

TAU

Server-less and unblock-able messenger with high-scaling blockchain economy.

Version 0.94

Author: <https://t.me/iMorpheusTau>

On-going notes: <https://github.com/wuzhengy/TAU/blob/master/README.md>

Github repo: github.com/Tau-Coin/dhtTAU

#blockchain #dapp #dht #messenger #mobile-mining #server-less #p2c #pot

July 2020

ABSTRACT

Telegram or WeChat provides good communication service on throughput and experience. However, centralized systems do not encourage an independent immutable economy in a digital group. Without financial incentive, a community carries lower value and puts more burden on volunteers contribution. This gives “big tech” chances to monopoly the ecosystem to force small players paying perpetual loyalty. The central controls data transparency and membership without negotiation. This is shown in WeChat situation.

Blockchain provides immutable ledger for an incentive system to function, but it is lack of scalability to satisfy massive consumer base. TAU aims to build a high-scaling blockchain economy in a server-less messenger.

TAU is composed of parallel mobile mining blockchains to achieve the unlimited scalability via multiple chains. Group creator issues fixed amount of coins independent from TAU. That the coins circulating through innovative functions will create financial reward to users and holders. As a result, any community will bear some value. The bigger a community grows, the higher value coins are.

The novel “Proof of Transaction” consensus algorithm, POT, uses on-chain transaction history as probabilistic weight in mining a new block. Chain’s fork selection is done through accumulative difficulty and peers voting. POT is a light blockchain consensus. A smart phone can mine thousands of parallel chains simultaneously .

TAU prioritizes on smart phones to collectively store and verify data. We use a novel multi-level Distributed Hash Table for “peer to consensus” communication. Building blockchain applications on DHT is the most important innovation TAU is about.

* All TAU source code is open and free, except for the ONE TAUcoin genesis secret key.

1. VISION

Blockchain technology needs to support high-scaling decentralized application for its general social acceptance. Current systems, such as BTC or EOS, are limited in scalability and require significant server resources, which causes mining monopoly. On the other hand, centralized services, such as Telegram and WeChat, are efficient, but not giving fair financial reward for small businesses to prosper. The “big tech” makes much revenue by over-taxing on information service, which reduces small player’s share of profitability. Big data and AI is heavily invested with hope to wipe out human engagement and make system even more centralized.

TAU envisions that high-scaling blockchains will eventually replace today’s “big tech” applications such as Uber, Priceline, Youtube, WhatsApp and more. It will provide fair incentive and computing efficiency for a decentralized application.

To prove this, TAU development is innovating a mobile blockchain messenger. The communication experiences will be similar to “Telegram”, except that it is server-less and blockchain coins enabled. The coins consumption and circulation will give value to the community. We believe that an unlimited scaling coins enabled messenger is a step to demonstrate blockchain potential to prevent the world from central dominance.

Individuals will be given transparent opportunity of making income according to their work and knowledge, rather than platform receiving overwhelming share by controlling data and process.

Furthermore, in most parts of the planet, the monopoly of information causes financial poverty and lack of education. TAU is commissioned to discover this uncharted blockchain ability to bring changes.

2. MOBILE PHONE INDEPENDENCE ON “TAU DHT PROTOCOL”

TAU enables any device to be independent. Without being permitted or assisted under servers, personal devices can build, mine and transact on any blockchains. When phone liberated from servers, it lays down the foundation for individual equalization in the computing world. In a server-less environment, there is no function difference between phone and server. This reduces the cost of operating an application. Because of this, TAU messenger has hundred thousands of bootstrap nodes ready on the day one without any spending on hosting.

The biggest technical challenge is in the mobile networking. In order to protect phones, operators install many firewalls and proxies. It is a good practice for security. However, this stops direct peer to peer communication. Phones have to go through a server, such as STUN or TURN, for data relay. A central-less over-lay network protocol for phones is needed for direct communication.

In the past, torrent used central trackers to coordinate clients. There is much legal pressure to stop trackers. As a result, torrent adopted Distributed Hash Table (DHT) to enable tracker-less network. DHT has supported torrent operation for decades with hundreds of millions of users. The protocol evolves from Pastry, Coral to Kademlia. Bittorrent has done great job to build Mainline DHT. Further more, Arvid Norberg has

proposed BEP 44 extension. This enables the arbitrary data cache service. TAU extends BEP 44 key-value pairs for describing block content and messaging. We believe DHT blockchain is TAU's **most important** innovation.

We add the following:

1. Data schema is used to structure blockchain, message or images in DHT cache. For different data, different size of cache is needed. BitTorrent DHT is used as level ONE cache of text communication. We are expecting level TWO for image and level THREE for video in near future. Each data item is an entry to a type of data schema existing in the TAU DAG, direct acyclic graph.
2. Republishing is an action to increase the data availability. BEP 44 delegates republishing to applications. TAU defines new republishing strategy according to different schema and uses block time as publishing interval.
3. The TAU DHT network is viewed as collaborative "**memory**" of a global computer, while storage of each personal devices will exchange data with "memory". However, a full traverse of peers through "memory" will incur $O(N)$ level complexity, which is not ideal. Through each peer's knowledge on latest state, it is possible to reduce traversal complexity to $O(\log N)$. This idea inherits from Dynamic Programming by MIT Prof. Erik Demaine. At $\log N$, the searching time for new information on a big scale user base is towards constant.

