Table of Contents

Introduction

The world has gone digital, evolving from the world of hard copies to the realm of soft copies the internet has provided. A lot of things done physically are now being done with ease on the internet. For example online stores.

In the past, buying and selling involved solely being in a physical market, rowdy with buyers and sellers haggling loudly and shoving each other, but the case has changed. The internet now houses a lot of online stores, markets and shops, where almost everything can be bought and sold with ease.

Cryptocurrency, otherwise called online money or currency is one of the new 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 a lot of people have heard of the term Cryptocurrency, can it be boldly said that a lot of people know of its meaning? In a layman's term, Cryptocurrency is basically online money, a form of exchange, accepted by a lot of people and recognized worldwide. It is fashioned out to provide anonymity, security and be hack proof all in one.

A reader might ask themselves 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 a lot of online criminals prowl the internet seeking for victims to rip off, just like pick pockets that stroll the earth, seeking someone to steal from. That was where Cryptography was born from. 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 system.

Unlike ordinary currencies that are capable of being easily confiscated by law enforcements 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, a lot of 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.

Alternative to Bitcoin

Thousands of Bitcoin exist, but only a few will rule the world of cryptocurrency.

- The first here is the Litecoin (LTC):

  This currency was created in 2011, and while Bitcoin is the king of the Cryptocurrency realm, the Litecoin is the prince.

- The second is the Ethereum (ETH):

  Created in 2013, very popular having the possibilities to create Tokens.

- The third one is the Ripple (XRP):

  Created in 2012, it's more a real-time gross settlement but very popular these days.

The next alternative will be ZeCash Coin

Blockchain

What is Blockchain?

For the Cryptocurrency to function well there is a feature called, 'the 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 layman's terms, is more or less a ledger, but in this case, it is on the internet. It has imprinted transactions on itself 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 to be invaluable in crowd funding, and even voting online. Many experts see this Blockchain as having important uses in technologies, such as online voting.

We keep hearing tales from doomsday preachers of how Cryptocurrency and its associates will crash in the near future. These naysayers, like Chicken Little, scream that the sky is falling because they are not educated on the issue nor have the thought it wise to broaden their horizons.

If the so-called Cryptocurrency and its associates were a bunch of scams, why do big names in the world financial sector- names that make the world tremble when they speak- like JP Morgan view the currency as efficient and the future of transaction processing? JP Morgan Chase views the currency as having the latent potentials to reduce to a large extent costs accrued from transactions, and even termed it efficient.

Each block linked using the cryptographic hash pointer, forms the Blockchain, and it possesses the transaction data and timestamp for each transaction completed. Being resistant to changes in data, it functions as a ledger managed and monitored by a network which functioned 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 making alterations to all subsequent blocks. It makes use of decentralization unlike the traditional banking that focuses on centralization.

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 a 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 which makes 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 Blockchain. If the selection is done via an 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 alternative methods have been devised. Before we discuss the Proof of Stake scheme and protocol in ZeCash coin, let's discuss the forerunner, Proof of Work (POW).

The Proof of Work protocol is used by the first type of crypto currency, the Bitcoin. It makes use of puzzles, not mere jigsaw puzzles, but complicated puzzles that align with cryptography to authenticate the transactions processed and even mine to create new blocks. Cryptocurrencies known to use POW are Bitcoin and Litecoin.

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

Advantages of POS

The currencies using Proof of Stake can be thousand times more cost effective than 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 equivalent to combusting 752 gallons of gasoline, in terms of carbon production.

Also, 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 minters. While in Proof of Stake, the miners guiding the coins are always the ones who own the coin.

Staking with ZeCash

It's an incentive process to reward people who lock their ZeCash coin into their wallet to validate transactions. Our users are involved in buying the coin and will remain in a wallet for a certain fixed period. It is same as putting money in a fixed deposit for a fixed period of time. Here, the owner of a new block is chosen based on the person's stakes. The stakes here 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 make sure transactions are authenticated.

Here, to authenticate transactions, the Minter, is expected to place their currency units on 'stakes', meaning they open their ZeCash Wallet to maintain the network. In a fixed deposit, you will get interested as a reward. In Proof of Stake, the additional coins would be the reward. The below-given factors will define how the amount is rewarded.

Interest

The more time our ZeCash holder will Mint (keep their coin), the higher is the reward. It would be like 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%.

Staking Advantages

There is no need to spend a lot of money to buy a big mining farm. Initial investment needed for that it's just a simple computer connected to internet and a Wallet with ZeCash Coin. The balance in the wallet will grow; you just need to be patient

At the same time, the value of ZeCash coins will grow. There is guaranteed money making involved as ZeCash Coin values will increase due to the success simultaneously with the number of coins you hold in your wallet.

That’s how ZeCash Minting is possible. The amount of coin which you would be able to mint is exactly equal to the amount of coin which you have in your wallet. It is very similar to holding the bank account on the personal computer.

