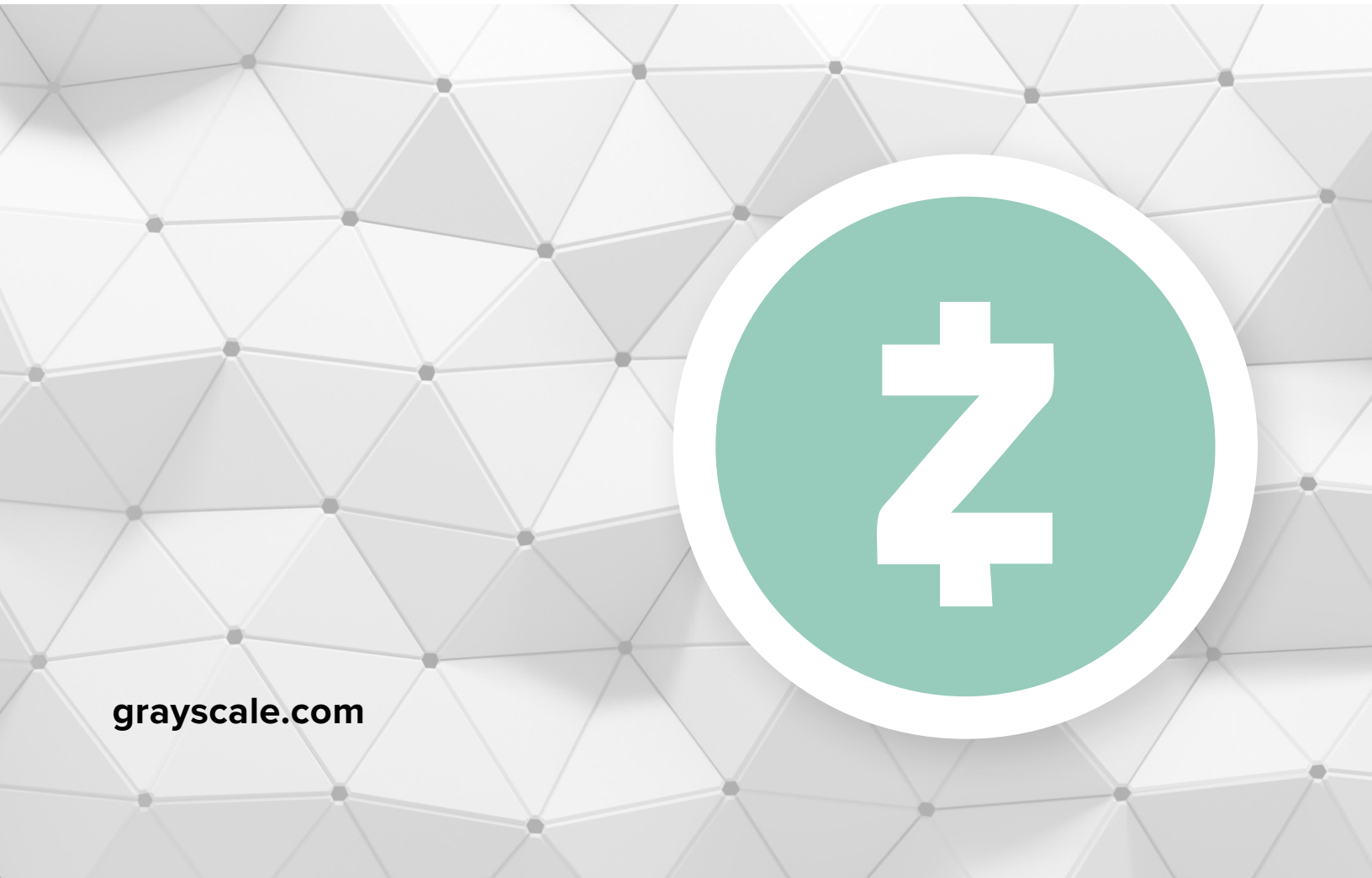
GRAYSCALE

An Introduction to Zcash



grayscale.com

Introduction

Zcash is a decentralized, peer-to-peer (P2P) digital currency and payment network equipped with privacy- and security-enhanced features. It is the first network to integrate zk-SNARKS,[1] an application of zero-knowledge cryptography featured in MIT Technology Review's 10 Breakthrough Technologies of 2018[2], which validates transactions without revealing information such as the address of the sender, receiver, or payment amount. Zcash is the implementation of the Zerocash whitepaper, published in May 2014 through the combined efforts of researchers from universities around the world.[3] The Zcash network was formally launched on October 28, 2016 by a privately held company known today as the Electric Coin Company (ECC), led by founder and CEO, Zooko Wilcox. Separately, in June 2017, a non-profit called the Zcash Foundation formed with the mission of building internet payment and privacy infrastructure for the public good, primarily serving the users of the Zcash protocol and blockchain.[4] Together, the ECC and Zcash Foundation have largely been responsible for the continued development and improvement of the Zcash network.

