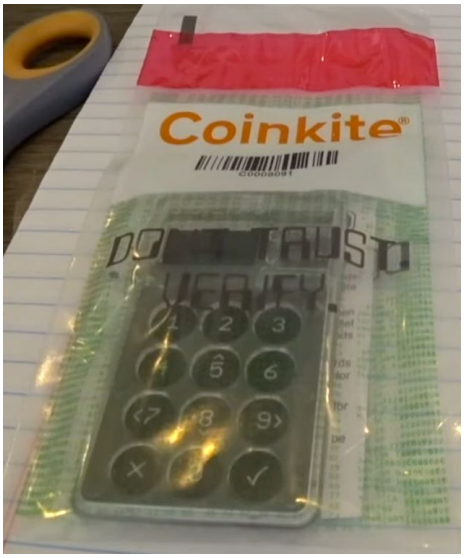
# Reference Guide

v0.1.1 - December 5th, 2019

Firmware: v3.0.5

| What You'll Need | |
|---|---|
| • **Coldcard wallet**<br>  ○ (Ideally a Mk3 or Mk2)<br>  ○ You should get yours in a sealed Coinkite branded bag<br>• **MicroSD card**<br>• **Laptop** | • **MicroSD reader**<br>• **USB to MicroUSB cable**<br>• **USB wall charger or portable USB battery**<br>  ○ (Wall charger recommended)<br>• **Dice (optional)** |

## 1. Inspect and unpack your Coldcard




Verify that your Coldcard's bag hasn't been tampered with. It should look like the photo on the left and be completely sealed.

Once you verify it hasn't been tampered with, take it out of the packaging. You can tear the red seal and get the cool VOID imprint show up or break the plastic with scissors. You may want to keep the bag, at least for now, to verify the serial number on the bag matches the serial number on the device.

Next, inspect your Coldcard to see if it's been tampered with. The clear case of the Coldcard allows you to see onto its chipboard, making any tampering glaringly obvious.


If everything looks as it does above, you should be good to go. The mk2 and older have slightly different designs and have no gold Coinkite logo or Maple Leaf on them.

In the bag you'll also get a Coldcard sticker and a piece of card paper (Wallet Backup Card) to write your device PIN, anti-phishing code words, and seed phrase (mnemonics) on.

🚨 **KEEP YOUR KEYS SAFE - Once filled-out, don't show the paper backup card to anyone** 🚨
This info allows access to the funds you put on your Coldcard without physical access to the device. You may want to store your mnemonic seed somewhere else long term, perhaps on a steel device, or at the very least, create multiple backups of it in multiple locations. We'll also go over how to make multiple encrypted MicroSD backups later in the guide.

For our workshop, we'll be using testnet BTC. When you take the device home and are ready to use it on mainnet, you should generate a new seed because the security of your Bitcoin depends on it.

**Rabbithole Reading:** Jameson Lopp's seed storage options with stress test
https://blog.lopp.net/metal-bitcoin-seed-storage-stress-test--part-ii-/

## 2. Plug-in and initialize Coldcard

Connect your Coldcard to your USB wall charger or portable USB battery using the USB to MicroUSB cable. You should never plug your Coldcard directly into a data-capable USB port such as the one on your computer or an airport charging station. If this is your only source of power, use a data-blocking USB adapter like PortaPow (see https://portablepowersupplies.co.uk/ for more details. They can be found on Amazon).

Once powered, you'll see the device confirm its factory firmware and have its light switch from red to green. You'll then be prompted with a terms of service agreement. You can page through it with the 5 and 8 buttons on the pinpad and accept it by pressing the "✓" (check) button.

You'll then be shown the device's serial number. It should match the number on the device's bag just beneath the barcode. Press the "✓" button to continue.

## 3. Set your PIN

Choose the PIN for your device with the keypad and record it on the paper backup card.

🚨 **Make sure you record the PIN you set because it cannot be reset like a seed can** 🚨
You must know the existing PIN in order to change it. It is good security practice to use a long PIN.

After you enter the first part of your PIN (the prefix), you'll see your anti-phishing words. Write down the anti-phishing words on your backup card. You should see these two words every time you fire up your device and enter the PIN prefix and they should only change if accessing a different wallet. If you see different words when booting up your Coldcard and entering your PIN prefix it might be a sign that the device has been tampered with or switched out with a compromised device to get your PIN or passphrase. Phishing words are device specific and will be different on each Coldcard you use.

Then enter the rest of your PIN (the suffix) and record it on the backup card. (Unless you choose to memorize). Make sure you record both parts as they are both required to sign in to the device.

**Example:** In the PIN 123-4567, the part before the dash, 123 is the prefix, and the part after the dash, 4567 is the suffix.

## 4. Upgrade Coldcard firmware

Go to **https://coldcardwallet.com/docs/upgrade**, and download the .dfu file for the latest Coldcard firmware at the top of the page.

You can manually verify the software if you like, with PGP, but the Coldcard will also verify it itself. Drag and drop the file onto your MicroSD card, eject it, and put it into the MicroSD slot on the Coldcard. *CLICK*

From the main menu on the Coldcard, go to **Advanced > Upgrade Firmware > Upgrade** from MicroSD. Select the .dfu file from the menu options and wait for the Coldcard to upgrade. While upgrading, the Coldcard's light should turn red, but once the upgrade completes, the light should flip back to green.

