Zcash

Market Research

Summary

Once on the fringe of society, cryptoassets and blockchain are now undergoing a great gentrification in order to appeal to a wider audience. **Zcash** is leading this charge by reinventing the way people think about privacy coins. Many authorities have shunned anonymous cryptocurrencies even though personal privacy is an ideal cherished by many. By using the power of the blockchain and zero knowledge proofs, **Zcash** brings personal privacy to online transactions, changing the perception of Internet money.

All information is valid as of March 15th, 2019. All feedback is welcome.

Mati Greenspan, Senior Market Analyst @eToro
eToro: @MatiGreenspan | Twitter: @MatiGreenspan | LinkedIn: MatiGreenspan

Basic Statistics

- **Cryptoasset type:** Money Coin
- **Max. Supply**: 21,000,000 ZEC
- **Current Circulating Supply**: 6,095,096 ZEC
- **Market Capitalization**: $319 million
- **Token Economics:** Deflationary asset
    - Similar to Bitcoin, the block reward is halved approximately every four years, reaching the asymptotic value of 21 million ZEC, thus making it effectively deflationary.
- **Protocol:** Proof-of-Work
    - Equihash

History

The conception of **Zcash** goes back to 2013 as a project named Zerocoin, led by Matthew Green, Ian Miers, Aviel Rubin and Christina Garman from John Hopkins University. Initially, it was conceived as a sort of add-on to **Bitcoin** that would implement privacy on the network. However, in mid 2014, a new independent coin under the name of Zerocash was conceived, with the collaboration of researchers from MIT and Tel Aviv University.

Later, with the support and leadership of Zooko Wilcox, the **Zcash** project was finally born in its current conception, and the first operational network was developed and launched in 2016. The code is open-source. **Zcash** was launched with the support of a private company known as the Zerocoin Electric Coin Company, LLC. $2 million raised in private funding in 2016 helped with the development before launch. The non-profit Zcash Foundation now shares responsibilities with the Electric Coin Company to further the growth of **Zcash**.

Development Team

Zooko Wilcox is Founder and CEO of **Zcash** and arguably the most renowned figure behind the project.

Zooko Wilcox is an American entrepreneur and computer security expert. He is responsible for the creation of different protocols, filesystems and hash functions, and is a respected figure in the cryptography community.

He is the founder of Least Authority Enterprises, which offers secure cryptographic storage solutions. In 2016, he became one of the founders of the **Zcash** project, and has since served as its CEO.

Matthew D. Green is a cryptography professor and researcher at the Johns Hopkins Information Security Institute. He proposed the Zerocoin privacy protocol with his group of graduate students, and has since been involved in the development of Zerocash and then **Zcash** as a founding scientist. He serves as a board member of the Zcash Foundation.

Mati Greenspan, Senior Market Analyst @eToro
eToro: @MatiGreenspan | Twitter: @MatiGreenspan | LinkedIn: MatiGreenspan

Josh Cincinnati is the Executive Director of the Zcash Foundation. After obtaining a Master's Degree in Business Administration from Stanford University, Josh has been involved with several companies and start-ups, from Lyft to blockchain platform, BlockCypher. An advocate of privacy and cryptocurrency, he joined the Zcash Foundation as Senior Program Manager and was appointed as Executive Director in March 2018.

Organizational Structure

The fact that **Zcash** is primarily maintained by a private company, instead of a non-profit organization like most crypto projects has drawn criticism but is an important aspect of the ecosystem. Some of the biggest concerns from the community about Zcash have to do with the "Founders' Reward" that splits a certain percentage (20%) of the mining reward of each block between the founders, initial investors, the company and the foundation. This, however, helps maintain a good team behind the network that can provide a high-quality and well-maintained piece of software that is less susceptible to potentially exploitable bugs, as pointed out by the well-known privacy advocate Edward Snowden.

Founder's Rewards are also not exclusive to **Zcash**. **Dash** has a treasury system, and **Decred** has a 10% so-called "Developers' Subsidy".

Independent from the Electric Coin Company is the Zcash Foundation, a non-profit organization and public charity with the goal of creating a privacy and payment infrastructure for all internet users. The Foundation acts as stewards for the Zcash protocol, supports scientific research reinforcing the coin's privacy ideal and offers governance over the Zcash protocol and network. This idea of stewardship is further reinforced by a partnership with Parity to develop an alternative full node client for Zcash. This independent implementation is just one of the steps the foundation has taken to increase decentralisation and separation of the Zcash protocol from the Electric Coin Company.

