Grayscale Building Blocks | October 2019

GRAYSCALE

An Introduction to Zcash

grayscale.co

GRAYSCALE

October 2019

An Introduction to Zcash

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] It 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

[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.

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.

Zcash seeks to become the model digital currency of choice for privacy and digital information security and has established itself to be one of the top 35 largest networks by market cap in the ecosystem.

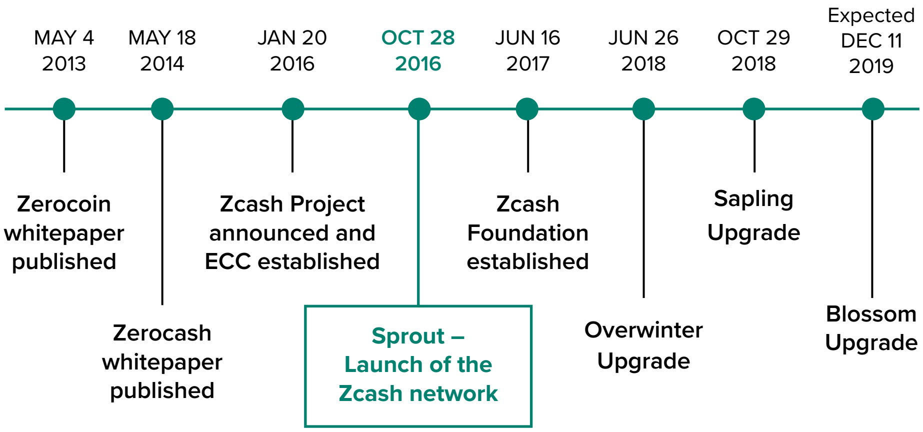
FIGURE 1: **ZCASH SUMMARY STATISTICS**[6]
As of October 15, 2019

Asset	Zcash (ZEC)
Inception of Network	October 28, 2016
Price (USD)	$37.02
Market Cap (USD)	$282.7 million
Circulating Supply (ZEC / % of Max Supply)	7.64 million / 36.4%
Max Supply (ZEC)	21 million
Current Mining Block Reward (ZEC)	12.5
Next Block Reward Halving Date (Expected)	October 2020
Average Block Time	Approximately 2.5 minutes
Market Segment	Digital Currency 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] Coin Metrics, CoinMarketCap.com, Messari / OnChainFX. As of October 15, 2019.

A Brief History of Zcash

FIGURE 2: **TIMELINE OF ZCASH NETWORK**


MAY 4 2013
MAY 18 2014
JAN 20 2016
OCT 28 2016
JUN 16 2017
JUN 26 2018
OCT 29 2018
Expected DEC 11 2019
Zerocoin whitepaper published
Zerocash whitepaper published
Zcash Project announced and ECC established
Sprout – Launch of the Zcash network
Zcash Foundation established
Overwinter Upgrade
Sapling Upgrade
Blossom Upgrade

In an era where information is increasingly digitized and data leaks revealing personal information are frequent, privacy and security are 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.[7]

Zerocoin laid the groundwork for **Zerocash**, for which the May 2014 whitepaper served as an outline for **Zcash**.[8] **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 approximately 98%.[9] 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.

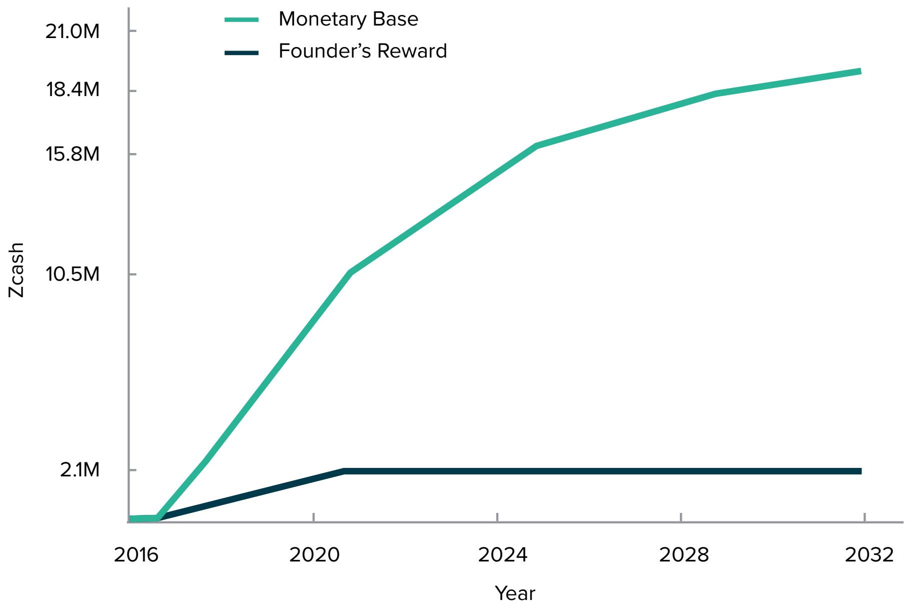
[7] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. "Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version)."*The Zerocash Project*. May 18, 2014. http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf.
[8] Zooko Wilcox. "Hello, World!" *Electric Coin Company*. January 20, 2016. https://electriccoin.co/blog/helloworld/.
[9] See footnote 7.

