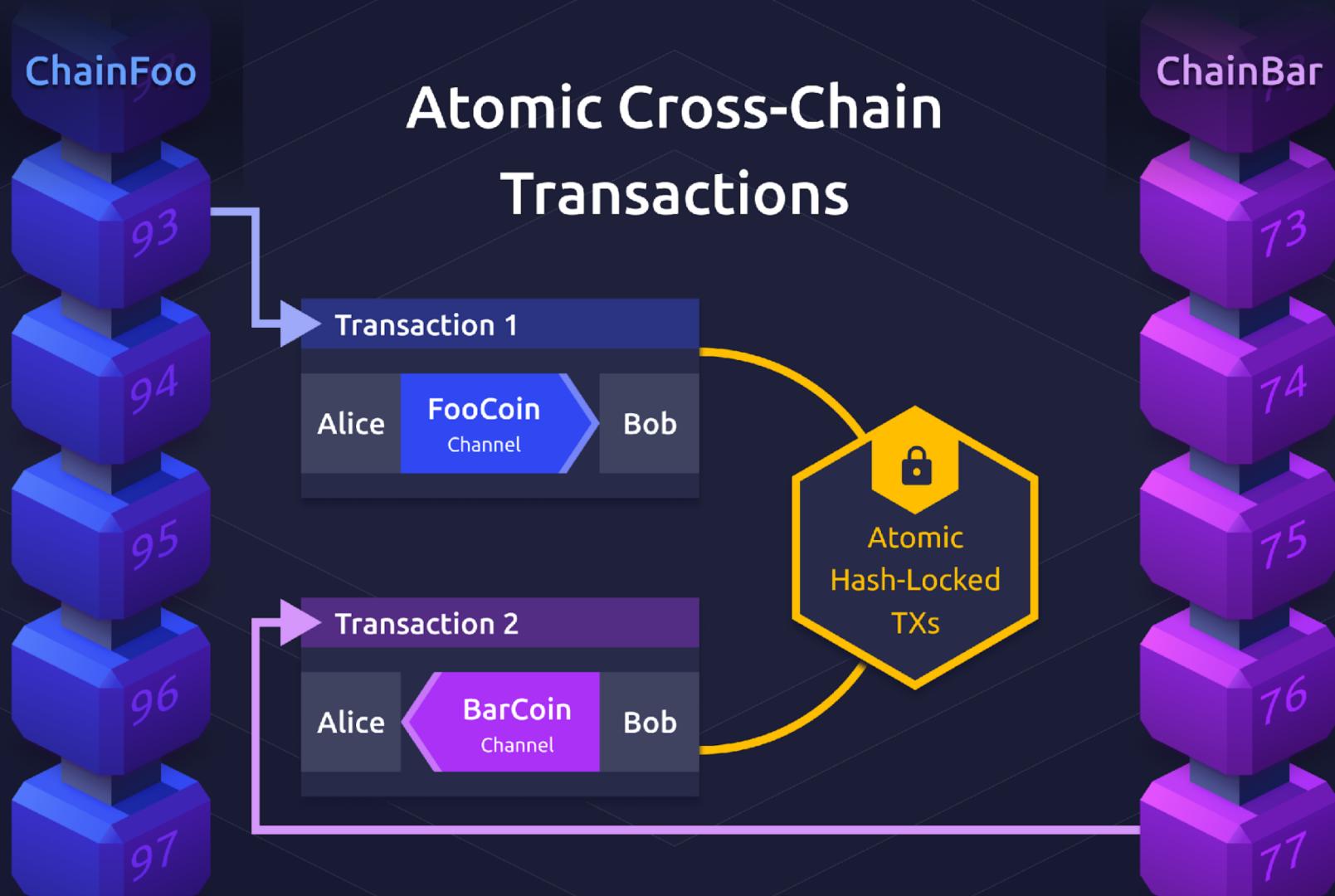


INTERCHAIN

Scaling & Security Models

Jae Kwon - Tendermint & Cosmos

Atomic Cross-Chain Transactions



Atomic Cross-Chain Transactions

“When transaction A succeeds, B succeeds”

- w/ hash commit-reveal scheme
- w/ “notaries”

Linked Payment/State Channels

Mutually signed checkpoints w/ “good” recovery.

