TAU – The Active Unit

An experimental Proof-of-Transaction cryptocurrency

Version 0.3, subject to change

genie854, imorpheus, Constantine Pappas and Zi Ren Teoh

September 2018

Abstract

TAU is an electronic currency that aims to promote essential financial behavior and increase economic circulation. We introduce a new consensus mechanism, Proof-of-transaction (POT), that is fair, secure and environmentally friendly. POT uses on-chain accumulated transaction fee as proof to generate new blocks. The reward is transaction fees contained in each block. Participants can form groups called mining club, which distributes block reward to all club members through an efficient club wiring transaction. Under POT, network security is maintained collectively by users' transactions.

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

Announcement thread: https://bitcointalk.org/index.php?topic=4757879

Bounty debate thread: https://bitcointalk.org/index.php?topic=4907712

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.

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.

Despite these issues, both have been able to build large coin ecosystems that are considered secure and trustworthy. It is our belief that we have created a new way of accomplishing an equal level of security without any of the mentioned drawbacks.

2. TAU overview

The first and most important contribution of TAU 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 TAU is still called mining like Bitcoin, but block reward only comes in the form of transaction fee. All tokens 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. See Chapter 4 for details.

The second improvement is that TAU supports signal transaction, a special transaction that establishes a predefined relation over the network. It can be used for on-chain voting and 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 TAU is club wiring, a single transaction that distributes mining reward to all mining club members. This removes the transaction overload for mining reward distribution. Both mining club and club wiring make the process of mining more convenient. See Chapter 3 for details.

Inspired by NXT and NEM, TAU 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, TAU 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, TAU uses node based, peer-to-peer best-effort broadcast and transaction pool.

3. Mining club

Signal transaction

Mining power of an address is determined by the number of historical transaction fees paid (details in Chapter 4). Every address can delegate its mining power to another address through a special type of transaction, called signal transaction, where the amount transferred is zero. When address A transfers zero token to address B, it means that A has delegated its mining power to B. When address A makes a zero transfer to itself, it resets the mining power to itself.

Mining power delegation is transitive, which means if A delegates to B and B delegates to C then A delegates to C. Delegation is permanent until a new signal transaction is confirmed. By default, when an address receives token for the first time on chain, its mining power is delegated to the address those tokens come from. When an address with an already declared delegation receives token from other address, nothing will change. The only exception is the addresses in the genesis block, which retain mining power by themselves.

In addition to on-chain delegation, signal transaction can also be used to voting. This is done by setting a

pre-defined section in each block to a certain value. It is planned that major rule change for TAU will be voted on-chain before any hard fork.

Mining club and club wiring

Mining power delegation can be represented by a directed graph, where each connected component is called a mining club. In each club, its leader mines by itself and other members delegate their mining power to the leader. See Diagram 1 for example.

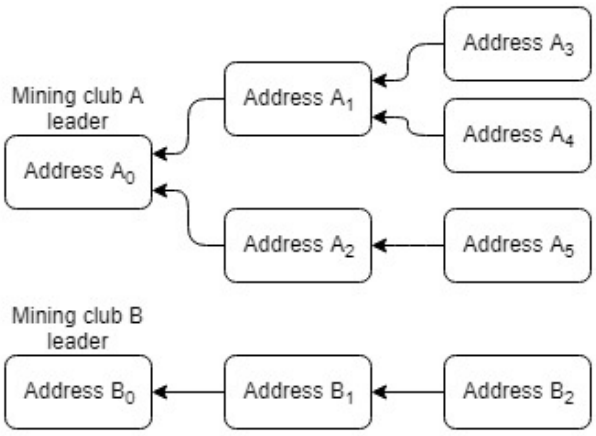

Diagram 1 Mining club example

Arrow means mining power delegation. The first mining club has leader A_0 and members A_1, A_2, A_3, A_4, A_5. The second has leader B_0 and members B_1, B_2, B_3. Note that one entity may own multiple addresses.

Mining club lowers the entrance barrier by removing the burden of running a full node, collecting new transactions and always on-line communication with peer nodes. In mining club, leader carries the responsibilities of hardware and communication. Compared with mining pool in Bitcoin, TAU's mining club is a virtual organization on the network. It is also expected to be more decentralized than Bitcoin, as hardware entrance barrier is much lower.

When a block is successfully mined by a club, its reward goes into the club leader's address. The leader chooses how much reward to distribute to its members. To avoid overload of reward distribution transactions, TAU has a special transaction, called club wiring. A certain amount of reward is declared by club leader for itself. The remainder goes to all club members automatically, in proportion to their share of mining power. Club leaders are free to choose what percentage they retain, so there is risk that greedy leaders may take most or all of the block reward. However, every user is free to choose which mining club to join. Therefore, market competition will bring an equilibrium between mining club leaders, who charge a certain percentage of reward, and club members, who contribute their mining power.

4. 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 club, 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 club is the sum over its members.

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 value T_b controls the average block interval time. The greater the base target, the faster (more easily) the next block is generated. It is adjusted by the product of the previous block's base target and the average time required to generate the previous three blocks.

- T_p is the base target of previous block.

- I is the average time interval of the previous three blocks.
- $R_{max} = 67$ 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.
- In our first version, target block interval time will be 60 seconds.

If $I > 60$, $T_b = T_p \times \frac{\min(I, R_{max})}{60}$.

If $I < 60$, $T_b = T_p - T_p \times \gamma \times \frac{60 - \max(I, R_{min})}{60}$.

