TIM

TIM: High Bandwidth Peer to Peer Digital Money

Prabhat Kumar Singh
prabhat@talking.im
www.talking.im (TIM)

A high bandwidth peer to peer money would allow commoditization of various types of societal values to be transacted on a single system increasing the cross-industry commerce, security, decentralism as well as reliability. Geolocation-based node identity provide part of the solution to create uniform load distribution aided by statistical block storage and quantum proof keys to achieve true decentralization along with performance.

The P2P network is a two-layer combination of multiple graphs in the lower layer and a global blockchain which stores a fingerprint representation of each of the graphs by time stamping the hash. The longest chain proves the validity of transactions and also the proof of participation by the majority of the graphs to generate maximum consensus (or supersingular isogenic encryption for 400+ graphs).

The structure of generated multigraph in the lower layer of the graphs of the network has other interesting properties like equivalence to Ramanujan graph (for n ~> 400) which would provide switchover to quantum safe encryption when the graph network grows above the threshold.

Introduction

The possibility of replacing intermediary-based financial or commercial systems is becoming a reality with the mass adoption of decentralized ledger technology (DLT). There are various types of utilities being tested on a DLT-based architecture, and while its earlier successes have fueled the digitization of various types of commerce, the bandwidth of blockchains have considerably limited its applicability.

The limited bandwidth is a challenge to onboard various new business models. Moreover, the bandwidth issue has increased the cost of transactions on popular blockchains.

The solution propagated so far have led to the centralization of the network or bottlenecks in the ease-of-usage in some two-layer approach; due to wallet warmup or similar restrictions. The current state of blockchains does not allow easy participation in mining. The cost related to mining fee or capex of becoming a miner inhibits the micropayments, which actually was a cornerstone of peer to peer money.

Another issue in the development of a healthy blockchain platform is the fragmentation of community. On one hand, this fragmentation has led to multiple innovations but has also created a loss of developmental focus on a stronger and useful platform in alignment with the father of current generations of blockchains, Satoshi Nakamoto. One probable reason could be the conventional software development approach which starts with small test cases and scales up gradually. But one cannot change the blockchain everyday like small patchwork in any enterprise system.

The patchwork and piecemeal approach have led to fragmentation. The support of the community and the fork proofing of the network by means of para-legal barriers as well as technological measures is going to guarantee a stable and sustainable blockchain. What is needed is a high-performance system which is future ready.

Everything from the bandwidth up to the cryptographic nature of the blockchain has to be future proof from the current edges of science. This is also to ensure that the irreversibility of transactions, double spending protection, and ensuring that honest nodes make up the majority of the network's strength. These are the key considerations while making this blockchain architecture.

For various types of security mechanism in this architecture implementation, loss of stake is one primary way of censuring the offenders. The network is built for high bandwidth, so flood attacks are most prominent. Apart from various verification mechanisms, the network penalizes attackers to have an economic toll of attacks.

Transactions

The electronic cryptocurrency is a chain of digital signatures created by a transfer of ownership. The owner signs a hash of previous transaction and the public key of next owner. The network and payee can verify the chain of ownership. The challenge of double spending is magnified in a two-layer architecture where both layers need to mitigate the double spending risk. An attacker can double spend in one partition (graph) or also in multiple partitions in the same epoch. We have solved this problem to control and check the multitude of double spending issues.

The first layer is a graph where the graph miners are collecting the transactions from the waiting pool of the same graph and verify that the previous owner did not sign any earlier transaction with the same nonce. The graph miners maintain the UTXO records of 3 graphs, one of a local graph, one of a randomly chosen neighbor graph having a common edge and one distant graph (if available when partition size is more than 3). The choice of neighbor and a distant graph are random for each graph miner. For the block size of UTXO from three graphs is less than 3 MB (88*10000*3 Bytes for a full load of graphs with 10K TPS).

