RESEARCH REPORT

Zcoin

INTELLIGENT
TRADING

Zcoin (XZC)

Type: Privacy coin
Date: 23-Jul-2018
Updated: 24-Jan-2019

Price: $5.16
Market Cap: $34,243,299 USD
Liquidity: Medium
Primary Exchange: Binance
Team strength: Medium
Project stage: Functioning product
Funding stage: Traded
HQ: Singapore foundation and Thai BOI company*
First USD Price: $0.37

Source: Tradingview

Summary

Zcoin was launched in September 2016 as the first altcoin implementing the Zerocoin protocol. The protocol introduced Zero-knowledge proof as an improvement to the bitcoin blockchain, aiming to enhance the privacy features. The Zcoin team is focusing on the development, searching for new privacy methods and aiming to foster the decentralized nature of blockchain with ASIC-resistant mining algorithm (MTP). With the objective of enhanced confidentiality and anonymity of transactions, Zcoin belongs to the sector of privacy coins. The general characteristics of the blockchain are similar to its predecessor bitcoin, but Zcoin adds incentivised ZNodes to maintain the network.

Strengths & Opportunities

- Technology-oriented project with strong development and sound privacy solution
- Open and honest communication building a good image of Zcoin and creating an engaged community
- If the team increases their marketing efforts, there will be potential for higher adoption
- Growing popularity of privacy coins and privacy solutions
- Strong position in Asia
- Promising new technology of next-gen protocol outlining increased scalability and potential for default privacy

Weaknesses & Threats

- Drawbacks of Zero-knowledge proof technology such as large transaction size and the initial trusted setup
- Lack of sound marketing strategy, no unified info about the project, currently no whitepaper
- Limited exposure to the US market
- Strong competition from more established privacy coins
- Regulations disabling the infrastructure and slowing down the adoption
- Tech4Tokens solutions offering better privacy that can be added on top of existing blockchains

* As per the Zcoin COO answer to the open letter on reddit, currently in process of setting up. Legal fees has been paid to SilkLegal.

Analysis of Zcoin (XZC)

Project Analysis

Description

Overview

Zcoin was launched in September 2016 as the first cryptocurrency implementing the Zerocoin protocol. The Zerocoin protocol originated as bitcoin cryptographic extension focusing on enhancing the privacy of the original currency. The transparent and permanent nature of the bitcoin blockchain makes the question of on-chain confidentiality extremely important. The crypto community is starting to realize this, and different privacy protection methods are emerging. The technique utilized for breaking the links between the transactions in Zerocoin protocol is the Zero-knowledge proof.

Zcoin is focusing on privacy in financial transactions and is continuously working on research into different privacy methods. On top of that, the team is concerned with the fundamental characteristics of the cryptocurrencies being corrupted, mainly the jeopardization of the decentralized character of cryptocurrencies caused by ASIC dominance. Zcoin aims to solve this with their Merkel Tree Proof (MTP).

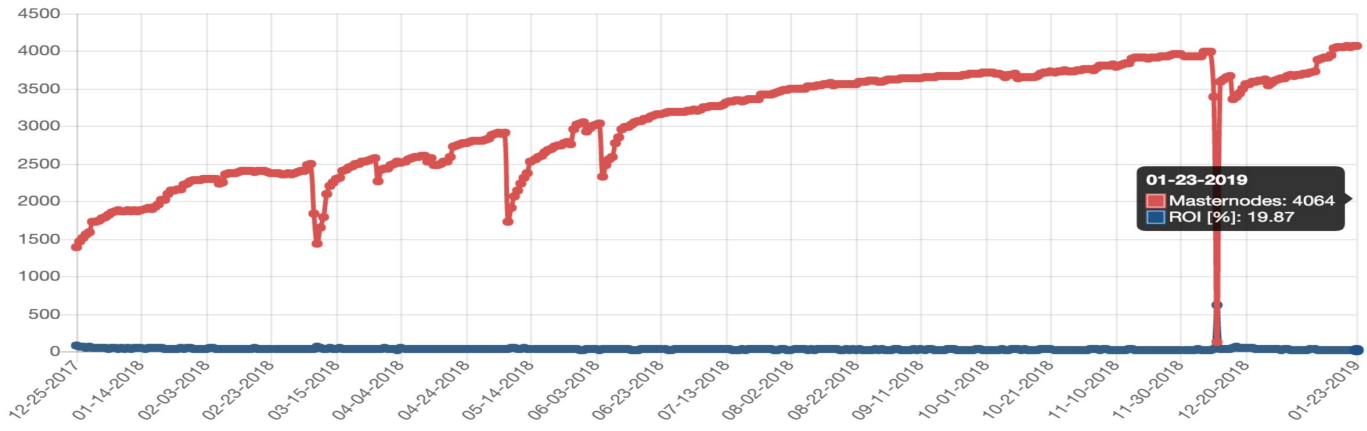
Business Model

The project's business model is based on the same principle as bitcoin. Miners are incentivised by transaction fees and miners' rewards, based on the Proof of Work (PoW) consensus. Additionally to this, in December 2017 Zcoin networks introduced ZNodes. In general, nodes are computers or other hardware devices storing a copy of the blockchain, maintaining its integrity. ZNodes are a special type of nodes, incentivised by 30% of the block reward. To run the ZNode, there is a collateral of one thousand (1,000) XZC. This ensures that the nodes are interested in the well being of the whole network.

