TAUT – Fast, Fair, Secure

An experimental Proof-of-Transaction cryptocurrency on PC Mining

Version 0.1, subject to change (ongoing)

June 2019

Abstract

We introduce a novel consensus mechanism, Proof-of-transaction(POT). POT uses accumulated transaction history as proof to generate new blocks. The reward is transaction fees contained in each block. Reduced the block size to 1mb per minute, TAUT is a non-inflation, light and secure crypto currency based on POT. TAUT protocol aims to support PC mining with no importance of having hardware and staking power, so that a large pervasive mining population is possible. The longer the chain transaction history, the higher security the network is.

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. We believe that good technology should be more pervasive and more efficient. As transaction volume goes up, transaction speed should go up and energy consumed per transaction should go down. We have created TAUT that accomplishes the above goals without the loss of security.

2. TAUT overview

The first and most important contribution of TAUT is an original consensus mechanism POT. It uses on-chain historical accumulated transaction fee to determine who can propose a new block. Block generation in TAUT is still called mining like Bitcoin, but block reward only comes in the form of transaction fee. All coins are generated in the genesis block. For every address, the probability of generating a new block is exactly in linear proportion to its historical transaction fee paid within a certain time window. This sum is called mining power, an analogue to hash power in Bitcoin.

The second improvement is that TAUT supports signal transaction, a special transaction that establishes a predefined relation over the network. It can be used for on-chain delegation. For example, every address can delegate its mining power to another address, forming of mining club and receiving its fair share of reward.

The third feature of TAUT is efficient, synchronized and fair distribution of block rewards. Blocks are grouped into epochs, during which mining power and its delegation remain unchanged. At the end of each epoch, a checkpoint block is generated to indicate finality. Reward distribution and mining power update also occur at the end of each epoch. All these serve to reduce computation loads on full nodes, thus lowering entrance barrier for mining.

Inspired by NXT and NEM, TAUT uses similar methods to generate random number among mining clubs, to adjust block interval times and to handle temporary chain forks. On a base level, TAUT uses Bitcoin technologies that have been proved reliable. These include public-key cryptography, digital signature, Merkle tree and address-based transactions. Blocks are organized in a way similar to Bitcoin, with block header containing essential parameters such as height, parent hash and Merkle tree root. As for communication, TAUT uses node based, peer-to-peer best-effort broadcast and transaction pool.

The basic unit of TAUT coin is TAUT. It is divisible to 8 decimal places with the smallest unit iTAUT (10^{-8} TAUT). It is the unit used in computer execution.

3. Proof of Transaction

Mining power

We first define window size w and time delay d, both counted in number of blocks. w is the length on which the sum of transactions is taken for competition of a future block. d is the delay after which a transaction can participate mining competition.

Given w and d, for generation of block n, mining power P of an address A is defined as

$$P = \sum_{i=n-d-w}^{n-d-1} (\text{transaction fee paid by } A \text{ in block } i)$$

For every mining address, its effective mining power P_e is

$$P_e = \sum_{\text{Addresses in this club}} P$$

In other words, transaction fee paid between blocks $n-d-w$ and $n-d-1$ determine the mining power on block n. Effective mining power of a mining address is the sum over its transactions.

Transaction is measured by a unit price (TAUT per byte) multiplied by transaction size. Foundation sets a default unit price and market price can go up when demand rises. For security reason, there is an upper bound and a lower bound for mining power gained, depending on transaction size (computer storage space). When transaction fee paid is greater than the upper bound, the mining power accumulated is capped. When transaction fee is lower than lower bound, it will not be accepted.

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, target block time is 60 seconds.
- $R_{max} = 67$ controls the maximum increase of base target.
- $R_{min} = 53$ controls the maximum decrease of base target.
- $\gamma = 0.64$ makes the decrease of base target smoother.

If $I_n > 60$, $T_{b,n} = T_{b,n-1} \times \frac{\min(I_n, R_{max})}{60}$.

If $I_n < 60$, $T_{b,n} = T_{b,n-1} \times (1 - \gamma \frac{60 - \max(I_n, R_{min})}{60})$.

