Zcoin

Privacy focused payments

MESSARI

Analyst: Jordan Levine

Updated: April 18, 2018

Zcoin is a privacy-focused currency token that launched in Sept. 2016 based off ideas proposed from the Zerocoin Project.

Zcoin focuses on using existing encryption and zero-knowledge proof technology from RSA. The team believes that by using these well defined cryptographic technologies they can create a secure network that removes the need for human involvement in the setup process. Zcoin operates a multi-node model where mining nodes verify blockchain transactions and Znodes store blockchain data.

Project Overview

Name	Zcoin
Issuer	Zcoin Project
Category	Currency token
Sector	Privacy
Sale Start	N/A
Sale End	N/A

Token Overview

Name	Zcoin
Symbol	XZC
Type	Native
Initial Distribution	N/A
Current Supply	4,400,000
Max Supply	21,400,000
Emission Type	Ongoing decaying

Resource Links

- Website
- GitHub
- Twitter
- Telegram
- Reddit
- Blog
- Whitepaper

Project Background

Zcoin is a privacy-focused cryptocurrency project that was the first to implement ideas from the Zerocoin project whitepaper written by a group of academics in 2013. By using RSA encryption and zero-knowledge proofs, the project aims to allow users to remain anonymous when sending or receiving payments. Zerocoin was proposed as a way to avoid the pseudonymity in Bitcoin that allows transactions to be traced to a specific user and creates the potential for specific coins to become tied to illicit activity.

The project competes directly with Zcash, which is based off a follow-up whitepaper from the same group that proposed Zerocoin. Though they both use zero-knowledge proofs, Zcoin believes that by using well-known RSA technology they can provide more security than the newer zK-SNARKs cryptography used in Zcash and create a more simple setup process compared to Zcash, which requires multiple human participants to generate pieces of the initial network keys from different geographic locations.

Zcoin is a rebranding of the earlier Moneta project, which was created from a fork of Litecoin. Founders Poramin Insom and Gary Le launched Zcoin with backing from private investors including Roger Ver, Tim Lee, and Startup Chile, an accelerator run by the Chilean government. Le also helped fund the project with a grant he received through a Thiel Fellowship. [1,2]

[1] Source: https://news.bitcoin.com/zero-knowledge-zcoin-launching-soon/
[2] Source: https://zcoin.io/a-message-from-our-new-investor-in-zcoin-tim-lee/

Technology

Zcoin is based on a fork of the Bitcoin Core codebase and uses Lyra2z as its mining proof-of-work algorithm making it mineable by GPUs and to a lesser extent, CPUs. The team plans to release a new mining algorithm based on merkle tree proof of work (MTP) in the second quarter of 2018, after delaying this integration in 2017. MTP integration aims to create an efficient and decentralized CPU mining network. New blocks are created every ten minutes and the difficulty is adjusted every six blocks.

In Dec. 2017 Zcoin initiated a hard-fork to allow for the addition of new non-mining nodes known as Znodes. These nodes are responsible for storing blockchain data which is necessary in the Zcoin network due to the relatively large amount of computational resources and storage needed to facilitate the cryptographic verification process. Nodes are required to stake 1,000 Zcoin (XZC) tokens as collateral and receive a portion of mining fees for their services.

In an effort to ensure fair distribution of rewards nodes are shuffled in rank based on when they last received a block reward, with the most recent recipient moving to the bottom of the list. The next node to receive a reward is selected randomly from the top 10% of the list. Nodes must meet certain activity requirements based on the overall size of the network and the confirmations on the collateral transaction. There are currently more than 2,900 active Znodes in the network.[3]

Zcoin's privacy is particularly focused on dissolving the ability to associate certain coins with distinct addresses from the past, thus eliminating traceable coin histories within the network. Using zero-knowledge proofs, users prove that they burned a specified amount of XZC without divulging which particular token within the network was destroyed. Upon XZC burn, a "Zerocoin" is minted by the user, which has no transactional history. When a coin is spent it appears the same as any new coin that had entered the network through a block reward.

Unlike other privacy focused cryptoassets, Zcoin has an auditable supply, due to the fact that the amount of coins originally burnt are not hidden. While this can add transparency by allowing others to check that users are using a legitimate process to create new coins, it creates the ability for third-parties to see addresses for large holders on the network.

Distribution

Zcoin started as a privately funded project and continues to receive funding through a "founders reward" that is distributed in every new block. This is used to continue the development of the platform and compensate early investors. After a four year period the founders reward is removed and all new tokens are allocated to miners and Znode operators.

New supply of tokens are created in every new block as a block reward. A total of 50 XZC are created in every block with 28 tokens allocated to miners, 15 to Znode operators, and 7 to the founders reward.[4] Zcoin follows the same halving schedule as Bitcoin, where block rewards are reduced by one half every four years.

[3] Source: https://zednode.com/znode-stats
[4] Source: https://zcoin.io/faq/

Team

Poramin Insom
Founder and core developer

- Masters in information security from Johns Hopkins University
- Previous experience creating cryptocurrencies

Peter Shugalev
Lead core developer

- Graduated magna cum laude with a masters in computer science and mathematics from Mos
- Previous experience creating network and security related services.

Reuben Yap
Chief operations officer

- Received an LLB from the University of Nottingham
- Spent ten years a corporate lawyer

Advisors

Alexander N.
Full-stack and cryptocurrency developer

Torphop Korgtadam
Co-founder of Creden and MHCON

Investors

Roger Ver

Tim Lee

Startup Chile

Additional Resources

- Zcoin Roadmap
- Zcoin Block Explorer
- Zcoin FAQs