TAU

Decentralized communication with high-scaling blockchain economy.

Version 0.92

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

July 2020

ABSTRACT

Telegram or WeChat provides good communication service on throughput and experiences. However, centralized systems do not encourage establishing an independent uncensored economy in a digital community. Without financial incentive, a community carries lower value and puts more burden on administrator's contribution. This gives "big tech" chances to monopoly the ecosystem of a sector to force small players paying perpetual high loyalty to the central. This is clearly shown in WeChat situation.

Current blockchain provides immutable coins ledger for an economy to grow, but it is lack of scaling to satisfy massive consumer base.

TAU aims to bring high-scaling blockchain economy to a community service, such as a messenger. TAU is composed of parallel mobile mining blockchains. Creator of a community blockchain issues fixed amount of coins in their group independent from TAU. The result is the unlimited scaling via multiple chains.

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 computing consensus. A smart phone can mine thousands of parallel chains simultaneously .

TAU prioritizes on smart phones to collectively store and verify data. Bittorrent Mainline Distributed Hash Table, is used to provide over-lay mobile communication. Building blockchains on DHT is the most important innovation TAU is about.

* All TAU source code is open and free.

1. VISION

Blockchain technology needs to support high-scaling decentralized application for daily consumer usage for its general social acceptance. Current systems such as BTC and ETH are limited in scale and require significant server resources, which cause mining monopoly.

On the other hand, centralized services, such as Telegram and Wechat, are efficient, but not giving enough financial reward for small businesses to prosper. The big tech makes too much profit by over-taxing on information service, that will eventually discourage small business growth and restrict technology innovation.

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 both strong incentive and data efficiency for digital economy.

To acheive this, TAU development is innovating a mobile blockchain messenger app. The communication experiences will be similar to "Telegram", except that it is server-less and community coins enabled. Chatting does not consume coins, while some functions require coins. This will create value to the community network.

We believe that demonstrating unlimited scaling blockchain messenger is a step to prove blockchain technology potential to change the world.

2. MOBILE PHONE INDEPENDENCE ON DHT

TAU designs to enable mobile device operating as independent node. With phone liberated from servers, it is the base for individual equalization in the computing world. In the server-less environment, there is no longer function difference between mobile phone and server. Without being connected or authenticated under servers, personal mobile devices can build, mine and transact on any global blockchains. This will much reduce the cost of operating a blockchain.

The biggest technology challenge is in networking. Historically, in order to protect mobile phones, ISPs install many firewalls, NATs and filters. From security point of view, it is a good practice. However, this stops direct peer to peer communication. Phones have to go through a central server. Technically, we need an over-lay protocol for decentralized communication.

In the history, torrent community used central trackers to coordinate peers. There was a big legal pressure to stop many trackers. As a result, torrent community adopted Distributed Hash Table (DHT) to enable tracker-less network. DHT has supported decentralized torrent operation for decades with hundreds of millions of users. They communicate to global DHT network, which does not have a central point. TAU adopts DHT to host cache for key-value pairs describing block content and messaging. Moving tight point to point IP communication to loose coupling cache-based cryptographic communication is an innovation idea. We believe DHT blockchain is TAU's most important innovation.

The new network paradigm is changing from "Peer to Peer" to "Peer to Temporary Cache". Temporary cache on DHT seems to be sloppy with much uncertainty. However,

with large number of nodes collectively maintain the “cache”, it will make communication robust overlaying on top of segmented global IP network. In the end, the network effect will make blockchain communication reliable in server-less environment. This has been proved in bittorrent world with daily 10 millions plus DHT nodes online to maintain a vast number of video downloading.

3. PROOF OF TRANSACTION

Proof-of-transaction is a permission-less consensus that miners compete on history transaction volumes. The more transactions a peer performs, 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 protocol to create POT consensus.

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.

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

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

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}.

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

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.

4. BLOCK CONTENT

Bittorrent DHT table allows 1k bytes for value storage. In order to fit the limit, TAU puts only one transaction into a block in version 1 protocol. One block equals one transaction. This simplifies the DHT lookup and blockchain operation. The current protocol generate one block every 5 minutes.