## 5. Generate Seed (and add entropy with a dice)

On this next screen, select **New Wallet**. It will generate a 24 word mnemonic seed phrase for you based on the entropy on the device. We can add our own external entropy by pressing 4 on the keypad while on this screen, which enables dice-roll mode. Roll to your heart's content with a dice. More rolls and more entropy can only help you. The advantage of adding randomness with the dice rolls is it reduces the threat of a faulty or tampered hardware in the Coldcard.

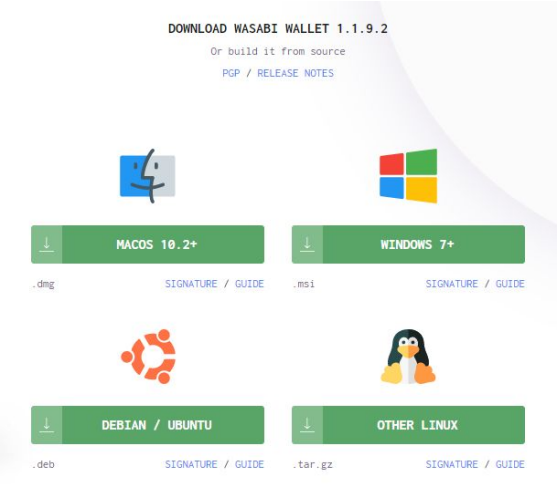
Hit the "✓" button when you're done and you'll get 24 brand new seed words.
🚨**Do not share these words with anyone or they will have access to your funds. This applies to electronics as well. Taking a photo of the seed, saving it to a file on a computer, or even typing it into a computer temporarily to do a printout could all lead to loss of funds.** 🚨

Write down your words and put them somewhere safe. Your Coldcard wallet will test you to make sure you have the seed recorded somewhere. If you are storing the paper backup in a place that may be accessed by other people, consider using the encrypted MicroSD backup feature. An

attacker would need both the SD card and the 12 word phrase to steal your funds. Best to keep them in separate locations.

**Rabbithole Reading:**
https://www.quora.com/Why-is-randomness-important-in-cryptography (2 min. read)

## 6. Download, verify, and install Wasabi




Open your browser and navigate to **https://wasabiwallet.io/#download**.

Download the Wasabi PGP key at the top of the page and import it into your PGP keychain. For OS-specific instructions, please see *the relevant section at the end of this guide*.

Next, download the Wasabi release for your OS (.deb, .exe, or .dmg) and the corresponding signature file (.asc).

## 7. Export your Coldcard wallet for Wasabi

On your Coldcard, go to **Advanced > MicroSD Card > Export Wallet > Wasabi Wallet**.

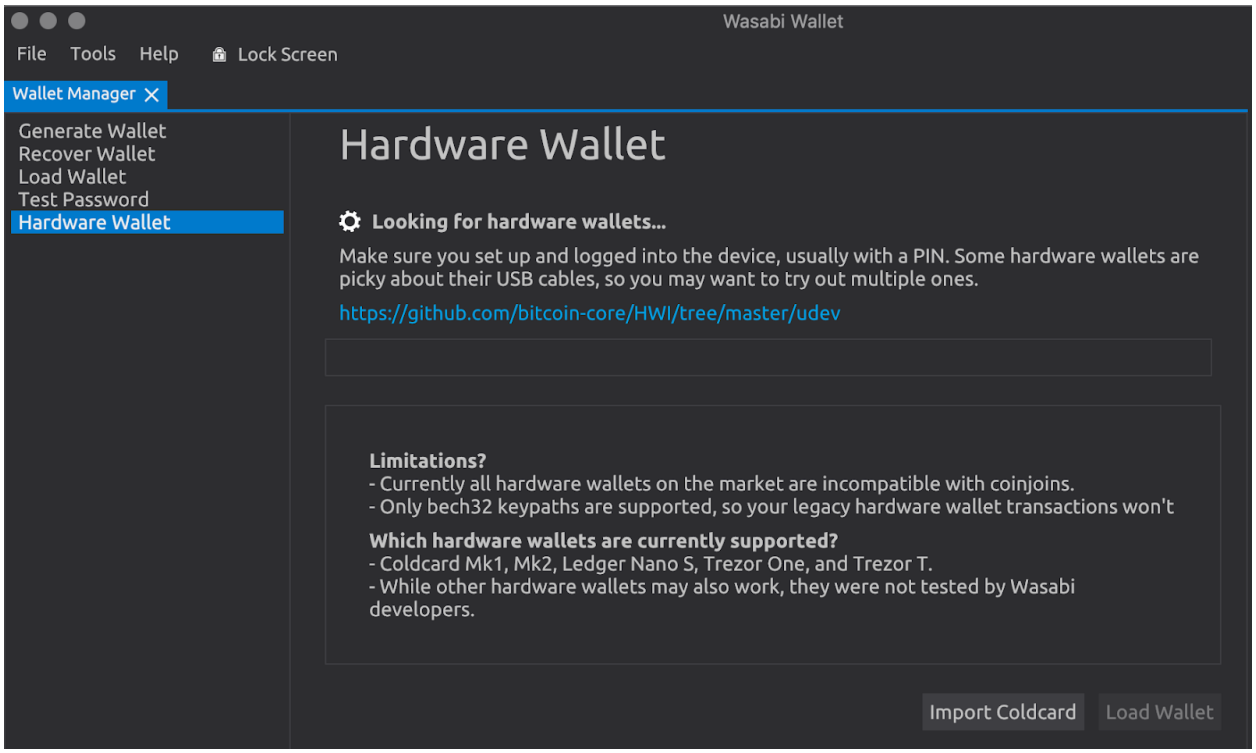
This will create a skeleton file formatted for Wasabi on your MicroSD card. Write the skeleton file to the MicroSD card, then eject it from the Coldcard. Next, insert the MicroSD into your computer.