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 oversees technical development of the network to this day. 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 comprised of the ECC, as well as founders, employees, advisors and investors of the ECC and the Zcash Foundation).[10] The monetary supply schedule for Zcash, including the Founders' Reward, is shown in Figure 3 below.

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



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 budget and expenses online and most recently, in the *Q3 2019 Transparency Report*. Shortly after 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.

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

Network Upgrades

Since the original Zcash protocol, Sprout, was released, Zcash has undergone two network upgrades: Overwinter and Sapling. 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.[11]

- **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 - Expected December 11, 2019**
  - Planned increase in mining frequency of blocks, allowing faster transactions with low fees

Defining Characteristics of Zcash

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-enhanced 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.

[11] Josh Swihart. "Zcash to 10 billion." *The Electric Coin Company. July 23, 2019. Updated: September 9, 2019.* https://electriccoin.co/blog/zcash-to-10-billion/`

Privacy Technology (zk-SNARKS)

Created by the SCIPR[12] 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 between the prover and verifier.[13] They add additional layers of confidentiality to transactions by concealing the amount, and sender and receiver of ZEC transactions, and 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 ASIC-resistant, as GPUs (Graphical Processing Units) are currently the preferred choice of equipment as they are relatively cheaper. 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 tradeoff for adopting Equihash is that computations are more memory intensive and are restricted to the memory capacity of the hardware.[14]

For more on the technicalities on 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 block rewards for their effort, providing an incentive and attributing to the exponential increase in network usage. For the first 850,000 blocks, or approximately four years, the block reward is 12.5 ZEC. As illustrated in Figure 4, miners receive 80%, equivalent to 10 ZEC per block, 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%, equivalent to 2.5 ZEC. The Founders' Reward was designed to incentivize those partaking in the development of the network. 14

[12] SCIPR is an acronym for Succinct Computational Integrity and Privacy Research.
[13] 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
[14] https://www.openwall.com/articles/Zcash-Equihash-Analysis

After four years, block rewards will halve every 840,000 blocks and 100% of the block rewards will go to the miners. As a result, miners will receive 90% in the final distribution of the ZEC supply, as described in Figure 5.

FIGURE 4: **ZEC INITIAL MINING AND FOUNDERS' REWARDS DISTRIBUTION**[15]

October 28, 2016 to October 2020 (Expected)

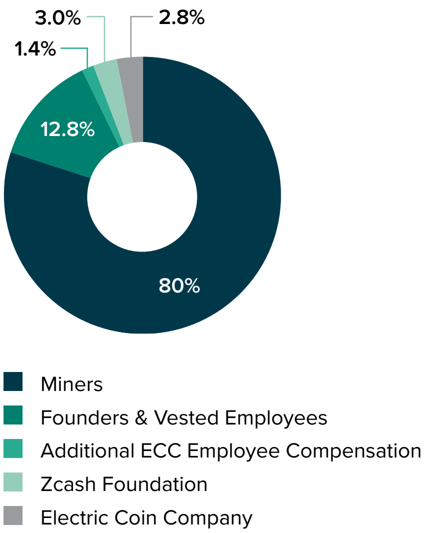
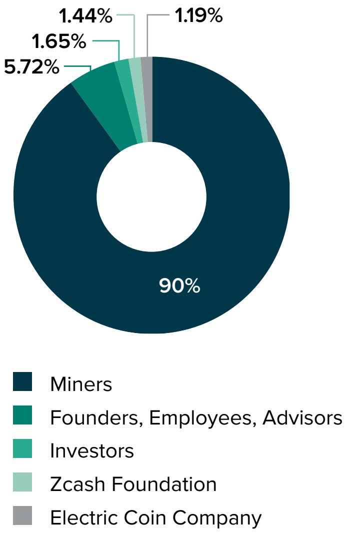


FIGURE 5: **ZEC TOTAL SUPPLY ALLOCATION**[16]

Decided at Inception



Block rewards are set to halve for the first time to 6.25 ZEC in October 2020. 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*.

