TAU – True Asset Unit

Introduce A mobile and decentral Proof-of-Transaction crypto coin

Version 0.7 - on going

imorpheus, genie854, Constantine Pappas and Zi Ren Teoh

Jan 2019

Abstract

That making each one's phone to run as a universal bank for verifying global transactions and storing asset is an essential protection to personal wealth; therefore, billions of people would not be afraid of currency inflation and control. In order to achieve this, we introduce a novel consensus mechanism, Proof-of-transaction(POT). POT uses transaction history based probabilistic weight as Byzantine General proof to produce new blocks. The longer chain time, the stronger the "total consensus strength" accumulates to be more secure. Minimizing the block header and its size, TAU protocol is light enough to allow mobile device to mine, so that pervasive mining is supported fairly.

This is an on-going work. We welcome content contribution and discussion on bitcointalk.org.

https://bitcointalk.org/index.php?topic=5041949.0

1. Background

Proof-of-work (POW) and Proof-of-stake (POS) have become two popular consensus mechanisms across the world of blockchain today. While POW is more secure with its resource intensive computational process, POS is more environmentally friendly with its staking solution. However, both mechanisms have their shortcomings.

In POW, miners compete against each other for block reward, which leads to an arms race of electricity and hardware. The race, while improving security level of the network, places a huge entrance barrier for most users. Due to economics of scale, only large mining pools with access to cheap electricity can remain profitable and the network becomes more and more centralized. As network utility grows, energy consumption per transaction for POW also grows.

POS by its nature inspires hoarding, as hoarding is the very mechanism that is used to find consensus. Concentrated and static wealth becomes the best way to compete for block generation. As a result, circulation of currency is not promoted or even discouraged, and wealth concentration increases as network grows.

Despite these issues, both have been able to build large coin ecosystems that are considered secure and trustworthy. The common bottleneck for them is the time accumulation. The longer the time, the more cumbersome develops both in energy consumption and stake power concentration.

2. TAU overview

The proposal of TAU is an original consensus mechanism POT. It uses on-chain historical accumulated transactions to determine who can propose a new block. Block generation in TAU is still called mining like Bitcoin, but block reward only comes in the form of transaction fee. TAU is a single utility chain that funds wiring is the only thing supported; therefore, transaction fee is the only income for miners. TAU block structure is designed to support mobile phone mining for decentralization.

Total 10 billions coins are generated in the genesis block, while the goal is for each individual to have a full TAU. For every address, the probability of generating a new block is exactly in linear proportion to its historical transaction. This sum is called mining power, an analogue to hash power in Bitcoin.

Inspired by NXT, TAU uses similar methods to generate random number among mining address, to adjust block interval times and to handle temporary chain forks. On a base level, TAU uses Bitcoin cryptographic technologies that have been proved reliable. These include public-key cryptography, digital signature and address-based transactions. Blocks are organized in a way similar to Bitcoin, with block header containing minimum parameters such as timestamp, hash and public-key. As for communication, TAU uses specially designed peer-to-peer best-effort broadcast and transaction pool to traverse the mobile NAT and firewalls.

The basic unit of TAU coin is TAU. It is divisible to 2 decimal places with the smallest unit 0.01 TAU.

3. Total Consensus Strength

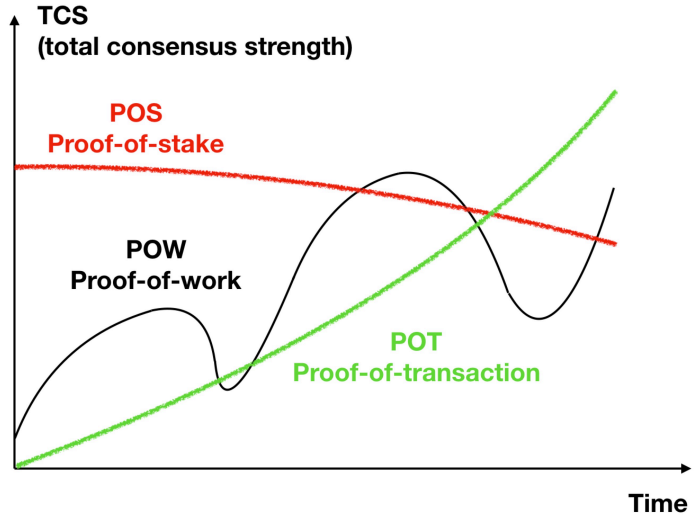
We use “total consensus strength”, TCS, to measure and compare the robustness of security development in a blockchain.

