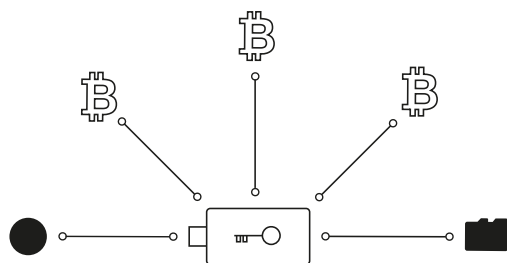


BitBox02

Bitcoin-only edition

Our minimalist hardware wallet is the physical key to your digital world.

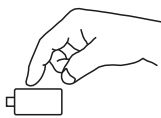


The BitBox02 Bitcoin-only hardware wallet enables you to independently generate and securely store your private keys.

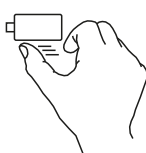
Minimize the attack surface when holding your most important asset.

Use three simple gestures to easily enter your password and navigate your BitBox02.

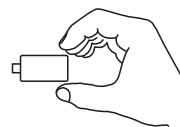
Tap



Slide



Hold



Easy backup and restore on microSD



OLED display and invisible touch sensors



Reduced attack surface



USB-C & A compatible, cable included



Protected using a secure chip

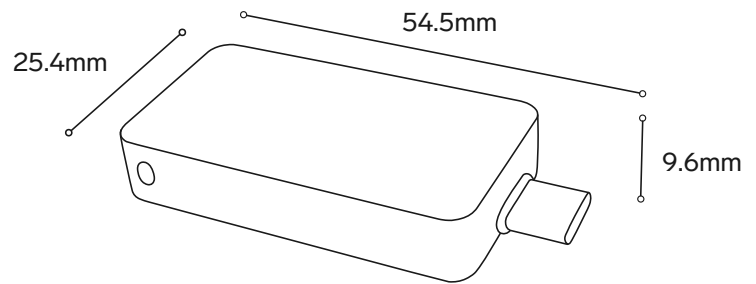
BitBox02

Bitcoin-only edition

BitBox02-Bitcoin
EAN: 7 675364 629452
HS: 8471.8000

In the box

BitBox02 Bitcoin-only edition
microSD card
USB-C to USB-A adapter
USB-C extension cable
Rubber pulls
Labelling stickers



Specifications

Supported coins: Bitcoin (BTC)

Connectivity: USB-C

Compatibility: Windows 7 and later, macOS 10.13 and later, Linux (x86_64)

Size: 54.5 x 25.4 x 9.6 mm including USB-C plug

Weight: Device 12g; with packaging and accessories 160g

Display: 128 x 64 px white OLED

Input: Capacitive touch sensors

Microcontroller: ATSAM51J20A; 120 Mhz 32-bit Cortex-M4F; True random number generator (NIST SP 800-22 and diehard random tests suites)

Secure chip: ATECC608B; True random number generator (NIST SP 800-90A/B/C)

Backup: Instantly on a microSD card; optionally displayed BIP-39 mnemonic seed to copy to paper

Country of origin: Switzerland

Security features

On-device password entry

Open sourced and deterministic builds as we live the motto "Don't trust, verify"

Secure verification of transactions and other data via display on screen and user gesture confirmation

Device attestation to detect counterfeits

Externally audited firmware

Encrypted USB communication between device and app with noise protocol to avoid eavesdropping

Encrypted seed stored on the MCU, protected by both the secure chip and user-chosen device password

Multiple sources of entropy for seed generation

Monotonic counter in secure chip to avoid brute force attacks by limiting total attempts

Password stretching in secure chip to avoid brute force attacks by making attacks take a very long time

Bootloader accepts only firmware signed by Shift Crypto

Bootloader can display the hash of the firmware before running it for binary transparency

Bootloader prevents firmware downgrades

Protection against nonce covert channel attacks

Optional BIP39 passphrase