TAU – The Active Unit

An experimental Proof-of-Transaction cryptocurrency

Version 0.4, subject to change

genie854, imorpheus, Constantine Pappas and Zi Ren Teoh

October 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 fast, 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. TAU supports signal transaction, applicable in on-chain delegation. Participants can form groups called mining club, which distributes block reward to all members through an efficient club wiring transaction. Under POT, network security is maintained collectively by users' transactions, and further enhanced by epoch rotation and checkpoints.

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. 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 TAU that accomplishes the above goals without the loss of security.

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 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 TAU 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 TAU 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. Mining on mobile phones, as we estimate, has been made possible on TAU.

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.

The basic unit of TAU coin 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.

3. Signal transaction

Signal transaction and channel

TAU supports a special type of transaction, called signal transaction, where the amount transferred is below a very small amount. This threshold is set as 100 iTAU for now. It is expected that such small amount will be much lower than transaction fee, therefore giving these transactions special meaning will not affect normal transactions on TAU.

Any amount between 0 and 99 iTAU is given a special meaning, which yields 100 signal channels in total. They are called signal channel 0 to 99. When a

certain amount between 0 and 99 iTAU is transferred, a special on-chain relation is established. Like normal transactions, transaction fee is needed for signal transactions to be included into a block. This fee is main cost of signal transaction, as the actual amount transferred is usually negligible.

Mining power delegation

For now, on-chain delegation is the most important application of signal transaction. Delegation is the transfer of right from one address to another on the chain. It is permanent until a new signal transaction is made and confirmed. To reset the right to itself, an address makes a signal transaction from and to itself. Delegation is transitive, which means if A delegates its right to B and B delegates to C then A delegates to C. The relationship of delegation can be represented by a directed graph. Each connected component of this graph is a rooted directed graph.

In mining power delegation, every address can delegate its mining power to another address through signal channel 0. By default, when an address receives coin for the first time on chain, its mining power is delegated to the address those coins come from. When an address with an already declared delegation receives coin from other address, nothing will change. The only exception is the addresses in the genesis block, which retain mining power by themselves.

Mining power delegation generates a relation graph, where each connected component is called a mining club. In each club, the root address is called its club leader. Club leader mines by itself and other club members delegate their mining power to the leader. See Diagram 1 for example.

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, whose relationship is kept and can be verified on-chain. It is also expected to be more decentralized than Bitcoin, as hardware entrance barrier is much lower.

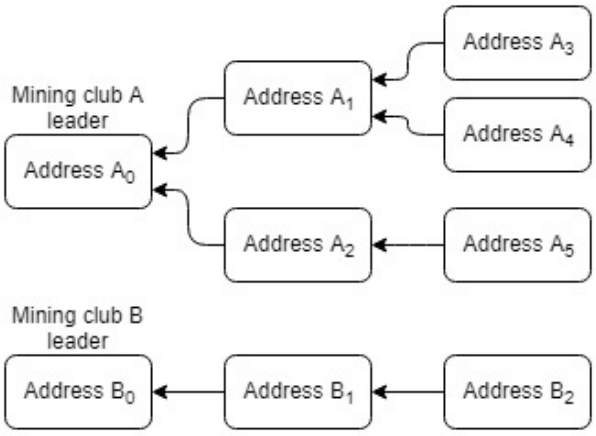

Diagram 1 Mining club example

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.

4. Proof of Transaction

Mining power

We first define window size w and time delay d, both counted in number of blocks, or group 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.

Transaction is measured by a unit price (TAU 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 club, 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 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

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

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. 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.

5. Epoch and reward distribution

Epoch and checkpoint

TAU'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 TAU client agrees on checkpoints. See Diagram 2 for example.