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, in which the nodes hold equal power in the network and must collaborate to validate transactions.[17]

  One caveat is that while governance is decentralized, there may be risks associated with the level of decentralization of mining pools in

[15] "Electric Coin Company Q2 2019 Transparency Report." *Electric Coin Company. May 14, 2019*. https://electriccoin.co/blog/electric-coin-company-q2-2019-transparency-report/.
[16] See previous footnote.
[17] Vitalin Buterik. "The Meaning of Decentralization." February 6, 2017. *Medium*. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

the Zcash network. As of October 15, 2019, the top three largest mining pools controlled over 60% of the hashrate of the network.[18]

- **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."[19] An attacker seeking to make a fraudulent transaction on the blockchain 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, in what is called a 51% attack. The primary deterrent of these attacks is that they are computationally expensive with uncertain payoff, and as a result, are unlikely.[20]

  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.[21]

- **Open-source**: The source code for the Zcash Project is viewable on the Internet, free for anyone to access, contribute to, or fork.[22] 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.

- **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.

[18] "Zcash Mining Pools (ZEC) Equihash." *Miningpoolstats.io*. https://miningpoolstats.stream/zcash.
[19] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System." *Bitcoin Project*. October 31, 2008. https://bitcoin.org/bitcoin.pdf.
[20] 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.
[21] 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/.
[22] 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.

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.

1. **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.

2. **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.[23] Community proposals for a continued development funding mechanism have been published and are detailed on the ECC blog, here.[24]

3. **Block size limit:** Zcash has a block size limit of 2MB, compared to Bitcoin's block size limit of 1MB.

4. **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.

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, but also perhaps the public internet and other digital networks, without requiring trust in known individuals or entities in the setup process.[25]

[23] 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.
[24] "An Update from ECC on the Initial Assessment of Community Proposals." *The Electric Coin Company. September 20, 2019.* https://electriccoin.co/blog/an-update-from-ecc-on-the-initial-assessment-of-community-proposals/.
[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/

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]

Potential Advantages of Zcash Compared to Bitcoin

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

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

2. **Faster transaction speeds:** Zcash transactions can be completed four times faster than Bitcoin since Zcash blocks are generated at a rate of 2.5 minutes, as opposed to 10 minutes for Bitcoin.[28] Additionally, if transaction volume increases on the Zcash network, blocks have the capacity to process more transactions, given the 2MB block size limit.[29]

3. **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 $0.01, compared to $0.63 for Bitcoin.[30]

4. **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.

[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.
[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 October 15, 2019.
[29] Bitinfocharts. https://bitinfocharts.com/comparison/confirmationtime-btc-zec.html. As of October 15, 2019.
[30] Bitinfocharts. https://bitinfocharts.com/comparison/transactionfees-btc-zec.html. As of October 15, 2019.

Potential Disadvantages of Zcash Compared to Bitcoin

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 disadvantages of Zcash compared to Bitcoin:

Level of Decentralization

There may be risks associated with the level of decentralization of mining pools in the Zcash network. As of October 15, 2019, 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 380 contributors to the "zcashd" codebase.[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 October 15, 2019 the total number of addresses on the Zcash network maintaining a balance greater than zero was approximately 557 thousand versus 27.5 million on the Bitcoin network.[33] 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 frontend payment processing-software.

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 implementation of cryptography is new and could ultimately fail, resulting in little to no privacy than initially publicized. This could adversely affect one's 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 October 21, 2019), https://github.com/zcash/zcash/graphs/contributors
[33] Coin Metrics. As of October 15, 2019.
[34] See footnote 21.

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 recommendations from 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.

Conclusion

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.

To learn more about other digital assets underpinning the Grayscale family of products, please visit the Building Blocks section of Grayscale Insights.

[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/.

About Grayscale Investments, LLC

Grayscale Investments is the world's largest digital currency asset manager. With a proven track record and unrivaled experience, we give investors the tools to make informed investing decisions in a burgeoning asset class. As part of Digital Currency Group, Grayscale accesses the world's biggest network of industry intelligence to build better investment products. We have removed the barrier to entry so that institutions and individual investors can benefit from exposure to digital currencies. Now, forward-thinking investors can embrace a digital future with an institutional grade investment.

