Proof-of-Stake-Participation (PoSP): White Paper

Crypto Bullion Core Development Team

http://www.cryptobullion.io

December 2015

Abstract

Presenting a proposal for a crypto-currency block chain security and distribution mechanism that engages a superior version of Proof-of-Stake to amplify network security to its maximum potential through the implementation of an intelligent pay-for-work configuration. *PoSP – Proof-of-Stake-Participation**, is specifically designed to incentivize participation in securing Crypto Bullion's network by calculating the total monetary supply's compounded interest of 2% per year and disseminating it among only actively staking Crypto Bullion allowing for enriched interest earning potential for contributors to network security and efficiency.

Introduction

Proof-of-Work (PoW) and Proof-of-Stake (PoS) are the two preeminent mechanisms (algorithms) in use today for block chain security, transaction confirmations and distribution of a crypto-currency. There are variations of each and also combination PoW/PoS 'Hybrids' such as the one currently employed by Crypto Bullion (CBX). This paper will provide a high level overview of each algorithm as well as CBX's Hybrid system. This background will lead into our proposal for what we consider to be a superior alternative

solution that provides not only vault-like security, but also does so in a resource-conscientious way that promotes decentralization by allowing any individual or entity to participate simply by owning some Crypto Bullion and an internet connection.

Proof-of-Work

Proof-of-Work[i] relative to crypto-currency is best known from its application in Satoshi Nakamoto's Bitcoin[ii]. Proof-of-Work functions to distribute a crypto-currency by awarding blocks of new coins to miners who process transactions and secure the network simultaneously by their combined, applied hash rate. The first miner to solve a correct hash for a block is rewarded with coins, which are then introduced into existence and logged into a public decentralized general ledger (block chain). The difficulty to solve these hashes is directly reflective of the competition level participating and thereby allows for a predetermined inflationary rate to be maintained.

Surprisingly, with regard to decentralization and security (2 key improvements over traditional monetary systems), Bitcoin has become a victim of its own success. At it's beginning, Bitcoin's PoW allowed for a true decentralized network as anyone with a CPU could participate and mine for new Bitcoins. As the mining competition increased, so did the technology. Advancements such as ASIC miners[iii] made CPU miners obsolete and triggered an arms race where the price to participate grew exponentially in congruence with Bitcoin's mining difficulty. Mining pools (where a network of miners consolidate their computational resources) and big money mining farms (where large capital investments are allocated to specialized computer centers dedicated to mining) became the norm and abolished the decentralization that had been provided with CPU mining. This evolution towards centralization, reminiscent of the

traditional monetary systems that require trust in a central authority, allow Bitcoin to be controlled by a shrinking minority group of the rich and powerful. Furthermore, centralization opens up the Bitcoin network to the threat of a 51% attack[iv] (which can be launched by a party with a majority share of the hash rate). Once again the majority finds they must trust that the controlling minority will do the right thing – sadly, something disproven time and again throughout human history.

Additionally, in critique we must look at environmental impact, as the collective conscience of mankind grows we are becoming more aware daily of the signs nature is giving us regarding the destruction of our environment and depletion of our resources. PoW depends on futile and highly energy consumptive work to be performed and like other wasteful resource depleting activities needs to be responsibly replaced with more efficient systems.

Proof-of-Stake

Proof-of-Stake[v], originally proposed and applied in conjunction with Proof-of-Work as a Hybrid algorithm[1] in Sunny King's Peercoin[vi], offered an alternative dual method of securing the network and distribution of new coins. In this more energy efficient system, miners are joined by coin owners that help protect the network relative to the amount of coins they own and stake. As compensation for their protective service, stakers generate or 'mint' new coins (similar to earning interest on savings) based off of consumption of coin age, a stark contrast to the energy wasteful PoW model. Coin age is calculated by number of coins held multiplied by number of days held unmoved and acts as the priority selector for awarding minted interest payments in traditional PoS systems.

