Privacy Considerations for Official Zcash Software & Third-Party Wallets

The improvements made in Zcash are a big step towards decentralized, financial privacy but there are some important considerations for users who want to maintain optimal transaction privacy, no matter which wallet software is being used.

Addresses & Transaction Graph Analysis

The address type you use can affect your spending abilities or privacy.

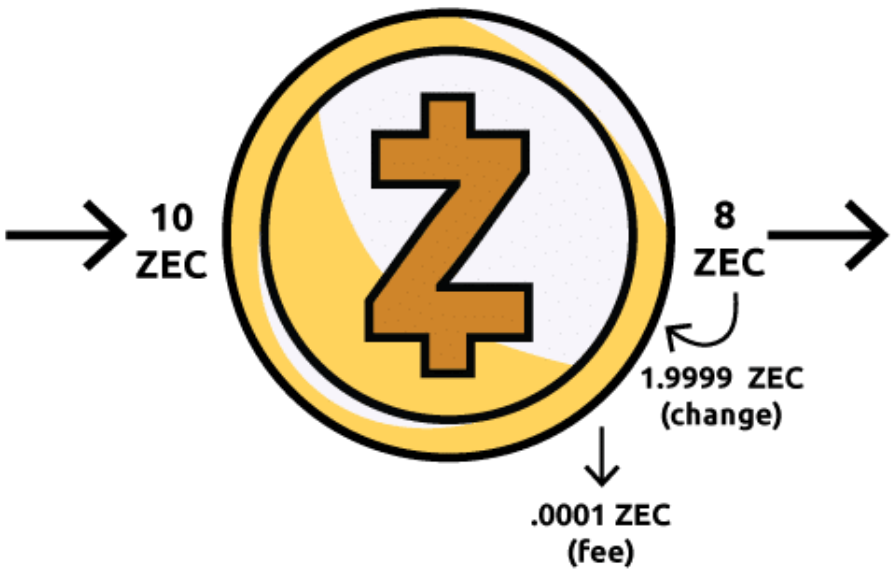
Recommendations

- **Use transparent addresses for ease of use on mobile devices and bitcoin compatibility**
- **Use shielded addresses with the wallet's standard fee selection for better privacy.**
- **Use a unique shielded address to receive money for each distinct purpose.**

Zcash has two kinds of addresses: **transparent addresses** (begin with "**t**") and **shielded addresses** (begin with "**z**").

Transparent addresses

- **Are visible in the blockchain**
- **When included as a sending or receiving address in a transaction, the value transferred should be considered public**
- **Do not offer strong privacy**



Shielded addresses

- **Are not visible in the blockchain**
- **When included as both the sending and receiving addresses in a transaction (fully shielded), the value transferred is private**
- **Offer strong privacy against transaction graph analysis**
- **Are not supported in some wallets**

Additional notes about shielded addresses

- The transaction fees are publicly visible for all transactions, so when using a shielded address it's best for privacy to rely on a privacy-focused wallet to select a fee rather than to select them manually.
- While it is safe to reuse one shielded address for receiving payments for a single purpose (e.g. donations to a non-profit), using one shielded address to receive payments for multiple purposes (e.g. a business service and donations to a non-profit), makes it possible for someone to compare the contexts where the address is used and build an identity profile.

Resources

- Transaction Linkability
- A Shielded Ecosystem
- Anatomy of A Zcash Transaction
- Payment Contexts & Reusing Shielded Addresses
- Encrypted Memo Field

Network Graph Analysis

A unique IP address can allow network observers to correlate your Zcash transactions with each other and with your other traffic.

Recommendations

- **Be aware of IP linkability between transactions sent *from* shielded addresses and your other network traffic.**
- **Advanced users may use Tor to obfuscate the IP address of their Zcash node.**

Notes about IP addresses

Zcash is a global network using IP addresses over TCP for maintaining connections between nodes and does not obfuscate users' IP addresses.

Users should be aware that when an adversary knows a person's IP address, other private details can easily be discovered (names, locations, business interests, etc). For example, in Zcash, correlations can be made between transactions sent **from** shielded addresses and those sent from transparent addresses.

Using Tor

Advanced users may opt to connect through Tor to obfuscate their node's IP address, however, further exploration is needed on a vulnerability combining Bitcoin's Denial of Service mitigations (inherited into Zcash) and anonymous communication networks like Tor before we can recommend users who are not familiar with the attack to route their Zcash nodes through Tor.

Resources

- Downloading the official Zcash client over Tor
- Tor Support in Zcash

Security Considerations for Official Zcash Software

This section is only relevant for the official Linux-based Zcash client. There may be security issues that aren't listed here, please check regularly to stay updated.

Warnings & Recommendations

- **Wallet encryption is disabled, use full-disk encryption (or encryption of your home directory) to protect your wallet at rest.**
- **Ensure no other users have the ability to execute code (even unprivileged) on the hardware your zcashd process runs on unless you have fully analysed your operational security.**
- **Make regular backups of your wallet.**
- **Choose a strong RPC password to prevent others gaining control over your node.**
- **Do not change the default setting that only allows RPC connections from localhost.**
- **Use a minconf of 10 (minimum number of confirmations) to defend against potential blockchain reorganizations (note: we may increase this number if ongoing research reveals notable risks).**
- **Setting the `-debug=zrpcunsafe` configuration is helpful for diagnosing issues but the log will contain private information, so be careful when sharing the contents of it with others. If this is too much liability, use `-debug=zrpc` instead.**

Resources

- Advanced Security Documentation

Keep your Zcash safe

The best way to store your Zcash may be with a digital wallet.

Get a wallet