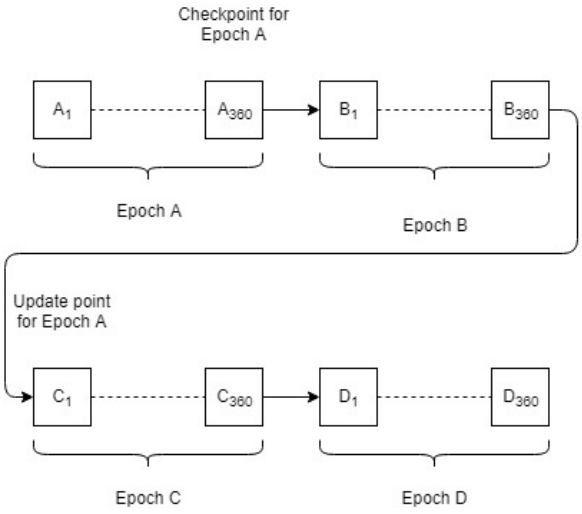

Diagram 2 Epochs in TAU

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 TAU'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 period is all the blocks in w (window size) consecutive epochs. It is a moving window that determines mining power after d (delay) epochs. For our current test, we fix window size $w = 1000$ epochs and delay $d = 1$ epoch.

Reward distribution

POT's use of transaction fee as mining power, while incentivizing currency circulation, opens way for abusive transactions. For example, users can make "meaningless" transactions, which do not come from economic need for trade. Instead, these for-profit transactions are made in the hope that future transaction fee will go up, so that future reward is greater than current transaction fee paid. To stop these for-profit abusive transactions, we introduce reward clipping.

For each address and fixed reward period, at an update point, we have the following variables.

- P is the mining power, based on cumulative transaction fees paid.
- R_u is the unadjusted reward to be distributed in the last epoch of the reward period. It is in linear proportion to mining power contributed in the epoch.
- R_a is the adjusted reward to be distributed in the last epoch of the reward period.
- CR_u is the cumulative unadjusted reward in the entire reward period before last epoch.
- CR_a is the cumulative adjusted reward in the entire reward period before last epoch.

Adjusted new reward from last confirmed epoch is

$$R_a = P \times (e^{-\frac{CR_u}{P}} - e^{-\frac{CR_u + R_u}{P}})$$

The adjusted reward increases as unadjusted reward increases, but its growth rate decreases exponentially. When transaction fee market is at equilibrium (steady flow of transactions paying equal fees), expected return for transaction fee paid is $1 - e^{-1} \approx 63.2\%$. Under this rule, cumulative adjusted reward CR_a for any address at any time cannot exceed its mining power. This means that there is no room for profit from block reward by making abusive transactions.

TAU has a fixed supply of tokens, all generated in the genesis block. The next step is to redistribute the clipped reward so that total supply of tokens does not change. We create a reward pool to "store" the clipped reward, also serving as incentive for mining club leaders. The balance of reward pool is written in the header of every block, making it part of TAU consensus. Reward pool is updated at the same time as reward clipping. It has the following income and expense.

- Income from reward clipping.
- Block reward for mining club leaders, called miner's reward.
- Initial funding.

For each update point, block rewards are equally given to all blocks generated in the last confirmed epoch. For each mining club leader, miner's reward

$$R_m = \frac{\text{Clipped reward}}{360} \times (\text{blocks mined})$$

Assume that transaction fee rate is 0.001 TAU per byte and blocks are 50% full, we have 184 TAU clipped reward when transaction fee market is at equilibrium. To stabilize miner's reward, we set upper and lower bounds as 200 and 50 TAU, respectively. The lower bound can further be adjusted when the reward pool runs low.

An alternative distribution method is to let mining club leader decide how much they take from each block. For every mined block, the mining club leader has the right to claim a certain amount. This amount can vary from block to block and cannot exceed total block reward. The remainder goes to all addresses that is a member of a certain mining club.

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.

Epoch rotation

Transaction censorship can be carried out by a super power that controls over 50% of total mining power. The super power can, while the network is under its control, make arbitrary decision on which transactions to be included in blocks. This can lead to serious security problems. For example, one's balance can be essentially nullified since there is no way to use it.