There are two options to run ZNode, The user can decide to host the node on his own or choose a ZNode provider. After the one thousand (1,000) XZC are deposited, the user sends the node provider the transaction ID or the address to where the XZC was posted. Currently, Zcoin lists twelve providers on their website, stating that the team is officially not running any of them and they are all run by a third parties.

There are also rewards for pooled Znodes offered by Satang Pro (TDAX) and Cobo wallet (The founder of TDAX is also the founder of Zcoin). The exchange and the wallet provider are running nodes on behalf of their customers and distributing rewards based on the amount of XZC on their account/in their wallet.

Currently there are over four thousand (at the time of writing 4,064) master nodes, with the highest density in the USA. Annual return on investment (ROI) of running the master node is approximately 20.33%. The graph below shows the trend of **ROI** (blue) and **Masternodes (red)** of XZC from December 2017 to January 2019. (Note: due to the switch to MTP on 12 December 2018, data on masternodes.online is missing, hence the irregularity in ROI.)



Source: masternodes.online

Project Analysis

Fiscal and Monetary Policies

Zcoin never did an ICO. The project is fully financed by seed investments. There are three seed investors, Roger Ver, Tim Lee and one anonymous investor*. Originally, 20% of each block, or 10 XZC, was dedicated to the founders' rewards and the bounty wallet. The distribution from each block was as follows:

- Founder and lead developer Poramin Insom: 2 XZC
- Seed Investors: 2 XZC each, together 6 XZC
- Team and Bounty Wallet: 2 XZC

In total 10 XZC

This plan was scheduled for four years, but after introducing the ZNodes, the founder and investors agreed to halve their rewards to compensate for the ZNodes share of block rewards and increase the bounty fund. The current distribution of rewards from each block is:

- Founder and lead developer Poramin Insom: 1 XZC
- Seed Investors: 2 XZC each, together 3 XZC
- Team and Bounty Wallet: 3 XZC

In total 7 XZC

On forums such as Reddit and AMA, Zcoin's Chief Operating Officer (COO) has mentioned some details of the reasons behind the hard fork. Disagreements about the founder rewards were one of them,

Team

The founder of Zcoin, Poramin Insom, is also the lead developer (Mr. Insom is an advisor to ITF). He was the one who came up with his own implementation of the Zerocoin protocol with RSA parameters. In an interview from 2017 Mr. Insom stated that he is considering changing the protocol, but he would need a more experienced crypto developer in the team.

A strong figure in the Zcoin team is the COO, Reuben Yap. He manages the community, introducing Zcoin and communicating with the public. Over time, he has become a bit of 'the face of Zcoin,' giving interviews and spreading awareness about their project and blockchain privacy in general.

* According to some sources (Messari, Bitcoin.com), the third investor is a startup accelerator run by Chilean government

Project Analysis

Technology

The team is focusing chiefly on development, hence the technology section of the report is the most comprehensive. There are several features and projects on which the developers are working. We distinguished them into two categories. The first category is concerned with the general blockchain characteristics, such as the mining algorithm, the second one is dealing solely with privacy solutions.

General

Zcoin is a fork of bitcoin and as such, the project has the bitcoin protocol base. This allows Zcoin to adopt the bitcoin protocol improvements. In September 2017 the update from core 0.8 to 0.13 was implemented, improving node connectivity and enabling blockchain pruning.* After that, several releases followed, the latest of which occurred in December 2018, fixing duplicate Zerocoin spends when doing multiple input. Other improvements included GUI revamps, ZNodes release and bug corrections.

In terms of consensus, the PoW protocol is currently transiting to Merkle Tree Proof (MTP).

MTP

In May 2018, the team announced the launch of a working version of a new mining algorithm on testnet. The algorithm called Merkle Tree Proof (MTP) is designed to solve the issue of mining centralization. Satoshi Nakamoto designed the bitcoin network to be decentralized with a mining algorithm based on one-CPU-one-vote principles. However, as the cryptocurrency became more popular and the mining more profitable, new technologies were developed to benefit from more advanced computing power.

The topic of ASIC mining centralization and protections against it is resonating in crypto forums and tech communities**. ASICs, which stands for Application-Specific Integrated Circuit, are equipment specialized for solving the PoW and mining cryptocurrencies extremely efficiently.

Producing hardware specialized on PoW mining of specific blockchains fosters centralization in two ways. First, the hardware producers' number is limited to ASIC manufacturers (e.g. ASICminer, China). The centralization of manufacturing can be risky. Due to the specialization on crypto mining, it is easier to ban ASIC than CPU (e.g. the ban in Venezuela, May 2018). Second, pools with more capital can invest in the ASIC chips, creating large mining farms with unbeatable power and influence over the mined blockchain.