[1] http://en.wikipedia.org/wiki/Hybrid_algorithm

Since Peercoin's initial implementation, Proof-of-Stake has evolved to be used alone without Proof-of-Work by a number of coins in existence today to provide an even more energy efficient solution. Typically these pure Proof-of-Stake coins will begin as a Hybrid (PoW and PoS) and after a variable initial distribution period abandon Proof-of-Work to rely solely on Proof-of-Stake for security, transaction confirmations and continued distribution.

Critiques with Proof-of-Stake working alone include the alleged lack of penalty for a double spend attempt, the fairness (or perceived fairness) of the length and method of the initial distribution method (typically PoW) and the security of a network built in a paradox that relies on continuous staking of coins for proper functioning and security yet encourages and rewards for non-continuous staking via the coin age based qualification methodology employed.

PoW/PoS Hybrid

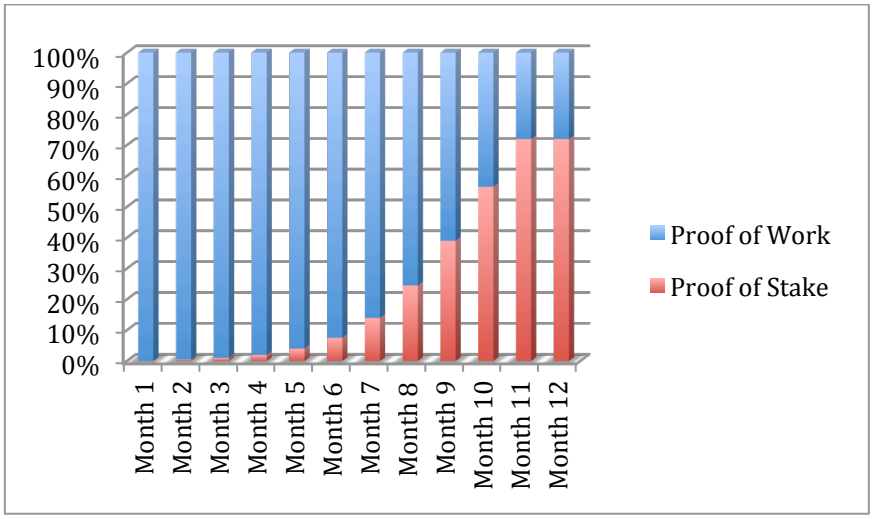
The PoW/PoS Hybrid, discussed here in reference to its implementation in Crypto Bullion at the time of this writing, uses a combination of Proof-of-Work and Proof-of-Stake to distribute new coins, process transactions and to secure its network. This dual level model is synergistic as it takes from strengths of each system. Proof-of-Work allowed for a yearlong, slowly tapering primary distribution period and provided network security as Proof-of-Stake gradually over time took over the majority share of the distribution activity.

The Hybrid system forces a potential attacker to need not only 51% of the hash rate via PoW, but also 51% of the staked coin age via PoS to successfully overtake the block chain in an attack. An attack on either of the mechanisms used in the Hybrid is expensive to the attacker, and when the two systems are combined, the cost of attack

essentially doubles while at the same deterring the attack by making the attacker the primary victim of their own attack.

Crypto Bullion, launched in late June of 2013, was designed to transition slowly and fairly over a yearlong distribution period from primarily Proof-of-Work to the now primarily Proof-of-Stake implementation. Both systems have been and continue to be used; only the primary and secondary distribution systems have traded places with Proof-of-Work relinquishing the lead reigns to Proof-of-Stake.

The graph below shows the monthly distribution for both Proof-of-Work and Proof-of-Stake for the first year of Crypto Bullion's life cycle. Months 11 and 12 show the distribution balance that continues today over 2 years into the life cycle of CBX.



