Nexus Proof-of-Stake with Tritium Trust

Colin Cantrell Scott Simon

October 3, 2018

1 Introduction

The Nexus network operates using three channels for producing valid blocks and minting new NXS currency – two Proof-of-Work channels and one Proof-of-Stake channel. The original Proof-of-Stake channel introduced the concept of trust as a core component to measure consistent and honest contribution by a node to the Nexus network. It followed the philosophy of "everyone has time" in rewarding people for their time investment.

With the release of Tritium Trust, this trust system is revised and enhanced. Through it, Nexus has improved its Proof-of-Stake channel for future growth and laid the groundwork for the development of a Trust and Reputation system as well as Trust Locks in future releases of the TAO framework.[1]

This paper discusses the updates in the Tritium Trust release with respect to how they affect Nexus Proof-of-Stake.

2 Proof-of-Stake

2.1 What is Proof-of-Stake?

The concept of Proof-of-Stake was first introduced in 2012 by King & Nadal[2] as a proposal to develop a form of mining that addressed the growing issue of energy consumption related to Bitcoin Proof-of-Work mining. It developed the idea of using proof of ownership of a currency as a means for granting the ability to mine blocks on the blockchain. These blocks would include a *coinstake* transaction that rewarded the currency owner in a manner similar to how *coinbase*[3] transactions reward Proof-of-Work miners.

Early incarnations of Proof-of-Stake built around the idea of *coin age*, defined as a measure of the holding period for the currency. Upon reaching a specified coin age, the currency owner would gain the ability to stake a new block on the blockchain.

[1] see "The Nexus Three Dimensional Chain Simplified" by gjsteele71
`https://steemit.com/bitcoin/@gjsteele71/the-nexus-three-dimensional-chain-simplified`

[2] King, S.; Nadal, S. (August 12, 2012). "PPCoin: Peer-to-peer crypto-currency with proof-of-stake" `https://peercoin.net/assets/paper/peercoin-paper.pdf`

[3] A coinbase transaction is included in each Proof-of-Work block to pay the mining reward to the miner who found the block. Not to be confused with the Coinbase exchange.

This design elegantly solved the issue of energy efficiency, but had the drawback that, unlike other forms of mining, the currency owner didn't have to do anything. They could simply leave their wallet off, and only activate it upon reaching the age level needed to earn rewards without contributing to the network as a whole.

As a result, Proof-of-Stake was gradually refined. It remained a form of energy efficient mining, but evolved into a mechanism whereby currency holders can earn rewards proportional to the size of their holdings in return for keeping a node up and running at all (or nearly all) times, thus contributing to the operation and security of the blockchain network.

2.1.1 Staking Concepts

Time
Proof-of-Stake introduced time as an input to mining, initially through the use of coin age. Using time in this manner inhibits the application of raw computational power to solve blocks more quickly, thus promoting energy efficiency. Requiring a significant time investment also introduces an external cost to staking that improves network security.

Weight
Different Proof-of-Stake systems use varying ideas for the concept of weight. Basically, all of these introduce an approach where the ability of currency owners is weighted in such a manner that some have a higher chance to generate blocks than others. Coin age based systems were often weighted based on the number of coins owned, so if two people had the same holding period, but one had twice as many coins as the other, that one would have twice as much opportunity to generate staking blocks.

Minting Rate
This rate, expressed as a percentage, is used to calculate the size of the coinstake reward in a Proof-of-Stake block. Over time, it has become commonly referred to as *interest rate* because it operates in a similar manner and people already have an understanding of that term. However, anyone staking should understand that their coins are not actually earning interest. They are mining staking rewards in return for helping operate and secure the blockchain network.

Distribution Problem
A pure Proof-of-Stake based currency suffers from a chicken-and-egg problem that you cannot create staking blocks unless you first have coins to stake. Therefore, most currencies that use Proof-of-Stake also employ an initial distribution based on Proof-of-Work mining, at least temporarily.

Nexus has realized the value of this type of multi-channel system as it relates to network security, and uses 3 minting channels, two based on Proof-of-Work and one based on Proof-of-Stake. As a byproduct, this system also supports initial distribution via the Proof-of-Work channels.

