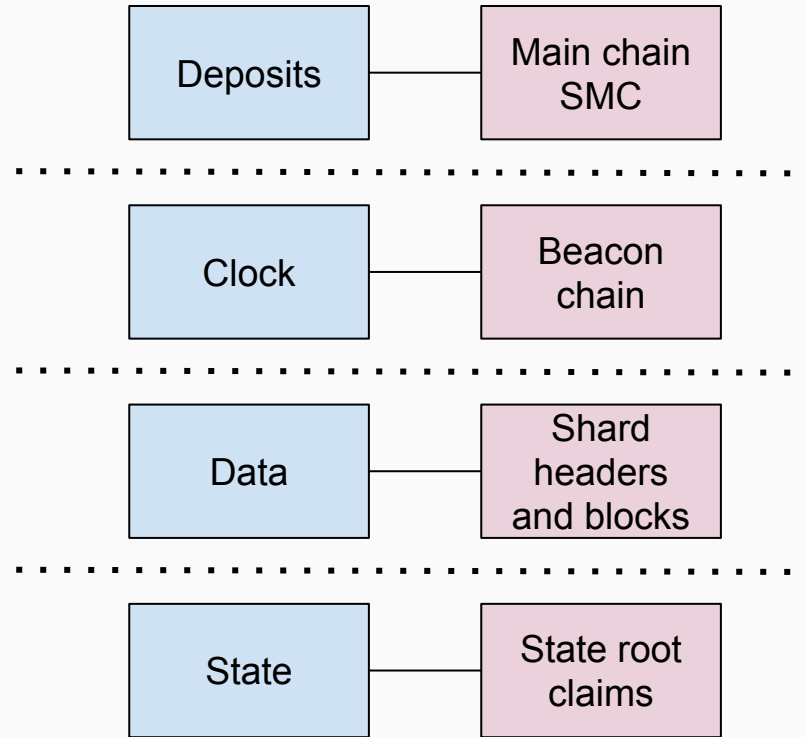


Ethereum sharding

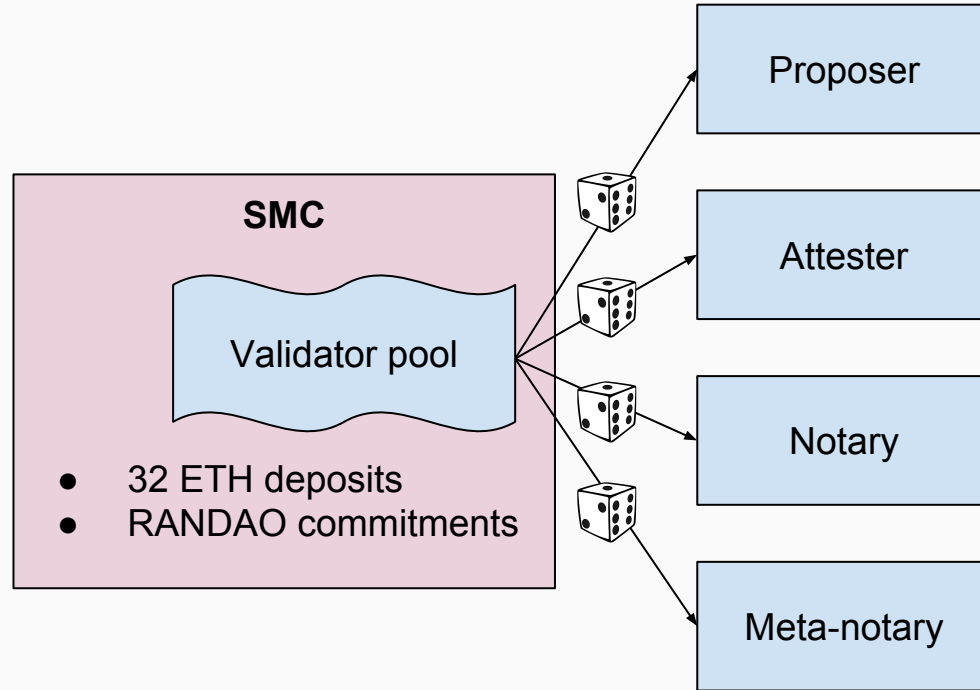
Research update



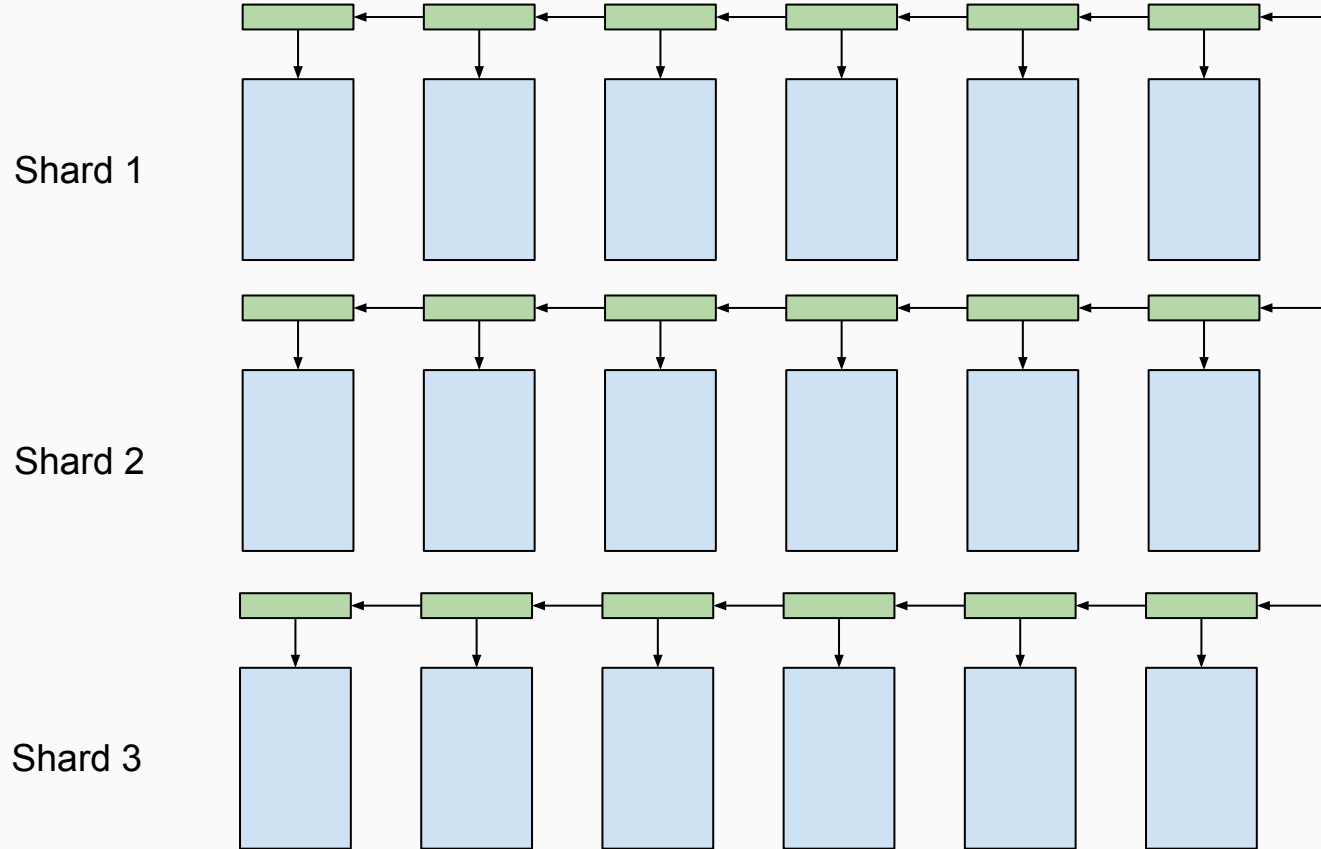
Modular design



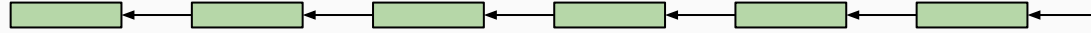
Validators



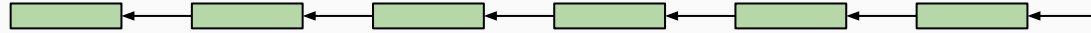
Shards



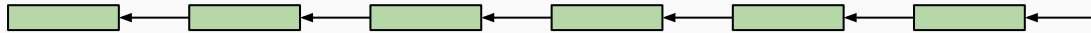
Shards



Shard 1

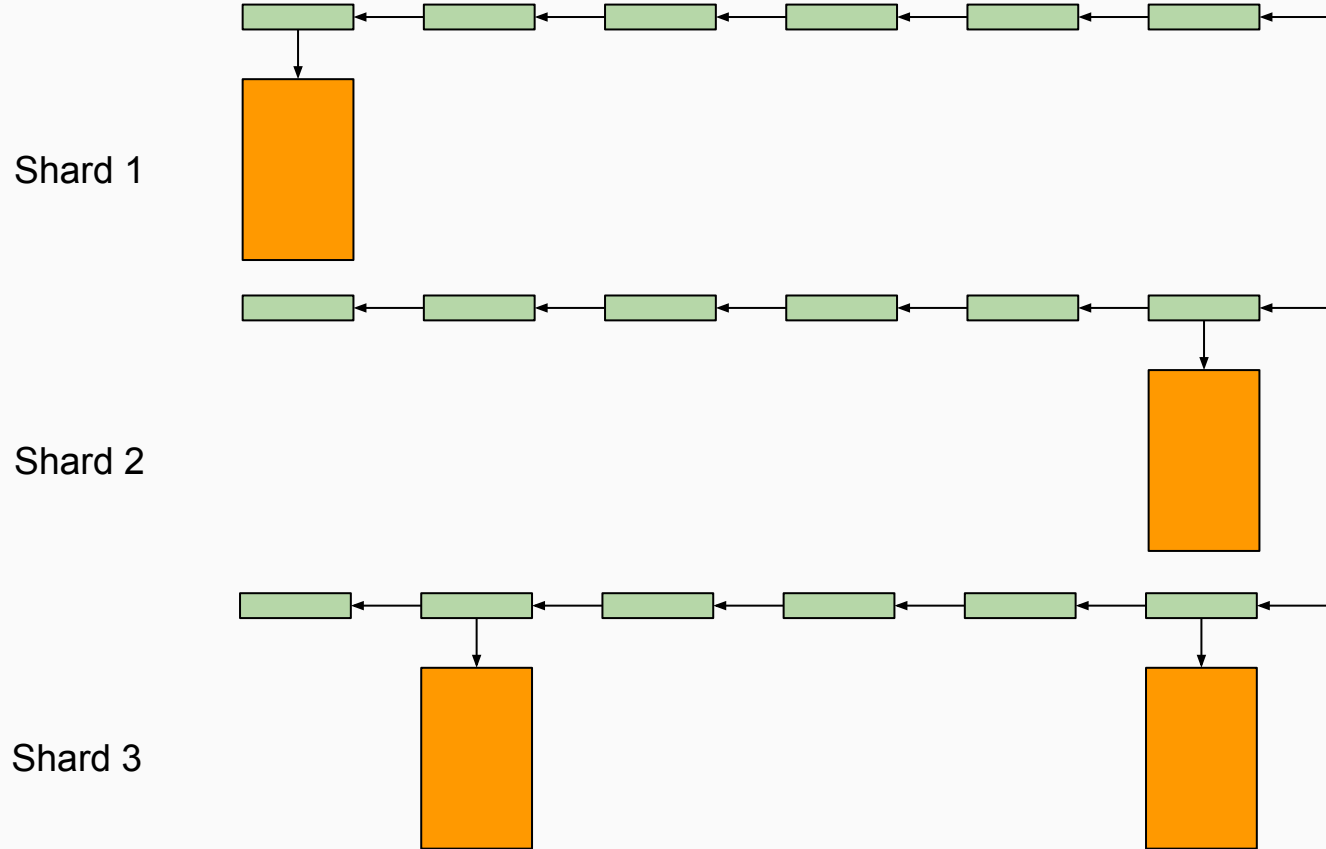


Shard 2



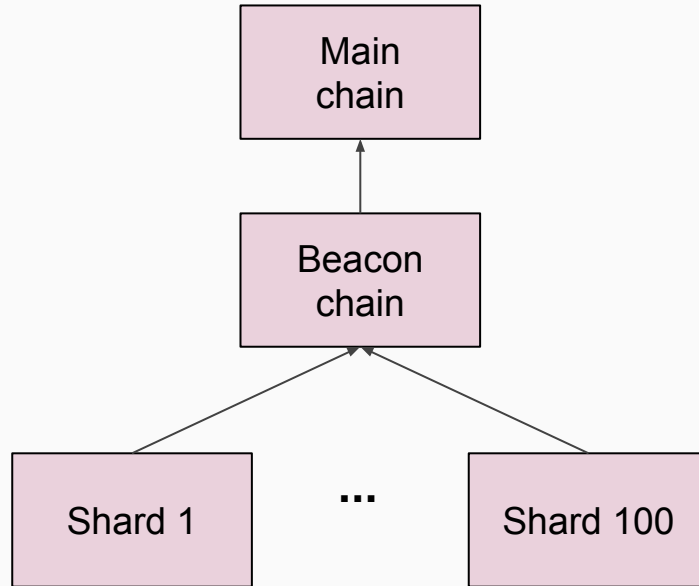