Keep the skeleton file secure to preserve privacy. The file includes an XPUB that can reveal all of your public addresses. In other words, they can see all of your funds, but they can't spend them.

## 8. Set up Coldcard Skeleton Wallet in Wasabi

Connect your SD card to your computer. In Wasabi, click on "**Hardware Wallet**" in the menu on the left. Click on "**Import Coldcard**" at the bottom of the app. Find your sd card among the files, probably on the left, and click on your skeleton file, named "**new-wasabi.json**". Wasabi will create a new wallet called "**Coldcard0**".

Delete the skeleton file from your SD card after completing this step.



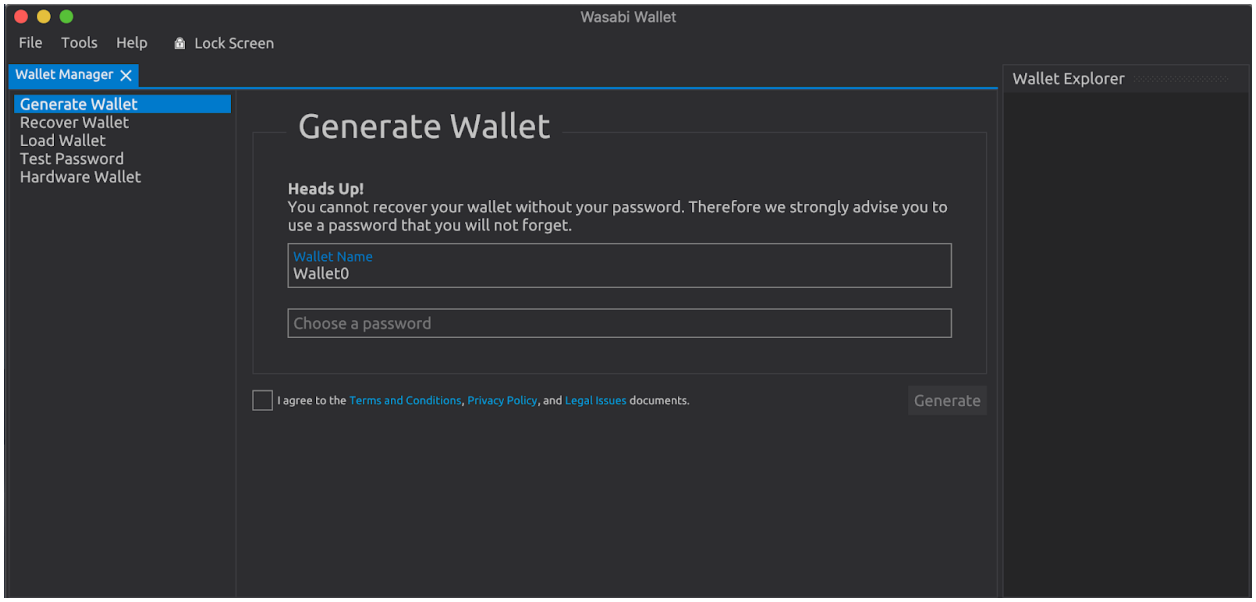
# 9. Set up hot wallet in Wasabi

Close and reopen the Wasabi application. Click on "**Generate Wallet**" on the top left of the app. You will have to give your hot wallet a snappy name and a strong password. Next, the Wasabi wallet will show you your seed phrase. **Be sure to record your seed phrase AND password carefully**. Store them in a safe secure place.

**🚨Do not share these words with anyone or they will have access to your funds.🚨**

Note that you don't have to verify the password the first time you enter it. This is by design as it forces you to carefully record it. You cannot send money to the wallet until you have confirmed that you know the password at a later point.