Crypto Bullion was designed to distribute the majority share of its less than 1,000,000-coin cap through Proof-of-Work mining during its yearlong expansion and adoption phase. On a monthly schedule, the Proof-of-Work reward declined for the first year until finally settling in at a 0.5% yearly inflationary rate (0.01 CBX reward per block, per minute). Proof-of-Stake interest is set at 1.2% annual interest for those staking every 30 days up to a maximum of 1.5%

annual interest for those staking every 90 days. To summarize, Crypto Bullion can inflate at a maximum rate of 2% per year with CBX that are brought into existence via payouts to participants who confirm transactions and secure the network via one or both of the applied algorithms of the Hybrid. *(It is important to note that this low inflationary rate was carefully selected to mimic that of gold, thereby positioning Crypto Bullion in a niche as the digital compliment to precious metals. Also, it is important to convey that this low inflationary profile will* ***not*** *be changed so as to avoid the long-term pitfalls of excessive inflation.)*

As the crypto-currency landscape has continued to evolve and grow over time, the environment has dramatically changed from what it was two years ago when Crypto Bullion was first conceived and launched. External factors, such as the introduction of hundreds of new coins, have led to a heavy saturation of the market and have spread crypto-currency investments and hash rates thinly over a broad spectrum of coins. This market saturation, like it or not, is the reality and in most cases results in a slowly declining hash rate for existing coins causing less network security. In the case of a Hybrid model, although the effectiveness of Proof-of-Work as a security system dwindles with the lowering hash rate, security is still maintained by Proof-of-Stake.

In response to the dwindling hash rate scenario, many coins have opted to evolve to pure Proof-of-Stake systems once their distribution target has been reached to remove the potential Proof-of-Work / low-hash rate weakness. Ironically, they have found that reliance on Proof-of-Stake alone has brought about new issues such as stalling block chains as coin owners opt out of staking resultant to lack of proper incentive, thereby causing transactions to not be processed.

Change Proposal Outline

As we have illustrated, there are presently opportunities for improvement with regard to Crypto Bullion's Hybrid algorithm. The Proof-of-Work hash rate is lower than ideal for security purposes. The Proof-of-Stake reward system is structured in such a way that it actually discourages what is best for the network's security – consistent staking. Also, the low PoS inflationary rate of 1.5% maximum does not generate sufficient motivation for CBX holders to stake consistently. Much research, study, brainstorming and debate has gone into determining the best options to consider for rectifying these issues. Solutions implemented in other coins have been reviewed and studied resulting in the discovery that the right solution for CBX had yet to be conceived. The resolution finally reached includes some dramatic changes to Crypto Bullion's algorithm, which we will now outline.

The lower than ideal Proof-of-Work hash rate issue will be resolved by removing PoW altogether. As mentioned earlier in this document, Proof-of-Work has been and continues to progress towards centralization and needlessly consumes an astounding amount of resources. Considering the negatives of retaining PoW in concept alone and that our comprehensive solution will provide superior security without it, PoW will be discarded.

Proof-of-Stake: With regard to a solution for enticing consistent staking by enhancing the pay-for-work reward, it is imperative to stay true to our commitment of remaining a low inflation and scarce store of wealth – Crypto Bullion's target niche since inception in June of 2013. This means that the solution needed must not only secure the network maximally at all times but must also incentivize the market to purchase and stake CBX consistently all while

remaining within the confines of our established low inflationary 2% per year promise (currently made up of 0.5% from PoW and 1.5% from PoS). The answer to this dilemma has been crafted with Proof-of-Stake-Participation (PoSP).

Proof-of-Stake-Participation (PoSP)

Let us now have a look at the current Proof-of-Stake implementation in Crypto Bullion and our proposal to improve it. Proof-of-Stake currently works to protect the network when owners 'stake' their CBX at a given time - a service for which they are compensated with an interest payment on their staked coins.

The current implementation operates based on the consumption of coin age and dictates that minted CBX be awarded as an interest payment on CBX staked at minimum intervals of 30 days to earn a 1.2% annual interest up to a maximum of 90 days to earn at 1.5% annual interest. Once this interest payment is awarded, the accumulated coin age is destroyed and the staked CBX starts to accumulate age again until it reaches the 30 to 90-day threshold to become eligible to earn it's next stake. This reward structure encourages owners of Crypto Bullion to hold their funds offline to accumulate the necessary amount of coin age for periodic staking to only then be returned off-line for the process to repeat. Periodic staking does not secure the network to its maximum potential, yet by design, this is exactly what is encouraged and rewarded. Please note that Crypto Bullion is not the only PoS implementation that rewards for counterproductive behavior – this is the norm for PoS implementations across a vast majority of coins.