Nothing At Stake Problem
Proof-of-Work mining requires the consumption of large amounts of energy, which is a valuable resource. A basic Proof-of-Stake system, on the other hand, only uses resources already within the network, and you don't lose anything for behaving dishonestly or signing all blocks on any fork in the chain, then attempting to build on all forks. There is no cost or "nothing at stake" for doing so. It is a hypothetical problem that nevertheless must be addressed by any staking system.

In addition to other benefits, the use of multiple channels in Nexus also addresses this problem, as the disparate channels keep each other honest. The Nexus network also uses the concept of trust to create a cost to misbehavior.

51% Attack
As with other forms of mining, Proof-of-Stake systems can potentially be exposed to a 51% attack that gives the attacker control of the network. Under this type of system, however, it requires an attacker to gain control of at least 51% of the currency on the network. This becomes incredibly expensive to do, and thus highly unlikely, especially when you add limitations to block frequency and combine it with a significant time requirement for generating staking weight.

Within Nexus, not only is it highly unlikely a 51% attack could occur on the Proof-of-Stake channel, but an attacker would also have to gain control of both Proof-of-Work channels to be successful.

Inflation
Defining the minting rate is an important aspect of any staking system. Too low and rewards are not significant enough to encourage nodes to stake. Too high and the resulting inflation of the currency supply will erode its value, especially when compounded over time. Inflation can rapidly become the nemesis for systems promising excessively high rewards.

The Nexus initial distribution will create a supply of 78 million NXS, ending on September 23, 2024. After that, it will follow an inflationary model based on the annual inflation of gold supply from mining. Gold has kept its value for centuries, so this level of inflation has proven economically sustainable.

Under this model, each Proof-of-Work channel will inflate supply by 1% per year, and the Proof-of-Stake channel will allow a maximum of 3%. This 3% value could only be realized if the entire NXS supply were staked at the maximum Interest Rate. Realistically, Proof-of-Stake inflation will likely fall in line with the 1% on the other two minting channels.

3 Nexus Proof-of-Stake

The Tritium Trust release builds on the previous Nexus Proof-of-Stake system. It employs many of the staking concepts developed in previous staking systems, enhances them, and adds new concepts that further enhance performance and security for Proof-of-Stake.

3.1 Genesis

Before a new wallet can stake successfully on the Nexus network, it must first create a trust key. This key is created by successfully mining its first Proof-of-Stake block, a process referred to as Genesis. The initial coinstake transaction is thus the Genesis transaction.

While staking for Genesis, the node will slowly build Trust Weight. Over time, this increases the chances of generating a Genesis transaction. The pre-Genesis value for trust only applies to the Genesis process and is based on coin age. It caps at a level of 11% of maximum, as shown in Figure 1.

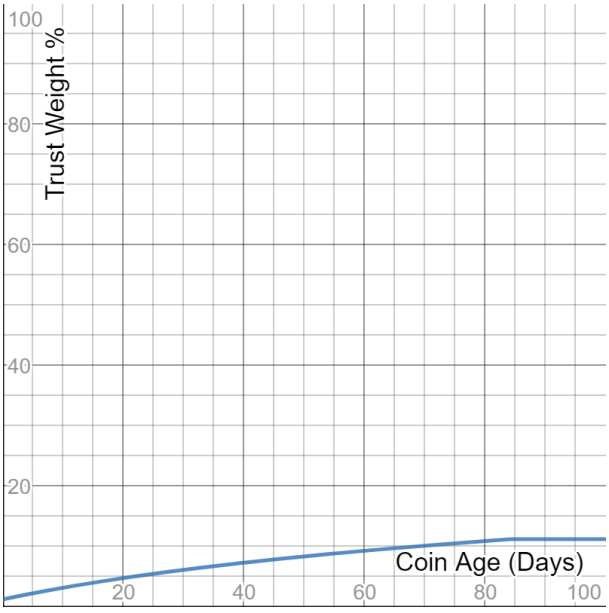

Figure 1: Trust Weight pre-Genesis

When the Genesis transaction is created, the wallet also creates the trust key and transfers all balance to that key for staking. This has no impact on the wallet balance, besides moving it to the new key.

