Proof-of-Stake-Velocity v2 (PoSV v2)

Enhancing the Social Currency of the Digital Age

Reddcoin (RDD) Core

August 2019

Written by:
Jay "TechAdept" Laurence & John "CryptoGnasher" Nash
An update to the original whitepaper written by Larry Ren, April 2014

Reddcoin's "Redd Paper": A Guide To PoSV v2

Table of Contents

Abstract

Proof of Stake Velocity (PoSV) was proposed and implemented in 2014 as an alternative to Proof of Work (PoW) and Proof of Stake (PoS) in order to secure the peer-to-peer network and confirm transactions of Reddcoin, a cryptocurrency created specifically to facilitate social interactions in the digital age. PoSV was designed to encourage both ownership (Stake) and activity (Velocity) which directly correspond to the two main functions of Reddcoin as a real currency: store of value and medium of exchange. Reddcoin can also function as the unit of account in a heterogeneous social context. Over our first five years, PoSV has been immensely successful at meeting its goals, and this updated paper is meant to reflect further refinements of the protocol after real-world implementation and feedback. The technological aspects of PoSV are presented after a detailed review of existing and future-looking designs. The economic aspects of Reddcoin to date and in future effect are then analyzed. The unique position of Reddcoin as a digital social currency in the competitive landscape of cryptocurrencies is discussed. Finally, an analysis of the past five years of chain operation, notable aspects, and the new enhancements to the existing Reddcoin PoSV protocol are explained.

1 Introduction

Bitcoin is among today's most discussed and controversial topics. Ever since Satoshi's seminal paper[1] in 2008, Bitcoin has evolved from a technological experiment embraced by a small group of computer enthusiasts to what some today consider to be the most important innovation since the Internet. Most recently, there are new variants of Bitcoin, called altcoins, created every day and a whole new industry of altcoin trading exchanges, mining pools, gaming websites emerged. Few topics today are more polarizing than cryptocurrency. Some merits of cryptocurrency touted by technologists are considered sins by economists.

Cryptocurrency is considered a movement by believers and a fad by disbelievers. Instead of an open and honest discussion involving all sides, what we have witnessed is a dialogue of the deaf, in which each camp justifies its own intellectual laziness by pointing to the intellectual laziness of the other camps. This is one of the main obstacles that prevent cryptocurrency from being accepted by the general public.

What do we really know about this evolution? Is cryptocurrency just a technological breakthrough or also an economic one[2]? Is mining cryptocurrency progress or retrogression[3]? Is cryptocurrency meant to replace government and financial institutions or compliment them? Is cryptocurrency designed for hoarding and speculation or spending and use? And, the most fundamental question of all: is cryptocurrency real currency or just virtual property for speculation[4]?

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008
[2] Paul Krugman. An Ubernerd Weighs In. 2013
[3] Paul Krugman. Adam Smith Hates Bitcoin. 2013
[4] David Yermack. Is Bitcoin a Real Currency? An economic appraisal. 2013

So far innovation in the cryptocurrency world has been almost exclusively technical. Technologists have proposed an improvement on various aspects of Bitcoin, such as new hash functions[5] to replace SHA256 and new mechanism[6] to replace Proof-of-Work. There have been very few cryptocurrencies designed to address the economic and social aspects of being a real currency. Reddcoin, at the time of writing, seems to be only one.

Goals of this Redd Paper:

We update and re-release this defining paper (our "Redd Paper") with four goals in mind:

1) To give a broad overview of the current issues around cryptocurrency; both the technological and economic, which might not have been foreseen by the original designers of those systems.
2) To address these issues with proposals which require coordinated changes in both low-level network protocol and a high-level economic and social eco-system.
3) To encourage a more open and objective discussion of cryptocurrency by the general public and promote more complete thinking for future innovation in the cryptocurrency world.
4) To explain development efforts to improve and enhance the Reddcoin protocol following five years of real-world observation of performance and "in vivo" user activity in its divergence from theory.

The rest of the paper is organized as follows:

Section 2 describes in detail the merits and drawbacks of Proof-of-Work (PoW) and Proof-of-Stake (PoS) from both technological and economic points of view. PoSV is then described to address those drawbacks in the specific context of a digital social currency. The technological design choices of PoSV are given in broad strokes. More detailed technical analyses will be presented in a companion paper, also updated for this release, and as it has been active for almost five years successfully, lessons learned and observed results are also described[7].

Section 3 addresses the most common criticisms by economists on cryptocurrency and shows how Reddcoin and PoSV together provide new answers and new opportunities for social research in general.

Section 4 emphasizes the main differences between Reddcoin, a digital social currency which focuses on integration with human social interactions and aims to concretize and quantify people's intangible asset of social influence, and the much more common digital commercial currencies which aim to facilitate transactions of goods and services and offer protection from hyperinflation.

[5] Colin Percival. Stronger Key Derivation via Sequential Memory-hard Functions. 2012

[6] Sunny King and Scott Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. 2012

[7] John Nash & Jay Laurence. Proof-of-Stake-Velocity v2: Technical Data & Review, To Be Published, Q32019

2 Technology

A cryptocurrency uses principles of cryptography to implement a distributed, decentralized and secure cash system. It solves the problem of double-spending in a distributed ledger by introducing a mechanism to secure the network against 51% attacks and Distributed Denial of Service (DDoS) attacks. The underlying principle of such a mechanism is the necessity of expending resources when confirming transactions. Once confirmed, transactions become irreversible as it's practically infeasible for an attacker to have access to the huge amount of resource required to modify them. Different mechanisms use different types of resources to accomplish this goal.

