Introduction
Version 2.6
Graphs + Blockchain

Table of Contents

Abstract

The paper is organized in 3 sections which begins by discussing various blockchain technologies and cryptocurrency platforms, goals of TIM platform, and lastly its technical specifications. The objective of this whitepaper is to provide detailed analytical description of TIM's inner workings to achieve 100 Million Tx/s. TIM evolved from enterprise implementation of blockchain for easing supply chain woes for postal companies like Singapore Post and e-commerce giant Alibaba. The project evolved from that phase to become a general purpose platform to provide fast and scalable blockchain. We introduced the feature of using geo-location in blockchain to identify and verify the independent nodes. Firstly the geo-location provided many benefits to build an energy wastage free consensus mechanism without compromising the decentralization aspects. It means that this algorithm provides as much security as proof of work (PoW) so that we need not operate certain privileged nodes like in proof of stake (PoS). This is proof of belongingness (PoB). Secondly, the geolocation allowed us to specify coordinates within which a smart contract can operate. This makes the smart contracts safer from outside interference. Also we extended this feature to host smart contracts having their own blockchain along with geo-fencing. We will go through the details in section of Hyperlocal Dapp. And finally, we designed continuous mining in TIM so that security and integrity can be maintained by community. This mining is also based on geolocation. In this mining process, nodes verify the location of neighbors based on what they advertise on p2p network against a special type of network ping checking. Pinging a computer or server tells you many details about their speed and location. We integrated pinging to check location. The attackers will not attack from within the network for getting instantly blocked and burning of stakes for signing 2 headers. The location test is part of graph network of TIM which is responsible to collect transactions in a specified region. These graph networks are dynamic triangular regions. We will start the technical discussion with graphs to build on top of graphs for achieving a high performance blockchain.

Keywords: Graph, Blockchain, GPS, geolocation, Performance

Introduction

The choice of choosing geolocation as a means of designing a blockchain was somewhat accidental. If we had not partnered with Singapore Post to make an IOT device to ease their track-&-trace worries, and if they had not put price pressure to reduce the cost per device, we would not have discovered TIM. We evaluated ethereum and uplifted it's tenets to achieve low cost of operation and making the network fault tolerant so that the clients could use a single blockchain unit across the world without worrying about the bottlenecks created by other regions. For example, the famous 'crypto kitties' dapp in Canada, slowed down the whole network around the globe. Such a situation was not acceptable to our clients. The supply chain of Australia cannot get impacted by games or festivals or ICO spree in China, as an example. Therefore we built parallel graphs to operate independently of each other. These graphs are made of computing nodes over an area in shape of triangle. We initially designed fixed geographic regions in shape of simplest geometrical shape of triangle, but it had security concerns. If the number of nodes in a region goes below critical level, that region can get compromised. Therefore we made the regions dynamic. Now the regions are created based on demand and destroyed when demand ceases. These regions are the graph networks. They exchange transactions, validate among each other based on preset rules, and achieve local consensus. After which the transaction headers from each of the region is sent to the blockchain, every 5 second. The blockchain is a state provider which is a mode of communication among all parallel graphs. Every block of the blockchain contains the transaction headers only without all the proofs. The total file size for each block is in kilobytes. These new features of TIM are exponentially higher bigger and faster in performance, bandwidth and speed.

The classical blockchains

Trust is money. The governments, banks, our community funds, school funds, piggy banks, kitty boxes, and even religious donations to God have an inherent value due to the trust we have in them. And we test this trust every day. And the signs of integrity of that trust keeps us going. But in the past, this trust has often been misused when the system did not provide for transparency so we had to compromise on our participation in that trust system. The crash of banking system due to sub-prime and mortgage crisis is one such example. The trust derived by social status and people leadership is susceptible to erosion with time. Due to impact of time, people change and their value system gets altered. Therefore, you can only trust whom you know a lot and see them growing in life. Regular interaction with those people is very important for you to keep trusting them. But it is not always possible in large cities, globalized world and mega societies of today.