Under Tritium Trust, each wallet will only perform Genesis once. After it creates a trust key, it will continue to use it for the remainder of the lifetime of that wallet.

3.2 Trust

Upon creating a new trust key, the network immediately begins to build trust on that key. Continued staking will generate additional Trust transactions whenever the node successfully mines a Proof-of-Stake block. Each of these rewards the wallet owner for continuing to operate their node.

As with the Genesis transaction, Trust transactions will also transfer any new NXS sent to the wallet onto the trust key for staking.

Trust is measured by the key's trust score, which initially equals the age of the trust key. As long as the key does not undergo Decay (see section 3.5) or get penalized for misbehavior, trust score will continue to grow in this manner.

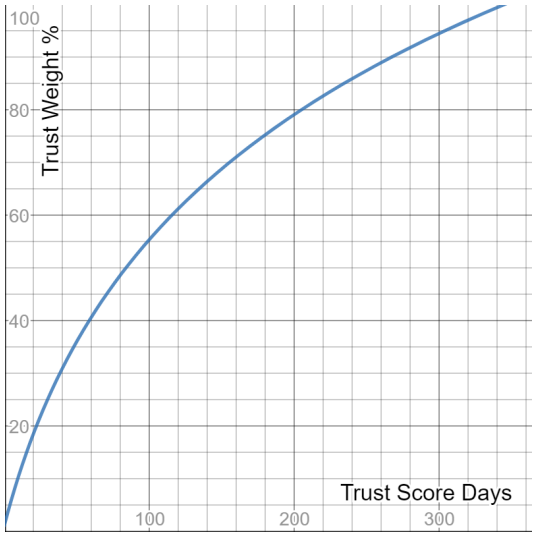

Figure 2: Trust Weight

The trust score reflects the network's level of trust in the node as a measure of the time it has been operating and producing new blocks in an honest, trustworthy, and timely manner. The significant investment in time needed to build trust score enhances the security of the overall network.

The trust score is used to calculate Trust Weight. Increased Trust Weight improves the chances of successfully staking a new block.

Figure 2 depicts how Trust Weight, expressed as a percentage of maximum value, grows as accrued trust score, expressed as days of time, increases.

3.3 Interest Rate

The size of each staking reward is based on the current interest rate (minting rate) for the wallet's trust key. The Genesis process uses a fixed rate of 0.5% (annual). After Genesis, future Trust transactions use an interest rate derived from the trust score.

This annual interest rate ranges from the starting rate of 0.5% to a maximum of 3.0% after the trust key has accrued one year worth of aggregate trust score.

Figure 3 depicts how Interest Rate, expressed as an annual percentage, grows

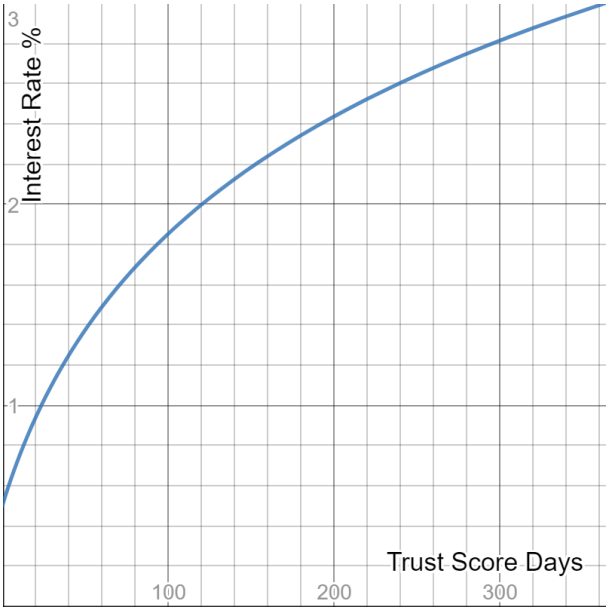

Figure 3: Interest Rate

as accrued trust score, expressed in days of time, increases. Interest Rate caps when it reaches the maximum value of 3%.

