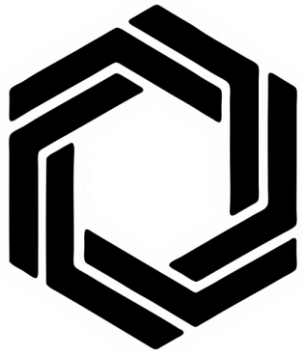


HEXXCOIN

WHITEPAPER: ver. 1

Published March 1, 2018

Content

1. Introduction

Cryptocurrencies became a novel phenomenon since an advent of Bitcoin in early 2009. People use them as a method of payment and a store of value. However, the original Bitcoin design has flaws. The biggest are scalability issue and lack of privacy for its users.

Hexxcoin started in early 2015 as a Crave fork but got quickly abandoned by the original developer, then in early 2017 a new developer emerged and proceeded with the "HexxCoin Swap 2017" on which the code got updated to a Zcoin fork. In late May this developer stopped responding so Hexx was again on the brink of being labelled a "dead coin". Then in late December our new developer took over. Quickly the community got together and an initial Hexxcoin team was introduced, a new Logo and Website were just the beginning...

Hexxcoin team is solving the privacy problem for the users. Below we provide some current solutions to the problem, examine cryptocurrencies for their strengths and weaknesses, and outline a rational for Hexxcoin design. Also, we address a model of governance, monetary policies, and future plans for Hexxcoin development.

2. Problem: Bitcoin transactions are not private.

It is commonly known that the users' anonymity is not a prominent design feature of Bitcoin as is the case for most cryptocurrencies. Furthermore, it is not possible to prevent an analysis of the existing transaction history by a blockchain graph. All transaction information is publicly available in the blockchains. Anyone with full node client can get access to this information.

There are three vectors of attack which can de-anonymize pseudo-anonymous bitcoin user's and can reveal user's identity via simple network analysis:

1. Transaction origins,
2. Transaction destinations,
3. Transaction amounts.

3. History of Privacy Solutions

There are several known approaches to mitigate this problem. First and oldest one is a use of transaction mixers. Ring signatures were the next solutions to be implemented into some cryptocurrencies. This approach is used in Monero, one of the well known privacy focused cryptocurrencies. Nowadays Monero uses a Ring Confidentional transactions as an extension of ring signatures. Two more recent approaches are ZK-Snarks and Zerocoin protocol. These two solutions use cryptographicaly proven techniques to solve a problem of privacy or lack thereof.

a. Transaction mixers

Transaction mixers operate in the following fashion: outputs of several transactions join together as inputs of a mixer transaction. Outputs of the resulting transaction send coins to the original recipients, however, since original inputs and outputs are mixed in one transaction they cannot be link to each other. But the transferred amounts can be traced back. It can easily be avoided by splitting output amounts randomly. At first glance it seems as a feasible solution to the problem. However, there are several problems with the Bitcoin mixers.

Mixer operator **-** Mixer operators take incoming transactions, mix them and send them back to their users. However, these operators accept incoming transactions from users and do not send anything back. To put it simple, they can just steal users' money. However, if a mixer operator has a long operation history and a good reputation the risk can be minimize, but not entirely ruled out.

The most damaging to users' privacy can be a case when a mixer operator is a malicious actor who facilitates creation of the joint transactions, but at the same time keeps all the information about original transactions. And it makes the whole purpose of mix transactions invalid. Moreover, there is no way to proof that a mixer operator does not keep information about the incoming transactions

Low volume - If a mixer has a low volume of the transactions, a network graph analysis is still possible.

As a result, we can conclude that the mixer is not a viable solution for providing a transactional privacy for Bitcoin users.

b. Ring signatures and Ring Confidential signatures.

Ring signatures use decoy inputs alongside with the intended signature inputs. As a result, a third party cannot differentiate real inputs from decoy ones. Ring Confidential signatures are an extension of Ring signatures, they hide an amount of money sent as well as using decoy inputs. However, there are certain problems with Ring Signatures as well.