The electronic media of internet paved the way for us to communicate with large number of people and social media became a utility for that means. Similarly the blockchain is an algorithmic media to maintain trust with many people on internet without actually knowing them in person. And with advent of smart contracts on blockchain, one can define conditions to specify the terms of exchanging value which is binding on parties. Though the applications developed to realize the potential of blockchain are themselves very limited for wider usage. For example, bitcoin and ethereum lack speed to be useful for any single bank. Also the cost of these blockchain applications is soaring everyday due to inflation and energy consumed for mining. Additionally, the design of rewards for mining and economics is so much engraved in commercial motives of the miners that changing these rules for ideological reasons or mass benefit is very difficult. The major limitations which we want to overcome with TIM blockchain are:

1. Rate of transaction (Throughput)
2. Cost of Consensus
3. Single Channel
4. Latency
5. Bandwidth
6. Forks
7. Security
8. Privacy
9. Pollution and wastage

10. Cost of entry
11. Size
12. Decentralization

We are solving these challenges using new algorithmic design principles which is already tested in enterprise environment.

Rate of transaction (Throughput)

The blockchains of bitcoin and ethereum have very low transaction rate of 10 per second. Though they are often compared with VISA which claims a rate of 50,000 transactions per second, but there is a difference. VISA and others like it settles the transactions in next 2 to 5 days. Therefore their actual ingestion rate might be 50,000 T/s but in reality the settlement is very slow. Thus their overall transaction rate would be very much like bitcoin. In the context of blockchains, the transactions mean a confirmed immutable transaction.

The primary factors limiting the transaction throughput of blockchain is the latency between nodes. Though the attempts like lightning nodes of bitcoin and plasma of ethereum are proposed solution, but they either become centralized or due to be implemented in case of plasma.

A centralized solution can have high throughput but in that case a single entity is making all decisions. A large number of computing nodes on cloud (like AWS) can achieve that feat. But that is a misnomer for blockchains. If it is not independent nodes being able to verify and add transactions using public rules, it is a pseudo blockchain, not a real one.

Cost of consensus

Achieving consensus in blockchain is related to the types of algorithm being used. In bitcoin and ethereum, the cost of mining is very high which reflects in the inflation of the respective token prices. In proof of stake (or it's variants) based platforms, the cost is fees paid to the master nodes. These master nodes have an expectation to earn back their investments by the fees paid for transactions. Such models are time dependent and may become costly or unviable based on macro-economic changes in general prices.

Achieving consensus in blockchain is essential to maintain the electronic copy of all past transactions so that new transactions can be added in one chain only and without any attempt to double spending. But their algorithmic implementation has so far eluded sustainability. Inflationary mining or predatory reward mechanism makes the blockchain captive to a select few. This can also be termed as cost of

freedom. As new players would need to invest substantially for ability to participate in consensus.

Single channel

Ethereum was put down by cats. The crypto kitties, a dapp based game, slowed down the total global network. Almost all blockchains have single channel. Every transaction goes through serially. Some multi blockchain platforms have emerged but the main blockchain still mines all the sub blockchains.

Latency

Latency impacts many things. And more so in peer to peer network of blockchain, nodes can be located anywhere in the world and also not all nodes might have higher bandwidth. Apart from slowing down the throughput rates, the latency also impacts the participation. Slow network regions of many under-developed regions cannot participate in mining.
Ethereum's ghost protocol ensures on the longest chain instead of parallel chains which are created by high latency.

Bandwidth

The size of blockchain is another limiting factor for ease of maintaining a node. Bitcoin has a blocksize of 1 MB and every node on its network needs to download every block to stay in consensus. A similar gas limit exists for ethereum. Every other blockchain need to have every block data be downloaded by every node globally to reach consensus. Though segwit method of bitcoin provides some relief by delaying the download requirements. The delay adds a temporary relief but globally this block has to be downloaded.
With increase in number of nodes, the bandwidth required will only grow. Thus theoretically, a million nodes on blockchain would need to exchange every block, resulting in 1 Million Megabyte of information exchange on network. Though there is no central location to download, the peers can download from each other's also. But as of now this is a limitation for mass adoption of network.

