TAU Idea

Torrent video and message publishing with blockchain economy.

Version 0.9

Author: https://t.me/iMorpheusTau

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

June 2020

Abstract

High-scaling server-less crypto-coin application is a “holy grail”. We don’t have it up to today. Several bottlenecks slow down the progressing. Firewalls prevent mobile devices from direct peer to peer connections. Transaction processing volume on a single blockchain is limited in low range. Lack incentive of sharing reduces the mass participation.

TAU system is composed of parallel blockchains accessible through same private key. Any community is free to build their blockchain. The result is the system-wide unlimited transaction per second, TPS.

TAU focuses on enable phones to collectively store and verify data. Distributed Hash Table, DHT, is used to provide asynchronous communication. Building blockchain on DHT is the most important innovation TAU is about.

Proof of Transaction consensus uses on-chain transaction history as probabilistic weight in mining a new block. Chain selection is done through accumulative difficulty algorithm or peers voting.

Torrent sharing community can use TAU to build coins economy and censorship resistant anonymous publishing. Our technology stack can be used in many areas such as forum, e-commerce or sharing economy apps. TAU focuses on using publishing as a show case. Developers are welcome to use open sourced TAU code to build apps.

1. Vision

Blockchain crypto-coin needs to support high-scaling decentralized application and independent mobile phone for daily usage. The current blockchain system are limited in scale and require significant server resources on public network. Mobile apps need to connect to some center to function.

TAU aims to innovate blockchain technology to fit it into a day to day application. Among many good projects, torrent file sharing is a decentralized successful case; however, publishing torrent is lack of financial reward and sometimes inhibited by censorship. We believe that building a blockchain system to make torrent publishing equipped with economy and censorship-resistance is a great step to prove blockchain's potential.

2. Mobile phone independence on DHT

TAU designs to enable mobile device operating as independent node. With mobile phone liberated from servers, it is the base for nodes equalization and individual engagement into blockchain full life cycle. Without connecting or subjecting to a server, mobile devices can create, mine and transact blockchains. This offers full permission-less access for normal consumers phones to participate the global computing.

The biggest challenge so far is the network. In order to protect mobile phones, ISPs install many firewalls, NAT and filters. From security point of view, it is a good practice. However, this stops direct peer to peer communication. They have to go through a central server.

Torrent community uses central trackers to coordinate peers. There is big legal pressure to make many trackers shutdown. Torrent community adopted Distributed Hash Table (DHT) technology to enable tracker-less network. DHT has supported torrent operation for decades with hundreds of millions of users. It is a good proof that "tracker-less" is working in torrent sector. Rather than peer talking to peer, peers now communicate to global DHT network, which does not have a central point.

This "tracker-less" solution provides a showcase for blockchain nodes communication. TAU adopted DHT key-value database for block content communication. We believe this is TAU's most important innovation. In the tracker-less or server-less environment, there is no longer function difference between mobile phone and server. Individuals can use a phone to run a full function blockchain application.

3. Proof of Transaction

Proof-of-transaction is a decentralized 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.

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

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}.

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

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 Structure

For fitting the current torrent DHT key-value storage limit, TAU puts only one transaction into a block. One block equals one transaction. This simplifies the DHT lookup and operation.

To increase transaction volume on one chain, it requires the community to agree on upgrade configuration of block frequency. It is currently set as one block every 5 minutes. When TAU has 1000 parallel chains, it is 1000 blocks every 5 minutes system

wide.The other case is, during genesis of a blockchain, the creator could customize the block frequency that leads to higher TPS and risk of communication congestion.

The block structure:

1. version;
2. timestamp;
3. blockNumber;
4. previousBlockHash;
5. immutablePointBlockHash; help voting the valid chain.
6. basetarget; for POT calculation.
7. cummulative_difficulty; for POT calculation.
8. generation signature; for POT calculation
9. msg; 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. signature;

5. Parallel blockchains structure

Single coin blockchain system such as Bitcoin and Ethereum is speed-limited by transaction per second (TPS), because any event has 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-coin ecosystem with parallel independent blockchains that enables community to create multiple coins and blockchains. Each chain is still limited by TPS, but overall blockchains system is unlimited in scaling.

The parallel blockchains share same peer's key pairs and allows peers to coordinate events among chains. Peer's key pair drives the software and cross-chain applications.

6. Block reward

Most of blockchain uses positive block rewards. TAU adopts positive and negative mining rewards to achieve decentralized coins distribution or airdrop.

- Mining the block: once your generation signature satisfies the mining requirements. You will win the block and get transaction fee. This is positive reward.
- The negative mining reward is a coins transfer from miner to a transaction maker. Miner could setup automatic or manual transaction approval to give away coins. For

transaction sender, it is a transaction with either nil or negative transaction fee amount. It can be used to provide airdrop to new members.

7. Voting and mutable range

For a new peer coming on-line, the peer uses voting to chose the right fork to follow. Voting is collecting blocks within the mutable range. Mutable range is the range of blocks from the current block number to a specific history block number. Blocks in mutable range is possible to change due to longest chain fork change.

New peer will read random blocks in the mutable range from global DHT records. These blocks will be statistically calculated to decide the right chain and a consensus block. Then the new node will continue the mining from the block.

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

8. Coins allocation

The total supply coins in TAU system is 10 millions. Each coin is divisible to 8 decimals. When each community established, there will be 10 millions coins issued into genesis account.

TAUcoin as one of the TAU blockchains, it is embedded as default chain in the software to provide announcement and bootstrap services to other community chains. 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 coins history ownership.

9. Torrent sharing economy

A good torrent community will generate many user traffic and enable publishing messages with commercial value for advertisement or some business model. Without crypto-coins, it is hard to build an economy for the community. With coins, new participants need to purchase coins to join the community to perform actions such as advertisement. This will lead to the trading of coins, which eventually drives up the total value of a community. Since everything is built on blockchain, all participants can trust ledger transparency and coins scarcity.