These upgrades will lead to the birth of TAU DHT protocol. We release TAU DHT on GitHub.

3. FROM P2P TO P2C (PEER TO CONSENSUS)

Temporary cache on DHT seems to be "sloppy" with much uncertainty. However, with large number of peers collectively maintain the "cache", it will make communication robust by overlaying on top of much segmented IP network. The network effect will make blockchain communication reliable in server-less environment. This has been proved in BitTorrent with daily millions of DHT nodes online to maintain video downloading.

However, a big "cache" without the address regulation is dangerous. For example, in a community, how members are supposed to know which one belongs to which group? If everyone can bring peers into a group to send messages, it will spam the network.

Through blockchain consensus, peers have a common understanding for membership, history and financials. Each peer posts information into consensus cache for other peers to retrieve, assuming others understand the blockchain state. In DHT, a piece of information is commonly stored in 8 nodes of the "cache". After a peer send out information, it can go off-line, which is not affecting other peers to read it. The communication in the consensus environment is similar to the pub/sub model and does not require counter-party to be connected.

It is in each peer's decision how to treat other peers based on blockchain data, such as blacklist or accepting messages. We call this "Peer to Consensus", P2C.

4. PROOF OF TRANSACTION

Proof-of-transaction is a permission-less consensus that miners compete on history transaction volumes. The more transactions a peer makes, the higher probability that the peer wins the right to generate the next block and get the reward. TAU uses “Power” to describe the transaction accumulation. We inherit much knowledge from NXT POS protocol to create POT consensus. POT encourages more peers to make transactions rather than holding coins for mining.

Power

For each mining peer, its mining power P is

$$P = \text{SQRT} \sum_{\text{History}} \text{Outbound Transaction Number}$$

Difficulty Target

Base target $T_{b,n}$ controls the average block interval time at block n . The greater the base target, the faster the next block is generated. It is adjusted by the previous block's base target and the average time required to generate the previous three blocks.

- $T_{b,n-1}$ is the base target of the previous block.
- I_n is the average time interval of the previous three blocks.
- Assumption is that the average block time is 300 seconds.
- $R_{max} = 335$ controls the maximum increase of base target.
- $R_{min} = 265$ controls the maximum decrease of base target.
- $\gamma = 0.64$ makes the decrease of base target smoother.

$$\text{If } I_n > 300, T_{b,n} = T_{b,n-1} \times \frac{\min(I_n, R_{max})}{300}.$$

$$\text{If } I_n < 300, T_{b,n} = T_{b,n-1} \times (1 - \gamma \frac{300 - \max(I_n, R_{min})}{300}).$$

For every address, we define target value T as the product of its power P , base target value $T_{b,n}$ and a time counter C . This counter is the time in seconds elapsed since the timestamp of the previous block.

$$T = T_{b,n} \times P \times C$$

Thus, target value T is proportional to the mining power and increases as time passes. It determines the difficulty for each address to generate the next block.

Generation signature

For block n , there is a field called generation signature G_n . To assemble a new block, each address concatenates its own public key with G_n and calculates a hash to create G_{n+1} .

$$G_{n+1} = \text{hash}(G_n, \text{pubkey})$$

We use the following formula to give each address a random variable of exponential distribution, called hit H of this address.

H = First eight bytes of G_{n+1}

Block generation and forks

An address can generate the next block when

$$H < T = T_{b,n} \times P \times C$$

Initially, time counter C is very small, which means T is very small and it is likely that no address satisfies the above inequality. As time goes, T gradually increases with C , until at some time one address for the first time satisfies the inequality. Then this address can generate the next block. If it does not, as time goes, there will be the second, third and more addresses that satisfy the block generating condition. Eventually, there will be one address to generate a new block.

A temporary fork may occur when two valid blocks are received by one node. We use cumulative difficulty to determine the “best” chain, which is the version to be accepted by every node under POT. Since base target value is the inverse of one block’s difficulty, we define cumulative difficulty D_n at block n as

$$D_n = D_{n-1} + \frac{2^{64}}{T_{b,n}}$$

Cumulative difficulty also serves to prevent nodes from tampering with the timestamp. If one node modifies its local time to generate a new block, difficulty on this block will be lower by the block mining inequality. So this fork will eventually be abandoned due to smaller cumulative difficulty.

5. BLOCK CONTENT AND GENESIS

Bittorrent DHT table allows maximum 1k bytes for value storage. In order to fit the protocol for level ONE cache, TAU puts one transaction into a block in version 1, that one block equals one on-chain transaction. This simplifies the DHT lookup and blockchain operation. The current protocol generate one block every 5 minutes in a single chain. TAU is relying on parallelism for high throughput. Based on blockchain

data, application message volume does not have throughput limit. Users in TAU messenger can send as many chat messages as fast as they can.