The Zcash Project sought to expand upon Bitcoin, which is considered by many to be the benchmark store-of-value and digital currency. By introducing several technical modifications to the original Bitcoin source code, users are granted the ability to decide on the degree of confidentiality associated with their financial activities. These features concentrate on safeguarding financial privacy, including a shift to the Equihash consensus algorithm, and other network upgrades. In addition, the ECC and the Zcash Foundation are backed by prominent digital currency investors[5] and development is supported by a team of world-class engineers and researchers specializing in cryptography.

In May 2020, Zcash announced it would integrate with Cosmos, a layer 1 blockchain like Ethereum, to bring transaction privacy to the chain. The announcement came as part of a broader effort to integrate with all layer 1 blockchains, bringing the transaction privacy of Zcash to the rest of the ecosystem. The following year in a November blog post, the ECC announced that Zcash would begin work to transition to Proof of Stake in 2024. The move to Proof of Stake[6] is an attempt to reduce sell pressure from miners and make the network more equitable through staking.

---

1. Short for "Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge"
2. MIT Technology Review: 10 Breakthrough Technologies of 2018. https://www.technologyreview.com/lists/technologies/2018/.
3. The authors of the Zerocash proposal in alphabetical order are: Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza.
4. The Zcash Foundation was established in 2017 as a non-profit organization under Section 501(c)(3) of the Internal Revenue Code. Notably, the Zcash Foundation's mission is dedicated to internet payment and privacy infrastructure in general, and not specifically the Zcash network. The Zcash Foundation has historically focused on the Zcash network because it believes ZEC is currently the best solution for financial privacy.
5. Digital Currency Group, Inc., the sole member and parent company of Grayscale Investments, LLC, owns an immaterial percentage of the Zcash in circulation and a minority interest in the ECC.
6. https://electriccoin.co/blog/ecc-roadmap-calls-for-focus-on-wallet-proof-of-stake-and-interoperability/

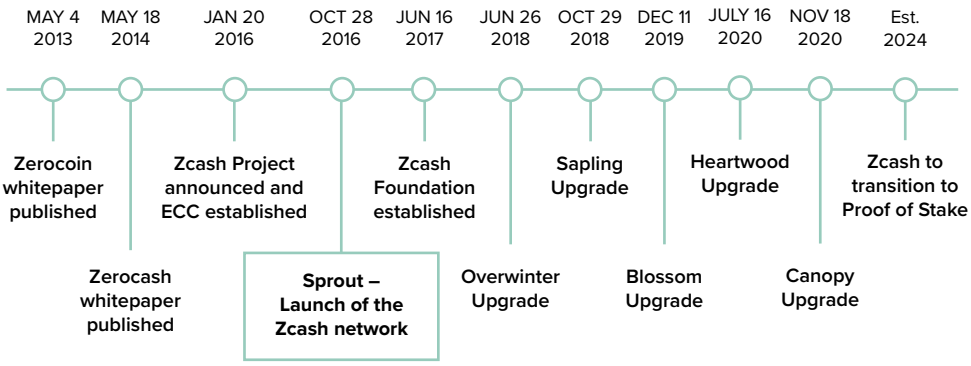
FIGURE 1: **ZCASH SUMMARY STATISTICS**[7]
As of March 31, 2022

Asset	Zcash (ZEC)
Inception of Network	October 28, 2016
Price (USD)	$178.65
Market Cap (USD)	$2.19 billion
Circulating Supply (ZEC / % of Max Supply)	12.28 million / 58.5%
Max Supply (ZEC)	21 million
Current Mining Block Reward (ZEC)	3.125
Next Block Reward Halving Date (Expected)	May 2025
Average Block Time	Approximately 1.25 minutes
Market Segment	Digital Currency Privacy

7. Coin Metrics. As of March 31, 2022

Brief History

FIGURE 2: **TIMELINE OF ZCASH NETWORK**



In an era where information is increasingly digitized and data leaks revealing personal information are frequent, privacy and security have become preeminent concerns for individuals and institutions around the world. Bitcoin attempted to address these concerns with its decentralized network, but, by nature, the Bitcoin blockchain records all transactions and makes them publicly viewable, prioritizing financial transparency at the expense of privacy.

The Zerocoin proof-of-concept was introduced in May 2013 as an extension of Bitcoin. Using cryptography, Zerocoin proposed an additional layer of privacy to the Bitcoin network that would potentially allow for anonymous transactions. It was published by researchers from Johns Hopkins University – Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. However, limitations in its technical design prohibited proper implementation.[8]

Zerocoin laid the groundwork for **Zerocash**, whose May 2014 whitepaper served as an outline for **Zcash**.[9] **Zerocash** addressed two problems identified in the Zerocoin proposal: (i) it enhanced privacy across all dimensions of a transaction, unlike Zerocoin, in which only the identity of the sender could be concealed and not the receiver or transaction amount, and (ii) it decreased both the projected transaction size and block confirmation time by

8. Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. "Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version)." *The Zerocash Project*. May 18, 2014. http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf.
9. Zooko Wilcox. "Hello, World!" *Electric Coin Company*. January 20, 2016. https://electriccoin.co/blog/helloworld/.