3.4 Block Weight

To continue accruing trust score, a wallet must successfully generate a new Trust transaction within a three day time requirement. The use of Block Weight serves two functions in this respect.

First, it acts as a timer. When Block Weight reaches 100%, the trust key will begin to undergo Decay (see section 3.5).

Second, a higher value for Block Weight slightly increases the chances of staking a block. Thus, as it gets closer to the three day time limit, chances to generate the required Trust transaction increase.

Figure 4 depicts how Block Weight, expressed as a percentage of maximum value, grows over three days of time.

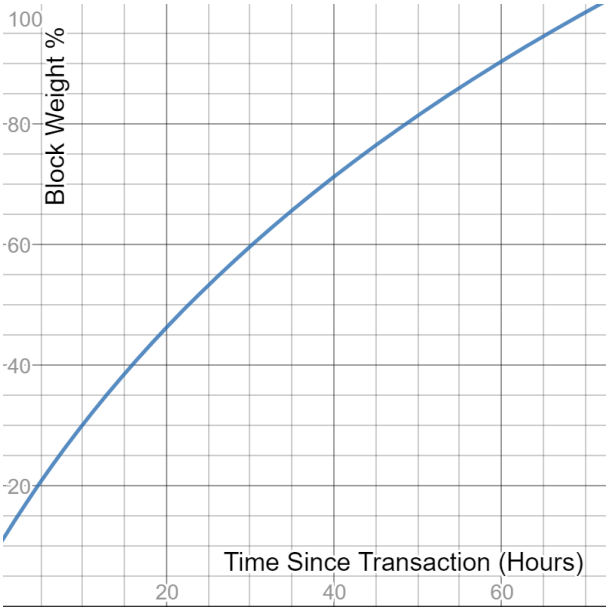

Figure 4: Block Weight

3.5 Decay

Tritium Trust introduces the process of Decay if staking fails to generate a Trust transaction within the required time limit. The trust key does not expire. Instead, it will reset back to the level of its previous Trust transaction, and begin to decay from that point. Trust score decays at a 3:1 ratio to the rate it was earned.

$$T_s = T_p - 3 \cdot (B_t - 259200) \tag{1}$$

Where T_s = new trust score, T_p = prior trust score at last transaction, B_t = time since last stake block, and 259200 is three days expressed in seconds.

Normally, Trust Weight depicted in Figure 2 moves forward along the curve as trust score grows. During Decay, you can think about it as moving backwards along the same curve. The same would be true of Interest Rate in Figure 3.

If, at any time, the wallet finds a new stake block and generates a Trust transaction, Block Weight is reset, Decay ends, and trust score begins accruing again from that point.

The benefit of Decay in Tritium Trust is that trust keys no longer expire. They simply add or subtract trust score. Those who have invested a lot of time staking a trust key won't have that key expire as the result of a random event such as a power outage. Trust might decay somewhat, but that can be earned back.

The time investment that it takes to build trust score, combined with this introduction of the ability to both add and subtract trust score, also supports administration of trust penalties for misbehavior or dishonesty, and forms the basis for future application as part of a Trust and Reputation system within the Nexus TAO framework.

3.6 Use of Coin Age in Nexus

Enough different Proof-of-Stake systems have used coin age in different ways that it becomes a matter of confusion. While this document already shows coin age in the places where Nexus uses it, summing this up in one section will clarify it better.

Nexus primarily uses coin age only during the Genesis process. It determines the minimum time to wait before you can stake new balance. It also determines Trust Weight and the reward included in the Genesis transaction.

After Genesis, Tritium Trust only uses trust score and block age (time since last staking transaction) for staking, with one exception. It uses coin age when you add new balance to your wallet, and then only when calculating the portion of the staking reward from that new balance. In this manner, you only earn rewards on new balance for the time after adding it to the wallet.

Other than that, the Trust process uses the full current wallet balance when attempting to find staking blocks, including any new balance. Balance changes also have no impact on your trust score.