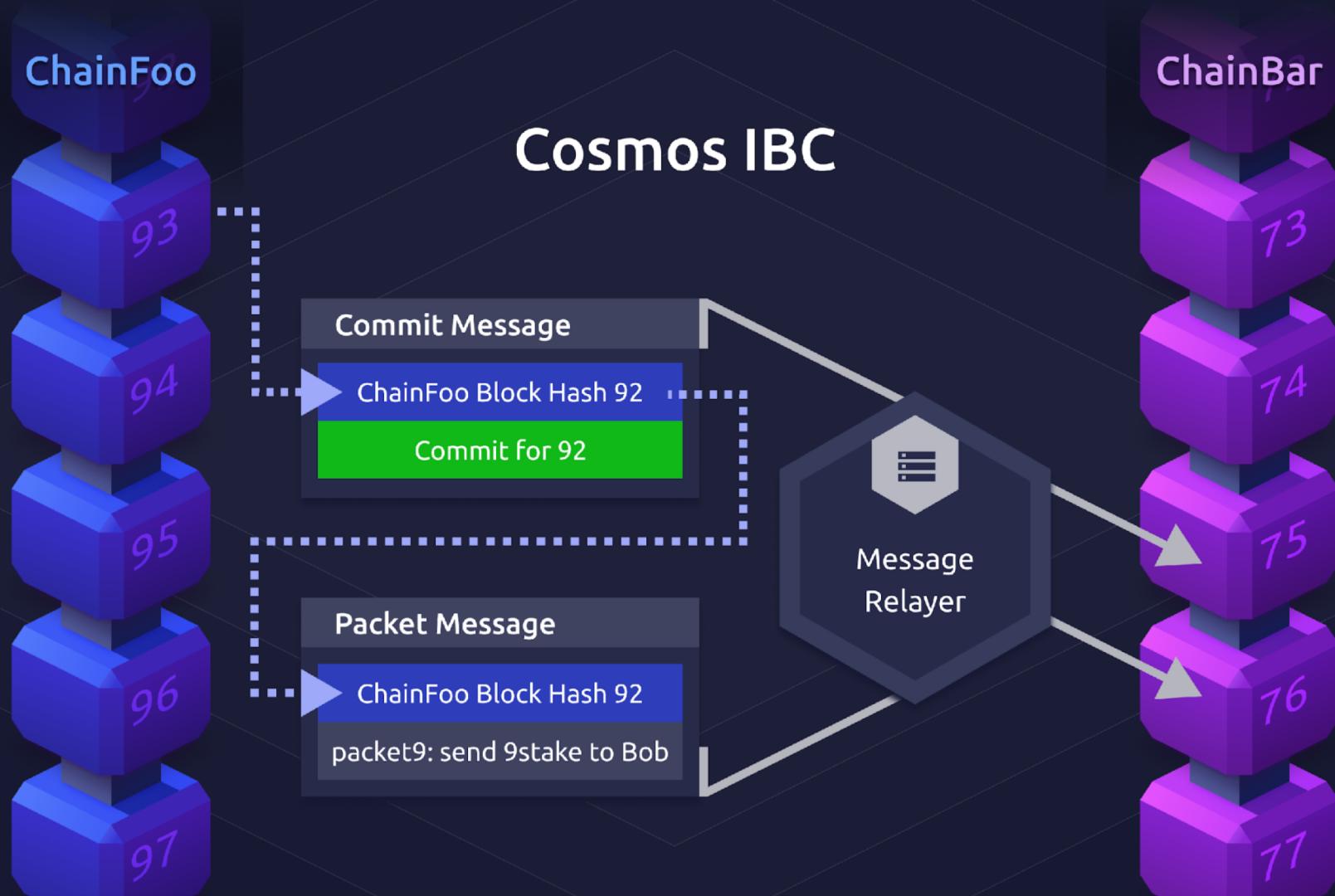
A connected network of channels (like the Lightning Network) can span across many independent blockchains.