**🚨If you lose or forget your password funds cannot be recovered even if you have the seed words. 🚨**



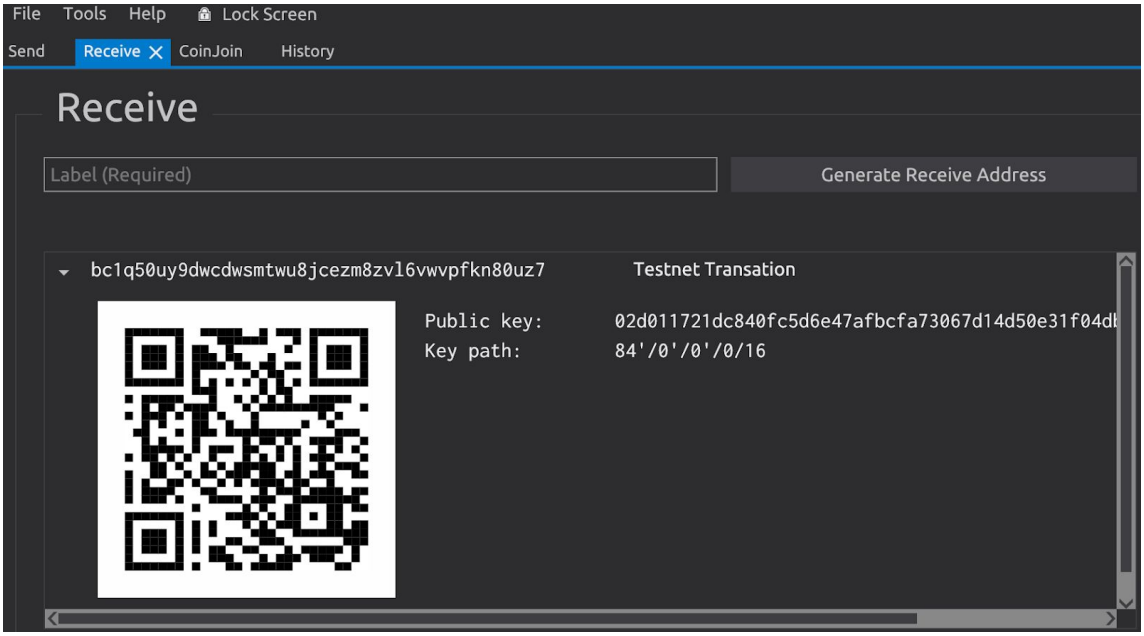
# 10. Receive testnet BTC to your hot wallet

In order to switch to Testnet click on the "**Tools**" menu at the top and then click on "**Settings**". Switch the network to "**Testnet**". You will have to close out Wasabi and restart it for this change to take effect. Load your hot wallet one more time.

Click on "**Receive**" at the top left of the Wasabi app.

When receiving transactions in Wasabi you will need to Label the incoming transaction in the "**Label (Required)**" field. ***BE SUPER SPECIFIC!*** This label is what will enable you to maintain your privacy down the road.

Wasabi has a minimum of 10M sats (.1 btc) per coinjoin on mainnet and 1M sats (.01 btc) on testnet. Transactions with the same label will be combined automatically to reach that threshold.
Type your label and click on "**Generate Receive Address**". Wasabi will create an address tied to the label you've chosen. In order to see the QR code, click on the arrow to the left of the address.




If you are following this tutorial from home, tweet your address to @btccitadel and we will send you some testnet btc to play around with, otherwise we will walk around the class funding wallets.

# 11. Coinjoin

Did you know that exchanges and other services can easily track your bitcoin transactions and link them to your identity? Bitcoin transactions can be easily tracked. Coinjoin helps you break that trail by mixing your transactions with others. Outside observers can tell when you've used coinjoin, but the more rounds you do, the harder it becomes for them to follow the trail. Privacy loves company - the more people who use it, the better it gets.

X1 --> --> X(1,2,3,4,or 5)
X2 --> --> X(1,2,3,4,or 5)
X3 --> coinjoin --> X(1,2,3,4,or 5)
X4 --> --> X(1,2,3,4,or 5)
X5 --> --> X(1,2,3,4,or 5)

**Rabbithole Watching:**
This video (https://youtu.be/sM2uhyROpAQ) contains a great explanation of how a coinjoin works and contains some good tips on managing your UTXOs in order to maintain privacy.

# 12. Send from hot wallet to Coldcard

Generate a receive address in the Coldcard portion of Wasabi and label it. Copy the address. Connect your Coldcard to power and turn it on. Navigate to the address explorer (**Advanced > Address Explorer**) and confirm the address on screen is the same address that Wasabi gave you.

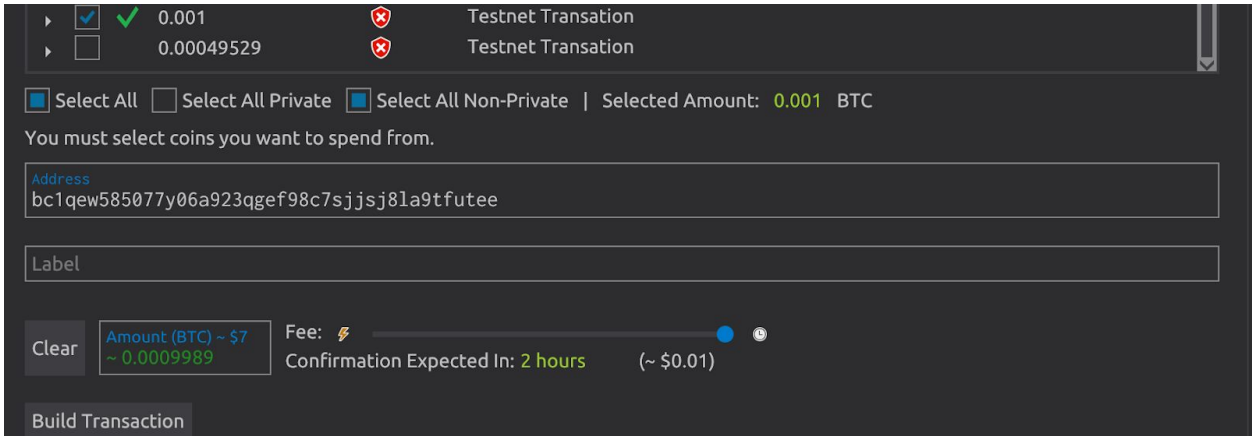
Close Wasabi and reopen it. Launch your Wasabi hot wallet. Go to send tab. Paste address. Confirm a second time that it is the same address shown in the address explorer on the Coldcard. Click Send.