There are several ways to to increase transaction volume on a single chain, it requires the community to agree on upgrading configuration. We are leaving this process open for future exploration.

1. put multiple transactions under one hash

2. increase block generation frequency

3. during genesis of a blockchain, the creator could customize the block frequency that leads to higher TPS

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

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 to run airdrop transactions. Airdrop is a method to give away coins to initial members.

The block includes:

1. version
2. timestamp
3. blockNumber
4. previousBlockHash; form the blockchain
5. immutablePointBlockHash; help voting the valid fork
6. basetarget; for POT calculation
7. cummulative_difficulty; for POT calculation
8. generation signature; for POT calculation
9. transactionMessage; transaction content with transaction sender's signature
10. chainID
11. `TxsenderTAUaddress`Noune; the accumulated transaction number
12. `Txsender`Balance
13. `minerTAUaddress`Balance
14. `Txreceiver`Balance

15. ED25519 public key as TAUaddress
16. ED25519 signature

5. PARALLEL BLOCKCHAINS

Single chain system such as Bitcoin and Ethereum is speed-limited by teen digits “transaction per second” (TPS), since events have to be agreed by all miners. Many scaling modifications on single chain are proposed, such as EOS dPOS and IOTA Graph. However, they are compromised either on permission-less or decentralization quality.

TAU fosters a multi-coins ecosystem with parallel independent blockchains. Each chain is still limited by TPS, but overall system is unlimited in scaling. These parallel blockchains share same peer key pairs and allows peers to coordinate events among chains. Peer’s key pairs drive the cross-chain applications.

Parallel blockchains can be viewed as open storage for application data, especially meta-data that describes business and social relationship. The openness of data will create many decentralized app innovation.

TAU uses public key as address, this is different from other blockchains hashed key. Public key as address simplifies DHT mutable data exchange. Due to massive number of mobile miners online, the volume of transaction pool is much higher in DTH cache than server-based blockchain system. As a result, the transaction pool cache can also serve as a medium of information exchange on a pub-sub like messaging mechanism. At the time of this doc, the performance of pub-sub based messaging system is still unknown.

6. 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 forks from all peers. Voting is random socially 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 number. Blocks in mutable range is allowed and logical to change due to potential fork switch.

New peer will read sampling blocks from random on-chain peers in the global DHT records. These blocks will be statistically calculated to decide the right chain and conclude a block with the most consensus. Then the new peer will continue the mining from the consensus block and its fork. Voting makes TAU blockchain much lighter than POW based system. It can verify blocks from the present than genesis time, which could be years ago and piled with big history data.

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

7. COINS ALLOCATION

The total supply for each coin in TAU system is fixed at 10 millions with 8 decimals, which can never be changed. 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 and bootstrap services to other community. 82% of TAUcoins will be distributed to community. The remaining 18% is reserved by the TAU foundation team for maintenance and development. For legacy TAUcoin holders, TAU genesis account will issue new TAUcoins to those public keys according to the ratio of their history ownership.

8. TAU AS PUBLICLY AVAILABLE SOCIAL RELATIONSHIP SUBSTRATE

Typically, a “big tech” application includes members relationship and business data. Such as in youtube, membership to a video host is the critical relationship that builds value for the video platform. Without the relationship knowledge such as community, friends or family, the pure data itself does not generate enough value.

TAU is able to make social relationship knowledge 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. Messenger can be viewed as a first simple data service collectively provided through community membership.

9. FUTURE - DECENTRALIZED SHARING ECONOMY ON TAU

With imagination, a good community will generate much social attention and carry commercial value for advertisement. Via coins, it is efficient and fair to build an economy for the community. Peers need coins to perform actions such as advertisement. This will lead to the trading of coins, which drives the total worth of a community. All participants can trust ledger transparency and coins scarcity due to blockchain technology.

Furthermore by removing central platform, a successful youtuber can create own community without paying YouTube commission. The same approach can be also used in any Uber type of projects. Drivers can publish service through DHT, 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 sharing economy and end the “big tech” monopoly.