A SHORT INTRODUCTION INTO INNOVATIVE WORLD OF MASTERNODE COINS

Mladen Opačić[1]*,
Mladen Veinović[1],
Dunja Adžić[2]

[1]Singidunum University,
Belgrade, Serbia,
[2]OmnitechIT,
Belgrade, Serbia

Abstract:

This paper aims to provide a short introduction into the world of so called masternode coins. Cryptocurrencies based on an incentivized node model that provides income to holders of cryptocurrency that run second tier nodes on the network.

Keywords:

blockchain, masternodes, dash, cryptocurrency.

1. INTRODUCTION

This paper is a very short review of this interesting and fast growing type of cryptocurrency. In the first part of the paper there is a short introduction about Bitcoin its history and circumstances that led to the development of thousands of altcoins. Then in the second part the paper introduces Dash and its major features such as masternodes, privacy, InstantSend, PrivateSend etc. In the third part of the paper there is a short review of five most valuable masternode coins according to current market value.

2. BITCOIN

When Satoshi Nakamoto published his now famous whitepaper [1] in 2008 little did he know about the impact that this new technology will have on modern world. Ten years later we live in a completely new world and bitcoin is globally recognized as Internet money. Its value skyrocketed from less than a cent to all time high [2] value of $20089 dollars per Bitcoin. However, Bitcoin still has much to go before it reaches full acceptance in everyday life.

Prehistory

Bitcoin didn't just appear out of nowhere it is based on the years of advancements in the fields of cryptography and economy. According to [3] the concept of electronic cash has been present since the 1980s. David Chaum introduced the concept of blind signatures and secret sharing

Correspondence:
Mladen Opačić

e-mail:
mladja@mladja.com

DOI: 10.15308/Sinteza-2018-147-152

1984. Advances such as CFN, e-cash, hashcash, b-money and BitGold served as the base on which bitcoin was built. We can say that bitcoin is the culmination of over 30 years of research in making electronic cash work.

Beginning

Although the beginning of Bitcoin is shrouded in mystery some facts are known. The founder of bitcoin is a person or a group of people under the pseudonym of Satoshi Nakamoto.

Bitcoin.com was registered on 18 August 2008. Later in the same year on 31st of October 2008 Satoshi Nakamoto published Bitcoin whitepaper [1]. Then 8th January 2009 the first version [4] of bitcoin was announced. Mining began shortly after announcement.

"Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority." [4]

With these words started the revolution.

Altcoins

Soon after bitcoin become popular many new coins were created. Popularly called altcoins these projects are usually copies or forks of bitcoin but there are also many projects that are written from scratch. Due to the fact that bitcoin is open source it is very easy to copy the code and start a new altcoin. Maintaining that coin however is a completely different story.

Coinmarketcap website [5] currently lists almost 1600 different coins. Some of them are actively developed projects with hundreds of contributors while some others are completely dead and unmaintained.

The idea behind the majority of altcoins is that they want to be better than Bitcoin in some way. Whether that is a new consensus algorithm, enhanced privacy or something completely different they all want to be better than Bitcoin.

3. DASH

Dash is an altcoin based on Bitcoin but with many new features. Originally known as XCoin it was released on 18 January 2014. Then on 28 January, developers decided to change the name to Darkcoin. But since they still were not satisfied with the name on 25 March, 2015, name Darkcoin was changed to Dash. Darkcoin whitepaper [6] defined it as:

"the first privacy centric cryptographic currency based on Satoshi Nakamoto's Bitcoin. DarkSend, a technology for sending anonymous block transactions is incorporated directly into the client using extensions to the core protocol. An improved proof¬ of¬ work using a chain of hashing algorithms replaces the SHA256 algorithm and will result in a slower encroachment of more advanced mining technologies (such as ASIC devices). DarkGravityWave is implemented to provide quick response to large mining power fluctuations"

Later Dash whitepaper [7] defines it as:

"A crypto-currency based on Bitcoin, the work of Satoshi Nakamoto, with various improvements such as a two-tier incentivized network, known as the Masternode network. Included are other improvements such as PrivateSend, for increasing fungibility and InstantSend which allows instant transaction confirmation without a centralized authority."