Grayscale is headquartered in New York City. For more information on Grayscale, please visit www.grayscale.co or follow us on Twitter @GrayscaleInvest.

Important Disclosures & Other Information

©Grayscale Investments, LLC. 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 paper is for informational purposes only and 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 paper to make an investment decision and any information contained herein should not be used as a basis for this purpose. This paper does not constitute a recommendation or take into account the particular investment objectives, financial situations, or needs of investors. Investors are not to construe the contents of this paper 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 research 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.

Investors should be aware that Grayscale is the sponsor of Grayscale Bitcoin Trust (BTC), Grayscale Bitcoin Cash Trust (BCH), Grayscale Ethereum Trust (ETH), Grayscale Ethereum Classic Trust (ETC), Grayscale Litecoin Trust (LTC), Grayscale Horizen Trust (ZEN), Grayscale Stellar Lumens Trust (XLM), Grayscale XRP Trust (XRP) and Grayscale Zcash Trust (ZEC) (each, a "Trust") and the manager of Grayscale Digital Large Cap Fund LLC (the "Fund"). The Trusts and the Fund are collectively referred to herein as the "Products". Any Product currently offering Share creations is referred to herein as an "Offered Product". Information provided about an Offered Product is not intended to be, nor should it be construed or used as investment, tax or legal advice, and prospective investors should consult their own advisors concerning an investment in such Offered Product. This paper does not constitute an offer to sell or the solicitation of an offer to buy interests in any of the Products. Any offer or solicitation of an investment in a Product may be made only by delivery of such Product's confidential offering documents (the "Offering Documents") to qualified accredited investors (as defined under Rule 501(a) of Regulation D of the U.S. Securities Act of 1933, as amended), which contain material information not contained herein and which supersede the information provided herein in its entirety.

The Products are private investment vehicles. Shares of Grayscale Bitcoin Trust (BTC), which are only offered on a periodic basis, are publicly quoted under the symbol: GBTC. The Products are not subject to the same regulatory requirements as exchange traded funds or mutual funds, including the requirement to provide certain periodic and standardized pricing and valuation information to investors. The Products are not registered with the Securities and Exchange Commission (the "SEC"), any state securities laws, or the U.S. Investment Company Act of 1940, as amended. There are substantial risks in investing in one or more Products. Any interests in each Product described herein have not been recommended by any U.S. federal or state, or non-U.S., securities commission or regulatory authority, including the SEC. Furthermore, the foregoing authorities have not confirmed the accuracy or determined the adequacy of this document. Any representation to the contrary is a criminal offense.

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.

Certain Risk Factors

Each Product is a private, unregistered investment vehicle and not subject to the same regulatory requirements as exchange traded funds or mutual funds, including the requirement to provide certain periodic and standardized pricing and valuation information to investors. There are substantial risks in investing in a Product or in digital assets directly, including but not limited to:

- **PRICE VOLATILITY**
  Digital assets have historically experienced significant intraday and long-term price swings. In addition, none of the Products currently operates a redemption program and may halt creations from time to time or, in the case of Grayscale Bitcoin Trust (BTC), periodically. There can be no assurance that the value of the common units of fractional undivided beneficial interest ("Shares") of any Product will approximate the value of the digital assets held by such Product and such Shares may trade at a substantial premium over or discount to the value of the digital assets held by such Product. At this time, none of the Products is operating a redemption program and therefore Shares are not redeemable by any Product. Subject to receipt of regulatory approval from the SEC and approval by Grayscale, in its sole discretion, any Product may in the future operate a redemption program. Because none of the Products believes that the SEC would, at this time, entertain an application for the waiver of rules needed in order to operate an ongoing redemption program, none of the Products currently has any intention of seeking regulatory approval from the SEC to operate an ongoing redemption program.

- **MARKET ADOPTION**
  It is possible that digital assets generally or any digital asset in particular will never be broadly adopted by either the retail or commercial marketplace, in which case, one or more digital assets may lose most, if not all, of its value.

- **GOVERNMENT REGULATION**
  The regulatory framework of digital assets remains unclear and application of existing regulations and/or future restrictions by federal and state authorities may have a significant impact on the value of digital assets.

- **SECURITY**
  While each Product has implemented security measures for the safe storage of its digital assets, there have been significant incidents of digital asset theft and digital assets remains a potential target for hackers. Digital assets that are lost or stolen cannot be replaced, as transactions are irrevocable.

