ZCash (ZEC) Alt Coin

By Emmett Steven
Motivation

ZCash (ZEC) is an alt coin with the primary motive of allowing for completely anonymous transactions and protecting user privacy as much as possible using advanced cryptographic mechanisms.
Transaction Types

ZCash allows for several different transaction types, each for exchanges between its two different address types, private and public (or z-addresses and t-addresses).
Transactions contd.

Z-Z transactions appear on the blockchain just as a normal transaction would, so that it is known to have occurred and to verify that all associated fees have been paid. But the addresses, transaction amount, and memo field are all hidden and protected through encryption. This encryption can only be accomplished through the use of zero-knowledge proofs and ZCash’s zk-SNARK technology.
zk-SNARKs

Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) refers to a proof construction 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. A zero knowledge proof must satisfy the following three conditions in order to be valid:

- Completeness: If the statement is true then an honest verifier can be convinced of it by an honest prover.
- Soundness: If the prover is dishonest, they can’t convince the verifier of the soundness of the statement by lying.
- Zero-Knowledge: If the statement is true, the verifier will have no idea what the statement actually is.
Transaction Information Disclosure

Another central feature to ZCash is the ability for users to selectively disclose information regarding a specific transaction with trusted third parties for any auditory or compliance needs they may encounter.
Additional Features

ZCash also provides the following additional features with its currency:

- Encrypted memo field, allowing for messages to be attached to transactions with the same protection as personal addresses.
- Interoperable address types, allowing users with both private and transparent addresses to complete transactions with each other.
- Transaction expiration, in order to minimize the impact of unmined transactions, a transaction will expire and funds unencumbered if the transaction remains unmined after 50 minutes.
Block Mining

ZCash utilizes Equihash for proof-of-work block mining, which uses an algorithm based on the Generalized Birthday Problem. The ZCash creators chose this algorithm for its efficiency and the lack of availability for optimization that might create unfair advantages amongst miners.
ZEC Stock History