From the collected transactions, only a certain percentage (< 1/3rd) of the least popular transactions are checked by a graph miner who signs the checked transactions. After which the graph miner again pools fresh information from local peer miners in the same graph. And the process of peer verification continues. This is the basic mechanism of Directed Acyclic Graph (DAG) called graph in general. In every subsequent cycle of pooling and verification, the number of both new and peer verified transactions increases. Attack possibility of a bad graph miner propagating false transactions is dealt with by burning the attacker's stakes (through submitting one burn transaction to network with proof of wrongdoing). Furthermore, on nearing the epoch cycle, the graph miners submit the most popular transactions (decided by a score of 3+ peers) and the most information-rich miner wins the stake in each graph.

In a scenario of very local nodes transacting information in peer format (in DAG), the latency and pooling can make a peer very information rich in a short span, so that with a 2-millisecond latency among graph peers, a rightly positioned graph can aggregate up to 50000 transactions with a low footprint in an epoch. For example, the gossiptrust (et. al. Runfang 2008) is one low footprint implementation, although for a large number of nodes.

We have built on a cuckoo filter (instead of bloom filter) based implementation which is 80% faster with a definitive yes/no so that "probably yes" conditions which do not warrant extra overhead (saving 60% processing time).

The top layer of TIM is a blockchain, where all the blockchain nodes (could be same as graph node in a parallel thread) pool all rich graphs from the lower layers by monitoring the first biggest richness claimer in each of the graphs who publicize their score to blockchain nodes.

The blockchain nodes work similarly to graph miners in agglomeration of respective cuckoo filters from the graphs (only the cuckoo filter is stored in the blockchain). The winner blockchain node to create next block is selected by a mechanism of either stake or strongest isogeny calculations. The isogeny requires a minimum of 400 graphs in a multigraph structure (a network of graphs which will be explained further in the partitioning section of this material), below which the network uses the proof of stake to find the worthy blockchain miner.

Attack possibility is mitigated:

- ✔ **Blockchain miner adding wrong filters:** Rejections of a block by concerned graphs and also burning of stakes of the attacker. In such case, the next submitted node with the best timestamp will be added. The top layer block in blockchain contains filters which are used by the payee to verify if it has received an originally unique transaction and not a double spend.
- ✔ **Double spending:** Honest payees can be sure of receiving a valid transaction. Attack

possibility of a double spender sending to self-owned addresses in hope of increasing its money is mitigated by challenger node, apart from 3UTXO checks. Here it is assumed that such attackers would not verify or honor filter test from the newly created block.

The role of the challenger node is to check for duplicate addresses in the cuckoo filters of the block. To ensure that challenger nodes get sufficient time for the test and not causing any (minimal) inconvenience to honest payees, the transactions are unspendable for 120 blocks from confirmation. After 120 blocks, the owner can again spend it. The locking is done by the block height rule of protocol applied after confirmation.

The challenger node gets to claim the original stake of the attacker and need not stake anything to act as a challenger. For self-double spenders, the graph peer reviews using 3 graphs UTXOs, and challenger nodes are a definitive deterrent, among others.

The solution to the problem of huge block size due to a large number of graphs (10000) adding up to ~50,000(max 2^16) transactions is a real success of this architecture.

We have completely mitigated the multi-tier double spending attacks with just less than 0.02% blocksize. Even when the network size is small (a few DAGs), the architecture is lighter than most of the prevalent single or mixed blockchains. And when the network grows to full capacity, graphs maintain the block size of 3 MB and UTXO pool increases by maximum 10MB thus providing very high optimization to graph miners who are the real bearer of workload. The network can thus achieve ~100 Million Transactions per second with much lower footprint than current generations.

Smart Contracts

The blockchain has a virtual machine to provide for generating and exchanging smart contracts. The transactions of smart contracts are performed in a usual two-layer format where the graph miners execute the contracts to validate and propagate consensus. The smart contract-based double spending attacks are handled in the same manner by 3UTXO checks and challenger nodes. Also one can configure a geofencing within which the smart contract can or can't be executed. Such hyperlocal smart contracts are useful for many kinds of permissioned applications where exclusivity is important for business or regulations.

Miners

This architecture has three types of miner nodes where any node can take a role of one or all types of mines:

1. Graph Miners 5 TIM stake is required. Earn 0.01 TIM in every epoch for richness.
2. Blockchain Miners 100 TIM stake is required for network size less than 400 graphs. Earn 0.01
3. TIM in every epoch for consistency with all graphs.
4. Challenger node No stake is required. Earn the attacker's transactions. Only happens for <1% statistical fall off in rare probability. The challenger node has a huge role in fee free subchains (in next sections).

