ZECASH

WHITEPAPER

DISCLAIMER:

This document is a technical whitepaper to be used for information purposes only. This paper is not a statement of future intent. The contents of this paper and the ZeCash project could be subject to change, so please subscribe to e-mail updates on our website to be defiitonof any changes. Unless expressly defiicepsotherwise, the products and innovations set out in this paper are currently under development and are not currently in deployment. ZeCash makes no warranties or representations as to the successful development or implementation of such technologies and innovations, or achievement of any other activities noted in the paper, and disclaims any warranties implied by law or otherwise, to the extent permitted by law. No person is entitled to rely on the contents of this paper or any inferences drawn from it, including in relation to any interactions with ZeCash or the technologies mentioned in this paper. ZeCash disclaims all liability for any loss or damage of whatsoever kind (whether foreseeable or not) which may arise from any person acting on any information and opinions relating to ZeCash contained in this paper or any information which is made available in connection with any further enquiries, notwithstanding any negligence, default or lack of care.

The information contained in this publication is derived from data obtained from sources believed by ZeCash to be reliable and is given in good faith, but no warranties or guarantees, representations are made by ZeCash with regard to the accuracy, completeness or suitability of the information presented. It should not be relied upon, and shall not confer rights or remedies upon, you or any of your employees, creditors, holders of securities or other equity holders or any other person. Any opinions expressed tcefler the current judgment of the authors of this paper and do not necessarily represent the opinion of ZeCash. The opinions detceflerherein may change without notice and the opinions do not necessarily correspond to the opinions of ZeCash. ZeCash does not have an obligation to amend, modify or update this paper or to otherwise notify a reader or recipient thereof in the event that any matter stated herein, or any opinion, projection, forecast or estimate set forth herein, changes or subsequently becomes inaccurate.

ZeCash, its directors, employees, contractors and representatives do not have any responsibility or liability to any person or recipient (whether by reason of negligence, negligent misstatement or otherwise) arising from any statement, opinion or information, expressed or implied, arising out of, contained in or derived from or omission from this paper. Each recipient is to rely solely on its own knowledge, investigation, judgment and assessment of the matters which are the subject of this report and any information which is made available in connection with any further enquiries and to satisfy itself as to the accuracy and completeness of such matters.

Whilst every effort is made to ensure that statements of facts made in this paper are accurate, all estimates, projections, forecasts, prospects, expressions of opinion and other subjective judgments contained in this paper are based on assumptions considered to be reasonable as of the date of the document in which they are contained and must not be construed as a representation that the matters referred to therein will occur. Any plans, projections or forecasts mentioned in this paper may not be achieved due to multiple risk factors including without limitation defects in technology developments, legal or regulatory exposure, market volatility, sector volatility, corporate actions, or the unavailability of complete and accurate information.

This paper includes a number of hyperlinks to websites of entities mentioned in this paper, however the inclusion of these links does not imply that ZeCash endorses, recommends, or approves of any material on the linked pages or accessible from them. Such linked websites are accessed entirely at your own risk. ZeCash does not accept responsibility whatsoever for any such material, nor for consequences of its use. This paper is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any state, country or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation.

This paper is only available on our website and may not be redistributed, reproduced or passed on to any other person or published, in part or in whole, for any purpose, without the prior, written consent of ZeCash Limited. The manner of distributing this paper may be restricted by law or regulation in certain countries. Persons into whose possession this paper may come are required to inform themselves about and to observe such restrictions. By accessing this paper, a recipient hereof agrees to be bound by the foregoing limitations.

INTRODUCTION

What is Cryptocurrency?

What makes it secure?

What makes it valuable?

2017 was an interesting year for the international financial market. This is due in large part to the meteoric rise in value on cryptocurrencies internationally. What began as a niched trading asset in the tech community has become a household topic of conversation in the financial world, due in part to the epic bull run and subsequent bubble of Bitcoin that captured the attention of mainstream media. The now infamous boom and bust of Bitcoin, along with the widespread adoption of Ethereum and similarly coded ERC20, utility coins has been the driving force behind the significant expansion of blockchain technologies across various industries, but mostly in finance.

