PULSE: Block Creation Adjusting to Network Activity in Quarkbar

f0o[#], JonesD[*]

Cryptocoin Revival Foundation

[#] f0o@cryptocoinrevival.com

[*] jonesd@cryptocoinrevival.com

www.cryptocoinrevival.com

Abstract— **PULSE is an effective feature that adjusts the creation of blocks in the blockchain to the transaction activity of the network. Blocks are created according to a slower time flow, and when a sufficient amount of transactions occurs a special PULSE BLOCK is created. The transaction will not have to wait on the slower creation, but will be sent immediately. This enables the block creation to slow down and in effect lower mining rewards when mining power is less necessary. PULSE will enable mature coins to slow down coin creation and use the remaining to be created coins to reward necessary mining that is needed for the flow of transactions.**

Keywords— altcoin, bitcoin, crypto currency, Quarkbar, economy, pulse

I. Introduction

Since the creation of Bitcoin in 2009 [1], the crypto currency economy has grown massively. At the time of writing, the combined market capitalization of all crypto currencies combined is projected between eight and nine billion USD[1]. The rise of value in Bitcoin lead to the creation of over 500 alternative crypto currencies, altcoins. The success of these altcoins relies on a combination of their (a) algorithm, (b) mining method, (c) scarcity, (d) privacy, (e) speed, (f) active developer and (g) strength of the supporting community.

One of the main features of these new coins was to speed up the speed of transactions. Where Bitcoin creates a block every ten minutes, new coins brought this down to several blocks a minute. On the one hand, this created a very rapid transaction speed, the network needed to create a lot of new coins as an incentive for miners to keep the network alive. The large influx tended to lower the price over time as new coins kept being added at a consistent rate.

To deal with this problem, the Cryptocoin Revival Foundation (CRF) has created a block creation feature that takes network activity into account. Just like animals, crypto currencies have a certain set amount of heartbeats (blocks) to use in their life. There is an inverse relationship between the rest heart rate and life expectancy [1]. Animals tend to preserve these precious heart beats to flee from predators or hunt for prey. During these active periods they require a far higher pulse. To prevent too much strain on their body, the animals will have long periods with low activity and low pulse to compensate. Crypto Currencies don't apply this principle yet. They produce the blocks at the same rate, regardless of the activity of the network. This requires coins to either have a slower block creation time or increase their number at a rapid rate.

PULSE will simulate the way the animal kingdom efficiently manages the way heartbeats are used. This block creation feature will create blocks at a slow rate, to ensure users the network is still synching. Once the network is being used for a sufficient amount of transactions, it will create a new block instantly. This will ensure that most of the blocks are actually used for activity, In the upcoming pages, the current inflation problem of the crypto currency economy will be discussed. Next to this, it will show how PULSE will deal with these problems.

II. Crypto Currency Economy

Crypto currencies are a system for electronic transactions that do not rely on trust [1]. This makes it possible to send transactions without going through a financial institution. At the basis of this lies a framework of coins that are made from digital signatures, enabling strong control of ownership. A

[1] Value retrieved from http://coinmarketcap.com/all.html

peer-to-peer network uses proof-of-work to record a publicly available history of transactions. This makes it impractically hard for an attacker to overtake a sufficiently high amount of the network computational speed to alter transactions. The users of the network "vote" with their CPU power which new block are valid and which ones are invalid. This leads to a block-chain of transactions that are agreed upon by more than 51% of the network.

A.. Value

The value of crypto currencies fluctuates rapidly. With a limited amount of coins to be created, inflation is less likely compared to fiat currencies. Due to the rapid rise in value, people tend to hoard Bitcoin instead of spending it [1]. This hoarding in turn decreases the volume of bitcoins that are used for transactions, making them more valuable. This is known as a 'deflationary cycle' as people are halting spending the coins, hoping for the prices of goods to drop even further. With fiat currencies this usually reaches a bottom, since people still need to use the money to pay for primary costs like living and food. Since most altcoins are not used for these kinds of payments, the deflationary cycle can go on for a much longer time, leading to massive increases in value.

Besides the deflationary issue, altcoins also have an inflationary/ longevity problem, where a speedy network is established by creating blocks at a fast rate. By having block times that are many times quicker than Bitcoin, the market is flooded with newly created coins. This does not only lead to a constant inflation of the amount of coins, it also shortens longevity as the total amount of coins will be reached quickly.