4 Beginning Staking with a New Wallet

4.1 Establishing a Trust Key

Trust is not something easily earned in real life. Nor is it easily established in Nexus Proof-of-Stake. Establishing a new trust key is a process. This process can take some time, especially when staking with smaller balances.

After Genesis, Trust Weight is low and transactions less frequent. It is normal that a new key might not create a Trust transaction within the required three day period. As the key is new, Decay immediately reduces trust score to its starting value (the trust level of its prior transaction) when Block Weight reaches 100%.

From that point, Block Weight will stay at 100%, while Trust Weight and Interest Rate stay at minimum starting values (1.11% and 0.5% respectively). These values will not change until the node finds a staking block and generates a Trust transaction. Then, trust score begins to grow again.

This cycle may repeat multiple times before a new key can generate enough Trust transactions to keep growing. This is normal. It is all part of earning trust.

4.2 Nexus Staking Requirements

Minimum Balance
No matter how much NXS you have, you can operate a node and stake your balance. There is no minimum amount required. You are guaranteed to receive at least the starting 0.5% Interest Rate for any balance amount. However, if you have higher balance, you will receive Trust transactions more frequently, and have a higher likelihood of growing trust score and Interest Rate to higher levels.

Minimum Coin Age
The Genesis process requires a minimum coin age of 72 hours before allowing the wallet to stake. A new wallet that just received its first NXS must wait this long to begin staking. Any sending or receiving of balance affects coin age, also, which may impact the ability to start staking.

Hardware
You can stake NXS on any system supported by the latest Nexus wallet version. Currently, that includes computers running 64-bit versions of Windows, MacOS, or Linux. Devices such as mobile phones or Raspberry Pi are not yet supported. The staking process does not require a high powered machine, though. Many use older laptops or mini-systems like the Intel NUC to minimize power usage.

Maturity
Staking is a form of mining and, as with Proof-of-Work, must wait a minimum period for a staking transaction to mature. For Nexus, maturity takes 120 blocks (around 90 minutes). During this time, the wallet balance will not be available for other use.

Three Day Requirement
As previously noted, a wallet must successfully generate a new Trust transaction within three days of its prior one. If not, the trust score will experience Decay.

5 Technicals

This section specifies how Tritium Trust revises and replaces the technical details originally published in the Nexus white paper.[4]

5.1 Trust Weight

Nexus Proof-of-Stake uses two distinct calculations to determine current Trust Weight, one based on coin age during the Genesis process and one based on current trust score for the remainder of staking.

The numeric value of Trust Weight ranges from 1 to 90, although it is commonly expressed as a percentage of its maximum value.

[4]Nexus: A Peer-to-Peer Network `https://nexusearth.com/nexus-white-paper/`

Pre-Genesis Trust Weight

$$W_t = Min(10.0, \frac{9.0 \cdot ln(\frac{2 \cdot a_c}{7257600} + 1)}{ln(3)} + 1.0) \tag{2}$$

Where a_c is the current coin age.

Staking Trust Weight

$$W_t = Min(90.0, \frac{44.0 \cdot ln(\frac{2 \cdot T_s}{7257600} + 1)}{ln(3)} + 1.0) \tag{3}$$

Where T_s is the current trust score.

5.2 Interest Rate

For the Genesis transaction, the staking reward is calculated using the starting interest rate of 0.5%. Trust transactions use the current interest rate calculated from accumulated trust score.

$$R_m = \frac{0.025 \cdot ln(\frac{9 \cdot T_s}{31449600} + 1)}{ln(10)} + 0.005 \tag{4}$$

Where T_s is the current trust score and R_m is the resulting minting rate (interest rate).

5.3 Staking Rewards

Genesis Transaction

$$S_r = \frac{C_w \cdot 0.005 \cdot a_c}{31449600} \tag{5}$$

Where C_w is the current wallet balance and S_r is the staking reward.