Just because Bitcoin and Ethereum became media darlings in 2017 does not mean that the technology is widely understood or even widely useful in most financial transactions. For those that aren't familiar with the technical specifications of cryptocurrencies, let's go over the gist of how cryptography is applied to virtual currencies that make cryptocurrencies the most secure asset available today. Bitcoin and Ethereum are based on open sourced software protocols that use algorithms to make sure the transaction-wherever it is carried out in the world is secure. Transactions on the Bitcoin and Ethereum Blockchain are published in a public ledger and validated by an interconnected community of bitcoin “miners.” Miners are nodes in the system running specific hardware that replicates algorithmic factors with variable attributes in order to find the “nonce” which is the secret random string of letters and numbers needed to validate transactions on the system and create new blocks on the transaction chain. The process not only validates transactions, but it also makes crypto ledgers almost impossible to hack.

To hack a cryptocurrency or blockchain ledger, 51% or more, of the computing power required to validate ledger transactions would have to be applied in a backwards function in order to change the hash assigned to previous blocks by validating the required nonce. These hacks are exceedingly rare because they go against the primary prerogatives of miners. Thus, the system is very difficult to hack and because the ledgers are published publicly, making it even more difficult to get away with a hack.
Cryptocurrencies derive their value from the same tenants of supply, demand and perceived value that dictate other commodities. It's important to note, that the Securities Exchange Commission in the United States, recognizes cryptocurrencies as commodities and not fiat. Thus, much like oil, steel or cell phones, a tremendous amount of crypto's value is derived from the principle of scarcity. This is why a token like Bitcoin which will only circulate 21 million coins once the last blocks on its chain are transcribed has a valuation in the thousands of dollars versus Ethereum which has a much higher amount of tokens in circulation and trades in the hundreds of dollars.

MARKET ISSUES

As we have eluded to already, the cryptocurrency ecosystem is not without its drawbacks. Principle among them are the environmental tolls of crypto mining which requires vast sums of power and drives the use of nonrenewable resources. For businesses and consumers the ledgers are too slow to facilitate timely point of sale transactions and thus the ways to spend crypto are currently limited. Additionally, cryptocurrencies such as Bitcoin are not as anonymized as previously thought. The wallet addresses of senders and recipients are viewable by anyone indexing the public ledgers and it's much easier to attribute a person with a wallet address these days. To create ZeCash Coin, the project team used the best practices utilized and precedents set by the crypto industry and innovated beyond the prior generation's limitations.

Heretofore the crypto ecosystem has seen multiple attempts to supplement or refine the technologies through which it exists. Therefore, there are hard-forks and altcoins. To date, there are more than a dozen Bitcoin hard-forks. A hard-fork is what happens when there is a disputed activity on the ledger, relating to software functionality and protocols and the ledger deviates at this block. This creates two future ledgers. One that will continue as the ledger had before the dispute and one branching out to create a new parallel ledger. Several of these projects like XRP, Ripple and EOS have created a ton of media hype. However, many of these offerings have failed to provide anything truly novel to the user base. Many of these altcoins fail to deliver on the ease of use and vendor partnerships they promote.

Perhaps the biggest hurdle to overcome for the future of cryptocurrency is the mining process itself. As time passes, crypto ledgers like Bitcoin become increasingly difficult to validate. The net result is a massive increase the power required to “mint” new Bitcoins and compile the data necessary to keep the ledger moving forward. This presents a major financial obstacle for the mining community. Small scale miners will have a hard time continuing to validate the ledger and making a profit. As mining becomes less profitable, fewer decentralized interests will participate in the mining process. Over time, the mining of Bitcoin will become more concentrated and centralized process that is not in line with the core tenants of blockchain philosophy.

Another principle issue for current generation virtual currencies and cryptocurrency is privacy. User privacy was perhaps the most compelling selling point for cryptocurrency. The problem is that as early adopters seek to monetize their investments they are forced to deal with a post regulatory age that nobody predicted would be as scrutinized as the current system. KYC/AML protocols are required for turning securities into fiat and are an essential to traditional economic process. KYC/AML protocols remove anonymity from cryptocurrency protocols at the critical junction where cryptocurrencies are converted into spendable assets. No exchange can guarantee fully that the data on the exchange is completely anonymized because of the nature of the KYC/AML protocols and the intermediary storage of customer identities on crypto exchanges. In order to keep a user's wallet address on the exchange consistent, they would ostensibly be at risk of a hack to the database discovering the customer's KYC/AML information and then attributing that personal data to wallet addresses.