MTP mining algorithm aims to solve this problem by increasing the memory requirements. The algorithm increases the cost of ASIC development as the ASIC chips are optimizing the computation function, not the memory use. To provide memory-hard algorithm without limiting the scalability of the network, MTP is based on principles of egalitarian computing (introduced in a paper from 2016).

The MTP is not implemented in any project yet, Zcoin may be the first to use it. The team started the research in 2017, officially released the first version on testnet in May 2018 and on mainnet on October 24. The the team was utilizing the bounty system to engage the public in development, offering ten thousand dollars ($10,000) bounty for MTP Audit and twenty-five thousand dollars ($25,000) for MTP Implementation bounty.

Implementation of MTP enabled ZCoin to halve their block time from 10 to 5 minutes.

* Pruning is a method of deleting the data about fully spent transaction from the blockchain. Since these data are unnecessary, deleting them reduces the amount of data needed for transaction verification. The validating node works only with current unspent output and data to handle re-orgs (BitcoinWiki)

** CryptoNews, BTCManager, Quantamize, HackerMoon, TechCrunch, CoinCentral, Coin Insider, Blockonomi, Coindesk, Ethereum world news

Project Analysis

Privacy

The second category is what makes Zcoin distinguishable from other altcoins. The focus on on-chain privacy, unlinkability of addresses and transactions and confidentiality of users' personal data classify Zcoin as a privacy coin.

Zero-knowledge proof

As already mentioned, the privacy features of Zcoin are based on the Zerocoin protocol. The method proposed in the Zerocoin whitepaper utilizes the Zero-knowledge proof. This cryptographic technique completely breaks the links between transactions into two steps. In the first one, the coins are burnt in a so-called Zerocoin mint. The fact that the coins were indeed made unspendable is verified through the Zero-knowledge proof*, without revealing the specific coins. The proof entitles the original coin holder the right to an equivalent of what was burnt. In the second step, the holder redeems new coins, the Zerocoin spend.

There is no way to find out the origin of the new coins. Like this, the sender's blockchain address is obfuscated and there is no way to link the shielded transactions with the address.

As the mixing is embedded in the protocol, there is no need for a third party mixer. Using the mint coins for mixing the transaction path allows for scaling of the anonymity set up to thousands. The drawback of this method is that it requires a one-time trusted setup generating the initial parameters. The big size of the proof also requires additional storage on the blockchain and additional computational resources for verification.

RSA

The weak point of the Zero-knowledge proof is the one-time trusted setup when the initial parameters are generated. You need to trust that those parameters were destroyed and cannot be used to generate new coins. To mitigate the risk resulting from the trusted setup, Zcoin is currently using the parameters from the RSA factoring challenge. The challenge to factor prime numbers (which were destroyed in several steps) was announced in 1991 and ended after sixteen years in 2007 without being completed by anyone.

Updates

The team acknowledges that even with RSA, the trusted setup jeopardizes the integrity of a zero-knowledge protocol solution. That is why they were developing Sigma protocol, with the objective to remove the trusted setup.

As per the May 2018 update, the crypto library for Sigma protocol is already created. However, a new solution has also appeared in the meantime. A new implementation of the non-interactive Zero-knowledge proof protocol called bulletproofs came out, promising enhanced scalability and privacy without the trusted setup. As bulletproofs appear to be a better option than the Sigma protocol, the team is currently looking into implementing it. Especially the scalability enhancement is relevant due to the fact that currently, the large proof size hinders setting privacy by default for all transactions.

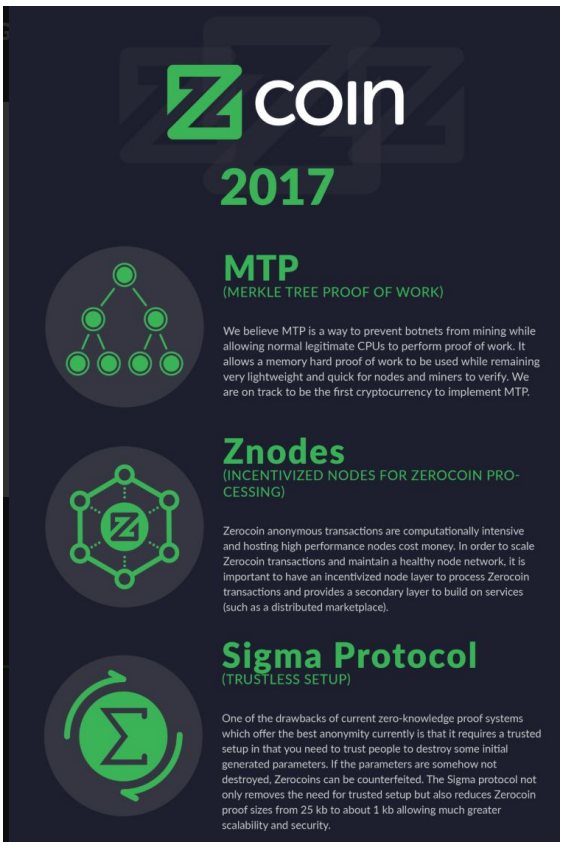
The next update on privacy was the new release 0.13.5.7 "French Drop", integrating TOR into Zcoin core wallets for better IP address protection and anonymous internet sourcing. The protection of IP addresses is also topic of a September update implementing the Dandelion. This method of routing provides protection to users that do not utilize Tor and enhance privacy for those who do.