For every mining address, we define target value T as the product of its effective power P_e, 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.

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

Thus, target value T is proportional to the address's effective 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.

$$H = 2^{59} \times \left| \ln \frac{\text{First eight bytes of } (G_{n+1}) + 1}{2^{64}} \right|$$

Under exponential distribution, probability of mining addresses with mining power H_1 and H_2 to generate new block is not affected by merging or splitting.

$$P(H_1) + P(H_2) = P(H_1 + H_2)$$

Block generation and forks

An address can generate the next block when

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

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. 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. Reward distribution

Epoch and reward period

TAUT's blocks are grouped into epochs. Each epoch contains 360 blocks, or approximately 6 hours. At the end of each epoch, a special block called checkpoint is generated. Checkpoints are irreversible when they are at least 1 epoch old. Checkpoints are on the consensus level, i.e. every node running TAUT client agrees on checkpoints.

During our test, we found that frequent mining reward distribution and change in mining power delegation may put a heavy computational burden on nodes. This issue is especially evident when forks occur, since every reversed block is accompanied by mining reward and delegation roll back. With epoch and checkpoint, we set delay in mining power and delegation update as 1 epoch. In Diagram 2, this means transactions made in Epoch A will have their mining power effective starting from Epoch C. The same update point applies to mining power delegation changes that occur in Epoch A. Any roll back will not lead to recalculation of mining power and delegation, which are fixed

after the previous checkpoint. Block rewards are also distributed after 1 epoch. Nodes have the time of one whole epoch (Epoch B in Diagram 2) to update mining power, delegation and reward distribution. Thus, under these rules, temporary forks will not be a computation burden on nodes.

Epoch and checkpoint are TAUT's tool against double spend, which is always possible under POW. If a user receives a large amount of coins, it is advisable to wait after a checkpoint to make sure that the transaction has been confirmed. As checkpoints are irreversible, double spend is impossible beyond checkpoint, even if the attacker has more than 50% of total mining power.

Reward distribution

Block reward comes in the form of total transaction fees contained in the block. For every mined block, the mining address has the right to claim a certain amount. This amount can vary from block to block and cannot exceed total block reward. The mining reward in TAUT is all the trx fee in that block, which all goes to the miner who package the block.

The distribution of block reward takes place after checkpoint of the epoch, as shown in Diagram 2. In other words, reward distribution occurs only when an epoch is considered finalized.

5. Economy and governance

Coin allocation

TAUT Coin as born from TAUcoin testnet of which the total supply of TAU was set at 10 billion. All coins were generated in the genesis block. After the birth of TAUT Coin, a total of 9.3 billion were burned, leaving TAU Testnet (TAUT) with 700 million supply, hence, the name TAUT Coin. Of these (700 million), 82% will be distributed through faucet and bounty program. The remaining 18% is reserved for the TAUT foundation team to support maintenance and future development of TAUT project.

Breakdown

A total of 9.3 billion testnet coins burned to make 700 million left on TAUT.

TAUT are fully distributed without any fiat sales, so you do not need KYC process. You get coins through effort and knowledge, not money. It is fully built, manage and distributed by the decentralized community and a new elected Chairman from the community, TAUT Chairman is elected March each year.

Long term economic effects

We expect some positive long term effect under POT mechanism. The first is that transactions of all kinds are promoted. They not only function normally, but also earn future block rewards. 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.

The third long term effect is an incentive for entities that handles large number of transactions to become mining address on TAUT. These entities, such as cryptocurrency exchange and on-chain merchant, will accumulate large mining power and many customers through normal business. The extra effort to run a full node and become mining address is negligible. Under a perfectly competitive market, it is predicted that these large entities will share a considerable portion of their block rewards with their customers. This means lower exchange fee or commodity price.

The fourth is long-running bounty program that lowers entrance barrier for normal users. In Bitcoin, a new user can obtain coins by mining, which is only feasible without specific hardware in the early stage, or by purchasing coins from exchange. In TAUT, everyone can participate by visiting, talking, referring and building TAUT. Bounty coins will be given to new users. Technical debate and software contribution are especially welcome and mat be rewarded.

