Proof-of-Stake-**Time**

by **VeriCoin**

PoST White Paper

Authors:

Douglas Pike, Patrick Nosker, David Boehm, Daniel Grisham, Steve Woods, and Joshua Marston

A time-accepted periodic proof factor in a nonlinear distributed consensus

Proof-of-Stake-Time

by VeriCoin

Abstract

A purely distributed consensus in an efficient digital currency would enable a nearly instant and nearly free transaction system across the globe; independent of border, nation, government or bank.

We herein propose a time-accepted nonlinear consensus that maintains the efficiencies of Proof-of-Stake, while increasing the distribution and security of the consensus system with a diminishing probability to find a proof and receive reward over time. This is achieved via a periodic time-acceptance function that is proportional to the coins held and relative to network strength. This time-acceptance model ensures that relatively active staking maximizes reward and probability to form consensus via proof. This incentivizes direct and active protection of the network. Furthermore, voluntary participation in the network is driven by an inflation targeted interest rate that is inversely proportional to network strength. This increasingly rewards nodes which consistently reinforce network security. This is in addition to a time-diminishing inflation rate that is proportional to network strength and active participation in reaching consensus, and relative to the Proof-of-Work distributed initial supply. A combination of costs and rewards favors direct participation in the protection of the consensus, providing enhanced security, equability, and distribution of both consensus and currency over time.

Introduction

Centralized to Distributed Systems

In network systems, there exists a spectrum of hierarchical control - from centralized to distributed. The current standard for most networks including banking systems, governments, and businesses is centralized. These network structures are simple, high capacity, and centrally controlled. They inherently give full control to a minority of administrators, in service of the majority of users of a system. This is beneficial in that it minimizes data sharing costs and control conflicts. Centralized systems are also intuitive by nature, due to strict hierarchical social systems having been the most efficient option available for development of societies since the dawn of civilization. Centralized power institutions have served empires, governments, and economies relatively well as information need only pass through the few. As technology progresses however, there is not only the ability to form efficient distributed systems over a global network, there is a growing necessity[5]. As evidenced in the recent breach of major banking institutions resulting in millions of identities and accounts stolen, centralized systems are vulnerable to attack. This vulnerability is structural in that one compromised target can grant access to majority control and ownership of the target data. This can make the upfront cost and time required to mount a successful security attack justifiable.

Conversely, distributed systems often require numerous simultaneous attacks, each with a diminished return proportional to distribution. As a result, attacks on distributed systems can be very costly, challenging, and ultimately unprofitable. This is in stark contrast to centralized systems, which are in a perpetual cat-and-mouse game. Much of the overhead cost of a centralized system is devoted to maintaining a competitive security edge, rather than developing improvements to the system itself.

Distributed systems by comparison become more secure as a network grows, allowing resources to be directed to the consumer or to development and innovation. The ultimate challenge of a distributed system is to reap the benefits of this robust architecture, without sacrificing efficiency. For the data and control to truly be distributed, information must pass through each node of the system equally, and the network must reach a consensus on the accuracy of this data.

Proof-of-Work Cost as an Incentive to Centralize

Bitcoin is the first publicly successful distributed consensus system where consensus certifies a store of value[1]. Value is a an ideal proof-of-principle vehicle, proving that distributed systems can be used to form public consensus, secured via proofs. Due to the structural security strength of distributed systems relative to fully centralized systems, Bitcoin's consensus ledger of transactions is both valuable and resistant to attack.

In Bitcoin, Proof-of-Work secures the ledger with a floating difficulty which determines the cost of each vote in the consensus as proportional to computational power. This system has proven its security [12], but it does come with significant overhead. The high costs of forming consensus; termed mining, has incentivized a centralization of resources that minimizes costs and risks for miners. Miners do not necessarily have stake in the currency itself after sale to recoup costs. Also, unlike the precious metal miner, they have keys to the security and consensus of the system. Minimizing these risks and costs has resulted in three to five large centralized pools of computational power contributing the vast majority of consensus. This results in a total operating cost in the millions of dollars per day, for what is often a three in five consensus. Though this distributed consensus achievement is remarkable in it's own right, and Proof-of-Work has many advantages unique to the system. Still, this centralization phenomena is a potentially slippery slope that has two significant security vulnerabilities.