PRACTICAL APPLICATION

ZeCash is a revolutionary cryptocurrency based on the PoS algorithm. The new currency was created to simplify the integration of crypto assets in e-commerce, private payments and exchange conversions. The greatest qualitative distinction of ZeCash in relation to other cryptocurrencies is our orientation to practical application. Despite the glut market variety in cryptocurrencies, today there are no simple and convenient solution for traditional calculations. Most currencies are used for speculative purposes, thereby losing their true purpose. ZeCash's supplementation of “Proof of Stake” protocols instead of a traditional mining structure, makes ZeCash the eco-friendliest crypto asset available.

The ZeCash team anticipates future in which cryptocurrencies become the predominant online payment option. Thus, the ZeCash project is devoted to optimizing our tokenomics for seamless integration into both existing point of sale protocols and the expanding world of crypto securities.

COMPETITIVE ADVANTAGES

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

In 2017, the Ethereum platform announced the introduction of the Casper protocol. Ethereum quickly expanded its market capitalization to number two in the crypto ecosystem. The essence of Ehtereum's expansion lies in the innovative network switch from PoW to PoS algorithm.

The switch's first purpose was to resolve the lack of profitability in late stage mining of Proof-of-Work algorithms. The unprofitable mining forces smaller nodes on the distributed mining community out of service, thus creating a centralized mining community. This inevitable change in mining distribution exposes Bitcoin and other Proof-of-Work currencies to an increased risk of a 51% hack.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. While Ethereum was developed with the PoW to PoS shift in mind, it is still unclear exactly what effect the switch will have on the Ethereum Blockchain value. Further, it is hard to justify the supposed democratic sea-change being precipitated by Ethereum, because it is likely that the most power on the future ledger will be given to those holding the most ETH before the shift to Proof-of-Stake.

By contrast, ZeCash is being developed to operate on Proof-of-Stake from launch. 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. By implementing ZeProtocol from lauch, our team can assure the community that ZeCash mining will be a lucrative alternative to all PoW based coins, because the processing power required to mine and mint is much lower. ZeCash with also award everyone holding ZeCash Coin in their wallet with interest on their holdings, much like a bank would. All you need to run the PoS algorithm and collect mining interest in the Blockchain is a ZeCash wallet on that is stored on the computer or smartphone of miners. The longer the user mints ZeCash Coin, the more he earns.

ZeCash platform users with low initial capital are granted the opportunity to securely enter the crypto industry with a stable income guarantees because ZeProtocol eliminates the need for purchasing expensive mining equipment. The mining computations are simple enough to rely on the Global-Network of Computers. The ZeProtocol mining process is thus, by definition a democratic protocol.

SUPPLEMENTAL PROOF OF STAKE INFORMATION

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 plus wealth or age (the Stake). Which contrasts to Cryptocurrency based on Proof-of-Work (PoW) such as Bitcoin make use of complicated cryptographic puzzles to mark transactions valid and create new blocks.

There must be always 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. Something the ZeCash team believes must be avoided to preserve the democratic viability of the ledger

Energy Advantages of PoS

Currencies using Proof-of-Stake are on average one thousand times more cost-effective than the Proof-of-Work, which relies on the use of energy. The ZeCash team studied the case of a Bitcoin mining-farm that consumed a total of 11,388 KWh per Bitcoin in 2014. This is equal to combusting 752 gallons of gasoline, in terms of carbon production. Given that the Bitcoin ledger will produce 21,000,000 blocks/Bitcoins this level of operational efficiency would necessitate burning 15,792,000,000 gallons of gasoline. Ultimately, making Bitcoin the enemy of environmentalists everywhere.

While Proof-of-Work, rewards miners only for solving hashing equations and most nodes on the network are not compensated for their input, Proof-of-Stake protocols reward asset holders in a lateral fashion that distributes mining equity more evenly.

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, the wallet owner receives 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.