Another factor in the value of altcoins is established is by the amount of hashing power it takes to mine new blocks and create new coins. Once more nodes are contributing power to the network, it becomes less likely for an individual miner to find a block. By contributing more mining power, this will become more likely, but will also increase the costs for the miner. This leads to an mining cycle that is currently the backbone behind most altcoin value. In an upward mining cycle when more miners contribute hashing power to the network, it is more difficult to mine new coins, pushing the price upward. In a downward cycle, the amount of mining power is decreasing, making it more easy to find a block, but also less expensive, pushing the price downward.

The final important aspect of the value is market trading. On a multitude of exchanges, crypto currencies are traded, leading to fluctuation in the price. Prices are influenced by emerging information about the coins, speculation about the future, moves by big players in the market and by pump-and-dump schemes. Due to the size of the markets, it is possible for big traders to steer the value of coins singlehandedly and create bull or bear markets. They can benefit from this by buying and selling at the right moments and further increase their coin holdings. This makes altcoin markets very vulnerable to huge price fluctuations.

With these four factors, the deflationary cycle, inflation/longevity issue, mining spirals and market speculation, the value of altcoins fluctuates heavily and can easily be pushed into an upward or downward spiral once one of these factors changes. The best way for altcoins to become more valuable is by focusing on their true purpose: being a medium for transactions.

B. Mining

Nodes of the network get rewarded for their contribution to the network As an incentive for nodes to support the network, there are several kinds of methods used.

1) Proof-of-Work: Most crypto currencies use proof-of-work [1] to stimulate people to contribute computing (mining) power to the network. Since new blocks can be found at random, the node that finds it will get the newly created coins and the transaction fees. With Proof-of-Work nodes get rewarded for their contribution to the network. Rewards are handed out at random, but more computing speed increases the chances on finding a block.

Once a coin increases in value, an upward mining spiral can occur, where the amount of hashing power increases and it becomes harder to mine new coins. This makes it not worthwhile to contribute to the network by mining via a wallet. The network mining moves to large mining farms. This makes it so hard to mine a block that natural centralization occurs and the amount of contributing nodes resemble an oligarchy. In case of Bitcoin, the recent risk of one of the major mining pools, Ghash.io[2], getting more than 51% of the network, turned the mining power of the network into a monopoly for a short period of time.

[2] http://www.coindesk.com/ghash-io-never-launch-51-attack/

The increasing difficulty in mining power during an upward mining cycle decentralizes the network and floods it with huge amounts of mining power it does not necessarily needs.

2) Proof-of-Stake: As an answer to the risk of centralization and waste of mining power, Proof-of-Stake was introduced. Instead of relying on large miners, the mining power was decentralized again and stemmed from the contribution of single members of the network. In return of partaking into the network by keeping the wallet synched and not moving their coins, users received a reward that was connected to their amount of coin holdings.

The upside of this way of mining is that it prevents upward or downward mining cycles making the value of the coin more stable. It has several downsides to counter this, though. Proof-of-Stake rewards users for not moving their coins and for the amount they're holding. While countering one of the main reasons for price fluctuation, it strengthens another one hugely. Next to this, Proof-of-Stake tends to flood the network with blocks as it is creating new coins to reward miners for their contribution. This does not only makes the network less efficient, it leads to a constant inflation of the coin.

To counter the hoarding of Proof-of-Stake, Reddcoin announced they will improve this by introducing Proof of Stake Velocity [1]. With this improvement, they aim to also reward coin holders for their activity in the network.

C. Wrong incentives

The current way the altcoin networks function lead to deflation, inflation, mining cycles, market speculation and centralization. Instead of using the network for transactions, most of the effort is toward anticipation in mining and market trading of which coin might be growing rapidly. The continuous creation of blocks is a waste as many of the newly created coins have a majority of blocks that don't even contain transactions. This goes against the purpose of a decentralized currency and lead to hoarding, price instability, wasted mining power and centralization.