Shard 3

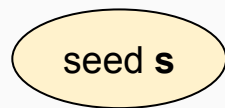
Shards



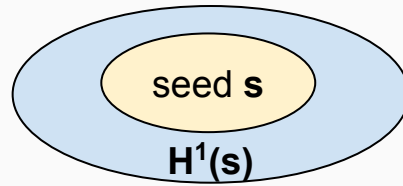
Random beacon

Common heartbeat

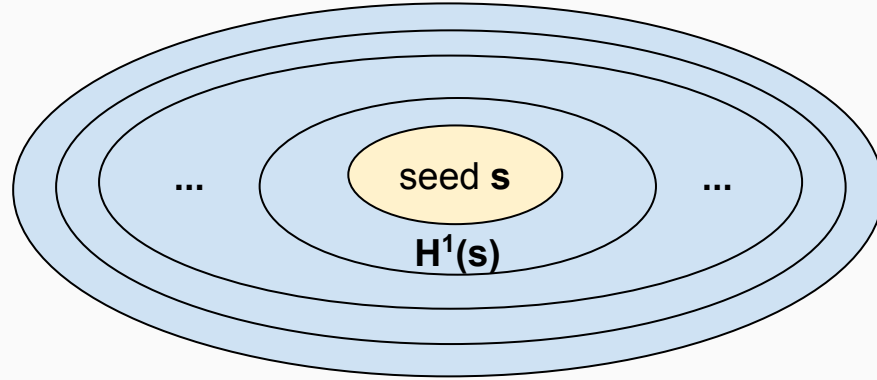




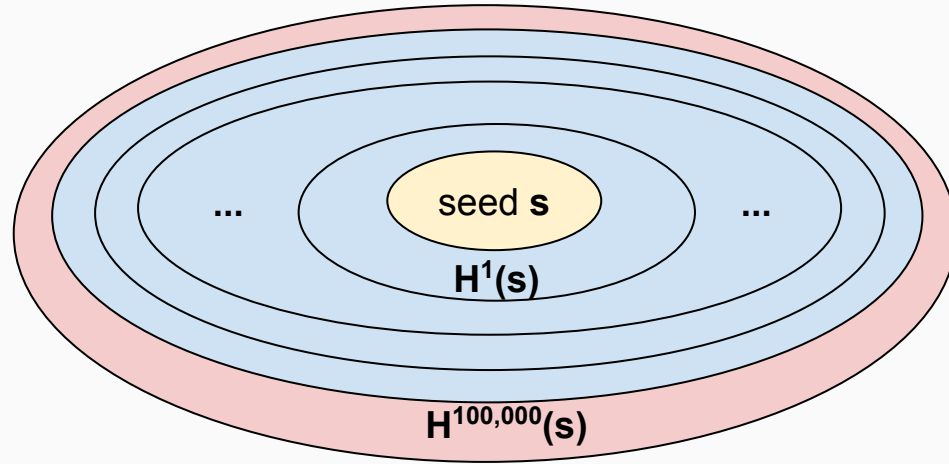
Hash onions



Hash onions

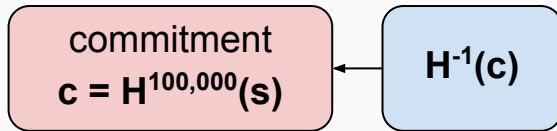
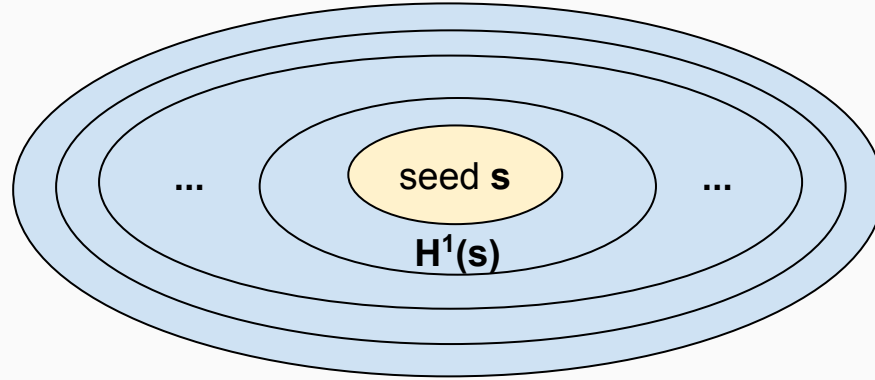


Hash onions

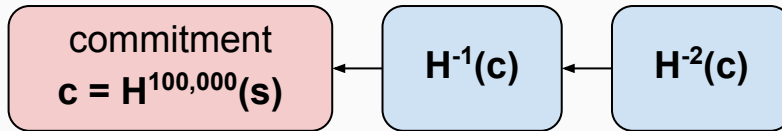
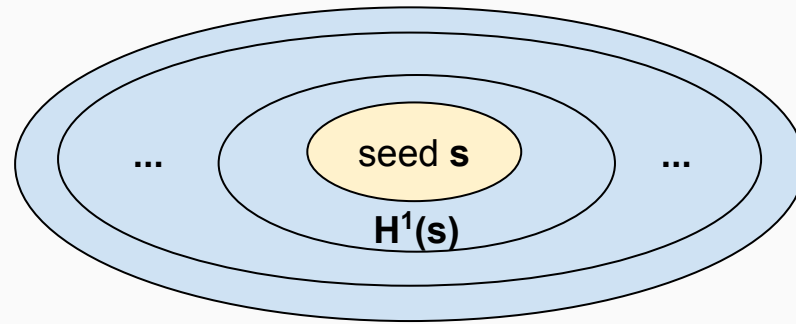