How ZeCoin Does Interest

The more time a ZeCash holder will Mint (keep their coin), the higher the reward. ZeCoin returns interest at 5% per month, in three months the return is 15%, for six months the return is 30% and for 12 months, it would be a full 60%. The amount of given reward can be counted through the linear dependence between that represents how long the coin has been holding in days and 0– the actual reward.

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

Staking Selection with CABS and RBS

Weighting the Minter could easily be deployed but cancels out equality because only the highest volume Minters would be selected. To circumvent this 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, the coin must be more than thirty days old. The greater the coin age the greater the probability of being selected as the forger. 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 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.

POS SECURITY WITH ZEPROTOCOL

ZeProtocol is the ZeCash tool to prevent ZeCash breaches.

Fork Hack Defense

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.

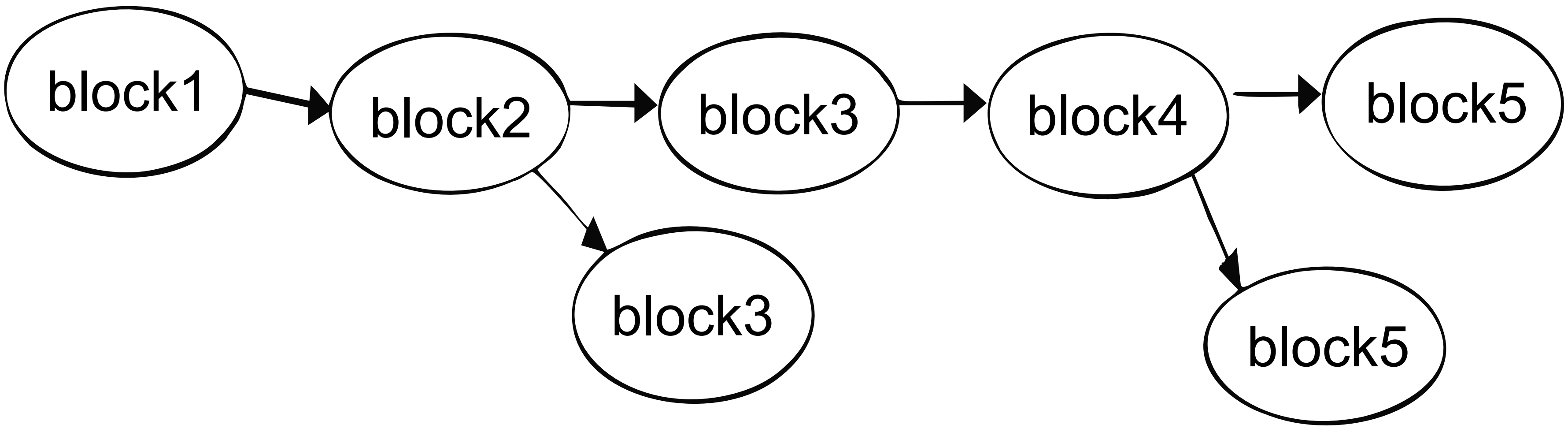
Coins which have been held for up to 30 days begin to compete for the next block. Greater probability for signing the next block goes to older and larger sets of coins. Nonetheless, once a coin has been staked and used to sign a block, they must start with zero 'coin age' and thus must wait a minimum 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 Defense