**Rabbithole Reading:**
https://bitcointechweekly.com/front/bip-174-psbt-partially-signed-bitcoin-transactions/
Also for better understanding of coin selection:
https://bitcoinedge.org/tutorial/dpp105-karl-johan-alm-bitcoin-wallets-coin-selection

# 13. Send from Coldcard back to hot wallet using Partially Signed Bitcoin Transactions (PSBT)

In order to send from Wasabi using Coldcard you will need your MicroSD card connected to your computer. In the Wasabi app, click on the "**Send**" tab at the top left. On the right, click "**Advanced**" and then "**Build Transaction**". From your list of UTXOs, choose the output that you would like to use by clicking the check box next to it. (NOTE that breaking up UTXOs that have been coinjoined will deanonymize them.)

In the text fields below, enter the address that you plan to send to. Set your fee with the slider. Then click "**Build Transaction**" on the bottom left.




This will bring you to a screen showing you a text field with a bunch of letters and numbers. You will feel like a hacker. Click "**Export Binary PSBT**" at the bottom of the screen. This creates the "partially signed" transaction and Wasabi asks you where to save it, Save the PSBT onto your SD card and then eject it from your computer.


Now, put your Micro SD card into your Coldcard. Select the first option in the Coldcard menu that reads "**Ready to Sign**" by pressing the "✓" button. Coldcard will ask "**OK TO SEND?**" and show you the details of the transaction; double check to make sure the address and amount are correct, then click the "✓" button. It should say "**PSBT Signed**" and will automatically write it to the SD card.

Now move your MicroSD card back to your computer. In the Wasabi app, click on "**Broadcast Transaction**" on the right. At the bottom, click on "**Import Transaction**".

Choose the file in your MicroSD card ending in "**.txn**". Now click "Broadcast" transaction.

Congrats! You have sent a bitcoin transaction using PSBT!

To avoid confusion moving forward, it is best to consolidate or delete the files associated with this transaction within your SD card.

## 14. Back-up your Coldcard to the MicroSD card

Go to **Advanced > Backup > Backup System**

You'll be given 12 words here. These 12 words will act as the password for your MicroSD backup. Write them down and confirm them with the Coldcard. Your backup will be written to **backup.7z** on the root of the MicroSD card. You will need both the sd card and the 12 word phrase to recover your funds. Multiple copies and brands of SD cards (since they will have different shelf life) kept in different locations is a good option. It's best to keep them separate from the 12 word phrase - an attacker needs both to steal your money.

## 15. Wipe Coldcard

Before wiping the device you may want to save a copy of the first few generated addresses (**Advanced > Address Explorer**) so that when you restore the device you can verify it's been done correctly by checking that the addresses match. This confirms not only that the words are recorded accurately, but that they've also been imported in the correct format (using the correct derivation path).

Go to **Advanced > Danger Zone > Destroy Seed**. Read the disclaimers, make sure you have your backup seed either in a backup.7z file or written down somewhere and pin recorded somewhere, then proceed.

## 16. Restore Coldcard

Login with your pin and go to **Advanced > Backup > Restore Backup** if recovering from an encrypted backup from your MicroSD card or **Import Existing** if recovering from a written seed. It's best to restore for the encrypted backup because it can take a while to type out your seed phrase on the Coldcard keypad.

This step is crucial to have practiced a few times before switching to mainnet. If you have to restore your Coldcard for the first time using mainnet funds you're going to be quite stressed, especially if the amount of funds is substantial. Practicing in a low-stress environment beforehand will give you confidence and reduce your stress levels.

## 17. Send it back to us as proof

We could use the testnet coins for the next class if you don't need them. Our public testnet address is 2MyjfT8S6UPUL2trLukJTQdpL71NAUoNqxK

## 18. (Bonus) set up new wallet with a password (BIP39)

Once you've upgraded your Coldcard to v2.0.0 or higher you can use this feature which can vastly improve your security.

The BIP39 standard (https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki) supports an optional passphrase which encrypts the seed words and creates a new wallet (master private key) for every possible passphrase. Think of it like adding a 25th word to your 24 word seed.

Go **Passphrase** on the main Coldcard menu, read the disclaimer, then hit the "✓" button to proceed. On the next screen you can create a passphrase with words, numbers, and symbols. Once you're satisfied with your BIP39 password hit **APPLY**. You'll be shown a master key fingerprint of the new wallet you just generated. You can write this down somewhere and compare it next time you enter in your BIP39 password to make sure you entered it in correctly and make sure you're dealing with the same wallet.

From here you can use the Coldcard as you wish. You can always return back to the Passphrase menu to change the passphrase in use and switch to another wallet. Note that you'll have to re-enter the passphrase next time you turn your Coldcard on again as it's not stored in memory.