The first of these vulnerabilities is, as distribution of the system is reduced in order to offset cost and risk for those who form the consensus, the number of compromised targets needed to manipulate consensus becomes increasingly tractable and less costly. The second of these vulnerabilities is, as the number of entities required for consensus decreases, risk of collusion increases exponentially. Though there may be other ways to address centralization of the consensus, efficiency may in fact be the most direct [9] and this is why we have developed VeriCoin and this new proof system.

We propose a distributed protocol system based on Peercoin's Proof-of-Stake [2], that addresses the two major security deficiencies of Proof-of-Work which stem from the exceptional cost to run the system. This is achieved while also directly addressing the most significant weakness in the current PoS protocols via a nonlinear time-accepted consensus proof and an inflation-targeted variable interest reward system.

Proof-of-Stake: A Solution With Drawbacks

Proof-of-Stake

To the best of our knowledge, the idea behind Proof-of-Stake originated in comments about Bitcoin by Nick Szabo in May 2011, discussing viable alternative proof systems [10]. Months later the term Proof-of-Stake and other aspects related to this potential proof system were described on the Bitcointalk forum by user QuantumMechanic [11]. Then, later that year in November 2011, Sunny King made the first commits on github and the development and implementation of this new proof system had begun.

One of the primary benefits of the Proof-of-Stake system is its efficiency. Proof-of-Work is inherently inefficient, as it is a brute-force proof in which only greater performance increases the probability of finding the correct hash and creating a block. This has resulted in a computational power horse race where cost and risks drive the system toward efficiency, and in some cases, further away from distribution of the consensus. We propose that a lower cost to perform the proof, more effectively enables a long term distribution of the consensus, while the consensus is more favorably formed by those with vested interest in the security of the system. However, Proof-of-Stake in it's current form does have significant drawbacks that mitigate the effectiveness of this distributed consensus system.

The Rich Can Rule or the Poor Can Attack

In Proof-of-Work the cost and difficulty of forming the consensus secures the history of the ledger as an attacker would have to out-compete more than half of the network power at any given time. This is a costly endeavor and will likely become more costly over time as the system grows. This is one of the greatest strengths of the Proof-of-Work system, and is in large part why it stands the test of time. In current Proof-of-Stake systems the consensus is weighted by coins, not computational resources. In this way, an inexpensive botnet cannot dominate the consensus by mere size. Each node must have a fraction of the supply that makes the probability to solve the proof possible. This is the cost that protects the consensus from trivial attacks and manipulation.

Another benefit of this weighting of the consensus is those with vested interest in the viability and security of the system are more directly forming the consensus. This coin weighting scheme does, however, enable collusion, where a minority of holders are approving the majority of blocks, and the majority of blocks are formed by this same minority.
In this scenario, distribution of the consensus is lost and those with few coins are merely owning a share of a semi-centralized, collusion-risk pool. Neither the rich ruling nor the poor

attacking is an acceptable outcome for a distributed consensus proof. Peercoin, the first Proof-of-Stake coin, offset both of these risks by implementing a hybrid Proof-of-Work and Proof-of-Stake system where the stake is defined as coin-age [2].

Coin-Age Versus Coin as Stake Quantity

Coin-age in Peercoin is defined as the product of the total coins from a transaction and the time difference between the current block and the block of its previous transaction. It generates a proof for Peercoin in the following form:

proof 1. $proofhash < coins * age * target$

In this proof coin lots most likely to find a proof are both high in coin and age. This results in a more diversified consensus, as smaller lots of coin can still take part, but require more vested time. This quantity ensures that nearly all coins available to stake, will eventually. Also, those that do stake are deeper in the main-chain, mitigating novel attack vectors. If uncapped however, age can be exploited to enable an attack vector where a moderate coin cost can gain the majority of the consensus. Peercoin chose to cap age at three months to prevent this type of attack from becoming too inexpensive over long periods of time.