Our proposed solution to the periodic staking concern is the implementation of Proof-of-Stake-Participation (PoSP). In this

version of Proof-of-Stake, coin age is removed thereby negating the incentive for keeping CBX offline where it does not protect the network. Additionally beneficial is the removal of a weakness for attack on the network via an accumulation of coin age. To gain control of the network, a nefarious party would need to own over 50% of CBX in circulation rather than having the opportunity to cheat the system by using the 'age' multiplier.

For example, with coin age (number of coins * days coins held) 100 coins held for 50 days becomes the equivalent of 5,000 coins (100 x 50). With the removal of coin age and its multiplying effect, 100 coins will always equal 100 coins so the would-be attacker is forced into a position of truly purchasing the majority share of existing CBX making the attack self-destructive, illogical and valueless.

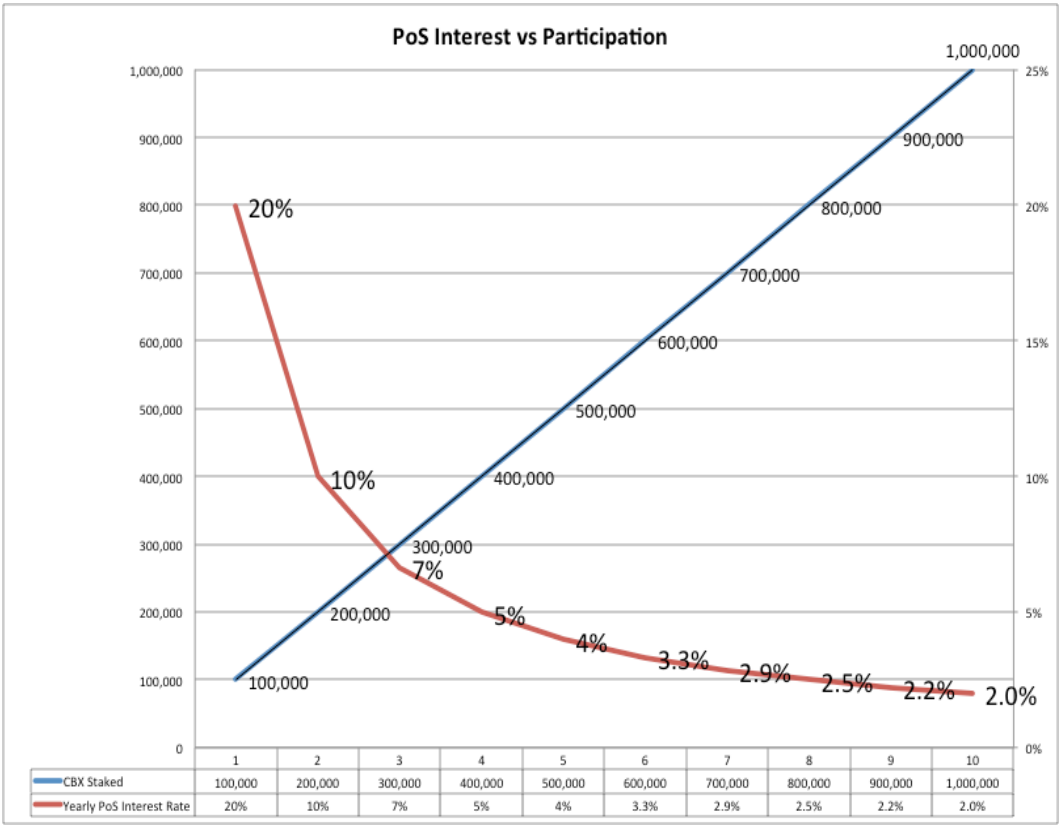
Crypto Bullion's inflationary profile allows for a maximum of 2% annual inflation, which had previously been shared between PoW and PoS. Since we are committed to this inflationary profile, we will stay within this framework with the applied solution. With the removal of PoW, its 0.5% inflationary rate can be added to the 1.5% currently existing in PoS. That being said, the maximum yearly inflation through Proof-of-Stake-Participation will be 2% of total coin supply.

