Karbo — New Decentralized Medium of Exchange

Whitepaper
version 1.0

Sberex, Aiwe, Zawy

May 30, 2018

Abstract

Devoted to the two-year Karbo anniversary!

There are few thousands crypto assets already present on the market. Nevertheless quantity does not mean quality. Crypto assets if we look at the top 10 of the list by capitalization still are represented by projects with limited or fixed supply, oriented on deflationary model with extremely high volatility. Still crypto assets are far away from mass adoption as a medium of exchange but they are more and more popular as a store of value. Thus fiat money are used by everyone on everyday basis leaving for crypto assets small space for nontraditional investments. Nevertheless there are few projects in crypto space pegged to fiat currencies like USD Tether, but it is difficult to call them a truly decentralised entities. By nature these projects are looking like fully centralised traditional financial companies. Which means that there is a niche and demand on the market for stable medium of exchange which will be decentralised and will operate without oracles or trusted parties.

In Karbo project we set a goal of creating such decentralised, community oriented medium of exchange, a stable cryptocurrency with low price volatility by introducing new to crypto world technics of regulating coin supply to stabilize its market price and exchange rate.

Karbo started on May 30, 2016 and has been developed as anonymous medium of exchange with **no premine and no instamine** based on CryptoNote protocol and CryptoNight Proof of Work (PoW) consensus algorithm [1]. Karbo is not an ICO, it has its own blockchain with classic PoW reward distribution. They key principle of CryptoNote is adaptive parameters. Karbo already has adaptive block size limit and difficulty. Hereby we describe forthcoming changes to make adaptive emission, minimal transaction fee, monetary deposit interest rate to achieve our goal of becoming low-volatile exchange medium or stablecoin.

The idea of so called stablecoin is not new and we were inspired in our work by the following authors: Vitalik Buterin [2], Ferdinando M. Ametrano [3], Vavrinec Cermak [4], Mitsuru Iwamura [8], Yukinobu Kitamura [8], Tsutomu Matsumoto [8], Kenji Saito [8], Adam S. Hayes [10].

Donate and support Karbo

Karbo address:
KgtzzKKLX2wDCpDNuNWEzg9p2uoTNkAZaKKzBNKhCroHRc575PzTSEX4xwS2dcLHRBX
DkHZeFBJkfUpkvmzB8Q5C58PxNXW

BTC address:
33t7CQTtFmaGf9vfDSJeteoaCGZxia1bmn

Karbo has no premine or instamine!
Community donations and initiatives are key source of Karbo development!

Your feedback and ideas are highly appreciated at: karbocoin@gmail.com

Contents

1. Introduction

“We have always had bad money because private enterprise was not permitted to give us a better one”
“Denationalisation of Money”
Friedrich von Hayek, Nobel Prize-winner economist

In a centralized economy, fiat currency has an unlimited supply. It is at a central bank’s discretion to inject money into or withdraw money from the banking system in order to match the growth of the economy. The central banks have distinct instruments of monetary policy, by which they control the monetary base. The most common methods are the open market operations, quantitative easing (QE), modifying the reserve requirements and changing the interest rates [4].

A good thing about crypto assets is that nobody owns it in the sense that it's a democratic arrangement through the distributed ledger we all own, the ownership of the block. And you can then buy parts of it — bits or part of the chain. In other words, you can't voluntary print more money, it has a discipline inherently built into the system [14].

But the negative effect of such rigid monetary rules specific for crypto assets is price volatility. For example, the price volatility of Bitcoin may reflect a rather naive understanding by the designers of the Bitcoin system that the monetary value of Bitcoin would be stabilized with a fixed money supply rule [8]. This belief is expressed by Bitcoin enthusiasts as follows *“Bitcoin permanently solves monetary inflation by removing monetary policy control from individuals and replacing it with rigid software. No matter how much energy is spent in creating new Bitcoins, there will never be more than 21 million unless an overwhelming majority (>95%) of the BTC community agrees, and I will never agree. If you own 50 million satoshis (.5 Bitcoin), you own exactly 1/42 million of the entire Bitcoin network. It’s impossible to measure the fraction of total USD or Euro you own because legacy currencies have no limit to the supply. Nobody is mandating that you use Bitcoin, and any upgrade to the network requires your approval if you choose to fully participate” [15].*

Apart of deflationary nature, the price volatility of crypto assets prevents their widespread adoption and actual usage as a **medium of exchange**, i.e. true money. Most businesses

need digital currency with stable value to be a basic **exchange medium** while *"...price volatility is bitcoin's Achilles heel". [4]*

Bitcoin system intrinsically manifests dual instability. The first instability stems from an inflexible supply curve of Bitcoin, which amplifies Bitcoin price volatility; the miners' revenue/reward fully absorbs any price changes. There is no price stabilization mechanism. The second instability comes from risks to the sustainability of mining. During a Bitcoin price boom miners engage in mining activity which guarantees the supply of Bitcoin. But during a Bitcoin price depression, no smooth way to induce exits from mining exists. The current situation of the Bitcoin system can be interpreted as a freezing equilibrium with dual instability [8] which makes Bitcoin and all other crypto assets with fixed coin supply bad medium of exchange.

It is obvious that if the system is decentralised we need to have decentralised means of monetary policy to stabilise Karbo valuation without any central authority which in classical case acts in a manual manner by decisions of central bank about interest rates and market interventions. This internal built in blockchain monetary policy represented by algorithm will allow us to make Karbo a new stable in value decentralized medium of exchange.

2. Crypto assets intrinsic value

“Everyone can create money, the problem is to get it accepted”
Hyman Minsky, an American economist

The target of stable coin design requires that this crypto asset has certain intrinsic value. Without this value it is possible to build stable coin only with exogenous factors involved. In other words manually managing its value by market interventions. There is no the only opinion regarding whether crypto assets have its own intrinsic value or not. Some authors [4] claim that crypto assets do not have any intrinsic value. Some authors on the other hand speak about this value represented by mining infrastructure [2, 8, 10].

Proof of Work (PoW) algorithm is usually criticised for excessive waste of energy on the one hand and it is postulated that crypto assets based on PoW consensus do not have intrinsic value [4] on the other. *“The criticism stems from the belief that Bitcoin violates Mise’s regression theorem of money because it is not backed by a commodity.” [4]* However mining infrastructure consuming megawatts of electricity is actually a commodity and if we accept the fact that it represents intrinsic value of particular crypto asset than we admit that mining infrastructure actually represents this commodity backing and energy spent on mining represents the real value of such an asset. The more real world resources we attract for mining the higher is crypto asset capitalisation. One can say that cryptocurrency is backed by the energy spent on its mining.

“Bitcoin production seems to resemble a competitive market, so in theory miners will produce until their marginal costs equal their marginal product. Break-even points are modeled for market price, energy cost, efficiency and difficulty to produce. The cost of production price may represent a theoretical value around which market prices tend to gravitate.

It seems to be the case that the marginal cost of bitcoin production matters in value formation. Instead of approaching bitcoin as a digital money or currency, it is perhaps more appropriate to consider it a virtual commodity with a competitive market of producers.” [10]

Any mineable crypto asset has a so-called positive feedback loop, which means that when the price of crypto asset decreases or block reward is decreasing, “mining” becomes less

profitable and some “miners” will be forced out of business. When there are less miners, the network automatically adjusts to decrease the difficulty of the cryptographic problems and therefore makes “mining” profitable again. In other words, proof of work mineable crypto asset is designed to make “mining” barely profitable on average [4].

