BWallet Frequently Asked Questions

Release 1.0

Bidixing

January 04, 2015

Contents

CHAPTER 1

Contents

1.1 Overview

1.1.1 What is BWallet?

BWallet is a single purpose device which allows you to make secure Bitcoin transactions. With BWallet, transactions are completely safe even when initiated on a compromised or vulnerable computer. Because the use of BWallet is very easy and intuitive we believe it will help Bitcoin adoption among common people.

1.1.2 How does BWallet work?

The Bitcoin protocol works by sending signed notes of payment across the Internet. These messages(which are referred to as Transactions) are signed using a special algorithm. In order to sign a Bitcoin transaction you need to

have a special key or password. BWallet holds that key. Since BWallet's job is to help you securely sign Transaction messages, you can think of you BWallet as a modern day stamp.

(image credit Petr Kvashin)

BWallet is better than an ordinary mechanical stamping mechanism, however. Each BWallet has a PIN code. If your BWallet gets stolen, thieves cannot misuse it to steal your money. Due to BWallet's clever design, even if the computer with which you use your BWallet is hacked, the hackers will never know your PIN.

In contrast to the various pieces of software and web services that allow you to store your Bitcoins BWallet is secure. Software and web based solutions keep your Bitcoin signing keys either on your computer, or worse, on the Internet! When you use such a service, hackers can easily steal your Bitcoins by hacking your computers or hacking the servers of the services that you use.

1.1.3 Which operating systems and devices support BWallet?

There is full support in Windows, OS X and Linux. Support for using your BWallet with Android devices which have USB On-The-Go (aka USB Host) support is planned in a future release.

1.1.4 What kind of hardware specs does the BWallet have?

CPU BWallet is using a 120 MHz embedded ARM processor (Cortex M3 to be precise) with a custom developed system.

Screen Bright OLED - 128x64 pixels. Enough to hold six lines of text. Can display all the details you need to verify a transaction in a single screenfull.

Case Both BWallet Classic and BWallet Metallic will have a similar case with dimensions of approx. 60 x 30 x 6 mm. The Classic edition is made of a reinforced plastic providing great durability. The Metallic BWallet is made of a polished CNC milled aluminum.

Safety and certifications The BWallet is CE and RoHS certified, so it meets all quality, reliability and environmental standards. Its fine to take your BWallet with you on the airplane. Like all modern electronics, the X-Rays won't hurt it.

Operating temperature -20°C to +60°C (-4°F - +140°F)

1.1.5 What if I lose my BWallet?

BWallet comes with excellent support for paper wallets. When you set up your BWallet for the first time you will be told a list of secret words to write down. Once you have written down this list, you can recover your Bitcoins at any time using a replacement BWallet.

1.1.6 Which wallets are compatible with BWallet?

- MyBWallet - full support
- MyBWallet Lite (Android) - allows to import xpub + watch only mode

1.2 How is BWallet different from ...

1.2.1 an ordinary Web Wallet?

When you store your Bitcoins in a traditional web wallet you put your Bitcoins at risk of being stolen, lost, or confiscated. Here is a list of ways people have lost their Bitcoins through use of a traditional web wallet:

- User's computer is hacked and web wallet password is stolen
- Web wallet server gets hacked and bitcoins are stolen
- Web wallet company goes bankrupt
- FBI or other enforcement agency confiscates coins
- Web wallet provider points to ToS violation and takes coins
- Owners of web wallet company run away with coins
- Bug in web wallet software leads to loss of coins
- Your computer or cell phone is stolen while you are logged in and thieves then steal your coins

If you keep your Bitcoins in a BWallet, none of these things can happen.

1.2.2 a desktop Bitcoin client?

If you keep your Bitcoins in your computer, when your computer is hacked or stolen your Bitcoins can be stolen.

1.2.3 your mobile phone?

There are a number of programs that will allow you to send bitcoins from your mobile phones. Some are simply mobile interfaces to web wallets, and suffer from the same flaws. Some are the same as desktop clients, and can suffer from malware or theft.

1.2.4 a USB flash drive?

A USB flash drive is just storage for private keys. It means that when you want to make a transaction, you must attach your drive to the computer and let your bitcoin software read the keys from the device. At this point your private keys are accessible to viruses and malware, just as to any other software on your desktop computer.

On the contrary, BWallet is a single-purpose computer, which stores your private keys and actively signs transactions without sending your private keys to the computer. When you want to make a bitcoin transaction, your bitcoin software just sends a transaction template to the BWallet device and asks for a digital signature. BWallet shows the requested amount and target address on its display. You will then confirm the transaction by pressing the hardware button. BWallet will sign transaction internally and send the digital signature back to the computer, without leaking your private keys. Thanks to this, you can use BWallet even on a vulnerable or hacked computer.

1.2.5 an encrypted wallet?

