UNIVERSITY *of* NICOSIA

MSc in Digital Currency

DFIN-511: Introduction to Digital Currencies

Session 4
Bitcoin in Practice – Part 1
Bitcoin clients, online wallets, paper wallets, cold storage, sending and receiving

DFIN-511: Introduction to Digital Currencies

UNIVERSITY of NICOSIA

Objectives of Session 4

- ***Sessions 3, 4 and 5 are devoted to the more technical side of Bitcoin. Sessions 6, and 7 will discuss alternatives to the blockchain and Bitcoin. The other sessions will focus on the interfaces with the existing financial systems, innovation and the potential effect Bitcoin could have on the developing world.***
- ***For the non-technical, as we mentioned when introducing Session 3, you will have to get acquainted with a number of new concepts, bearing in mind the overall goal of the MOOC; to provide you with the framework and fundamentals of this emerging field.***
- The objectives for this session are to:
  - Understand the concept of Bitcoin wallets
  - Get an introduction on Bitcoin clients
  - Analyze how a Bitcoin transaction is performed using blockchain.info
  - Learn about the concepts of “cold storage” and “paper wallets”

Agenda

1. Bitcoin/Crypto wallets
2. Clients
3. Wallet Protection
4. Cold storage – Hardware and Paper wallets
5. Conclusions
6. Further Reading

1. Bitcoin/Crypto Wallets

Fun Facts

- Almost 33 million Blockchain Bitcoin Wallets have been created compared to 17 million a year ago

- Coinbase announced 13 million users by early 2018. Approximately 5% of Americans own Bitcoin/Crypto.

- Bitcoin market capitalization is approximately $60B. Have reached $320B a year ago.

- Not all of these funds are participating in transactions

- Poor user management can lead to loss of passwords, private keys, theft of coins etc.

Bitcoin/Crypto Wallets

“A wallet is software that holds all your addresses. Use it to send bitcoins and manage your keys.”

(from Antonopoulos, Mastering Bitcoin)

- As described in Session 3, bitcoin ownership is established through digital keys and digital signatures.

- These keys are generated locally on Bitcoin end-users’ computers using special software called a Bitcoin client. They can be stored in a file, in a database, or just printed on a piece of paper, but most commonly they are stored in a ***Bitcoin wallet.***

- The keys within each user’s wallet allow the user to sign transactions, thereby providing cryptographic proof of the ownership of the bitcoins sourced by the transaction.

- Keep in mind that if you ***don’t know who generates your private keys, where they are stored, or if someone else has them (as when using a cryptocurrency exchange), they are not actually yours,*** as seen in the case of Mt.Gox, which discontinued operations in February 2014.

Bitcoin/Crypto Wallets

“Like email addresses, Bitcoin addresses can be shared with other Bitcoin users who can use them to send bitcoins directly to your wallet.

Unlike email addresses, you can create new addresses as often as you like, all of which will direct funds to your wallet.

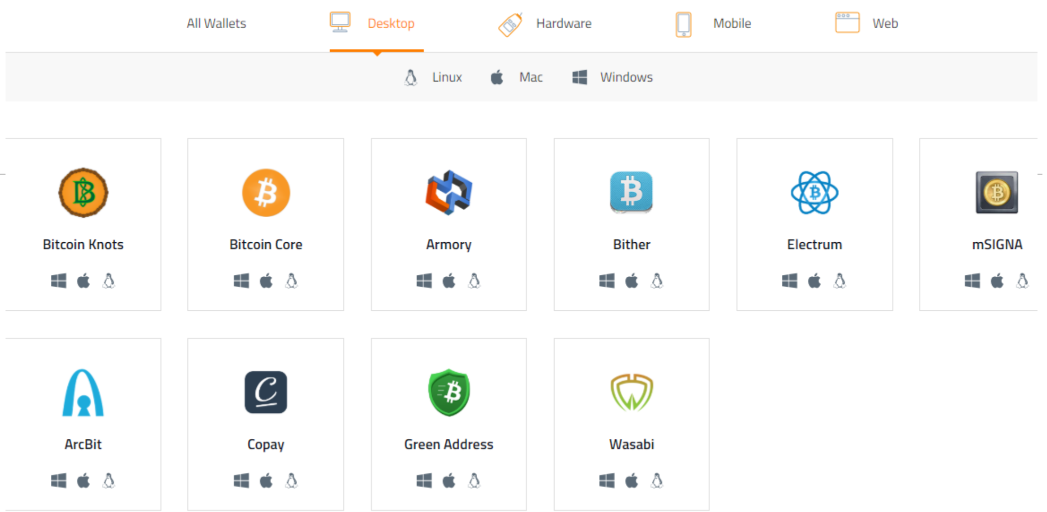
A wallet is simply a collection of addresses and the keys that unlock the funds within.