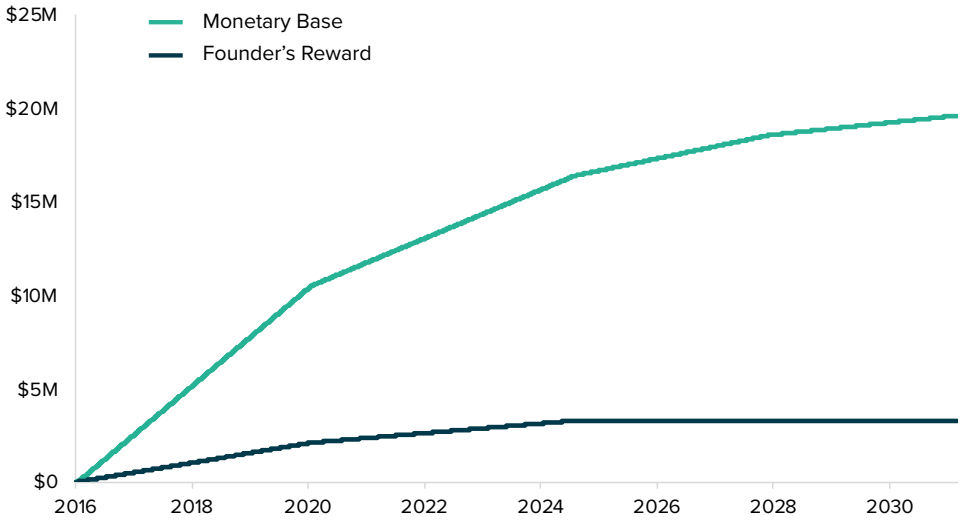
approximately 98%.[10] It was developed in collaboration with the original Zerocoin authors, excluding Rubin, and four academics – Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. Funded by private, federal, and university grants, **Zerocash** is the product of research conducted by scholars from the top universities in the world.

All of these contributions led to the creation of the **Zcash Project** in January 2016. Around the same time, the Zcash Company (now known as the Electric Coin Company, or ECC), led by Bryce "Zooko" Wilcox, was founded, and under its supervision, the **Zcash** network was launched in October 2016.

Electric Coin Company and Zcash Foundation

At inception, the founders of Zcash deliberated over how to fund the ECC, which continues to oversee technical development of the network. The solution they decided upon is known as a "Founders' Reward", which automatically allocates 20% of mining rewards for the first four years after the launch of the network to certain predetermined beneficiaries comprising the ECC, as well as founders, employees, advisors, and investors of the ECC and the Zcash Foundation).[11] In November 2020, the Zcash community voted to extend the founders reward for another four years to continue funding the development of Zcash. The monetary supply schedule for Zcash, including the Founders' Reward, is shown in Figure 3 below.

FIGURE 3: **ZCASH MONETARY BASE AND SUPPLY SCHEDULE**



10. See footnote 5.
11. Zooko Wilcox. "Funding, Incentives, and Governance." *The Electric Coin Company. February 1, 2016. Updated: September 23, 2019.* https://electriccoin.co/blog/funding/.

In addition to the Founders' Reward, Zcash development is funded by early-stage investments. In an effort to be transparent about how their ZEC reserves are used, the ECC publishes their budgets and expenses online, most recently in the *Q3 2019 Transparent Report*. Following the Zcash network launch, the Zcash Foundation, a nonprofit, was established in March 2017. The Zcash Foundation is also funded by the Founders' Reward in tandem with donations from the ECC, amongst others. Though the ECC and the Zcash Foundation operate independently, they also work together to advance Zcash technology and its adoption within the digital currency community.

Network Upgrades

Since the original Zcash protocol, Sprout, was released, Zcash has undergone multiple network upgrades. Each upgrade is supplemented with comprehensive testing of features in testnets. Over time, Zcash has evolved according to community consensus. Contributors to the Zcash Project work towards reaching its final stage, to become the premiere global digital currency with privacy-enhanced features.[12]

- **Sprout – October 28, 2016**
  Inception of the network with initial technical modifications to Bitcoin
- **Zcash Foundation established – June 16, 2017**
- **Overwinter Upgrade – June 26, 2018**
  Installed the foundation for future upgrades
- **Sapling Upgrade – October 29, 2018**
  Improved efficiency of private transactions to increase commercial adoption
- **Blossom Upgrade – December 11, 2019**
  Planned increase in mining frequency of blocks, allowing faster transactions with low fees
- **Heartwood Upgrade – July 16, 2020**
  Enabled more third-party integrations and enhanced network privacy
- **Canopy Upgrade – November 18, 2020**
  Development fund established – miners receive 80% of block rewards, and 20% is distributed to the Zcash foundation to fund development
- **Zcash to Proof of Stake – Expected 2024**
  The Electric Coin Company announced plans to reduce sell pressure from miners and network emissions by transitioning the network to Proof of Stake, expected to occur in 2024.

