Zcash ($ZEC) Investment Memo

By Jacob Koch-Gallup — August 26th, 2022

Overview

Zcash is a bitcoin-forked L1 that uses advanced cryptography and zero-knowledge proofs, specifically zk-SNARKs, to provide enhanced privacy. Zcash allows for fully shielded transactions that encrypt information about the sender, recipient, and amount.

In 2013, several scientists from John Hopkins University designed the protocol that would later become Zcash. Zcash was officially created in 2016 by Zooko Wilcox-O'Hearn, a security specialist and core contributor to the first cryptocurrency DigiCash in 1996. The current team consists of 29 employees at Electric Coin Co. (founding company of Zcash) and 13 employees at the Zcash Foundation.

Thesis

Zcash uses unmatched privacy measures to fully shield crypto transactions. As crypto further becomes a mainstream payment system, an increasing number of users will want to have their transactions private. This becomes especially apparent when considering the future mass adoption of blockchain gaming & metaverses. Most gamers will not want to publicly display their wallet holdings in-game, so a privacy aspect will be required.

Given Zcash's current FDV of $1.36B and potential to 3.4x-10x, *Zcash is a viable investment.* Similar to $BTC, $ZEC accrues value with increased demand due to its capped supply of 21 million tokens. Zcash will continue to be a leader in the privacy coin space and as crypto and blockchain gaming becomes mainstream, Zcash will become increasingly more valuable.

Market Size

The overall privacy coin market cap (opcmcap) is currently around $6B. Compared to the total crypto market cap of $1T, privacy coins make up .60%. If we assume similar growth from the last bull cycle to the next bull cycle (total crypto mcap ~$290B to $2.9B — 10x), then Zcash has the potential to reach an addressable market cap of $60B. If we assume that privacy coins become the narrative again in the upcoming bull cycle, then the addressable market cap could exponentially increase as privacy coins gain total crypto market share.

Compounding

Currently, Zcash has a $1B mcap, an FDV of $1.4B, and at its peak, an FDV of $4.77B. $ZEC is down 70.5% from ATHs and has the potential to 3.4x in value if it were to reach ATHs again. If Zcash maintains its current market share of ~16.4% of the opcmcap and the opcmcap increases to $60B, then Zcash could potentially see a mcap of $9.8B or 10x current value.

Risks

Regulation: The recent sanctions against Tornado Cash highlight the regulatory limbo that Zcash and other privacy coins are in. While Tornado Cash sanctions are concerning for the future of Zcash, it highlights its usefulness; the U.S. government would not sanction Tornado Cash or privacy coins if they weren't integral.

Competition: ZCash's top competitors are Monero, Oasis Network, and Secret. While Monero has a larger mcap than Zcash, it is not as secure. Monero uses Bulletproofs to hide the transaction amount but not the transaction graph. Advanced forensics and analytics companies claim to be able to trace these types of transactions. Zcash's use of Groth 16 proofs, R1CS circuits, and UltraPLONK-style circuits hides both the transaction amount and the transaction graph.