commitment
 $c = H^{100,000}(s)$

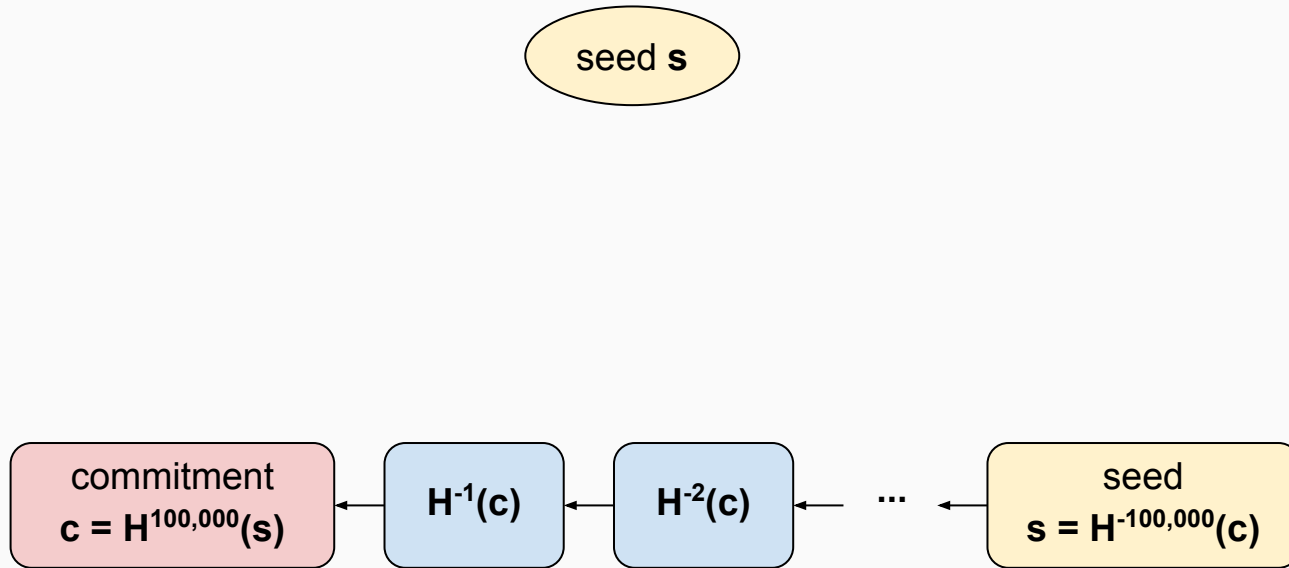
Hash onions



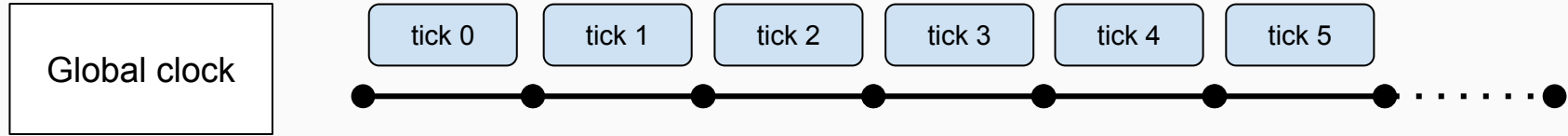
Hash onions



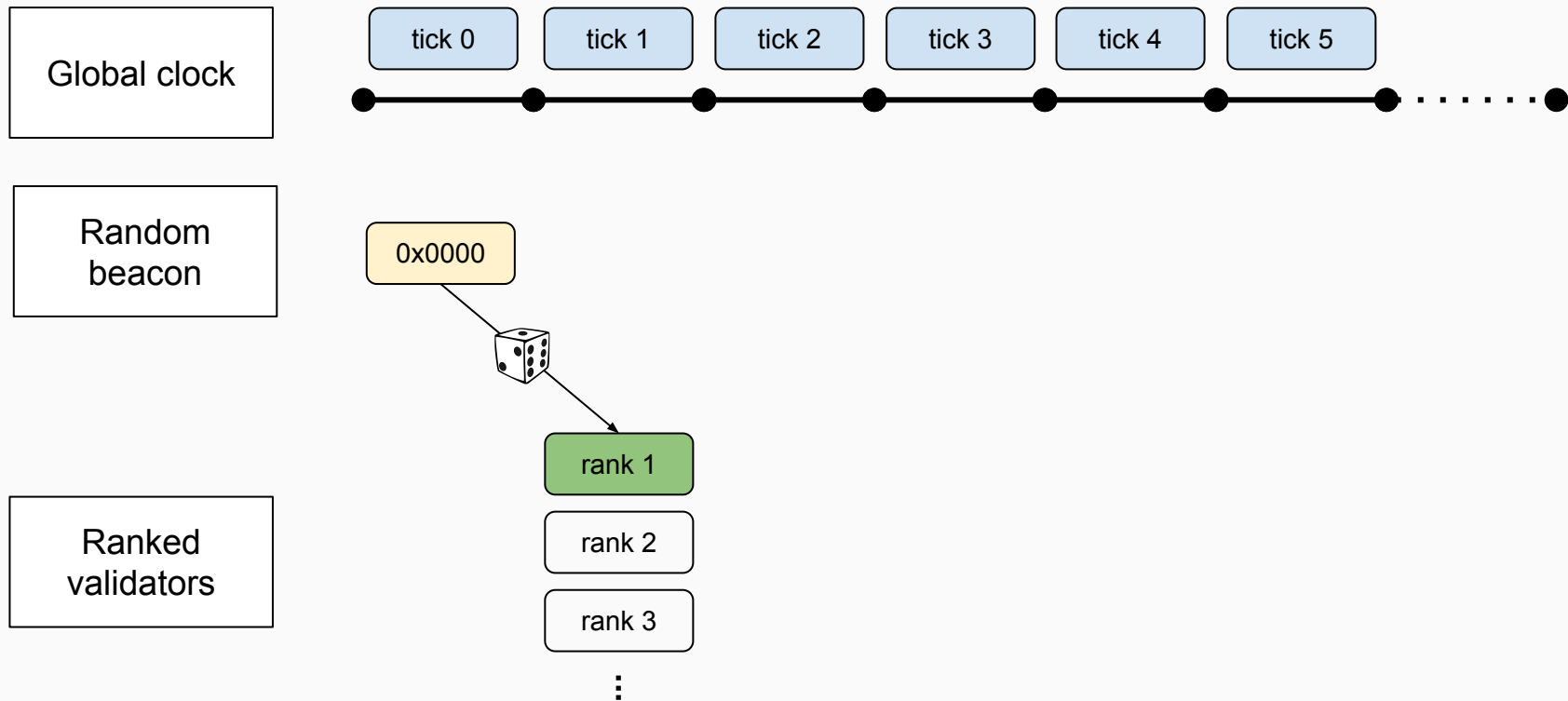
Hash onions



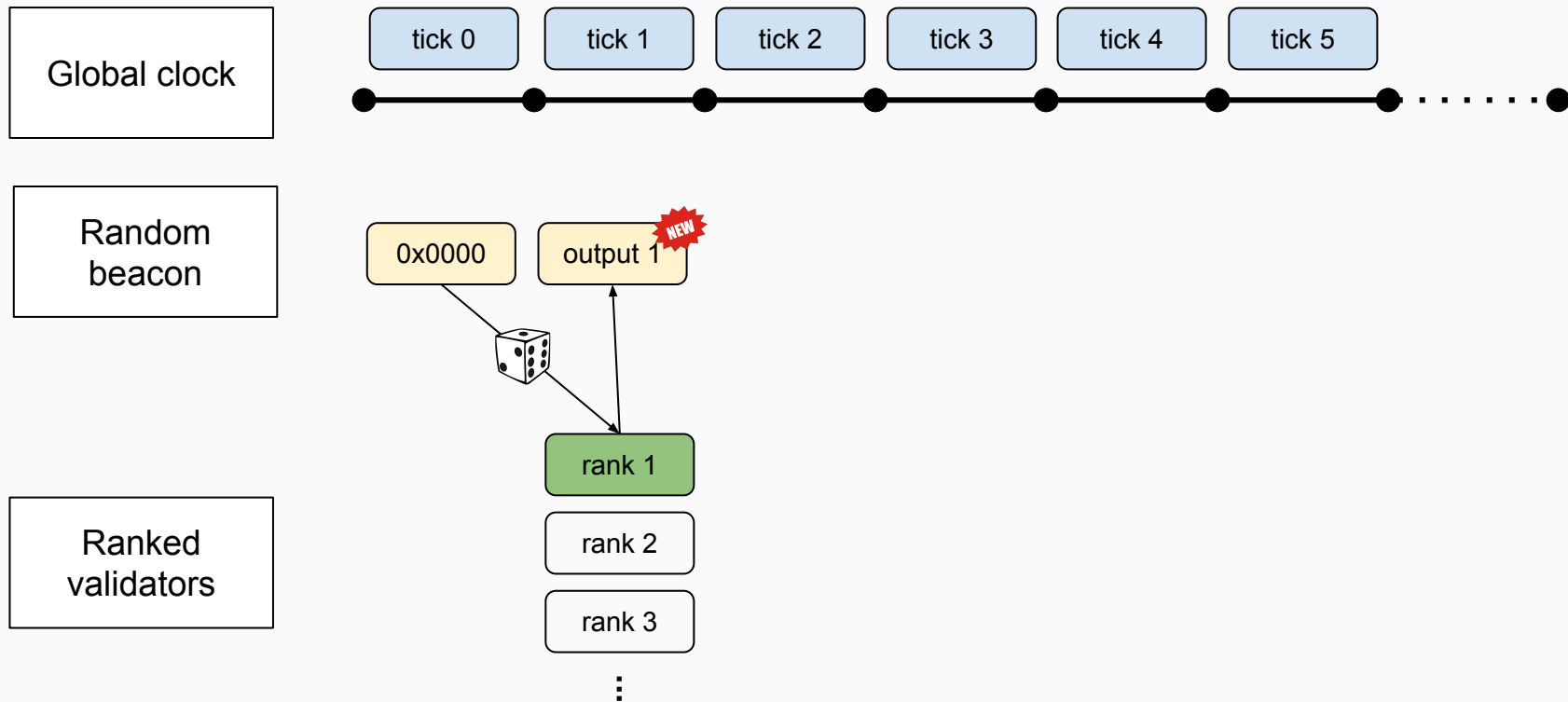
RANDAO



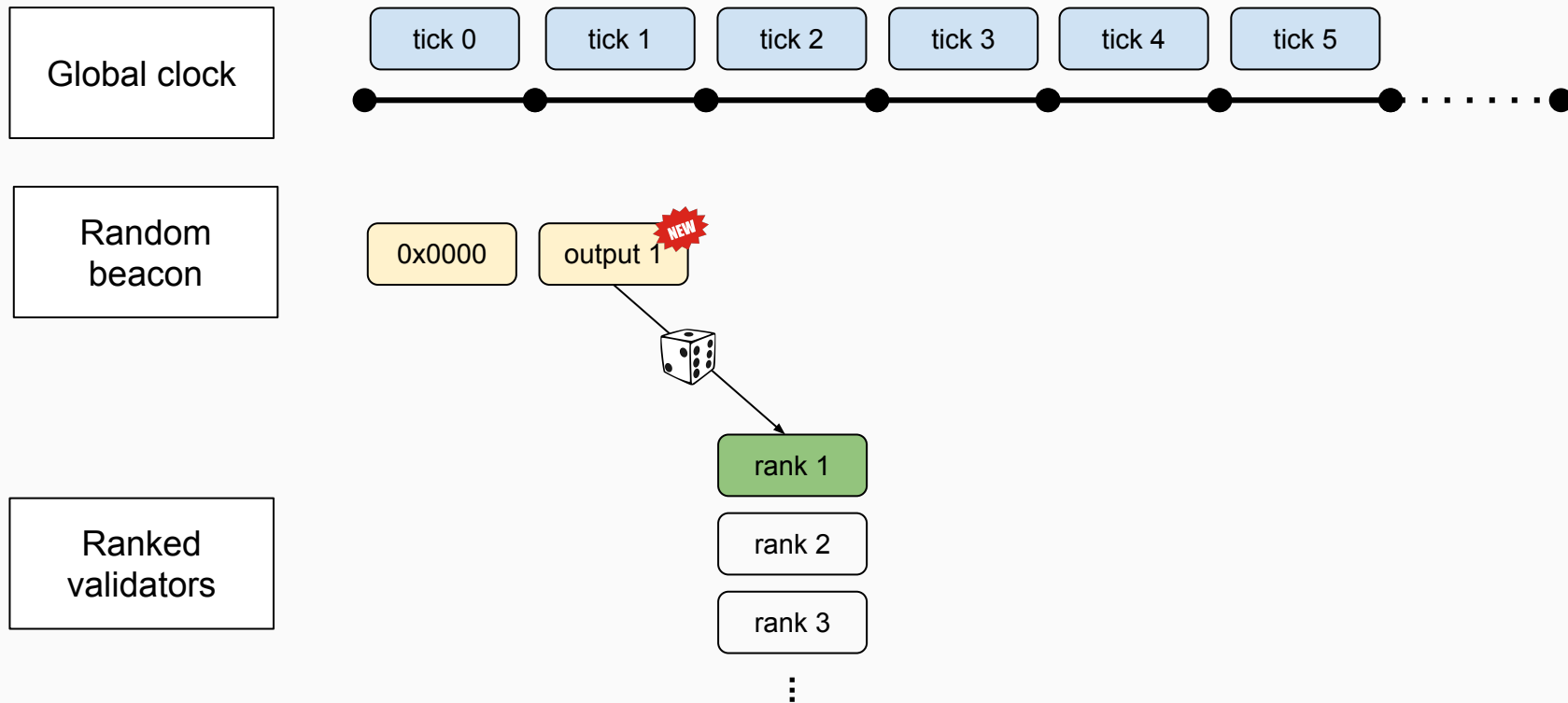
RANDAO



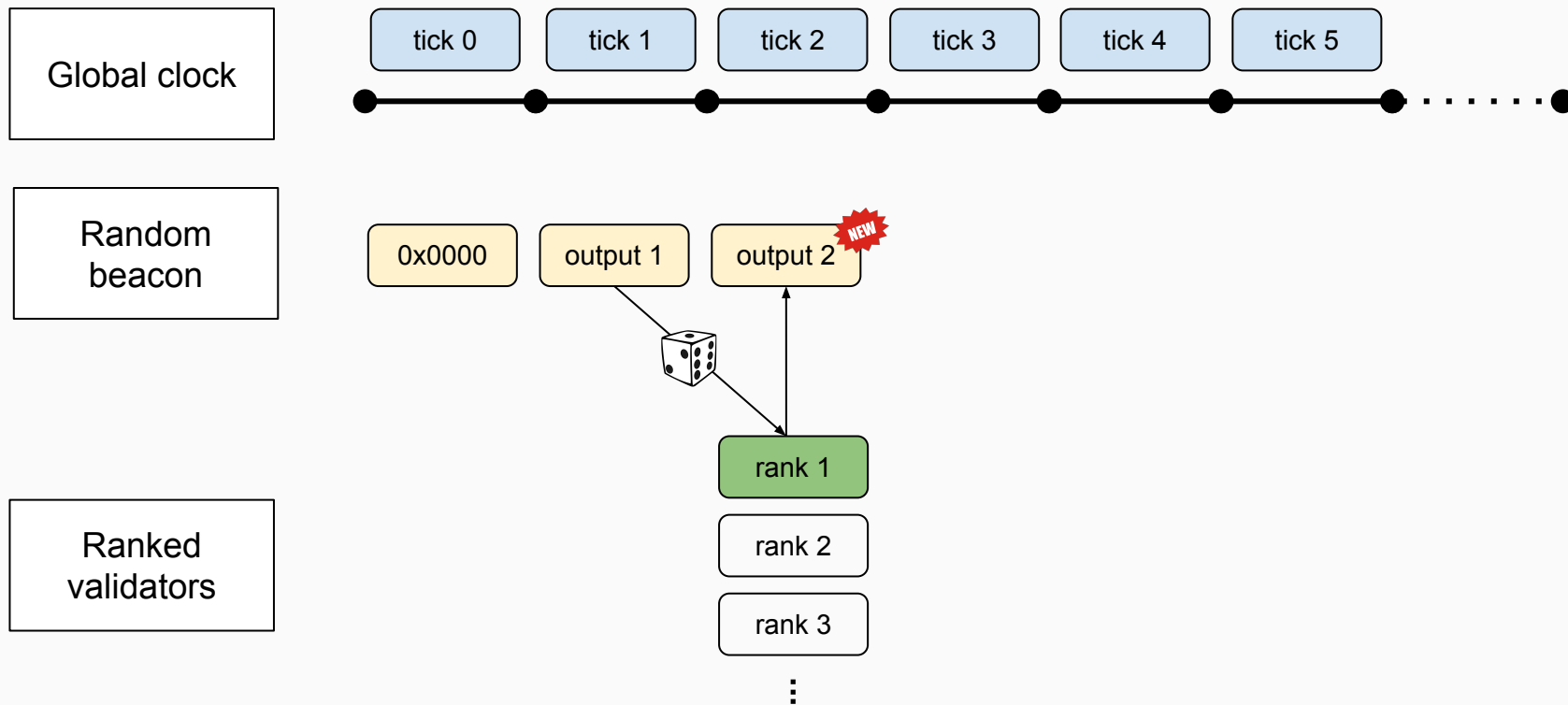
RANDAO



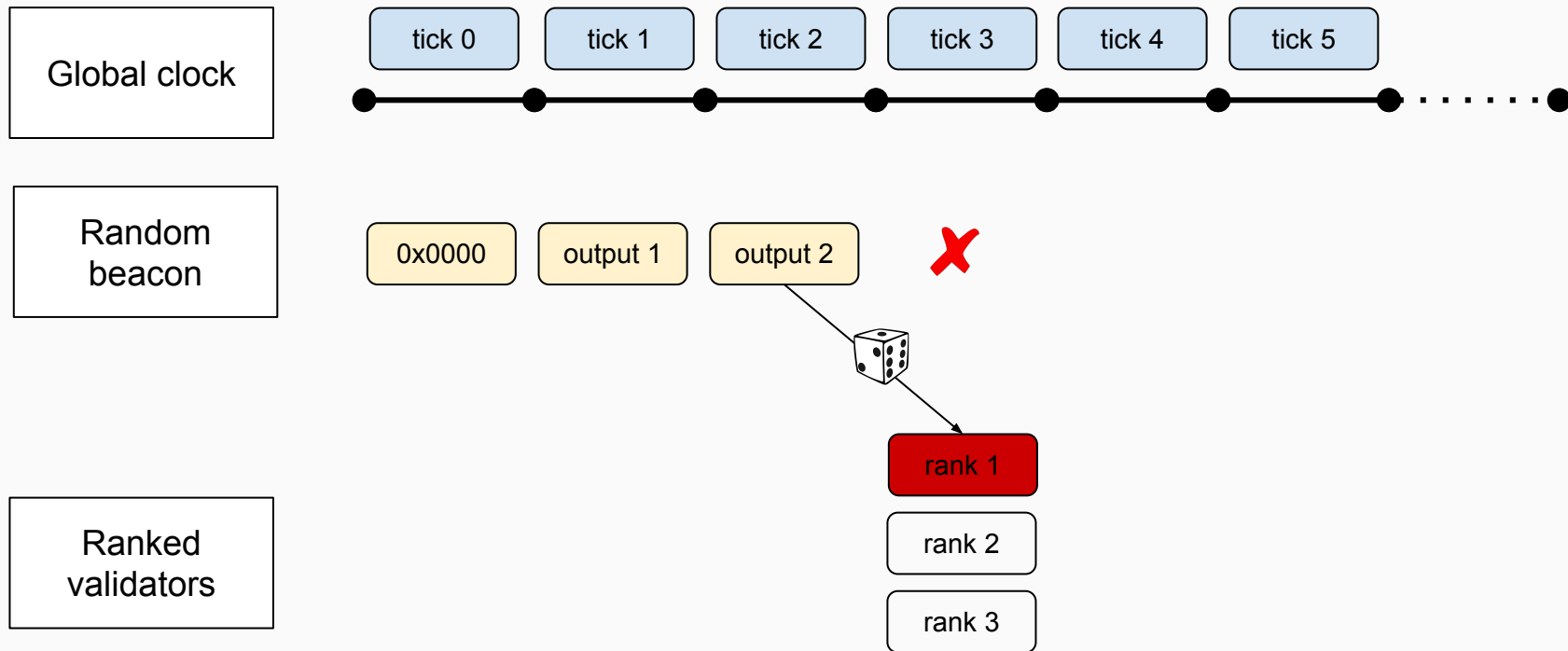
RANDAO



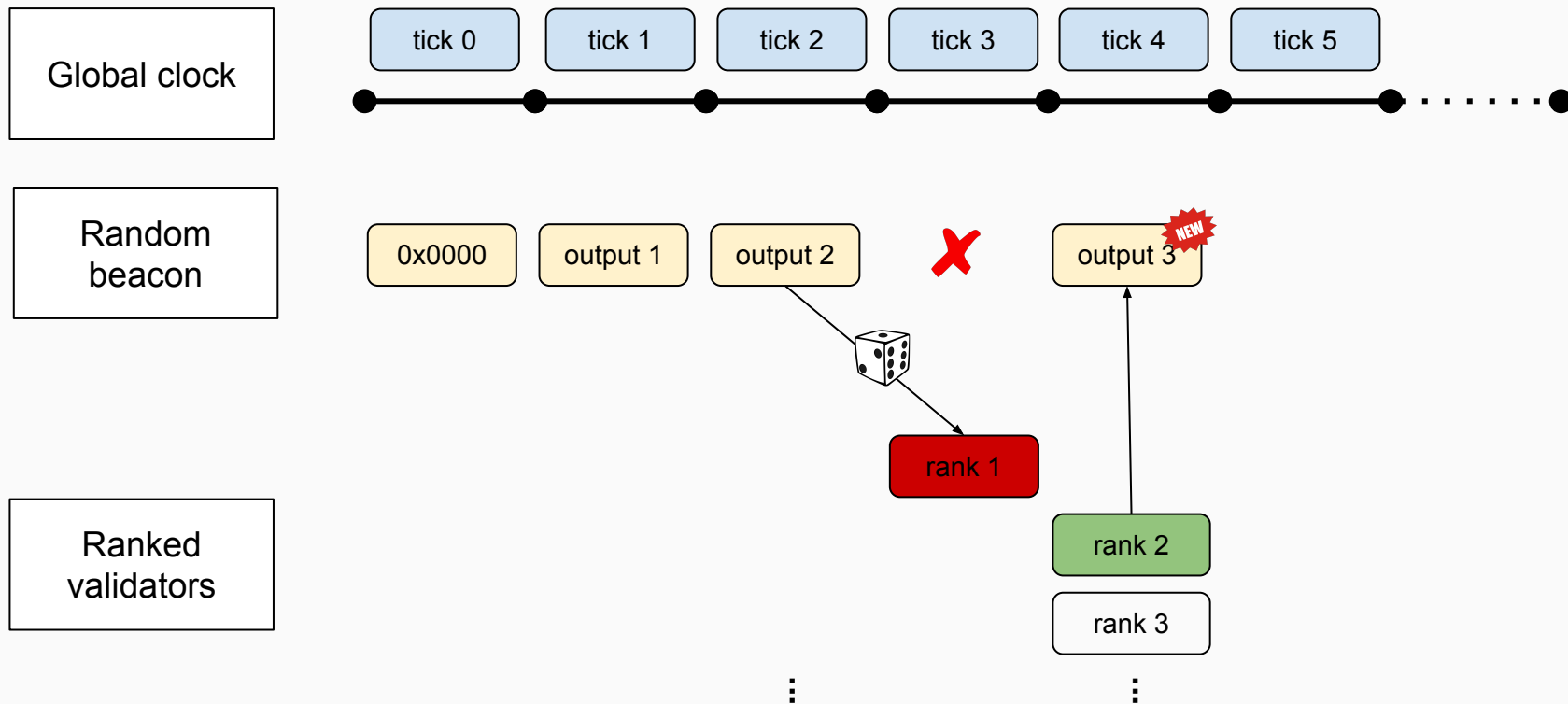
RANDAO