The main idea of those who believe in crypto asset intrinsic value is based on the fact that production or mining being a competitive process represents the value which we are looking for. In that sense we can call Karbo and any other mineable crypto asset a ***commodity money*** backed by electricity and hardware expenditure consumed for network support. This approach will let us to find endogenous factors or data from blockchain to first estimate and than keep crypto asset value stable over time without relying on any third party or exogenous impact. This is the key point in building such a system because any third party involved in a process could be compromised and/or hacked over time.

Previous works like Ferdinando M. Ametrano’s proposal [3] relied on some exogenous commodity indexes consisting from crude oil and wheat, but we think that it makes sense to peg crypto asset to electric energy as a commodity stable in its value. Difficulty represents this energy spent on mining and therefore, from our point of view, difficulty [2] is endogenous factor which in the best way reflects crypto asset intrinsic value. Difficulty gives us real estimate of mining efforts expressed in electric energy and hardware commodity costs spent in real world on our crypto asset network support and emission.

Scott Roberts in his blog proposes a solution how to use blockchain data to determine the coin price being outside, real world parameter: *“Difficulty is exactly proportional to network hashrate, and network hashrate is closely proportional to coin price”* [6]. Our solution is based on his work, that finds confirmation by the research of Vitalik Buterin, published in his blog post [2], where he describes methods of the decentralized measurement problem. According to Buterin, there are two known major classes of solutions: *exogenous solutions,* mechanisms which try to measure the price with respect to some precise index from the outside, and *endogenous solutions*, mechanisms which try to use internal variables of the network to measure price [2]. We chose second method which was independently discovered and described by Scott Roberts.

The research of Vitalik Buterin confirms Scott Roberts’ idea [2]: to measure the price of a currency endogenously, what we essentially need is to find some service inside the network

that is known to have a roughly stable real-value price, and measure the price of that service inside the network as measured in the network's own token. Examples of such services include:

- Computation (measured via mining difficulty)
- Transaction fees
- Data storage
- Bandwidth provision

A slightly different, but related, strategy, is to measure some statistic that correlates indirectly with price, usually a metric of the level of usage; one example of this is transaction volume. Statistical methods, however are prone to be manipulated therefore we will not use them.

Aside manipulations, *"...the problem with all of these metrics is, however, that none of them are very robust against rapid changes due to technological innovation"* he adds. [2] Therefore we have to include Moore's Law compensation. As Buterin states, *"difficulty is a function of both price and Moore's law, and so it gives results that depart from any accurate measure of the price exponentially over time."* [2] "*The first immediate strategy to fix this problem is to try to compensate for Moore's law, using the difficulty but artificially reducing the price by some constant per day to counteract the expected speed of technological progress; we'll call this the* ***compensated naive estimator***" [2].

Having determined the leading factor influencing crypto assets, we can proceed with an attempt to estimate the crypto assets fair value, for which we take as a basis the suggestions of Scott Roberts [12]. The basis for his approach is the assumption of a relationship between the crypto asset price and the mining cost, ideally energy costs. The equation is valid for the PoW (Proof of Work) mining algorithm:

$$P1 * R1 / D1 * L1 = P2 * R2 / (D2 / M) * L2 \quad (1)$$

where,

1 and 2 = moments in time 1 (now) and 2 (future);

P = USD price per crypto asset unit;

R = reward, crypto assets units per block;

D = PoW mining difficulty;

M = Moore's Law adjustment which represents the reflective change over time in the mining

equipment productivity (H/s), is calculated as 2^n, where n is the number of doubling productivity periods;
L = loss factor, equal to the estimated volume of lost crypto assets units due to private keys loss. Coefficient 1 means that 100% of crypto assets units are available, a coefficient of 0.75 means that every fourth unit of crypto assets is unavailable due to the private keys loss.

If hash power is not able to keep up with coin price (which is a temporary effect), the value would be larger than expected. Otherwise, the real-world value slowly decreases as hashing efficiency increases, which may be a desired effect if it is for dev fees because software gets outdated. But Moore's Law has gotten very slow for computers. Hashing should get closer to being a constant hardware cost per hash. Also, electricity is more than half the current cost of hashing and could soon be 3/4 or more of the cost. Worldwide electricity cost is very stable and possibly the best single-commodity measure of constant value [6].

The same equation can be rewritten simpler:

P1 * R1 / E1 * L1 = P2 * R2 / E2 * L2 (2)

where,
E= mining electricity consumption in kWh.

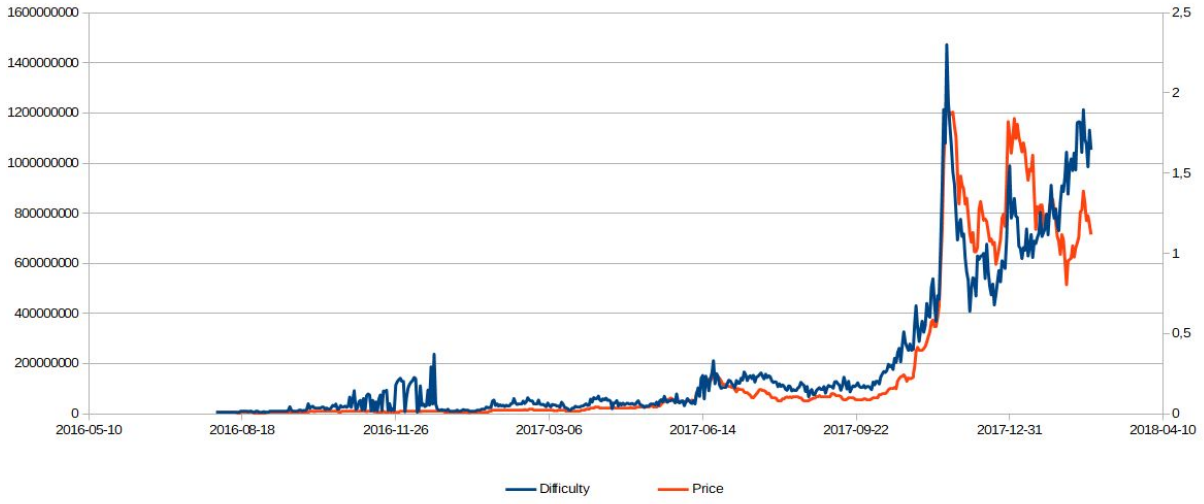
Now we rewrite the equation having in mind that P1 = P2 to define R2 (next reward for the block):

R2 = R1 * (D2 / M) / D1 * L1 / L2 (3)

The logic that determines the next block reward is as follows:
R1= previous block reward;
(D2 / M) / D1 = increase in complexity, that is, an increase in the mining capacity leads to an increase in the crypto asset price, taking into account the Moore’s Law adjustment;
L1 / L2 = over time, an increasing number of crypto assets units are lost due to the private keys loss, a reduction in the issuance of crypto assets in this way increases its price.

We have to mention that this equation gives crypto asset fair price estimate and does not take into account the speculative component, the so-called pumps and dumps.

The comparison of the average historical prices per day with the average difficulty per day in Karbo blockchain confirms the idea of Scott Roberts:



On this chart we can see the average difficulty and price, and it leaves no doubts that they are definitely interconnected.