Use Cases

Zcash was born with the main idea of privacy in mind. A commonly used comparison to describe the difference between Zcash and other cryptoassets is that **Zcash** represents *https* to **Bitcoin**'s *http*. All relevant information is still stored in a secure and publicly verifiable blockchain, but when using shielded addresses, sensitive elements like the addresses and balances involved in the transaction are kept private.

This is done using zero-knowledge proofs, which are further described in the technical description. These proofs are able to verify that a specific transaction is valid without revealing the contents of the transaction.

Privacy is more important than simply not allowing others to see the nature of the transactions we perform on the blockchain. It also guarantees the fungibility of the currency. Fungibility simply means that one unit of currency is exactly as valuable as another. Traditional currency, like US dollars or Euros, are generally fungible, something that does not occur with many cryptocurrencies.

Cryptoassets with a public ledger containing information of all transactions can lead to parties declining the use of coins based on their public transaction history. With shielded addresses in **Zcash**, it is not possible to check the history of transactions of a coin or user without the permission of the user themselves, hence guaranteeing the fungibility of the currency. This way, each unit of Zcash is equally acceptable to all parties regardless of where they may have been used in the past.

Regulation and Selective Disclosure

Regulation has long been a recurring problem for the crypto industry in general and for so-called privacy coins in particular, due to reservations from governments around untraceable currency exchanges, which can facilitate illicit transactions.

The **Zcash** team is well aware of this and in fact does not fully identify as a privacy coin. It is here where the concept of selective disclosure becomes important.

Users have the choice to send completely private transactions, and unlike fully public blockchains like **Bitcoin**, **Zcash** will not show the details of these transactions to anyone on the network.

However, users can select to disclose this information to certain people using “viewing keys”. This allows for potential regulatory compliance but helps to maintain a higher level of privacy. In fact, this also facilitates compliance with regulations that require fundamental privacy for consumer financial information. **Zcash** is, in fact, listed in several of the most important regulated exchanges and financial apps like Gemini, Coinbase, Circle, Galaxy and, of course, **eToro** in part due to this feature of selective disclosure.

The Winklevoss brothers, behind Gemini, even stated that **Zcash** is most likely the privacy coin regulators will be more comfortable with. **Zcash** is also one of the few cryptocurrencies that have been approved by the New York State Department of Financial Services for trading.

Trusted Setup

In order to secure the network against counterfeiting attempts, a unique procedure was performed during the creation of **Zcash** called Multi-Party Computation Ceremony (video of the ceremony). This refers to the generation of a secret cryptographic material that is later used in the blockchain protocol behind **Zcash**. This procedure was done for the launch of the network and is repeated whenever there is a hard fork of **Zcash**. Several

parties are involved to assure that the system is not compromised. In particular, 6 people participated in the first ceremony and two groups of 80 people in the second one. It is important to understand that if only one of the participants deletes the "cryptographic waste" after the ceremony it is impossible to recreate the parameters of the network and it can be considered secure. However, if all of the participants are compromised at the same time, it would theoretically be possible to generate coins out of thin air even without breaking privacy.

Technical Description

The technology of **Zcash** is based on the concept of **zk-SNARK**s, which stands for *zero-knowledge succinct non-interactive argument of knowledge*. **Zcash** was the first large-scale application of zk-SNARKs, which are what guarantees that transactions can be verified by miners without revealing their contents. The different elements of the name explain the nature of these proofs:

- They are *zero-knowledge*, which means that one can verify certain information without the need to know anything about the information itself.
- *Non-interactive* means that no further exchange of information is needed other than a first communication from the prover to the verifier. Besides, it is possible to verify the correctness of the computations without executing the computations themselves.
- Proof of knowledge (or *argument of knowledge*) suggests that the prover can convince the verifier not only that the information exists and is true, but that he knows the content of this information.
- *Succinct* simply means that the verification process is fast and light-weight, even when the information to be verified is large.

To show how important zk-SNARKs can be for the industry, they are being implemented into **Ethereum** and in a prior collaboration with Electric Coin Company, into JP Morgan's blockchain platform Quorum.

Zk-Snarks are an extremely complex and advanced cryptographic concept that only a few mathematicians and cryptography experts fully understand. Some people have pointed out that this could be risky given that not many people can verify if the code powering the network is secure and error-free.

