ZCash (ZEC) Alt Coin

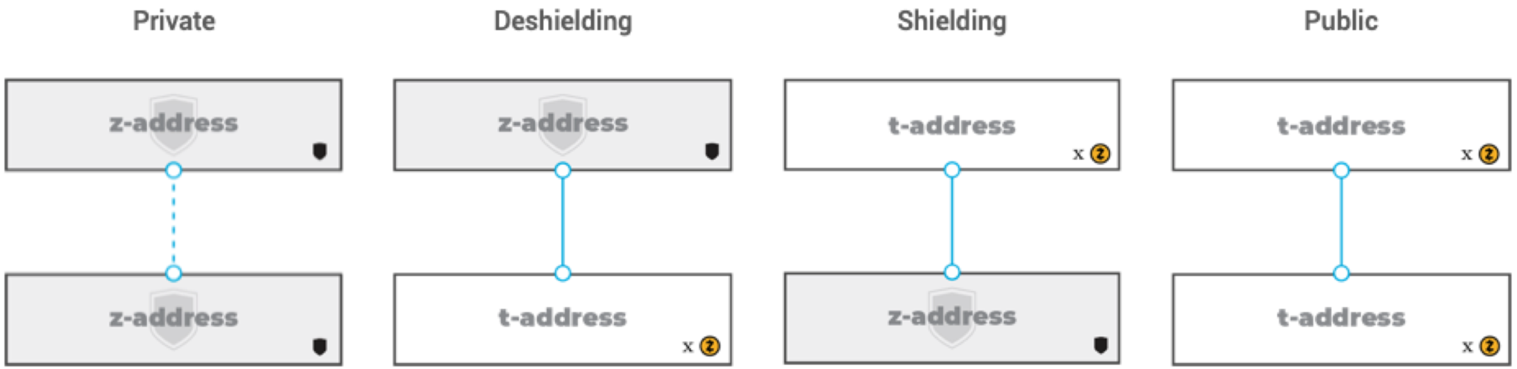
By Emmett Steven

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.

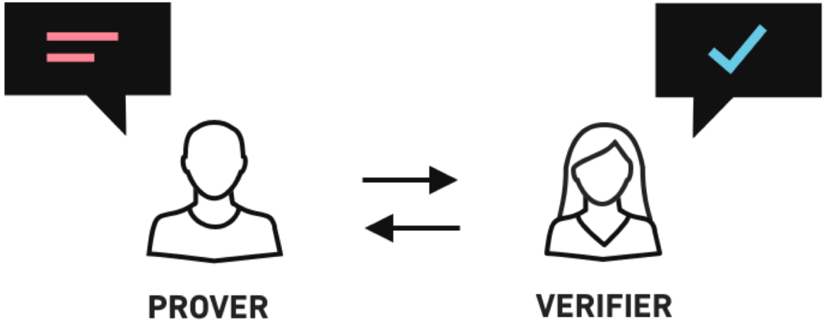
Transaction Types

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 occured 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.

