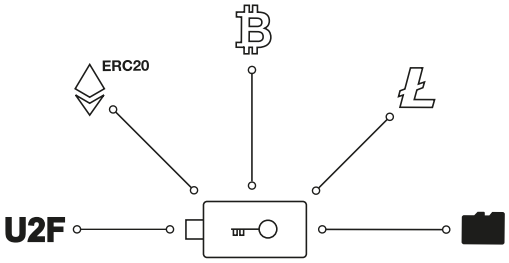
BitBox02 Nova

Multi edition

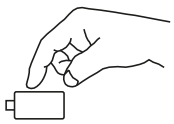
Self-custody made simple.
On all your devices.



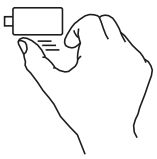
The BitBox02 Nova is the next-generation hardware wallet for securely managing your cryptocurrency. It combines Swiss-made quality with enhanced security and refined design.

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

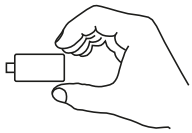
Tap



Slide



Hold



- Effortless backup and restore with microSD
- Glass OLED display and invisible touch sensors
- Dual-chip security architecture
- USB-A & Apple Lightning adapters included
- Protected using a certified secure chip
- Works on desktop and mobile

go.bitbox.swiss/nova

Swiss made open source

BitBox02 Nova

Multi edition

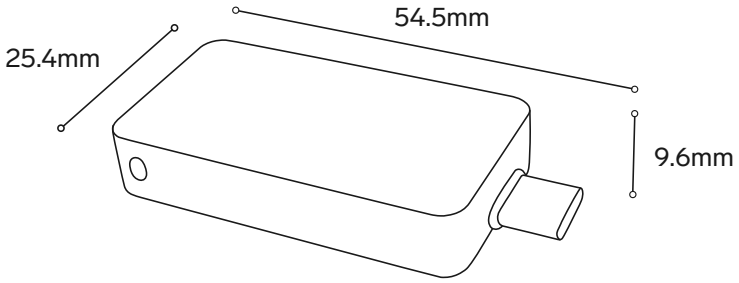
BBNV1A-MLT-**BLK**
EAN: 4262541120104

BBNV1A-MLT-**WHT**
EAN: 4262541120111

HS: 8471.80

In the box

BitBox02 Nova Multi edition
microSD card
USB-C to USB-A adapter
USB-C to Lightning adapter
USB-C extension cable
Rubber pulls
Labelling stickers



Specifications

Supported coins: Bitcoin, Ethereum, ERC20 token, EVM, Cardano, Litecoin; FIDO U2F for authentication
Connectivity: USB-C, Bluetooth® Low Energy
Compatibility: Windows 10+, macOS 10.15+, iOS 16+, iPadOS16+, Android 9+, Linux (x86_64)
Size: 54.5 x 25.4 x 9.6 mm including USB-C plug
Weight: Device 13g; with packaging and accessories 250g
Colors: Midnight Black, Polar White
Display: 128 x 64 px white OLED with glass top
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)
Bluetooth chip: SmartBond TINY™ DA14531
Secure chip: OPTIGA™ Trust M V3
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 source and reproducible builds as we live the motto "Don't trust, verify"
Secure verification of transactions and other data via display on-device
Device attestation to detect counterfeits
Externally audited firmware
Encrypted 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 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 BitBox
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