12. Josh Swihart. "Zcash to 10 billion." *The Electric Coin Company. July 23, 2019. Updated: September 9, 2019.* https://electriccoin.co/blog/zcash-counterfeiting-vulnerability-successfully-remediated

Key Features

By design, Zcash is similar to Bitcoin. It is a software project clone of Bitcoin, often referred to as an altcoin, in which the original source code was copied, then modified to be a secure and privacy-driven digital currency alternative to Bitcoin. To accomplish this, the Zcash protocol has two types of addresses and therefore four types of transactions, as well as features unique to the network:

Address & Transaction Types

Addresses

- Public, or transparent addresses, which always begin with *"t"*.
- Private, or shielded addresses, which always begin with *"z"*.

Transactions

- **Public:** ZEC transferred from a t-address to a t-address. Public transactions appear on the public Zcash blockchain just like Bitcoin. The sender and receiver addresses and transaction amount are all publicly visible.
- **Private:** ZEC transferred from a z-address to a z-address. Private transactions appear on the public Zcash blockchain, but the sender and receiver addresses and transaction amount are all encrypted and not publicly visible.
- **Shielding:** ZEC transferred from a t-address to a z-address. Shielding transactions appear on the public Zcash blockchain, but the receiver address is encrypted and not publicly visible.
- **Deshielding:** ZEC transferred from a z-address to a t-address. Deshielding transactions appear on the public Zcash blockchain, but the sender address is encrypted and not publicly visible.

Privacy Technology (zk-SNARKS)

Created by the SCIPR[13] Lab, zk-SNARKs is an acronym for Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge. Zk-SNARKs are a form of zero-knowledge proofs originating from a 1989 paper published by MIT researchers, where one can prove possession of certain information (e.g., a secret key) without revealing that information and without any interaction

13. SCIPR is an acronym for Succinct Computational Integrity and Privacy Research.

between the prover and verifier.[14] They add additional layers of confidentiality to transactions by concealing the amount, and sender and receiver of ZEC transactions, which are easily verifiable in milliseconds.

Equihash Algorithm

Equihash was conceived in 2016 by Dmitry Khovratovic and Alex Biryukov, research students at the University of Luxembourg. Specifically, Equihash is a proof-of-work (PoW) consensus algorithm, which is fundamental to how miners, or nodes, in the network validate transactions. This authentication process hinders attacks and abuses of the network by requiring computational power on behalf of the miner, which is resource intensive and expensive.

Equihash is designed to verify transactions quickly. To an extent, it is considered to be ASICs-resistant, as GPUs (Graphical Processing Units) are relatively cheaper and therefore currently the preferred choice of equipment. Consequently, the Zcash mining process is more egalitarian by reducing the cost barrier to entry. It also reduces the probability of mining centralization and subsequent risk of attacks on the network. However, the trade-off for adopting Equihash is that computations are more memory intensive and are restricted to the memory capacity of the hardware.[15]

For more on the technicalities of Equihash, please refer to Biryukov and Khoratovich's paper, *Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem*.

Mining Rewards

Miners who successfully confirm a transaction and upload it on the blockchain receive an incentive for their effort in the form of block awards, contributing to the exponential increase in network usage. As illustrated in Figure 4, miners receive 80% of the block reward plus any transaction fees accrued. The beneficiaries of the Founders' Reward (e.g., founders, employees, advisors, investors, the ECC, and the Zcash Foundation) receive 20% of the block reward. The Founders' Reward was designed to incentivize those partaking in the development of the network and end after the 2020 halving.

However, in November 2020, the Zcash community voted to extend the Founder's reward until the next halving. After approximately four years, block rewards are estimated to halve again and 100% of the block rewards will go to the miners unless otherwise decided by the community. As a result, miners will receive 80% of the block reward distributions, while the remaining 20% will be

14. Shafi Goldwasser, Silvio Micali, and Charles Rackoff. "The Knowledge Complexity of Interactive Proof Systems." *Siam Journal of Computing (Vol. 18, No. 1, pp. 186-208).* https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf
15. https://www.openwall.com/articles/Zcash-Equihash-Analysis

divided differently than it was before the Canopy upgrade and will be distributed to a developer fund instead of Founders & Vested employees, and ECC's parent company, Bootstrap. The Zcash foundation will retain the previous allocation as shown in Figure 5.

FIGURE 4: **ZEC INITIAL MINING AND FOUNDERS' REWARDS DISTRIBUTION**[16]
October 28, 2016 to Expected October 2020 (expected)

