Welcome [edit]

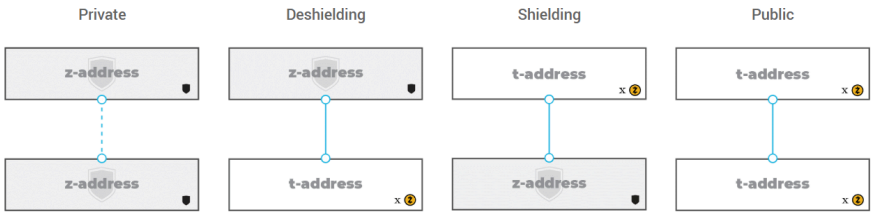
Hi, welcome to wikipedia. We have very strict policies related to cryptocurrency. We are only allowing mainstream sources for cryptocurrency articles, such as NYT, WSJ, etc. Coindesk, zcash blogs, etc are all not ok. Thanks! Jtbobwaysf (talk) 19:04, 4 May 2020 (UTC)

- Zcash Generates Price Frenzy, New York Times, 2016
- Known Unknown, The Economist, 2016
- A blockchain that beats bitcoin on privacy, IEEE Spectrum, 2016
- Bitcoin isn't anonymous enough, Bloomberg, 2016
- Zcash, Blockstack, Oh My!, Techcrunch, 2016
- New Bitcoin Rival, Fastcompany, 2016
- Zcash Launches in Alpha, Wired, 2016
- JP Morgan integrates Zcash tech, Forbes, 2017
- Could this man build a better bitcoin, Fortune, 2017
- Winklevoss add Zcash to Gemini, Forbes 2018
- Zcash creators invest in Bolt, Forbes, 2019
- Zcash bug could have allowed for infinite counterfeiting, Fortune, 2019
- Privacy is key to adoption, Forbes 2019
- Bring Zcash To Law-Abiding Masses, Forbes, 2020
- RadioLab, The Ceremony, 2017

Zcash

Zcash is a cryptocurrency that uses advanced applied cryptography to provide enhanced privacy for its users compared to other cryptocurrencies such as Bitcoin. Zcash is the first practical application of zk-SNARKs, a specific type of zero-knowledge proof.

Like Bitcoin, Zcash has a fixed total supply of 21 million units.[5] Unlike Bitcoin, Zcash offers two types of addresses: private (z-addresses) or transparent (t-addresses). [Zcash Technology] These two address types allow for four different transaction types that offer varying levels of privacy protection. Today, most wallets and exchanges exclusively support t-addresses, although support for shielded addresses is available for mobile and desktop wallets. [z.cash/wallets]



History

- Pre-launch
  - Zcash grew out of “Zerocash/Zerocoin,” an experimental proposal from seven scientists to improve privacy protections in Bitcoin.[1] The Zerocoin company, known today as the Electric Coin Co., raised $3M in funding to develop the initial protocol. [Messari profile]
- Creation
  - Zcash launched on October 28, 2016 by Electric Coin Co., a private company founded by Zooko Wilcox.[2] Zcash relies on a novel mathematical proof called a [[zk-SNARK]]. “SNARKs are the engine that can quickly and efficiently verify a transaction and add it to the blockchain without revealing any details to the public.”[3] SNARKs require a set of public parameters which allow users to construct and verify private transactions. These parameters are set up in an elaborate secure multi-party computation; for Zcash, this is known as the Trusted Setup. [Spectrum article] [Radiolab episode]
- 2016 - 2018
  - After the Zcash launch, the Zcash engineering team released a series of upgrades known as the “Sprout series.”[4] The team also put forward plans for two core protocol upgrades known as Overwinter and Sapling. The Sapling upgrade

[1] ZeroCoin
[2] Grayscale
[3] https://minezcash.com/zcash-trusted-setup/
[4] https://electriccoin.co/blog/the-near-future-of-zcash/

made efficiency improvements and enabled new kinds of core protocol features. The Zcash Foundation was formed in March 2017 with an initial endowment of 273,000 ZEC, taken from the Founder's Reward. [IBTimes article] The Zcash Foundation organized the Powers of Tau ceremony, which was at the time the largest multi-party computation ceremony ever performed. [ZF blog post] [need secondary source] In 2017, enterprise partnerships like the Zcash collaboration with JP Morgan [Coindesk article] further fueled a wider interest in blockchains and zk-SNARKs.[5]
    - The Sapling upgrade activated October 29, 2018, almost two years to the date from the initial Zcash launch.