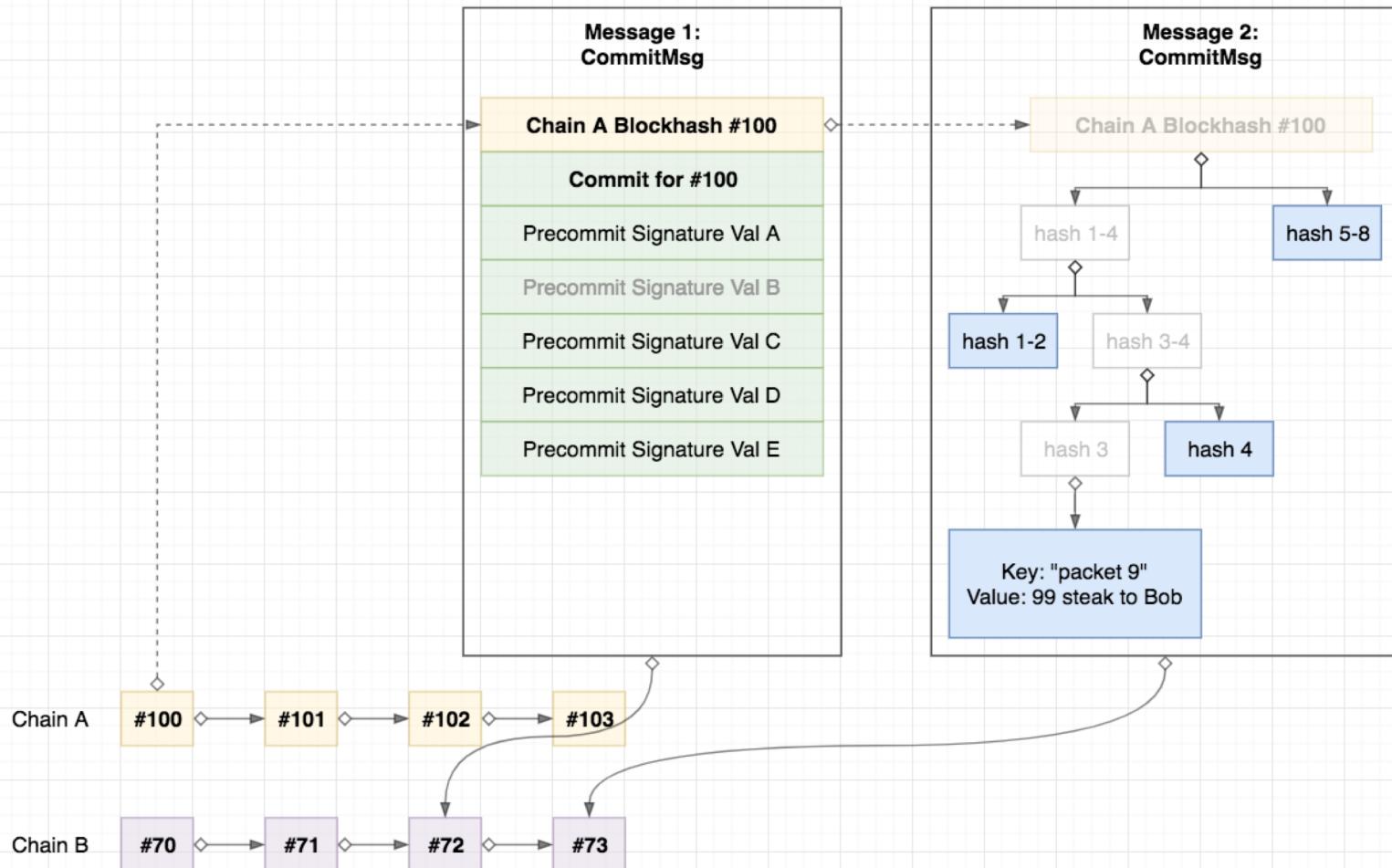
For fungible things, maybe have more checkpoints (e.g. sending pennies w/ credit buffer).

Linked Payment/State Channels

Want: many participants to sign a checkpoint.
Get: asynchronous communication failure issues.
Need: BFT Consensus. (maybe).