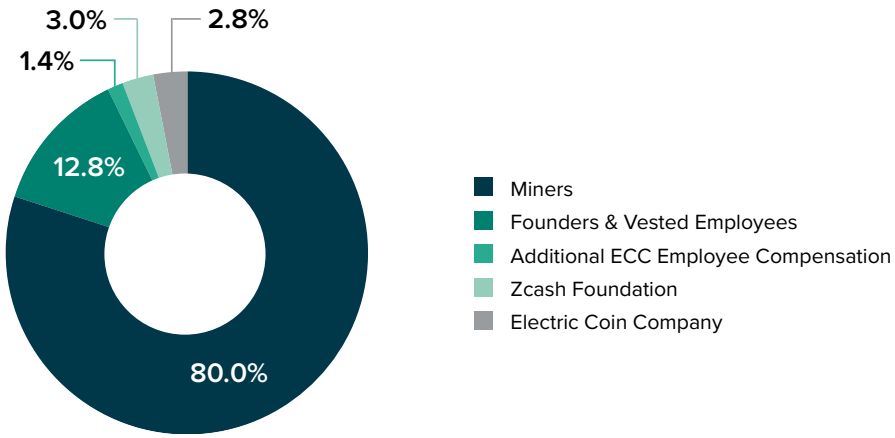
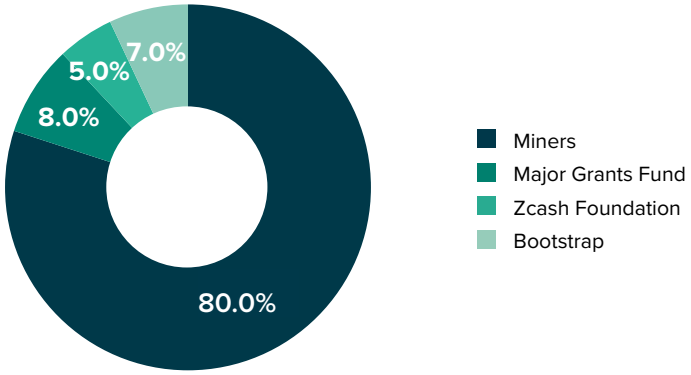


FIGURE 5: **ZEC FOUNDER'S REWARD CONTINUATION ALLOCATION**[17]
Voted on Nov. 18 2020



Block rewards are set to halve for the third time to 3.125 ZEC in May 2025. As a result, profit margins from mining could decrease significantly without any offsetting increase in the ZEC price. For more information on the potential consequences of halving the price of a coin, please refer to our report, *The Next Bitcoin Halving*.

16. "Electric Coin Company Q2 2019 Transparency Report." *Electric Coin Company. May 14, 2019.* https://electriccoin.co/blog/electric-coin-company-q2-2019-transparency-report/.
17. See previous footnote.

Like Bitcoin, Zcash possesses the following qualities, making it an alternative digital currency and payment network:

- **Decentralized**: Zcash is supported by a P2P blockchain protocol, effectively eliminating the need for a central authority (e.g., governments and financial institutions). Vitalik Buterin, the creator of Ethereum, asserts that blockchains are politically and architecturally decentralized, but behave in a logically centralized way, such as the nodes hold equal power in the network and must collaborate to validate transactions.[18]

  One caveat is that while governance is decentralized, there may be risks associated with the level of decentralization of mining pools in the Zcash network. As of October 1, 2021, the top three largest mining pools controlled over 65% of the hashrate of the network.[19]

- **Permissionless**: Anyone can participate in the network.

- **Secure**: In PoW protocols, the network "is secure as long as honest nodes control more [power] than collective attacker nodes."[20] An attacker seeking to make a fraudulent transaction on the blockchain, through what is called a 51% attack, would have to locate the desired block, change the transaction data, then mine each consecutive block until the fraudulent one was accepted by the network. The primary deterrent of these attacks is that they are computationally expensive with uncertain payoff and are therefore unlikely.[21] A month later, the team had successfully remediated the bug with no action required by Zcash users.

  In February 2019, the ECC announced that it had found a potentially debilitating bug and patched it in the Sapling network upgrade before any malicious entity could exploit it.[22]

- **Open-source**: The source code for the Zcash Project is viewable on the Internet, free for anyone to access, contribute to, or fork.[23] This is an important characteristic for building trust and accumulating users.

  Users can introduce Zcash Improvement Proposals (ZIPs), which are feature suggestions designed to improve the network and follow strict technical guidelines.

- **Immutable and irreversible**: Transaction amounts cannot easily be changed or reversed once added to the blockchain.

---

18. Vitalin Buterik. "The Meaning of Decentralization." February 6, 2017. *Medium*. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.
19. "Zcash Mining Pools (ZEC) Equihash." *Miningpoolstats.io*. https://miningpoolstats.stream/zcash.
20. Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System." *Bitcoin Project*. October 31, 2008. http://satoshinakamoto.me/bitcoin.pdf.
21. Saravanan Vijayakumaran. "The Security of the Bitcoin Protocol." *Indian Institute of Technology Bombay*. May 19, 2018. https://static.zebpay.com/web/pdf/Bitcoin-Security-White-Paper.pdf.
22. Josh Swihart, Benjamin Winston, and Sean Bowe. "Zcash Counterfeiting Vulnerability Successfully Remediated." *The Electric Coin Company. February 5, 2019*. https://electriccoin.co/blog/zcash-counterfeiting-vulnerability-successfully-remediated/
23. Forks are modifications to the source code and there are two main types. Soft forks are software upgrades to the main protocol and are backwards-compatible. Hard forks result in the creation of an entirely new blockchain, allowing for two currencies to exist concurrently, and are not backwards-compatible.

- **Finite supply**: Zcash has a maximum supply cap set to 21 million ZEC and is equipped with a disinflationary supply schedule. An established and transparent monetary supply and issuance schedule is critical for evaluating a digital currency's investability.