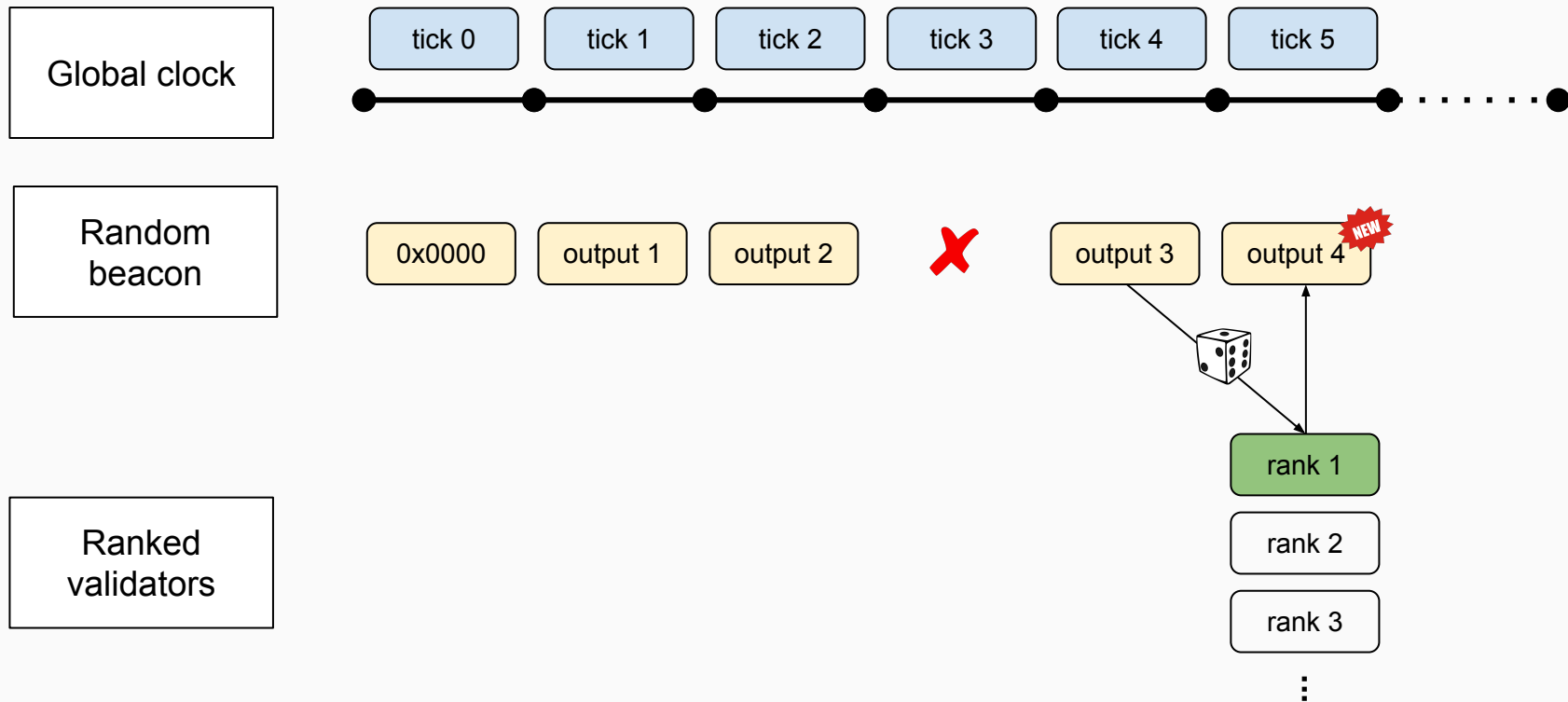
RANDAO



RANDAO

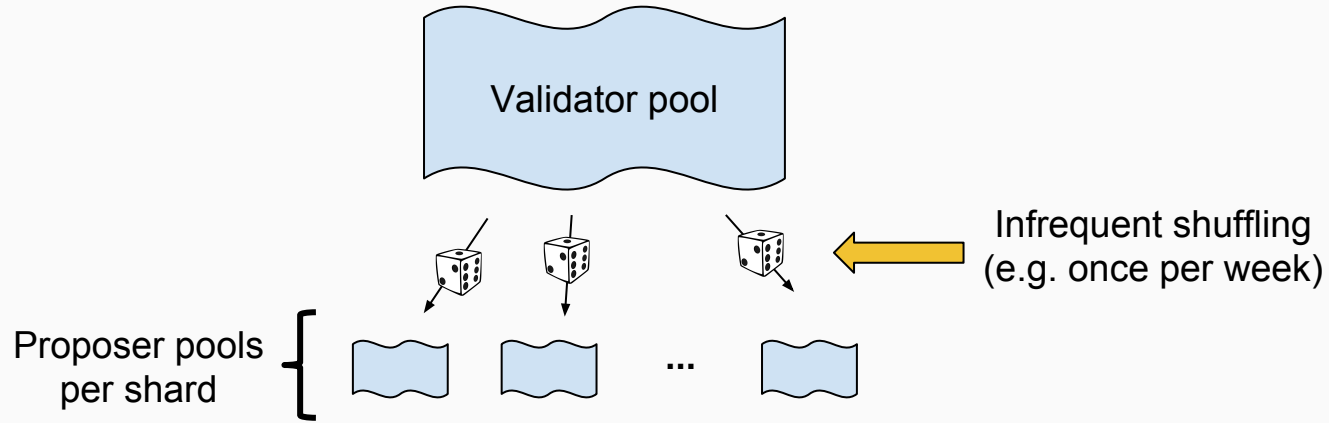


RANDAO

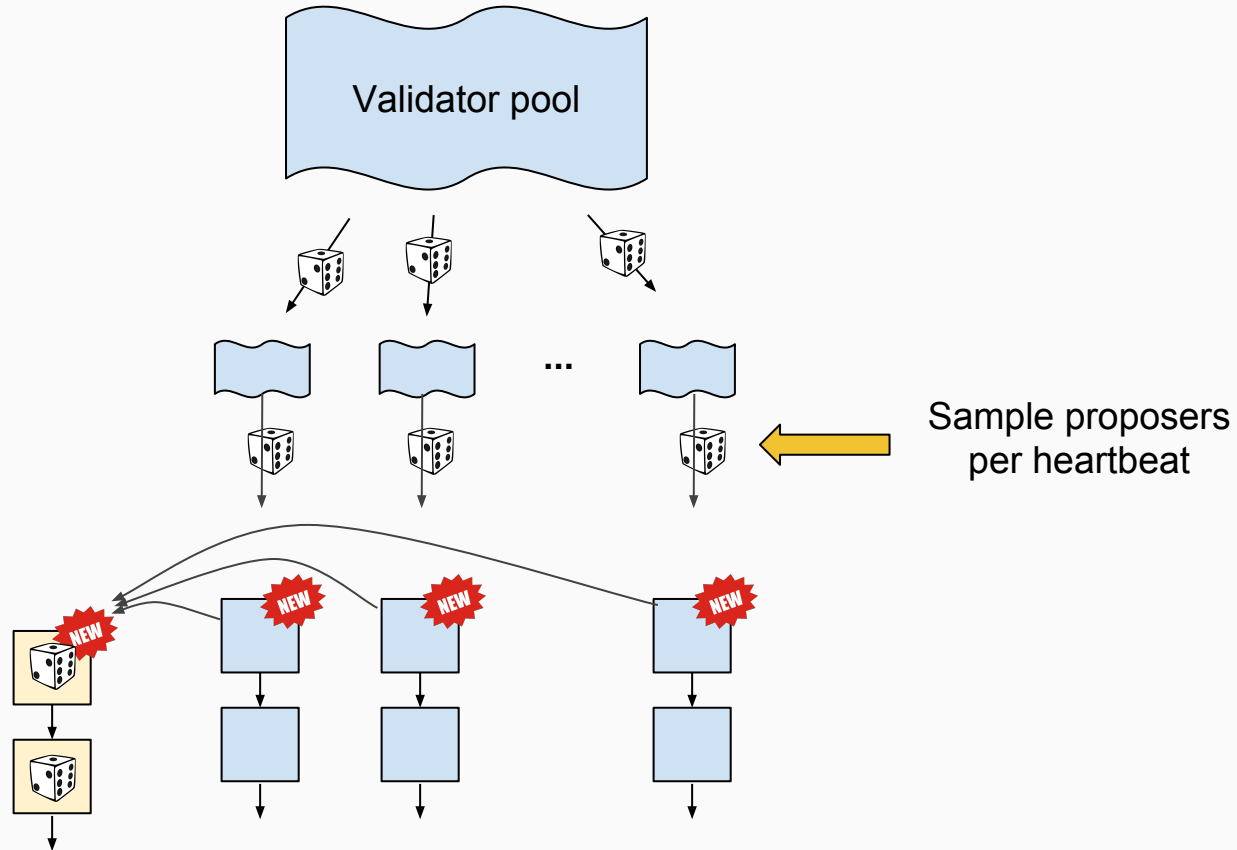


Data layer

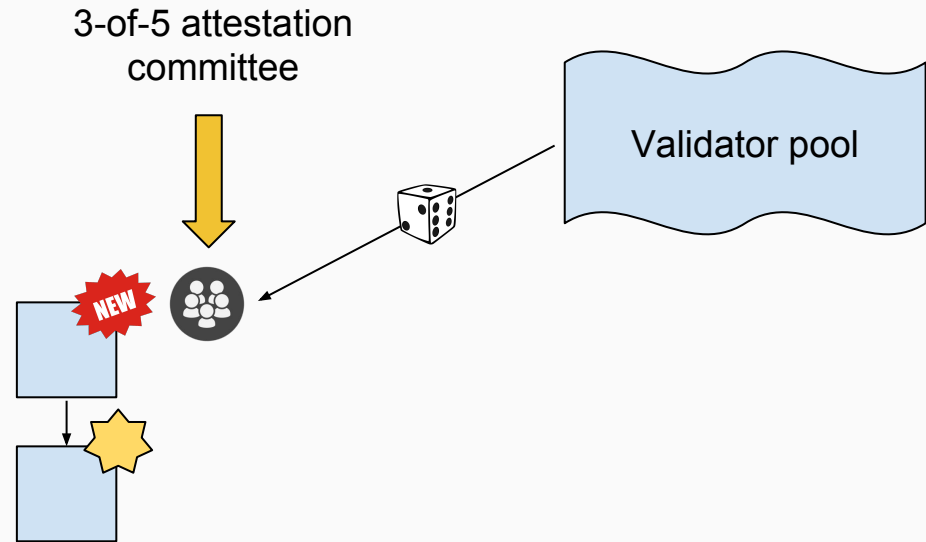
Proposals



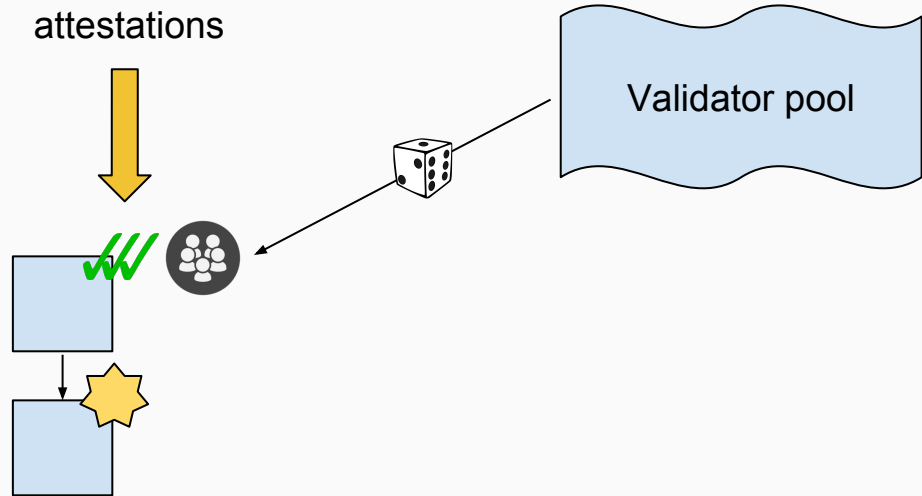
Proposals



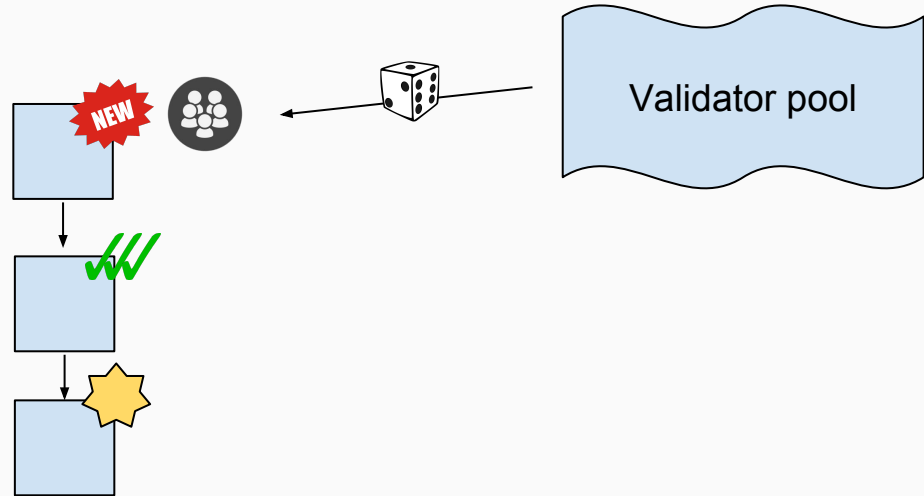
Shard lifecycle—Attestation



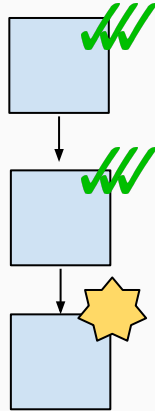
Shard lifecycle—Attestation



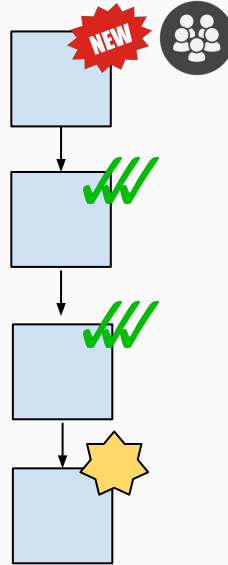