Two critical developments in Proof-of-Stake currencies are Nxt and Blackcoin. The Nxt currency [4] was the first exclusively Proof-of-Stake currency, which is important in that it completely eliminated the overhead cost which is common in Proof-of-Work systems. It also is one of the few currencies where the codebase is not forked from Bitcoin. This sets the stage for iterations that further depart from Bitcoin's original architecture. The Nxt developers did not include age as a factor in reaching consensus in order to mitigate the risks associated with excessive age. Blackcoin is a currency based on the Peercoin protocol that is also exclusively Proof-of-Stake, and in many ways ushered a new era of Proof-of-Stake currencies. This is due to the fact that most Proof-Of-Stake currencies are forked from the Blackcoin source. Blackcoin protocol development outpaces most, and remains a leader with Nxt in Proof-of-Stake development and implementation. In the development of their own custom proof system, they also removed age similarly to Nxt, where the proof is in the form [2]:

proof 2. $proofhash < coins * target$

VeriCoin forked from the Blackcoin source code prior to their implementation of a custom protocol, and launched with a NovaCoin modified version of the Peercoin protocol. To further iterate, we are proposing a new protocol that retains the distribution of consensus that coin-age enables while also preventing inexpensive attacks. After the hack of Mintpal [13] that resulted in approximately 30% of total VeriCoin supply being stolen from a centralized, security deficient exchange, we experienced directly the inherent weaknesses of both centralization, as well as the Proof-of-Stake system.

When a dishonest entity captured enough coin to control the vast majority of the consensus and potentially exploit the system, we, along with the community, opted to hard-fork the blockchain to prevent this attack. With or without age, this potential attack could not have been stopped. After much debate and reconciliation with the community and market at large, we knew we needed to develop a system that is far superior, and mitigates this risk as completely as possible.

Introducing the Proof-of-Stake-Time Protocol

Stake-Time as an Alternative to Coin-Age

We propose a solution to a number of the major deficiencies in current Proof-of-Stake models. This is achieved by introducing a nonlinear proof function that defines a fraction of time active and idle, at a given block. Idle-time is defined as the fraction of age that no longer supports the distribution of consensus and instead begins to degrade it. This quantified idle-time is unique to each stake, as It decreases the probability to meet the proof and impacts the fraction of earnable matured interest via consensus. Where the fraction of accepted age (f) is equal to the squared cosine of the product of π and that transactions' consensus power (p), defined as the fraction coin-age (g) of the average network wide stake-time weight (n) over 60 blocks (1 hour) [figure 1]. If the consensus-power (p) is greater than 0.45 all age is lost and the Time-active fraction is equal to the minimum stake time (m) of 8 hours.

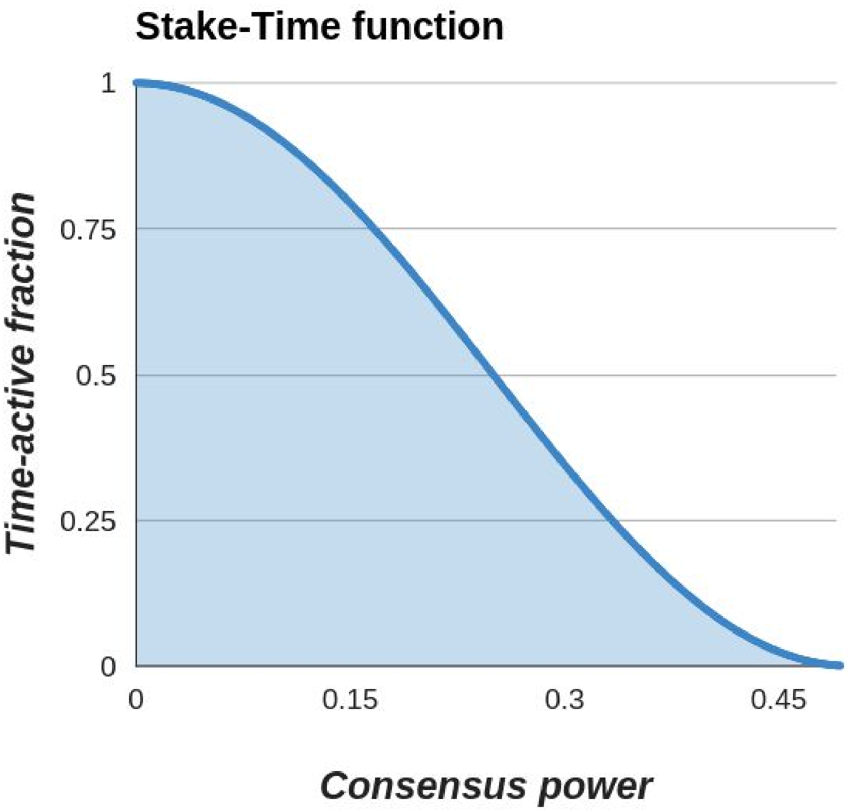
eq 1. Consensus-power (p)