Here is an interesting video that explains zero knowledge proofs in simple terms.

There are two types of addresses in the **Zcash** network, known as *shielded addresses* (or *z-addresses* because they start with the character "z"), which are private, and *transparent addresses* (or *t-addresses* because they start with the character "t"), which are transparent. Transactions between shielded addresses are private and the information is not available to the public, despite the existence of the transaction is written on the blockchain.

Transactions between transparent addresses are public and show the associated information similar to how a **Bitcoin** transaction works.

Transactions between shielded and transparent addresses are also possible, where the ZEC being transferred can be *shielded* or *deshielded*. Depending on whether **ZEC** is transferred from a shielded address to a transparent address or vice-versa, the input or output will be known, something that is important to consider when making any transactions involving transparent addresses. Shielded addresses can still be audited, but unlike **Bitcoin** where everything is public, it can only be so with the user's permission.

Zcash allows fast transactions with a small fee of around 0.0001 ZEC, or approximately $0.005 at current prices. **Zcash** code is open-source and, like many cryptocurrencies, was originally based on the technology powering **Bitcoin.**

Recent & Future Developments

On October 29th, 2018, **Zcash** achieved an important milestone by activating *Sapling* and reaching version 2.0. Sapling is an important update to the network that improves the efficiency of shielded addresses, making private transactions more prevalent in the network. It was also recently disclosed that this update solved a critical bug that could have allowed exploiters to print infinite coins. The team waited to make the vulnerability public until solving the problem in the new version of the source code and giving other vulnerable projects with relatively high market caps time to fix the problem as well. This action was well received by the community and even IOHK's Charles Hoskinson praised the development team for their disclosure procedure. Charles Hoskinson himself revealed the existence of a similar bug in **Bitcoin** that could have allowed for the creation of billion of coins that was fixed in the early phases of the currency.

Zcash is a fully operational network that is in friendly competition with other privacy coins like **Dash** and **Monero**. The latter two have a larger market share right now, and **Zcash** has been the subject of some criticism regarding the centralization of how it was launched by a private company as previously mentioned. However, the importance of privacy-focused secure currencies in the crypto sphere cannot be underestimated and the technology behind **Zcash**, particularly zk-SNARKs, has been praised by many experts, including **Ethereum**'s founder Vitalik Buterin, who refers to zk-SNARKs as the "single most under-hyped thing in cryptography right now".

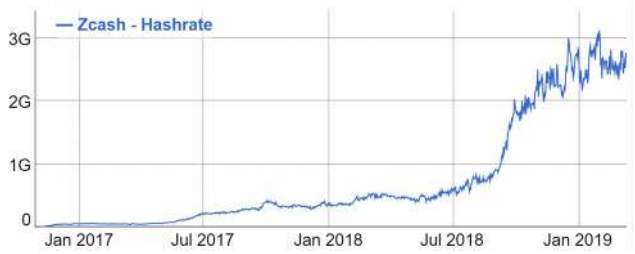
Government regulation has for now focused on larger players of the cryptoasset space, like **Bitcoin**, and utility tokens that could be deemed as securities. Authorities are however aware of the possibility of privacy coins gaining more widespread use, in occasions for money laundering or other illicit purposes. It is unclear how these regulations will affect the evolution of these coins since it is possible for users to privately disclose

transaction details to third parties, it is possible to implement sound regulatory policies for services and individuals. That said, like physical cash, it would be hard for governments to completely regulate **Zcash**.

Coin Evaluation

The token economics of Zcash are very similar to those of Bitcoin. It has the same maximum supply and the same halving schedule. Therefore, we felt it more fitting to focus this section on unique evaluation metrics that apply specifically for privacy coins.

An important resource that will be referenced in this section is the Privacy Coin Matrix, a spreadsheet that compares different privacy coins in terms of many different attributes.



Regarding trading and value, **Zcash** ranks third amongst actual privacy coins, behind **Monero** and **Dash**, with approximately a third of their total market capitalization. The daily volume is slightly higher than for **Monero** and much smaller than for **Dash**. According to Zooko himself, **Zcash** is a top-5 cryptoasset in terms of OTC volume, proving that it is a coin with great institutional demand. The most relevant OTC desks, like Genesis, Galaxy and Circle offer trading with **Zcash**. Besides, hashrate is growing, which not only indicates increased interest but also the possibility of having a more secure network.