Cosmos IBC





Cosmos IBC

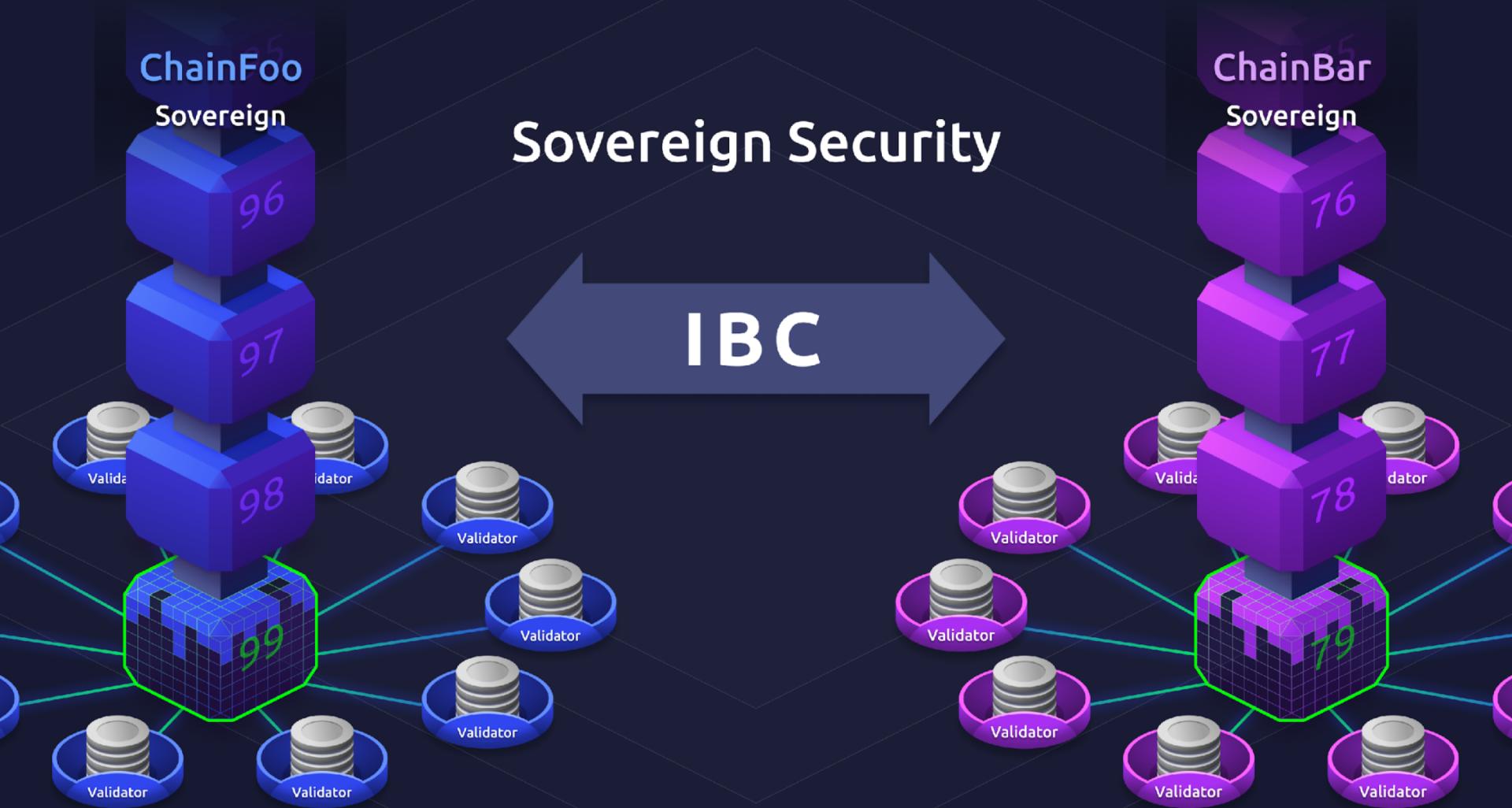
Chain A and chain B are light clients of each other.

IBC Packet (kinda like TCP/IP):

1. Prove the hash commit w/ signatures
2. Prove the packet w/ Merkle proof

Or, IBC State proves state.

Sovereign Security



Sovereign Security

2 chains w/ independent validator sets.

IBC connected between chain A and B.