However, the following characteristic is unique to the Zcash network:

- **Privacy Preservation:** Private transactions can conceal sending and receiving addresses and the payment amount. Zcash gives users the option to remain anonymous, if desired. All transactions, public or private, are recorded on the Zcash blockchain. However, private transaction information is encrypted and not publicly viewable.

Differences Between Zcash and Bitcoin

In the hopes of creating the preferred privacy-enhanced digital currency of choice, Zcash differs in the following ways from the Bitcoin network.

- **Consensus algorithms:** Both Zcash and Bitcoin use PoW consensus algorithms to validate transactions. However, Zcash's Equihash is, to an extent, ASIC-resistant and memory-intensive, with a focus on privacy and security, whereas Bitcoin's SHA-256 requires ASICs and is processor-intensive. As a result, the cost for specialized Equihash mining equipment often outweighs the increased mining rate.

- **Mining rewards:** Zcash enlists a unique mining schedule, in which 20% of mining rewards are allocated to the Founders' Reward in the first four years of the network. In October 2020, the original Founders' Reward will be fully allocated, miners will receive 100% of the block reward thereafter, and, like Bitcoin, block rewards will experience their first halving and continue halving every four years. However, a recent appeal has been made by Zooko Wilcox for the creation of a new development fund to incentivize and financially support development work on the Zcash network beyond the expiration of the Founders' Reward.[24] In November 2020, the proposal was approved by the community and implemented on the network, extending the Founders reward until the third halving estimated for May 2025.

- **Block size limit:** Zcash has a block size limit of 2MB, compared to Bitcoin's block size limit of 1MB for increased transaction speed.

- **Organizational oversight:** Zcash has the Electric Coin Company and the Zcash Foundation overseeing continued development and improvement, whereas Bitcoin does not have any designated organizational oversight.

24. Daniel Palmer. "Zooko Wilcox Pushes for New Developer Fund to Support Zcash." *CoinDesk. August 1, 2019.* https://www.coindesk.com/zooko-wilcox-pushes-for-new-developer-fund-to-support-zcash.

Latest Innovations

Halo for Scalable Privacy

On September 10, 2019, ECC announced via its blog that Sean Bowe, a cryptographer and engineer at the ECC, had discovered a practical technique for creating far more scalable and "trustless" cryptographic proving systems using a recursive proof-composition called Halo. Halo has the potential to enable the implementation of far more scalable digital privacy technology into blockchains such as Zcash—and possibly the public internet and other digital networks—without requiring trust in known individuals or entities in the setup process.[25]

According to the post, "Recursive proof composition holds the potential for compressing unlimited amounts of computation, creating auditable distributed systems, building highly scalable blockchains and protecting privacy for all of humanity. The concept is a proof that verifies the correctness of another instance of itself, allowing any amount of computational effort and data to produce a short proof that can be checked quickly."

ECC is exploring the use of Halo for Zcash to both eliminate the trusted setup required for the implementation of zk-SNARKs privacy technology and to scale Zcash at Layer 1.[26]

Proof of Stake

On November 19, 2021, ECC announced that Zcash would be transitioning away from proof-of-work to proof-of-stake in 2024. The proposal came from the founder of Zcash, Zooko Wilcox, in an attempt to continue building the network in accordance with Zcash's mission of providing economic and social freedom for everyone.

Zcash has experienced downward price pressure partially due to miners selling portions of their mining rewards to cover operating costs. Proof-of-work mining requires recurring maintenance expenses to maintain mining hardware in addition to constant node software updates. For the average user, this level of complexity makes earning rewards through mining to contribute to network security nearly impossible.

Transitioning to proof-of-stake will allow Zcash to better operate within its mission of providing economic freedom to everyone. Average users will be able to earn yield on the Zcash by simply staking their tokens – eliminating the technical barriers and hardware costs required for proof-of-work mining.

---

25. "Halo: Recursive Proof Composition without a Trusted Setup." *The Electric Coin Company. September 10, 2019. Updated: September 13, 2019.* https://electriccoin.co/blog/halo-recursive-proof-composition-without-a-trusted-setup/
26. We refer to on-chain (Layer 1) transactions as those settled on the main blockchain versus off-chain (Layer 2) transactions that are settled outside of the main blockchain. For the Zcash network, the Zcash blockchain is Layer 1, with Layer 2 solutions still being explored. For the Bitcoin network, the Bitcoin blockchain is Layer 1 and the Lightning Network is Layer 2.

Advantages

The differences in network designs lead to four potential advantages of Zcash over Bitcoin with respect to on-chain[27] transactions:

- **Additional layer of privacy:** zk-SNARKs allows users to conceal the ZEC transaction amount, as well as origin and destination of payment. This is advantageous to the Zcash network in light of increasing concerns over financial and digital privacy.