$$p = g / n$$

eq 2. Time-active fraction (f)

$$f = cos^2(\pi p) \ \{if \ (p > 0.45), \ \ f = m\}$$

figure 1.



As the contribution of coinage approaches a majority of the network weight, a greater fraction of age is deemed as idle-time and is not accepted by the network. The resulting effect of this function is that it requires a network activity level that is proportional to the number of coins held, and relative to the network strength. In this method, actively staking is incentivized to maximize both the likelihood to sign a block, and to earn all of the matured interest in reward. The Stake-Time function is used both in the proof and in the quantification of reward.

We define Stake-Time as “The coin-age of a transaction or set of transactions in which the Stake-Time is the product of the total coins (C) and the fraction (f) of acceptable age(a)” in the form:

eq. 3. Stake-Time (s)

$$s = C * (af)$$

Like coin-age, the network accepted Stake-Time is a trust score for coins and depth on the main chain, but also for activity in the network. Unlike Proof-of-Work or Proof-of-Stake, the likelihood to participate in consensus can decrease over time. The combination of these two factors must be in delicate balance with the network, in order to maximize the probability to stake coins. This proof is in the form:

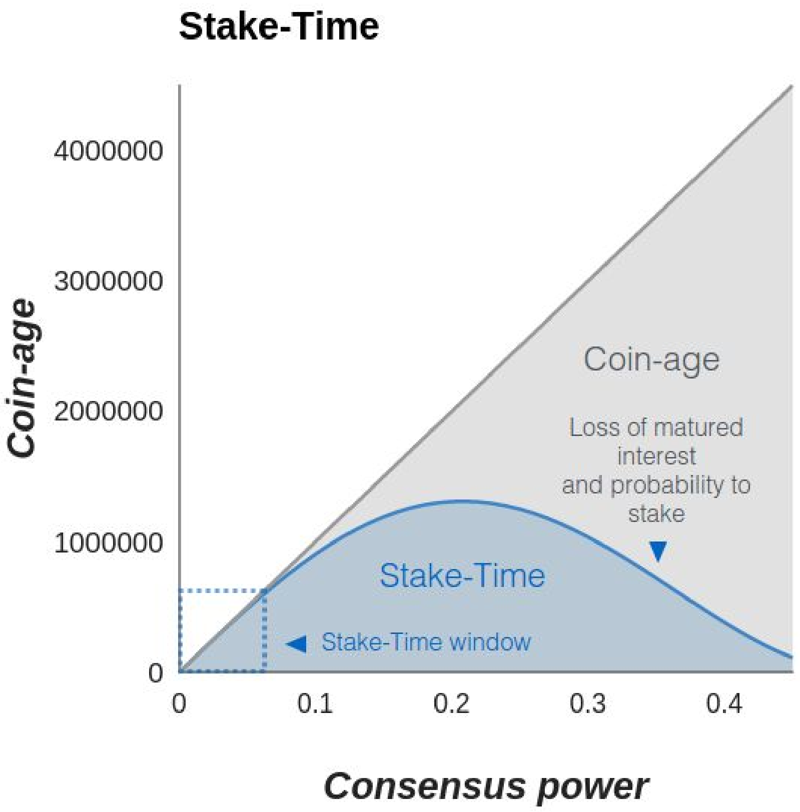
proof 3. $proofhash < coins * staketime * target$

Distribution of a Consensus Majority

Maintaining a minimal idle-time inherently increases the probability to stake while reducing the probability of a successful attack. This results in a moving window that is exponentially more difficult to target for attack, enhancing security of the system from the core structure of a nonlinear consensus. The trust score diminishes with increased idle-time towards a minimum trust score which is equal to the number of coins. While the network approaches equilibrium with the PoST protocol, age will accumulate and plateau across the network. After achieving equilibrium of accumulated age, a network race results to stake as many coin lots as possible before a lot leaves the Stake-Time window [figure 2].