Even using a strong password doesn't prevent viruses to silently sit on your computer and wait until you want to transfer coins out of your wallet. This is a vulnerable point, because a virus has access to the wallet file and can read your passphrase from your keyboard.

On the contrary, BWallet never sends private keys to the computer, because when you want to send some coins out of your wallet, BWallet asks bitcoin software for payment details, signs the transaction internally and then sends back just a digital signature of the transaction. There's no point where malware on your computer could access the private keys or send away your coins without your permission.

1.2.6 Yubikey?

There is a significant difference between the two. The Yubikey is a device which helps the service to verify that it is actually you who is signing the transaction. However, it does not protect you against signing a different transaction than you intend to.

1.2.7 a paper backup of my keys?

A paper backup is a quite safe method to protect bitcoins, but you still need to load private keys from paper using a trusted computer to send your coins to somebody else.

1.2.8 Comparison Table

	TREZOR (Classic)	USB flash drive (Kingston DataTraveler SE9)	Common security token (Yubikey NEO)	Paper backup (small piece of paper)	Computer (Acer Aspire E1)	Smartphone (Samsung Galaxy S III Mini)
Size	small	small	small	small	large	medium
Weight	11g	22g	3g	3g	2500g	120g
Waterproof	resistant	no	yes	possible	no	no
Battery usage	no	no	no	n/a	yes	yes
Usability Fast use for transactions	yes	yes	yes	no	no	yes
Transaction signing The device signs transactions directly	yes	no	yes	no	yes	yes
Backdoor-proof I can trust the software the device is running	yes Entire software stack is open-source.	n/a Has no operating system.	no Some proprietary parts, e.g. JavaCard VM.	n/a	no Lots of proprietary parts.	no Lots of proprietary parts.
Software hack-proof My private keys are secured against malware	yes	no	yes	no	no	no
Physical hack-proof My private keys are protected in case of theft	yes	possible If encrypted.	no	no	possible If encrypted.	possible If encrypted.
Disaster Recovery There's a way to recover my wallet in case of theft/loss	yes Paper backup enables disaster recovery into a new device / other wallet.	no	no User must report the device online to have it blocked.	no	possible If regular backups done.	possible If regular backups done.
Phishing protection I know when an unwanted transaction is being signed	yes The user can verify the transaction he is signing on the display.	no	no	no	no	no
Private keys leakage protection Private keys never leave the device	yes	no	yes	no	no	no
Hierarchical wallets support The device supports BIP32	yes	no	no	no	yes	no
Firmware upgrade I can update or use a custom firmware	yes Lifetime firmware upgrades. Custom firmware possible.	no	partially Applications can be updated, but not the underlying firmware.	n/a	yes	yes
Auditable software It's possible to perform a full software audit	yes	no	no Applications can be open, the underlying firmware is not.	n/a	no Too much code to do the full audit, also lots of proprietary parts.	no Too much code to do the full audit, also lots of proprietary parts.
Bitcoin payment protocol The device supports BIP70	soon Cryptographic proof that the address sent to you is correct.	no	no	no	soon	no
NFC support The device supports wireless data transfer	no NFC does not make payments more secure.	no	yes	no	no	yes
Deterministic signatures Device avoids using randomness for signing, making attacks against weak random generators impossible	yes	no	no	n/a	possible Depends on used software.	possible Depends on used software.
External random entropy sources The device provably uses external entropy while generating private seed	yes Combines sources of entropy from computer and TREZOR.	no	no	n/a	no	no

1.3 Security threats

1.3.1 What happens if my BWallet gets stolen?

- Can the thieves take all my coins?
- Is there some way to recover my account once I get a new BWallet?

The short answers:

- No. Each BWallet has a PIN code to prevent misuse in case of physical thief.

- Yes. See recovery.

Just how easy (or hard) is it to get some bitcoins out of a stolen BWallet?

Brute forcing the BWallet PIN

Your BWallet is protected by a PIN code, which can be up to 10 digits between 1 and 9. There are 6561 possible 4 digit PINs for the BWallet. If you choose a good PIN, it will take hundreds to thousands of guesses to guess your PIN. Each time you enter a wrong PIN, the wait time increases by a power of 2. After the first few failures, you have to wait several seconds before you'll be able to try another PIN. Even just trying the top 20 PINs would take about 6 days(150 hours). Trying 30 PINs would take around 17 years. Trying 100 random PINs would take a VERY LONG time.

The number of PIN entry failures is stored in the BWallet's memory. This means that power cycling the BWallet won't magically make the wait time go to zero again. The best you can do by turning the BWallet on and off again is make the timer start over again.

Reflashing the BWallet with evil firmware

Official BWallet firmware is signed by the Bidixing master key. Installing unofficial firmware on the BWallet is possible, but doing so will wipe the device storage and BWallet will show a warning every time it starts. Reprogramming the bootloader is impossible, because all BWallets ship with their secure programming fuse blown.