There are several ways to increase transaction volume on a single chain, it requires users to agree on upgrading software. We are leaving this process open for future exploration. Options are:

1. put multiple transactions under one hash
2. increase default block generation frequency
3. during genesis of a blockchain, the creator could customize the block time that leads to higher “transaction per second”, TPS

Increase single chain TPS will put more risk on congestion. It is still unknown of how DHT network reacting to this type of upgrade. We will explore this along the product adoption and experiment result.

In genesis block, the creator’s public key will be issued **10 million coins and one year’s accumulative transaction power**. The transaction power is reserved for creator to obtain ability for airdrop transactions. Airdrop is a method to give away coins to initial members.

The block includes:

1. version
2. timestamp
3. blockNumber
4. previousBlockHash
5. immutablePointBlockHash; help voting the right fork
6. baseTarget; for POT calculation
7. cumulativeDifficulty; for POT calculation
8. generationSignature; for POT calculation
9. transactionMessage; transaction content with transaction sender’s signature
10. chainID
11. `TxsenderTAUaddress`Nonce; the accumulated transaction number
12. `Txsender`Balance
13. `minerTAUaddress`Balance
14. `Txreceiver`Balance
15. ED25519 public key as TAUaddress
16. ED25519 signature

6. PARALLELISM

Mono-chain system such as Bitcoin and Ethereum is speed-limited by teen level TPS, since events have to be agreed by all miners. Many scaling modifications are proposed, such as EOS dPOS and IOTA Graph. However, they are compromised on permission-less purity.

TAU fosters a multi-coins ecosystem with parallel independent blockchains. Each chain is still limited in speed, but overall system is unlimited in transaction processing. These blockchains share the same key pairs and allows users to coordinate events cross chains. TAU uses public key as address to satisfy DHT structured data operation, such as the mutable item. This is different from other blockchain's hashed key address.

Parallel blockchains can be viewed as public storage for application meta data, which describes persist-able business and social relationship. The availability of such data will create opportunities for many innovations.

7. VOTING AND MUTABLE RANGE

When a new peer joining the community, it uses voting process to chose the right fork to follow, rather than computing the entire blockchain. Voting is randomly collecting a certain block sample prior to the mutable range. Mutable range is the range of blocks from the present to a specific history block. Blocks in mutable range is allowed to change due to voting fork switching.

New peer will read $\log(N)$ number of sampling blocks from random on-chain peers in the public DHT records. These blocks will be statistically calculated to decide the right chain fork. The new peer will start the mining from the consensus block. Voting makes TAU blockchain much lighter than POW based system. It only verifies blocks from the voted point forward, rather than the genesis time, which could be long time ago.

In the process of mining, if a peer find a fork splitting the chain prior to the mutable range, the peer will start a voting process to ensure itself is on the right fork. If the fork point happens prior to 3 times of mutable range, it will give user options to make human decision on the potential history attack.

8. COINS ALLOCATION

The total supply for each community coin is fixed at 10 millions with 8 decimals. TAU overall system can hold unlimited types of coins. When a community established, all coins are issued into genesis public key.

TAUcoin as one type of the TAU blockchains, it is embedded as default chain in the software to provide announcement services. 82% will be distributed to community. The remaining 18% is reserved by the TAU foundation. For legacy TAUcoin/TAUT holders, TAU genesis account will issue new TAUcoins to them according to their history ownership percentage.

9. TAU AS PUBLICLY AVAILABLE SOCIAL RELATIONSHIP SUBSTRATE

Typically, a “big tech” application includes member profiles, relationship and business data. Such as in YouTube, relationship to a video host is the critical data that builds up value for the platform. The video content by itself does not complete the whole YouTube business model.

TAU is able to make social relationship data operating independently from central infrastructure. The knowledge of the relationship will become public domain asset. Any service provider can provide data service to the relationship graph by joining the blockchain. Application developer can compete on innovations using these public assets.

TAU Messenger could be viewed as the first data service on the relationship meta data. We are very much open to competition to do the same business model using the available data.

10. DREAM THE FUTURE - DECENTRALIZED SHARING ECONOMY

A good group will generate much social attention and carry certain commercial value. Via coins, it is efficient and transparent to build a wealth in it. Peers need coins to perform actions such as advertisements, commerce or services. This will lead to the trading of coins, which drives up the total worth of a community. Participants can trust ledger transparency and coins scarcity thanks to blockchain technology.

Furthermore by removing central platform, a successful youtuber can create own network without paying YouTube commission. The same approach can be also used in any Uber type of projects. Drivers can publish service through consensus, therefore central platform can not charge commission for life. The business data is made as much public available as possible. This will encourage cross-app data sharing. TAU aims to be the source code used to decentralize the economy and end “big tech” monopoly.