- **Faster transaction speeds:** Zcash block sizes are smaller, with an average block size of 4.3 kB compared to 719.9kB for Bitcoin.[28] This allows for Zcash transactions to be completed four times faster than Bitcoin – Zcash blocks are generated at a rate of 1.3 minutes as opposed to 10.4 minutes for Bitcoin.[29] Additionally, if transaction volume increases on the Zcash network, blocks have the capacity to process more transactions, given its 2MB block size limit.

- **Lower transaction fees:** Transaction costs for Zcash are also lower compared to Bitcoin -- as of October 15, 2019, the average transaction cost for Zcash in USD was $0.06, compared to less than $2.8 for Bitcoin.[30]

- **Lower barriers to entry for miners:** Zcash mining is more accessible to those who are limited by equipment, as the expense of confirming a block, in terms of electricity costs and computational capacity, is cheaper compared to Bitcoin. Therefore, Zcash mining may be attractive to potential miners because it requires less processing power and has lower operating costs.

27. We refer to on-chain (Layer 1) transactions as those settled on the main blockchain versus off-chain (Layer 2) transactions that are settled outside of the main blockchain. For the Zcash network, the Zcash blockchain is Layer 1, with Layer 2 solutions still being explored. For the Bitcoin network, the Bitcoin blockchain is Layer 1 and the Lightning Network is Layer 2.
28. Bitinfocharts. https://bitinfocharts.com/comparison/size-btc-zec.html. As of March 31, 2022.
29. Bitinfocharts. https://bitinfocharts.com/comparison/confirmationtime-btc-zec.html. As of March 31, 2022.
30. Coin Metrics. As of March 31, 2022.

Potential Risks

There are important trade-offs to consider when choosing between different digital currency networks to use and invest in. Selection will often depend on the one that best satisfies the needs of the user. We outline four key risks related to investing in Zcash:

- **Level of decentralization:** There may be risks associated with the level of decentralization of mining pools in the Zcash network. As of March 31, 2022, the top three largest mining pools controlled over half of the hashrate of the network.[31]

  Development of the Zcash protocol is arguably somewhat less decentralized than the Bitcoin network, as the ECC and Zcash Foundation have largely been responsible for the continued development and improvement of the Zcash network. However, based on GitHub, there are over 470 contributors to the "zcashd" codebase on GitHub.[32] Furthermore, many of those in the top 100 contributors (including upstream Bitcoin contributors) do not appear to be affiliated with the ECC or Zcash Foundation.

- **Low adoption:** Zcash has a relatively low rate of adoption and use when compared to Bitcoin. For example, as of March 31, 2022 the total number of addresses on the Zcash network maintaining a balance greater than zero was approximately 796 thousand versus 41.3 million on the Bitcoin network. Moreover, this lower rate of adoption is not constrained to users. It also extends to exchange listings and basic network infrastructure, such as wallet- and front-end payment processing-software.[33]

- **Volatility with new technology**: The innovative cryptographic techniques used in the Zcash protocol are still under development and may have vulnerabilities that have yet to be discovered. In addition, this cryptography is new and could ultimately fail, resulting in little to no privacy than initially publicized. This could adversely affect the ability to complete transactions on the blockchain and compromise the integrity of the Zcash network.

  For example, in March 2018, a developer on the Zcash team discovered a vulnerability that would have allowed an attacker to create counterfeited ZEC without detection.[34] This bug was subsequently fixed with Sapling upgrade in October 2018.

31. "Zcash Mining Pools (ZEC) Equihash." *Miningpoolstats*. https://miningpoolstats.stream/zcash.
32. Zcash, GITHUB (last accessed March 31, 2022), https://github.com/zcash/zcash/graphs/contributors
33. Coin Metrics. As of 3/31/2022.
34. See footnote 17.

- **Legal & regulatory uncertainty**: The SEC has stated that certain digital assets may be considered "securities" under the federal securities laws. To date, the SEC has only identified two digital assets, Bitcoin and Ethereum, for which it does not intend to take the position that they are securities. As a result, any other digital asset, including Zcash, is at risk of being deemed a security, which may have material adverse consequences for such digital asset.

  Furthermore, law enforcement agencies have often relied on the transparency of blockchains to facilitate investigations and comply with laws, such as anti-money laundering (AML), countering financing of terrorism (CFT), and economic sanctions. Because of the privacy-preserving features of the Zcash network, law enforcement agencies may have less visibility into the types of transactions being conducted and there are concerns over whether the Zcash network may be used to conduct criminal activities, which could adversely affect the attractiveness of the Zcash network.

  The ECC recently addressed some of these concerns in a statement describing how the Zcash network complies with the Financial Action Task Force (FATF), the intergovernmental organization that recently finalized its recommendations on how the digital currency sector should be regulated with respect to AML/CFT risks.[35] Despite these efforts, law enforcement agencies may still find that the Zcash network does not comply with laws, such as AML, CFT, and economic sanctions.

35. Jack Gavigan. "How Zcash is Compliant with the FATF Recommendations." *The Electric Coin Company. September 24, 2019.* Updated: September 27. 2019. https://electriccoin.co/blog/how-zcash-is-compliant-with-the-fatf-recommendations/.