Masternodes

Masternodes [8] are the most important innovation of Dash. Users who run and maintain special nodes on the network called masternodes receive rewards equal to the rewards of miners in traditional Proof of Work (PoW) systems. To run masternode user has to provide and lock 1000 dash as collateral. In Dash 45% of the block reward is allocated towards masternodes. Masternodes earn their rewards for providing special services to the network:

- InstantSend – feature that allows for near-instant transactions
- PrivateSend – enables users to send funds privately
- Governance and treasury – enables masternode owners to vote on budget and other proposals
- Dash Evolution – an upgrade that aims to make using Dash as easy as using PayPal

Return on investment per annum can be seen on the diagram below Fig 1.:

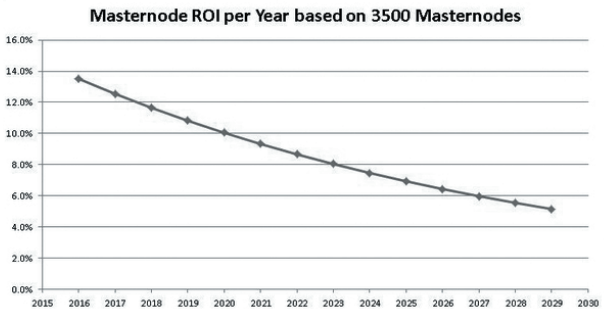

Fig. 1. Masternode ROI per year - taken from [8]

PrivateSend

As mentioned earlier privacy is the central feature of dash cryptocurrency. Privacy is attained by using PrivateSend process. Basically coins are mixed among multiple users so that origin of the coins is obscured. Coins are mixed without ever leaving the wallet so users maintain control of their funds at all times. This is how PrivateSend [9] works:

- Step 1: System breaks transaction inputs into standard denominations of 0.01,0.1,1,10 DASH
- Step 2: System contacts masternodes anonymously
- Step 3: System waits for two other people who want to send coins privately and then mixes the coins
- Step 4: Process is repeated multiple times to obscure the funds even further. Each additional round makes the funds exponentially more private

This process is illustrated on the Fig 2. diagram:

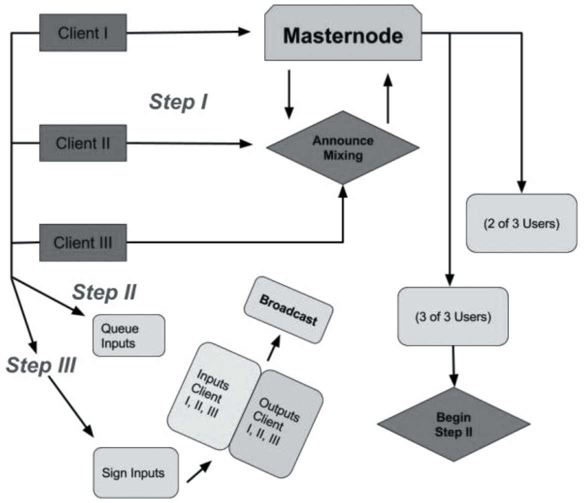

Fig. 2. PrivateSend process - taken from [9]

InstantSend

As the name implies InstantSend functionality of dash allows the option to send funds instantly. Again masternode network is utilized Fig. 3. to allow instant transfer of data while still protecting the network from double spend problems. Here is how instant sent works:

- Step 1: Miner that has found the last winning block submits the hash of the block to be used as seed to randomly select a quorum of 10 masternodes
- Step 2: In the time between the blocks these 10 masternodes become instant send authorities. They lock the inputs of the transactions and broadcast the message about locked coins to the network. So now any other transaction that would like to use those same funds in double spend attack will get rejected.
- Step 3: Both sender and receiver see 5 confirmations of the transaction in less than 1 second of the transaction.

