Table of Contents

Introduction 1

Market issues 2

ZeCash Missions 3

Practical application 3.1

Competitive advantage 3.2

Blockchain application 4

ZeCash on Proof-of-Stake 4.1

What is Proof-of-Stake 4.1

Advantage of POS 4.1

Staking with ZeCash 4.2

Advantage of POS 4.2

Staking Selection with CABS and RBS 4.2

POS Security with ZeProtocol 5

Nothing at Stake 5.1

51% Attack 5.2

Double Spend 5.3

Stake Grinding 5.4

Synchronized Check Pointing 5.5

ZeCash Anonymity with ZeAnon 6

Stealth Transaction 6.1

Transaction Re-Mixing 6.2

Ring Signature 6.3

ZeCash Fast Processing 7

ZeCash will offer Lightning Network System 7.1

ICO Details 8

ZCH Token 9

ZeCash will offer Lightning Network System 9.1

Conclusion 10

This document describes the approach to creating ZeCash Coin. Below is a detailed description of the project concept, the proposed solution technical characteristics, as well as the projected benefits that ZeCash token holders and ZeCash project investors will extract. The document is of an informational nature, not being an offer or an appeal to buy or sell shares or other securities.

1. Introduction

The changes that the world economic system has experienced in the current decade are more significant and weighty than anything that happened throughout the twentieth century. The reason why all the usual financial institutions are forced to change for the better, reviewing the basics of their existence, is the widespread dissemination of cryptoeconomics.

Its development is extremely rapid, as it does not tolerate its weaknesses and imperfections. This development course is most evident on the example of digital economy key element self-improvement - cryptocurrency.

Cryptocurrency, otherwise called digital currency is one of the innovations the Internet has to offer. Years back, the thought of online currency would have earned a shrug or the scrunching of noses, but after Bitcoin came and rocked the world, the thoughts of millions have changed.

Cryptocurrency is now a household name. Notwithstanding that, many people have heard of the term Cryptocurrency, can it be boldly said that many people know of its meaning? In a nonprofessional's term, Cryptocurrency is online money, a form of exchange, accepted by many people and recognized worldwide. It is fashioned out to provide anonymity, security and be hack proof all in one.

A reader might ask himself or herself what makes the currency secure and hack proof. That would be no other than the cryptography system. This online system makes use of algorithms to make sure the transaction-wherever it is carried out in the world is secure. It not only secures the transaction carried out, it ensures that illegal creation of additional bits of the currency is impossible, and tops it all off, with verification of the assets transferred.

It is, in fact, old news that many online criminals prowl the internet seeking for victims to rip off, just like pickpockets that stroll the earth, seeking someone to steal from.

That was where Cryptography was born. Unlike in the case of a pick-pocketed, one could do little or nothing to stop his effort, but in Cryptocurrency, one is rest assured that the online currency would remain in his wallet for as long as he wants because of the cryptography.

Unlike ordinary currencies that are capable of being easily confiscated by law enforcement agencies, currencies held in the crypto form are difficult to be seized because of the cryptography. The foremost online currency known to man is the Bitcoin, created in 2009, and still lording over the realm of Cryptocurrency.

For the past decades, many cryptocurrencies have reared their heads, offering various packages and benefits to their investors. Many have lived up to their promises, while some are left trailing behind trying to punch through the realm. More than a thousand currencies orbit around the internet, with Bitcoin, raising the flag.

Ten years ago, Bitcoin committed a financial revolution, irrevocably undermining the basis of the notion what money is and how it should function. Now it is obvious the first cryptocurrency has many flaws. Each of the altcoins appearing on the market carries an attempt to improve a number of decisions sealed in Bitcoin.

To create ZeCash Coin, the project team used the best created by the crypto industry, successfully combining the tools and procedures customary for users and developers with original, plagiarism free innovations, because even today we can guarantee a high interest in ZeCash Coin.

2. Market issues

Despite the fact the crypto industry emergence has saved the financial world from the traditional economy remnants, it has also created a number of internal problems requiring the attention and participation of developers.

Turning to Bitcoin, an improved alternative offered by ZeCash team, we find out that a number of the system technical aspects are hopelessly out of date, which deprives Bitcoin of the ability to fully meet the needs of users, especially if it is a long-term investment perspective.

One of the most pressing issues that BTC users face daily are high commissions for transactions. In 2018, their value was somewhat reduced, but still remains unreasonably high in comparison with the commission of Bitcoin alternative platforms. In addition, the transaction speed is reduced and will continue to decline. In the Blockchain by Bitcoin, the increase in the number of users stimulates a drop in the speed of operations.