* For more details about Zero-knowledge proof please see our Privacy coins report, pages six and seven

Project Analysis

Roadmap fulfilling and future updates

On top of the already mentioned Dandelion routing and the MTP, the Zcoin implemented in 2018, the current roadmap outlines further technology updates. In order to assess the ability of the team to fulfill those objectives, we first evaluated how successful they were in meeting milestones set in their previous roadmap year.



Source: https://Zcoin.io/roadmap/Zcoin_roadmap_2017-01/

The 2017 roadmap had three highlights. The Merkle Tree Proof of Work (MTP), incentivized Znodes for Zerocoin processing and Sigma protocol for the trustless setup. In previous pages, we have described all three updates and mentioned also the phase of their implementation.

Out of the three, both the Znodes update and MTP is now fully up and running on the mainnet. However, the MTP was not ready till the end of 2018, due to complications with the research and development.

As for the Sigma protocol, the evaluation of the success of this update is complicated. Even though the cryptographic library was completed, it was not earlier than in March 2018. What is more, the team decided not to implement it in the end, preferring to look into other solutions.

As per Reuben's update, the team was looking into the bulletproof protocol. At this team, they are back to Sigma, postponing it in their roadmap as a future update for 2019, under "coming soons" section.

Overall, even though the final implementation of the 2017 roadmap milestones took some time for the MTP and was questionable for Sigma, as the team is by all accounts working on the development and meeting the milestones. The huge plus is the open communication of reasons for any delays or changes in the roadmap.

That said, we can move to the updated roadmap for 2018 and beyond. The most notable updates are promised for the flexibility of the GUI design, reducing proof size with new Zerocoin update, and implementation of the Sigma protocol, completely removing the need for a trusted setup.

The most interesting in terms of privacy and long-term development is the commitment to introduce a next-generation privacy protocol. The name is not decided yet and the features and solutions implemented have also not been disclosed in detail.

According to the roadmap, coding of the next-gen protocol framework has already begun in mid-June. Teasers such as support of smart contracts with privacy applications in 2019 or research of quantum resistant Zero-knowledge proofs in 2020 are promising. The question is, how successful will the team be with the implementation of this roadmap.

Market

Market Players

The market of privacy coins has been dominated by three major players. Monero (XMR), ZCash (ZEC) and Dash (DASH) are featured at the top of nearly every list of privacy coins.* (Some of the contributors to this Research Report currently hold ZEC. Additionally, the Intelligent Trading Foundation has confirmed that it currently holds ZEC.) We have covered the main characteristic of each player in our previous report, analyzing the whole privacy coins sector (full report can be found here), thus in this report, we will just briefly summarize the main characteristics of the top three.

Top Three

Source: Tradingview

The coin with arguably the best privacy solution is currently **Monero (XMR)**, offering privacy by default. The solution utilized in the Monero project is automated decentralized mixing in an improved version of ring signatures, RingCT. In combination with the Stealth address, this provides full privacy shielding the sender, recipient and amount. The limits of the solution are a low anonymity set, which is set by default to be 7, and the initially larger transaction sizes. The team did find a way to reduce transaction size, however, implementing Monero compatible bulletproofs on 18 October, 2018, which saw transaction fees drop 95% in a single week. In terms of scalability in comparison to the other two, Monero has the fastest block time (2 minutes), but the fact that the blockchain is not completely prunable limits the chain size reductions.

ZCash (ZEC) is utilizing the Zero-knowledge proof as well, similar to Zcoin it is building on the Zerocoin protocol. For this reason, we will look at the characteristics in more detail in a separate section.

The last project from the top three is **Dash (DASH).** Its position in the list of privacy coins is slightly questionable. Privacy is optional and the traffic for DASH is driven mostly by transactions without the privacy features. The privacy technology utilized for PrivatSend (private transactions) is mixing through CoinJoin. The mixing process is expedited by a "masternode", a server which the users have to trust is not recording the users' information. The masternode protocol is similar to Znodes used in Zcoin. The CoinJoin solution is relatively simple and easy to implement on top of the blockchain, but the provided privacy is limited by the anonymity set (three addresses in each mix, option to choose up to eight mix rounds).

* Hackernoon, Blockchain blog, Steemit,CDO Trends, Invest in Blockchain, CoinCodex, BitcoinExchangeGuide, Investopedia, CryptoTicker...

Market

Comparison

The chart below compares Zcoin with two of the three coins mentioned above, representing different privacy methods. Monero combines several techniques including Ring Signatures and Stealth address for obfuscating the sender, recipient and amount. It is the only coin providing privacy by default, which makes it arguably the best in performance in terms of privacy. However, the blockchain is not completely prunable and does not allow for supply auditability.