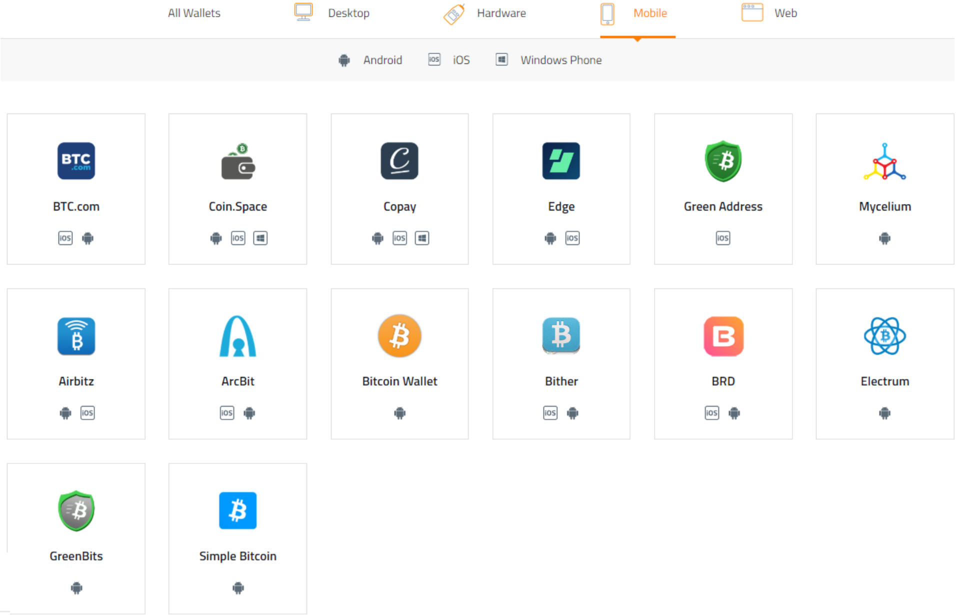
There is practically no limit to the number of addresses a user can create.”

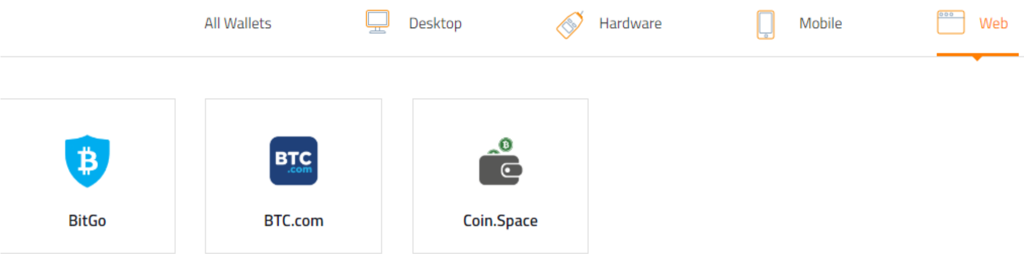
(from Antonopoulos, Mastering Bitcoin)