Forks

This is the most pervasive challenge to blockchain. In a way, forks also spur innovation. But many unnecessary forks are created which is also forking the community and communication with end users. There has been many fatal attempts of forking bitcoin which resulted in people believing the new chain as better but only time was the witness to their undesirable intents behind forking. Though forking may be due to necessity, like Ethereum's 2017 Metropolis upgrade.

Security

PoW blockchains are most secure. The other variants like Proof of stake are lesser secure due possibility of Sybil attack, where an attacker creates multiple addresses and then orchestrates a coordinated attack to reverse the past transactions. Though a substantial stake would be lost in such an attack. The concept of finality is one method, being recently implemented in Casper to 'finalize' the blocks from future changes.

Privacy

Though blockchain transactions are hash based, but it is possible to trace an identity by the inlet-outlet monitoring where a user might en-cash their crypto assets or invest in one through a public exchange. Other forms of identity facing dapps can reveal a user. There are some new blockchains who provide privacy by zero-knowledge based algorithm.

Pollution & wastage

Apart from burning energy for proof of work, the blockchains are adding many other types of waste. They need every node to participate in new blocks by creating a copy, at least if not full node to have past transactions also. The energy burnt in network traffic and creating replica of all global activities contributes to pollution and wastage of resources.

Cost of entry

It was easy to mine bitcoin in early years. Then the complexity started to increase. This ensures that most computationally efficient participants are in favor of network. The cost of stakes in proof of stake based blockchains is another form of entry barrier for new entrants. This limits the adoption of technology in a way. If the entry in bitcoin economy had somehow stayed as easy as in 2009, people could have participated in the network itself rather than forking or participating in newer forks.

Size

The increasing size of blockchain is another form of limitation on blockchains. The bitcoin and ethereum blockchain files are more than 500 terabytes. And with increase in usage and adoption, the size is going to accelerate.

Decentralization

This is the most underrated feature of blockchain, and it is often undistinguishable. There are certain p2p network like Ripple which are completed centralized, and in reality are not blockchain. Decentralization is very important for freedom and independence of p2p network from one-sided forced changes in rules. In decentralized network, the rules are enforced only when everyone or a majority has accepted them. Whereas in centralized network, a single entity makes those rules, and without an opt-out choice.

Even in proof of work and proof of stake type networks, the decentralization become compromised due to a few number of mining nodes who accept or reject the changes based on their interests. Whereas in any network, it is not only the miners who are participants. The hierarchy created due to higher entry barrier to become a miner in p2p network, puts the generic user of a network at the mercy of miners. This is another form of centralization, which has features of decentralization as well.

The project goals

During the creation of this project after our enterprise experience into logistics, we asked one question which is an endeavor through this journey.

◙ How can the internet of money solve key burning problems in making our daily lives easier, fun and limitations free?

With this quest in mind we discovered new solutions for our enterprise clients to make server-free scalable track and trace system in logistics businesses. We borrowed from some of the existing projects, like ethereum, while also built on new solutions for achieving the desired outcomes. The core goals of TIM are:

1. Infrastructure - Build an infrastructure of blockchain which adds value to everyone's daily lives
2. Applications - Develop flagship applications to build a community
3. Extendibility - Build API for all kinds of integration and hosting of services which merges the cloud and blockchain into a single system.

Infrastructure

We are building an infrastructure blockchain deriving our learnings from enterprise experience of fusing geolocation with blockchain. The creation of TIM platform is going to build a wide area blockchain which provides high level of performance, along with fee-less blockchains so that everyone can build applications tomorrow without concerns of entry cost.