Managing block reward according to equation (3) we have opportunity to keep exchange rate stable. If difficulty grows at the rate higher than Moore's Law adjustment we increase Karbo supply to reflect increase in mining efforts. If difficulty falls we decrease next block reward according to equation, making Karbo more scarce and thus creating deficit required for price stabilisation.

3. Karbo is a new stablecoin and decentralised medium of exchange

"We need a POW that consumes electricity equally per hash without regard to the hardware it is run on, then never change the POW"
Scott Roberts

3.1. Karbo fungibility

Fungibility is the property of a good or a commodity whose individual units are essentially interchangeable [33]. Bitcoins are not fully fungible. Any two bitcoins have the same exact value. But because all transactions are publicly available, it is common for bitcoin exchanges to discriminate between bitcoins based on the owner or their history. For example, some exchanges will attempt to block bitcoins, which have been confirmed as stolen or obtained illegally. This becomes an issue because when not every exchange accepts the so called "dirty" bitcoins, the "dirty" bitcoins become less valuable [4].

The fungibility and privacy problem is solved in Karbo by CryptoNote protocol [1]. Transactions in Karbo are untraceable and unlinkable. Karbo provides anonymity and privacy using cryptographic technology of ring signatures [1]. All transactions signed on behalf of a group so that it is impossible to determine who exactly from the group signed the transaction and, accordingly, one can not say with certainty who carried out the payment. The more participants in the group, the more confidential the operation is. In addition, the transactions cannot be associated, – even if outgoing transactions are untraceable, everyone may still be able to see the transactions you have received. However, by using a variation of the Diffie-Hellman exchange protocol, a receiver has multiple unique one-time addresses derived from his single public key. After funds are sent to these addresses they can only be redeemed by the receiver and it would be impossible to cross-link these transactions. Unique one-time addresses and ring signatures of transactions are providing resistance to blockchain analysis. Every transaction only increases entropy and creates additional obstacles for those who wish to dig into financial operations with Karbo. Resistance to the analysis, in turn, provides a very important characteristic inherent in real

money, – fungibility. Fungibility of money means that all units of one denomination have the same purchasing power.

3.2. Difficulty algorithm update

"The problem of hash rate instability has been well known for many years in the altcoin community. Multipool mining, where miners could quickly switch between mining coins with compatible Proof of Work algorithms, led to hash rate oscillation and instability. This rapidly switching hash power would often lead to unpredictable confirmation times, and long periods with very slow blocks. There were also more serious problems when coins had widely divergent market values, which could leave the smaller coin vulnerable to miners gaming of the difficulty algorithm, and manipulating timestamps" [13].

In 2016 Karbo mitigated to some extent this problem by changing the default CryptoNote difficulty algorithm to the one proposed by Scott Roberts called "Zawy difficulty algorithm" [29].

The author developed better version of his algorithm and it is proposed to update difficulty algorithm to one of his newest versions: "LWMA (WHM)" [30] or "The Simple DA" [31] for better protection against hashrate attacks. The LWMA (WHM) algorithm was implemented after the attack in which vulnerabilities of previous version were exploited.

To mitigate part of other mentioned threats one solution that is considered is to change the POW algorithm.

One of the possible solutions against hashrate attacks, which are mostly conducted by renting hashing power on the Nicehash and similar services, is to change POW hashing algorithm to make it incompatible with Nicehash and thus remove from multipool hoppers the possibility to switch to Karbo when it's profitable for them.

The second reason is the threat of ASICs, developed for the CryptoNight algorithm. ASICs will cause undesired centralisation of mining and hashing power. From the other hands, ASICs provide large hashrate that is the best protection against attacks on POW based coins that Karbo was suffering. Therefore we consider to stay ASICs-compatible given the fact of presence of at least four vendors offering ASICs on the market.

3.3. Revalution to fit medium of exchange purpose

Since the first block mined at May 30, 2016 for two years Karbo price has increased from 0 to 0,67 USD at May 25, 2018.

Source: https://coinmarketcap.com/currencies/karbo/

To avoid situation with Bitcoin's price which is relatively high when compared to goods and services we propose Karbo revaluation. Today it creates a confusion for Bitcoin users and makes price comparisons in BTC fairly complicated [4]. If we were to buy a Big Mac, which costs 3.99 USD, it would equal to 0.00053425 BTC in prices as of May 25, 2018.

To meet anticipated demand for medium of exchange at scale the current cap of 10 million Karbo coins is not enough. Therefore it is decided to move decimal point for three decimals. Nothing will change if we count Karbo in minimal atomic units. Currently in Karbo there is 12 decimal points, in this notation 1 KRB is 1000000000000 atomic units. If we move decimal point for three decimals and will have 9 decimal points instead of 12 then 1 KRB will become 1000 KRB. It is made for sake of convenience because it is more convenient and more familiar to people to have round figures in prices (e.g. 1 KRB instead of 0.001 KRB). This requires minimal changes in software and services like exchanges, web-wallets, gateways

and mining pools. Revaluation is required for the changes in Karbo concept described below.

3.4. Stablecoin with adaptive emission for dynamic difficulty driven price volatility curbing

In paper titled “On the instability of Bitcoin without the block reward” [11] presented on October 21, 2016 authors stated that at a deeper level, research results suggest a fundamental rethinking of the role of block rewards in cryptocurrency design. The prevailing view is that the block reward is a necessary but temporary evil to achieve an initial allocation of coins in the absence of a central authority. The transaction-fee regime is seen as the ideal steady state of the system. But work [11] shows that incentivizing compliant miner behavior in the transaction fee regime is a significantly more daunting task than in the block reward regime. So perhaps designers of new cryptocurrencies should make the block reward permanent and accept monetary inflation as inevitable. Transaction fees would still exist, but merely as an incentive for miners to include transactions in their blocks [11]. In Karbo transaction fees serve for another purpose that will be shown below, and when in comes to monetary inflation it is desirable because deflationary nature, as it was shown, is not suitable for the Karbo aim and mission.

Volatility is affecting demand in a more complicated and important way. Because of volatility fluctuations, the value of Bitcoin can change significantly in a short amount of time. When there are a lot of transactions taking place, it can potentially take days to record them all, during which time Bitcoin's value could have changed by thousands of dollars.

Merchants risk losing money if they lock in a price with a customer and the value of Bitcoin falls before the transaction is completed. That's not a risk many merchants or Bitcoin traders take lightly, so many have been willing to accept higher fees to speed the recording of their transactions [5]. The upsurge in users and transactions increased the demand for miners' services [5]. The sooner you want a transaction written to the blockchain, generally the higher mining fee you'll have to pay. The advantage of having a transaction recorded quickly is that the sooner it's recorded, the sooner you can spend or sell the coins you've received — and the sooner a merchant will mark a deal as completed [5].

This results in users being pushed to second layer solutions (e.g. sidechains, Lightning Network).

Karbo already has technically infinite but slowly raising supply reducing its deflationary nature because of so called “tail emission”. On November 11, 2016 “tail emission” was implemented in Karbo [16]. There were several purposes of this change. The technical reason was described above where we cite paper which demonstrates that Bitcoin is unstable without the block reward [11]. For that reason it was decided to provide incentive for miners to mine and not rely on fees only as was shown above.