6. Products

Mobile Wallet - Mobile Wallet is your true universal, and permission less bank. It stores any of your entire balance and able yo send and receive funds. Private keys are stored decentrally within the wallet and and user is responsible for its safety.
PC Wallet - This is PC Mining Wallet where users get their mining experiences. It can store the entire blockchain, receive and send funds independently. It is tested and based on Linux OS

7. Outlook and debate

In the development of TAUT, we found a lot of interesting problems and challenges, some specific to POT and some generic. We came up with a partial solution or a basic idea for most problems and would like to hear from our community for suggestion and help.

Scalability, space and time

Scalability of space has been a major issue for Bitcoin, as more and more transactions compete for limited block size. Since technology will always bring more bandwidth and shorter network delay, we need adaptive solutions rather than fixed numbers.

Another possible solution is to remove the upper bound for block size and fix target block time. Research has shown that block propagation delay is positively related to block size. Block orphan rate, in turn, is positively related to block propagation delay. Thus, increasing block size means more block reward but higher risk that the block will not be accepted. There will be an equilibrium where a miner maximizes its reward expectation, depending on transaction fee market and network condition. In times of high transaction volume, mining addresses (full nodes) determine their optimal block size.

Another solution is to remove the mining clubs, which now makes 51% attack power accumulation harder to achieve and manipulate. Checkpoints are implemented to avoid long range attack. For short range attack, POT has unique feature, when the chain is older enough to secure more short term power is very hard with limited time.

Abusive transactions

With new POT consensus, TAUT can be susceptible to new types of attacks that are based on manipulation of transactions. Potential abusive transactions fall into two categories: for-profit, whose goal is to maximize profit in future block reward; and for-control, whose goal is to manipulate block generation and control the network regardless of economic gain or loss.

For control attack usually takes the form of controlling more than 50% of total mining power, regardless of cost. This can cause serious problems, including double spend, long range attack to rebuild the chain and transaction censorship. TAUT has periodical checkpoints to solve that.

Permanent fork due to checkpoints

Checkpoint is a good tool to keep network security, but it also comes with cost. When temporary forks occur, they are reconciled by comparing cumulative difficulty. In normal circumstances, forks rarely extend beyond checkpoints, which are at least 360 blocks away. In the event of a fork existing beyond a checkpoint, the fork becomes permanent and the network is partitioned.

Our test showed that this never happened naturally. However, attacker might make permanent forks deliberately. For example, attacker can make a secret chain with greater cumulative difficulty, probably with over 50% total mining power. Just before a checkpoint is to be made, the attacker broadcasts its secret chain to some part of the network. Those nodes who hear this chain before checkpoint will switch to it due to greater cumulative difficulty and those who do not hear it will stick to their original chain. As a result, network is partitioned into two permanent forks that are not compatible after that checkpoint.

Transaction propagation

In most POW and POS blockchain systems, there is little incentive for a node to propagate transactions without a known source. In fact, it is profitable for a mining node not to relay any transaction it receives, since holding a transaction as secret increases the chance for a miner to collect its transaction fee. This is not a major concern for Bitcoin now, as transaction fee only makes up a small portion of block reward. There are thousands of non-mining (or mining with negligible hash power) full nodes that relay transactions, possibly in an altruistic way.

Block reward in TAUT only comes from transaction fee, so there is a stronger incentive for mining nodes to hold transaction they hear as secret, in the hope of collecting its fee. The transaction propagation problem might be a concern for TAUT.

Unpredictability of block generator

In addition to mining power, randomness is also needed to pick the block generator. TAUT's current solution comes from NXT, which uses a series of generation signatures and their hash. In the long term, it is very difficult to predict block generator. However, short term prediction can be very accurate. In particular, if one controls $\frac{1}{M}$ of total mining power, then on average it has a chance of producing k consecutive blocks every M^k blocks.Other address (node(s)) can predict when this is about to happen. This opens door for various attacks such as double spend.

We are in search of better unpredictability for block generators. In theory, we need an entropy source that is unpredictable and can be put under consensus among all nodes. A potential solution is the hash of some previous blocks, preferably before the last check point.

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).