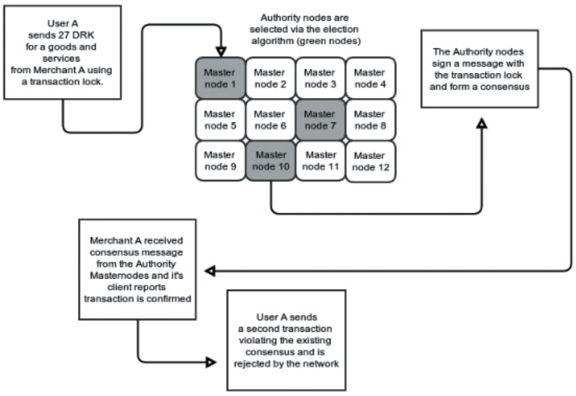
User A sends 27 DRK for a goods and services from Merchant A using a transaction lock.
Authority nodes are selected via the election algorithm (green nodes)
Master node 1
Master node 2
Master node 3
Master node 4
Master node 5
Master node 6
Master node 7
Master node 8
Master node 9
Master node 10
Master node 11
Master node 12
The Authority nodes sign a message with the transaction lock and form a consensus
Merchant A received consensus message from the Authority Masternodes and it's client reports transaction is confirmed
User A sends a second transaction violating the existing consensus and is rejected by the network

Fig. 3. InstantSend process – taken from [10]

X11 algorithm

One of the upgrades to original bitcoin code X11 algorithm chains 11 different hashing algorithms blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd and echo instead of only one algorithm sha256 that is used by bitcoin. This makes the proof-of-work much safer than bitcoin. Algorithm is predominantly mined with ASIC miners which makes it even safer.

Multi-Phased Fork

Multi-Phased fork [11] or Spork is a failsafe mechanism built in into Dash that allows developers to rollback changes or to turn of features if something goes wrong without the need for all nodes to update their version of the software.

Budgeting system and governancee

Unlike bitcoin that has no clear mechanism to make decisions Dash governance and budgeting system allows the network of masternodes to resolve issues by voting. Each masternode gets one vote on every proposal and the whole system is automatic. If the proposal passes funds are automatically allocated to the address stated in the proposal. A total 10% of the block reward is allocated towards monthly budget. This allows the network to pay for activities such marketing or development.

Evolution

Evolution is the codename for next major upgrade in Dash. It is a decentralized currency platform with a goal to provide simple access to Dash blockchain technology. List of new features includes DashDrive, DAPI, DashPay Decentralized wallets, second tier, budgets, governance, quorum chain and social wallet.

4. INOVATIVE MASTERNODE COINS

The same way Dash forked bitcoin other coins forked Dash. So now we have hundreds of masternode coins. Although some of them are not Dash clones the idea and principles on which they operate generally come from Dash. The way Dash wanted to make a better bitcoin these altcoins almost always want to make a better Dash. Innovations that they make in order to succeed will be discussed in following section.

Website masternodes.online currently lists 204 masternode coins and 103037 running masternodes. With prices ranging from $0.0001 to $29. ROI ranging between 0.13% and 24602.93% and coins required for running masternode ranging from 20 to 10000000. First five coins by marketcap currently are Dash, PIVX, Zcoin, Blocknet and Smart Cash. What majority these coins have in common is that they all have self-funded teams of developers and community of masternode owners that run the masternode network and are hoping that one day one of these coins will become a new Dash and that they will be able to retire on masternode income. Pivx is possibly the most serious masternode coin besides Dash. It has a professional website and clearly communicated goals so it will serve us perfectly to show the direction where this whole little world of open source coins is going.