Bloating the Blockchain - If cryptocurrency uses Ring signatures, and does not make them mandatory to all transactions in the network, then only small amount of people will use Ring signatures. The main reason for this is the transactions with Ring signatures have much larger size than normal transactions and a user has to pay a higher fee for such transactions. This results in a low number of people who use Ring signatures leading to a possibility of the network analysis which is going to de-anonymize users even if decoy inputs are taken into account. Monero, is one of the well known cryptocurrencies, that mitigates this problem by enforcing Ring signatures for all transactions. Since they have high volume of transactions every day, a network analysis is infeasible at this point. But it comes with the cost of a bloating blockchain.

Timing analysis of the network - An adversary can monitor a time when a transaction is submitted to the network, and link it to the identities of the real people. It can be done by controlling a large proportion of the network nodes. It is possible for any party with sufficient resources.

c. ZK-Snarks

A full technical description for ZK-Snarks protocol we refer you to the Zcash Protocol Specification paper. The following is a high level overview of this technology. There are several cryptocurrencies which implement this protocol in order to achieve privacy for their users. Zcash is well known and is the first cryptocurrency to implement this protocol.

Firstly, private transactions are optional for Zcash network. This solution prevents unnecessary blockchain bloating caused by private transaction usage. Secondly, all private transactions get into the private transaction set, and in order to spend a transaction from that set a spender must reveal a cryptographical proof that the transaction exists in the set without revealing which one. It means that it's impossible to know which transaction is spent from the set. Moreover, since it can be any transaction from the set, it becomes impossible to trace ZK-Snarks transactions. And it's clearly an improvement over Ring signatures which we discuss in the previous section, since Ring signatures are using only a limited set of the transactions in order to obfuscate private transaction.

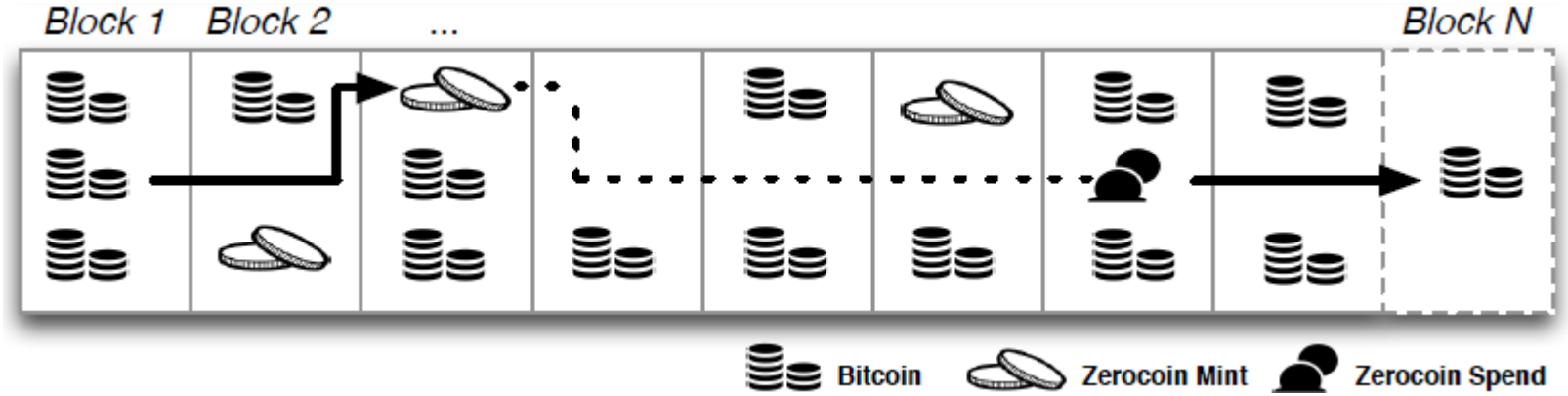
From cryptographical point of view ZK-Snarks protocol sounds as a viable solution for private transactions. However, there several problems with it as well.