In the post at Bitcointalk Russian thread it was explained by Karbo developers. Additional emission (tail emission) (like in Monero) - after the reward for block will reduce to 1 KRB it will not reduce further, but will stay at that level constantly. It will happen in approximately 7 years or after we reach 97% of initial coin supply of 10 million KRB. This means that theoretically we will have infinite but slow emission with increase a little more than 1% per year to the initial supply, i.e. about 130 000 KRB per year additionally.
Properties [17]:

- deceleration of deflation;
- stimulation of interest for the miners to the mining and, thus, to support and protect the network: the mining will not depend only on fees that will not be enough to support interest, because, since we have an adaptive block size, that is unlimited, unlike the Bitcoin, the market of fees is difficult to create. This means that there will be no increase in fees to get into the blok, accordingly, only fees to maintain the network may not be enough.

In short, Karbo being CryptoNote currency has dynamic block size, therefore given the absence of hard block size limit and due to competition between miners they will include into the block transactions with any fees even with very low fees. Thus the fees market will not emerge and the they will not increase, moreover they will eventually decrease. This will render mining unprofitable due to a high cost and low reward, miners will lose their incentive and will quit mining, reducing the security of the network [18]. This has been acknowledged by Peter Todd [19]: *“IMO Bitcoin should have had an explicit 1%/year or so security tax, implemented via inflation... ”*

The other purpose was to create a inflation pressure at rate of about 1% per year and decreasing because with total supply increasing over time the proportion of the total supply growth lowers every year with the fixed block reward. It was because even on that time back in 2016 we were setting a goal for Karbo to be used as a currency rather than a store of value [20], and for this purpose deflationary model is not suitable. But we see the flaw in this first approach of setting constant block reward with decreasing although slowly inflation.

There is central banking policy for the annual rate of inflation called “inflation targeting”. Inflation levels of 1-2% per year are generally considered acceptable (even desirable in some ways, e.g. to provide additional liquidity to the economy, to stimulate spending and increase the velocity of money), while inflation rates greater than 3% represent a dangerous zone that could cause the currency to become devalued [21].

Hence we are planning to transform “tail emission” into “adaptive emission” to create “inflation targeting” of 1% per year without being decreasing but dynamic instead.

This second proposed change, a dynamic emision will respond to the price changes that are represented in the blockchain by the difficulty to achieve a low volatility, price-stable cryptocurrency. This change is well aligned with CryptoNote philosophy of adaptive limits.

Assuming that difficulty reflects price [6] taken in appropriate scale it is possible to respond to the price changes in macro level by adjusting emission accordingly: as difficulty increases, the emission rate increases too, issuing more coins to the market to meet demand. When demand and increased supply achieves equilibrium, the price stops raising, which leads to the stabilising of the difficulty and emission. If the difficulty decreases, the emission in this case is also decreasing, reducing supply and thus supporting demand and indirectly the price.

This algorithm will not react to the rapid price movements but will curb its undesired sways in any direction in larger scale and time spans. Thus the system will make interventions in case of price movements reflected by the difficulty with emission adjustment in the same manner central banks are acting, i.e. we will emulate central bank functions in decentralized currency.

Japanese researchers in their paper question *"can the proof of work contribute to the stability of Bitcoin value?"* [8] They cite Satoshi Nakamoto: *"once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free"* [9] and state that the answer is no, describing that demand for Bitcoin, regardless of the motivation for holding (i.e. payment or speculation), increases as its price decreases and vice versa. The demand curve of Bitcoin, therefore, would be downward sloping while supply curve of Bitcoin at any point of time would be vertical. All demand shocks must be absorbed in price adjustments [8].

To tame volatility in a decentralized and robust against attack way it is necessary to measure coin price in a decentralized way. The method described in previous section is suitable for this purpose. As we stated already, we are going to use internal variables of the network to measure price, a so called *endogenous solution,* proposed by Vitalik Buterin in his thorough analysis of stablecoin that confirms our assumptions [2]. In the comment to the post he notes [2]: *"If my empirical analysis and math is correct, then we should be able to give stability almost as good as fiat…"* — which is exactly our goal, namely we want to reduce the volatility as much as possible, but there is no intent to strictly tie Karbo value to any fiat currency.

Current coin emission is a strict function of block number. It is not directly in the equation, but since current coin per block is based on past coin/block, going all the way back to the beginning it is still a function of the block number which could be derived [22].

When the initial emission will reach level of "tail emission" rewards it will be dynamically adjusting to curb volatility and/or to keep above mentioned "inflation targeting" of 1% per year.

The logic that determines the next block reward is as follows according to formula (3):

$$R2 = R1 * (D2 / M) / D1 * L1 / L2 \quad (4)$$

where:

R2 = calculated block reward. The minimum block reward whatever the hashrate and difficulty is not less than 1,5% of annual inflation from total supply or 1000 KRB (which figure is larger) after revaluation. The maximum block reward is limited by 200% (annually) from

total supply. For example if total supply is 6 000 000 000 coins minimum block reward is 1000 KRB (6 000 000 000 KRB * 1,5% / 131 400 blocks per year = 685 KRB, we take 1000 KRB as a minimum), the maximum possible reward is 91 324 KRB (6 000 000 000 KRB * 200% / 131 400 blocks per year = 91 324 KRB). To reach maximum reward difficulty has to increase by about 100x times;

R1e = 1000 Karbo (first starting after hard fork block reward);

D2e = new block difficulty;

M = Moore's Law adjustment which represents the reflective change over time in the mining equipment productivity (H/s), is calculated as *2^n*, where *n* is the number of doubling productivity periods (24 months in our case);

D1e = 10 000 000 000 (difficulty equal to desired stable price level);

L1 / L2 = over time, an increasing number of crypto assets units are lost due to the private keys loss, transfers to a wrong address, etc. We estimate that around 1% of total emission is lost every 12 months [23].

Attack vectors and possible risks

There is potential attack vector exploiting the feedback from market on miner reward or risks of death spiral if malicious agent will try to sell or dump large amount of Karbo. Big and continuous dump of the price can cause self-propelling decline of the difficulty and reward. To mitigate this risk we have minimum miner reward whatever the difficulty of 1000 KRB or 1,5% from current total supply divided by 131 400 blocks (one year). Another supporting factor is stable market demand to stop and prevent such a threat.

3.5. Dynamic difficulty driven transaction minimal fee regulation

Bitcoin initially designed as medium of exchange and small transaction friendly tool failed because as Bitcoin has soared in popularity its transaction costs have gone up in tandem with it and it has become too expensive to use in small transactions. Under the term 'costs' we mean that the value of fees in fiat equivalent became more expensive and that the fees themselves in BTC became higher. As a result, high fees are pushing businesses away from Bitcoin.

There are few reasons for this: in Bitcoin, transaction fees are proving to be profitable for miners and there is a limit of block size in Bitcoin. The price of Bitcoin does not have a direct impact on transaction fees. It's not like miners are charging more or Bitcoin users are having to pay higher fees just because Bitcoin is worth more. Instead, all of the volatility in the price

of Bitcoin had led to more people buying and selling the cryptocurrency — which means a lot more demand for space in blocks. And more demand has led to higher fees [5].