Experienced miners repeatedly stressed the fact mining the first cryptocurrency in the face of the computing tasks' high complexity became an unprofitable enterprise. Therefore, they have to mine the altcoins, and then, if necessary, change them to BTC.

Up to date, the issue of anonymizing the network has not been resolved. With some effort, the origin of transactions can be a detailed representation of the financial history of any user. That is the reason many traders and bitcoin-entrepreneurs wanting to remain anonymous, gradually declare off Bitcoin.

All mentioned downsides require immediate resolution, but from the point of the technologies used, Bitcoin remained at the same level as ten years ago, from the launch moment.

Crypto environment regularly encounters attempts to supplement or refine the technologies through which it exists. Therefore, there are hardforks and altcoins. To date, there are more than a dozen Bitcoin hardforks. Each of these projects is accompanied by a broad media coverage, but it is worth acknowledging that often the interest is maintained artificially, since none of them is an essential innovation, representing a secondary copy of the first cryptocurrency.

ZeCash team has focused on eliminating the above downsides by implementing a technical initiative that will gain wide popularity among all the crypto holders.

3. ZeCash missions

ZeCash team does not set excessively global goals, does not make loud promises. We are talking only about the mechanisms' improvement and processes inherent in the cryptocurrency structure. We got rid of the downsides that prevented the first cryptocurrency full operation for ten years of existence, taking care of the following opportunities for users:

- **You can Mint/Mine and earn fixed interest with low fees.**
- **PoS security with ZeProtocol, which contain a Chain trust, and Delegated Shuffle.**
- **Anonymity with "ZeAnon" protocol, which allows transaction re-mixing, ring signature.**
- **Very fast transaction speed, no pending transactions guaranteed.**
- **ZeCash Proof of Chain/Stake always fair with Coin Age Based Selection.**

3.1 Practical application

ZeCash is a revolutionary cryptocurrency based on the PoS algorithm. The new currency was created to simplify e-commerce, make private payments, online businesses, and retail stores. Transactions in the network do not have commissions and are quickly implemented. Since free ZeCash mining is impossible, we can confidently talk about strict emissions and high security at the transactions time. The coin can be considered decentralized, unlike other cryptocurrencies, most of the capacities of which are controlled by only a few large pools.

Qualitative distinction of the new cryptocurrency is orientation to practical application. Despite the glut of the market with a variety of cryptocurrencies, today there is no simple and convenient solution for traditional calculations. Most currencies are used for speculative purposes, thereby losing their true purpose.

Globalization of cryptoeconomy will inevitably lead to the fact that soon almost all services will be paid for using digital currency, as it happened with bank cards in due time. This will be an important condition for scaling the ZeCash project.

3.2 Competitive advantages

The top altcoins' developers come to the perception that further development of their projects is impossible without technological changes.

From 2009 to 2012, all the cryptosystems, starting from Bitcoin, have been functioning using one-and-only Proof-of-Work algorithm. In 2012, through the efforts of the Peercoin team, a fundamentally different from PoW, the Proof-of-Stake algorithm appeared in the crypto world.

In 2017, the Ethereum platform, the second cryptocurrency after Bitcoin by market capitalization, announced the introduction of the Casper protocol. The essence of the innovation lies in the network switch from PoW to PoS algorithm.

The need for switch is due to several reasons. First, mining on the platform becomes unprofitable; the situation is similar to that experienced by Bitcoin. The unprofitable mining has a negative effect on the coin popularity. Miners prefer to obtain other altcoins, changing them after to BTC or ETH, if necessary.

PoW protocol implementation requires expensive mining equipment, a huge amount of electricity, and computing power. Large mining pools using expensive ASICs have a better chance of profitable mining than ordinary miners do. With the transition to PoS, Ethereum plans to return the democratic nature to crypto industry, re-opening access for all comers.

It is worth emphasizing that Casper for Ethereum is a future issue. It is still unclear how the security issue within the network will be resolved in case of switching to PoS. PoW, which is "used" by Ethereum, does not allow replacing the newly added block chain, but it is quite feasible in PoS. It is planned that at the beginning the system will function in PoW + PoS mode.

The democracy promised by the Ethereum creator looks unjustified because the vast majority of the profit will come to those users who have the most ETH coins when switching from PoW to PoS.

ZeCash works on PoS even today. The project team had time to make sure that the implementation of the algorithm was as safe as possible for holders and traders. To do this, we use a special tool, ZeProtocol, developed by ZeCash. Below we outlined the principles of its functioning.

