TAU

Phone Mining Blockchain Technology Key Ideas

Version 1.0

Author - iMorpheusTau

On-going notes - https://github.com/bloockchaindev/TAU/README.md

Github repo - github.com/bloockchaindev/Tau

#blockchain #dht #phone-mining #pot #bloom-filter

Feb 2021

ABSTRACT

Bitcoin provides an immutable ledger for crypto coins, but it is based on heavy resources consumption required by Proof of Work(POW) computing.

TAU aims to build a Proof of Transaction(POT) blockchains network on phone mining. POT is a light blockchain consensus. An average smart phone can mine hundreds of blockchains simultaneously without tie to servers.

TAU network is composed of many independent blockchains to achieve high scalability. Anyone can create a blockchain permission-lessly without using TAUcoins. The bigger a blockchain community grows, the higher value the coins are.

The POT consensus uses on-chain transaction history as probabilistic weight in mining a new block. Chain's fork selection need to satisfy both accumulative difficulty and community history bloom filters.

Building blockchain on Distributed Hash Table and resisting secret chain attack via local Bloom filters are the key innovations.

* All TAU source code will be open source after mainnet.

1. VISION

Current blockchain systems, such as bitcoin or ethereum, require significant server resources, which causes mining concentration and prohibits common users to participate an essential blockchain task: the mining.

TAU is creating a phone mining technology. Without being permitted or assisted under servers, personal devices shall be able to build, mine and transact on blockchains. When phone liberated from servers, it lays down the foundation for individuals' equality and freedom in the digital world. In a server-less environment, there is no permission difference between phone and server. This further reduces the cost of operating a network application.

2. PHONE MINING BUILT ON "DHT"

A technical challenge to the vision is the traditional mobile networking. In order to protect phones, mobile operators install firewalls, NATs and proxies. It is a good practice for security. However, this stops direct peer to peer connections. Phones have to go through a server to carry out communication.

In the past, torrent community used central tracker servers to coordinate video download. There was strong legal pressure to stop trackers. As a result, torrent community adopted Distributed Hash Table (DHT) to enable central-tracker-less network. DHT has supported torrents for decades with hundreds of millions of users. Bittorrent has done great job to build Mainline DHT. Further more, Arvid Norberg has proposed BEP 44 extension. This enables the arbitrary data service on DHT. TAU uses BEP 44 mutable data for blocks, transactions and messaging.

3. PEERS WITH CONSENSUS

Mutably storing data on DHT nodes seems to be "sloppy". However, with peers collectively maintain the "cache", it will make communication robust even by overlaying on top of segmented IP networks. This has been proved in BitTorrent with daily millions of DHT nodes online to maintain video downloading meta-data.

However, a big "cache" without the membership regulation is dangerous. For example, in a group chat, how members know who belongs to the community? If anyone can bring peers into a group to send messages, it will spam the group chat.

Through blockchain, peers have a common understanding of the membership. Peers in the consensus posts information into DHT for other peers to retrieve. It is in each peer's decision how to treat other peers based on blockchain data, such as blacklist or accepting messages. There are no delegates to make membership decision for peers.

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 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. POT also use community members bloom filters of blocks to prevent secret chain attack which is a common risk for POS blockchains.

Power

For each mining peer, its mining power P is

$$P = \sum_{\text{History}} \text{Annual Outbound Transaction Number} \times \text{Annual Fibonacci Coefficient}$$

Each year, the power one transaction receives grows according to Fibonacci series. For one transaction in the first year, it will receive 1 power; 2nd year, 1 power again; 3rd year, 2 power; 4th year 3 power; and so on.

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

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

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, 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

Libtorrent DHT allows maximum 1k bytes for value storage due to UDP MTU size. In order to leverage the speed of UDP, TAU puts one transaction per block, that one block is limited to 1k. The current protocol generate one block every 5 minutes in a single chain. TAU is relying on parallelism for high transaction throughput. Messages do not have throughput limit. Users in TAU messenger can send as many messages as fast as they can.

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

1. put multiple transactions under one block, which might sacrifice the MTU efficient transmission benefits.

2. increase default block generation frequency, which might be more storage demanding on phones.

In genesis block, the creator's public key will be issued **1 million coins**. The block includes follow fields:

1. version
2. timestamp
3. blockNumber
4. previousBlockHash
5. immutablePointBlockHash; help to prevent the secret chain attack by checking with community history blocks bloom filters
6. baseTarget; for POT calculation
7. cummulativeDifficulty; for POT calculation
8. generationSignature; for POT calculation
9. transactionMessage; transaction content with transaction sender's signature
10. chainID
11. TxsenderNonce; the accumulated transaction number, TAU puts essential states on chain to provide stateless mining capability.
12. TxsenderBalance
13. minerBalance
14. TxreceiverBalance
15. ED25519 public key as address
16. ED25519 signature

6. PARALLELISM

Mono-chain system such as Bitcoin and Ethereum is speed limited by teen level TPS, since transactions have to be agreed by all miners. Many scaling modifications are proposed, such as EOS dPOS and IOTA Graph. However, they are compromised on the quality of the permission-less participation. In TAU view, permission-less is the most important feature of a blockchain.

TAU fosters a multi-coins ecosystem composed of parallel independent blockchains. Each chain is still limited in speed, but overall eco-system is unlimited in transaction processing. One blockchain in TAU world provides a scope of a community, through this consensus members of the same community can interact without throughput limit.

7. BLOOM FILTERS AND MUTABLE RANGE

When a new peer joins the blockchain, it will be initially following the chain that invitation link includes. At the minimum security, the peer validates blocks to the immutable point rather than the entire blockchain to build up the initial state database. Therefore, TAU essentially is a partial state blockchain, which does not require entire state information to operate.

In the process of mining, when the peer finds a new block, it will check whether the hash of the block immutable point is in the community blocks bloom filters. If more than half of the community bloom filters do not include this immutable hash, the new block is part of the secret chain.

If the new block is not an attacker, the peer will sync up and validate the chain to the merging point.

When peer is online, it will always collecting community peers' bloom filters for future validation.

Bloom filters are also used in data communication between peers. TAU peers exchange data through broadcasting to DHT cache a distribution of a set of data and its bloom filter, rather than connection based sequential transmitting such as TCP.

We upgraded classical bloom filter with combining a pair of sequential data as a member unit of the set, to further reduce the false positive rate in data exchange.

8. COINS ALLOCATION

The total supply for each community coin is fixed at 1 billions with 8 decimals. TAU overall system can hold unlimited types of coins. When a community established, all coins are issued into the genesis key. TAU does not implement the block reward, the only income for a miner is from transaction fee which is connecting to POT consensus. All TAU community coins are deflationary in nature.

TAUcoin as one type of the TAU blockchains, it is embedded as default chain in the software to provide some public services such as bootstrap nodes information. 82% of TAUcoins will be distributed to community. The remaining 18% is reserved by the TAU foundation for R&D purpose.

9. TAU AS PUBLICLY AVAILABLE SOCIAL RELATIONSHIP KNOWLEDGE

Typically, a “big tech” application includes member profiles, relationship and business data. Such as in YouTube, relationship to a video host builds up much value for the platform. The video content alone does not complete the 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 knowledge by joining the blockchain. Application developer can compete on innovations of using these public information.

By removing central platform, a successful YouTuber can create own network without paying commission. The same approach can be used in any Twitter, Priceline, Uber type of projects. Drivers and hotels can publish service through consensus, therefore central platform can not charge them. Requiring only a phone, TAU aims to be the initial sample code to decentralize the digital economy and end “big tech” monopoly.