As a public blockchain, TAU fights against such risk by epoch rotation. After each epoch, every address that participates in generating blocks in this epoch goes into a cooldown period, during which its mining power is temporarily set to zero. The cooldown period is measured in epochs. If it is set as n epochs, then honest mining power only needs $\frac{1}{n+2}$ of total mining power to fight against a super power. For example, if super power controls 90% of total power, then honest power that controls 10% may lose to super power in 9 consecutive epochs but not more. In this case, setting $n = 9$ gives honest users chance to win at least 1 epoch out of 10.

Epoch rotation gives honest minority power on the chain a chance to "rebel" against a super power attack. In traditional POW mechanism, when a super power takes control of the network with over 50% power, it can ignore any block generated by the minority power and make arbitrary transaction censorship. This essentially kicks minority power and many users' assets out of the network. With epoch rotation, even 10% minority power has a chance to "rebel" in one epoch, if cooldown period $n \geq 8$.

6. 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 TAU-X program and bounty program. The remaining 18% is reserved for the TAU foundation team to support maintenance and future development of TAU project.

TAU-X is a coin swapping program between BTC pool and TAU pool that makes a swap every epoch (360 blocks). Everyone can freely put BTC or TAU into respective pool to receive opposite coin. In each swap, 60,000 TAU (out of the 82% part) go into the pool and community can put much more to obtain available BTC. TAU-X program increases liquidity for existing TAU coin holders and provides a fair option for BTC holders.

TAU bounty program gives rewards to participants who visit, refer, talk or build TAU. It is a convenient approach for common users to join and get familiar with TAU. Coins received through bounty program are free to enter TAU-X.

Under reward clipping rules, reward pool circulates clipped block reward to mining club leaders, who get a fixed reward (during each epoch) for each block generated. Thus, they are incentivized to attract more members to join, so that one's club has more mining power and generates more blocks.

Stakeholders in TAU include users, miners (mining club leaders) and developers. Their relation and incentives are shown in Diagram 3.

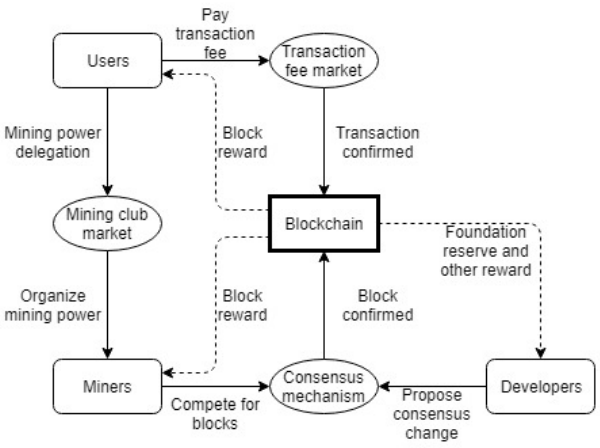

Diagram 3 Economy in TAU

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 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 distribution.

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. Everyone 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 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 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 coins will be given to new users. Technical debate and software contribution are especially welcome and will be rewarded decently.

7. 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. Research has shown that "hand over" time, required when one block generating node relays its right to the next block generator, is a major source for network delay. Therefore, one possible solution is to let one node generate more than one blocks in consecutively when transaction volume is high. This has been applied in Byzantine Fault Tolerance (BFT) solutions such as EOS. But more research is needed for public chain where BFT solution is not possible.

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.

With reward clipping, it is impossible for any address to receive more reward than its total transaction fee paid. Therefore, abusive for-profit transactions cannot make profit unless they are subsidized by external payoff, such as "bribery" from mining club leader.

For control attack usually takes the form of controlling more than 50% of total mining power. This can cause serious problems, such as transaction censorship and block denial. TAU uses epoch rotation to fight against transaction censorship.

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 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.

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 checkpoint.

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).