Shard lifecycle—Attestation



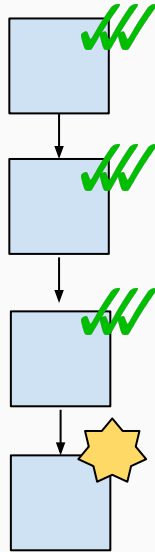
Shard lifecycle—Attestation



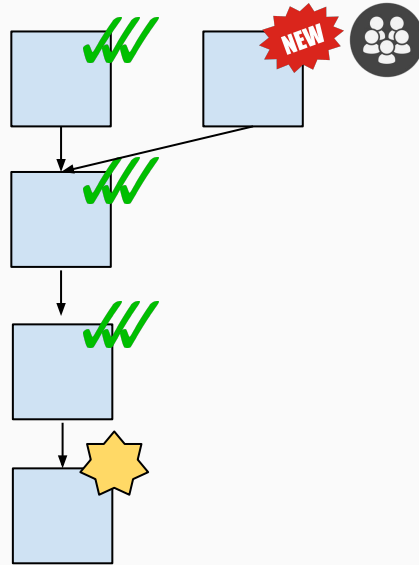
Shard lifecycle—Attestation



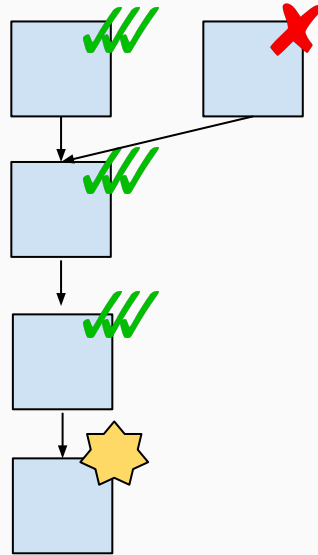
Shard lifecycle—Attestation



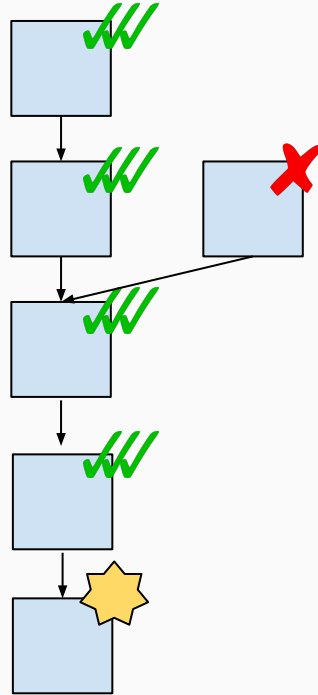
Shard lifecycle—Attestation



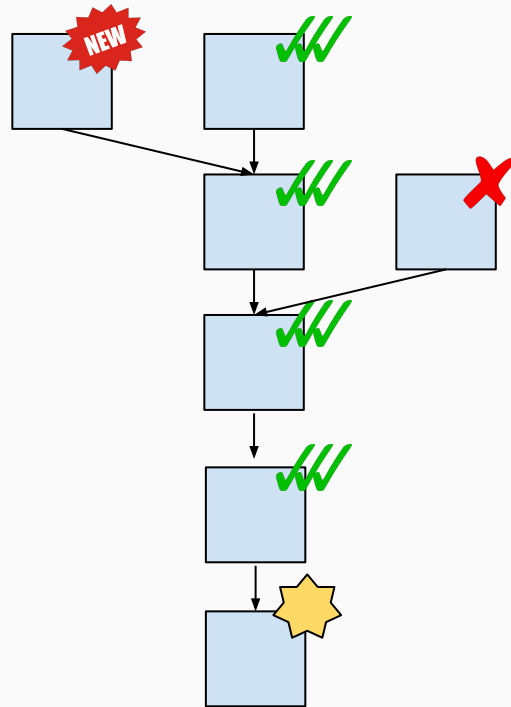
Shard lifecycle—Attestation



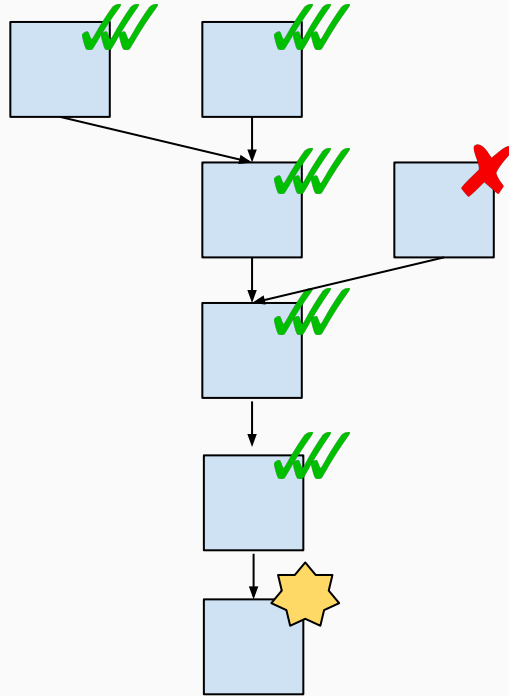
Shard lifecycle—Attestation