Dash and Zcoin are both offering optional privacy, however, both of these offer blockchain prunability. Their blockchain is also auditable. This allows them to verify that new coins are not being generated and determine the exact number of coins. Even though Zcoin offers the highest anonymity set, the drawback is the initial trusted setup it requires.

	Zcoin	Monero	Dash
Total supply	21.4 million	18.3 million + tail emission	18.9 million
Block time	5 minutes	2 minutes	2.5 minutes
Prunable blockchain	Yes	No	Yes
Master nodes	Yes	No	Yes
Supply auditibility	Yes	No	Yes
Privacy technology	Custom Zerocoin protocol	Ring Signatures, Stealth Address, Pedersen Commitments	CoinJoin variant
Anonymity set per tx	Thousands (depends on denominations)**	7 set by default	1-16, chosen by the user, with each mix
Requires trust of mixers	No	No	Yes
Trusted setup	Yes	No	No
Privacy by default	No	Yes	No
Hides Sender	Yes	Yes	Yes
Hides Recipient	No	Yes	Yes
Hides Amount	No	Yes	No

** Zerocoin denominations are 1, 5, 10, 50, 100, 500, 1000, and 5000. Zcoin use denominations up to 100

Market

Zerocoin based segment

The market of privacy coins is active and booming. To provide the most relevant comparison, after briefly covering the top three, we focus on privacy coins based on the Zerocoin protocol. In the table below, we put Zcoin next to ZCash, PivX, and Horizen (formerly ZenCash). All four coins utilize the Zero-knowledge proofs and are building on the Zerocoin protocol. ZCash comes with Zerocash protocol, aiming to solve some downsides of the Zerocoin protocol with zk-SNARKs.

There are other privacy coins based on the Zerocoin/Zerocash (e.g. Bitcoin Private (BTCP)), however, due to its novelty and relatively limited information it is not included in the comparison. There are also new methods using Zero-knowledge proofs, which are not implemented in any altcoin yet, e.g. bulletproofs or zk-STARKs. Those methods can be added on top of existing blockchains, so they have been excluded from this comparison as well.

	Zcoin	ZCash	PivX	Horizen
Total supply	21.4 million	21 million	Dynamic	21 million
Block time	10 minutes*	2.5 minutes	60 seconds	2.5 minutes
Algorithm	PoW Lyra2z transition to MTP	PoW Equihash	PoS	PoW Equihash
Master nodes	Yes	No	Yes	Yes
Supply auditibility	Yes	No	Yes	No
Privacy technology	Custom Zerocoin protocol	Zerocash protocol with zk-SNARKs, Stealth address	Custom Zerocoin Protocol based on libzerocoin	Zerocash protocol with zk-SNARKs, Stealth address
Anonymity set per tx	Thousands (depends on denominations)**	All mint transactions	Thousands (depends on denominations)**	All mint transactions
Privacy by default	No	No	Partially ***	No
Hides Sender	Yes	Yes	Yes	Yes
Hides Recipient	No	Yes	No	Yes
Hides Amount	No	Yes	No	Yes

* To be halved after MTP is released on the mainnet
** Zerocoin denominations are 1, 5, 10, 50, 100, 500, 1000, and 5000. Zcoin use denominations up to 100, PivX the whole set from Zerocoin
*** Automint converts 10% of all balances to the private token by default. When doing the transaction, the user choose to send from public piv or shielded zPIV balance

Market

Comparison

Horizen (ZEN, previously ZenCash)

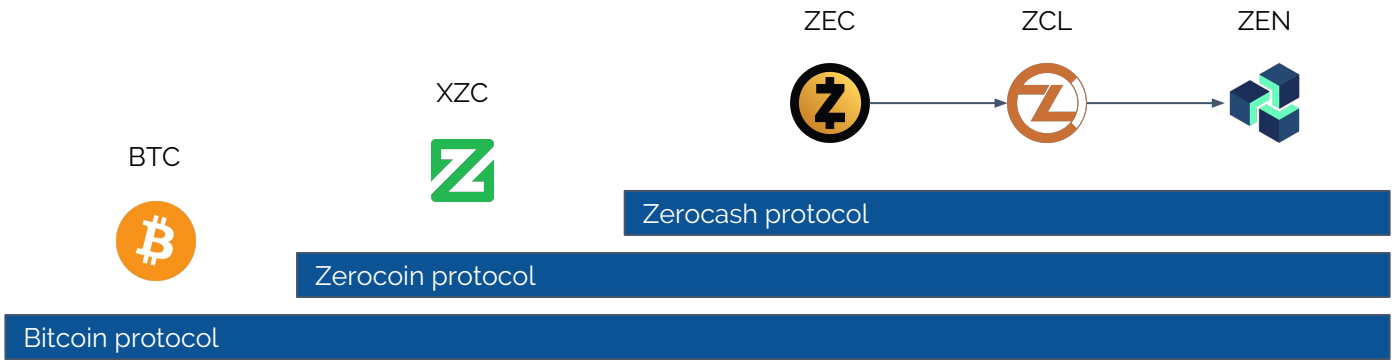
The last coin in the comparison is Horizen, a coin forked from Zclassic which itself is a fork of ZCash. As such, the privacy features of Horizen are very similar to what ZCash is offering. However, the goals of Horizen go beyond private currency. The team behind ZClassic wanted to enhance it to create a decentralized global community and that is when Horizen (at the time, ZenCash) was created, as a foundation for communication, file-sharing, and economic activities.