Ethereum lead developer Vitalik Buterin admits [24]: *"Things we learned in 2017: in the full-blocks equilibrium, transaction fee prices are even more volatile than cryptocurrency prices. This suggests that for costs incurred over time rather than immediately (eg. storage space), setting a fixed fee may actually be not that bad."*

In Karbo, we set the goal to make the main-chain accessible to everyone by keeping fees reasonable.

Adaptive limits is crucial part of CryptoNote protocol upon which Karbo is built and follows its guidelines [25]: *"A decentralized payment system must not depend on a single person's decisions, even if this person is a core developer. Hard constants and magic numbers in the code deter the system's evolution and therefore should be eliminated (or at least be cut down to the minimum). Every crucial limit (like max block size or min fee amount) should be re-calculated based on the system's previous state. Therefore, it always changes adaptively and independently, allowing the network to develop on its own"*.

The CryptoNote [1] technology that is used in Karbo provides the solution to the part of the problem — the *adaptive block size* vastly reduces the necessity to pay higher fees to get transaction into the block and to be processed promptly[1].

But this introduces another problem to be solved – prevention of spamming the network. In 2010, a block size limit of 1 MB was introduced into Bitcoin by Satoshi Nakamoto. He added it hidden in two commits in secret, when challenged publicly he said it is a safety measure to prevent miners from creating large spam blocks.

Because the block size limit is adaptive in CryptoNote, zero minimum fee can lead to transaction flooding which was addressed by introduction of minimum transaction fee which is hard coded as a flat rate in the default CryptoNote solution. Transactions cheaper than the minimum transaction fee wouldn't be accepted by the Karbo network. Thus the funds in the

[1] However it is still possible to pay higher fee to get transaction into the block sooner in case the block size is close to the current median maximum size, i.e. fee market is not completely removed because space in blocks has to cost something to retain scalability and reduce blockchain uncontrolled and unreasonable growth. In other words Karbo has the priority of transactions defined by fees paid for their processing by the miners.

wallet repeatedly sending transactions to spam the network sooner or later will exhaust. The minimum transaction fee solves two problems, — it introduces the costs of spamming the network and helps to motivate miners to continue to support the network.

The minimum transaction fees can not be too small to effectively prevent abusing. Karbo network had very small flat rate transaction fees (set to 0.0001 KRB). This allowed to conduct the attack on Karbo network by spamming the large number of transactions with tiny amounts during the beginning of April 2018. Karbo developers were forced to set higher transaction fees (0.1 KRB) to stop and prevent spamming which was leading to blockchain bloat. The attacker's goal was also to clog the queue of transactions waiting to be included into the block and to cause denial of service. The other potential risk is that attack was aimed to make it possible for the attacking party to deanonymize Karbo blockchain which is addressed in other parts of Karbo development roadmap.

The problem is that with the raise of cryptocurrency price its transaction costs in fiat equivalent will go up as well and it will become too expensive to use currency in small transactions if transaction fees are hardcoded as flat rate minimum limit. This is confirmed by the high fees that we can observe in the CryptoNote currency Monero with the upsurge of its price. Its minimum transaction fee is not flat rate and is based on the size of the transaction instead, but yet it became quite high when the price of Monero surged because the part of the fee calculation is hard coded as well. The developers of Monero compare the Monero's per kB fees to the per kB fees of other (hybrid) proof-of-work coins for a typical transaction (2 inputs + 2 outputs):

Bitcoin: ~$26.90
Ethereum: ~$2.91
Bitcoin Cash: ~$0.07
Litecoin: ~$0.10
Dash: ~$0.07
Monero: ~$0.24

They state that the per kB fee of Monero is fairly low to their opinion. However, due to the high transaction size, the absolute default fee (in fiat equivalent terms) is quite high, they admit [26].

This leads us to the conclusion that the minimum transaction fees should be adaptive instead of being hardcoded as flat rate. The naive and easiest possible solution to change the hardcoded minimum fee is therefore not acceptable. *"The notion of devs having to release new binaries with lower fees is myopic, because (i) it'd merely kick the can down the road, (ii) changing the constants or formulas requires a hard fork, i.e., they are enforced on a consensus level, and (iii) constantly intervening would be contradictory to our grass-roots, decentralized nature"* — was well expressed by the Monero developers [26].

Therefore it is necessary to develop algorithm that will keep the minimum transaction fee on the stable level in fiat equivalent automatically without intervention of the developers or any trusted agents. This algorithm should adapt the minimum fee to the change of the coin price in fiat currency equivalent. To create such algorithm we need to find a way to establish a feedback from external, real world data to the algorithm, when the blockchain is the only source of data that is available to it; i.e. to measure the coin value in a decentralized way.

We propose several changes in the Karbo including dynamic, difficulty driven minimum transaction fee adjustment.

Up to the April 2018 in Karbo network a static minimum transaction fee value was used, hard coded as 0.0001 KRB. As we described above, because it was cheap, the spamming attack occurred. It was manually raised by developers during hardfork to more reasonable level to prevent future possible abuse and attack vector by spamming the blockchain. But, in the case of significant price rise, the hardcoded minimum fee can become quite expensive as we can observe in various cryptocurrencies and as it was described above. To prevent such fee upsurge, we propose a dynamic minimum transactions fee algorithm, that includes difficulty tailing. Using Scott Roberts' assumptions, it is possible to measure average difficulty at the chosen price level in chosen fiat currency and calculate corresponding fee. The formula of calculation of minimum transaction fee is:

$$F = S * A / D$$

where,

Fe — minimum transaction fee in native currency, KRB

Se — starting fee in fiat equivalent, USD

Ae — Average difficulty constant, corresponding to the chosen level of fiat price

De— Current difficulty.

In this equation current difficulty is used for simplicity because it is easy to get from daemons in existing implementation. The average difficulty, **A** is the measured average difficulty per day that corresponds to the average price of 1 USD and it is and rounded for the sake of simplicity to 10 000 000 000.

Dollar value here is constant-value relative to when the ratio was determined [6] when difficulty was at $1.

Simple formula described above is not suitable for use because rapidly changing difficulty will also change minimum fee that may render transaction invalid if in the meanwhile difficulty will raise and will therefore raise minimum fee. It is necessary to use more smoothly changing and slowly reacting fee. It is proposed to use average difficulty per day for the calculation of the minimum transaction fee calculated using Simple Moving Average (SMA).

daily_D = (cumulative_D[height] - cumulative_D[height-360]) * T / (0.5*T*360 + 0.5*(timestamps[height] - timestamps[height-360])

And the formula for the minimum transaction fee would be:

F = S * A / daily_D

But we also have to include block reward into the equation:

current_value = prev_value * current_D / prev_D * prev_R / current_R

F = S * A * R / daily_D / C

where,
Re— reward per block at 1$
Ce— current reward per block

The formula then is:

minFee = fiatEquivalentGauge * avgReferenceDifficulty / dailyDifficulty * currentRewardPerBlock / avgReferenceReward;

This formula would work in the environment of stable hashrate. But recent emerging of ASICs for the CryptoNight algorithm used in Karbo POW shows us that is is needed to include Moore's Law adjustment:

minFee = fiatEquivalentGauge * avgReferenceDifficulty / dailyDifficultyMoore * currentRewardPerBlock / avgReferenceReward;

Where:

dailyDifficultyMoore = dailyDifficulty / pow(2, std::min(height, height - blockConst) / blocksInTwoYears);

Where **blockConst c**onstant is starting height of application of this approach.