For every mining club, we define target value T as the product of its effective power P_e, base target value T_b and a time counter C. This counter is the time in seconds elapsed since the timestamp of the previous block.

$$T = T_b \times P_e \times C$$

Thus, target value T is proportional to the club'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 clubs 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

$$H < T = T_b \times P_e \times C$$

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. 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.

Potential attacks

There are many attacks that can be attempted on blockchain. We would like to discuss a few potential threats to TAU.

Both POW and POS are subject to 51% attack, where nodes with more than half computing power or stake choose to start a secret but better fork and revert some blocks. POT is not immune to this attack, but the power is now determined by cumulative transaction fee paid in a pre-set history window. A combined total of more than half of entire historical transaction fee can lead to 51% attack. To make 51% attack harder, TAU sets window size to one year and sets upper bound for mining power gained per transaction. TAU's governance is also community lead, which means in the rare case of a successful 51% attack, community voting can over overthrow the attack via a hard fork.

Nothing-at-stake attack, where a node keeps record of every fork it receives due to almost zero cost, is common under POS consensus. Like NXT, TAU's cumulative difficulty discourages this attack, since keeping forks with low cumulative difficulty carries no benefit.

Mining power depends on historical transaction fees and carries a future reward. Thus, speculators might want to make speculative transactions between their addresses in the hope that they will make a future profit through block reward. To stop these abusive transactions, we plan to implement reward clipping, an algorithm that caps the reward for each transaction fee paid. When future reward is capped by current fee paid, there is essentially no room for speculation.

Another POT-specific attack is the selfish cherry-pick of transactions by mining club leaders. Under POT mechanism, they can decide which transactions to include in the new block. They are incentivized to select or ignore transactions as they see favorable. In this process, club leader gains individually at the cost of current block reward for all of its club members. For example, club leader can choose to ignore any signal transaction that is made to leave the club or include any signal transaction that joins the club, regardless of transaction fee paid. We propose to resolve this by largely depending on mining club market competition and third party ranking services.

5. Economy and governance

Token allocation

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

The total supply of TAU is set at 10 billion. All tokens will be generated in the genesis block. Of these, 74% will be allocated to ICO funding to promote initial distribution. 18% is reserved for the foundation team to support development and maintenance of TAU project. 8% will go to bounty programs for testers and initial participants.

Governance

In blockchain world, governance is needed mainly in three areas: on-chain consensus, new project (bug fix and feature upgrade), and funding (for developers). While on-chain consensus has been covered by software, project and fund governance involves coordination among stakeholders, such as end users, on-chain businesses, full nodes (mining club leaders) and developers. The common goal of all stakeholders is secure and efficient value exchange over the blockchain. Major changes will be voted on-chain and be implemented if it gets majority support. These include change of consensus rule or key network parameters, such as block time/size, transaction fee bound and reward clipping threshold.

TAU will apply a loose coupling method for project and fund governance. Community discussion among all stakeholders is the key step to decide any rule change, including hard forks. When some new rule takes effect, full nodes and end users can choose whether to follow. In case of a serious attack, community has the right to stop and punish the attacker through a hard fork. Developers are incentivized by funds from the foundation and future reward clipping (see Chapter 6). Anyone, whether a member of the foundation, is welcome to participate.

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 tokens 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 club leader on TAU. 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 club leader 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 TAU, everyone can participate by visiting, talking, referring and building TAU. Bounty tokens will be given to new users. Technical debate and software contribution are especially welcome and will be rewarded decently.

6. Outlook and debate

In the development of TAU, 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. One possible solution is to fix the block size upper bound and make target block time an adaptive variable. In times of low transaction volume, actually block size is lower than the bound and blocks are generated, on average, at intervals determined by target time. In times of high transaction volume, a block can be generated as soon as its size reaches the limit, regardless of target time. Due to propagation issue, there still needs to be a lower bound for block time, but it can be much lower than target time.

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 club leaders (full nodes) determine their optimal block size.

Long confirmation time is another major problem for blockchain implementation. Our planned solution is a two-step block generation method. The generation of a new block can be separated into transaction confirmation step, where a selected node verifies and signs every transaction he receives, and block generation step, where the next selected node assembles all transactions signed by the first node and signs the whole block. Transactions with low amount can be considered as confirmed in the first step, thus greatly reducing confirmation time. Larger transactions may need more time, sometimes after several blocks, to be considered secure.

Abusive transactions

With new POT consensus, TAU 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.

As discussed in Chapter 4, reward clipping can thwart for-profit abusive transactions. If future block reward is bounded by current block transaction fee, there will be no room for any for-profit abusive transactions. The clipped reward can be redistributed into the network through several possible ways, including lottery, redistribution to club members, or burn.

To prevent for-control transactions, we currently rely on the relatively long window size (one year). More methods are planned for the future, such as regular check points and transaction hash ink, which requires every transaction to include a recent block hash.

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 TAU 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 TAU.

Accounting model

In the development of TAU, we faced a choice between UTXO and account based model. The former is better for privacy and data compression. The latter is simpler and more efficient in some application, including TAU's club wiring reward transaction. We decided to use an address based model with balance. It is an approach that keeps privacy and conveniently supports club wiring transactions. The burden of calculation and record keeping shifts to the full nodes, which we believe is small. However, a better solution is possible, which lowers requirement for a full node.

Unpredictability of block generator

In addition to mining power, randomness is also needed to pick the block generator. TAU'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 club controls $\frac{1}{M}$ of total mining power, then on average it has a chance of producing k consecutive blocks every M^k blocks. Its club leader 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).