In addition, all participants in the consensus must have reached at least a marginal depth in the main chain and be actively processing transactions to achieve maximal consensus weight. This staking behavior directly protects the blockchain. Ultimately, a maximum network strength is directed away from consensus majority. This results in, on average, a more evenly distributed and more secure staking system, which is exponentially more difficult to attack.

figure 2.



Actively Staking is Most Profitable

In order to maximize the probability of earning all matured interest and signing a block during a period of time, a node must stake actively to ensure passage through the Stake-Time window for all coins held. When network strength is lower, the fraction of age deemed idle-time increases. This results in inactive stakers being penalized, with some loss of matured interest, and decreased probability to stake. By decreasing the likelihood to stake, the inactive staker is susceptible to accumulating age at a faster rate than those actively staking. To regain optimal probability of earning all matured interest, this staker must resume active staking to make up lost time. Conversely, individuals who are staking with little to no idle-time earn their full matured interest reward even in a weaker network state, when acceptable age is low and interest rate is high due to the PoST targeted inflation rate [figure 3]. As a workaround, accumulated idle-time could be reset by sending coins to another wallet, but this comes at a cost: fees are paid to those who are actively staking, and all matured interest due is lost. In summation, the behavior that is by far the most profitable is to stake as actively as possible. This further incentivizes a stable, well-supported network.

The Active Rich and the Vested Poor

This protocol addresses other major drawbacks of the PoS system, one being the "Rich Rule" problem. In PoST, the richest holders must actively stake more often, since the protocol requires an activity per coin to receive proportional reward. This has two impacts once the age of the network has achieved equilibrium. The first of these impacts, is that those with fewer coins have the ability to contribute more to consensus over time, as depth in the main chain increases, further distributing the consensus. The second impact, is that larger holders will have a more significant vote in the consensus proportional to their coin amount, but must also earn their ability to maintain an optimal trust score. This means that the fewer coins held, the greater the age required to successfully stake, and the less idle-time registered. As a result, each coin lot will be met with a relative definition of idle-time. The consensus field is significantly more distributed across a wider range of coin totals, while the blockchain is still protected by the cost of a coin. As a low coin wallet earns a maximal trust score, the quantification of idle-time is exponentially steeper. Due to the Stake-Time product, any loss of age is more significant as fewer coins are held, preventing inexpensive votes.