In addition, the ZeCash mining is a lucrative alternative to other coins' mining, because the processing power is not used as it is replaced by a virtual resource. Acquiring ZeCash Coin, you get additional profit in ZeCash Coin just because you already have this coin in your wallet. All you need to run the PoS algorithm in the Blockchain is wallets on computers or smartphones of miners. The longer the user mints ZeCash Coin, the more he earns. The project team returns to the status of a highly profitable industry of crypto business.

Through the ZeCash platform, users with low initial capital have the opportunity to securely enter the crypto industry with a stable income guarantees, because the need of purchasing the expensive mining equipment is eliminated.

4. Blockchain application

For proper functioning, the cryptocurrency requires such a feature as Blockchain. The blockchain is a collage of blocks, which are records growing incessantly, and these blocks are joined with the cryptography system securing it from outside attacks.

The blockchain, in an average person explanation, is more or less a ledger, but in this case, it is on the internet. It has imprinted on itself transactions using the Cryptocurrency like Bitcoin, and its associates, the cryptography is at hand to reduce the attack by hackers. The usage of blockchain is not subjected solely to Cryptocurrency, but has been proven invaluable in crowd funding, and even voting online. Many experts find out Blockchain important value in technologies, such as online voting.

Each block is linked using the cryptographic hash pointer, forms the block chain, and possesses the transaction data, timestamp for each transaction done. Being resistant to changes in data, it functions as a ledger managed and monitored by a network in a peer-to-peer mode that validates the creation of new blocks, using a line of protocols. Once data is earmarked to a block, it is impossible to be changed without altering all subsequent blocks. It makes use of the decentralization unlike the traditional banking that focuses on centralization.

4.1 ZeCash on Proof-of-Stake

What is Proof-of-Stake?

Proof-of-Stake (PoS) is a type of algorithm in which distributed harmony is achieved by a Cryptocurrency blockchain network. The creator of the next block in PoS based Cryptocurrency is selected or chosen through various combinations of random selection and wealth or age (the Stake). Compared to Cryptocurrency based on Proof-of-Work (PoW) such as Bitcoin make use of complicated cryptographic puzzles in order to mark transactions valid and create new blocks.

There must be a way of choosing the next valid block in any block chain. If the selection is done via account balance, it would result in an undesirable centralization as the single richest member would have a permanent advantage. In order to avoid this, some methods have been devised. Before we discuss about the Proof of stake scheme and protocol in ZeCash coin, let us discuss the forerunner, Proof-of-Work (PoW).

The first type of cryptocurrency, the Bitcoin, uses the Proof-of-Work. It makes use of puzzles that align to cryptography to authenticate the transactions done and even mine, create new blocks. Bitcoin and Litecoin are cryptocurrencies known to use PoW.

- **Proof-of-Work use Miners to mine blocks**
- **Proof-of-Stake use Minters to mint blocks**

Advantages of PoS

The currencies using Proof-of-Stake can be thousand times more cost-effective than the Proof-of-Work, which relies on the use of energy. Following a Bitcoin mining-farm operator, the energy consumption totaled 11,388 KWh per Bitcoin in 2014. This is equal to combusting 752 gallons of gasoline, in terms of carbon production.

In addition, the incentives gained by block-generators are different. In the case of Proof-of-Work, the generator may or may not own any of the currency they are mining. Maximizing their own profits is the only incentive of the miners. While in Proof-of-Stake, the miners guiding the coins are always the ones who own the coin.

4.2 Staking with ZeCash

It is an incentive process to reward people that mint their ZeCash into their wallet for transaction validation. Our users are involved in buying the coin that will remain in a wallet for a certain fixed period. It is same as putting money in a fixed deposit for a fixed period. Here, the owner of a new block is chosen on the person's stakes. The stakes translate to the extent of the user's wealth or amount of ZeCash coins the holder has in his possession. In staking, mining does not occur; instead, the creation of new blocks is minted. The Minter creates the new blocks in the system and makes sure transactions are authenticated. To authenticate transactions, the Minter is expected to place his currency units on "stakes", meaning they access their ZeCash Wallet to maintain the network. In a fixed deposit, you will get interest as a reward. In Proof-of-Stake, the reward would be the additional coins. The below-given factors will define how the amount is distributed.

