General
zCOLX Backups & Security

zCOLX introduces changes to backups & security best practices that we want to make users are aware of.

When a COLX wallet is created, 1000 private keys and their public addresses are automatically generated and added to the local COLX keypool. This is used when a COLX user requests a new receiving address: The wallet application pulls a pre-generated address from the keypool instead of creating a new one on the fly.

Because of this design, COLX users benefit from a security perk: If COLX is received at a NEW address that was generated AFTER the most recent backup, and the wallet.dat becomes lost or corrupted, the COLX can still be recovered from an older backup, because that "new" address / key pair was already contained in the pre-generated keypool.

This feature allows users to get away with being less diligent about creating regular backups.

However, the introduction of zCOLX requires a more disciplined approach!

A wallet's minted zCOLX is stored in the encrypted wallet.dat file as a RSA-2048 generated serial number, along with each zerocoin's random seed and public address. This data is **NOT pre-generated**, and is **NOT** stored in the wallet until zCOLX minting is complete. Thus, **new zCOLX can NOT be restored from an older backup the way that COLX can be.**

The ColossusXT wallet application helps by creating automatic backups every time zCOLX is minted.

To access the backup location in Windows:
Press Windows + R, enter %appdata%\ColossusXT\backups and click OK

To access the backup location in OSX:
Press Command + Shift + G, type
~/Library/Application Support/ColossusCoinXT/backups and click GO.

To access the backup location in Linux:
From a terminal prompt, type cd ~/.ColossusXT/backups and press Enter.

Keep in mind that this backup is only as secure as your computer and hard drive! If your PC becomes comprimised, or your hard drive dies or the files are accidentally deleted, you could permantently lose COLX and zCOLX.

Remember: It is **ALWAYS** recommended to copy the ColossusXT backups folder and its contents to **secure, offline, redundant** devices such as a thumb drives, external hard drives, etc!

General

Unique solution ID: #1036
Author: n/a
Last update: 2018-10-10 00:12