2.1 Proof of Work

A Proof-of-Work (PoW) is a piece of data which is costly to produce so as to satisfy certain requirements but is trivial to verify. Bitcoin uses the Hashcash PoW[8]. Mining, the process of producing PoW, plays the central role in creating, distributing and securing Bitcoin and many its variants. The most common criticism of PoW mining is its massive waste of energy. At the time of writing, the total daily revenue of mining Bitcoin is growing daily. Depending on the aggregate profit margin and the fraction of overall cost that electricity accounts for, we estimate the daily total electricity cost at approximately “enough to power Iceland”. In addition to this wastefulness, there are several more reasons why mining remains a very controversial aspect of PoW cryptocurrencies.

2.1.1 Mining Arms Race

Mining is by nature extremely competitive. Mining costs include initial expenditure on equipment plus on-going energy cost. Miners are predominantly rational profit seekers. Their top concern is how long it takes to recover the initial cost, i.e. the length of Return on Investment (ROI). During the very early age of Bitcoin, mining was carried out by CPU. When mining later became available on graphics cards (GPU), mining on CPU became immediately loss-making. As Bitcoin price continued to soar, mining operation witnessed a mini industrial revolution. Application-Specific Integrated Circuits (ASICs) designed to carry out PoW computation at several magnitude higher speed and lower energy cost started to emerge and soon rendered GPU mining obsolete. This relentless arms race causes constant worry among average miners who usually fail to recuperate initial investment and cannot afford continuous hardware upgrade.

Bitcoin uses SHA256as the hash function in PoW and is the first to experience this arms race[9]. The same arms race is happening to cryptocurrencies that use the Scrypt hash function[10]. Scrypt was initially touted as “ASIC-resistant" due to its heavier memory usage. In reality, ASIC-resistance is one of the most misleading and over-abused marketing slogans in the cryptocurrency world. The correct word is “ASIC-ignored". ASICs can be designed and manufactured to perform all hash functions. The entry barrier is not technical but financial. Unless there is sufficient market demand for mining Scrypt-based cryptocurrencies, it's simply financially unprofitable for manufacturers to invest in the production of such ASICs. While Scrypt is under the threat of ASIC, many cryptocurrencies have been created to use alternative hash functions such as Scrypt-N, Scrypt-Jane, and X11. These cryptocurrencies all market themselves as the latest and best generation of ASIC-resistance when this resistance is entirely

[8] Adam Back. Hashcash - A Denial of Service Counter-Measure. 2002

[9] National Institute of Standards and Technology. Secure Hash Standard (SHS). 2012

[10] Colin Percival. Stronger Key Derivation via Sequential Memory-hard Functions. 2012

dependent on being a minority. It's deeply self-contradictory for a cryptocurrency to pitch ASIC-resistance as its main merit to gain wide adoption when this sole merit depends on it being unpopular.

In theory, it can be preferable to have a separation between mining a cryptocurrency and using it. It's more efficient to leave mining operation to specialists who use their domain knowledge to achieve economy of scale. This is indeed the case for Bitcoin, the most established cryptocurrency. However, for many newly created variants, average GPU-miners make up the vast majority of user communities and the fear of ASIC directly threatens their social fabric.

2.1.2 Miner Incentive

Miners provide a paid service to cryptocurrency networks, that of security and consensus. It should be remembered that they are all profit-seekers first and foremost. At a fixed cost, it's perfectly rational for them to mine the most profitable cryptocurrency and sell it quickly in the market to limit exposure to price risks. Hence were born the so-called “multipools" which fully automate this process. Multipools create two new problems in the cryptocurrency world.

First, the profit-seeking by multipools pushes many cryptocurrency prices to just above mining production cost. As mining production costs inevitably go down due to technological advances, many cryptocurrency prices suffer from a downward death spiral, which hurts the morale of the corresponding communities.

Second, multipools employ strategies that exploit the lag in the readjustment of difficulty of PoW. Multipools switch to a cryptocurrency with low difficulty and keep mining it while its difficulty gradually catches up. The moment the difficulty rises to its fair value, multipools switch again. As a consequence, multipools mine blocks at a significantly lower average difficulty than other miners. Although from a pure Darwinian point of view multipools help improve market efficiency and filter out the weakest, they do force most cryptocurrencies to focus on extremely short-term interests rather than long-term growth and innovation.

2.1.3 Manufacturers of ASIC Mining Equipment

To be the most profitable miner, one must be the first to get the latest equipment that offers the highest hash rate per unit of cost. Therefore manufacturers of ASIC mining equipment have a strong financial incentive to use their own product for mining first and only start shipping equipment to buyers after mining profitability drops enough. This inherent conflict of interests has a profound impact on every aspect of the mining business. For example, the vast majority of manufacturers ask for prepayment in exchange for a promise. The actual delivery is usually delayed by months, which reduces mining profitability for their buyers to almost zero. Manufacturers often offer no refund for a shipping delay or product defect in their terms and conditions, effectively eliminating their own liabilities and openly exploiting the desperation of buyers.

All these frustrations reduce the confidence of average miners and undermine the soundness of PoW mining as the guardian of cryptocurrencies' decentralized networks.[11]

[11] Eyal and Sirer, Majority is not Enough: Bitcoin Mining is Vulnerable 2013

2.2 Proof of Stake

Proof-of-Stake (PoS) is an alternative to PoW first introduced in Peercoin [12]. The resource used by PoS is “coin age": currency amount times holding period. Similar to energy, coin age as a resource is expensive to amass in huge quantity. For an attacker to accumulate enough coin age to attack the distributed network, he either has to buy on open market a large amount of the very currency he's trying to attack, driving up its price during the process and diminishing his economic incentive, or hold coins for a very long time, reducing the frequency of his own attacks.