You can see the complete BIP39 passphrase docs over at https://coldcardwallet.com/docs/passphrase

---

# Coinjoin Tips

- Coinjoining is an excellent technique for preserving privacy but it's only as good as your coin control.
- Avoid sending your separated Coinjoin outputs to the same address, this will cause you to lose privacy.
- Avoid consolidating your Coinjoin change outputs. It may be tempting to meet a minimum mix requirement or a maximum input requirement but this will cause you to lose privacy. If you have dust (very small amounts that can't be mixed) consider donating them to a Bitcoin core or Bitcoin project developer
- For further insight, check out the Wasabi guide by 6102bitcoin https://github.com/6102bitcoin/FAQ/blob/master/wasabi.md

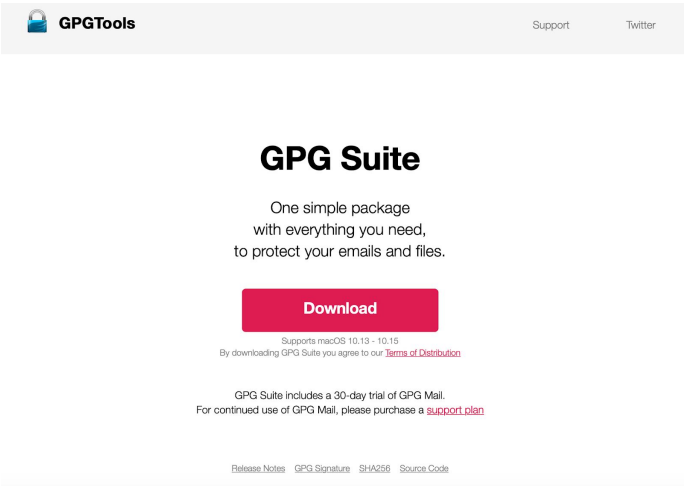
# PGP Verification

## Verify PGP Signatures - Linux

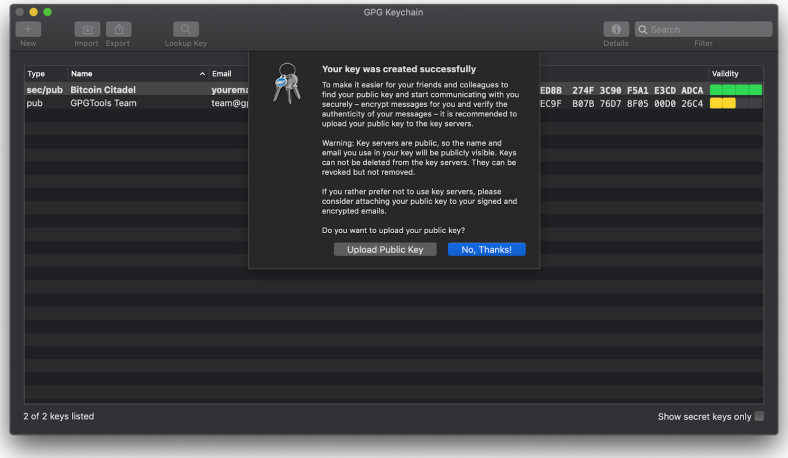
1) Download Wasabi PGP public key.
2) Open command line terminal with Ctrl+Alt+T.
3) import key with gpg --import PGP.txt. The fingerprint should be 6FB3 872B 5D42 292F 5992 0797 8563 4832 8949 861E.
4) Download the latest Wasabi release(.deb) and the signature file(.asc).
5) Verify the signature in the Download repository with gpg --verify Wasabi-1.1.9.2.deb.asc.
6) Install Wasabi.

## Verify PGP Signatures - MacOS

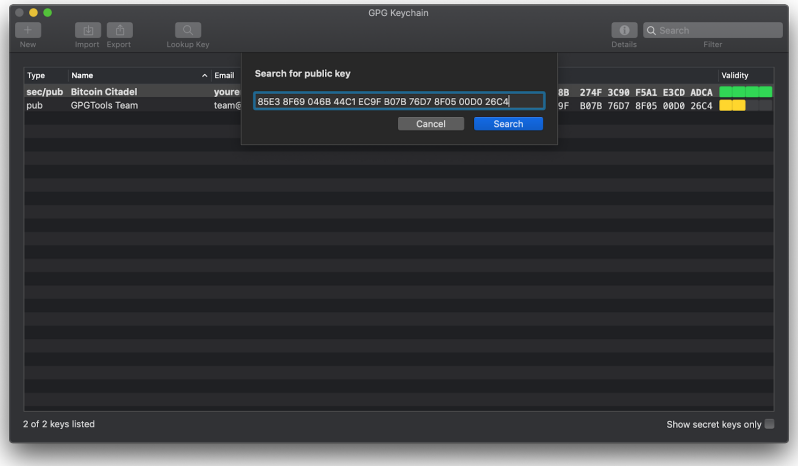
1) Go to gpgtools.org
2) Download the latest version.




3) Open the download and proceed with installation.
4) Approve access to the keychain.
5) Create your first GPG key. Enter your name, email, and choose a password.
6) Choose whether or not you want to upload your public key to server so people can look it up with your email.