Time at Stake

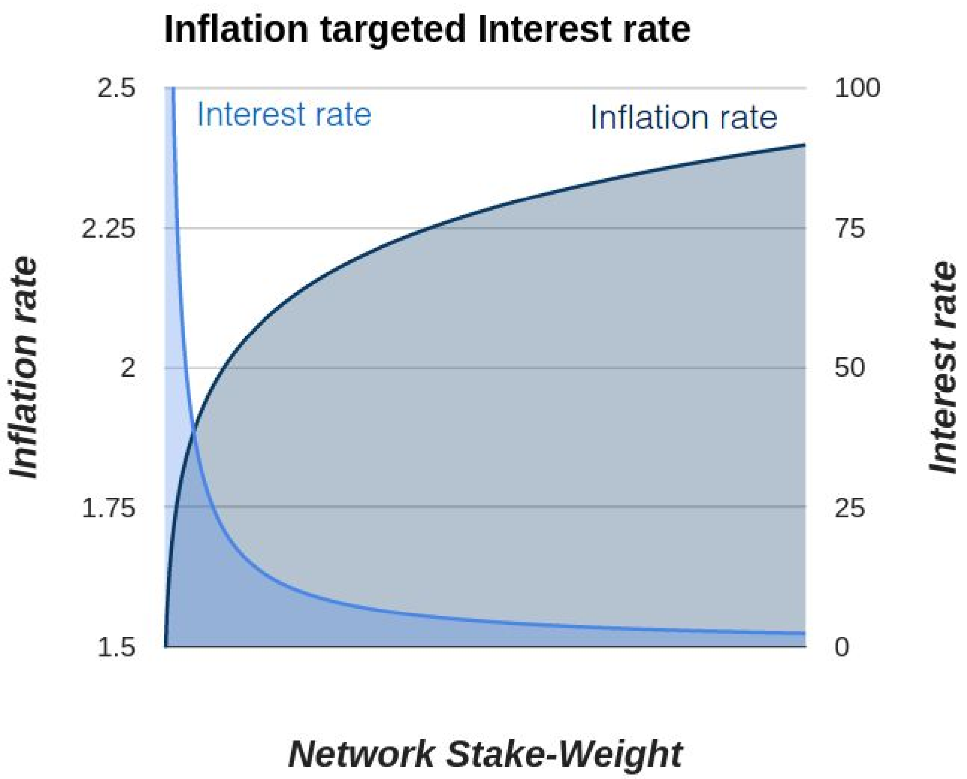
Another significant advantage to this system is its ability to address the nothing-at-stake incentive challenge of PoS [8]. In Proof-of-Stake, chain-splitting can be common due to a lack of work required to become the longest chain. In PoST, however, as a wallet approaches a majority of network weight, its individual weight diminishes proportionally in age. Stake weight in the event of a fork is contributed to the weight of that particular fork, so If a wallet has the majority of coin necessary to fork the main chain, it is impossible for it to not have a majority of the weight for that fork. In PoST, the result is a stake weight that will rapidly diminish, slowing a fork considerably relative to that of the main chain. Ultimately, this mechanism can prevent a competing chain with a less distributed consensus from surpassing the more distributed main chain and thus remove any realistic incentive for attempting to stake on multiple chains. This in all practicality eliminates the risk of the ‘nothing-at-stake’ fork attack vector.

Inversely Paired Interest Model

In PoST, it is nearly impossible to effectively manipulate the interest rate, despite the fact that this variable interest rate falls within a wide range. As network weight increases, the degree of idle-time quantified on average is less, resulting in more matured interest earned over longer periods of time. Due to a new inflation-targeted variable interest rate, however, the interest in these periods will be significantly lower. Conversely, if network strength is low the interest rate will rise and quantified idle-time will be greater. If any node attempts to subvert this system by staking during high interest rates, or by waiting for network idle-time to diminish, they will either experience a reduced interest rate, or a loss of matured interest entirely. This results in a network where only those who have earned minimal idle-time by actively staking will reap full benefit of their staking across the spectrum of interest and accepted maturity.

Inflation Targeted Interest for Incentive-Driven Security

figure 3.



Network Stake-Dependent Interest Rate

VeriCoin initially launched with Network-Stake-Dependent-Interest (NSDI) in order to provide a variable network interest rate, ranging between approximately 1.8% and 2.6% contingent on the network stake weight according to the formula:

eq. 4. Interest reward (r)

$$r = gi \ast 33/(365 \ast 33 + 8)$$

where-in interest reward (r) is the product of coin-age (g), interest rate (i), and an approximation of the number of days in a year. Interest rate is then calculated in the form:

eq. 5. Interest rate (i)

$$i = (17 \ast (log(n/20))/100$$

where-in interest rate (i) is logarithmically proportional to network stake weight (n).
If each VeriCoin holder were to actively stake, an inflation rate of approximately 2.6% would be realized. Since not all holders actively stake their coin, VeriCoin achieved a true inflation rate of 1.2% in its first year.

The expected incentive of network-stake-dependent-interest has been insufficient to both enable an exceptionally stable network while achieving the goal inflation rate of 2%. The original model can however still be realized by targeting for a network-stake-dependent-inflation rate, inherently in the protocol.

Inflation-Targeted Interest Rate

Addressing the need for both enhanced incentive, as well as consistent inflation. Vericoin Development has implemented an inflation-targeted variable interest rate. By specifically targeting a network-stake-dependent-inflation rate rather than interest rate, the network maintains an inflation rate that falls within the original goal range of 1.8-2.6%. This inflation rate rises as market supply diminishes. In addition, by allowing those who actively stake to receive the entire inflation amount via interest, the protocol greatly increases incentive for staking without excess inflation.