Protocol Parameters - ZK-Snarks protocol needs a trusted setup for choosing initial protocol parameters.
And, an adversary who can get access to those parameters can compromise all transactions which are currently in a private transaction set. Also, such an adversary can counterfeit as many coins as he wishes in the private set. And what makes this problem more severe, an outside observer cannot detect it.

Zcash team had an elaborated procedure during which those original parameters were destroyed. We refer our readers to Z cash website for more information. However, it's a matter of trust to the Zcash developers and some people reserve some doubts about it.

d. Zerocoin protocol

Zerocoin protocol was first described in "Zerocoin: Anonymous Distributed E-Cash from Bitcoin" paper by Ian Miers et al. As with ZK-Snarks we refer our readers to this paper for extensive description of the Zerocoin protocol. Here we are going to give only its short outline.



Firstly, Zerocoin protocol uses a cryptographically strong accumulator, which is similar to the private transaction set of ZK-Snarks protocol. However, there are some differences. Users can mint coins of predetermined value for using in private transactions (1, 10 ect.).

Those coins can be sent to the accumulator. And later be retrieved by a spender without revealing which coins he is spending. As a result any coin from a whole set of coins in the accumulator can be an original coin. It makes it impossible to trace private transactions which use Zerocoin protocol.

Secondly, as with Zcash, private transactions are not mandatory in the network. It prevents unnecessary blockchain bloating.

To set up a cryptographical accumulator Hexxcoin used parameters from RSA Factoring Challenge which was announced by RSA Laboratories on March 18, 1991. During this challenge two big prime numbers were chosen, multiplied together and then destroyed. After that the participants of that challenge tried to find the original prime numbers to receive a monetary reward.

After 27 years from the start of the challenge no reward has been claimed. And it will probably be impossible to factor out the integers of factoring challenge. A number from RSA-2048 challenge is used in Hexxcoin network.

4. Hexxcoin description

a. Parameters

Hexxcoin has an average block time of 2.5 min, which makes it 4 times faster than Bitcoin. Given a recent huge delays for transaction confirmations in Bitcoin network, Hexxcoin block time seems more reasonable than the original 10 min average block time for the Bitcoin network. Also, it has a good balance between the confirmation time and the block orphanage rate which is clearly an issue for a short confirmation time between the blocks.

Currently, the Hexxcoin block size is 4 Mb. At the current network load it seems as an appropriate value for the foreseeable future. However, if there is a need to increase that number Hexxcoin team is ready to accommodate such demand without extensive delays.

b. Monetary policy

Current supply of Hexxcoin is just shy off 1.5 mil and the max supply is 9,999,999 hexxcoins. Reward per block is **2** hexxcoins, which means the lowest inflation rate out of all coins that use Zero protocol. Distribution of the rewards:

- Mining – **0.7** hexxcoin per block will be distributed among miners.

- Xnodes – **0.7** hexxcoin block reward on every block will be distributed between Xnode owners.
- Xnodes require to have 2000 hexxcoins, a dedicated IP address and to be able to run 24 hours a day.
- Community fee - **0.5** hexxcoin per block.

Funds will be used to pay for new exchange listings, marketing and to the development team. Approximately in 2 years, once enough Xnodes are built, the block reward for the community fee will be removed and instead used for staking. **0.1** hexxcoin per block is going to be allocated for Community nodes. In order to be able to cut 0.5 rewards per block for the community funds in the future, some of the members propose an idea of building enough Xnodes so that the project can be funded from Xnode rewards. For that reason 0.1 hexxcoin reward will be used to build Xnodes. Once a sufficient amount of Xnodes is reached, **0.5 + 0.1** rewards per block will be removed. Instead, 0.6 hexxcoins per block will be used to introduce staking. In 2 years Hexxcoin is going to have mining, Xnodes and staking at the same time.

c. POW algorithm

Hexxcoin is using Lyra2z330 algorithm which is designed primarily for CPU-mining. ASIC-GPU resistance ensures a better decentralization than Bitcoin, since powerful mining farms will have a much harder time running huge amounts of computers. CPU only mining also encourages anyone with a Computer / Smartphone to become a miner. Greater number of miners will guarantee better security and efficiency of the network.

