santacroce tech

opinion & insights

MARCH 6, 2025

CONTENTS

INTRODUCTION

Our fourth newsletter explores Bitcoin self-custody, a concept often mistaken for hardware wallets—devices designed to interact with the Bitcoin network. However, as we will demonstrate in this analysis, security depends less on the device itself and more on the setup process.

Many users, even experienced ones, often place too much focus on passphrase complexity or using multiple authentication devices. While these are important security measures, they frequently overlook a key element: a reliable physical backup.

In practice, security is only as strong as its weakest link, reinforcing the need for a well-structured approach.

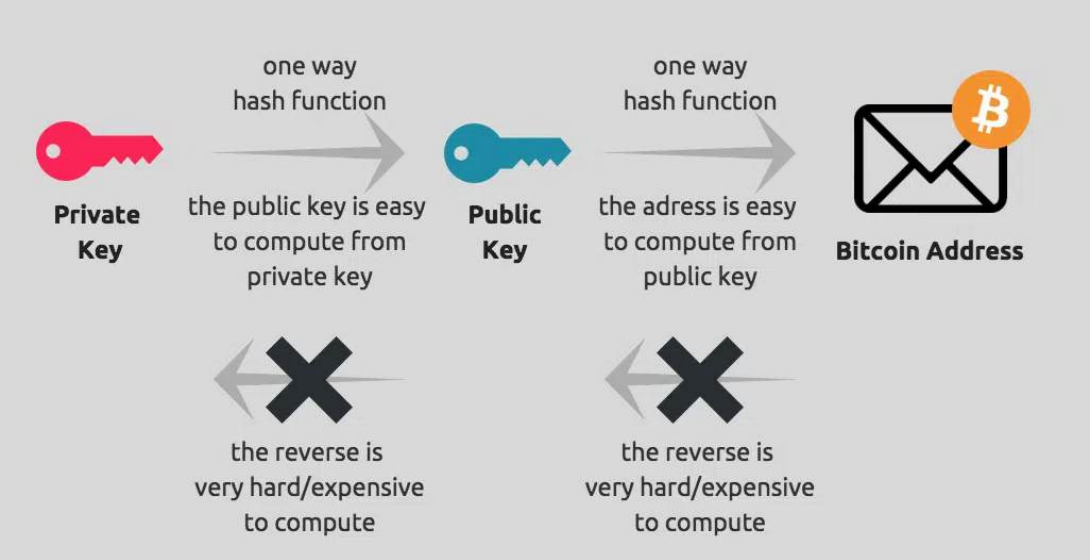
If you have never used a cryptocurrency wallet before, don't worry. This guide will cover the fundamentals and provide step-by-step instructions for securely generating and storing your passwords. Let's get started!

Roberto Santacroce Martins
Programmer, Santacroce Tech Founder

HOW IS BITCOIN MOVED AND SECURED?

A Bitcoin wallet consists of millions of addresses linked through public and private keys. Wallet management is streamlined using a master key, commonly known as the seed phrase. This seed phrase is a series of words that grants access to and control over all addresses within the wallet.

When executing a transaction, the wallet software generates a cryptographic code containing essential details, such as the sender's and receiver's addresses and the transaction amount. This ensures that no private data or passwords are shared while the transaction propagates through the Bitcoin network, keeping user information secure.