Pivx

Pivx website [12] defines Pivx as:

"PIVX is an open source crypto-currency focused on fast private transactions with low transaction fees & environmental footprint. It utilizes a custom Proof of Stake protocol for securing its network and uses an innovative variable seesaw reward mechanism that dynamically balances 90% of its block reward size between masternodes and staking nodes and 10% dedicated for budget proposals. The goal of PIVX is to achieve a decentralized sustainable crypto currency with near instant full-time private transactions, fair governance and community intelligence."

Main features of PIVX include:

- Proof-of-Stake
- Seesaw reward balance system
- Zerocoin protocol

Pivx is a proof-of–stake coin which means that coins are created by the network without solving expensive mathematical problems. This offers less security for the network but is more economical and environment friendly.

Seesaw reward balance system aims to balance distribution of rewards between masternodes and staking wallets Fig. 4.

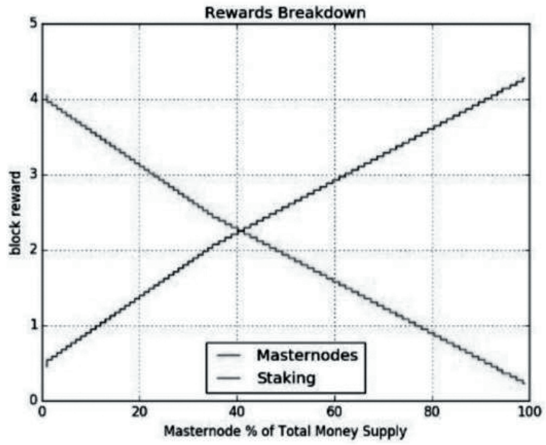

Fig 4: Diagram shows annual percentage return [13]

PIVX coin is trying to have better privacy than Dash by implementing Zerocoin [14] protocol. Since version 3.0.0 Zerocoin [15] anonymity is enabled by default although it is still possible to send transparent transactions. Main advantages of Zerocoin include:

- Users can now hide their balance from public
- Transaction history of the coin can be hidden
- Fast anonymous transactions

In all Bitcoin based cryptocurrencies privacy presents a very big problem since the ledger is public. This leads to an unpleasant fact that if someone knows users public address that person can easily see how much funds that user has on his account. If someone malicious can trace a user to substantial amounts of coins this can lead to serious problems.

Similar to the problems with public ledged transaction history can lead to many problems for the user. For example, if the coin that he received can be traced to be stolen user could be required to return the coin and prove that he didn't have anything to do with the robbery.

Zcoin

Third masternode coin by marketcap is also a coin [16] that implements Zerocoin privacy protocol but unlike PIVX it is a proof-of-work coin that aims to implement MTP mining algorithm [17]. Developed by Alex Biryukov and Dmitry Khorvatovich MTP is algorithm that would allow even playing field between CPU, GPU, FCPGA and ASIC miners and by doing so increase the security of the network. So called egalitarian computing aims to establish the same price/cost per computation unit on all aforementioned mining platforms. In this way potential attacker would have to spend much larger amount of money to mount an attack on the network. This then leads to much better safety of the network. MTP is extremely memory and computationally intensive while searching for a solution, once solution is found verification is done with only a small requirement of memory. Current Zcoin implementation uses 2gb of RAM but if needed it can be increased to 10gb. For comparison SCRYPT algorithm uses only 128kb of RAM making it very easy to make profitable ASIC chips.

Zcoin masternodes are called Znodes. To run a Znode user must lock 1000 coins. Total 30% of block reward is allocated towards masternode. Current system requirements are VPS/Server with 1GB RAM a static IP address and 25 GB free hard drive space.

Blocknet

Blocknet [18] wants to become a decentralized blockchain platform that will connect different blockchains and allow nodes of different to transfer value and data between blockchains. With all the regulation coming into the market of cryptocurrencies centralized methods of exchange might be forced to stop trading with certain coins in that case platforms like Blocknet will thrive until the time comes for them to be regulated.