The main difference between Horizen and ZCash is that Horizen is implementing a Secure Node system. Secure Nodes (similar to Zcoin's and Dash's master nodes) maintain the blockchain and receive coinbase rewards. The nodes do not prevent 51% attack, as the double spend attack in June 2018 proved.

The privacy oriented infrastructure of the Zen framework features in five aspects. Horizen is doing the same as ZCash, value transfer. As the privacy is still optional, there are both regular and shielded transactions. ZenChat is a messaging service, storing messages permanently in the blockchain. ZenCash increased the character limit of ZCash to one thousand twenty-four (1,024) characters. ZenPub enables anonymous and censorship-resistant content publishing from shielded addresses. And lastly, ZenHide, currently under development, is using domain fronting to hide the endpoint of communication and enables anonymity for web traffic.

Up and coming improvements and updates for Horizen are concerned with scaling and governance, implementing a protocol-level voting system in the DAO (decentralized autonomous organization). In 2019, the project is planning to deliver the DAO protocol-level voting system to the market together with Dandelion integration.

To clarify the relationship between Zcoin, ZCash and Horizen, see the graphic below:



The visualization shows the development of protocols. Zerocoin protocol was built based on the Bitcoin protocol and the Zerocash protocol with zk-SNARKs was building on the improvements of Zerocoin. On the top of the protocols, there are the coins utilizing each of them. On the Zerocash protocol, the forks are demonstrated. From ZCash the ZClassis forked and Horizen originated as a fork of ZClassic

Strategic Analysis

Strengths

The main strength of the project is its strong focus on technology. As a pioneer in the implementation of the Zerocoin protocol, the development team has experiences with the privacy methods. Based on the roadmap, the team is looking into different methods and acknowledge the shortcomings of their current solutions, chiefly the initial trusted setup and scalability. If they succeed in solving these issues with their next-gen protocol, for example by implementing bulletproofs, they would gain a significant advantage.

This technology-driven strategy is fueling not only the privacy features but also general blockchain improvements. MTP ASIC resistant algorithm is about to go live in mid-September and may offer an alternative to Equihash. This may be extremely relevant. Based on a study by ZCash foundation and the University of Luxembourg, in May 2018 30% Equihash Mining Algorithm is Likely Mined by ASICs and in June, Bitmain came with Equihash ASIC.

The self-sufficient funding is also an advantage of the Zcoin project. Based on the latest interview with the team, they are able to continue with the project for the next two years even without revenue or rewards. The interview is one example of the open and honest communication the team is pursuing. This strategy is paying off by creating another one of the team's strengths, engaged community.

The last thing that can foster further acceptance of Zcoin are some of the partnerships, mainly with the hardware wallets Ledger and Trezor.

Weaknesses

As the technology is the main driving force behind the project, this can be considered both a strength and weakness. The big question of the trusted setup and a huge size of proofs and transactions are some of the issues of Zero-knowledge proof based privacy solutions. A second concern lies in privacy being optional, not a default feature, which weakens the position of Zcoin in comparison to e.g. Monero.

The two mentioned issues are prevalent in a discussion forums of all Zerocoin based altcoins compared in the section of Market segment comparison. However, in the Zerocoin roadmap it is not communicated when and how they will be solved. The next-gen protocol is promising improvements in both, but for a more detailed description, we will have to wait for the whitepaper release.

The current lack of a whitepaper and a unified communication strategy is something that is damaging the otherwise positive brand image of Zcoin. The description of the technology, vision, mission and overall strategy is communicated through blog posts and podcasts but there is no one unified source. Hopefully, the team will improve this with the release of the new whitepaper.

In terms of the general project, the whole team and partnerships are strongly oriented on the Asia market. Even though this opens some opportunities, it limits US exposure and global presence. In the crypto world, where law enforcement may affect the future of the whole market, geographical diversification may be important for mitigating the risk of regulations.

The potential of the US market is yet to be seen. However, with the SEC (US Security Exchange Commission) opening the CBOE (future exchange) Bitcoin ETF filing for public comments, there is certainly an interesting outlook. If the SEC approves the ETFs, it could mean an indirect approval of mainstream investments in all other cryptocurrencies as well.

Strategic Analysis

Opportunities

As we have already outlined in our previous report, there is a certain potential for privacy solutions. With the increasing popularity of cryptocurrencies, the question of on-chain privacy and confidentiality of transactions gains more and more attention. The coins that will be able to provide enhanced privacy while assuring scalability at the same time can seize the opportunity and gain significant market share.

The main focus of the Zcoin team on the technology and development is leaving unused opportunities in the marketing. Once the development of the new-gen protocol is up and running with the whitepaper out and unified and clear in message, the team can start investing in marketing and explore the benefits of reaching out to the audience in a more active way.