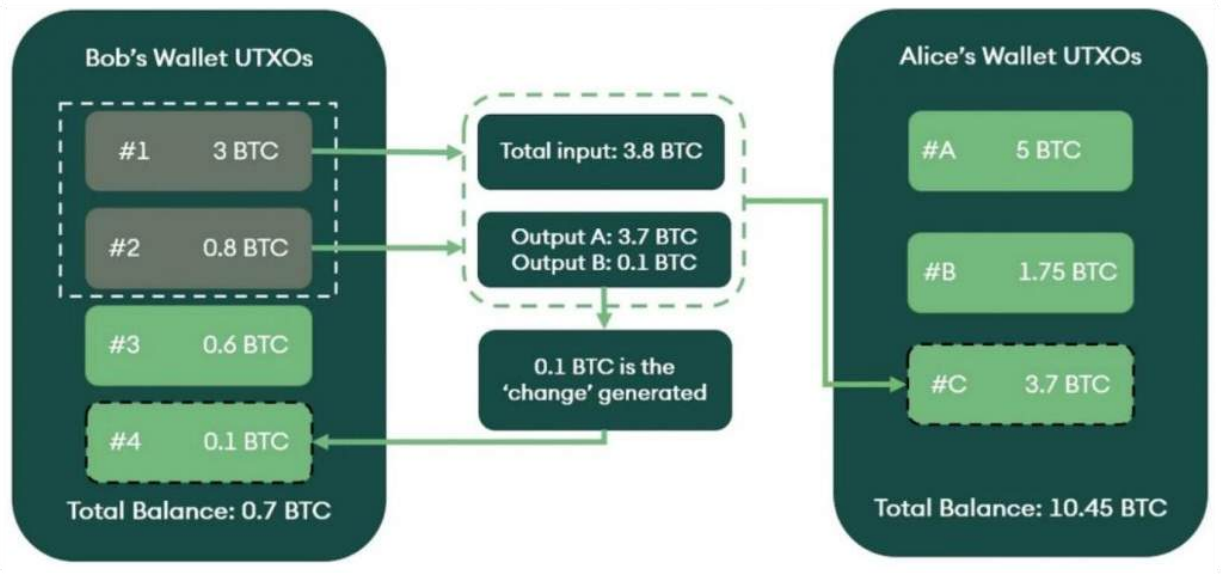


Public and private key concepts. Source: Mycryptopedia

HOW IS BITCOIN SPENDING TRACKED?

A Bitcoin wallet interacts with the network by managing Unspent Transaction Outputs (UTXOs), which represent the available Bitcoin in an address. When a transaction is initiated, the wallet selects the necessary UTXOs to spend, combining them if required. Each UTXO corresponds to an unspent output from a previous transaction.

The wallet generates a new transaction, signs it with the private key to prove ownership of the UTXOs, and broadcasts it to the Bitcoin network. Miners then verify and include it in a block. The wallet continuously tracks spent and unspent outputs, updating the balance accordingly.



Bitcoin UTXO transaction model. Source: Phemex

WHAT ARE MULTISIG AND PASSPHRASES?

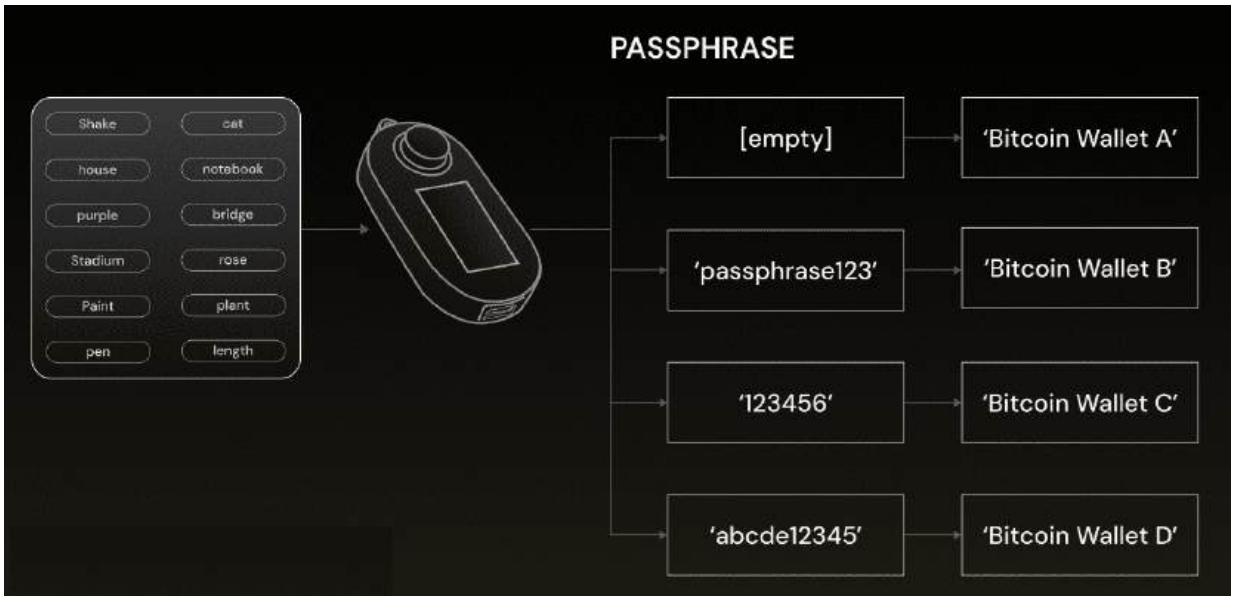
[redacted]

Multisignature (Multisig) and passphrases are security features designed to protect Bitcoin wallets. Multisig requires multiple private keys to authorize a transaction, adding an extra layer of security. For example, a wallet might require two out of three keys to approve a transaction, preventing any single individual from having full control.