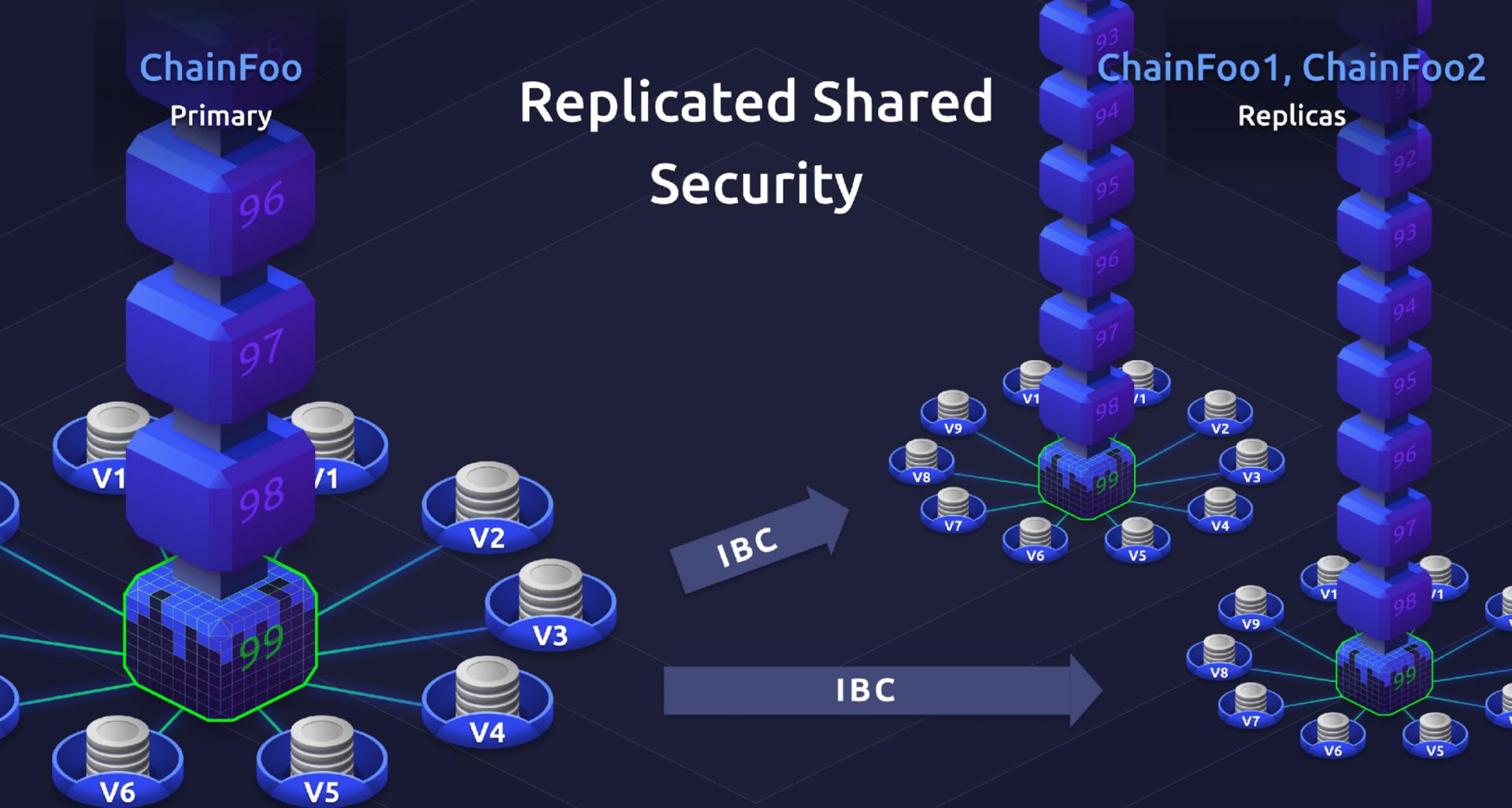
What about chain failure?

Sovereign Security

Fault recovery options (when B fails):

1. don't have one (CosmosClassic?)
2. decrease required signers over time
3. manual intervention aka “governance”
4. poll signers over period of time and decide
 - a. on chain A (the non-faulty chain)
 - b. on chain C, chosen by B (or D?)