Staking Selection with CABS and RBS

Weighting the Miner could easily be done by basing the mining on the amount of coins the user has, but it will cancel out equality because only the rich will be selected. To tackle such a problem, 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 getting 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.

RBS (Randomized Block selection)

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

POS Security with ZeProtocol

No better way to list the most used security breaches on Proof of Stake network and how ZeCash fixes them, than with our proprietary ZeProtocol.

Nothing at Stake

Problem

In the event of a fork, whether the fork is accidental or a malicious attempt to rewrite history and reverse a transaction, 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 crypto currency), 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.

51% Attack

Problem

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

ZeProtocol Solution

ZeProtocol will implement the MOS (Maturity Operation System) a proprietary Algorithm where ZeCash coin has to be matured over a period of time, then it can be used at the stake again. Another option in study, coin can be locked for a period of time and therefore can not be sold on an exchange or likewise.

In order to do that you have to compare it with the working of Bitcoins where the machines for mining are uninterrupted by 51% of attacks. With ZeProtocol the attacker needs to be waiting for a long period of time before he can use the coins in a new attack.

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

Double Spend

Problem

Double spend attacks happen like this. The attacker first sells all his coins and then will publish a new version of the Blockchain in which the sale of the coins will not work. In the above scenario, the market will be able to absorb the very large amount of the coins from the total supply. This would create a market crash for example 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.

This confirmation N will be adjusted by the network depending on stakeholder variance and network difficulty. ZeProtocol will also make any block cemented. By that time 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.

Stake Grinding

Problem

The attacker has a small amount of stake and goes through the history of the Blockchain and finds places where their stake wins a block. In order to consecutively win, they modify the next block header until some stake they own wins once again. This attack requires a bit of computation, but definitely isn't impractical.

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. And in order 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 based on who is the most underrepresented in a given minting period. They would be chosen to be the next block minter. After a new block is created, the representation is updated and the next minter is chosen in the same fashion.

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 in the initial phase. When a node creates a block then it is known as minting. As the number of minting nodes increases the network would become more and more secure and safe. When the network is early in the initial phase the attack is relatively very cheap.

The bootstrapping phase of the network 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 which 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 to this, ZeCash will be also using synchronized checkpoints. Coins which are spent on the latest checkpoints can't be used so all coins get accumulated after that checkpoint.

ZeCash Anonymity with ZeAnon

Users are given a degree of anonymity that traditional banking systems don't 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 doesn't 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, there are other steps that can be taken to seal the deal:

- One way is to reduce revealing a lot of 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. A lot of technologies exist that could further encrypt your Cryptocurrency address. These include: CryptoNote, CoinJoin, Secure Wallet, TumbleBit, Tumblers, Tor and Co

ZeAnon of ZeCash will use the below feature to reinforce anonymity of transactions:

Stealth Transaction

ZeCash/ZeProtocol's 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 which has never been generated or has never been never seen before. Why?

In the view of increasing your privacy which 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 in itself but it will make it significantly harder to connect with this address in the real world. This identity would be used both in the sending and the receiving end of the transactions.

This also means that the receiver has to share the new address with the sender every time a transaction is made. This will be a lot of hassle and in some cases, this would be almost impossible and inconvenient in the long run. It is not considered an ideal solution with the perspective of privacy either. When the new address is shared on the insecure channel then the privacy is also potentially lost.

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, since in that way once the transaction is created there is no way of telling which input correspond to each output. Whereas if the inputs hold different values it will be much more straight-forward.

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.

Ring Signature

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

Therefore, when a message is signed with the ring signature then it can be endorsed easily by someone from the group of the people. One of the main security features is that it was totally infeasible to determine which of the group member has used this key to produce this secure signature.

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 theses protocols to provide an un-likable solution?

All coins are not really 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 also by anti–money laundering regulations.

This is not a great privacy feature. Users might not want to let the world about know their personal spending and also about how much they are earning and how much they own. This business information can be leaked to the competitors easily and we believe that each human deserves to choose or not choose, anonymous transactions like he’s able to choose anonymous messaging like Telegram.

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 7 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.

A lot of 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 than for others.

Fast block times don't 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. With Segwit transaction malleability will be gone transactions are instant, but immutable confirmations will still take time.

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 one-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 under lying technology of the Blockchain. By using real Bitcoin/Blockchain transactions and using 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.

Bidirectional Payment Channel

Two participants create a ledger entry on the Blockchain which require both participants to sign off on any spending of funds. Both parties create transactions which 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. This entry can be closed out at any time by either party without any trust or custodianship 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 (either the entire payment 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 how one makes many legal contracts with others, but one does not go to court every time a contract is made.

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

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

Conclusion

After looking at Cryptocurrency and its corresponding Blockchain technology, it can be said that discussing their importance cannot be overstated. They are here to stay, and their advantages over the traditional system cannot be overlooked. Your private key is your bank account which doesn't have any censorship or surveillance.

The question is, will you decide to be on the part of those who are clueless about this opportunity or will you take the shield of faith and take a stand with other big financial minds in the world? Be part of ZeCash revolution.