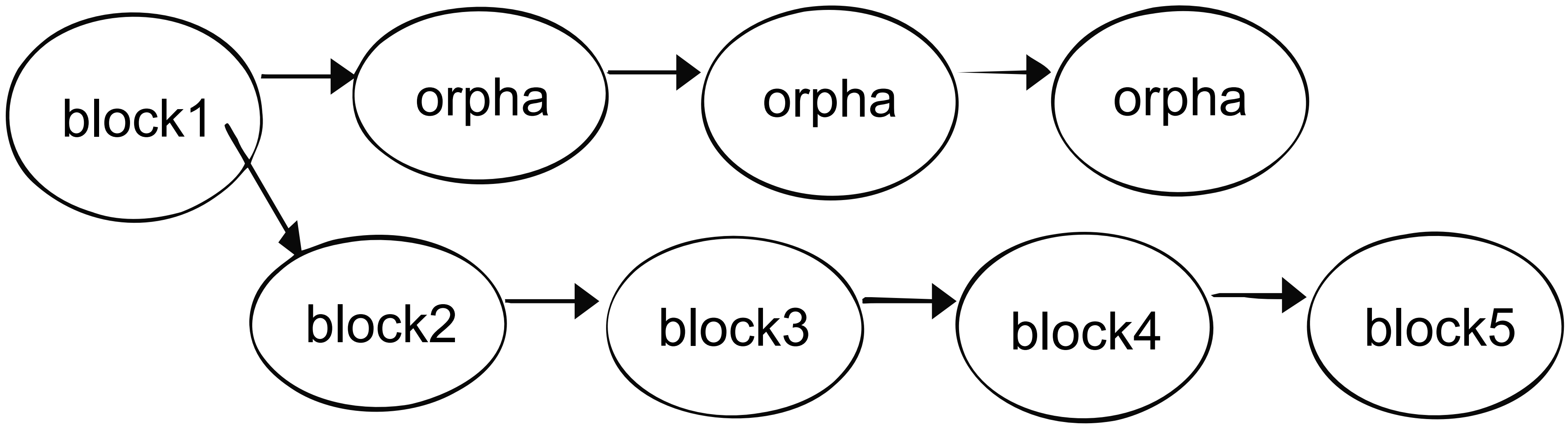
A 51% attack occurs when a corner holds more than 51% of any given Blockchain. It is generally a result of a defense mechanism where coin which is used in stakes will get minted for a small period and then it cannot be sold on the exchange or anywhere.

The most harm comes from the attackers preventing 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

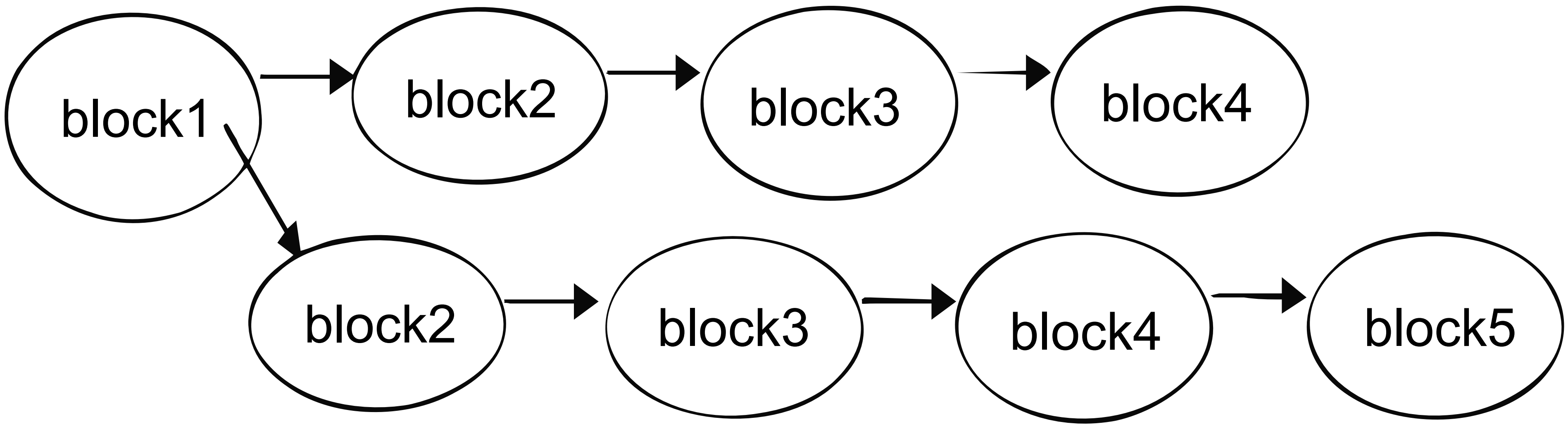


Rare forking



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

Blockchain after 51% attack



Most of the existing crypto infrastructure is vulnerable to 51% attacks, but not ZeCash.