In terms of economics, two noteworthy metrics can be identified about **Zcash**. First, its inflation is much higher than all other coins studied, sitting at around 30% annually since the block reward has not halved yet. On the other hand, there is the aforementioned 20% treasury block reward for every block mined until the first halving. The importance of this has already been described, and how it can help ensure higher security for the network with a dedicated development team, which has proven to maintain a consistent release schedule in the past.

Privacy is indeed a very important aspect for valuation. In **Zcash**, like in virtually all privacy coins except **Monero**, private transactions are actually optional and not default. **Zcash** is the only major privacy coin along with **Monero** that offers cryptographic privacy and hides information about the sender, receiver and amount transacted. Additionally, unlike **Monero**, **Zcash** truly breaks the link between sender and receiver and does not simply mix the transaction with others. In that sense, it can be argued that **Zcash** offers more privacy than **Monero** and especially **Dash**.

Scalability is also an issue for many blockchain networks. **Zcash** offers a current theoretical maximum of 62 transactions per second, or 7 private transactions per second, compared to **Bitcoin**'s 7.7 tx/s for instance.

Investments Risks

Trading cryptocurrencies can potentially be very profitable as seen in the past, but it is also a very challenging activity that can carry a significant level of risk. Cryptocurrency markets are associated with high volatility, and **Zcash** is no exception.

It is important to carefully assess your investment goals, methodology and level of experience before deciding to start investing in a new market. It is also extremely important to diversify and view cryptocurrency as an additional element of your portfolio. Given the high risk associated with this type of asset, it is recommended not to allocate more than 20% of your portfolio into cryptocurrencies. Given that the possibility to lose a part or even all the money invested exists, it is extremely important to invest only money that you can afford to lose.

In any case, all the information presented in this Market Report does not constitute financial advice, and introduces no obligation or recommendations for action.

Special thanks to: The Electronic Coin Company, Kobi, Bogdan, Katie, Tom, the Beam Privacy Project, and CryptoAnalyst.

Resources

- Official Website
- Zcash Community Chat
- Zcash Community Forum
- Zcash Foundation
- List of stores and services accepting Zcash
- Zcashd on GitHub
- Fortune article on Zcash
- Zcash documentation

Disclaimer

Cryptocurrencies are not regulated. You will not benefit from the protections available to clients receiving regulated investment services. The content is intended for educational purposes only and should not be considered as investment advice. Your capital is at risk. eToro's officers, directors or employees may own or have positions in investments mentioned. Past performance is not an indication of future results.

Opinions, interpretations and conclusions represent our judgement as of this date and are subject to change. The information and opinions contained in this document are based on sources believed by eToro to be reliable. No guarantees or warranties are made to its accuracy, completeness or suitability for any purpose. This document is supplied solely for your information and may not be re-produced, redistributed or passed to any other person or published in whole or in part for any purpose.

Any price or investment predictions, analysis, and/or advice contained in this report is not endorsed by the Zcash Company, and is not a reflection of any public or private communications from the Zcash Company.

All the information presented in this Market Report does not constitute financial advice, and introduces no obligation or recommendations for action.

Mati Greenspan, Senior Market Analyst @eToro
eToro: @MatiGreenspan | Twitter: @MatiGreenspan | LinkedIn: MatiGreenspan

Contact Us

eToroX Crypto Exchange: Info@etorox.com

Corporate Accounts: corporate@etoro.com
Affiliate Marketing:
https://www.etoropartners.com/
Public Relations: PR@eToro.com
Customer Support:
https://www.etoro.com/customer-service/

eToro By Regions

Iqbal Gandham
UK Managing Director
Iqbal.v.Gandham@eToro.com

Jasper Lee
South East Asia Managing Director
JasperLee@eToro.com

Guy Hirsch
United States Managing Director
Guyhi@etoro.com

George Verbitsky
Russia & CIS Managing Director
Georgeve@eToro.com

Robert Francis
Australia Managing Director
Robertfr@eToro.com

Elie Edry
French & LatAm Regional Manager
Elieed@eToro.com

Emanuela Manor
Italian Regional Manager
Emanuela@eToro.com

Dennis Austinat
Germany Regional Manager
Dennisau@eToro.com

George Naddaf
Arabic Regional Manager
GerogeNa@etoro.com

Yael Moscovitch
ROW Regional Manager
Yaelmo@etoro.com

We're hiring!!! Come see which positions are available at: www.etoro.com/about/careers/