Interest

The more time our ZeCash holder will Mint (keep their coin), the higher is the reward. For three months, you will get 15%, for six months you would be getting 30% and for 12 months, it would be a full 60%. The amount of given reward can be counted through the linear dependence between The amount of given reward can be counted through the linear dependence between n_d that represents how long the coin has been holding in days and X_0– the actual reward.

$$X_0 = \frac{n_d}{365} * 5\%$$

It can easily be calculated that for 3 months you will get 15%, for 6 months you would be getting 30% and for 12 months it would be full 60%.

Staking Advantages

There is no need to spend a lot of money buying a big mining farm. Initial investment needed for that is just a simple computer connected to the Internet and a wallet with ZeCash Coin. The balance in the wallet will grow; you just need to be patient. Simultaneously, ZeCash coins value will grow as well. A profit is guaranteed as ZeCash Coin values will increase due to the price growth along with the number of coins you mint. That is how ZeCash Minting is functioning. The amount of coins you would be able to mint is exactly equal to the amount of coins you have in your wallet. It is very similar to holding the bank account on the PC.

Staking Selection with CABS and RBS

Weighting the Miner could be easily executed based on the amount of coins the user has, but it will cancel out equality because only the biggest Minters will be selected.
To tackle such an issue, ZeCash will use:

CABS (Coin Age Based Selection)

Here the minter is selected using ZeCash Coin age. Coin age can be translated loosely to how long the coins are held, and the coin age is multiplied with the stakes of the coins. To compete, your coin age must be above thirty days, and the longer the coin age the greater the probability of being selected. Once selected, the forger can stay on the throne for only ninety days to prevent those with longer coin age from reigning as forgers forever.
In practice it means that if we have Lina with 10 ZeCash coins been holded for 2 days, John with 20 coins each 3 days old, Andy with 15 coins each 4 days old, Jessy with 3 coins each 30 days old and Chris with 70 coins each 8 days old, Coin age for them will be 20, 60, 60, 90 and 560 respectively. In this case Lina isn't participating in minting at all, John and Andy have equal chances to sign a block as well as Jessy and Chris do despite Chris's obviously bigger Coin age.

RBS (Randomized Block selection)

The randomized selection method decides who will be the next Minter by combining the size of their stake and the lowest hash value. Since the stake sizes are made public, it is completely transparent. Staking schemes are more environmentally efficient and indeed friendly compared to the alternative that expends a lot on electricity for mining.

5. PoS Security with ZeProtocol. ZeCash solution

The best way to list the most used security breaches on Proof-of-Stake network and check how ZeCash fixes them, is to implement our ZeProtocol.

5.1 Nothing at Stake

Problem

In the event of a fork, the optimal strategy for any miner is to mine on every chain, so that the miner gets their reward no matter which fork wins. Thus, assuming a large number of economically interested miners, an attacker may be able to send a transaction in exchange for some digital goods (usually another cryptocurrency), receive the good, then start a fork off the Blockchain from one block behind the transaction and send the money to themselves instead. Even with just 1% of the total stake, the attacker's fork would win because everyone else is mining on both.

ZeProtocol Solution

ZeProtocol of ZeCash resolves this issue by using a double-block protection mechanism and coin age consumption.

Coins which have been held for up to 30 days begin to compete for the next block. Greater probability for signing the next block goes to older and larger sets of coins. Nonetheless, once a coin has been staked and used to sign a block, they must start with zero ‘coin age’ and thus have to wait for a minimum of 30 days before signing another block. It is also best to note that the probability of finding the next block reaches a maximum after 90 days to help prevent or stop very old or very large collections of stakes from controlling the Blockchain.

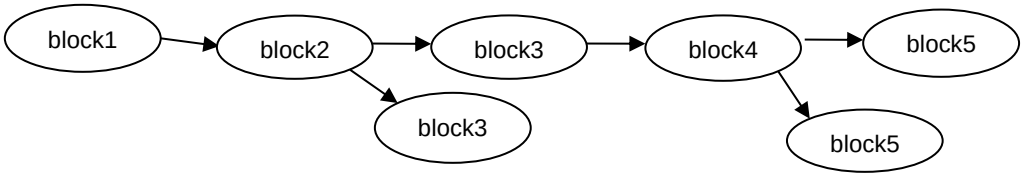
5.2 51% Attack

Problem

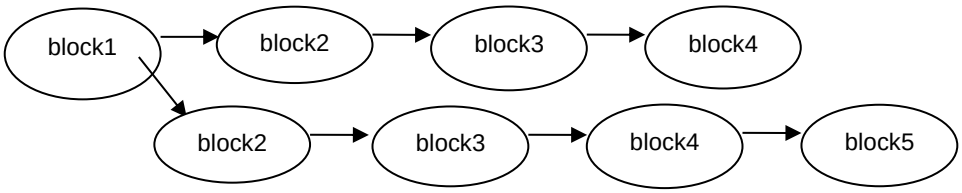
This problem occurs when a corner holds more than 51% of any given Blockchain. It is generally a result of a defense mechanism where coin which is used in stakes will get minted for a small period and then it cannot be sold on the exchange or anywhere.