We think that the 2 years Moore's law correction is enough, based on Buterin observation *"...as we see the Bitcoin mining economy stabilize toward something closer to an equilibrium where technology improves only as fast as the general Moore's law rule of 2x every 2 years"* [2] assuming that CryptoNight POW will behave in the similar way.

Transactions count that reflects the usage of the network is included in this formula via the current block reward and is causing fluctuations which have to be addressed by using ceil function to round up actual fee to pay when it is calculated in wallets to prevent possible transaction stuck if fee that was enough will become too small before it was included into the block in case if minimal fee rapid upsurge. This means that minimum transaction fee fluctuations are undesired. That is why the average daily difficulty is used. And we are considering to enlarge this window to a week or even a month to make minimum transaction fee fluctuation very smooth reacting only to large changes in difficulty filtering out small variations.

We include full current block reward into equation (emission reward + transaction fees) to create positive feedback by larger reward from fees paid for increased number of

transactions (which reflects increased usage) resulting in increased fees, i.e. the more transactions, the more space is used in blockchain — the bigger minimal fees become.

This is justified because more transactions use more space in blockchain which should be paid for. This is better approach than per-Kb approach of fees to limit uncontrolled blockchain growth and bloat, we believe. Instead of creation of a market for fees, we are limiting block size via enforced minimum fees and these fees instead of miners should go to nodes, since their expenses are bigger if transactions are large.

The transaction fees will be divided between miners and masternodes to mitigate the risk of abuse from the miners which could form a cartel collusion and generate more transactions themselves knowing that they will eventually return their fees anyway to raise minimum fee level and get more feed from users; and to protect from the same abuse from the masternodes, as collusion between nodes and miners is less likely.

"The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions," [9] wrote Bitcoin founder Satoshi Nakamoto in the white paper. We agree, that this cost must be present, but it does not have to be too high. We hope that proposed solution will keep transactions costs in the Karbo network reasonable and stable which will facilitate the adoption of Karbo by merchants. Thus we continue the vision and goal of CryptoNote developers making more network parameters adaptive [25].

3.6. Blockchain monetary deposits with adaptive interest rates

We are also going to implement a system of deposits on blockchain and adjust deposit interest rate according to the coin price using the same difficulty method as above but inverted: increase deposit interest rate when difficulty is dropping to stimulate deposits and therefore create deficit of coins which will lead to price support; and vice versa — lower deposit interest rate when difficulty is raising. This is the additional method of curbing price volatility that will react at different speed than emission method. We believe that this additional method will reduce the risks of dangerous feedback loops in either direction of the first emission method and will help to achieve more than 50% cancel out of price volatility.

Another dimension of monetary deposit rates could be depending from their total percent from the Karbo emission up to date. The lower this percent the higher the monetary deposit

rate. As soon as amount of deposits in relation to Karbo total supply will increase the deposit rate will decrease.

The deposits on blockchain based on CryptoNote protocol is already studied, described and implemented by DigitalNote [7]. In 2015 XDN introduced new blockchain based feature: time-locked deposits with variable annual interest rate. In general it allows users to “lock" some of their XDN for a while (from one month to a ten years) and after some time, withdraw it back with some interest as a part of main DigitalNote reward supply.

Deposits are implemented via new types of transaction outputs. It includes amount, destination key (or keys) and time (expressed in blocks) to lock. Transaction itself contains the field unlock_time but output-specific parameters is much more convenient, because user may want to sent some money back as change (and surely doesn't want them to be locked). The transaction is included in the blockchain as usual and the counter starts.

When the lock expires user can spend this output as usual, but the new transaction amount will be increased with the interest. It also means that deposits act as new source of emission [7].

Interest rate should constantly grow with 0,025% step until difficulty is decreasing. For example, as soon as difficulty growing, interest rate for monetary deposits is 0%. It does not make sense to absorb liquidity in this situation. But as soon as difficulty starts falling meaning that Karbo price is decreasing it make sense to start absorbing liquidity by increasing interest rate from zero percent to 0,025% annually measured interest rate. If after 360 blocks or 24 hours average difficulty is still decreasing we will have another step of rate increase to 0,05% and so on on until we will not see stabilisation or growth of difficulty. The maximum interest rate is proposed at level of 1,5%. Inflation levels of 1-2% per year are generally considered acceptable, while inflation rates greater than 3% represent a dangerous zone that could cause the currency to become devalued [21]. Whatever the difficulty trend monetary deposit interest rate could not exceed 1,5% and it takes 30 days to grow from 0% to maximum with 0,025% step if we suppose that difficulty will fall 60 days in a row. If difficulty is decreasing constantly in the end we will have no more than 3% annual inflation consisting of 1,5% minimum mining reward plus 1,5% monetary deposit interest rate. In practise inflation will be lower than 3% due to fact that it is not possible in real life that 100% of total supply will be deposited.

One can place monetary deposit for 24 hours (360 blocks) up until 1 month (10800 blocks). Interest rate does not depend on term and stays the same. Long term deposits for 2 and more month are dangerous as sources of inflation in conditions of rate changing every 360 blocks or 24 hours. If we imagine that 1 year deposits are possible than with a few spikes up to the maximum 1,5% interest rate we can end up with major part of Karbo emission more than 50% placed at maximum rate of 1,5% for 1 year.

Attack vectors and possible risks

There is a monetary deposits possible exploit from crypto exchanges which collect significant amounts of Karbo on their accounts and can deposit part of this liquidity which they think is stable in the long term. We have to accept this risk taking into account that major amount of Karbo 80-90% will be held not by exchanges as exchanges being centralised entities is risky place to keep Karbo with them for long term. For the sake of your security do not keep Karbo with centralised entities like crypto exchanges, etc.

3.7. POW/POS hybrid with masternodes for network security

The current implementation of Karbo blockchain utilizing POW algorithm has it downsides and weaknesses. Some of them were exploited. On April 2018 Karbo was attacked using weakness in difficulty adjustment algorithm. These are the problems to be resolved:

- Double spends
- >50% attacks
- Selfish mining (various forms)
- 'Jump' pools
- Side chains
- Centralisation of mining
- Erratic block times
- Transaction capacity limitation
- Sybil attack
- Stalled blockchain

Some vulnerabilities were removed by the changes in difficulty adjustment algorithm described below.

The change of POW algorithm alone is not sufficient to fight against all threats. A popular solution that many virtual currencies have switched to is Proof of Stake (POS). But POS suffers from various new problems of its own. Combined POS/POW is therefore proposed as a better alternative. But instead of being as strong as both, it is only as strong as the weakest of the two, thus opening the coin up to more attacks and not less. Despite the various problems of POS and combined POS/POW the core idea behind them is viable if applied properly.

Karbo has so called masternodes. The masternodes are providing miscellaneous services to the network, e.g. they work as servers for lite and mobile wallets, they propagate and distribute blockchain etc. These are merely full nodes operating in Karbo network that have full blockchain. They currently have only one incentive to stay online and provide services to the network — fees paid by lite and mobile wallets for transactions.

The possible transition to POW/POS hybrid was announced back in September 07, 2016 along with “tail emission” that was implemented shortly afterwards [32], i.e. the proposed change was planned long time ago.

