Welcome to this lecture where we’ll be discussing the differences between hot and cold wallets in detail. This will help you understand just how these wallets are different!

We’ve talked a lot about hot and cold wallets in previously, and you might have already figured out what they mean, “hot wallets” are wallets where the private keys are on a device that’s facing the internet, and “cold wallets” are wallets where the private keys have never contacted an internet facing device.

You can see that the definition doesn’t quite cover all of the possible scenarios. For example, what if the private keys were created on a machine that faced the internet, but while it was offline, and the history was deleted from it before it came back online? Or what if you took a “cold” paper wallet, and plugged it into an online wallet?

Hot and cold wallets are indeed a sort of a spectrum, which is defined by how “sterile” the environment you’re using to generate and secure your keys is.

Let’s start with the easy part, hot wallets.

You download an app, create a new wallet, back up your seed as we’ve demonstrated, and bam! You’ve got yourself a properly backed up hot wallet. Very accessible and easy to transact with.

We recommend doing it on your mobile or tablet, because mobile operating systems are more modern than desktops, and most of them were designed with security in mind.

And now for the challenging part: making a strong protected cold wallet.

As we’ve said, cold wallets are a spectrum, and in this lecture we’re focused on giving you a great balance of very high level security, and a process that’s manageable even if you don’t have a lot of technical skills.

So, here’s how you can create a secure cold wallet:

1. Reset the device (always good to clear out the memory, for the paranoid, you can also go with a factory reset)

2. Download the recommended wallet app, BreadWallet from the app store or MyCelium from google play

3. Set your device to airplane mode (this turns off your connection to the internet)

4. Go into the app and generate a new wallet

5. Back up your seed on paper, with no one around, no cameras around, and type it into the app to make sure you backed it up correctly.

6. Copy a receiving address to your device.

7. Get out of the wallet app, go into your phone app settings and wipe the apps data.

8. Remove the app from your device

9. Restart the device

10. You may get out of airplane mode now, you’re done!

So now, what you have is a receiving address that’s backed up by a passphrase, which you have written on a piece of paper, and this has actually never faced the internet.

You can also search for your address in any blockchain explorer site, like blockchain.info, and see how much money it holds.

So now you’re holding a piece of paper that’s potentially worth a lot of money, and i know what you’re thinking, why won’t you tell us where to keep it?

Well, there’s bad news and good news here. The bad news is that this is the one thing we can’t, and potentially no one can teach you, this is where the protocol that is bitcoin end, and your personal responsibility begins.

You see, if there was a standard for where to hide your seed, very quickly thieves would catch on to this standard and that will become the first place they’ll look for.

Also, this may change depending on the situation you’re in. If you’re in a place where hurricanes hit year after year, the way you secure your seed backups will probably be very different then someone in other circumstances.

The good news is, we humans have a long history of securing papers and condensed value such as gold. From safes, to stories about buried treasures, to spy movies, and so on.

Be creative, but keep in mind that the number one reason people lose their cryptocurrency today, by far, is because they forget their passphrases, not when they are stolen.

Join me in the next lecture where I’ll be going over how to choose a trustworthy cryptocurrency exchange, when it comes to trading your tokens.