D. Wasted blocks in exchange for speed

One of the main advantages of crypto currencies are a limited amount of created coins, preventing inflation in the long run. On the short run, though, inflation is rampant. With every newly created block, new coins are created, directly decreasing the value of the coins that are already in existence. This would not be a problem, if all the blocks are used for transactions. Many blocks end up being empty, leading to a waste of created blocks as they were created solely to increase the amount of coins.

Bitcoin on average only creates a block every ten minutes, so newly created coins speeded up this block creation by having blocks every 2.5 minutes (Litecoin) or thirty seconds (Quarkbar). This speedier flow of new blocks leads to a lot of blocks generated remaining empty. For Litecoin, the number two coin on Coinmarketcap, 5-10% of the blocks is empty. Somewhat further down the list, you can find Darkcoin with around 10-15% of empty blocks, Vertcoin with around 30%, Fedoracoin with about 75% empty blocks and Frycoin even around 90%. This quick block generation leads to a quick increase of the amount of coins. Newly created coins are not used for necessary transactions, but wasted on unnecessary mining.

E. Value

The true value of crypto currencies is not in the mining power backing the coin, but in the usage of it. The flooding of the market with coins that are faster than Bitcoin or have more features, will not be fruitful when inflation is rampant, due to the large influx of coins in the early stages of these coins. The mining power must be preserved to support mining for blocks that contain transactions.

III. PULSE

Pulse is an answer to the current inefficiency of altcoin networks. The current incentives require a constant creation of new coins into the network (PoW) and stimulate hoarding of coins (PoS). Pulse, on the other hand, links the creation of new coins to the amount of network activity.

A. Block Creation

Instead of creating new blocks at a constant rate, Pulse adjusts its block creation to the activity of the network. When no notable transactions occur, the network creates new blocks at a very slow rate (for example one every ten minutes). When the network becomes busier, Pulse will create new blocks immediately once a certain threshold is reached. This will enable users to send transactions immediately, but not hand out mining rewards when the network is not very active.

This will link the mining rewards to the actual usage of the coin and counter up- and downward mining cycles. New coins will mostly be created when the usage increases, will it will slow down when a lot of people are hoarding the coins.

B. Adaptation to Coin Lifecycle

The speed of block creation can be adjusted during the life cycle of a coin. In the earlier stages it is important to have a speedy creation of new coins, to have a sufficient amount for usage. Once a coin reaches maturity, the speed of block creation can be adjusted to the amount of incentive that is needed by miners to keep the network up.

In the case of Quarkbar, where 75% of the available supply is mined, Pulse will make it possible to use the newly created coins mostly for when the network is active and not waste them on empty blocks.

C. Efficiency

Adjusting the network's required mining power to the usage of the coins, makes is very efficient. Tests have shown that the network can be easily supported by hashing speeds between 10 and 20kh/s. This is the equivalent of 1-10 solo miners.

D. Release

Pulse will be implemented into Quarkbar in the middle of July 2014.

IV. Technology

Pulse is a versatile feature that can be adjusted during the lifetime of a coin and is easy to implement.

A. Pulse Block Creation

Pulse represents a highly configurable set of constrains that a block must match in order to be allowed into the blockchain. In order to constrain the creation of Null-Blocks, Pulse provides a set of different switches that determine whether or not to allow a Block into the blockchain.

The rate switch is the most fundamental switch. This switch is triggered if the newly created block is N amount of time older than it's predecessor. The Rate switch is the backbone of Pulse, it keeps the blockchain updated and avoids 'Out-Of-Sync' issues that are being reported by several broken implementations of Proof-of-Stake coins. It is advised to have it set to a high value like 10-30 minutes.

On busy networks the Minimum-Rate Switch is almost as important. The Minimum-Rate ensures that there is no flooding of the blockchain by adding a minimum amount of time to be passed before a new block can be accepted into the blockchain. It will also cap the difficulty, further information of difficulty readjustments later on.

Transaction dependent sSwitches like Value, TX-Amount or Fee Switches are the core functionality of Pulse. Depending on the coin's desire, Pulse can be configured to trigger on any or all of these switches. All of these Switches obey Minimum-Rate if enabled:

- The Value Switch ensures that transactions of larger amounts of coins are processed nearly instantly. The Value is determined by the accumulation of all inputs in the proposed block. Due to the nature of the blockchain and crypto currencies itself it does not inherently matches the amount of coins that are being sent in a transaction. To allow algorithmic approaches to determine a more suitable Value factor, a developer can (re)write an own Value-function that will be used instead of a fixed amount.