The algorithm is most efficient on using only a part of the CPU. Most mining procedures require device to be at a 100% load all the time, Hexxcoin with an "ECO friendly" approach tends to lower the global footprint of power consumption.

d. Advantages over other Zerocoin protocol implementations

There are several Zerocoin protocol implementations for cryptocurencies except Hexxcoin. Zcoin and Zoin are two examples of such implementation. On the protocol level Hexxcoin uses the same Zerocoin protocol in order to bring privacy into the blockchain. However, there are some differences on the project governance and monetary policy levels.

Firstly, Hexxcoin has a limited total supply of 9,999,999 coins which is substantially lower that other coins implement.

Secondly, Hexxcoin project does not have any investors. As a result, the decisions about coin development are entirely driven by the community and not by some outside entity.

Thirdly, the community development fund tax, as percentage of total supply, is much lower than other implementations have.

e. Hexx Masternodes – Xnodes

Xnodes are a new addition to Hexxcoin blockchain, adding transparency, security, speed and finally decentralization. With that anyone holding 2000 HXX is able to run a Xnode and with that generate passive income. Profitability will depend on the number of Xnodes in the network, but one value is certain - global revenue – all Xnodes will generate on average 403.2HXX per day.

f. Future plans – Merging – BitcoinZeroX

Hexxcoin with its low circulating supply and unique features will be used to "extend" the functionality of other cryptocurrencies with a low markup – this type of solution is also called merging or co-forking.

In Q3 2018 it is planned to merge Bitcoin blockchain with Zero protocol, creating completely new coin BitcoinZeroX (BTCZ). It is going to be the first Bitcoin fork that have zerocoin protocol and Masternodes. After Combining Unspent Transaction Output (UTXO) set of Hexxcoin with the UTXO of Bitcoin, every Hexxcoin and Bitcoin holder will receive BitcoinZeroX (BTCZ) at 1:1 ratio. BitcoinZeroX will not have developer fund and will be completely independent from Hexxcoin. On the other hand, the development of Hexxcoin will also continue.

The BitcoinZeroX project will be an independent initiative from Hexxcoin and will therefore require its own dedicated whitepaper that will follow this one shortly. A future announcement will be made soon.

g. Future plans – Development

With regular income from the development fund the future looks bright, once the initial functionalities get hardened we will proceed with PoS integration and Light Wallets / Mobile Wallets. We will also try to accept all community suggestions in future development.

h. Future plans – New Exchanges

Hexxcoin team will provide at least one new Exchange listing in 2018. All major decisions will be decided with a community vote, leaving everyone to provide their input.

5. Conclusion.

Hexxcoin is a privacy focused coin. It uses Zerocoin protocol in order to provide transaction privacy for its users. Privacy transactions are optional for the coin users. We strongly believe that Zerocoin protocol has several advantages over other privacy focused solutions. Our model of governance and monetary policy put Hexxcoin ahead of the other Zerocoin protocol based coins and with that our main objective is to maintain and further develop an easy to use cryptocurrency made for the future!

6. References

- Analysis of Anonymity in the Bitcoin System, Fergal Reid, Martin Harrigan, 2012
- Bitcoin Transaction Graph Analysis, Michael Fleder et al, 2014.
- Ring Confidential Transactions, Shen Noether, Monero Research Lab.
- Zcash Protocol Specification, Daira Hopwood et al. 2018
- Zerocoin: Anonymous Distributed E-Cash from Bitcoin, Ian Miers et al.
- A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, Sarah Meiklejohn et al.