One useful feature of PoS is the significant savings in energy consumption. Another main feature is the better alignment of incentives between miners and stakeholders because miners are now the stakeholders. PoS, however, has several limitations:

2.2.1 Initial Distribution

PoS, by construction, relies on a fair and wide distribution of a cryptocurrency but doesn't deal with the logistical issue of how to achieve this fair distribution in the first place. By comparison, mining in PoW, despite all its drawbacks, also serves as a potent channel of distribution. This chicken-and-egg problem was and remains a major challenge for all PoS cryptocurrencies. So far there have been two popular workarounds: a) “pre-mine", i.e. similar to a subscription to stock IPO in financial markets and b) a hybrid system of PoW and PoS with PoW gradually fading away after an initial period. The main criticism of “pre-mine" for PoS coins, is its lack of guarantee of either fair or wide adoption. The vast majority of “pre-mine" turned out to be a fraud. For those which were not, investors and speculators with deep pockets can easily control a large stake in the currency, transforming its nature into more of a speculative vehicle than a currency. Over-concentration of stakes also increases the security risk of the decentralized network.

The PoW-PoS hybrid system alleviates these concerns by running PoW and PoS in parallel. PoW mining works as both a steady distribution channel and a fall-back network security mechanism. As PoW block rewards go down over time, PoS has enough time to move to the spotlight. Unfortunately, it doesn't matter what particular model a PoS cryptocurrency uses for initial distribution. The mere knowledge by the public that a cryptocurrency will eventually rely on PoS compromises its ability to achieve a fair and wide distribution. This is the inherent paradox of Proof-of-Stake.

Editorial Note: While the above still holds true, in retrospect after five years, in large part due to the economic cycles and current development status of Reddcoin, it can be said that a perfect storm of circumstances has allowed Reddcoin to overcome many of the above challenges simply by continuing to exist and evolve. RDD at present is highly distributed, a “utility” by all current legal standards, and subject to only Proof-of-Stake (PoSV, specifically) generation.

2.2.2 Hoarding

The entire PoS network depends on coin age as the scarce resource. Coin age can only be earned by holding coins. To earn coin age at a higher rate than others, one must hold more coins. Coin age is consumed when a coin is spent in a transaction. PoS mining require a user to repeatedly send coins to them self, thus consuming his reserve of coin age in exchange for probabilistic winning a PoS block reward without reducing the size of the holding. Coins spent in transactions facing other users also have

[12] Sunny King and Scott Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. 2012

their coin age reset to zero but this consumption of coin age is outside the scope of PoS mining, unqualified for block rewards and is considered a “waste" by most PoS stakeholders.

It now becomes clear that PoS has been designed to encourage hoarding and discourage spending. Some PoS coins, such as Peercoin, openly declare their philosophy to “function more as a long-term store of value than a medium of exchange." In this sense, PoS coins are created to be collectibles rather than currencies. Scarcity is a necessary but insufficient condition for collectibles to have value.

PoS coins are actually designed to encourage hoarding and discourage spending!

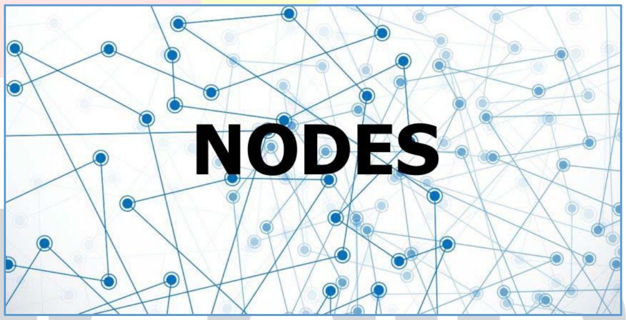
Collectibles must also offer some form of utility such as aesthetics and historic significance. Considering the fact that anyone can access and modify the source code of PoS coins and potentially offer an improved version, in theory, there is infinite supply. The scarcity condition doesn't hold.

It remains an unsolved puzzle where PoS coins marketed as collectibles derive their value from.

2.2.3 Full Nodes

PoS transforms all stakeholders into miners. All they need to do to collect interest rate is to leave their wallets running and connected to the PoS network and participate in the confirmation of transactions. Wallets which stay online for extended periods of time are called full nodes. Staying online seems to be a rather simple requirement. So it comes as quite a surprise that PoS coins tend to suffer from an insufficient number of full nodes. This seeming paradox can be explained by two reasons.

First, in typical PoS networks, coin age equals the number of coins times the holding period. It doesn't matter whether a wallet is connected to the PoS network during the holding period. An offline wallet accumulates coin age at the same rate as an online one. The only difference is that an always-online wallet receives block rewards in a fashion that's more evenly spread out over time while an occasionally-online wallet receives block rewards in a few concentrated clusters. This difference alone is insufficient to encourage most stakeholders to stay online.



Second, it's commonly perceived by average PoS stakeholders that running wallets and staying connected for long periods of time significantly increases security risk. This was a particularly grave concern when early versions of PoS wallets didn't support wallet passphrases during mining. Since then there has been work to reduce the security risk.

By considering the two reasons above, an average PoS stakeholder tends to make the rational decision of connecting to PoS network only sporadically and infrequently. The lack of a sufficient number of full nodes can result in a higher risk of a security breach on PoS networks.