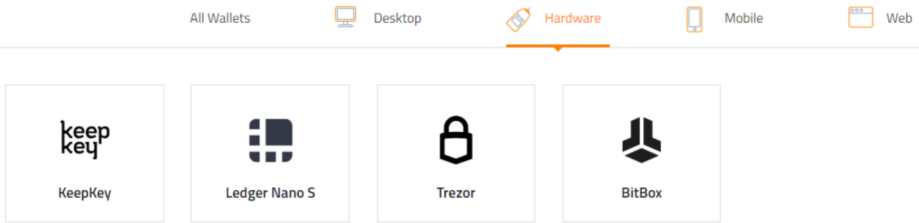
Bitcoin/Crypto Wallets

- In this session we will explore various types of wallets/clients (web, desktop, mobile, hardware, paper). An individual may choose which wallet better suits his/her needs.
- Selection of a wallet/client type depends upon an individual's amount of funds committed, IT proficiency, type of mobile device, desired frequency of transactions, willingness to give up security responsibilities to third parties, which cryptocurrencies are aimed to be transacted etc. https://bitcoin.org/en/choose-your-wallet









2. Clients

Clients

There are different types of Bitcoin clients:

- Full client
- Web client
- Lightweight client
- Mobile client

Image source: bitcoinargentina.org

Bitcoin Clients

- We have been using the terms Bitcoin *"wallet"* and *"client"* interchangeably since this is what most people tend to do. Let's distinguish wallets and clients as follows:
  - A **wallet** is a collection of data (e.g. the Bitcoin user's private/public key-pair and his address) enabling a user to receive and send bitcoins, in the form of spendable outputs.
  - A **client** is the **software** that connects a user to the Bitcoin network. It handles all the communication, updates the wallet with incoming funds and uses information from the wallet to sign outgoing transactions.

http://bitcoin.stackexchange.com/questions/20487/whats-the-difference-between-a-bitcoin-client-and-wallet

Bitcoin Clients

- A **Full client**, or "full node" is a client that stores the entire history of Bitcoin transactions, manages the user's wallets and can initiate transactions directly on the Bitcoin network. This is similar to a standalone email server, in that it handles all aspects of the protocol without relying on any other servers or third-party services. In full clients, the private keys are never communicated and are stored locally.
- A **Lightweight client** stores the user's wallet but relies on third-party owned servers for access to the Bitcoin transactions and network. The lightweight client does not store a full copy of all transactions and therefore must trust the third-party servers for transaction validation. This is similar to a standalone email client that connects to a mail server for access to a mailbox, in that it relies on a third party for interactions with the network. Lightweight clients store private keys locally, just like full clients.

- Node=a point on a network contributing towards validating transactions – in this case your computer

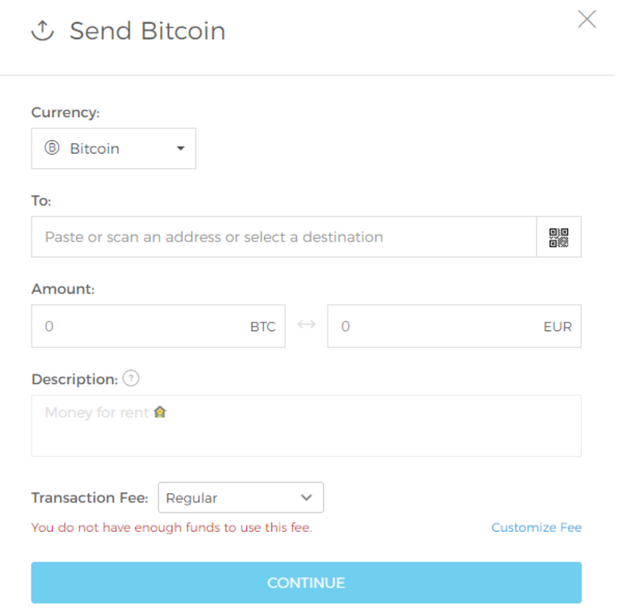
Bitcoin Clients

- A **Web client** is accessed through a web browser and stores the user’s wallet on a server owned by a third-party. This is similar to webmail, in that it relies entirely on a third-party server. Some web clients are just an interface with the service’s servers (e.g. Coinbase) where the private keys are stored, and others (e.g. Blockchain.info, greenaddress.io) also store the users’ private keys encrypted, but only the user can decrypt them locally on his computer.

- A **Mobile client**, usually used on smartphones, can either operate as a full client, a lightweight client, or a web client. Some mobile clients are synchronized with a web or desktop client, providing a multi-platform wallet across multiple devices, with a common source of funds.