The mining rewards are low due to short block durations and focus more on mining fees so that greater rewards are achieved by acting in favor of masses.

Proof of Belongingness

This is a mechanism to avoid hash flooding where an attacker may try to destabilize the network by fire-hosing a region with very high amounts of transactions. In a rational world, the transaction would be distributed evenly over the continents. The attacker would spoof their geolocation and submit transactions.

This is not a concern when the number is low. And this attack has no bearing on anyone's stakes. This is a DDOS type attack on geolocation-based partitioning to trigger a large number of partitions. Also, the attack's effect will be gone after the nodes blacklist or attacker exhausts the money. But another form of protection against such attackers is required to provide 100% network availability.

The network has a uniform distribution of graph nodes and blockchain nodes who maintain the peer list. This list is organized in a hash table in a hierarchical level of distance like a level of maps data to provide navigation to search for nearest peers. This list is a geographically distributed hash table (GDHT). The flooding affects the utilities who just use the GDHT, irrespective of the money feature. Therefore these utility apps perform a test of belongingness on randomly chosen addresses and defaulters are published in the respective graphs.

The test involves pinging a node to establish TCP/IP and the translation to ascertain real location. Such tests are not fully concordant but act as a possible deterrent. This helps in blacklisting the offending nodes and is a non-blockchain mechanism to maintain network reliability and is a symbiotic response of the P2P utilities for their own benefits as well.

Partitioning & Multigraph

The network starts with two default graphs across the globe with a partition across the equator line *(as shown in Figure. 1)*. With an increase of transactions, the graphs are forked to create a more parallel partition that could increase the overall throughput of the system.

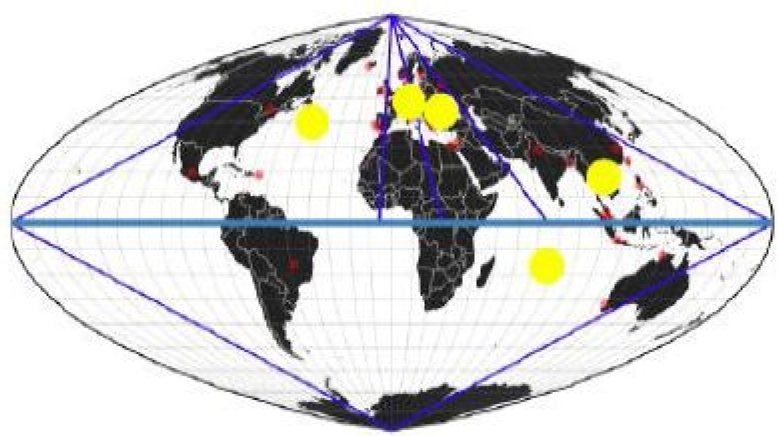

Figure 1 – The multigraph network available at https://www.talking.im/network/. Convex Triangles shown in straight lines instead of great arc for showing the triangle nature.

The partitions are created based on the increase in demand. The triggers for partitioning is as follows:

- ✔ A graph has >30% waiting transactions when compared to consensus, starts polling for a fork. The poll runs for 120 blocks (10 minutes).

- ✔ Upon reaching the block height, if 51% of the time the poll was in favor, a fork is announced from the subsequent 120th block. This ensures that all graph miners are sufficiently aware of the upcoming change
- ✔ Upon reaching the block height, the network gets forked, and the new region is added to the network state file which is also published by the blockchain miner.
- ✔ For the next 120 blocks, the new graphs are locked for any polling to fork or merge. This is a buffer to avoid chaos in the network.

Similarly, a merger is managed by polling, announcing and locking with each of 120 block duration. The condition of the merger is that it has less than 10% of utilized capacity calculated by consensus trend over the surface area.

For the edge cases of transactions waiting from the older graph, the miners keep accepting the transactions for some duration. The network state file is composed of all the graphs and their coordinates arranged in a list. It can have a maximum of 10,000 rows for the cap of the number of graphs.