The worse is that attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users and reverse transactions that were completed while they were in the network control. It happens because of Blockchain organization and its responses when fork appears.

Normal occasional forking

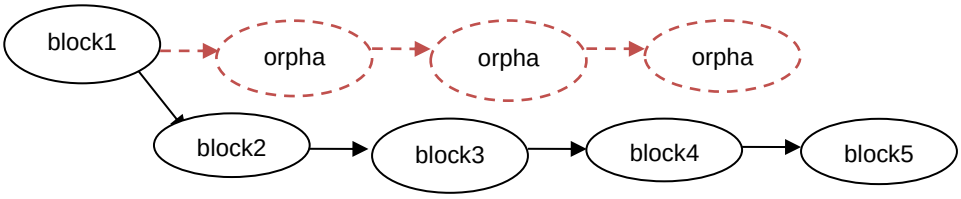


Rare forking



The attacker who can generate new blocks faster than others replaces the original part of the blockchain with the one created by himself and the protocol accepts the fictitious branch because now it is the longer one. Genuine blocks turn into the orphans.

Blockchain after 51% attack



Although many existing coins are highly vulnerable to 51% attack, but ZeCash is well protected.

ZeProtocol Solution

ZeProtocol will implement MOS (Maturity Operation System) a proprietary Algorithm where ZeCash coin has to be matured over a period, and then it can be used at the stake again. Coin can be minted for a period and therefore cannot be sold on the exchange.

In order to do that you have to compare it with the working of Bitcoin where the machines for mining are uninterrupted by 51% of attacks. Through ZeProtocol the attacker needs to wait for a long period before using the coins in a new attack.

In other words, 51% attack can easily be carried out without implemented MOS with $\propto$>50% for a particular holder, where

$$\propto = \frac{holdedCoins}{allCoins} * 100\%$$

For ZeCash this formula changes a bit

$$\propto = \frac{holdedCoins - immatureCoins}{allCoins} * 100\%$$

This means much more than 50% of all coins need to be possessed by one person to succeed in such type of an attack. Even if attackers achieve their aim $\propto$ sharply decreases to low value like nearly 5%, which make the next attack almost impossible.

Note that our simulation results show that 51% attack is less likely to happen in Proof-of-Stake, as it would result in purchasing more than half of the coins and is more expensive than acquiring 51% of Proof-of-Work hashing power.

5.3 Double Spend

Problem

Double spend attacks happens in the following way: the attacker first sells all his coins and then will publish a new version of the Blockchain in which the coins' sale will not work. In the above scenario, the market will be able to absorb the large amount of the coins from the total supply. This would create a market crash, as coins will no longer be viable.

ZeProtocol Solution

ZeProtocol will use a proprietary Adjusted Confirmation Based on Volume (ACBV). For example, increasing the confirmation N from 6 to 10 will reduce the chance of a double spend by ~100 times for an attacker who has gathered 30% of network minting power.
Let us take a closer look at possibility *p* of a successful attack that can be calculated as

$$p = \frac{n * dayWeight}{difficulty * 2^{32}}$$

Where *n* coins are passing the minting hash test.

When the coins have reached max age (90 days), day Weight is 60:

$$p = \frac{n * 60}{difficulty * 2^{32}}$$

The hash test is done every second, so the probability to mint a block within 10 minutes is:

$$p_{10} = 1 - (1 - p)^{60*10}$$

$$p_{10} = 1 - (1 - \frac{n * 60}{difficulty * 2^{32}})^{600}$$

To reorganize the blockchain and change the last N blocks, an attacker will have to find *N* consecutive blocks. Let us imagine that the attacker has m_{90} coins at least 90 days old distributed evenly in n transaction outputs of $\frac{m_{90}}{N}$ coins each.

The probability of success is:

$$p_N = p_{10}^N$$

$$p_N = (1 - (1 - p)^{600})^N$$

$$p_N = (1 - \left(1 - \frac{\frac{m_{90}}{N} * 60}{difficulty * 2^{32}}\right)^{600})^N$$

$$p_N = (1 - \left(1 - \frac{m_{90} * 60}{N * difficulty * 2^{32}}\right)^{600})^N$$

6 blocks deep reorganization with 10000000 coins has while for *N = 10* this probability will only be 0.000015% which is about 700 000 times less.