SOVEREIGN MONEY: [Multisig Jade/Blue Wallet]

A passphrase, on the other hand, provides additional protection for a private key or seed phrase. Even if someone gains access to the seed phrase, they cannot access the wallet without the correct passphrase. Both features strengthen security by requiring multiple factors to access or move funds.

BITCOIN UNLOCKED: [Trezor Safe 3 / Sparrow]



Bitcoin passphrase used to generate multiple wallets. Source: Cypherock

HOW TO ACHIEVE GOOD ENTROPY?

For strong entropy in Bitcoin seed generation, an offline method is crucial. A Jade or SeedSigner device allows users to roll a six-sided die multiple times, input the results, and generate a secure seed phrase. Since these devices remain offline, they prevent remote attacks. The seed should be written down, verified, and stored securely with no digital copies.

Another approach is using an offline BIP39 tool to turn entropy into a 12/24-word seed. Install VM software like VirtualBox on your PC/Mac and set up a fresh, isolated Linux environment. Download the Ian Coleman BIP39 tool on an online device, then transfer it to the VM via USB. Run the HTML file in the VM's browser, input your entropy, and generate the seed.

Wicked Smart Bitcoin: Dice roll seed generation

Crypto Guide: Zero-Trust BIP39 wallet generation

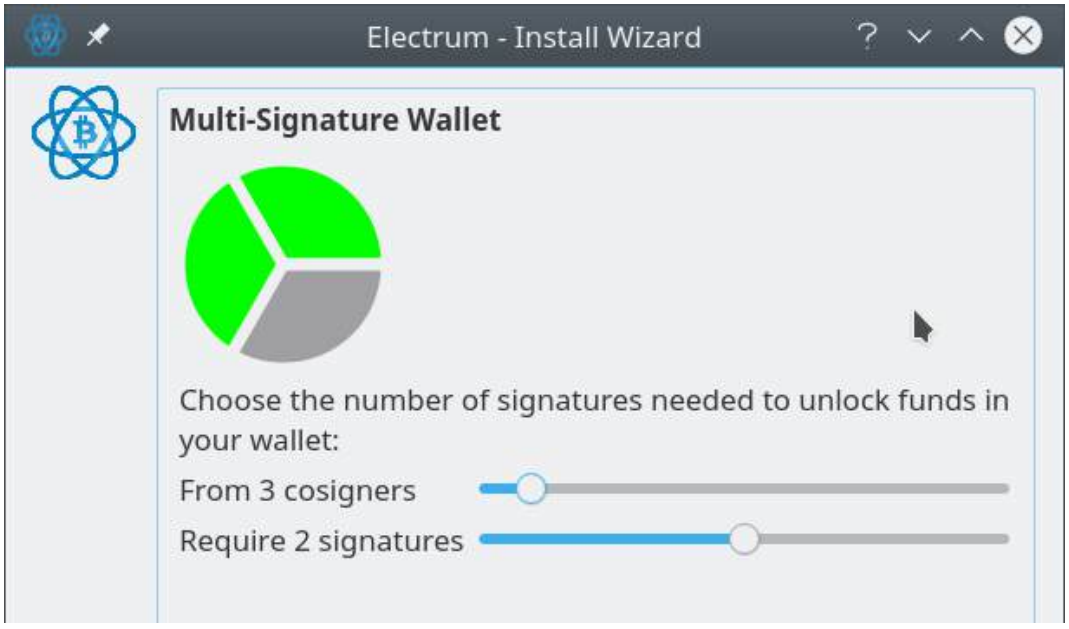
IS MULTISIG WORTH IT?

[redacted]

It depends. For most users, a passphrase provides sufficient security, solving 90% of potential risks without the complexity of multisig. However, if securely storing the passphrase is difficult, multisig becomes a viable option. It is particularly useful for inheritance planning and corporate wallets, where multiple parties need access control. Institutions often use multisig to prevent a single point of failure.