- **TAX TREATMENT OF VIRTUAL CURRENCY**
  For U.S. federal income tax purposes, Digital Large Cap Fund will be a passive foreign investment company (a "PFIC") and, in certain circumstances, may be a controlled foreign corporation (a "CFC"). Digital Large Cap Fund will make available a PFIC Annual Information Statement that will include information required to permit each eligible shareholder to make a "qualified electing fund" election (a "QEF Election") with respect to Digital Large Cap Fund. Each of the other Products intends to take the position that it is a grantor trust for U.S. federal income tax purposes. Assuming that a Product is properly treated as a grantor trust, Shareholders of that Product generally will be treated as if they directly owned their respective pro rata shares of the underlying assets held in the Product, directly received their respective pro rata shares of the Product's income and directly incurred their respective pro rata shares of the Product 's expenses. Most state and local tax authorities follow U.S. income tax rules in this regard. Prospective investors should discuss the tax consequences of an investment in a Product with their tax advisors.

- **NO SHAREHOLDER CONTROL**
  Grayscale, as sponsor of each Trust and the manager of the Fund, has total authority over the Trusts and the Fund and shareholders' rights are extremely limited.

- **LACK OF LIQUIDITY AND TRANSFER RESTRICTIONS**
  An investment in a Product will be illiquid and there will be significant restrictions on transferring interests in such Product. The Products are not registered with the SEC, any state securities laws, or the U.S. Investment Company Act of 1940, as amended, and the Shares of each Product are being offered in a private placement pursuant to Rule 506(c)

under Regulation D of the Securities Act of 1933, as amended (the "Securities Act"). As a result, the Shares of each Product are restricted Shares and are subject to a one-year holding period in accordance with Rule 144 under the Securities Act. In addition, none of the Products currently operates a redemption program. Because of the one-year holding period and the lack of an ongoing redemption program, Shares should not be purchased by any investor who is not willing and able to bear the risk of investment and lack of liquidity for at least one year. No assurances are given that after the one year holding period, there will be any market for the resale of Shares of any Product, or, if there is such a market, as to the price at such Shares may be sold into such a market.

- **POTENTIAL RELIANCE ON THIRD-PARTY MANAGEMENT; CONFLICTS OF INTEREST**
  The Products and their sponsors or managers and advisors may rely on the trading expertise and experience of third-party sponsors, managers or advisors, the identity of which may not be fully disclosed to investors. The Products and their sponsors or managers and advisors and agents may be subject to various conflicts of interest.

- **FEES AND EXPENSES**
  Each Product's fees and expenses (which may be substantial regardless of any returns on investment) will offset each Product's trading profits.

Additional General Disclosures

Investors must have the financial ability, sophistication/experience and willingness to bear the risks of an investment. This document is intended for those with an in-depth understanding of the high risk nature of investments in digital assets and these investments may not be suitable for you. This document may not be distributed in either excerpts or in its entirety beyond its intended audience and the Products and Grayscale will not be held responsible if this document is used or is distributed beyond its initial recipient or if it is used for any unintended purpose.

The Products and Grayscale do not: make recommendations to purchase or sell specific securities; provide investment advisory services; or conduct a general retail business. None of the Products or Grayscale, its affiliates, nor any of its directors, officers, employees or agents shall have any liability, howsoever arising, for any error or incompleteness of fact or opinion in it or lack of care in its preparation or publication, provided that this shall not exclude liability to the extent that this is impermissible under applicable securities laws.

The logos, graphics, icons, trademarks, service marks and headers for each Product and Grayscale appearing herein are service marks, trademarks (whether registered or not) and/or trade dress of Grayscale Investments, LLC. (the "Marks"). All other trademarks, company names, logos, service marks and/or trade dress mentioned, displayed, cited or otherwise indicated herein ("Third Party Marks") are the sole property of their respective owners. The Marks or the Third Party Marks may not be copied, downloaded, displayed, used as metatags, misused, or otherwise exploited in any manner without the prior express written permission of the relevant Product and Grayscale or the owner of such Third Party Mark.

The above summary is not a complete list of the risks and other important disclosures involved in investing in any Product or digital assets and is subject to the more complete disclosures contained in each Product's Offering Documents, which must be reviewed carefully.

GRAYSCALE

General Inquiries:

info@grayscale.co
Address: 250 Park Ave S 5th floor, New York, NY 10003
Phone: (212) 668-1427
@GrayscaleInvest