Applications

Apart from strengthening the logistics applications of TIM blockchain, we are extending the applicability into blockchain taxi solution. A p2p taxi service connects all the drivers (offering rides) and users (seeking rides) in a nearby location without any central server. Based on a smart contract, the users and drivers can enter into a pickup-drop smart contract and achieve a meaningful outcome. The smart contract binds both the parties in fulfilling their duties. Since, TIM is geolocation based, it can securely ascertain the drop-off location and time conditions. The users and drivers everyone benefit from this arrangement. And the eco-system becomes self-reliant without any third party to pay for. In general, the third party taxi aggregator companies charge average of 30% of the money as service fee. The blockchain taxi makes the economics work in favor of drivers who earn their livelihood. Also the data of users and drivers does not travel across continents into a server. Due to which the users do not face any data congestion. All the traffic

always remains local. In all this, the match making is done by blockchain.
Integration of payments, applying machine learning and many other services will only improve the overall benefits of blockchain taxi.
Blockchain taxi is our flagship application launch.

Extendibility

There are huge scope of applying the taxi like service for many other applications. We will be developing the APIs for many such applications. The codebase in based in python and golang. And the blockchain codebase has been derived from ethereum-go project.

Technical specifications

TIM is 2 layer blockchain, with top layer of blockchain and bottom layer of graphs. The bottom layer has many graphs covering all of the world. At a time, there can be 2 or more graph regions. Each graph region manages its own consensus (locally). The consensus works by validating geo-location of participating nodes. This process is called geo-mining.

The second concept is hyperlocal dapps. In the above explained TIM blockchain, one can create a blockchain. This new blockchain can have geo-fencing, i.e. valid for a geographical region only. In that case, it cannot be mined outside that geographical limit. Such blockchains are not mined but are monitored by the main blockchain of TIM for integrity. If a node tries to double spend in the new blockchain, the geo-mining nodes intervene by mining it and removing any conflicts. The attacker loses stakes. And that is the mining fee for hyperlocal dapp. In essence, hyperlocal dapps, do not pay any mining fee themselves.

Since, everything in TIM is based on geo-location, therefore geolocation integrity is at stake. Attackers would try to spoof or confuse the nodes by faking geo-location. Therefore, the consensus algorithm is called proof of belongingness.

Graphs + Blockchain

The graphs in lower layer are ABFT DAG. These class of graphs provide best in class fault tolerance while providing guarantee of linear time convergence in x-hop neighbors.

$hp(v)=\{u|\ D^x(u,v)\}$ where D is distance of x matrix between u & v

In one of the implementation of real-time push-pull communication mode, the graphs surpass 10,000 transaction per second in a local area network. Such graphs exhibit sparseness based consensus as well, where not everyone has to know everything. But a local knowledge level Ki is determined over time based on historical performance or neighborhood performance history.

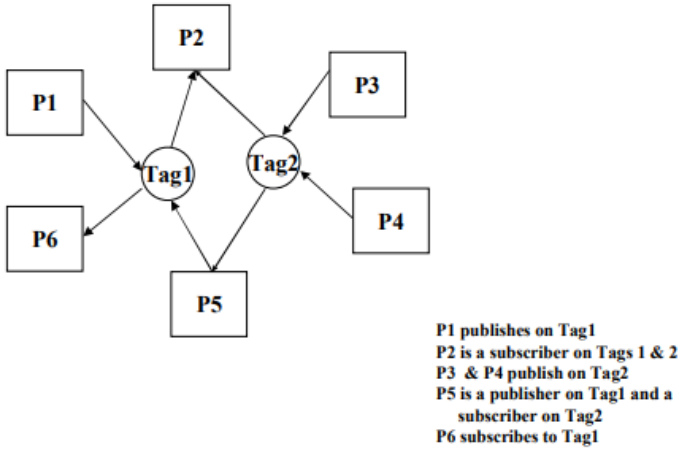
$Gs = \sum g + F(b)$, where

Gs is global performance,

g is local performance $\epsilon(2, 10000)$,

F(b) is fixed time txhash for blockchain

The global performance Gs in above formula can reach up to 100 Million T/s by summation over many such g graphs (limited to 10,000 due to latency and computational time ceiling).