- 2019-2020
    - In early 2019, the Zcash Company rebranded to the Electric Coin Co.[6] to differentiate from Zcash the protocol and the Zcash Foundation. The Zcash community began a several-month-long governance discussion regarding the continuation of the Founder's Reward and the Zcash trademark.
    - In February 2019 it was revealed that a serious cryptographic flaw had affected the zk-SNARK proving system, called BCTV14, that was used by Zcash before the Sapling upgrade. This flaw could have allowed counterfeiting. [Fortune article] [Coindesk article] [ZDNet article] The Electric Coin Co. stated in a blog post that they "believe that no one else was aware of the vulnerability and that no counterfeiting occurred in Zcash". [ECC blog post]
    - Electric Coin Co. announced a research project to increase the scalability of Zcash by 2021. [blog post] One of the results of this research is the Halo proving system. [Coindesk article]
    - Blossom, the third network upgrade for Zcash, activated in December 2019. This upgrade halved the target block interval, to 75 seconds. [BitcoinInsider article]
    - Funding discussions culminated in early 2020 with community consensus around ZIP 1014, a Zcash Improvement proposal that describes a structure for a newly established Zcash Development Fund. [BTCManager article] [Coindesk article] [maybe include a more critical article questioning the degree of consensus, e.g. [this one]]
    - Heartwood, the fourth network upgrade is scheduled to activate in July 2020.

Design

- Units and divisibility
    - The unit of account of the Zcash system is a ZEC. The ticker symbol used to represent Zcash is also "ZEC". As a nod to Bitcoin's creator, a zatoshi is the smallest amount within Zcash representing 0.00000001 ZEC, one hundred millionth of a ZEC.
- Funding Structure
    - Zcash pays out a portion of each block reward to fund protocol development and (for the first year) to pay back investors. During the first four years of Zcash, 10% of the block reward was transferred to the Founders Reward fund and distributed

[5] https://electriccoin.co/blog/zcash-in-2017/
[6] https://electriccoin.co/blog/goodbye-zcash-company-hello-electric-coin-company/

to the Electric Coin Co., Zcash Foundation and initial investors. After network upgrade 4, 8% of the block reward will be transferred to the Dev Fund and managed by a Major Grants Review Committee.

- Governance
  - Zcash is recognized for having a robust decentralized governance system as evidenced by the “Dev Fund” discussions. [Messari, Coindesk] [need to include opposing view]
- Transactions Types / Transaction fees
  - The two Zcash address types, public t-addresses and private z-addresses are interoperable. Z-addresses start with a “z,” and t-addresses start with a "t.” Private addresses are also referred to as shielded addresses. Funds can be transferred between z-addresses and t-addresses. However, it is important that users understand the privacy implications of shielding or de-shielding information through these transactions. More information on the various transaction types is available.
  - Transactions between two transparent addresses (t-addresses) work just like Bitcoin: the sender, receiver and transaction value are publicly visible. Transactions involving shielded addresses are (z-to-z, z-to-t or t-to-z) offer varying levels of privacy protection. A z-to-z transaction appears on the public blockchain, so it is known to have occured and that the fees were paid. But the addresses, transaction amount and the memo field are all encrypted and not publicly visible.
- Viewing Keys
  - The owner of an address may choose to disclose z-address and transaction details with trusted third parties — think auditory and compliance needs — through the use of view keys and payment disclosure.
  - Zcash affords private transactors the option of "selective disclosure", allowing a user to prove payment for auditing purposes. One such reason is to allow private transactors the choice to comply with anti-money laundering or tax regulations. "Transactions are auditable but disclosure is under the participant's control."[8] The company has hosted virtual meetings with law enforcement agencies around the U.S. to explain these fundamentals and has gone on the record of saying that "they did not develop the currency to facilitate illegal activity".[5
  - Need to add more info on current plan for viewing keys
- Mining
  - Originally Zcash could be mined at home, using CPU or GPU machines. As mining hardware evolved, ASIC machines became the preferred mining machine for professional cryptocurrency miners and mining pools.[7] ASICs can be customized for a particular use (such as mining Zcash) and therefore outperformed previous mining hardware such as CPUs and GPUs. Zcash community members voted against ASIC-resistant protocol updates in mid-2018 citing security concerns. [Coindesk] The top mining pools for Zcash include Flypool, Nanopool and Slushpool.[8]
  - The next network upgrade, Heartwood includes ZIP 213, which would allow

