Ethereum Sharding

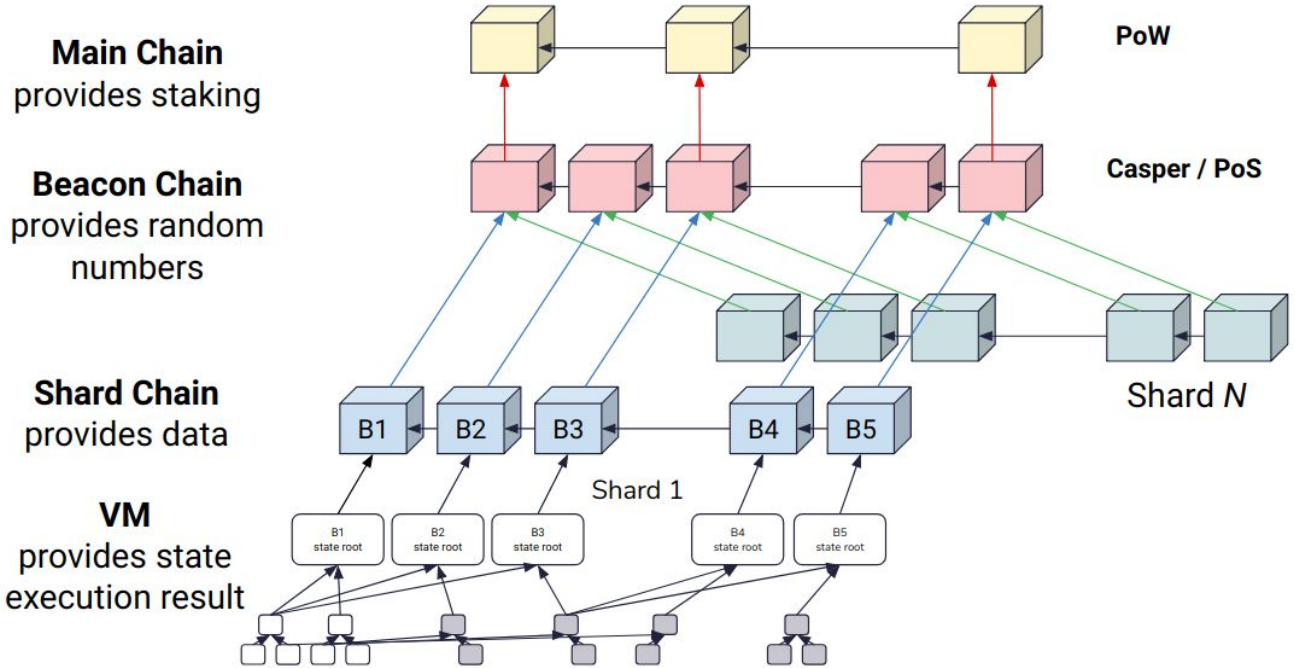
Yijie Hong
09/28/2018

Roadmap[1]

- Phase 0: PoS beacon chain without shards
  - Based on Casper FFG (Casper the Friendly Finality Gadget)
  - Target at 2019[2]
- Phase 1: Basic sharding without EVM
- Phase 2: EVM state transition function
- Phase 3: Light client state protocol
- Phase 4: Cross-shard transactions: see here and more.
- Phase 5: Tight coupling with main chain security: here and more.
- Phase 6: Super-quadratic or exponential sharding

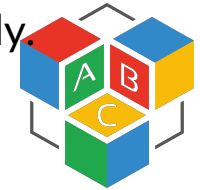
Ethereum Phase 1 architecture

Ethereum sharding research by Prysmatic Labs.[5]



Casper- the friendly consensus mechanism

- Start since 2014
- Two research projects
  - Casper the Friendly Finality Gadget (FFG) led by Vitalik Buterin
  - Casper the Friendly Ghost: Correct-by-Construction (CBC), led by Vlad Zamfir
- Casper FFG[3]
  - A hybrid PoW/PoS consensus mechanism that will assist in the transition to PoS.
  - A checkpoint is added after 50 blocks.
  - Help scaling & Mitigate the “wasted electricity” used in mining.
  - Initially, keep POW and only use PoS to validate "checkpoints" periodically.
  - A Proof of Stake Design Philosophy



Ethereum Phase 1 solution

From Ethereum research team (slides)

- **Client** submits transactions to Tx pool
- **Collation proposers** create collations which pay a fee to validators
- **Validators** download potential collation proposals and validate them
- **Validators** submit collation header to the root chain
- **Committee** votes for collation heads from notaries and generate new block for main chain.
- **Detailed process with animation!!!**[4]

Ethereum Sharding FAQs (my notes)

- Some solutions not work
  - More blockchains & more altcoins => N-factor decrease in security
  - Bigger block => only supercomputers can support => centralization
  - Merge mining => more load to miner => less miners => centralization
- Some solutions might work
  - Classic PoW requires over 95% CPU time for hashing; bitcoin-NG can spent more CPU for block validation.
  - Channel-based solutions scale Tx by constant factor, which however cannot scale storage.
  - PoS (Casper FFG): more scalable and decentralizable.
  - Above-mentioned solutions can be applied with sharding.

Single-shard takeover attacks (51%)

- Random sampling is good enough
  - N: # of nodes in a shard; p: % of bad nodes.
  - size N = 150, 0.000183% if 1/3 of total nodes are bad. (binomial distribution)

	N = 50	N = 100	N = 150	N = 250
p = 0.4	0.0978	0.0271	0.0082	0.0009
p = 0.33	0.0108	0.0004	1.83 * 10-5	3.98 * 10-8
p = 0.25	0.0001	$6.63 * 10^{-8}$	$4.11 * 10^{-11}$	1.81 * 10-17
p = 0.2	$2.09 * 10^{-6}$	$2.14 * 10^{-11}$	$2.50 * 10^{-16}$	$3.96 * 10^{-26}$

- PoS is easy for random sampling
  - Run the random function based on the stake.
- PoW is more difficult
  - Malignant node can keep running random function until it is assigned to a specific shard.
- Reshuffle frequency
  - Downloading the whole Ethereum state snapshot take 2~8 hours ==> reshuffling every few days.

Other topic mentioned

- Cross-shard contract yanking
- Data availability problem
- Congealed gas
- Heterogeneous sharding
- Synchronous and semi-asynchronous cross-shard messages messages
- Guaranteed cross-shard call
- Bitcoin-NG

Reference

1. https://github.com/ethereum/wiki/wiki/Sharding-roadmap
2. https://www.coinstaker.com/ethereum-sharding-casper-release-dates/
3. https://bravenewcoin.com/insights/ethereums-move-to-pos-first-version-of-casper-released
4. https://docs.google.com/presentation/d/1f97Dhm1ZMnZQb2a6LrT53GTwidLk9LL8oCb7F0EmJss/edit#slide=id.g3595449e9e_0_337
5. https://medium.com/prysmatic-labs/ethereum-sharding-biweekly-development-update-9-prysmatic-labs-f2b1ad55e825
6. https://ethfans.org/posts/ethereum-casper-101