Hardware Wallets: Secure Storage of Bitcoins

Nicolas T. Courtois

- University College London, UK
Goals
Prevent your bitcoins from being stolen.

Expert advice, yet practical.
We failed to protect our DATA
Security of Bitcoin

We failed to protect our MONEY
Solution = Decentralized P2P
Goals
Prevent your bitcoins from being stolen.

How to Manage Keys in Practice?

Not easy, many pitfalls, see our paper:
Wallets
Bitcoin Hardware Wallets

WALLETS - HARDWARE

https://bitcoin.org/en/choose-your-wallet

Mobile  Desktop  Hardware  Web

TREZOR  HW.1  LEDGER ...

Nicolas T. Courtois 2009-2014
Bottom Line

Main Functionality:
- Private Key Generation
- Export public key
- ECDSA sign

(optional):
  - sign full BTC transactions
  - and confirm recipient on the screen

(huge classical pb with all smart cards and digital signature devices,
Ledger has a clever solution: regurgitates inputs on another device USB keyboard)

Nicolas T. Courtois 2009-2014
BTChip HW.1

since Jan 2013

Ledger HW.1

Visit website  Source code

Control over your money
Variable validation
New app
Very secure environment
Variable privacy

HW.1 is a hardware wallet built upon a ST23YT66 banking smartcard platform. It keeps the user private keys safe, validates transactions, can be used as a secure prepaid card or a multisignature party. While not open-source, it can be deterministically validated.
*Features of USB card **ST23YT66**

**NESCRIPT** crypto-processor for PK crypto

- 900 ms for 1 ECDSA signature
- 900 ms for key gen
- Encrypts private keys on the card

(`content` key) 3DES CBC

- Content key can be protected with “a GlobalPlatform Secure Channel” authentication mechanism

Nicolas T. Courtois 2009-2014
Bitcoin Hardware Wallets

Trezor

released March 2014

by Satoshi Labs Prague, CZ

+ display: know to whom you send the money!
+- has open source firmware: https://github.com/trezor/trezor-mcu

TREZOR is a hardware wallet providing a high level of security without sacrificing convenience. Unlike cold storage, TREZOR is able to sign transactions while connected to an online device. That means spending bitcoins is secure even when using a compromised computer.
Bitcoin Hardware Wallets

+ Trezor Lite App

Allows to see your money when you don’t have your device with you!

Based on BIP032 audit capability

=> quite dangerous: see

Wallets and Key Management

BIP032

![Diagram showing key derivation and management processes for BIP032.](image-url)
Ledger

- have their own operating system!
  - closed source, their Chrom front-end is open source
  - due to the current JavaCard limitation:
    - cannot implement deterministic ECDSA (RFC6979)
- bitcoin tx processing implemented inside (unlike HW.1)
  - claimed to be a “more secure” evolution of HW.1
- communicates with Google Chrome directly, no middleware
- data retention: 30 years
- open: no NDA for any wallet to support this
It Implements:

- Standard Multisig, P2SH style (BIP016)
- BIP032 : HD Wallets
  ⇒ danger, see our paper…
  ⇒ Solution: implements RFC 6979, deterministic signatures
- BIP039: seed mnemonic (list of words in English)
- BIP044: specific wallet structure
Bitcoin Hardware Wallets

Security

• master backup
  – printed card with master private seed
  + long passphrase to be written on paper (used only to recover)
  – recovery also possibly if the hardware is lost
    • standard method BIP39, no lock-in, can be recovered on 3rd party soft/hard
  – enter wrong PIN 3 times=>all data are claimed to be erased
  – claimed totally anonymous
    • except browser IP address will be revealed when you send Tx to the network

• each device is paired with a printed card A=>3, to be kept with the wallet,
  – this card=second factor authn. (malware cannot use the device)
  – duo edition has the same card: can create 2 identical hardware wallets
  – Pb: PIN code is entered on a PC: BUT
    • to sign a transaction, need to enter correspondance codes A=>3
      “based on a random sampling of the payment address”
Pi Wallet

- Fully Open source
- OS+Electrum,
- no WiFi,
- can remove/swap SD cards and move them to a safe
BitStash

- Not released yet,
- a large hardware box + standard USB key (encrypted)
  - so similar capabilities like Raspberry Pi solution…
  - move SD Card/USB to a safe!

- Main advantages:
  - works through Bluetooth
    - [connection is claimed to be hardened],
  - can be connected to a laptop/tablet
Combined Solution [Sept 2014]
Combined Solution [Sept 2014]

- Next version: smaller
CoinKite

- card + terminal with HSM
+ supports multisig

Reading their security FAQ:
- they use HSMs at many places,
  - can be very secure
  - all private keys always stored inside HSMs
  - Everything happens on the bitcoin blockchain
    • no off-chain transactions
- servers are hosted in Canada
CoinKite Security

• Pb 1.
  – “each new member receives a "welcome email" which contains the "xpubkey" (extended public key) for their deposits.”
  – super dangerous!

• Pb 2.
  – all private keys for all accounts are known to CoinKite
    • Except for “shared multi-sig accounts”
  – User receive an encrypted backup copy of the private extended key,

• Pb 3.