2.2.4 Mining on Multiple Forks

In PoS mining, each stakeholder spends coin age while looking for the next valid block. If another stakeholder finds a valid block first, the coin age consumed in the unsuccessful attempt is fully reimbursed.

Forks do happen on all distributed networks of cryptocurrencies. PoW addresses this issue by enforcing at protocol level that the blockchain with the largest sum of difficulty always wins. This allows all the nodes on the network to converge on a consensus rapidly. Miners all have a clear incentive to mine blocks only for the most difficult blockchain. Mining for any other fork is almost guaranteed to be wasteful.

The situation is very different when it comes to PoS. When there are multiple forks on a PoS network, by the nature of the blockchain, a stakeholder has the same stake replicated across all the forks. Technically the stakeholder can simultaneously mine on all these forks by running multiple copies of the wallet. What causes the biggest trouble is the fact that PoS protocol picks a winning blockchain based on length. And the length of a blockchain in a decentralized network heavily depends on timing. It can be quite common for different subsets of the network to have different ideas about which blockchain is the longest while the information is still being propagated.

The lack of synchronization of network time further complicates it. It's a much less robust way, compared to PoW, to reach a consensus. PoS can't use the sum of difficulty in blockchains as the criteria for chain selection because difficulty in PoS is adjusted by each stakeholder based on their consumption of coin age and therefore remains local knowledge. There is no network-wide agreed-upon block difficulty.

When stakeholders on PoS networks find it difficult to pick the blockchain winner, they have the incentive to “bet on all horses" by simultaneously mining on all the forks. This significantly aggravates network security. Most PoS coins alleviate, but don't solve, this problem by enforcing “duplicate stake detection" at the client wallet level but not at the protocol level. They also argue that in practice the financial rewards for multi-fork miners are small enough to deter such attempts.

2.3 Proof of Stake Velocity (PoSV)

2.3.1 What is the Velocity of Money

The velocity of money is the frequency at which one unit of currency flows through an economy while being used by members of the society within a given time period[13]. All else being equal, a higher velocity of money

$$V_T = \frac{nT}{M}$$

[13] Joshua Kennon. The Velocity of Money for Beginners. 2012

indicates a more flourishing economy, richer members and a healthier financial system. The formula to measure the velocity of money in a given time frame is the following one:

Where VT is the velocity of money; nT is the aggregate notional of transactions and M is the total amount of money in circulation. In an economy, we can also replace nT with nQ which is the nominal national or domestic product. In other words, given a fixed amount of money in circulation, the velocity of money must be increased in order to increase the size of the economy.

2.3.2 Higher Velocity for A Better Economy

The vast majority of the drawbacks of PoW and PoS aren't due to flaws in technical design but the disconnect from the economic and social aspects of being a real currency. It's fair to say that most cryptocurrencies are created as technological products but are “mis-sold" as currencies. PoSV builds upon the strength of PoS and introduces new features to address its flaws. PoSV is designed to encourage ownership (Stake) and activity (Velocity), the two main criteria for being a social currency.

It must be emphasized that PoSV is designed specifically for the digital social currency Reddcoin and is not intended to serve as a drop-in replacement for other cryptocurrencies that don't share the same economic and social goals. PoSV should be evaluated as a piece in the Reddcoin ecosystem and not stand-alone.

"Coin Age" and "Transaction Frequency" are the game changers, when it comes to expanding the benefits of a "Social Cryptocurrency"!

Given a fixed amount of coin, coin age is calculated as a function of time. Let's denote this function the coin-aging function. The form of the coin-aging function is of ultimate importance. It not only decides the growth rate of coin age as a resource over time via its first derivative but also decides the utility function of stakeholders. The main limitations of PoS, too much incentive for hoarding and too little incentive for staying online, result from the fact that the form of its coin-aging function is linear. The linear form leads to a constant coin age growth rate and a utility function that disobeys the law of diminishing returns.

Changing the form of coin-aging function has a profound impact. For example, let's assume coin-aging function in PoSV is an exponential decay function. The coin age growth rate gradually decreases with time. The exponential decay constant is chosen to achieve a particular half-life such as 1 month. Each coin accumulates one coin day per calendar day during the first month, half a coin day per calendar day during the second month, a fourth of a coin day per calendar day during the third month, etc. As the holding period of a coin approaches infinity, the total accumulated coin age asymptotically approaches 2 coin months.

This exponential decay function dramatically changes stakeholders' incentives. New coin accumulates coin age at a much higher rate than stale ones. With a fine-tuned half-life, PoSV encourages stakeholders to be active in moving their holding, either by mining/staking or transacting with counterparties, both of which increase money velocity and improve the health of the Reddcoin economy.

Stakeholders are also encouraged to stay online and contribute to verifying transactions on the PoSV network. The asymptotic limit of coin age due to exponential decay function provides extra security for the network. The maximum amount of coin age a stakeholder can earn now equals coin amount times twice the half-life.

This significantly increases the difficulty of any successful 51% attacks.

The coin-aging function can take on other forms. Linear and exponential decay functions are both monotonic. What about trigonometric functions which are non-monotonic and periodic? Non-monotonicity produces a positive and negative growth rate of coin age at different points in time which along with periodicity translate into rewarding and penalizing holding with a seasonal pattern.

This can be used to fine-tune the seasonality in money velocity. The bottom line is that PoSV is designed to accommodate different forms of coin-aging functions in order to implement the necessary monetary policies in the Reddcoin economy. To alleviate the problem of mining on multiple forks, PoSV helps the nodes to reach a quicker consensus by giving preference to the head block with the largest sum of coin day spent among all the transactions.

