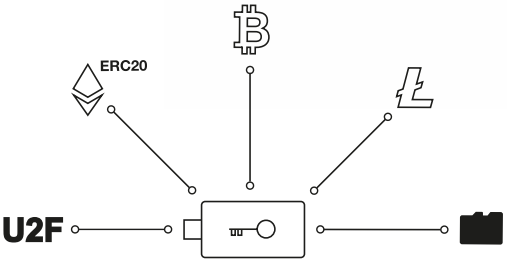
BitBox02

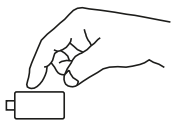
Our latest Swiss engineered minimalist hardware wallet is the physical key to your digital world.



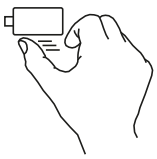
The BitBox02 cryptocurrency hardware wallet enables you to independently generate and securely store your private keys. You can also use it as a second factor authenticator (FIDO compliant U2F).

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

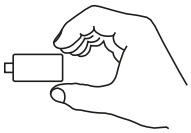
Tap



Slide



Hold



- Easy backup and restore on microSD
- OLED display and invisible touch sensors
- Supported cryptocurrencies
- USB-C & A compatible, cable included
- Protected using a secure chip
- U2F function for secure logins

shiftcrypto.ch

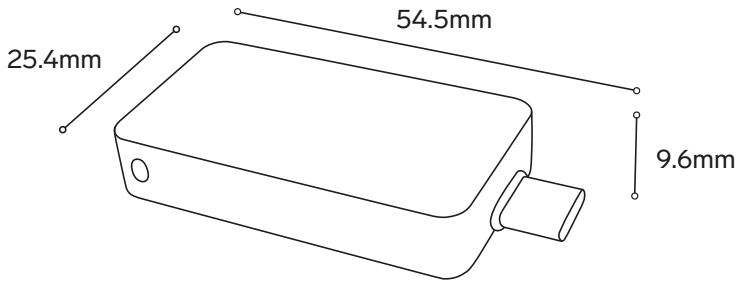
SHIFT CRYPTOSECURITY

BitBox02

BitBox02
EAN: 7 675364 629445
HS: 8471.8000

In the box

BitBox02 hardware wallet
microSD card
USB-C to USB-A adapter
USB-C extension cable
Rubber pulls
Labelling stickers



Specifications

Supported coins: Bitcoin, Ethereum, Litecoin, ERC-20 tokens
Authentication: FIDO U2F compliant
Connectivity: USB-C
Compatibility: Windows 7 and later, macOS 10.11 and later, Linux
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: ATSAMD51J20A; 120 Mhz 32-bit Cortex-M4F; True Random Number Generator (NIST SP 800-22 and Diehard Random Tests Suites)
Secure chip: ATECC608A; 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 Cryptosecurity
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