The fact that the whole project is based in Asia and the strong position of Mr. Insom in the Asia crypto scene may represent an opportunity for the project to gain a strong user base in the Asia market. Mr. Insom is currently also a CEO of Satang Pro (TDAX), a Thailand based digital asset exchange. This may help Zcoin to become spendable throughout Thailand.

Whether the Ethereum ZoKrates (toolbox for creation and verification of Zero-knowledge proofs in ethereum smart contracts) will open new opportunities for Zcoin is yet to be seen. Zeth is the result of research into implementing the Zerocoin protocol into ethereum with the goal to offer an alternative to privacy enabled by zk-SNARKs.

Threats

A significant threat to the position of Zcoin in the market of privacy coins represents the strong competition. As already mentioned, there are three leading coins in the sector, each with a specific advantage. In the sector of coins utilizing the Zero-knowledge proof for privacy solution, all projects seek to solve the issue of initial trusted setup and scalability. The first to introduce a satisfying solution will gain a significant market share.

Regulation represents a potential threat to privacy coins. As the attractiveness of cryptocurrencies to criminals is a common argument for increased regulation, authorities may affect the market. The weakest points of the crypto ecosystem would be centralized infrastructure providers, for example, the exchanges.

When looking at the Asia region, there are already intentions to regulate the crypto market in several countries. Japan and Korean exchanges were pushed to delist some of the privacy coins such as Monero, ZCash, and Dash. From July 4, Thai regulations for ICOs came into practice. This legislative restricts ICOs as a way of fundraising by implementing a two-tier vetting procedure. The first tier is represented by accredited ICO portals, scanning the applications and passing those that fit into the SEC (Securities and Exchange Commission).

Based on the announcement from July 4, applicants to the two-tier process will have to comply with several conditions, such as the minimum capital of 5 million Thai baht ($150,000). Starting with July 16 the projects would also have to provide a business plan and token distribution strategy. In the announcement, the SEC has mentioned such details as checking the source code and evaluating the risk readiness of investors.

Other potential threat may come from the technologies the team is currently looking into. The Tech4Tokens (T4T)" model as introduced by the zk-STARKs team or implementation of bulletproofs on top of an existing established blockchain such as bitcoin may potentially provide privacy inside of established project. Right now, we can see the utilization of bulletproof range proofs for hiding the transaction amount on bitcoin. However, the solution is probably to be implemented in scope of a sidechain, not to assure the privacy on the whole chain,

Conclusion

Overall, the segment of privacy coins promises potential and opportunities for investments. The demand generated by not only privacy conscious users but also big companies creates a ground for broader acceptance of coins focusing on privacy and confidentiality of the users' private information.

The value of Zcoin depends chiefly on the technology the team will be able to deliver. Currently, the privacy solution based on Zerocoin protocol has its limitations and does not offer a significant advantage over the competition. The outlined potential of the next-gen protocol is very promising. If it provides a solution to the trusted setup and scaling issues, investors can certainly expect a value increase.

There are still some open questions. How will the team cope with tightening regulations in Thailand, their headquarter? Is the team capable of seizing the whole potential of the right brand image and capturing the opportunity of exploring a stronger marketing strategy? The answers are to be seen in the near future.

Even though it is a valid project with a strong development team and technology behind it, in comparison to the market leaders in privacy coins, Zcoin still has room for improvement to distinguish their project from the competition. Also, the absence of a whitepaper is a clear example of lacking a marketing strategy and focus.

ITF & Disclosure

We are a fintech organization that provides cryptocurrency traders with a suite of trading tools to better achieve their goals. Our mission is to give traders more power, control, and confidence over their cryptocurrency trades through technology.

Check our website for more cryptocurrency and blockchain-related content, guides and research reports.

Personnel disclosures: As noted earlier in the report, Poramin Insom is a founder of Zcoin and is currently CEO of TDAX. Mr. Insom is also an advisor in ITF. Sebastian Bausch, also an advisor to ITF, is a member of TDAX's Board of Directors. Additionally Benjamin Lakoff, the head of Finance and Strategy at ITF and IT Alpha (ITA), is a Director at TDAX. Several members of the ITA are long Zcoin, including Mr. Lakoff. Finally, it has been confirmed that ITF currently holds Zcoin.

Disclaimers

ITF, is engaged in providing trading services to the cryptocurrency trading market. Through its bot and other services it alerts its subscribers/followers ("Users") to certain market conditions based on those Users' preselected settings and trading preferences. Additionally, ITF does make available, from time to time, written or electronic communications that include research analysis, and/or a opinions concerning the DLT/cryptocurrency markets ("Reports"). The views expressed in such Reports are based solely on information available publicly/internal data/other sources believed to be true. The information is provided merely as a complementary service and do not constitute an offer, solicitation for the purchase or sale of any financial instruments, inducement, promise, guarantee, warranty, or as an official confirmation of any transactions or contract of any kind.