Blocknet is a proof-of-stake masternode coin similar to PIVX in the sense that the network consists of masternodes and staking nodes. In Blocknet masternodes are called service nodes. To run service node on Blocknet network users need to lock 5000 blocknet as collateral. Service nodes earn 70% of the block reward while staking nodes earn 30%.

SmartCash

SmartCash [19] is a fast growing masternode coin that focuses on development and community unlike other coins where the team takes usually 10% of the block reward in SmartCash system 70% goes to community treasury, 5% to miners, 15% to smart rewards and 10% for smart nodes. Interestingly it is also Zerocoin based and uses keccek algorithm.

SmartCash concept is best explained by this quote from their website [19]:

"SmartCash is a project born out of the desire to create a viable, fungible, fast, merchant oriented, user friendly and community driven cryptocurrency with a decentralized governance system. We aim to create the most nimble and fast growing cryptocurrency by aggressively prioritizing block rewards to growing our community, hiring developers, gaining merchant acceptance and via grassroots community outreach efforts and established marketing methods."

SmartCash is also very innovative in the decentralization department. Instead of building one centralized core team of developers they want to build multiple independent teams of developers to prevent corruption that centralization usually brings. Also to prevent centralization SmartCash will allow everyone who has at least one SmartCash coin to vote by making voting system to allow one vote per coin.

5. CONCLUSIONS AND FUTURE RESEARCH

Masternode coins or Dash clones are still very young projects filled with huge potential for future growth and innovation. It is evident that absolute privacy is very important as most successful clones are the coins that are more private than Dash. However, that might change soon with more regulation coming into cryptocurrency markets. We might see major centralized exchanges be forced to delist private coins. In that case projects like Blocknet will become even more important in the future. Besides privacy decentralization is a very important issue with Zcoin inventing a whole new algorithm or SmartCash giving voting rights to anyone who has at least one SmartCash coin in their wallet and making multiple teams of developers.

This research opens a large number of topics for further research. There is a large number of masternode coins that we didn't cover in this paper. Some of masternode coins that we didn't cover have very interesting and innovative technology behind them and deserve further study. There is also a question how these little innovative teams will respond faced with regulation. Will they just stop their networks or will they find some innovative ways to survive? Will regulation be enforced and how? How will this influence the Internet? Will masternode income be taxed? And many other similar questions.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2009

[2] https://athcoinindex.com/price/page/all

[3] I. Bashir, Mastering Blockchain. Packt Publishing Limited, 2017.

[4] http://www.metzdowd.com/pipermail/crypto graphy/2009-January/014994.html

[5] https://coinmarketcap.com/

[6] https://dashpay.atlassian.net/wiki/download/attachments/132120878/Darkcoin%20Whitepaper.pdf

[7] https://dashpay.atlassian.net/wiki/spaces/DOC/pages/5472261/Whitepaper

[8] https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146920/Masternode+Network

[9] https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146924/PrivateSend

[10] Duffield E., Schinzel H., Gutierrez F., "Transaction Locking and Masternode Consensus: A Mechanism for Mitigating Double Spending Attacks", 2014

[11] https://dashpay.atlassian.net/wiki/spaces/DOC/pages/19169298/Multi-Phased+Fork+Spork

[12] https://pivx.org/what-is-pivx/white-papers/

[13] https://pivx.org/wp-content/uploads/2017/03/PIVX-purple-paper-Technincal-Notes.pdf

[14] Miers I., Garman C., Green M.,Rubin A. D., "Zerocoin: Anonymous Distributed E-Cash from Bitcoin" https://isi.jhu.edu/~mgreen/ ZerocoinOakland .pdf

[15] https://pivx.org/zpiv/

[16] https://zcoin.io/tech/

[17] Biryukov A., Khovratovich D.,"Egalitarian Computing" https://arxiv.org /pdf/1606.03588v1.pdf

[18] https://blocknet.co/18-03-15_Blocknet_Design_Specification_v.1.0.pdf

[19] https://smartcash.cc/what-is-smartcash/