3 Economics

There has been extensive economics debate about Bitcoin through its history. Most economists remain unconvinced of Bitcoin's status as a real currency. Reddcoin and PoSV are designed to address some of those concerns and offer new angles to reexamine these fundamental questions.

3.1 Medium of Exchange

There is largely consensus on Bitcoin's function as a medium of exchange. In fact, almost all the merits of Bitcoin talked about today boil down to how it acts as a better medium of exchange, e.g. global reach, lower fees, much quicker transaction and easy to use. However, the fact that the Bitcoin network must be secured by “mining" which expends real resources (energy) is considered by many economists to be a drastic retrogression[14] - a retrogression that Adam Smith scorned at in his immortal work The Wealth of Nations written in 1776. By comparison, PoSV and PoS mining/staking require little energy consumption and can be done by any average user on any computer and even mobile devices.

[14] Paul Krugman. Adam Smith Hates Bitcoin. 2013

3.2 Unit of Account

Many economists point out that Bitcoin cannot be used as the base currency for accounting or tax-reporting and therefore fails as a unit of account. ***Interestingly, the German Finance Ministry has officially classified Bitcoin as a unit of account.*** More and more merchants are accepting Bitcoin for payment. Especially in the world of cryptocurrencies, Bitcoin has assumed the special status of a reserve currency and is the choice of the denomination for more and more goods and services. Reddcoin and PoSV bring a whole new question: what is the “unit of account" for human social interactions if any?

Currently, social interactions are quantified in different ways on different social networks. On Facebook, it may be measured in the number of Like and Share; on Twitter, the number of retweets; on Amazon, the number and quality of product reviews; on blogs and forums, the number of posts and replies. The total lack of a universal yardstick makes it impossible to measure and compare social interactions in heterogeneous context. In other words, there is no useful unit of account for human social interactions right now. Social influence remains a significant yet opaque asset.

Reddcoin was created to fill this gap by becoming the first digital currency integrated with all major social networks, extensible to any others, and beholden to none, and serving as the “unit of account" for social interactions in the digital age. Inside the distributed ledger of Reddcoin, transactions can be interpreted not only in purely financial terms but also as proxies for human behaviors. Researchers in social sciences have long been looking for a way to track, organize and study human social behaviors on large scales. Reddcoin offers a unique global platform for these areas of research and opens up new possibilities for value-added services and an entire ecosystem of derived value from that insight and activity.

Reddcoin was created to be "Integration Agnostic", so it does not require integration with any Social Media tech team - to work.

3.3 Store of Value

Economists are largely skeptical of Bitcoin's function as a store of value. They compare Bitcoin with gold and US dollars and point out its lack of a fundamental floor of the value [2][15]: Underpinning the value of gold is that if all else fails you can use it to make pretty things. Underpinning the value of the dollar is a combination of (a) the fact that you can use them to pay your taxes to the U.S. government, and (b) that

[15] Brad DeLong. Watching Bitcoin, Dogecoin Etc... 2013

the Federal Reserve is a potential dollar sink and has promised to buy them back and extinguish them if their real value starts to sink at (much) more than 2% per year. Placing a floor on the value of Bitcoins is what, exactly?

PoSV, PoW or PoS by themselves don't provide a fundamental floor for the value of a cryptocurrency. However, Reddcoin, the digital social currency that PoSV is specifically designed for, does enjoy a floor of its value due to its aim to function as the global reserve currency of human social influence. Humans are by nature social animals. Social activities are embedded in the very fabric of societies. As Aristotle famously pointed out in Politics, “*Society is something that precedes the individual. Anyone who either cannot lead the common life or is so self-sufficient as not to need to and therefore does not partake of society is either a beast or a god*.”

Based on Aristotle's insight,
underpinning the value of Reddcoin is simply
its utility of helping humans being human.

More on that in section 6!

3.4 Deflation vs Inflation

Any discussion of a monetary system is incomplete without discussing inflation. Bitcoin and many of its variants were created with a deflationary model in which the total quantity of the cryptocurrency is capped. In effect, Bitcoin has created a modern digital version of the gold standard world in which the money supply is fixed rather than subject to increase via printing press.

Bitcoin advocates believe deflation is a virtue by preserving the value of Bitcoin versus inflationary fiat currencies and thus making it a better store of value. Bitcoin price has indeed soared in the last few years, further validating the merit of deflation in its supporters' mind. However, deflation and a soaring price both provide strong incentives for people to hoard Bitcoin rather than spending it. Indeed, according to this paper[16], as much as 64% of Bitcoin was never spent in 2013. To make matters worse, prices of goods and services when measured in Bitcoin have plunged; the Bitcoin economy has in effect suffered a major depression[17].

[16] Meiklejohn, Pomarole, Jordan, Levchenko, McCoy, Voelker, and Savage. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. Internet Measurement Conference, 2013

[17] Paul Krugman. Golden Cyberfetters. 2013

All Cryptocurrencies are not the same when it comes to Economic Functionality. The details matter when it comes to Adoption & Usability.

PoS and PoSV both employ an inflationary model with a fixed nominal interest rate. For example Peercoin adopts a nominal interest rate of 1% per annum compared to PoSV's 5%. Central banks in developed countries, e.g. Bank of England, European Central Bank and Federal Reserve, have a long-term inflation target of around 2%. PoSV chooses 5% because Reddcoin, as the digital social currency, should encourage more spending, i.e. social interactions, than other cryptocurrencies which do not share this goal. Also given the global nature of social networks which involve users in both developed and emerging markets, 5% seems to strike the balance when addressing both monetary and non-monetary causes of inflation[18]. The monetary system of Reddcoin is not created to make individuals who hold money rich, but to facilitate transactions and make the Reddcoin economy, as a whole, rich in a much different sense.