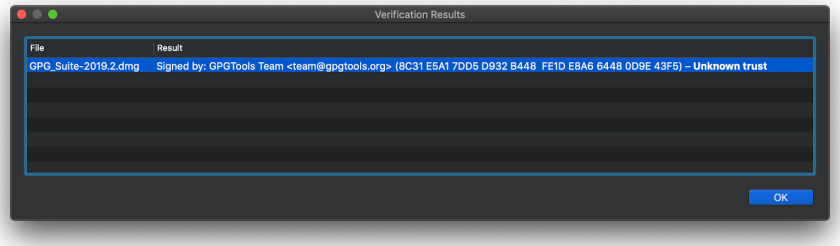



7) Add GPGTools' key to your keychain by copying the fingerprint (Should be 85E3 8F69 046B 44C1 EC9F B07B 76D7 8F05 00D0 26C4) and entering it into the lookup box accessible at the top of the window.

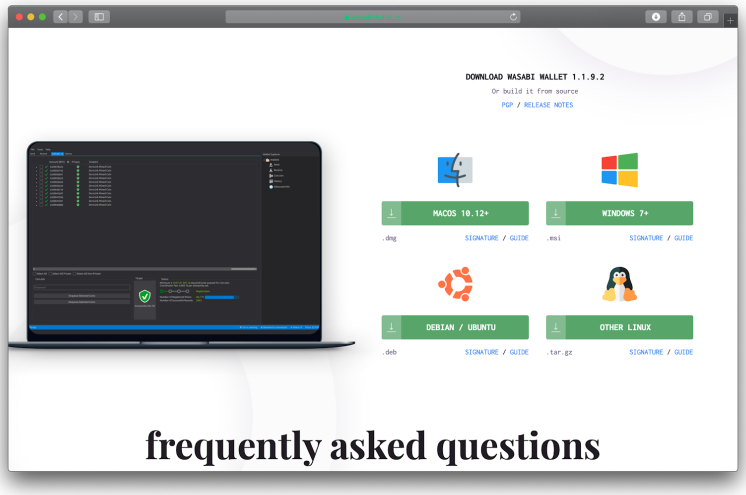



8) Download the signature file at gpgtools.org into the same folder as the install file.

9) Click to open the signature file and the app will verify it.

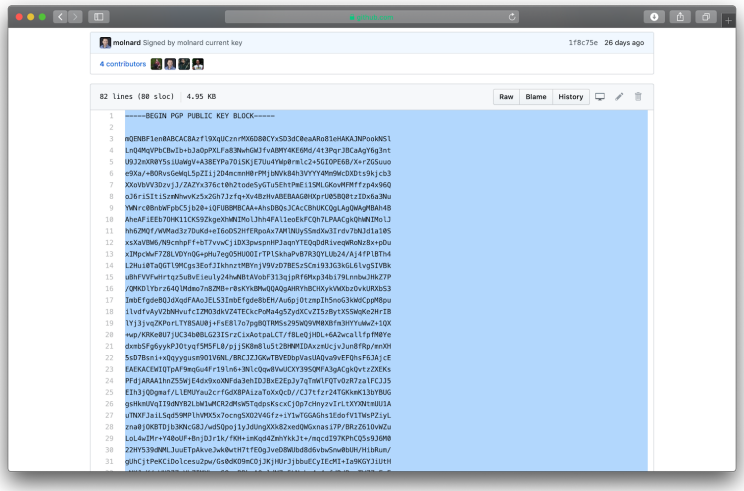


10) Go to Wasabiwallet.io and download the app and signature files.

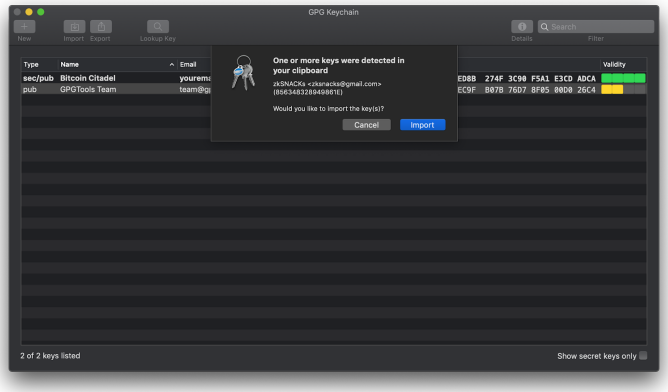



11) Click the PGP link on the top to go to their GitHub page.

12) Select and copy the entire public key block to your clipboard.

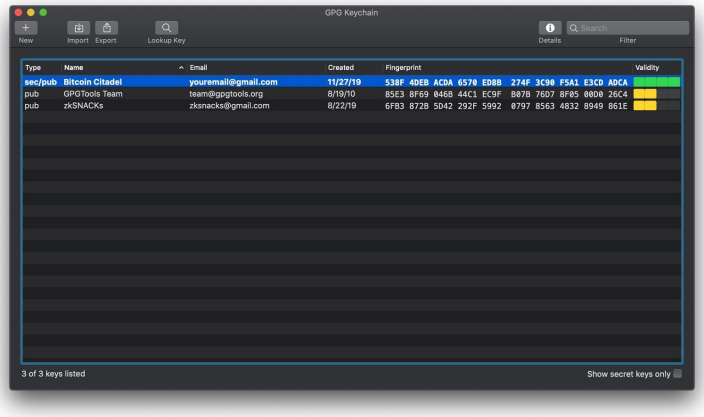



13) Open GPGTools which automatically recognizes it in your clipboard and add the key.

