Leviatom: Bringing Trust to Block Chain Network of Million Nodes

***Abstract*—To achieve high throughtput in the POW based blockchain systems, a series of methods has been proposed, and DAG is one of the most active and promising field. We designed and implemented the StreamNet aiming to engineer a scalable and endurable DAG system. When attaching a new block in the DAG, only two tips are selected. One is the 'parent' tip whose definition is the same as in Conflux [3], another is using Markov Chain Monte Carlo (MCMC) technique by which the definition is the same as IOTA [5]. We infer a pivotal chain along the path of each epoch in the graph, and a total order of the graph could be calculated without a centralized authority. To scale up, we leveraged the graph streaming property, high transaction validation speed will be achieved even if the DAG is growing. To scale out, we designed the 'direct signal' gossip protocol to help diseminate block updates in the network, such that message can be passed in the network in a more efficient way. We implemented our system based on IOTA's reference code (IRI), and ran comprehensive experiments over different size of clusters of multiple network topologies.**

***Keywords*-Block chain, Trusted Computing, Graph Theory**

I. Applications

A. Using StreamNet to cache TRIAS requests

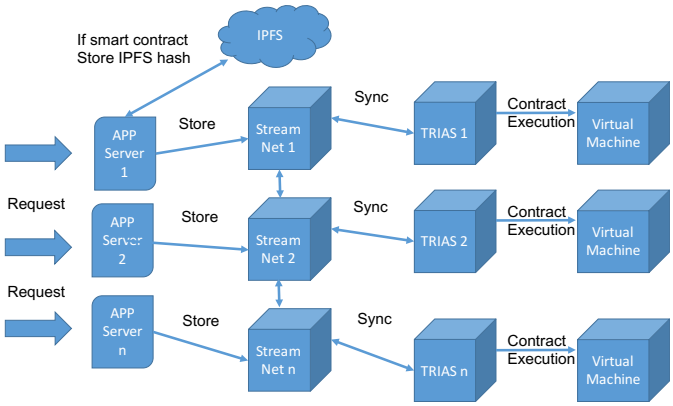

Figure 1. StreamNet used for caching the TRIAS requests

To avoid the selfish mining problem [1], [9], there must be a way to let everyone in the network to know the request from the client side. StreamNet can be used to cache and pre-confirm the information (including transactions and smart contracts) of other blockchain systems because of its high throughput. $TRIAS$ [6] as a cross-blockchain system can take advantage of this feature to achieve elasticity. The structure is shown in Figure 1. There is a distributed APP server and each StreamNet deployment can have one APP server. APP server accept the TRIAS requests including the transaction and smart contract requests. If the requests are transaction requests, APP server will send them directly to StreamNet in a batching mode (for instance, every 100 transactions is a batch) or a single mode. If the requests are smart contract requests, APP server will send the info to IPFS to get a hash, then send this hash to StreamNet. When the traffic is small, StreamNet can directly pass throught the content to $TRIAS$ after confirming it, When the traffic is large, StreamNet will continue to cache and pre-confirm the new blocks, as $TRIAS$ is idle, it will pull the confirmed information from StreamNet and process it.

B. Using StreamNet to rank TRIAS nodes in TEE environment

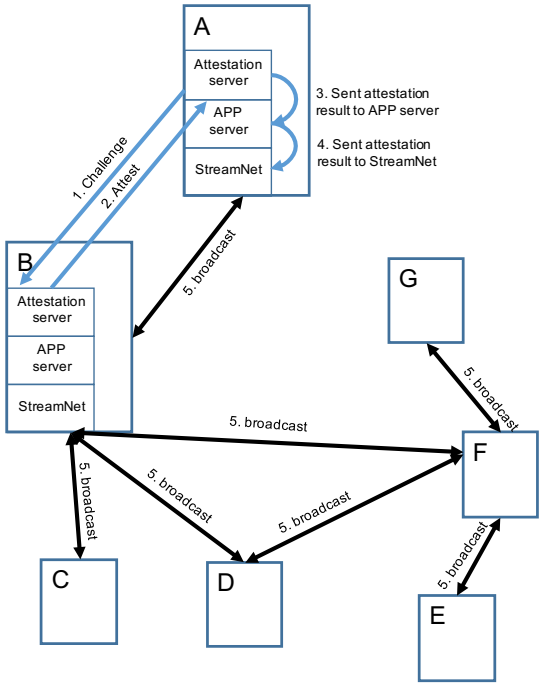

Figure 2. StreamNet involved in attestation.