4 Digital Social Currency

4.1 Social vs Commercial

A commercial currency is the most common form of currency. Its main function is to facilitate transactions in exchange for goods and services. Bitcoin and its variants have been pushed as the latest innovation of commercial currencies and compete head-to-head with fiat currencies, such as USD, GBP and EUR, for shares of commercial transactions in the global economy.

A social currency is of an entirely different nature. According to Wikipedia[19]: Social currency is a common term that can be understood as the entirety of actual and potential resources which arise from the presence in social networks and communities, may they be digital or offline. It derives from Pierre Bourdieu's social capital theory and is about increasing one's sense of community, granting access to information and knowledge, helping to form one's identity, and providing status and recognition.

Very recently, a small but growing number of companies have come to embrace the concept of “social currency", allowing customers to pay via Facebook posts, Twitter tweets and other social media content. However the lack of a yardstick to measure the “fair value" of social media content and influence is the

[18] Nathan Lewis, This Is Why We Want 5% “Inflation”, Forbes.com 2018
[19] Wikipedia, https://en.wikipedia.org/wiki/Social_currency, last edit 2018

main obstacle. To our knowledge, Reddcoin is the only digital social currency that was created, designed and has continuously evolved to become the “reserve currency" of people's social interactions.

Reddcoin has two main objectives:

1) To concretize and quantify one's intangible asset of “social influence”, and
2) To facilitate social interaction especially for content creators within & between social networks, both on- and offline.

Reddcoin doesn't compete with commercial currencies, fiat or digital, but rather strives to complement them[20]. Merchant support is encouraged, and on- and off-ramps to fiat and sensibility are being pursued, especially when the commercial activities form parts of a collective social experience.

Reddcoin does not compete with commercial currencies, fiat or digital, but rather strives to complement them!

But the social aspect will always remain the utmost focus of Reddcoin. Reddcoin is, at bottom, about sharing oneself, about sharing one’s love, about being part of a ReddHead community that welcomes, and does not limit or judge.

The three most important assets in the ecosystem of Reddcoin are brand, community and infrastructure. Reddcoin developers have always gone to great lengths to create a brand that's professional, friendly and consistent.

Great care is taken to foster a community of “ReddHeads” that shares a clear long-term mission and the same set of values of being friendly, helpful, generous, caring and rational.

All system infrastructures are built with special emphasis on providing a uniform, simple and secure user experience.

Again, Reddcoin is, at bottom, about sharing oneself, about sharing love.

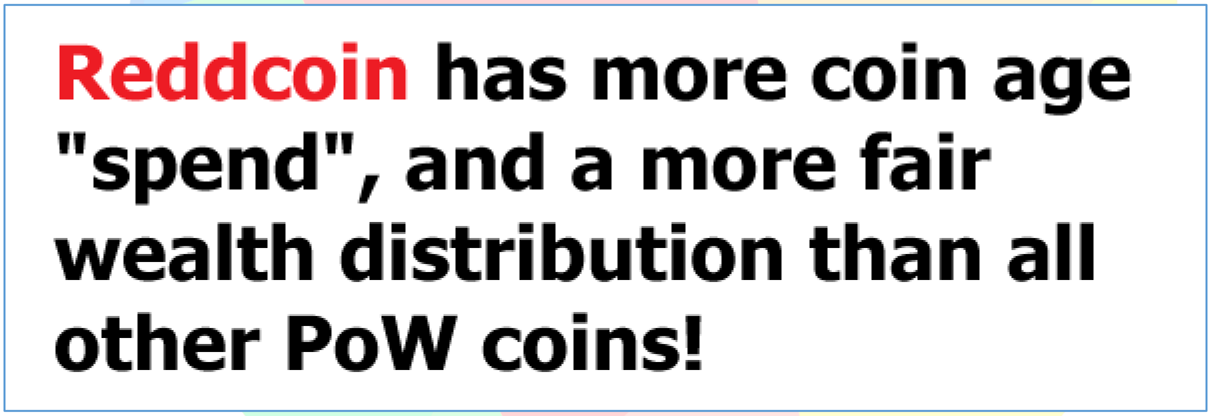
[20] Pfajfar, D., Sgro, G. and Wagner, W. ‘Are Alternative Currencies or a Complement to Fiat Money? Evidence from Cross-Country Data’ *International Journal of Community Currency Research* 2012

NOTE: Even five years later, this branding and ethos still seems to hold true and lasting value for Reddcoin. Some competitors have positioned as alternatives to more established coins like RDD and BTC as well as fiat for payment and transactions, but none have fit the model of a social currency. We see this as a validation of the above tenets and beliefs.

4.2 Transition from PoW to PoSV

Reddcoin was launched in January 2014 and as of the writing of the original White Paper, was still using PoW. The chain transitioned to active PoSV in 2014 and has been performing objectively well in the five years since. This Paper is intended to form the foundation of the upgrade to PoSV v2 in 2019.

Since the very beginning, Reddcoin has been distributed to a large and diverse user base through multiple channels that include one of the very few successful and honest Initial Public Coin Offering (IPCO) (liquidated by the original team in 2015 in Reddcoin's transition to a volunteer team), mining, trading on multiple exchanges, a genuine community promotion events, generous giveaways and user tipping on multiple social networks such as Reddit, Twitter and Facebook. Reddcoin stakeholders include people from hundreds of countries, with diverse background, age and interests.