The New Interest Determination Function is as Follows:

eq. 6. Interest reward (r)

$$r = si * 33/(365 * 33 + 8)$$

where-in interest reward (r) is the product of Stake-Time (s), interest rate (i), and an approximation of the number of days in a year. The interest rate is then calculated in the form:

eq. 7. Interest rate (i)

$$i = t * 26,751,452 \,/\, n$$

where-in interest rate (i) is the product of inflation rate (t) and the total Proof-of-Work initial VeriCoin supply, divided by average network weight (n). Inflation rate (t) takes the same form as the interest rate in the previous reward system as follows:

eq. 8. Inflation rate (t)

$$t = (17 * (log(n/20)))/100$$

This allows for rapidly increasing stake interest rates while network strength is low, creating a powerful incentive to stabilize the network when staking is needed most. In addition, an individual who actively stakes receives significantly larger interest payments over the lifespan of a node compared to the current model. Lastly, since the interest rate is targeted to an inflation rate which is calculated against 26,751,452 (the total number of VRC produced during the initial Proof-of-Work phase), PoST inflation rate is non-compounded and decreasing relative to total supply over time. This inflation-targeted interest mechanism ensures an inflation rate which gradually diminishes over time, even further increasing incentive to stake, while encouraging distribution of consensus.

Conclusion

Finally, we conclude that the nonlinear time-accepted proof system further distributes consensus by accepting time that enhances distribution and rejecting time that diminishes it. The Stake-Time window is an exponentially more difficult attack target, where significant threats are detected and addressed proactively by the network, and finding suitable proofs becomes progressively more difficult. Simultaneously, distributed threats are also discouraged by PoST, and heavily penalized in cost. The system also significantly incentivizes participation in staking with greater overall rewards to those actively participating in the consensus, particularly at times when needed most. The inversely proportional relationship between accepted-time and interest rate prevents dishonest nodes from bypassing the dynamics of this system, and taking what isn’t due in proof.

With this work we aim to bring Proof-of-Stake to a new level of security, with strong incentive and fair distribution. This delivers more favorable rewards for more favorable actions, securing the network in a very direct and tangible way. It is our goal to create an environment where consensus collusion and manipulation are as far from practical as possible, where a near costless distributed network can thrive for years to come via voluntary participation in a provable consensus.

PoST

by VeriCoin

Acknowledgements

A sincere thank you to the Altcoin Community in general and to all of those who have supported VeriCoin and continue to do so unconditionally.

Special thanks to Jay Jay Abels, Bruno Proença, Scott Allyn, Ernest Chubb III, Jan Wieczorek and many others for their relentless efforts to help deliver a unique brand, an active Community and a cohesive message that truly captures the essence and pursuit of VeriCoin.

Resources

VeriCoin Website // www.vericoin.info
VeriCoin Forums // www.vericoinforums.com
VeriCoin YouTube // www.youtube.com/user/vericoinchannel
VeriCoin Facebook // www.facebook.com/vericoin
VeriCoin Twitter // www.twitter.com/vericoin
VeriCoin Google+ // www.plus.google.com/+vericoinchannel

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. bitcoin.org, 2008.
[2] Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. peercoin.net, 2013.
[3] Pavel Vasin. BlackCoin's Proof-of-Stake Protocol v2. blackcoin.co, 2014.
[4] Alias et. al. Whitepaper: Nxt. nxt.org, 2014.
[5] Nick Szabo. The dawn of trustworthy computing. unenumerated.blogspot.com, 2014.
[8] Vitalik Buterin. Proof of Stake: How I learned to love weak subjectivity. blog.ethereum.org, 2014.
[9] Laurie B. : Decentralised currencies are probably impossible (but let's at least make them efficient). http://www.links.org/files/decentralised-currencies.pdf, 2011.
[10] Nick Szabo. Bitcoin, what took you so long? unenumerated.blogspot.com, 2011.
[11] QuantumMechanic. Proof of stake instead of proof of work. bitcointalk.org, 2011.
[12] Dan Kaminsky. I tried to hack Bitcoin and I failed. Business Insider, 2013.
[13] Stan Higgins. 8 Million Vericoin Hack Prompts Hard Fork to Recover Funds. Coindesk, 2014.