The definition of TCS:

(total consensus strength) = (number of active miners) X (average mining power)

The chart shows robustness of three types of consensus along with time passing.

Proof-of-work is a permission-less consensus that miners compete on computing power. The stronger one miner’s computing power, the higher probability it will generate next block. Financial ability to maintain cost on the computing power leads to centralization. Strength of POW is affected by declining miner numbers and the increasing cost of computing power. When the mining community is limited, drop-out of a few miners will cause fall of the strength such as hash rate decrease in the bitcoin bear market. The root cause is the increasing physical cost to maintain power, so that the total strength is fluctuating along the cycle. The unstableness is vulnerable for attack as we have seen in BCH and ETC, when extra hash rate could rented forming 51% power in short time period.



Proof-of-stake is a decentralized permission-less consensus that miners compete on holdings of coins. It is lower cost in maintain computing power. Most of POS generates all coins on the first day, so the maximum total strength is fixed. Along with lost of coins and silence of holders, the strength is declining and eventually concentrating on few miners.

Proof-of-transaction is a decentralized permission-less consensus that miners compete on transactions history. It does not support mining pool from design and low cost to maintain. The strength of consensus is increasing along the transaction numbers accumulated on the blockchain. The longer the chain, the higher strength of consensus it will obtain. The total strength is ever increasing while transactions happening and potential block size and generation frequency upgrade.

4. Single Utility

Protocol architect tends to put multiple benefits into one chain such as peer-to-peer payment, coin-base reward, ERC20 contract or privacy algorithm, and the list can go long and fancy. Each one of these functions is good and essential in many applications. However, putting them all together in single protocol is not only crowded but also dangerous.

Let's analyze the situation that two utilities coexist on one chain, such as BTC. Miners could make both transaction fee and coin-base mining reward. Each function, mining or funds-wiring has its own supply and demand ecosystem. For example, in order to receive coin-base block reward, you need to compete by paying for physical resources; on the other side, in order to support peer to peer payment and receive transaction fee from users, you need to generate the block as well. However, two system valuation is different enough to cause discrimination. Connecting them together was thought as a smart design for one stone getting two birds, but now coin-base reward is significantly more weighted than transaction fee. This makes the cost of transaction too high to maintain. Some miners does not care whether there are transactions in the block at all.

Simple math shows that each block cost $100K to produce in Jan 2019, one block can support 2000 transactions, that is $50 per wiring as total cost from the bitcoin community. Now mining is the game on coin-base reward than the transaction fee market, so that no miner will care this $50 per transaction total cost. BTC is designed to provide peer-to-peer trust-less payment, not competing reward. Its core function is now jammed by mining reward hunters. This is not miner's fault but the result of putting TWO utilities in single blockchain, so that the volatility is inevitable to reflect two markets.

The same argument exists in ETH as well. ERC 20-ICO market is much stronger than the coin-base reward and p2p payment. This makes ETH price too high to support its origin goal as a global computer.

TAU proposition is that pure blockchain design should only have single primary utility, either p2p payment, ICO, anonymous or speed. If you put two utilities into one protocol, a competition between two utility will eventually cause endless volatility.

Based on the experimental learning from BTC and ETH, Taucoin is designed to reward miners transaction fee only and support single function.

5. Block Structure

Block header: 1–4; the block header allows nodes to find out which chain has the highest accumulative difficulty. Using timestamp and public key in block header is sufficient to compute each block target base and difficulty number. Header is small of 58 bytes, full day's header info is 17Kbyte. With this small data set, it is efficient for nodes to find highest difficulty chain globally to avoid forks. We removed merkle root on purpose, because TAU block size is only 5K.