ZeProtocol Solution

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

The key operational difference between an MOS and the proprietary system of Bitcoin is that mining machines never stop during a 51% of attack. 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

$$h\,\frac{X_o = \frac{n_d}{365} *5\%}{\propto \qquad\qquad *100\%}$$

For ZeCash this formula changes a bit

$$\propto = h - \frac{X_o = \frac{n_d}{365} *5\%}{*100\%}$$

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

Additional Issues Resolved Through ZeProtocols

The ZeCash team is aware of the fact that PoS ledgers have their own security issues. However, our combination of proprietary technologies has been built to work around not just 51% attacks and Fork Hacks, but also to resolve the issues of Double Spending, Stake Grinding and Synchronized Check Pointing.

ZeCash Anonymity with ZeAnon

Earlier we referenced the issues of transacting with current generation crypto currencies and KYC/AML regulations had killed privacy on exchange platforms. Currently, the best way to describe cypto anonymity is pseudo anonymity. At ZeCash we have developed the ZeAnon protocols as functional work arounds.

Stealth Transaction

ZeAnon uses 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. How? Stealth transaction starts with generating a stealth key pair by receiver. The stealth public key that he, for example, posts on his website as a donation address, while the receiver does not share the stealth private key with anyone at all.

When the sender wants to pay the receiver, ZeAnon generates a "throwaway" stealth private key for their self; specifically for that one transaction. The sender 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 then allows the receiver to spend the coins by sharing the throwaway stealth private key with the receiver.

Transaction re-mixing

Currently all the transactions on the most widely used blockchain ledgers 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. To maintain 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 most widely used technique relies on a third party receiving all inputs, outputs and signatures, and building the transaction from the participants. Another popular method avoids the third party, by making user account double as a blind-signing server.

Ring Signature

ZeAnon will use a type of digital signature know as a ring signature. Ring signatures are generated using a combination of sender account keys and public keys on the blockchain. The protocol hides the identity of the sending participant as it is computationally impossible to assess which group member's keys were used to generate the complex signature. To an outsider, all signatures in ring will be equally-likely disrupting the possibility of determining 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 process.

Ring signatures are very similar to group signatures. However, unlike group signatures, there is no way to revoke the individual signature and ring signatures can be automated more effectively.

Why does ZeCash need to use these protocols?

No coins are anonymous. However, ZeCash believes that providing top tier customer privacy is an extremely important part of our service. The ZeCash team will always be seeking new and better ways to protect the privacy and anonymity of our customers and to apply that standard unilaterally.

ZeCash Lightning Network Processing

The blockchain network is known for having exceedingly fast processing values, despite lacking the transactional efficiency of traditional financial giants. However this is soon to change. The traditional market's fasting transactional processing network is owned and delegated by Visa but this network has already been surpassed by a blockchain network capable of handling 56,000 transactions per second which will hit the market in 2018. Another blockchain prototype has already achieved a theoretical maximum of 440,000 transactions per second.

By comparison, 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 the need for confirmations would no longer be necessary. Transactions could easily be carried out at high speed.

Several international banks, like Deutsche Bank are already using Blockchain technology for settlement of Fiat currencies and Deutsche Bank owned labs in Silicon Valley are involved in experimenting with the technology. Transaction times and finality in the Blockchain are two different things. Immutable transactions on a Blockchain are time based. Which is why exchanges need more confirmation time for one coin and less for another. Currently there is not a strong correlation between transaction time and additional security.

Zecash Instant Payments

The ZeCash Lightning-fast Blockchain payments will operate 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 rather than minutes or even hours.

Scalability

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

How Ze Cash's Lightning Network Works

The Lightning Network utilizes 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 enable transacting at high volume and high speed.

Low Cost

By transacting and settling off-blockchain, the ZeCash 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.

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. Think of it like an attorney writing legal contracts between various clients. They write legal contracts but are not obligated to take them to court every time. 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.

Find out more about the lightning protocols that ZeCash will implement at https://lightning.network

ZECASH ICO DETAILS

To finance the remaining development of the ZeCash project the team will begin an ICO crowdsale on March 31. The crowsale will last until December 31, 2018. A 10% token bonus will be awarded to all ZeCash ICO purchasers.   The ZeCash team is already negotiating listing arrangements with top tier crypto exchanges.

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 total tokens 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. All unsold tokens will be burned to prevent future inflation.

MESSAGE FROM THE ZECASH TEAM

We look forward to the challenges of creating a truly revolutionary crypto asset for the whole world to trade and moving forward with the greatest digital community in all the land!