$$\boldsymbol{Annual\ Inflation} = \boldsymbol{Total\ coin\ supply} * 2\%\ (\boldsymbol{compounded})$$

In order to encourage and reward active and consistent staking to the network, we will take this maximal potential annual inflationary rate and lock it in as the actual annual Proof-of-Stake-Participation inflationary rate. Meaning that Crypto Bullion will inflate at a rate of 2% each year through PoSP, regardless of how many coins are staked. I.e. If only 10% of the supply of CBX is staking, then that subset of the overall supply can expect 10x higher interest (or 20%

annually), as they will earn the unclaimed stake from non-staked CBX in addition to their own interest potential. CBX owners will have the choice to earn interest by staking their funds and providing a protective service to the network or they can opt not to stake and forfeit their earnings potential to those who are providing a protective service.

Below is a diagram showing the variable annual interest rate in accordance to how many CBX are being staked at a particular time.



As you can see, the PoSP interest percentage can vary widely in this implementation without compromising Crypto Bullion's 2% annual inflationary promise. We feel this is the ideal configuration to insure and fairly incentivize for maximum network security by a true pay-for-work contract.

The Proof-of-Stake-Participation target block time will change ever so slightly to 65 seconds so that CBX's fast transaction precedent

continues. Every 65 seconds the Vault (CBX's client) will conduct the following calculation and then distribute the output to a selection of staked CBX participating in securing the network over that particular 65 second time span.

$$\frac{\boldsymbol{Total\ coin\ supply} * 2\%\ (\boldsymbol{annual\ inflation})}{\boldsymbol{485,169\ blocks\ per\ year}} = \boldsymbol{PoSP\ reward\ per\ minute}$$

In order for CBX to be eligible to stake, they must be held unmoved and online in an unlocked Vault for at least 1 hour. After the 1-hour has passed, the staked CBX will enter the queue to mint the PoSP blocks occurring each minute. Once a PoSP block is awarded, the winning group of staked CBX will have to wait the 1-hour eligibility time in order to qualify again for PoSP interest, thereby providing a better opportunity window to those staked CBX that missed out on that particular block.

The less CBX being staked to the network, the higher the chance to earn a block reward for staking CBX. This structure will compensate owners that hold their own CBX under their control in their personal Vault protecting the network rather than with a 3rd party exchange or in offline storage, both of which do nothing beneficial for the network's security and contradict a major advantage of crypto-currencies which allow the individual or entity to 'be their own bank'.

In addition to enhancing security, this configuration is designed to encourage long-term investment into Crypto Bullion by inspiring the removal of CBX from the exchange market. Less CBX on the market for sale will have the effect of upward pressure on price and market cap making Crypto Bullion more attractive to new investors and more profitable to those earning stake by protecting the network.

Conclusion

We have begun by outlining the current framework of different security, transaction, and distribution methods employed today in crypto-currencies and provided a high level explanation of the strengths and weaknesses of each. This progression led us to recognize the weaknesses of existing crypto-currency algorithms. From this foundation we have recommended solutions in order to maximize network security by designing and implementing an honest pay-for-work contract known as Proof-of-Stake-Participation (PoSP). To summarize, we have proposed removal of Proof-of-Work and implementation of the innovative Proof-of-Stake-Participation mechanism to maximize network security via the re-appropriation of the rewards from non-participants to better incentivize active and continued participants.

---

[i] https://en.bitcoin.it/wiki/Proof_of_work
[ii] http://en.wikipedia.org/wiki/Bitcoin
[iii] http://en.wikipedia.org/wiki/Application-specific_integrated_circuit
[iv] https://en.bitcoin.it/wiki/Weaknesses
[v] https://en.bitcoin.it/wiki/Proof_of_Stake
[vi] http://en.wikipedia.org/wiki/Peercoin