1. *version: 8 bits; keeping version is for upgrade to define the transition grace peroid.*
2. *timestamp: 32 bits*
3. *previousHeaderHash: 160 bits; use SHA256, RIPEMD 160*
4. *generatorPublicKey: 264 bits; compressed public key in ECDSA.*
5. block signature: 512 bits; to ensure the integrity of the block without supporting public key recovery, since public key is available on 4.
6. option: 8bits; this is left for future use.
7. transactions stack

“Hit” number is the first 8 bytes of hash (previous block generator public key 64 bytes+ current generator public key 64 bytes); with this network random number, TAU network can decide who is the current winning miner and predict the future mining sequence to detect secret chain.

The block common area is total 984 bits, 123 bytes.

Transaction: only support transaction from one address to another address.

1. version: 8 bits; keeping version is for upgrade to define the transition grace peroid.
2. option: 8 bits; for future use.
3. timestamp: 32 bits; transaction will expire in 12 hours and not be added to block 12 hours ahead of the header timestamp. 24 hours, 288 blocks, are needed to confirm the expiry for funds sender. User can resend transaction on 2nd day once expired. We choose timestamp over nonce(ETH) to avoid complexity of transaction sequences.
4. toAddess: 160 bits, this is SHA256-ripemd160 on a public key.
5. amount: 40 bits
6. fee: 16 bits
7. transaction signature: 520 bits

Every transaction is total 784 bits, 98 bytes. Block contains 50 transactions on average 5 minutes time interval.

6. Checkpoint and mutable range

Tau defines checkpoint is the block height and block signature hardcoded in software, such as genesis block or blocks periodically added into Taucoin Implementation(TIP).

Once a node is confused with which chain to follow, it always goes back to software last checkpoint and searching highest difficult chain available in the network.

Who decides checkpoint content? Initially TAU foundation will maintain checkpoint signature information on website, in the future, we expect community to have a rating service to provide checkpoint validation in social media, due to the “weak subjectivity” matter.

In order to avoid “secrete chain attack” which are double spending and long range reorganization attack, TAU defines “mutable range” for each miner from current block to previous 144 blocks; blocks. Before the mutable range, it is immutable range. Within mutable range, miner can switch blocks chain according to received difficulty value. Software can not switch into “immutable range” unless external intervene such as instruction from human to go back to last checkpoint or the true highest difficulty chain.

When a block with higher difficulty forks out after checkpoint and before mutable range, TIP shall alert miners such attack happening, then transparent mining data shall be in place to give analysis whether this was a secret chain to kick out and make new checkpoint.

7. Proof of Transaction

Mining power

For every mining address, its mining power P is

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

There is no set range for transaction fee. All depends on market.

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 previous block.
- I_n is the average time interval of the previous three blocks.
- In our current version, 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 timestamp. It 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.

8. Client to Client architecture

All coin mining requires public IP address for nodes to communicate with each others on IP network, that is Internet. It is required for BTC, ETC, EOS and all as I know. On today's Internet, only server has public IP, and blockchain network consensus is really built on "server to server". You wallet is a client connecting to one of those servers, therefore wallet is not decentralized neither have the full picture of the pubic ledger to running by itself.

Clearly, good wallet shall run on mobile phones. However, mobile phone does not have "real IP address" due to IPv4 network is not able to provide many IP addresses. IPv6 needs many years to come, so that the mobile industry using NAT, network address translation, to make many phones sharing one public IP and giving cell phone internal IP address behind firewall. Without public IP address, mobile phone can only be client and not able to be a full mining node on public internet. Different cell phones behind firewall need centralized server to communicate to each other such as you see in whatsup and wechat.

TAUcoin is solving this industry bottleneck, to build true "client to client, server-less" networking allow blockchain to be maintained on mobile phone systems without any super node software. Every wallet is a full node running on mobile phone behind NAT firewall using internal IP address. So that we makes "server", "client" and "wallet" all the same to achieve true decentralization.

9. Products

mWallet - mobile mining Wallet is your true universal bank. It stores entire block chain and able to mine independently.

