Definitions

:

- Eth2.0 Validators

: The block producers (BPs) in Eth2.0 are validators that are randomly selected from a validator pool, and each validator is assigned to one shard. Given the initial number of shards M = 1024

, we may require V > 100

validators in the network to achieve the desired security level (Security Level of Random Sampling With Sharding).

- Super-Full Node

: A super-full node processes the ledgers of all shards, and may be able to produce a block in any shard (as long as the block satisfies the consensus of the shard such as PoW, PoS)

According to the definitions, my first observation is that

Observation

1: The network cost of Eth2.0 (in terms of BP nodes) is O(MV)

.

Meanwhile, for a super-full node, we have

Proposition 1

: A super-full node is equivalent to a cluster of sub-nodes, with

- One-to-one correspondent

: Each sub-node processes one shard data and each shard has one sub-node. Therefore, we could safely assume that the cost of a sub-node has the same order as a validator in Eth2.0.

- Trust Within the Cluster

: Each sub-node trusts

other nodes in the same cluster, and communicate the verified

cross-shard messages within the cluster.

- Untrust Between the Clusters

: Each sub-node does trust any sub-nodes in other clusters, i.e., other super-full nodes.

- Cost

: The cost of a super-full node is O(M)

.

As a result, I have

Corollary 1

: Assuming a sub-node in a super-full node cluster has the same order of the cost of an Eth2.0 validator, the network cost of Eth2.0 has the same order of V

super-full nodes, i.e., O(MV)

.

In fact, from Corollary 1 and Proposition 1, I have

Observation 2

: Eth2.0 with MV

validators equals to V

super-full nodes with all sub-nodes in an untrusted

mode.

Now, I give my another observation.

Observation 3

: Eth2.0 validator model respects equality

, which means

- Each validator is expected to have the same order of cost as other validators (cost of the node and maybe others)
- All validators have the same right to produce a block in a shard (although when and which shard should be unpredictable)

Observation 4

: While in reality, the node operator would be diversified

in terms that

- Different node operators could have different levels of power

to run nodes such as a super-full node, a partial-full node (a cluster with sub-nodes covering a subset of all shards), or a single shard node. E.g., pools, banks, large organzations, or a group of trusted blockchain fans may run a super-full node, while a student working on a blockchain class may run a single shard node for experiment.

- Different node operators may have different interest

on different shards. E.g., a bank may manage the assets in some specific shards.

- Different node operators may require different security levels

. A BP may just mine a specific shard by running a shard node, while a pool may run a full-node to provide pool service to all shards and make sure every block produced is correct.

In all, my major question is that could we optimize the following parameters for a blockchain network

- Trusted or Untrusted

: It is possible to find a middle ground between the trust model of super-full nodes and untrust model of validators in Eth2.0?

- Equality and/or Diversity

: Everybody could free to join the network and produce a block. However, depending on their power, interest, and security levels, different node operator could participate in the network in either super-full node, or partial full-node or a single shard node.

Taking M = 1024

, and V = 100

as an example, a network offering the middle ground may like

- ~30

super-full node clusters

are run by pools, banks, large organizations, groups of trusted blockchain fans, etc, and maintain the full ledgers of all shards.

- ~500

partial-full node clusters

are run by smaller pools, organizations. A partial-full node cluster will process the ledgers of several shards of interest, and run as light clients of other shards (using SPV and/or data fraud and availability detection to process cross-shard message and increase security)

- ~10000

single-shard node

in the network for solo miners or a developer that is interested in dapp in a shard). The cost of such node is expected to be 1.2x-1.5x cost as current Ethereum (with 0.2x~0.5x for processing cross-shard messages)

Note that the network is completely permissionless, and a node operator is free to run in any type of nodes/clusters.