[7] https://en.bitcoin.it/wiki/ASIC
[8] https://coinswitch.co/news/top-5-best-zcash-mining-pool-options-in-2020

miners to mine directly to a shielded coinbase. [Messari article] [Crypto-News-Flash article]

- Shielded transactions
  - Zcash coins are either in a transparent pool or a shielded pool; as of December 2017 only around 4% of Zcash coins were in the shielded pool and at that time most wallet programs did not support z-addrs and no web-based wallets supported them.[6] The shielded pool of zCash coins were further analyzed for security and it was found that the anonymity set can be shrunk considerably by heuristics based on identifiable patterns of usage.[7]
  - Need to add more info on current stats for shielded
- Scalability
  - Scaling is a central discussion for blockchain projects[9]. There are several approaches to making blockchains scalable, both at the protocol layer (layer 1) and at the application layer (layer 2). In September 2019, Sean Bowe, researcher at Electric Coin Co., proposed Halo[10,11], a novel technique for practical recursive zero-knowledge proofs. ECC researcher Daira Hopwood presented a research proposal for sharding architecture. This proposal calls for the use of sharding, a technique that partitions a database into sections or "shards" to improve the throughput limit, in order to scale to high transaction volumes.

Ecosystem

- Zcash is available on top global exchanges and is supported by 7 out of 10 of the Bitwise Real 10, which measures cryptocurrency exchanges by real (vs. faked) transaction volume. At the time of this writing (May 2020), Zcash is ranked 10th for adjusted 24 hour transaction volume, a measurement of on-chain economic activity.
- Zcash is supported at top cryptocurrency payment providers including Flexa and Gemini Pay.
- Zcash can be used at over 39,000 major retail locations, coffee shops, movie theaters and more. For a community-curated directory of merchants, visit paywithzcash.com.
- Regulation
- There has been an increase in novel applications of Zcash that utilize the encrypted memo field of shielded transactions. The memo field lets a Zcash user sign and encrypt messages that are appended to the blockchain. ZECpages is an anonymous messaging board and directory. Since inception, 137 people have shared nearly 200 unique messages on the platform. Zbay is a peer-to-peer marketplace that uses Zcash shielded transactions and encrypted memos to communicate and transact.

Criticism

- Inflation: Several opinion articles point out that Zcash has an 'rampant inflation' issue, or link its inflation rate to alleged price performance problems.
- Trusted Setup

[9] https://cointelegraph.com/explained/vertical-and-horizontal-blockchain-scaling-explained
[10] https://www.coindesk.com/zcashs-halo-breakthrough-is-a-big-deal-not-just-for-cryptocurrencies
[11] https://decrypt.co/9107/cryptographic-breakthrough-could-solve-zcash

Zcash's Zero knowledge proofs "rely on a set of public parameters which allow users to construct and verify private transactions". The construction of such parameters requires a "ceremony" involving multiple parties sampling random numbers. The output of each party sampling process is often referred to as "Toxic Waste". This is named after the fact that the sub product of the parameter generation can be used to breach the cryptography and Zcash's integrity. Although the details of the Zcash Ceremony were detailed publicly and chronicled by scientific reporters, the sole existence of such 'waste' is a source of criticism to Zcash and related privacy coins.

In popular culture

In an episode titled, "The Ceremony," the Radiolab podcast covered Zcash's trusted setup ceremony with a detailed recap of how the elaborate process unfolded.

An episode in season 2 of the Netflix show, [[Altered Carbon (TV Series)|Altered Carbon]], set 400 years in the future, shows a shop with prices listed in a variety of cryptocurrencies, including Zcash. [NewsBTC article] [Bitcoin.com article]

See also[edit]

- Legality of bitcoin by country
- Zerocoin protocol
- zk-SNARKs

External links[edit]

- Official website
- Electric Coin Co
- Zcash Foundation