Web Wallet - web wallet is an launchpad for your experiences in TAU. You will receive your initial coins and start to do transactions. However, web wallet is centralized and private key is stored in central server. It is not as secure as mWallet in your phone.

TAU work - a taucointalk function provides users buy and sell services via TAUcoin. We expect this will generate internal value for TAU community.

10. Economy and governance

Coin allocation

The total supply of TAU is set at 10 billion. All coins will be generated in the genesis block. Of these, 82% will be distributed through faucet and bounty program. The remaining 18% is reserved for the TAU foundation team to support maintenance and future development of TAU project.

Long term economic effects

We expect some positive long term effect under POT mechanism. The first is that transactions of all kinds are promoted. In theory, fee of every transaction can be divided into two parts, normal fee and future investment. As a result, users are willing to make more transactions than they do on POW or POS chains. Hoarding coins carries no reward at all and is thus discouraged. We believe this effect will bring an increase in velocity of currency and is healthy for overall economy growth.

The second long term effect is wealth redistribution that favors the normal participants instead of “making the rich richer”. It is assumed normal participants make more normal transactions than the “rich”, when grouped sum is considered. So POT gives the normal participants better rewards than POW or POS does, under which the majority of users have almost no computing power or stake to get any reward. Under POT, mining power is more pervasive than POW and POS, which we believe is beneficial to the network.

11. Outlook and debate

Fight 51% attack—51% attack is unavoidable on decentralized ledger according to Satoshi, and just happened in BCH community. With 51% power, one can do both short range (double spend or censorship) and long range attack (rebuild a new chain).

TAU aims to make it harder for anyone to obtain 51% of the total power.The most scarce resource to build is “time” rather than equipment and stake. In a blockchain, the transactions are representing “time”. Transactions cost fee to happen, so that it is immune to Sybil attack luckily.

Checkpoint is used to contain long range attack, TAU will inherit that although it is still at mercy of “weak subjectivity”. For short-range attack, when POT blockchain lives many years, in order to secure 51% POT power, one need to either secure enough miners’ private keys to get power or build own power through same time period. The older the chain, the harder to achieve that, due to time can not be created.TAU ecosystem might need some social media to monitor who is the true chain. We will add that into mWallet.

TAU focuses on mobile node to make more people be able to mine and secure the chain. This will make “nothing at stake” hard to implement on massive small forks. POT total mining power will be very distributed among many addresses, it will be hard to form 51% power to fight against network. We recently removed the mining club to make 51% formation even harder, and reduce the block size to 5kb to allow maximum data availability in the network.

Transparent forging is unique in POT to predict next miners. This technology is potentially able to give us more information when certain attack happening.

Block size and generation frequency upgrades, when 5G network is prevail.

Reference

1. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
2. "Nxt Whitepaper" and "The math of Nxt forging"
3. "Security Analysis of Proof-of-Stake Protocol v3.0"
4. King, Sunny, and Scott Nadal. "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake." *self-published paper, August* 19 (2012). "
5. NEM Technical Reference Version 1.2.1"
6. Kiayias, Aggelos, et al. "Ouroboros: A provably secure proof-of-stake blockchain protocol." *Annual International Cryptology Conference*. Springer, Cham, 2017.
7. Bentov, Iddo, Ariel Gabizon, and Alex Mizrahi. "Cryptocurrencies without proof of work." *International Conference on Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2016.
8. Bentov, Iddo, et al. "proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y." *ACM SIGMETRICS Performance Evaluation Review* 42.3 (2014): 34-37.
9. Garay, Juan, Aggelos Kiayias, and Nikos Leonardos. "The bitcoin backbone protocol: Analysis and applications." *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 2015.
10. Larimer, Daniel. "Transactions as proof-of-stake." (2013).
11. Decker, Christian, and Roger Wattenhofer. "Information propagation in the bitcoin network." *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*. IEEE, 2013.
12. Rizun, Peter R. "A transaction fee market exists without a block size limit." *Block Size Limit Debate Working Paper* (2015).