- The TX-Amount Switch makes sure that in case a busy Network in terms of having many transactions being issued, disregarding of their Value, the queue of pending transactions gets flushed by accepting the block after passing the configured threshold. Note: this can allow a user to send a high volume of low-amount transactions in order to trigger the switch and thus allow creation of a pulse-block.

- The Fee Switch allows high priority transactions, i.e. with a high fee, to be accepted nearly instantly. This is especially useful for merchant and commerce as it allows very fast processing of at least 1 confirm.

B. Explicit or Implied Switches

Pulse can process switches in two different ways:

- Explicit: All switches apart from Rate have to be triggered to cause creation of a pulse-block.

- Implied: Any switch has to be triggered to cause creation of a pulse-block.

C. Factorial or Absolute Values

Pulse can interpret the values of transaction dependant Switches in two different ways:

- Factorial: the configured values represent a factor of the proposed BlockReward (excluding fees).
- Absolute: the configured values are to be interpreted as absolute values.

D. Implementation

The reference implementation of Pulse can be found at:

- https://git.voodoo.systems/crf/pulse (active development)
- https://github.com/CryptocoinRevival/pulse (mirror)

E. Difficulty and readjustment algorithms

Most coins depend on a non-linear difficulty readjustment function like Kimoto-Gravity-Well (KGW) or Dark-Gravity-Wave (DGW). These algorithms recalculate the difficulty of a block, or a set of blocks, upon the mean time between creation of the last N blocks. As Pulse remains an addition to Proof-Of-Work, it is subject to difficulty readjustments. By limiting the speed of block creation to either contain transactions of certain types or amounts it will already lower the difficulty over time. However, on busy networks this can still lead to an increase of difficulty if not used together with the limitation of Minimum-Rate.

The essence of Minimum-Rate is to freeze the difficulty on busy networks allowing the network to spare some miners. Please note that some difficulty readjustment algorithms do not solely rely on the time distance between the last couple of blocks but also add a quantifier depending on the current blockheight. Minimum-Rate will not be able to completely freeze the difficulty for these algorithms. Also note that even though Pulse lowers the difficulty of blocks over time, it is still required to have steady amount of miners in the transition phase from PoW-only into Pulse.

F. Conducted tests as time of writing

Whilst development of Pulse we set up two testnets, one Scrypt based and one Quark based. We pushed a combined force of 10 Megahash/sec on the Scrypt based testnet and ran on the Rate Switch only for 200 blocks using DGWv3 from the start on. We noticed that the difficulty remained extremely low and very steady rate setting of 5 minutes.

The Quark based testnet was powered by 4x 3 kilohash/sec and DGWv3. This testnet was used with a Rate setting of 5 minutes, a Min-Rate of 100 secs and several TX-Amount, Value and Fee settings that all have been triggered nearly continuously. Difficulty was still bearable for the 4 miners leveling out at 1 block per 90 secs. By the time of release of this paper there will be an open test using QuarkBar testnet. Feel free to join. More info about it in our IRC-Channel at freenode.net #coinrevival.

V. Conclusion

PULSE is an effective measure that adjusts the creation of blocks in the blockchain to the transaction activity of the network. Blocks are created according to a slower time flow, and when a sufficient amount of transactions occurs a special PULSE block is created. The transaction will not have to wait on the slower creation, but will be sent immediately. This enables the block creation to slow down and in effect lower mining rewards when mining power is less necessary. PULSE will enable mature coins to slow down coin creation and use the remaining to be created coins to reward necessary mining that is needed for the flow of transactions.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf. [Accessed 2014].

[2] W. Z. G. Q. Zhang, "Heart Rate, lifespan, and mortality risk," *Ageing research reviews*, vol. 8, no. 1, pp. 52-60, 2009.

[3] J. Surowiecki, "Technology Review," MIT, [Online]. Available: http://www.technologyreview.com/computing/28392.

[4] L. Ren, "Reddcoin," 2014. [Online]. Available: http://www.reddcoin.com/papers/PoSV.pdf. [Accessed 21 06 2014].