Ideally, a time lock feature should be in place—allowing, for example, a 2-of-3 multisig to revert to 1-of-3 after a set period. This ensures emergency access while maintaining security. While multisig adds protection, it also increases setup complexity and recovery challenges.

BITCOIN EDUCATION: [Timelocked Bitcoin + Decaying Multisig]



Multisig wallet setup using Electrum

IS A HARDWARE WALLET WORTH IT?

[redacted]

A hardware wallet is worth it but should not be blindly trusted for seed generation. Instead, using dice rolls or similar offline methods ensures stronger entropy while remaining compatible with most hardware wallets. For most users, the main difference among the devices available lies in user experience and software rather than security.

Options include Trezor, SeedSigner, Krux, Jade, KeepKey, BitBox02, and Passport. Always purchase directly from the official supplier—never from third-party marketplaces to avoid tampering risks. Ideally, choose air-gapped methods for transactions, such as QR codes or cameras, reducing exposure to potential exploits.

Crypto Guide: Trezor tutorial

Southern Bitcoiner: BitBox02 tutorial

Examples of hardware wallets

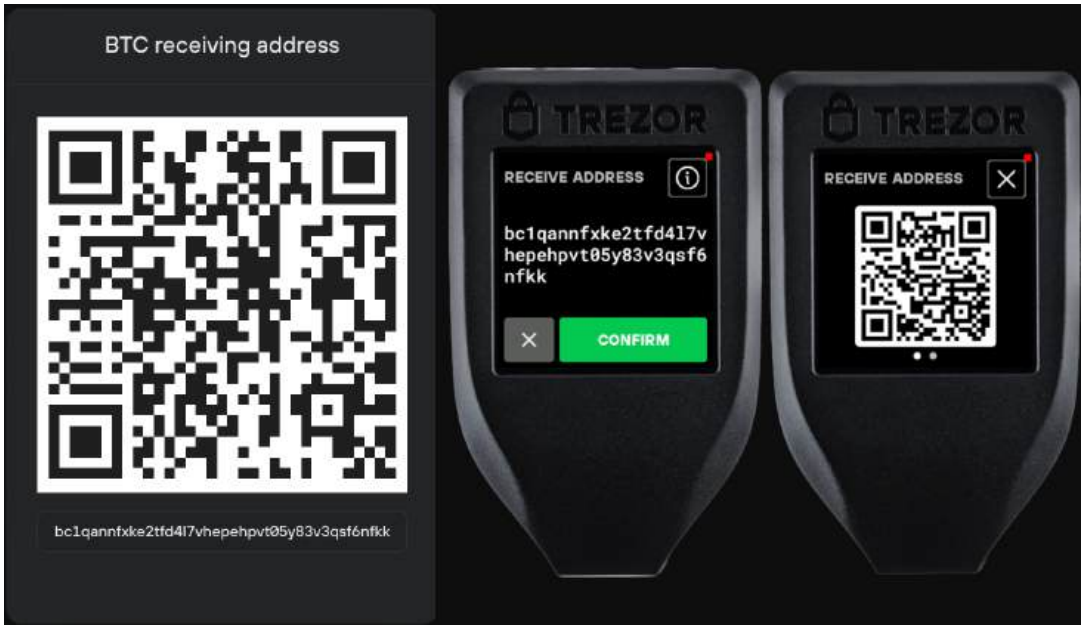
HOW TO USE AIR-GAPPED METHODS?

To use air-gapped methods with Jade, start by exporting your wallet's extended public key (xpub). On Jade, go to the settings menu, select "Export xpub," and display the QR code. Open Sparrow Wallet on an online computer, create a new wallet, choose "Watch-Only," and scan the QR code from Jade. This allows Sparrow to view balances and create transactions without accessing private keys.

To send Bitcoin, enter the recipient's address and amount in Sparrow, then click "Create Unsigned Transaction." Display the generated QR code. On Jade, scan this QR code, sign the transaction offline, and generate a new QR code. Scan it back into Sparrow and click "Broadcast" to send it to the Bitcoin network. This keeps private keys completely offline.