Real-time push pull(Figure above) : Each graph has a linear time of achieving consensus in push-pull real-time network as explained above, to easily and quickly disseminate information across heterogeneous nodes with flexible communication patterns. Realtime push-pull communications is an extension of the real-time publisher / subscriber model, and represents both “push" (data transfer initiated by a sender) and “pull" (data transfer initiated by a receiver) communications. Nodes with widely differing processing power and networking bandwidth can coordinate and co-exist by the provision of appropriate and automatic support for transformation on data. In particular, unlike the real-time publisher / subscriber model, different information sources and sinks can operate at different frequencies and also can choose another (intermediate) node to act as their proxy and deliver data at the desired frequency. In addition to the synchronous communications of the publisher-subscriber model, information sinks can also choose to obtain data asynchronously. This service has been implemented on RT-Mach, a resource-centric kernel using resource kernel primitives*.

How TIM performs on 12 parameters?

TIM is able to provide highest, biggest and fastest performing blockchain. The below table provides a summary.

Problems	How is TIM solving?	Measurement	Competitor
Rate of transaction (Throughput)	2 layers of graphs and blockchain.	100 Million T/s	NA
Cost of Consensus	Tx fee is maintained at lowest by splitting into multiple graphs.	Up to 10,000 graphs	NA
Single Channel	Hyperlocal Dapps are parallel blockchains	Unlimited H-Dapps	Plasma
Latency	Creating new regions	Regions in Africa etc.	NA
Bandwidth	Segregated witness in each graphs	Up to 500 MB of consensus data	
Forks	License + Patent Apache V3	TIM is not fork	NA
Security	Immutable SHA256	Blockchain can't be reversed.	All blockchains
Privacy	H-Dapp can be optionally made private	ZK proof	Zcash, Monero
Pollution and wastage	Geo-mining	No energy intensive mining	NA
Cost of entry	5 TIMs for staking	Easy entry in TIM	NA
Size	Global blockchain has kilobyte sized blocks	100M T/s has low footprint	NA
Decentralization	Geo-mining is highly participative	TIM supports millions of nodes	NA

Supply & Distribution

TIM has constant generation rate of max 65 Million tokens per year. There are max of 110 Million pre-mined TIMs, of which 100 Million is available for ICO and 10 Million for bounty and developers.

Annual Generation	**6,307,200 blocks x 10 TIMs**
Block Reward	Each block awards 0.001 TIM in each graph where a max of 10,000 graphs can exist.
Node Reward	Each node can get average 0.001 TIM in each block.
Hash	SHA256, QFE Isogeny
Pre-Mined TIMs	110 Million - Burnt
• **ICO**	100 Million
• **Developers**	10 Million(For bounty, developers)
• **Tiers**	20 Million for Tier-1, 80 Million for Tier-2
• **Hard cap**	Max of USD 50 Million or 50,000 ETH
• **Smart contract**	0x01e4031d7338c3ae80233b1d66c96d85be98ff90
• **Symbol**	TIM
• **Decimal**	8

Reference
TIM technical paper

D.L. Tao, C.R.P. Hartmann, Y.S. Han, "New encoding/decoding methods for designing fault-tolerant matrix operations", *Parallel and Distributed Systems IEEE Transactions on*, vol. 7, pp. 931-938, 1996, ISSN 1045-9219.

A. Roy-Chowdhury, P. Banerjee, "Algorithm-based fault location and recovery for matrix computations", *Fault-Tolerant Computing 1994. FTCS-24. Digest of Papers. Twenty-Fourth International Symposium on*, pp. 38-47, 1994.

R. Yousefi, M. H. Sargolzaie, S. M. Fakhraie, "Online and offline test unification in digital filters", *Innovations in Information Technology 2008. IIT 2008. International Conference on*, pp. 111-115, 2008.

Triangle Detection Versus Matrix Multiplication: A Study of Truly Subcubic Reducibility∗ Virginia Vassilevska Williams† Ryan Williams

A Real-Time Push-Pull Communications Model for Distributed Real-Time and Multimedia Systems Kanaka Juvva Ra j Ra jkumar J anuary; 1999 CMU CS 99

Ra j Ra jkumar, Kanaka Juvva, Anastasio Molano and Shui Oikawa. Resource Kernels: A Resource Centric Approach to Real-Time Systems. In Proceedings of the SPIE/ACM Conference on Multimedia Computing and Networking, January 1998