Reddcoin has more coin age "spend", and a more fair wealth distribution than all other PoW coins!

At the original time of writing (2014), according to information at http://bitinfocharts.com, Reddcoin had a fairer wealth distribution per wallet address than all the top cryptocurrencies such as Bitcoin, Litecoin, Dogecoin and Peercoin. Reddcoin also had 2 - 3 times more coin age spent then than all the other PoW cryptocurrencies. Reddcoin, without PoSV, was already the currency with the fairest stake ownership and the highest monetary velocity. Over the ensuing years, that place in crypto history has only been maintained and improved with products like ReddID, Redd POS and others.

4.3 Hard to Clone

There is no shortcut to cloning Reddcoin. In particular, the clone cannot adopt PoSV from inception because, as discussed in section 2, the mere knowledge of the eventual adoption of PoSV or PoS will lead to people hoarding from the very beginning. To achieve a fair and wide distribution, an element of surprise at protocol level plus dedicated efforts at community level are both indispensable. Reddcoin's existing brand, community, infrastructure and the publication of this paper make it very difficult to duplicate what has already been achieved. NOTE: *Even more so, we believe, with the update to PoSV v2.0 in 2019.*

5 Conclusion

We have implemented “Proof-of-Stake-Velocity (PoSV)” as an alternative to “Proof-of-Work (PoW)” and “Proof-of-Stake (PoS)”. We started by going through all the major drawbacks of PoW and PoS and then showed how PoSV significantly reduces the wastefulness of mining, eliminates mining arms race, averts the threat of multipools and ASICs, avoids the inherent conflict of interests by ASIC manufacturers, introduces new forms of coin-aging functions to discourage hoarding and encourage spending and greater contribution to the network. Following a multi-year real-world observation period, we have planned some small adjustments to the core protocol to further realize the promise of Reddcoin’s ecosystem. General concerns by economists toward cryptocurrency were discussed and addressed in light of the recent development of Reddcoin and PoSV. In particular, Reddcoin continues to be well positioned to fill the niche of a digital social currency that's tightly integrated with human social interactions and acts as the yardstick to concretize and quantify people's intangible asset of social influence, as well as providing dynamic and live insight into social network content and publishers of note intrinsic to the system as a natural follow-on to backend analysis of tipping data. All of these facets taken together offer Reddcoin the “perfect storm” of a unique and compelling use case, a technological advantage, and a growing and genuine community to support Reddcoin’s evolution and continued success.

6 Five Year (2019) Retrospective

This paper was originally written in 2014 as part of Reddcoin’s protocol and consensus evolution. As the blockchain and protocol have evolved, so has the team and those responsible for advancing the Reddcoin mission and goals, an integral part, we have found, of making Reddcoin a successful social currency. Though RDD has been an actively used and traded currency and remained in the top 100 ranked crypto-assets throughout this period, recognized by **BITA50**[21] and ALT100[22] crypto-indices, we have observed some overarching and addressable issues in the design and mechanism of PoSV. Thus, we submit for evaluation the new proposed version, PoSV v2.

6.1 Analysis, Discussion & Proposed Enhancements – “Introducing PoSV v2.0”

During the last five years of Reddcoins PoSV v1.0 existence and operation, the targeted growth of the network was targeted at a conservative 5% annual growth, however the observation and analysis of this period of time has been measured to closer to the order of 2%[23]. The variation is due to the nature of PoSV coinage weighting and the clearly noted tendency for some large stakeholders to intentionally fail to stake.

In the larger economic scheme, that growth has been coupled with a slower-than-expected penetration of crypto concepts, whether Reddcoin or other, into the mainstream. We have discovered that with more users and more velocity and activity, come pragmatic concerns on multiple fronts.

[21] Reddcoin officializes its entry into the BITA50 Index!, medium.com 2018

[22] RDD included in ALT100 crypto-index, 2018

[23] Analytic tools and blockchain data available at https://bitinfocharts.com/reddcoin/. In addition, a supporting Technical Analysis document will be published in Q3 2019 by the Reddcoin team.

1) How to more appropriately incentivize online staking to take place to keep the network as secure as possible, with as many online nodes as possible.
2) How to facilitate the onboarding of new users and introduce users to network functionality without requiring excessive cost on their part, but still limiting spam and squatting on ReddID and other product lines.
3) How to provide a non-traditional funding mechanism to team and development activities in keeping with the community-driven and anti-corporate philosophy of Reddcoin, in the absence of a profit-seeking motive to attract traditional VC, angel or other investors.

We believe that with two minor adjustments to the current unique PoSV protocol that we can achieve our goals on all of these fronts and more, thus fulfilling more steps on the path the Reddcoin's success as the pre-eminent social currency.

1) **Enhance regular user stake rewards to multiples of what they are to drive more users to stake and secure.**
2) **Provide a funding stream from the network to facilitate development and ecosystem work directly from that pool of increased user rewards.**

6.1.1 User Stake Payment Returns Enhancement

At present only a small proportion of wallets on the Reddcoin network are staking online and thus actively securing the network and establishing consensus on the correct chain. As of this writing, that proportion is ~20%, or 1/5 of the network.

We propose in PoSV v2 to multiply the current reward scheme by the inverse of that value, in order to cause more users and wallets to want to stake and capture these enhanced rewards, while securing the network.

The multiplier will be recalculated with each block and will apply to successfully staked and accepted blocks, unless and until 100% of wallets are online and staking at which time the expected reward s can be considered to be at 1:1.