The network depending on stakeholder variance and network difficulty will adjust the confirmation N. ZeProtocol will also make any block cemented. Meanwhile, it is safe to assume that the network recognizes this block and will not easily switch to a different block, even if a longer branch is presented. Once a block from ZeCash achieves a majority (and some more time is allowed for this majority to spread in the network), it is unlikely the network will ever switch away from this block.

5.4 Stake Grinding

Problem

The attacker has a small amount of stake, goes through the history of the Blockchain, and finds places where his stake wins a block. With an object of winning, he modifies the next block header until some stake he owns wins once again. This attack requires a bit of computation, but definitely is not impossible.

ZeProtocol Solution

ZeProtocol will use mixed inputs of delegated Proof-of-Stake where each block minter gets to create one block before the order is reshuffled and everyone gets another turn. In addition, to have fair distribution between a minter who has 50% support rather than 10% support, we will reward all minters in proportion to their stake / support. ZeProtocol will start by creating blocks in a deterministic fashion. Each block minter would be chosen basing on the user that is the most underrepresented in a given minting period. They would be chosen to be the next block minter. After a new block created, the representation is updated and the next minter is chosen in the same fashion.

5.5 Synchronized Check Pointing

Problem

In this attack, you would be able to add the fake node and the entities in the network of the Blockchain. As there are no checkpoints, this attack would be quite successful and cheap initially. When a node creates a block then it is known as minting. As the number of minting nodes increases, the network would become more secure and safe. When the network is in the initial phase, the attack is relatively very cheap. The network-bootstrapping phase during this time uses the synchronizing checkpoints to deter and protect against the malicious entities. It is used as a temporary measure and when more mining nodes are added to the network then this precaution is no longer needed.

ZeProtocol solution

ZeProtocol uses hardcoded checkpoints that would be able to mitigate this kind of attack when a new node connects to the network, which is yet to be downloaded by the Blockchain. In addition, ZeCash will be also using synchronized checkpoints. Coins which are spent on the latest checkpoints cannot be used so all coins are accumulated after that checkpoint.

The concept is that the standard client will accept all transactions up to the checkpoint as valid and irreversible. If anyone tries to fork the blockchain starting from a block before the checkpoint, the client will not accept the fork. This makes those blocks "set in stone".

6. ZeCash Anonymity with ZeAnon

Users are given a degree of anonymity that traditional banking systems do not offer. The traditional banking system is obligated by law to show and expose whoever deals with them, and this kills whatever anonymity the traditional system might have claimed to have. Since the Blockchain ledgers are made public, the cases of anonymity over the years have been raised. Quite a number of users love the comfort of anonymity for private reasons, which might range from its not being able to be confiscated by law enforcement agencies, and the sake of privacy. Bitcoin uses pseudo anonymity that does not allow a user to be linked to his name or home address, but can instead be linked using the public Bitcoin address. One can be traced only through the address, but not through the personal details.

Though Cryptocurrency offers pseudo anonymity, other steps can be taken to seal the deal:

➢ one way is to reduce revealing many personal details. It is noteworthy not to link Cryptocurrency address to your personal details.

➢ another method involves the simple way of trading Bitcoins for cash. Many technologies that could further encrypt your cryptocurrency address exist. These include CryptoNote, CoinJoin, Secure Wallet, TumbleBit, Tumblers, and Tor etc.

ZeCash will use the below feature to reinforce anonymity of transactions.

6.1 Stealth Transaction

ZeAnon use of several cryptographic tricks is mostly based on the Diffie-Hellman key exchange. This will let the users accept the payments on the address that has never been generated or has never been seen before. Why?

In the view of increasing your privacy that will also give you the security benefits as well, we strongly believe that users will generate a new address for every transaction they receive. This is not an airtight solution but it will make it significantly harder to connect with this address in the real world. This identity would be used in both the sending and the receiving end of the transactions. This also means the receiver has to share the new address with the sender each time a transaction is made. This will be a lot of hassle and this would be almost impossible and inconvenient in the end. It is not considered an ideal solution with the perspective of privacy either. When the new address is shared on the insecure channel, the privacy is also potentially lost.

Stealth transaction starts with generating a stealth key pair by receiver, what can possibly be done even before any payment was going to be made. It is this stealth public key that he, for example, posts on his website as a donation address. (As such, it has also called the “Stealth Address.”) He does not share his stealth private key with anyone at all.