It is proposed to introduce two distinct class of miners on the network: POW miners and POS miners. The masternodes will become POS miners. It will be possible thanks to collateral (special type of deposits) that will be available to masternodes.

In order to run a masternode, a node wallet must hold collateral of a dynamically selected minimal amount of KRB. The minimal amount of collateral will be adaptive by the same difficulty based value measurement technique used for minimal transaction fees and emission regulation.

The POW/POS will work as follows:

- Mining of blocks is done by POW miners in the usual manner. When a miner finds a block it is submitted to the network.
- Nodes validate, accept and relay the block as usual however it does not yet get added to the tip of the chain.
- When receiving an unsigned block an eligible masternode will sign the block using his private key converting it into a signed block adding additional data to the block, this includes a singing timestamp, any additional transactions (subject to the existing

block size limit) and a transaction to pay out the masternode reward. Masternode reward is proposed to calculate based on it's collateral. As soon as a valid signed block is created it is rebroadcast to the network.

- Once peers receive a signed block they add it to the tip of the chain as in usual POW and POW miners attempt to mine a new block on top of the new tip of the chain, the cycle repeats [27].

In classic POS it is required to reveal the balance at stake. CryptoNote balance of particular account is not visible therefore classic POS is impossible for CryptoNote protocol. But monetary deposits that will be implemented in Karbo network allow to make POS on CryptoNote protocol as described in "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake" [28].

When POW miner generates empty block and broadcasts it to the network N pseudo-random numbers are derived from the result hash. These numbers correspond to the N Karbo atomic units selected from all coins currently deposited as masternode collateral. Since this information is public, it is possible to map every number to a specific output and its public key.

These N public keys belong to selected stakeholders, who should sign the block. First N - 1 stakeholders just provide their signatures, whilst the Nth user forms the block and signs all data. The reward and transaction fees are divided between POW and POS participants. If chosen N stakeholder is offline, the next participant is selected and the process continues [7].

References

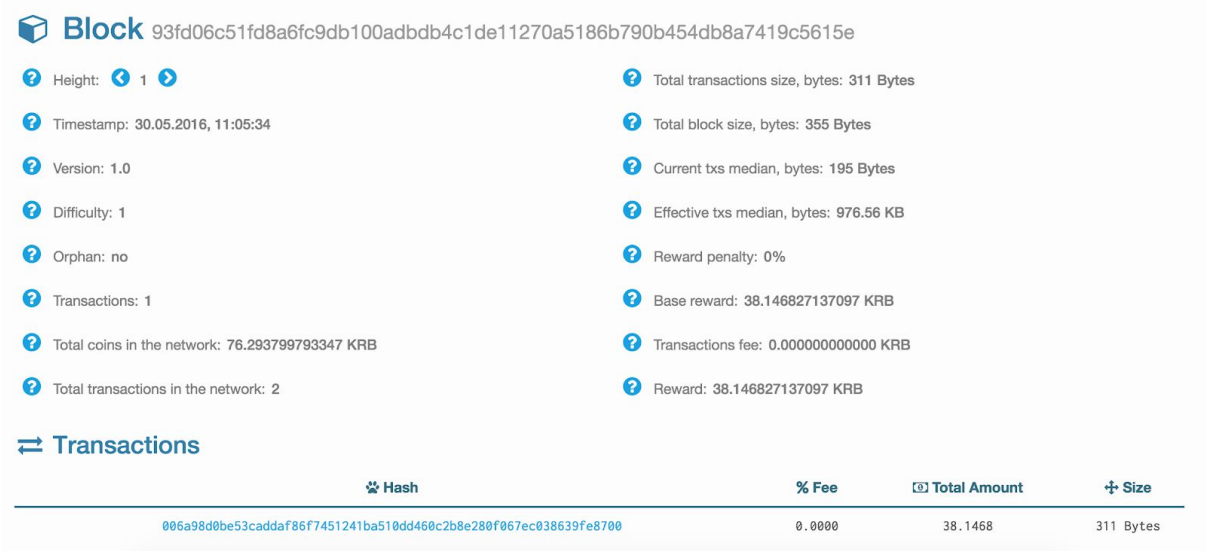
1) “CryptoNote v 2.0 Whitepaper”, Nicolas van Saberhagen, 17.10.2013, https://cryptonote.org/whitepaper.pdf
2) “The Search for a Stable Cryptocurrency”, Vitalik Buterin, 11.11.2014, https://blog.ethereum.org/2014/11/11/search-stable-cryptocurrency/
3) “Hayek Money: The Cryptocurrency Price Stability Solution”, Ferdinando M. Ametrano, 17.04.2014, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425270
4) “Can Bitcoin Become a Viable Alternative to Fiat Currencies? An empirical analysis of Bitcoin’s volatility based on a GARCH model”, Vavrinec Cermak, 02.05.2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2961405
5) “The cost of bitcoin payments is skyrocketing because the network is totally overloaded”, Becky Peterson, 29.12.2017, http://www.businessinsider.com/bitcoin-payment-mining-fees-hit-new-high-2017-12
6) “Using difficulty to get constant-value dev fees”, Scott Roberts, 27.12.2017, http://zawy1.blogspot.com/2017/12/using-difficulty-to-get-constant-value.html
7) DigitalNote XDN-project Whitepaper, 06.06.2015, http://digitalnote.org/whitepaper.pdf
8) “Can we stabilize the price of a cryptocurrency? Understanding the design of Bitcoin and its potential to compete with central bank money”, Mitsuru Iwamura, Yukinobu Kitamura, Tsutomu Matsumoto, Kenji Saito, Institute of Economic Research, Hitotsubashi University, Kunitachi, Tokyo, 186-8603 Japan, 25.10.2014, https://ru.scribd.com/doc/245827939/SSRN-id2519367-Japan-Improved-Bitcoin-IBC
9) “Bitcoin: A Peer to Peer Electronic Cash System”, Satoshi Nakamoto, 2008, https://blockchair.com/bitcoin/whitepaper/bitcoin.pdf
10) “A Cost of Production Model for Bitcoin”, Adam S. Hayes, Department of Economics The New School for Social Research, New York, February, 2015, http://www.economicpolicyresearch.org/econ/2015/NSSR_WP_052015.pdf
11) “On the Instability of Bitcoin Without the Block Reward”, Miles Carlsten, Harry Kalodner, Matt Weinberg, Arvind Narayanan, 2016, http://randomwalker.info/publications/mining_CCS.pdf
12) https://github.com/monero-project/monero/issues/3766#issuecomment-387437584