Inspect the BWallets memory with an electron microscope

You might imagine yourself dissolving the BWallet CPU in acid, finding the reprogramming fuse, repairing it, and then loading evil firmware on the BWallet. I'm no science fiction author, but my guess is – this might be possible. However, the Cortex M3 is a sensitive multilayer chip. The components inside are much smaller than those fake eBay amps. Chances are, all you'd end up doing is destroying the chip. Even if you succeeded in doing so, this will be a costly and time consuming task. In the end the bitcoins will already gone because the original owner will have changed their recovery seed upon discovering that their BWallet was stolen.

Evil maid attack - replace the BWallet with a fake

It might be possible for an evil ninja, or your little brother, to steal your BWallet and replace it with a fake BWallet. If the fake BWallet was embedded with a wireless transmitter, then the fake BWallet could wirelessly transmit any PIN it received. The attacker would then have full access to your funds.

If you are concerned about such an attack, it is a good idea to sign the back of your BWallet with a permanent pen. Don't forget to check the signature before each use.

The BWallet's chassis is sealed using ultrasound. Opening the BWallet without destroying the case is nearly impossible.

1.3.2 What happens if the Bidixing servers are hacked and the firmware signing key is stolen?

First off, this won't happen ;). The Bidixing master key is kept very safe. However, you don't need to rely on the Bidixing signature. You can verify the build yourself. Our hope is that a few trusted BWallet users will make a habit of verifying firmware checksums. If you are concerned about this, we suggest making a habit of checking our blog or social news channels such as reddit before applying any updates. If there ever was a problem with the firmware not matching the source code, you can be sure someone will have written about it.

You don't need to worry about the firmware being updated by a computer virus. Your BWallet will ask you to manually confirm the update before anything is written to the BWallet's memory.

1.3.3 What happens if the Bidixing shuts down?

There are no such plans because we love bitcoin, but even if we had to close down, there's nothing to worry about. You can use your BWallet together with other BIP32, BIP39 and BIP44 compatible wallets. Since our code is opensource, developers from around the world can maintain it and add new functionalities.

1.3.4 What happens if my recovery seed is stolen?

You need to keep your recovery seed safe from theft. If your recovery seed is stolen and you haven's set a passphrase protection, then your bitcoins can be stolen as well. However, if you like, BWallet can protect against recovery seed theft with a passphrase, and therefore eliminate this risk.

1.3.5 What if I run the BWallet recovery process on an infected computer?

During the BWallet recovery process you are asked to enter your recovery seed into the computer with the words in a random order. By default, the BWallet uses a 24 word recovery seed.

If your computer has a keylogger installed on it, then the randomly ordered words may be stolen. One might try to re-arrange these words, until they found the correct word ordering. They can check the order of the words, by generating a bitcoin address using each ordering and checking if the address belongs to you.

There are 24! possible orderings of a 24 word seed. That is 620448401733239439360000 possible orderings.

Each 24 word BWallet recovery seed is verified with an 8 bit checksum . Using the checksum to eliminate invalid seeds, you can reduce the search space by a factor of 256. This gives us a search space of:

24! ÷ 256 = 2423626569270466560000

Going from BWallet recovery seed to public bitcoin address takes 2 × 2048 iterations of PBKDF2, which in turn uses SHA-512. All in all, going from a potential BWallet recovery seed to a bitcoin address, is slightly more difficult than running SHA-512 8096 times.

To summarise, in order to check all possible orderings in a 24 word seed, you need to run SHA-512:

24! ÷ 256 × 8096 = 19621680704813697269760000 times

The bitcoin network is capable of preforming 176 537 883 000 000 000 iterations of SHA-256 each second.

If we wave our hands a bit, we can claim that SHA-512 and SHA-256 are the same difficulty (which they aren't but let's pretend they are). Therefore, it should take somewhere around half of:

(24! ÷ 256 × 8096) ÷ 176 537 883 000 000 000 ÷ 60 ÷ 60 ÷ 24 ÷ 365 = 3.5 years

for the **ENTIRE BITCOIN NETWORK** to crack the seed. If you have that kind of hashing power, you'd make better money mining for Slush's Pool than trying to steal bitcoins. :-) On a normal botnet cracking a BWallet seed would take millenia.

1.3.6 What doesn't BWallet protect against (yet)?

Phishing

If you wish to make a payment to someone on the Internet, you have to be able to figure out their bitcoin address. If you cannot trust your computer, however, you cannot be sure that the bitcoin addresses being displayed on your screen

are not being maliciously modified. It's best to confirm the address via second channel (for example SMS, phone call or meeting in person).

Currently, BWallet has no built in defence against phishing attacks. In the future, we plan to support so-called Payment Protocol defined in BIP-0070 which aims to replace addresses with signed messages containing name of the payee, address and requested amount. Using that method we'll be able to show the payee's name on the BWallet's screen instead of a meaningless address.

CHAPTER 2

License

CHAPTER 3

Contributing

The project is hosted on GitHub and pull requests are welcome!