Replicated Shared Security

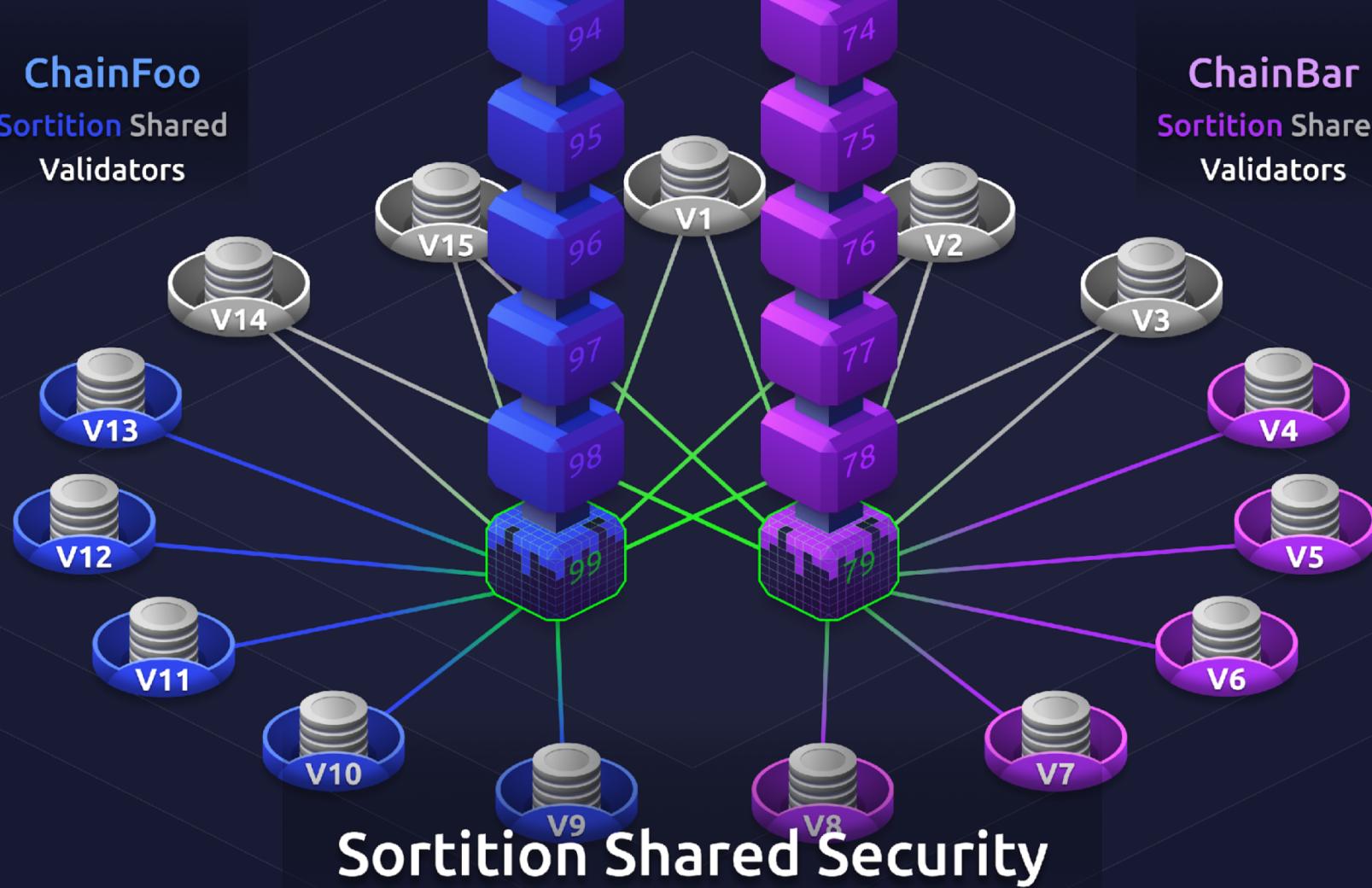


Replicated Shared Security

- Same validator set across many blockchains.
- Double-sign on chain B or C, and get slashed on A.
 - Chain A is the “master” - handles delegation etc
 - Chain B and C are “replicas”
- Hosted validator-as-a-service for scaling.

ChainFoo
Sortition Shared
Validators

ChainBar
Sortition Shared
Validators



Sortition (Sampled) Shared Security

- Pros: faster w/ smaller sortitions
- Cons: security is less w/ less at stake
- Combinations are also possible
 - e.g. Cosmos Hub validator signing on a sortition chain w/ shared atom staking.

Plug:

<https://cosmos.network>

github.com/cosmos/cosmos-sdk

<https://tendermint.com>

github.com/tendermint/tendermint

// build stuff that matters

[careers@tendermint.com](mailto:ccareers@tendermint.com)