Member: Samiya Kazi

Week 5

Future Trend for Reducing the Overhead

Three common pitfalls in existing sharding mechanisms prevent the system from being horizontally scaled to the theoretical upper bound due to the communication and storage overhead.

1. An existing global chain that is needed to be stored by all participating miners/validators. Such a global chain tends to be responsible for all global operations, such as generating randomness, cross-validating transactions in different shards, reshufﬂing operation. However, this simply poses the bottleneck threat back to a single global chain, which is the root issue sharding technologies would have tried to solve.  
   Trend 1: Restricting the use of a global chain in any operations, and the bottleneck requiring to be solved if used.
2. Requiring miners/validators to store ledgers from other shards. This is necessary in some of the existing sharding mechanisms in order to cross-validating transactions and reshufﬂing operation. However, it leads to miners/validators incurring high communication and storage overhead in O(n)(n is the number of shards).  
   Trend 2: Balancing the storage and communication overhead for miners/validators in sending cross-shard transactions and reshufﬂing, so that the order can be lower than O(n). One of the potential solutions might be the fraud proof that enables light nodes to be as secure as full nodes without needing to store the whole ledger, yet it has not been mature at the time of writing.
3. Allocating participating nodes to shards based on their business requirements in order to bypass the overhead of using the sharding technology. Business-driven members allocation for shards has been proposed and discussed in some designs, e.g., Ethereum 2.0 [100]14 in order to reduce, 1) the frequency that a participating node gets swapped out; and 2) the ratio of non-cross-shard transactions, for the ease of management and lower overhead. However, this results in a very long epoch reconﬁguration for participating nodes and unevenly shard size, which ultimately poses a risk of crowed transactions to a single shard as time passes and the size and throughput increases, thus hitting the bottleneck of intra-consensus.  
   Trend 3: Avoiding simple business-driven members allocation that risks shards suffering from crowed transactions.

Future Trend for Strengthening the Security and Atomicity

This trend corresponds to the intra-consensus and atomicity of cross-shard transactions, respectively. We point out the potential direction on more secure intra-consensus and more

efﬁcient cross-shard transactions, as shown in the following.

Intra-consensus:

* Trend 4: Scaling the unbiased and unpredictable randomness generator in large-scale networks with as few third-party hardcoded settings as possible. The unbiased and unpredictable randomness plays an important role in BFT-based intra-consensus design. Improving this kind of algorithms can signiﬁcantly prevent the validators from being under DDoS attacks.
* Trend 5: Improving the PoW-based intra consensus, and generalizing it into other types of Nakamoto-based consensus algorithms. Chu-ko-nu mining of Monoxide takes advantage of PoW to bypass the vortex of randomness, nevertheless, the security of which is dependent on the storage. As such, the future direction can be potentially decoupling the security and storage, and generalize the concept to other Nakamoto-based consensus algorithms, e.g., Proof-of-Stake.

Source: <https://www.researchgate.net/publication/338492335_Survey_Sharding_in_Blockchains>