Research data and reports published/emailed/Telegrammed/etc. and or those made available/uploaded on social networking sites (e.g. Facebook, Twitter, LinkedIn, etc.) or disseminated in other print or electronic media by ITF, or entities with which it partners and any subsidiaries or partners thereof ("Affiliates"), or those opinions concerning cryptocurrencies expressed as and during the course of a public appearance, are for informational purposes only. Reports are provided for assistance and are not intended to, and must not, be used as the sole basis for an investment decision. The User assumes the entire risk of any use made of this information. Reports may include projections, forecasts and other predictive statements which represent ITFs or its Affiliates' assumptions and expectations in the light of currently available information. These projections and forecasts are based on industry trends, circumstances and factors which involve risks, variables and uncertainties. The actual performance of a company, project, token or currency represented in a Report may vary from those projected. The projections and forecasts described in any Report should be evaluated keeping in mind the fact that they:

- are based on estimates and assumptions;
- are subject to significant uncertainties and contingencies;
- will vary from actual results and such variations may increase over a period of time;
- are not scientifically proven to guarantee certain intended results;
- are not published as a warranty and do not carry any evidentiary value; and
- are not to be relied on in contractual, legal or tax advice

Prospective investors/traders and others are cautioned that any forward-looking statements are not predictions and may be subject to change without notice. Reports based on technical analysis ("TA") are focused on studying charts and movements of a given currency or token's price movement and/or trading volume. As such, a Report based on TA may not match with a Report on fundamental analysis. Though Reports are reviewed for any untrue statements of material facts or any false or misleading information, ITF does not represent that ANY REPORT is accurate or complete and again emphasizes that NO REPORT should be relied on in connection with a purchase, investment, commitment, or contract by anyone whatsoever. ITF does not guarantee the accuracy, adequacy, completeness or availability of any information in any Report and therefore CANNOT be held responsible for any errors or omissions or for the results obtained from the use of such information. ITF, its Affiliates and the officers, directors, and employees of either, including analysts/authors shall not be in any way responsible for any direct, indirect, special or consequential damages that may befall any person from any information contained in any Report nor do they guarantee or assume liability for any omission of information from therein. Information contained in any Report cannot be the basis for any claim, demand or cause of action. These data, Reports, and information do not constitute scientific publications and do not carry any evidentiary value whatsoever.

Disclaimers Continued

ITF's Reports are not for public distribution. Reproduction or dissemination, directly or indirectly, of research data and/or ITF Reports, in any form, is prohibited except with the written permission of ITF. Persons into whose possession the Reports may come are required to observe these restrictions. Opinions expressed therein are current as of the date appearing on the report only. Data may be subject to update and correction without notice. While ITF endeavors to update (on a reasonable basis) the information discussed in the Reports, there may be regulatory, compliance, or other reasons that prevent ITF from doing so.
The Reports do not take into account the particular investment objectives, financial situations, risk profile or needs of any person, natural or otherwise. The User assumes the entire risk of any use made of this information. Each recipient of a Report should make such investigation as deemed necessary to arrive at an independent evaluation of an acquisition of the asset referred to in any Report (including the merits and risks involved).

Cryptocurrencies involve substantial risks and are not suitable for all investors/traders. Investors can lose their entire investment relatively easily in the cryptocurrency markets. Before acting on any advice or recommendation in this material, Users should consider whether it is suitable for their particular circumstances and, if necessary, seek professional advice. The price and value of investments referred to in research reports and the income from them may fluctuate.

Certain information set forth in this Report contains "forward-looking information", including "future oriented financial information" and "financial outlook", under potentially applicable securities laws (collectively referred to herein as "Forward-Looking Statements"). Except for statements of historical fact, information contained herein constitutes Forward-Looking Statements and includes, but is not limited to, the (i) projected financial performance of a company, project, token, or currency; (ii) completion of, and the use of proceeds from, the sale of tokens being offered to the public; (iii) the expected development of a company, project, token, or currency's business, projects and joint ventures; (iv) execution of the company's or the project, token, or currency's developers' vision and growth strategy; (v) sources and availability of funding for the company, project, token, or currency; (vi) completion of any projects that are currently underway, in development or otherwise under consideration; (vi) renewal of any material agreements; and (vii) future liquidity, working capital, and capital requirements. Forward-Looking Statements are provided to allow potential investors the opportunity to understand ITF's beliefs and opinions in respect to the future of a given company, project, token, or currency so that they may use such beliefs and opinions as one factor in evaluating an investment.
NO statement issued on ITF's website or in any Report is a guarantee of future performance and undue reliance should not be placed on them. Such Forward-Looking Statements necessarily involve known and unknown risks and uncertainties, which may cause actual performance and financial results in future periods to differ materially from any projections of future performance or result expressed or implied by such forward-looking statements.

Although Forward-Looking Statements contained in this presentation are based upon what ITF and/or its Affiliates believe are reasonable assumptions, there can be no assurance that Forward-Looking Statements will prove to be accurate, as actual results and future events could differ materially from those anticipated in such statements. Neither ITF nor any of its Affiliates undertake any obligation to update forward-looking statements if circumstances or management's estimates or opinions should change except as required by applicable laws. The User is cautioned not to place undue reliance on forward-looking statements.

The User should consult their own advisors to determine the merits and risks of ANY investment.