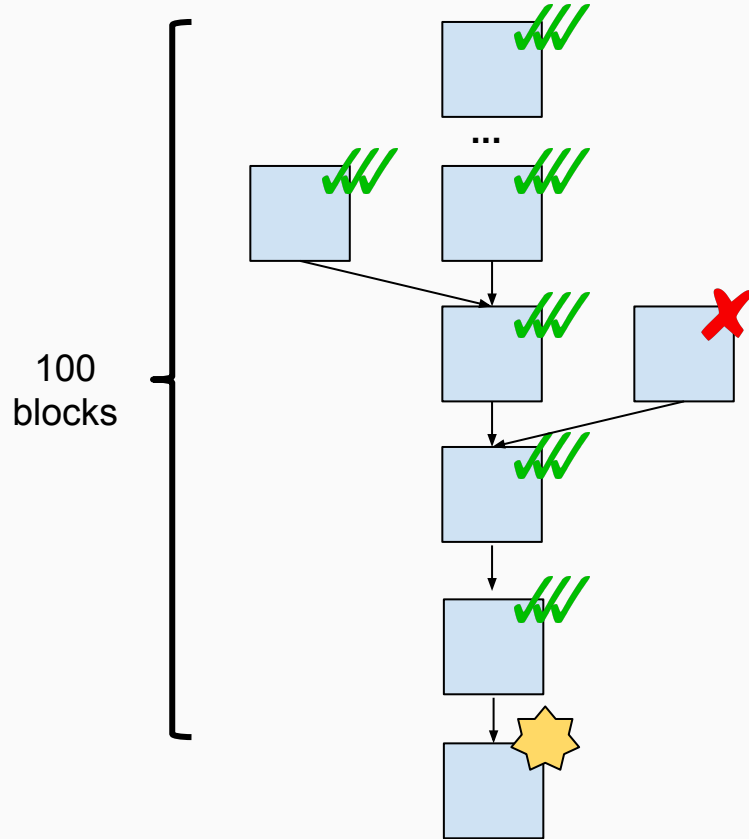
Shard lifecycle—Attestation



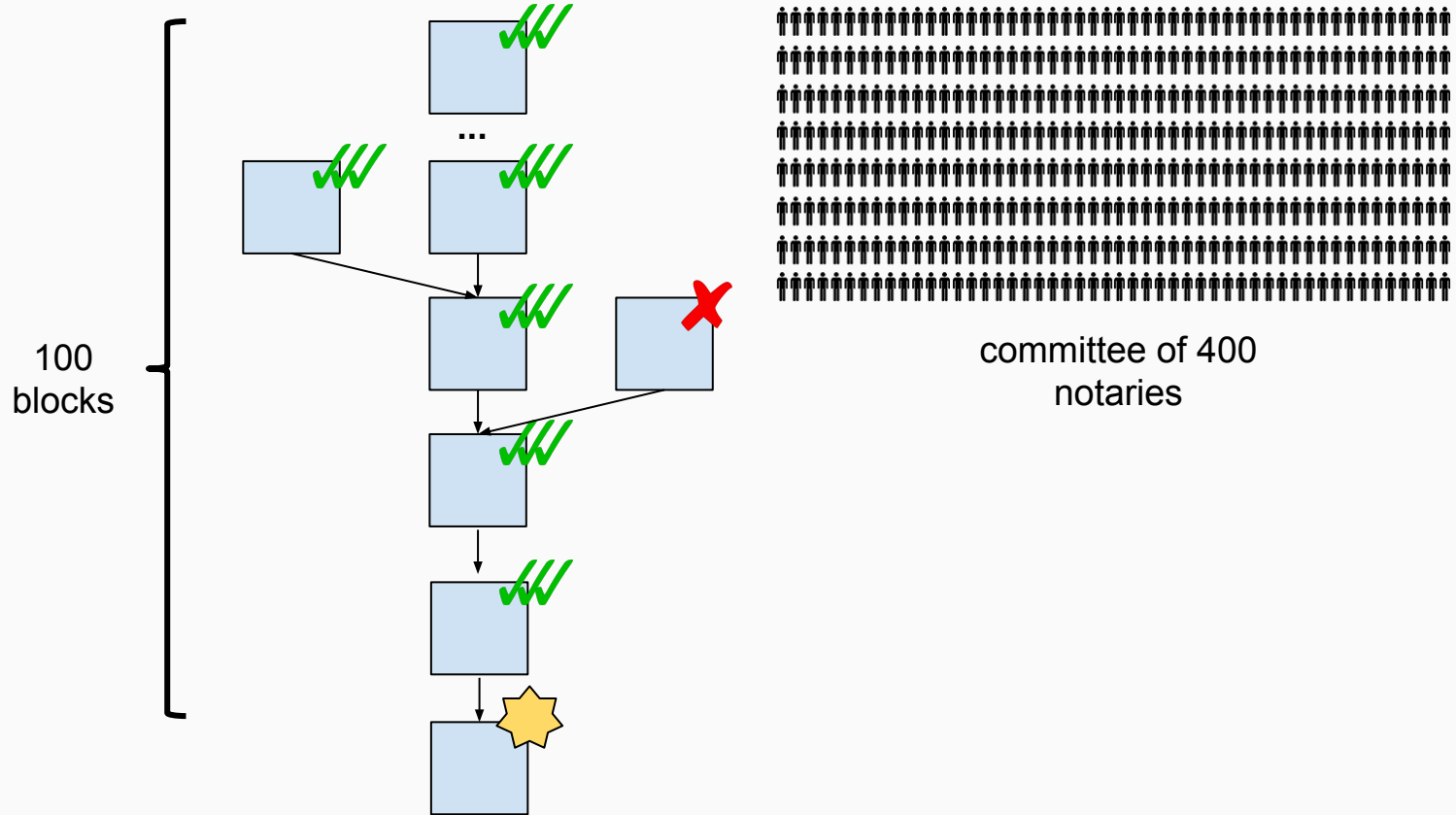
Shard lifecycle—Attestation



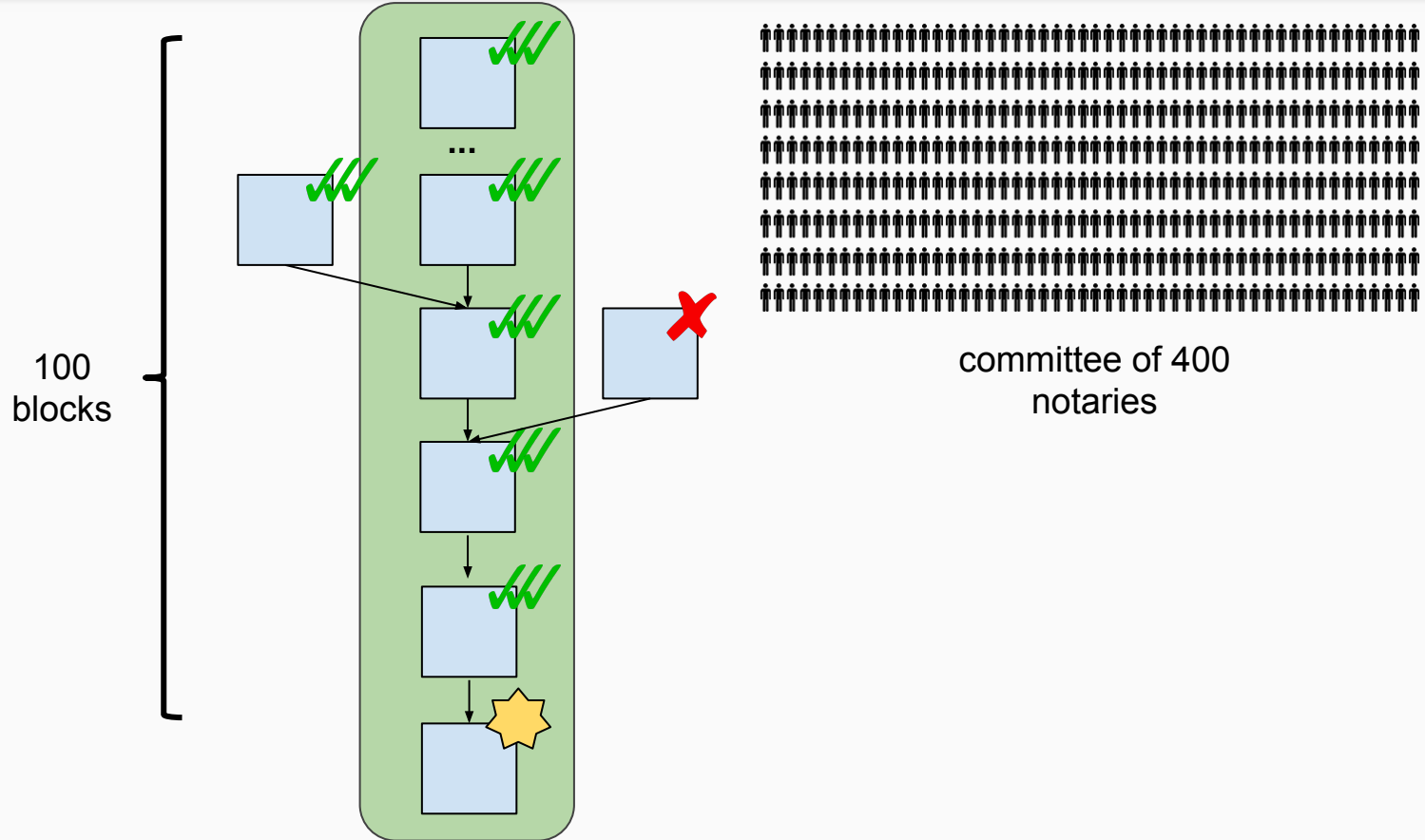
Shard lifecycle—Notarisation



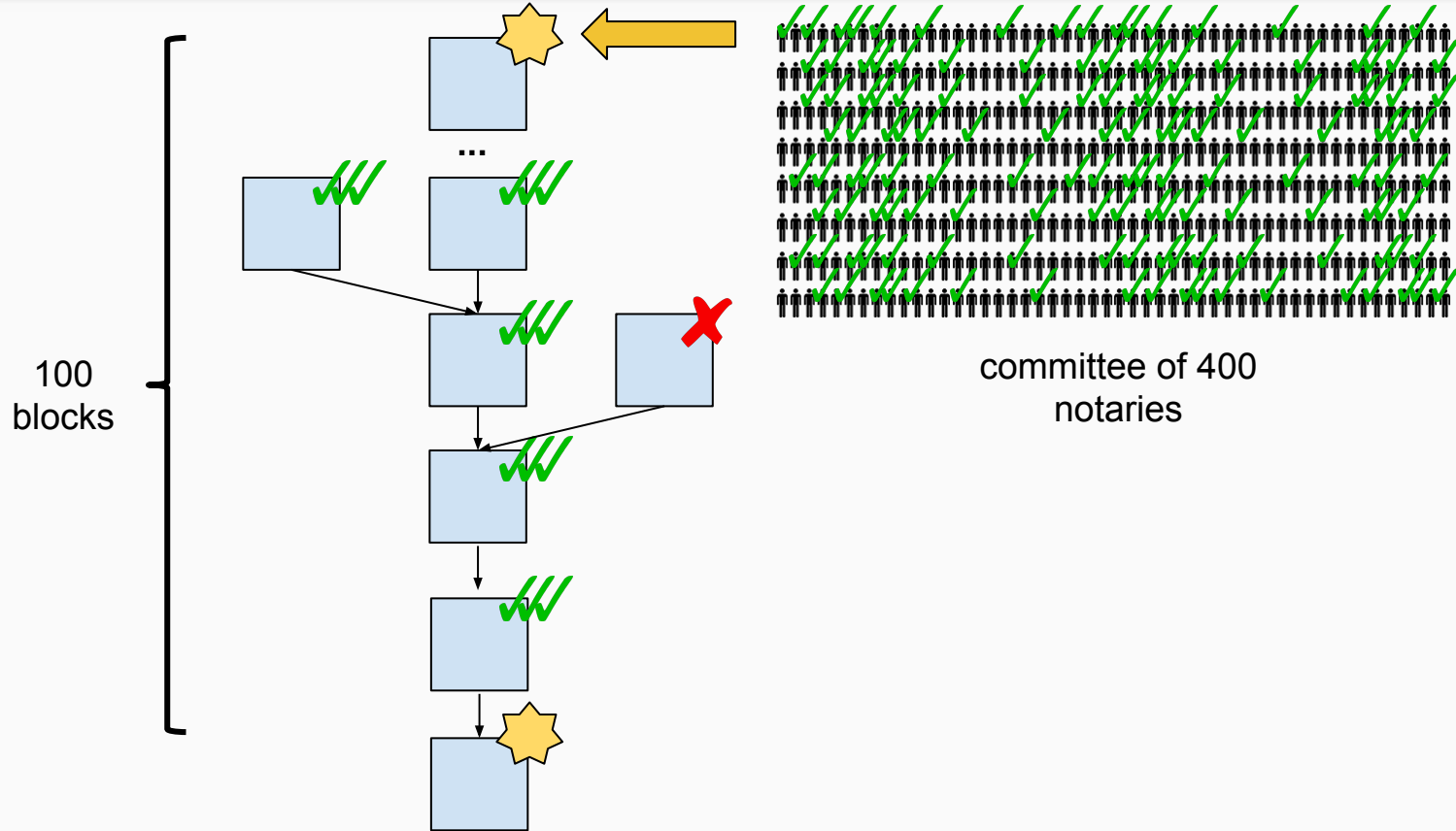
Shard lifecycle—Notarisation



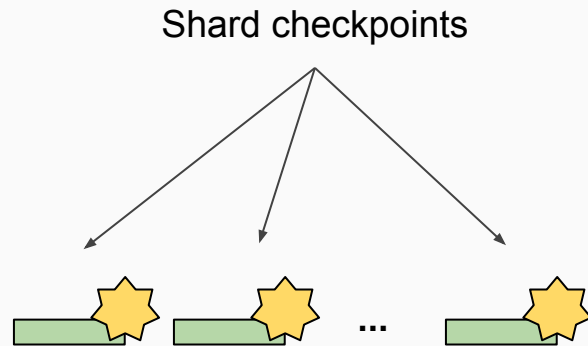
Shard lifecycle—Notarisation



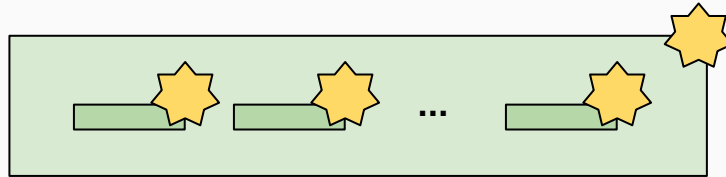
Shard lifecycle—Notarisation