1) Attestation and synchronization of results: Hybrid chain based systems usually use POW or POS to elect super nodes. Another thread of method utilized the trusted computing method [8], [7] to help elect super nodes. The general idea is, the blockchain system should run on the trusted computing environment (TEE), and those who elected as the super node should prove that they are the most trustable nodes. To achive this, there are attestation

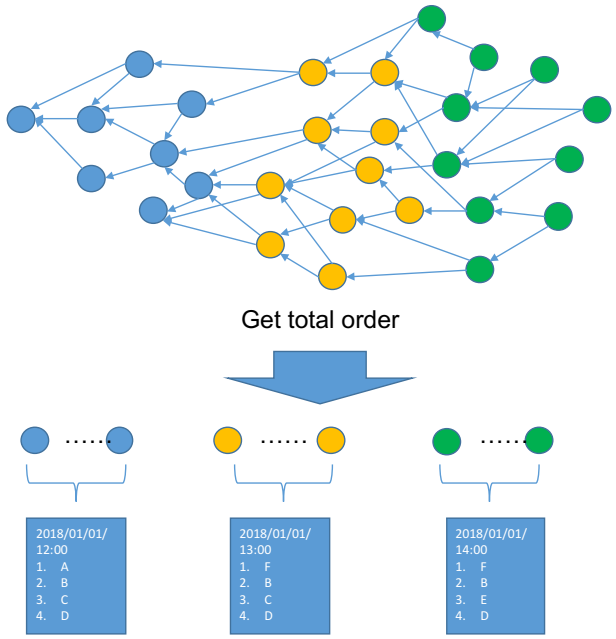

Figure 3. TRIAS ranking calculation based on the attestation information stored in StreamNet. Different color of blocks represent different periods.

service periodically check the trusted status by attesting their neighbors. After the attestation result is collected, the attestation server will send this information to APP server, and it will be further directed to StreamNet. By leveraging the gossip system of the StreamNet itself, these attestation information will be synchronized all through the network. The 5-step process is as Figure 2 shows.

2) Global Tik Tok period: One of the important issues in the attestation based reputation system in the open p2p network is that there is no common agreement of time. In the private network, the typical solutions could be achived by using time oracle [4] or TrueTime [2]. Since StreamNet can provide with a total order, there is no need for TRIAS nodes to maintain a timer service. StreamNet itself can provide with the concept of time (for instance the tik tok period of 1 hour). The algorithm to determine current period and the blocks contained in current period is as Algorithm 1 shows. By using this algorithm, the attestation server will determin the current TikTok time $T_{current}$ and the last TikTok time T_{last}, and get all blocks between the time period. Once this step is done, the attestation server will send a TikTok time stamp to StreamNet for the next polling. The $getTikTok()$ function in StreamNet tries to get the common consensus of the start point of a specific period.

Algorithm 1: TIKTOK ALGORITHM.

Input: StreamNet SN, TikTok period P, last time T
Output: All attestation blocks in last TikTok period

do
  $T_{current} = SN.getTikTok()$;
  $T_{last} = SN.getTikTok(T_{current})$;
  $B_{period} = SN.getBlocks(T_{current}, T_{last})$;
  $SN.sendTikTok(System.currentTime())$;
  $T = T_{current}$;
  return B_{period} ;
while *System.currentTime()* - $P < T$;

3) Super node election based on HCGraph polling results: This process is shown in Figure 3. The calculation of rank is achived in attestation server. For each period, TRIAS will update its super node rankings, and the ranking is calculated by infering the attestation information in the StreamNet which is dicussed in the last section. Suppose we use v to represent a node in network, and use $s_{v,u}$ to represent the attestation score between v and u, which is actually an weighted edge. These vertices and weighted edges consititute a heterougenerous graph (HCGraph). By computing the KATZ centrality of this graph, the vetex with the highest scores will represent the super nodes.

REFERENCES

[1] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar, "On bitcoin and red balloons," in *Proceedings of the 13th ACM conference on electronic commerce*. ACM, 2012, pp. 56–73.

[2] J. C. Corbett, J. Dean, M. Epstein, A. Fikes, C. Frost, J. J. Furman, S. Ghemawat, A. Gubarev, C. Heiser, P. Hochschild *et al.*, "Spanner: Googles globally distributed database," *ACM Transactions on Computer Systems (TOCS)*, vol. 31, no. 3, p. 8, 2013.

[3] C. Li, P. Li, W. Xu, F. Long, and A. C.-c. Yao, "Scaling nakamoto consensus to thousands of transactions per second," *arXiv preprint arXiv:1805.03870*, 2018.

[4] D. Peng and F. Dabek, "Large-scale incremental processing using distributed transactions and notifications." in *OSDI*, vol. 10, 2010, pp. 1–15.

[5] S. Popov, "The tangle," *cit. on*, p. 131, 2016.

[6] A. Ruan, "Trustworthy and reliable intelligent autonomous systems," 2018.

[7] A. Ruan and A. Martin, "Neuronvisor: Defining a fine-grained cloud root-of-trust," in *International Conference on Trusted Systems*. Springer, 2014, pp. 184–200.

[8] ——, "Repcloud: Attesting to cloud service dependency," *IEEE Transactions on Services Computing*, no. 5, pp. 675–688, 2017.

[9] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *International Conference on Financial Cryptography and Data Security*. Springer, 2016, pp. 515–532.