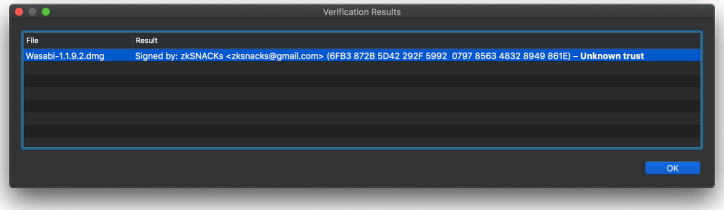



13a) *Optional* Ask someone you trust if it is the same key they have. (The fingerprint should be 6FB3 872B 5D42 292F 5992  0797 8563 4832 8949 861E)

14) You now have both Wasabi and gpgtools keys in your keychain. You don't need to read them in the future unless their keys change - which should be suspicious if that happens. So steps 7, 11, 12, and 13 only need to be done this first time.




15) Open the Wasabi signature file to verify the download.



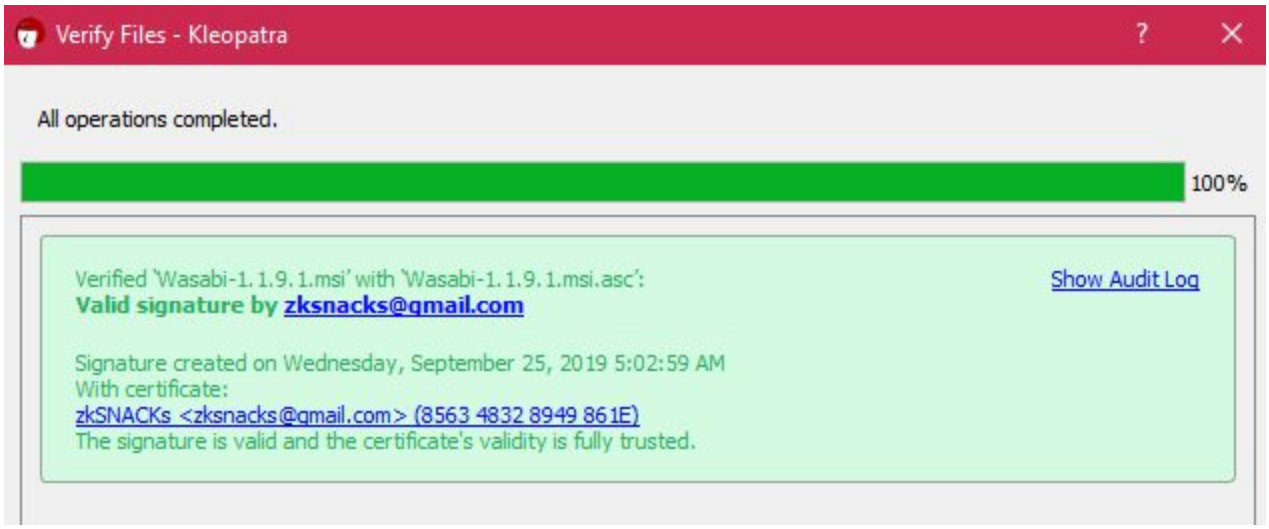

16) Always verify future upgrade downloads through this method before installation.

17) Install Wasabi.

## Verify PGP Signatures - Windows

1. Navigate to **https://gpg4win.org/download.html** and download GPG4Win.
2. Install it.
3. Open your Downloads folder where you previously downloaded the Wasabi Wallet executable and signature file. They must be located in the same folder.
4. Right click on the signature file (ends in **.msi.asc**) and choose **More GpgEX options > Verify**


5. A program called Kleopatra will open up with a prompt saying the data could not be verified. This is because you haven't imported zkSNACKs public key yet. Note the PGP fingerprint.
6. Click the **Search** button and Kleopatra will look for the public key matching the fingerprint. It should find the PGP key for **zkSNACKs@gmail.com**. Import it.
7. It'll ask you to certify the certificate for zkSNACKS. Make sure the fingerprint listed is: 6FB3 872B 5D42 292F 5992 0797 8563 4832 8949 861E
8. Once certified, it should be able to verify the file.




9. Install Wasabi.

# Additional Resources

*TFTC Guides: Coldcard + Wasabi Wallet Basic Setup and Usage*
https://www.youtube.com/watch?v=sM2uhyROpAQ

Anything you would ever want or need to know about the technical side of Bitcoin.
https://github.com/chaincodelabs/bitcoin-curriculum

# Stuck or have questions?

Keep your eyes peeled on http://btccitadel.org for updates or shoot us questions on Telegram (https://t.me/btcCITADEL) or on Twitter (https://twitter.com/btcCITADEL).

You can also find us individually on Twitter:
@evankaloudis
@awayslice
@matt_odell
@tikawamoto
@StopAndDecrypt
@pedromvpg
@martybent

Thanks to jimbo from the Citadel for providing feedback on the first draft of the document.

# The Fine Print

This document provides education as to privacy and security practices for a certain amount of Testnet Bitcoin. Said amount of Testnet Bitcoin has no value. Should you choose to apply the practices taught in this document to any Mainnet Bitcoin or any other digital asset you own now or may purchase in the future, you do so at your own risk and the Citadel shall in no event be liable for any financial loss suffered. Nothing shall be construed as providing consulting, financial advice or advice as to securing any digital asset of value.