

Zcoin (XZC)

About :

Zcoin is the first full implementation of the Zerocoin Protocol, which allows users to have complete privacy via Zero-Knowledge cryptographic proofs.

It is worth noting that Zcoin is unrelated to other cryptocurrencies utilizing the Zerocash Protocol. Although Zerocash is a development from Zerocoin, their respective implementations are not simple forks of each other, but rely on different cryptographic assumptions with various tradeoffs. Both approaches supplement each other quite nicely, and a good way to describe them would be sibling projects.

Advantages :

- 1. Privacy-Enhancing Technology: Zerocoin Protocol :** With Zcoin, the anonymity set is on a dramatically higher

magnitude. Instead of having an anonymity set limited to the few dozen, Zcoin has an anonymity set that encompasses all minted coins in a particular RSA accumulator that can scale to many thousands and unlike other solutions is not subject to transaction graph analysis.

2. Zcoin Improve Privacy Of The Bitcoin Protocol :

- **mint** : With Zcoin's Zerocoin Technology, you can "mint" a coin found on the public ledger into a private coin
- **spend** : When it is time to spend your minted coin, the owner of the minted coin does not need to be revealed
- **repeat** : The process of minting and spending a coin can be completed as many times as you want, ensuring complete privacy