Shard lifecycle—Meta-notarisation



Shard lifecycle—Meta-notarisation



Meta-checkpoint ...put on chain main

Crypto-economic gadgets

Proof of custody

File

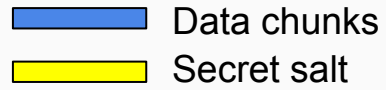


Proof of custody




 Data chunks

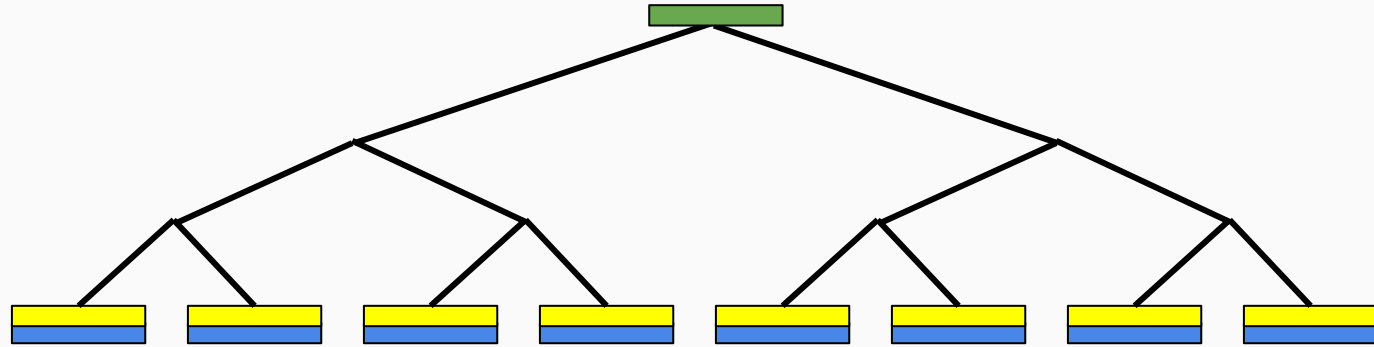


Proof of custody

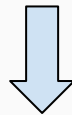


Proof of custody

-  Data chunks
-  Secret salt
-  Proof of custody



Aggregate signature



Signature claims bitfield

```
01001110101010101010111001010101011101010101001011
10101010111001010101011101010101001011010011101010
01000101010101111101010101001011100101010101110101
010111011010101011100101010101001011010011101010
0100111010101010101011100101010101110101011010101
10101010111001010101011101010101001011010011101010
01000101010101111101010101001011100101010101110101
010111011010101011100101010101001011010011101010
```



Bad claim! Challenge!

Thank you :)