Quantum Safe Encryption (Experimental)

TIM is future ready blockchain. And quantum safe encryption is a design feature of the network. The multigraph generated by partitioning of the network has Ramanujan's graph equivalence. Above a certain size (~400), the multigraph is used for generating supersingular isogeny encryption keys.

The generation mechanism is collaborative, where each of the graph miners computes the isogeny contribution by keeping oneself at the root. The root nature can be easily verified when the block is signed. This also mandates that the block is to be created by one of the graph miners. To reach this stage, the size of multigraph is key criteria. It also warrants that the network has an equivalent demand to support that many graphs (> 800,000 TPS). Further details of the algorithm will be made available at a later date.

Fee Free Subchains

TIM can host up to 2^60 -1 subchains in a single namespace.

- The subchain participants need to stake a minimum of 5 tokens or specified by the subchain creator.
- The subchains function on the reliability of challenger nodes and without any continuous mining.
- The double spending is mitigated by the challenge from the payee as well as challenger nodes.
- Upon detecting an attack, the offender is submitted to the local graph with proof which the graph miner resolves by assigning the stake of the attacker to a challenger.
- There is a lock-in of 120 blocks for every transaction in subchains which is removed automatically once the block height crosses the limit.

Future Readiness

Blockchain security depends on trust and stability of network participants. One of the newer learnings from the uncountable forks of bitcoin is to build a millennium ready architecture so that the creator of minor changes find it beneficial to stay in the original network. The vision has to be clear towards a growth-oriented future and that has to show in execution as well.

We built a grand architecture based on enterprise experience to provide a high bandwidth and congestion free network with all kinds of security and reliability. We also secured the IP of core tech to avoid fragmentation of community's focus. Thus, we have also made the network fork proof so that the clones don't achieve performance and also not pervasive enough by IP restrictions.

Conclusion

We have proposed a high bandwidth peer to peer money blockchain architecture which can store and exchange money. The digital cryptocurrency and two-layer architecture ensure that the owners can reliably store and exchange their money. We have solved the challenge of block storage by minimizing the cost up to 0.02%. Also, the usage of internet is only to exchange the most important information of hash filters saving the cost of data transmissions.

We solved the problem of multilayer double spending. The network also has provisions to allow smart contracts along with hyperlocal smart contracts which work in certain geographies only. The hyperlocal smart contracts (hdapp) should usher a new era of applications. The geolocation awareness provides for GDHT to enable various kinds of utilities to be symbiotically hosted on TIM blockchain.

We are able to create uniform partitions to allow for larger coverage and inclusivity of low bandwidth regions. The generated multigraph is Ramanujam's graph equivalence which is able to generate SIDH quantum safe encryption after reaching a threshold size. We finally presented the fee free subchain which is mined on-demand and provides a mechanism for everyone to hold a personal blockchain. Also, the fee free subchains are very suitable to host frictionless utilities which need security at the lowest cost. The fee free banking could become a reality with subchains.

Overall, we have pushed many boundaries with this new architecture making this reliable and trustworthy for support of community. The blockchain is for the community.

Appendix

Supply & Distribution

TIM has constant generation rate of max 65 Million tokens per year. There are max of 110 Million pre- mined TIMs distributed as follows:

Annual Generation	6,307,200 blocks x10.01 TIMs(max)
Graph Reward	Each block awards 0.01 TIM in each graph where a max of 10,000 graphs can exist
Block Reward	Each node can get average 0.01 TIM in each block
Hash	SHA256, QFE Isogeny
Pre-Mined TIMs	1100 Million- Burns at end of ICO
❖ ICO	460 Million- Burns at end of ICO
❖ Bounty	20 Million- Burns(For Bounty, developers)
❖ Pre-ICO	30 Million
❖ Seed	90 Million
❖ Team	45 Million- Burns (Locked for 2 years)
❖ Advisors/Partnership	125 Million- Burns (Locked for 1 year)
❖ Foundation	330 Million- Burns (Locked for 3 years)
❖ Lock-in	All tokens except ICO, pre-ICO & Bounty are locked
❖ Hard Cap	USD 19 Million
❖ Pre ICO Smart Contract	0x01e4031d7338c3ae80233b1d66c96d85be98ff90
❖ Symbol	TIM
❖ Decimal	8