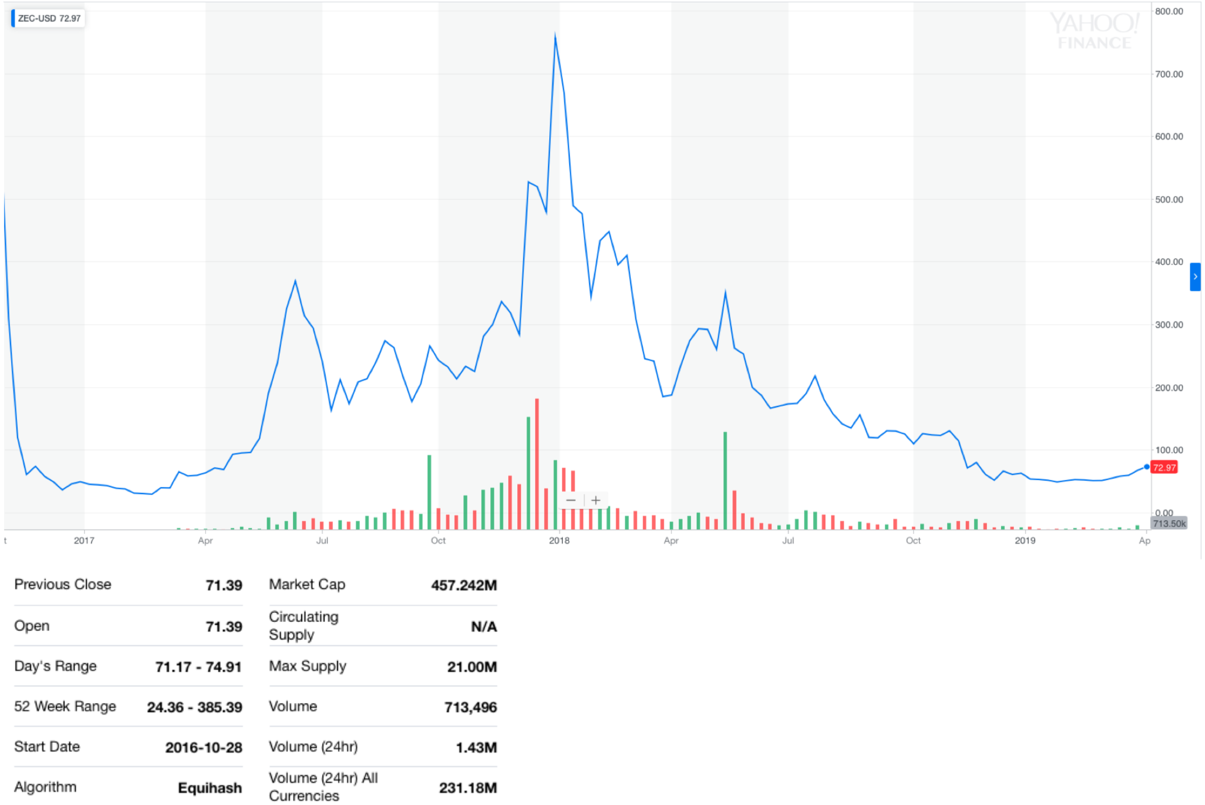
Block Mining

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.

```
iner.exe -l equihash.usa.nicehash.com:3357 -u 1zXgKRqyrjj6zx4jZgs8FRKorY

==== www.nicehash.com ======================
 CPU&GPU Miner for NiceHash v0.4a
developers for providing base of the code.
hanks to tromp, xenoncat, mbevand
 eXtremal-ik7 for providing
CPU, CUDA and AMD equihash solvers.
==== www.nicehash.com ======================


sing SSE2: YES
sing AVX: YES
sing AVX2: YES
tratum | Starting miner
tratum | Connecting to stratum server equihash.usa.nicehash.com:3357
tratum | Connected!
tratum | Subscribed to stratum server
iner | Extranonce is 02 de
tratum | Authorized worker 1zXgKRqyrjj6zx4jZgs8FRKorYcCX4AsL
tratum | Target set to 01e1e1e1e000000000000000000000000000000000000000000
tratum | Received new job #000000386b5fde5f
peed [300 sec]: 0 I/s, 0 Sols/s
peed [300 sec]: 0 I/s, 0 Sols/s
peed [300 sec]: 0 I/s, 0 Sols/s
peed [300 sec]: 0 I/s, 0 Sols/s
peed [300 sec]: 0 I/s, 0 Sols/s
```



Previous Close	71.39	Market Cap	457.242M
Open	71.39	Circulating Supply	N/A
Day's Range	71.17 - 74.91	Max Supply	21.00M
52 Week Range	24.36 - 385.39	Volume	713,496
Start Date	2016-10-28	Volume (24hr)	1.43M
Algorithm	Equihash	Volume (24hr) All Currencies	231.18M

ZEC Stock History