A Note on Paper Wallets

Author josh
Date 2021-02-25 20:30:35

I recently saw an article from CoinDesk about users losing Bitcoin to malicious paper wallet software. I thought it would be helpful to write up, from a technical perspective, why paper wallets are a very bad idea.

Paper wallets are the outdated practice of generating and storing a single keypair on paper. One private key and its associated public address, usually in WIF format and a QR code.

Here's why this is a bad security practice:

- The wallet generation takes place on a general purpose, networked device. You are trusting JavaScript cryptography and software that may have a backdoor, generating key data on a device that could be compromised
- WIF encoding is very hard to read and error correct for humans. Water damage or mis-printing could make critical key data unrecoverable
- Change addresses can and have caused a loss of funds. When you import the address into an online wallet and only spend *some* of the funds, the change will usually go back to an address generated by that wallet, NOT back to the paper wallet address. If you don't notice and delete that online wallet, you are hosed.

INSTEAD use modern, well vetted standards for offline storage

- Use a dedicated hardware wallet that gives you a 12-24 word seed phrase (BIP39/BIP32/BIP44 standards).
- This wallet will generate and store keys entirely offline on a microcontroller with firmware that does one thing and one thing only - Bitcoin related cryptography. This lowers the attack surface for malware and key theft.
- Back up the 12-24 word phrase on paper or metal, and store it somewhere safe
- NEVER type this phrase into a networked device like a laptop. Even if you encrypt it or try to use some other technical scheme. It doesn't matter if you are a technical user - typing the phrase into a general purpose device breaks the security model of hardware, offline storage.

Don't get stolen from or make a mistake that results in key loss. Use *modern* standards for key storage, and stay safe.

Hope this helps!