When the sender wants to pay the receiver, he generates a “throwaway” stealth private key for himself; specifically for that one transaction. He then takes the receiver's stealth public key (or Stealth Address) and combines this with his own throwaway stealth private key, to generate an address and sends coins to this address.

At this point, no one can spend coins on this address because no one knows (nor is able to generate) the corresponding private key.

The sender can allow the receiver to spend the coins by sharing his throwaway stealth private key with him.

6.2 Transaction re-mixing

Today all the transactions are recorded and then made available publicly to the Blockchain. ZeCash will use different mixing techniques in which several users create a transaction by joining their inputs. In order to maintain their privacy, all inputs should share the same value, as once the transaction is created there is no way of telling which input corresponds to each output. If the inputs hold different values, then it will be much more straightforward.

There are several ways of implementing a transaction re-mixing scheme, the first and more simple one relies on a third party receiving all inputs, outputs and signatures, and building the transaction from the participants. The other one, which is more elaborate, does not need any third party, since every user acts as a blind-signing server.

6.3 Ring Signature

ZeAnon will use a type of digital signature, which is used with the cryptography and is performed by members of the users' group that have the keys.

Ring signatures are generated using a combination of sender's account keys with public keys on the blockchain. It makes it private as well as unique. It hides the identity of the sending participant as it is computationally impossible to assess which group members' keys were used to generate the complex signature.

To an outsider, all signatures in ring will be equally-likely without the possibility of knowing which is the genuine one. The transaction's key image on the network, which is used to authenticate and verify the transaction during the mining exercise, ensures that the transaction is confirmed only through a secure and standard manner without any possibility of duplicity or hacking.

Ring signature is very similar to the group signature but they are different in two significant ways. First, there is no way you will be able to revoke the individual signature. Secondly, any group of users can use this without doing the additional setup.

Why does ZeCash need to use these protocols to provide an unlikeable solution?

No coins are anonymous. If you monitored the peer-to-peer network and analyzed the public Blockchain, then you would be able to trace the identity. This can also be done by knowing your customers and by anti–money laundering regulations. This is not a great privacy feature. Users might not want to let the world know their personal spending and incomes. This business information can be leaked to the competitors easily and we believe each human deserves to choose or not choose anonymous transactions, as each person is able to choose anonymous messaging like Telegram.

7. ZeCash fast processing

Blockchain technology is known to possess a fast processing system. Though the present technology is fast, the VISA network is currently faster, but that will change. A new prototype faster than the VISA network which is 56,000 transactions per second, is about to meet public consumption. It is expected to be about 440,000 transactions per second. Currently, the Bitcoin network processes about seven transactions per second, while PayPal does over 450 payments per second. The prototype of the new Blockchain network is expected to be resistant to forking. Without forking as expected by the new research, the need for confirmations would no longer be necessary. Transactions would easily be carried out at a fast pace.

Many international bodies use Blockchain technology such as Deutsche Bank. It uses the technology in phases like settlement of Fiat currencies, and their labs in Silicon Valley are involved in experimenting on the technology. Transaction times and finality in the Blockchain are two different things. Immutable transactions on a Blockchain are time based. This is why exchanges need more confirmation time for some coins.

Fast block times do not mean they are as secure as long block times. A Bitcoin transaction with one confirmation is more secure than a Litecoin transaction with two confirmations. Segwit transaction malleability will allow transactions to be instant, but immutable confirmations will still take time.

7.1 ZeCash will offer Lightning Network System

Instant Payments

Lightning-fast Blockchain payments without worrying about block confirmation times. Security is enforced by Blockchain smart-contracts without creating a single Blockchain transaction for individual payments. Payment speed measured in milliseconds to seconds.

Scalability

Capable of millions to billions of transactions per second across the network. Capacity blows away legacy payment rails by many orders of magnitude. Attaching payment per action/click is now possible without custodians.

How It Works?

The Lightning Network is dependent upon the underlying technology of the Blockchain. By using real Bitcoin/Blockchain transactions and its native smart-contract scripting language, it is possible to create a secure network of participants, which is able to transact at high volume and high speed.

Low Cost

By transacting and settling off-blockchain, the Lightning Network allows for exceptionally low fees, which allows for emerging use cases such as instant micropayments.

Cross Blockchains

Cross-chain atomic swaps can occur off-chain instantly with heterogeneous blockchain consensus rules. So long as the chains can support the same cryptographic hash function, it is possible to make transactions across blockchains without trust in 3rd party custodians.