13) “Bringing Stability to Bitcoin Cash Difficulty Adjustments”, Mengerian, 26.08.2017, https://medium.com/@Mengerian/bringing-stability-to-bitcoin-cash-difficulty-adjustments-eae8def0efa4
14) “National Government Digital Currencies Versus Globally Distributed Cryptocurrencies: in Depth”, Rainer Michael Preiss, Cointelegraph, 21.05.2018, https://cointelegraph.com/news/national-government-digital-currencies-versus-globally-distributed-cryptocurrencies-in-depth?utm_source=Telegram&utm_medium=Social
15) “Bitcoin ends the era of inflation”, Phil Geiger, 17.05.2018, https://medium.com/datadriveninvestor/bitcoin-ends-the-era-of-inflation-aba15935a224
16) Karbo Tail Emission Implementation, https://github.com/seredat/karbowanec/commit/74cb7bfe013ea15dd1f65d06de09959f982680a8
17) https://bitcointalk.org/index.php?topic=1513025.msg16924025;topicseen#msg16924025
18) https://getmonero.org/resources/moneropedia/tail-emission.html
19) https://twitter.com/peterktodd/status/697532042553065472
20) https://bitcointalk.org/index.php?topic=1491747.msg16180390;topicseen#msg16180390
21) “Inflation Targeting”, Investopedia, https://www.investopedia.com/terms/i/inflation_targeting.asp
22) https://github.com/seredat/karbowanec/commit/231db5270acb2e673a641a1800be910ce345668a#commitcomment-24044240
23) “Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says”, Jeff Roberts, Nicolas Rapp, 25.11.2017, http://fortune.com/2017/11/25/lost-bitcoins/
24) https://twitter.com/VitalikButerin/status/957400121557307392?s=09
25) https://cryptonote.org/inside#adaptive-limits
26) https://getmonero.org/2017/12/11/A-note-on-fees.html
27) “Gulden 2.0 - Improving the blockchain”, Malcolm J. MacLeod, https://github.com/Gulden/gulden-official/raw/master/technical_documentation/Gulden_PoW2.pdf
28) “Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake”, Iddo Bentov, Charles Lee, Alex Mizrahi, and Meni Rosenfeld, 2014, https://eprint.iacr.org/2014/452
29) https://github.com/seredat/karbowanec/commit/231db5270acb2e673a641a1800be910ce345668a#commitcomment-22615466

30) https://github.com/zawy12/difficulty-algorithms/issues/3
31) https://github.com/zawy12/difficulty-algorithms/issues/21
32) https://bitcointalk.org/index.php?topic=1491747.msg16180390;topicseen#msg16180390 and https://bitcointalk.org/index.php?topic=1513025.msg16184687;topicseen#msg16184687
33) https://en.wikipedia.org/wiki/Fungibility

Appendix 1. State of Karbo blockchain

Statistics of Karbo blockchain for 2 years of existence from first block published on May 30, 2016 till block number published on May 30, 2018



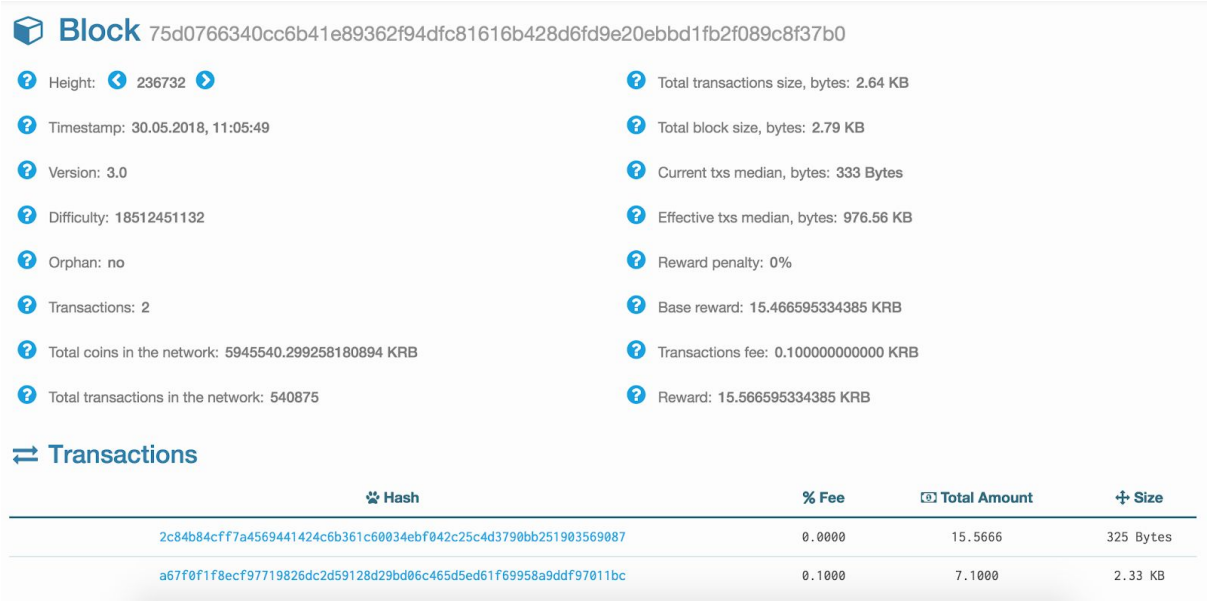
Block 93fd06c51fd8a6fc9db100adbdb4c1de11270a5186b790b454db8a7419c5615e

Height: 1	Total transactions size, bytes: 311 Bytes
Timestamp: 30.05.2016, 11:05:34	Total block size, bytes: 355 Bytes
Version: 1.0	Current txs median, bytes: 195 Bytes
Difficulty: 1	Effective txs median, bytes: 976.56 KB
Orphan: no	Reward penalty: 0%
Transactions: 1	Base reward: 38.146827137097 KRB
Total coins in the network: 76.293799793347 KRB	Transactions fee: 0.000000000000 KRB
Total transactions in the network: 2	Reward: 38.146827137097 KRB

Transactions

Hash	% Fee	Total Amount	Size
006a98d0be53caddaf86f7451241ba510dd460c2b8e280f067ec038639fe8700	0.0000	38.1468	311 Bytes

Source: https://explorer.karbo.io/?hash=93fd06c51fd8a6fc9db100adbdb4c1de11270a5186b790b454db8a7419c5615e#blockchain_block



Block 75d0766340cc6b41e89362f94dfc81616b428d6fd9e20ebbd1fb2f089c8f37b0

Height: 236732	Total transactions size, bytes: 2.64 KB
Timestamp: 30.05.2018, 11:05:49	Total block size, bytes: 2.79 KB
Version: 3.0	Current txs median, bytes: 333 Bytes
Difficulty: 18512451132	Effective txs median, bytes: 976.56 KB
Orphan: no	Reward penalty: 0%
Transactions: 2	Base reward: 15.466595334385 KRB
Total coins in the network: 5945540.299258180894 KRB	Transactions fee: 0.100000000000 KRB
Total transactions in the network: 540875	Reward: 15.566595334385 KRB

Transactions

Hash	% Fee	Total Amount	Size
2c84b84cff7a4569441424c6b361c60034ebf042c25c4d3790bb251903569087	0.0000	15.5666	325 Bytes
a67f0f1f8ecf97719826dc2d59128d29bd06c465d5ed61f69958a9ddf97011bc	0.1000	7.1000	2.33 KB

Source: https://explorer.karbo.io/?hash=75d0766340cc6b41e89362f94dfc81616b428d6fd9e20ebbd1fb2f089c8f37b0#blockchain_block

Appendix 2. Karbo official resources

Karbo Official Website: https://karbo.io/

Official Wallets: https://karbo.io/download/

Karbo Blockchain Explorer: https://explorer.karbo.io/#

GitHub Repository: https://github.com/seredat/karbowanec

Karbo Mobile Wallet & Masternodes: http://www.karbo.cloud/

Karbo Promo Kit: https://karbo.io/promo/

Karbo Mobile Wallet for Android Phones:
https://play.google.com/store/apps/details?id=org.karbo.karbon