BTC Sessions: Jade Plus + Sparrow

Crypto Guide: SeedSigner/Krux + Sparrow/Electrum



Air gapped transaction. Source: Ledger

METAL PLATE BACKUPS

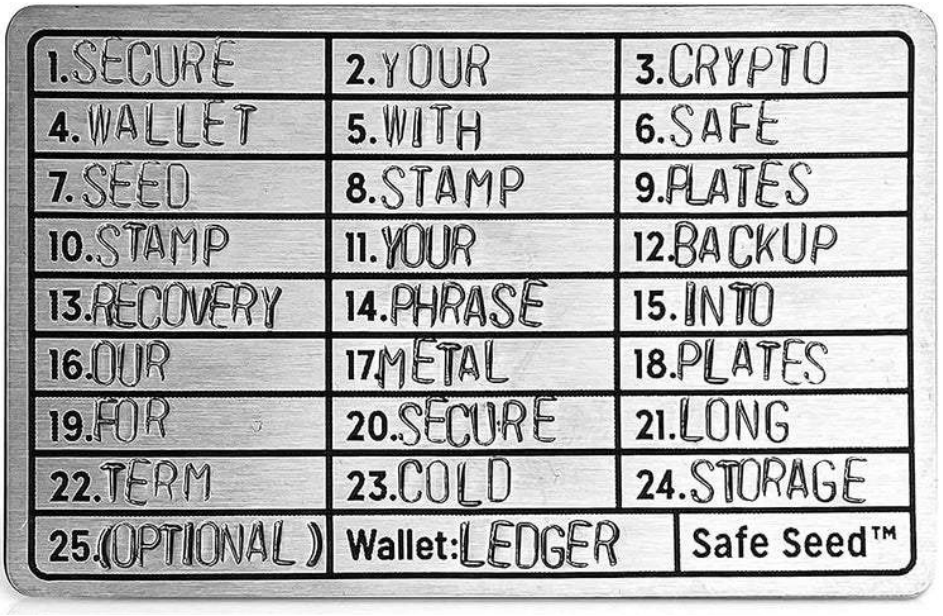
[redacted]

An easy and secure method to create a metal seed plate is using a metal punch stamping—grab a set of letter punches and a hammer, then tap the words into a stainless steel plate. Similarly, an automatic center hole punch offers an excellent result for those using BIP39 number equivalents. It's durable, resists fire and water, and works without fancy equipment.

Unlike the hardware wallets, the metal plates can be acquired in online marketplaces, as there is no risk of tampering–as long as you, and only you, are responsible for manually entering the words or punching the holes. In short, no printers or digital methods including images, even offline.

WICKED SMART BITCOIN: Metal Backup Demonstration

CRYPTO GUIDE: OneKey KeyTag (TinySeed)



WHAT ARE THE BIGGEST THREATS?

Every case of lost Bitcoin—whether through hacks, theft, or accidental loss—stems from human error. The most common failures include not securing a durable physical backup of seed phrases, trusting insecure devices or software, and falling victim to social engineering. Even exchanges, which should have robust security, often suffer breaches due to preventable design flaws. To mitigate these risks, follow four key principles:

- ☐ **Never share your private keys or seed phrases—avoid entering them on websites, apps, or sharing wallet-generated QR codes.**
- ☐ **Verify software integrity—check digital signatures and hashes before installation.**
- ☐ **Beware of phishing attacks—never click on links from emails, ads, or social media messages.**
- ☐ **Avoid scams—never send Bitcoin to strangers, fake promotions, or urgent alerts.**

SANTACROCE'S PICKS

[redacted]

Energy Frontiers: Bitcoin Mining, AI and the Future of Power | AIM Summit Dubai 2024

Moderator: John D'Agostino - Head of Strategy, Coinbase Institutional

https://www.youtube.com/watch?v=ZbKey5-hku8

ABOUT US

Santacroce Tech specializes in expert-driven consulting and custom software solutions in Bitcoin, artificial intelligence, private LLMs, software architecture, and Web3 smart contracts. With deep technical expertise, we build secure and scalable blockchain and AI solutions.

We are actively involved in Bitcoin open-source development, contributing to projects like Stratum V2 and Drivechain. Our team has decades of experience and strong industry connections.

Our work includes initiatives like the Bitcoin Center NY, Brazil's first stablecoin BRZ, and Alkimiya, which focuses on tokenizing financial streams in crypto mining. These experiences make us a strategic partner, ready to advise executive teams on key technology decisions.

CONTACT INFO

[redacted]

Count on Santacroce Tech to keep you informed about digital assets, artificial intelligence, and the Web3 industry. Subscribe now for expert insights that matter. For business inquiries or general questions, reach out to us at info@santacroce.xyz

=-=-=-=-=-= block 886,490 =-=-=-=-=-=