In today's example, with only 1/5 of the network staking, the stake reward would be multiplied by 5. If a user would normally have received 100 RDD for their reward based on today's protocol rules, with this change in place, today they would receive 500.

If, hypothetically, by next week, lots of users decided to stake online and the Reddcoin network was at a staking participation level of 50%, or ½, the multiplier would still be 2x today's "normal" rewards.

In summary, this change can be expected to multiply current rewards by anywhere from 1-10x over current, ensuring the network grows at the desired 5% annually, no matter how many stakers are active online, and that those who are active are suitably rewarded more.

Economic opinion seems to give us to expect that these enhanced stake rewards and more globally available coins may have a negative price pressure effect in terms of absolute market price, but as the value of RDD itself is in its social and shareable/spendable value and has never been meant as a speculative tool, we do not see that as a negative. In addition, it may also be noted that “a growth in the money supply does not necessarily lead to inflation **if there is an equal growth in the value of the goods and services in an economy**.”[24]

We expect that the overall network security and participation enhancement, as well as further inducement to avoid hoarding, will bring users to the network to stake and spend, especially as core wallet software itself is enhanced and products requiring RDD are released, such as ReddID.

6.1.2 Reddcoin Development Fund

As this proposed staking change above will provide all users of the Reddcoin blockchain with more available coins, and community sentiment in the form of donations and crowdfunding have supported this approach and the Core team’s work throughout the past five years, the team has also decided to integrate an option to support the Reddcoin development team and ecosystem development efforts directly into the core protocol.

6.1.2.1 Operational funding for development activities

To date, the team has functioned as a loosely democratic consensus of involved individuals. All significant actions are executed as approved by team consensus. We have agreed internally that in order to make Reddcoin a success, that there needs to be a reliable if minimal, revenue stream behind the development work to pay for operational costs, salaries, legal and other fees, marketing/PR, listings and other engagement with the commercial financial tech world.

These costs have been borne by donations of community members as well as directly by team members to date. But this model in the long term is not sustainable, regular, or fair. Instead, we have determined that simply applying a small percentage as an operational fee while staking in the “enhanced” mechanism above, in official wallets that this will provide an adequate operational fund for all of the above needs, essentially future-proofing the Reddcoin network and allowing it to grow organically by self-funding.

These funds will be under the control of the dev team as a tool for growth and will be reported on regularly to the community. We expect the fee to be set at 8% of enhanced staking rewards (ESR) after economic and tokenomic modeling.

That is to say that after the stakes have been multiplied as above, that the above donation/fee will be deducted and sent to the dev wallet directly. The net result as designed is that users will see multiples of current earnings with their same stake, and the dev team will be able to use that revenue to drive other less obvious aspects of the ecosystem to success. And the network will grow at the expected and designed-for 5% annually without any changes to that core metric.

The team will publish periodically an account of how these funds are to be or have been, spent and are planning to build more of a governance and voting mechanism around that in the future. We are aware that such decisions should be democratized and decentralized to stake-holders, and will be working toward that direction will full openness, honesty, and transparency, as we have the past five years since our inception. We welcome suggestions to that as well as any other parts of our work.

[24] C Daly/Blockchannel, Understanding Inflation in Crypto Networks, medium.com, 2019

6.1.2.2 Portion of the fund to support philanthropic activity and other viable-and-vetted needy causes.

A major component of the Reddcoin and Reddhead community is the spirit and loving philosophy we have tried to build. That includes both making it easier for users to find and reward socially positive efforts by others individually, and to highlight and reward such efforts as much as possible with the power of the ReddHead community together.

It is for that reason we are committing to spend at least 10% of received funds toward such "social mandate" causes such as positive social events, individuals, groups and others as seem to deserve it, separate from other promotional or marketing activities the team might be sponsoring. Charity, philanthropy, and altruism have always been, and should always be, a part of the crypto and specifically ReddHead community, and we see this as an opportunity to support those deserving of help both within and without that community.

We hope to have components of this effort built into both the Reddcoin website and ReddID and other products as they evolve to spotlight those types of truly deserving causes, and will target the above percentage towards those goals.

6.1.2.3 Reimbursement/Repatriation Fund

For users who've verifiably lost funds, either through no fault of their own or those outside their personal control that could not reasonably have been avoided. The team and/or community will need to establish governance around this as well as above philanthropic efforts, but observed human behavior shows that no one is perfect, and allowances should be made if possible.

The team has received many inquiries that would be subject to this fund if available, some entirely legitimate. This would allow at least a degree of positive outcomes when funds have been lost or otherwise made inaccessible. We commit to spending at least 10% of collected funds toward a fund of this nature meant to make whole, or fairly resolve, individual issues on a case-by-case basis for user support. We do not expect that this will provide "insurance" for the entire community, it will certainly take some of the risks from users who've made mistakes with smaller amounts, that otherwise could not be restored.

As we all have been beginners at one time, and have all lost coins on our journey, it is the feeling of the team that dedicating a proportion of incoming assets to this purpose, as well as using those funds to more efficiently enable user support in general, will make our community a much more welcoming, forgiving and friendly one than the typical crypto community, as it has been since the beginning, of course.

Reddcoin is a vibrant top 100 cryptocurrency, and enjoys a diverse, inclusive and open-minded community, now five years since our humble beginnings. Our technology is unique and our community welcomes all willing to engage socially. The Reddcoin Core team is pleased to bring you these next steps into Reddcoin's future as the pre-eminent as well as the original social currency of the future.

Stake On!!

reddcoin
LinkedIn
facebook
YouTube
last.fm
digg
orkut
redd id

WWW.REDDCOIN.COM