Trust Transaction
The Trust reward has two possible components. The first part is the reward for balance staked on the trust key, based on the block age (time since last staking transaction). The second part accounts for any new balance added

to the wallet. This balance only earns rewards for the time since adding it.

$$S_t = \frac{C_t \cdot R_m \cdot a_b}{31449600} \tag{6}$$

Where C_t is the trust key balance, a_b is the block age, and S_t is the staking reward from the trust key.

$$S_n = \frac{C_n \cdot R_m \cdot a_c}{31449600} \tag{7}$$

Where C_n is any new balance added to the wallet, a_c is the coin age of that new balance, and S_n is the staking reward from any new balance. This balance is then transferred to the trust key for further staking.

The total reward for a trust transaction $S_r = S_t + S_n$

5.4 Block Weight

The Genesis process does not use Block Weight and its value remains zero. After Genesis, the numeric value of Block Weight ranges from 1 to 10, although it is commonly expressed as a percentage of its maximum value.

$$W_b = Min(10.0, \frac{9.0 \cdot ln(\frac{2 \cdot a_b}{259200} + 1)}{ln(3)} + 1.0) \tag{8}$$

5.5 Stake Weight

Stake Weight is a derivative measure that depicts the combined effect of Trust Weight and Block Weight on overall chances to generate a block. The Required Threshold (see Section 5.6) uses Trust Weight and Block Weight directly, so the value of Stake Weight is for informative purposes only.

$$W_s = W_t + W_b \tag{9}$$

As shown previously, absolute values for Trust Weight range from 1-90 and Block Weight from 1-10. Thus, Stake Weight will range from 2-100, and can be directly expressed as a percentage.

5.6 Required Threshold

$$R_t = \frac{(108 - W_t - W_b) \cdot 1000}{(C_w + S_r)} \tag{10}$$

The value for Energy Efficiency Threshold must be above this value for the wallet to attempt stake block generation.

5.7 Energy Efficiency Threshold

$$E_t = \frac{100 \cdot t_b}{N_{once}} \tag{11}$$

Where t_b is the time since the last block was added to the blockchain, in seconds.

The Nexus stake minter will iterate over the process of attempting to find a block hash that meets staking difficulty requirements, incrementing N_{once} with each iteration. Whenever this causes the value for the Energy Efficiency Threshold to fall below the Required Threshold, it will stop.

As the time since the last block increases, so will the Energy Efficiency Threshold and it can begin iterating again. Higher Trust Weight, Block Weight, and wallet balance allow for a greater number of iterations, increasing the possibility of finding a block.

This continues until it finds a stake block or it receives a new block from the network. When it receives a new block, the process resets and starts over.

Another way of looking at this process is through the understanding that Proof-of-Stake is a form of mining. All that the math, weights, and thresholds really do is determine the effective "hash rate" of the stake minter. In the end, the hash rate determines how often, on average, it will find a block and earn a reward, just like with Proof-of-Work mining.

Unlike Proof-of-Work, however, the reward is not fixed, but is determined by the amount of time invested in finding the block. The staking algorithm also produces a non-intensive, efficient process[5] whereby it attempts to generate new staking blocks using the parameters of the wallet's trust key.

6 Tritium Trust with Tritium Core

The Tritium Trust release for Nexus Proof-of-Stake represents only the first update towards full implementation of the Tritium protocol[6], itself the first phase of full implementation of the Nexus Three-Dimensional Chain within the TAO Framework. After Tritium Trust will come the Nexus Tritium Wallet release, then the release of Tritium Core.

Tritium Core introduces the use of signature chains and one-time-use keys within the Tritium layered architecture. Balance will reside on account registers in place of key-based transaction outputs. How will this impact staking?

Much of the content of this document will still apply. However, the use of trust keys for staking will be replaced by a *trust account*. Staking transactions will still take place using keys, now within the signature chain, but balance will be moved to the trust account in place of moving it to a trust key as it does in the legacy Nexus blockchain.

With this in place, Nexus will have a fully functioning account-based trust system. A system that will firmly position the protocol to move forward with the next phase: a Trust and Reputation system supporting L2 Trust Locks within the Three-Dimensional Chain architecture.

[5] One with "hash rate" typically a few h/s and not Mh/s

[6] Nexus: The Tritium Protocol `https://nexusearth.com/tritium-white-paper/`