Summary

A privacy-enhanced currency and financial network such as Zcash provides global citizens with the freedom to choose how they allocate and spend capital to meet their own economic interests, with selective disclosure determined by users. The growing importance and complexity of the right to privacy in the Digital Era provides Zcash with ample opportunities to satisfy a role as an alternative and private way to exchange and store value. Furthermore, innovations like zk-SNARKs and Halo for combined privacy and scalability of blockchain-based networks may have wider and more profound applications.

Check out our in-depth reports on different digital currencies here.

About Grayscale Investments, LLC

Founded in 2013, Grayscale Investments is the world's largest digital currency asset manager. Through its family of investment products, Grayscale provides access and exposure to the digital currency asset class in the form of a security without the challenges of buying, storing, and safekeeping digital currencies directly. With a proven track record and unrivaled experience, Grayscale's products operate within existing regulatory frameworks, creating secure and compliant exposure for investors.

Grayscale is headquartered in Stamford, Connecticut. For more information on Grayscale, please visit www.grayscale.com or follow us on Twitter @Grayscale.

Important Disclosures & Other Information

All content is original and has been researched and produced by Grayscale Investments, LLC ("Grayscale") unless otherwise stated herein. No part of this content may be reproduced in any form, or referred to in any other publication, without the express consent of Grayscale.

This information should not be relied upon as research, investment advice, or a recommendation regarding any products, strategies, or any security in particular. This material is strictly for illustrative, educational, or informational purposes and is subject to change.

This content does not constitute an offer to sell or the solicitation of an offer to sell or buy any security in any jurisdiction where such an offer or solicitation would be illegal. There is not enough information contained in this content to make an investment decision and any information contained herein should not be used as a basis for this purpose. This content does not constitute a recommendation or take into account the particular investment objectives, financial situations, or needs of investors.

Investors are not to construe this content as legal, tax or investment advice, and should consult their own advisors concerning an investment in digital assets. The price and value of assets referred to in this content and the income from them may fluctuate. Past performance is not indicative of the future performance of any assets referred to herein. Fluctuations in exchange rates could have adverse effects on the value or price of, or income derived from, certain investments.

Certain of the statements contained herein may be statements of future expectations and other forward-looking statements that are based on Grayscale's views and assumptions and involve known and unknown risks and uncertainties that could cause actual results, performance or events to differ materially from those expressed or implied in such statements. In addition to statements that are forward-looking by reason of context, the words "may, will, should, could, can, expects, plans, intends, anticipates, believes, estimates, predicts, potential, projected, or continue" and similar expressions identify forward-looking statements. Grayscale assumes no obligation to update any forward-looking statements contained herein and you should not place undue reliance on such statements, which speak only as of the date hereof. Although Grayscale has taken reasonable care to ensure that the information contained herein is accurate, no representation or warranty (including liability towards third parties), expressed or implied, is made by Grayscale as to its accuracy, reliability or completeness. You should not make any investment decisions based on these estimates and forward-looking statements.

Carefully consider each Product's investment objectives, risk factors, fees and expenses before investing. This and other information can be found in each Product's private placement memorandum, which may be obtained from Grayscale and, for each Product that is an SEC reporting company, the SEC's website, or for each Product that reports under the OTC Markets Alternative Reporting Standards, the OTC Markets website.

Reports prepared in accordance with the OTC Markets Alternative Reporting Standards are not prepared in accordance with SEC requirements and may not contain all information that is useful for an informed investment decision. Read these documents carefully before investing.

Investments in the Products are speculative investments that involve high degrees of risk, including a partial or total loss of invested funds. Grayscale Products are not suitable for any investor that cannot afford loss of the entire investment. The shares of each Product are intended to reflect the price of the digital asset(s) held by such Product (based on digital asset(s) per share), less such Product's expenses and other liabilities.

Because each Product does not currently operate a redemption program, there can be no assurance that the value of such Product's shares will reflect the value of the assets held by such Product, less such Product's expenses and other liabilities, and the shares of such Product, if traded on any secondary market, may trade at a substantial premium over, or a substantial discount to, the value of the assets held by such Product, less such Product's expenses and other liabilities, and such Product may be unable to meet its investment objective.

The shares of each Product are not registered under the Securities Act of 1933 (the "Securities Act"), the Securities Exchange Act of 1934 (except for Products that are SEC reporting companies), the Investment Company Act of 1940, or any state securities laws. The Products are offered in private placements pursuant to the exemption from registration provided by Rule 506(c) under Regulation D of the Securities Act and are only available to accredited investors. As a result, the shares of each Product are restricted and subject to significant limitations on resales and transfers. Potential investors in any Product should carefully consider the long-term nature of an investment in that Product prior to making an investment decision. The shares of certain Products are also publicly quoted on OTC Markets and shares that have become unrestricted in accordance with the rules and regulations of the SEC may be bought and sold throughout the day through any brokerage account.

The Products are distributed by Genesis Global Trading, Inc. (Member FINRA/SIPC, MSRB Registered).

General Inquiries

info@grayscale.com
Address: 262 Harbor Drive, 1st Floor, Stamford, CT 06902
Phone: (212) 668-1427
@Grayscale

grayscale.com