Bidirectional Payment Channel

Two participants create a ledger entry on the Blockchain, which requires both participants to sign off on any spending of funds. Both parties create transactions that refund the ledger entry to their individual allocation, but do not broadcast them to the Blockchain. They can update their individual allocation for the ledger entry by creating many transactions spending from the current ledger entry output. Only the most recent version is valid, which is enforced by Blockchain-parsable smart-contract scripting. Either party without any trust or custodianship can close out this entry at any time by broadcasting the most recent version to the Blockchain.

Lightning Network

By creating a network of these two-party ledger entries, it is possible to find a path across the network similar to routing packets on the internet.

The nodes along the path are not trusted, as the payment is enforced during a script, which enforces the atomicity (the entire payment either succeeds or fails) via decrementing time locks.

Blockchain as Arbiter

As a result, it is possible to conduct transactions off-Blockchain without limitations. Transactions can be made off-chain with the confidence of on-Blockchain enforceability. This is similar to the person that makes many legal contracts with others, but does not go to court every time a contract is made.

By making the transactions and scripts passable, the smart-contract can be forced on-Blockchain. Only in the event of non-cooperation, the court is involved. However, the result is deterministic with the Blockchain.

Credit to https://lightning.network/ protocol that ZeCash will implement for his transactions.

8. ICO details

To finance the ZeCash revolutionary cryptocurrency development, an ICO will be conducted. On March 31, the public sale to investors was launched; it will last until December 31, 2018. To date, a system of bonuses allows you to get an additional 10% benefit.

After the fundraising phase ends, the project development will take place according to the compiled and declared Roadmap on the website. To date, the project team is already negotiating the token listing on leading crypto-exchange exchanges.

9. ZCH Token

The ZCH token will be released on the ERC-20 basis. 500 million tokens will be issued at an initial price of $ 0.10.

Sixty five percent of the tokens' total number sold will be directed to the development and launch of the new ZeCash cryptocurrency; 20% will be distributed to the product marketing campaign, the remaining 15% will cover other operational and legal costs.

As the ICO ends, all unsold tokens will be burned. At this stage, the token is already available for reservation on the official website.

9.1 ZCH price growth drivers

The following number of factors provides the ZCH price growth:

- The combination of unique technological developments made up in a safe and convenient platform, functioning according to user-friendly principles. The making profit scheme for investors and token holders is calculated and presented in the most detailed manner. ZeCash is a safe investment and guaranteed income.
- The primary entry availability into the crypto industry will ensure the popularity of the coin among people who are still not connected with the crypto world, for example, among the owners of offline business.
- Considering each user has the right to confidentiality of the financial history, our team returns anonymity to the ancestors. Every user interested in conducting anonymous transactions will use the ZeCash platform.
- There is no better existing coin for mining as ZeCash. Mining requires only two conditions: a created wallet and the presence of ZeCash Coin in it.

10. Conclusions

An essential shortcoming of the solutions suggested by the teams of different projects in trying to cope with the difficulties of the current crypto-economic situation is the lack of an integrated approach to the operation of existing platforms and their derivatives. Often a single project solves one-and-only task, but in modern conditions, this is not enough because several major problems are at the forefront of crypto community.

The biggest problems among them:

- Lack of proper security level both in case of users' anonymity and in the matter of the inviolability of stored crypto funds.
- Manipulation of the cryptocurrency rates through inside trading and fake news.
- Unprofitability of mining (costs for purchasing and maintaining equipment are not compensated by income from extraction).
- Slow transactions and high commissions.

ZeCash team has developed a comprehensive solution aimed at eliminating all the listed problems.

ZeCash is a chance for those who did not have time to enter the crypto industry on favorable terms, i.e. without major investment risks and the purchase of expensive mining equipment. Having reconsidered the developments created before us and supplemented them with the missing technological solutions, we created an ideal platform, the functionality of which supports all the usual operations in the cryptosphere, but at a new level. The cardinal revision proposed by ZeCash is a combination of PoS algorithms (the use of which is aimed at the implementation of highly profitable mining) and ZeProtocol (guaranteeing the maximum level of security in the system), and ZeAnon (maintaining absolute anonymity of each user).

Having spent a lot of time on the technical implementation of the ZeCash concept, we managed to create a system that fully meets the challenges of today's crypto-economic situation.

ZeCash is a win-win option for investors and ordinary users, since everything that used to frighten and repel regular inclusiveness in the crypto environment has now become a set of convenient and understandable tools suitable for widespread use.