Get started with a web wallet

- This is the easiest way to start using Bitcoin. We highly recommend that everyone creates at least one web(online) wallet.
- How to create a web wallet:
  - Navigate to a web wallet provider such as https://blockchain.info/
  - Click on option “Get a Free Wallet”
  - Sign up for a free wallet by providing your username and choose a secure password
  - BTC, Ether and BCH can be exchanged and stored
  - Explore wallet options for advanced security such as recovery phrase, Google authenticator etc.



Send Bitcoin

Currency: Bitcoin

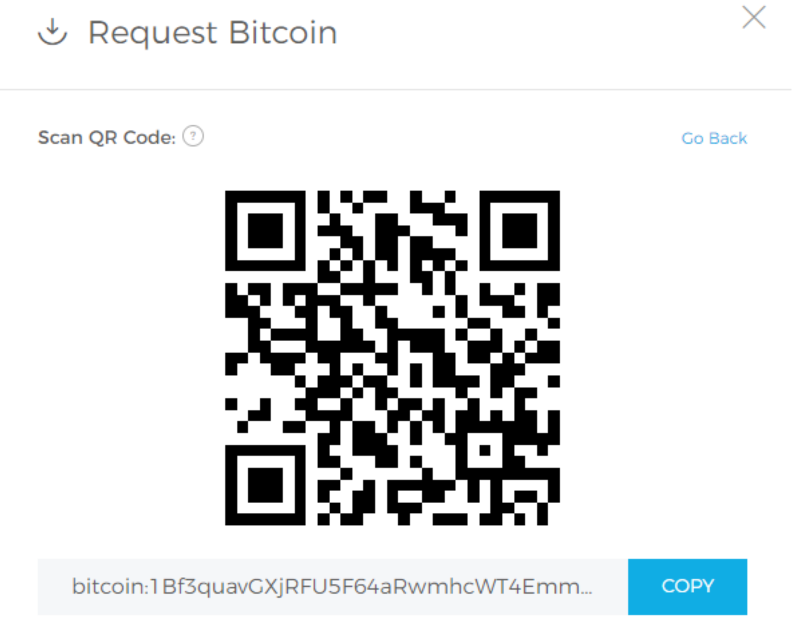
To: Paste or scan an address or select a destination

Amount: 0 BTC ↔ 0 EUR

Description: Money for rent 🏠

Transaction Fee: Regular

You do not have enough funds to use this fee.



Request Bitcoin

Scan QR Code:

bitcoin:1Bf3quavGXjRFU5F64aRwmhcWT4Emm...

3. Wallet Protection

Sending and Receiving Bitcoins

- There are few ways for you to get your first bitcoins:

  - **Offer a Service or Product for bitcoins**. There are many ways you can go about this and many businesses and individuals already accept bitcoins.
  - **Accept bitcoins as a donation** e.g. if you are running a charity.
  - **Purchase bitcoins through an Exchange** e.g. to get relatively large amounts of bitcoins at the current market price. A very comprehensive list of Bitcoin exchanges, categorized by country, can be found here. Identity verification will typically be required before you can buy/sell bitcoins and deposit/withdraw fiat currencies. Thus, it might take some time.

- Another way of getting bitcoins is through faucets. A list of faucets can be found here: http://www.bit-sites.com/p/best-bitcoin-faucets-2017.html You may get a few bits (1/1,000,000 of a BTC) for free, however, most faucets are not operational anymore. Be very wary of faucets promising bitcoins in exchange for some kind of activity from you.

Sending and Receiving Bitcoins/Cryptocurrencies

- When first created, a Bitcoin/cryptocurrency wallet is empty.
- In order to receive some bitcoins or another cryptocurrency you have to inform the sender about your wallet’s address, just like we would provide our email address to someone who wants to send us an email.
- In this case, to send bitcoins, a sender can just copy and paste the receiver’s address: e.g. 1NmCXMB8R8y1ewiPs2zKF7Me7tbkLeVG4i
- If the sender is using a mobile wallet, it could be more convenient to scan the relevant QR code

- After every transaction is confirmed, it becomes a part of Bitcoin history, and is included in the public ledger, i.e. the **blockchain**.
- Each transaction corresponds to a chain of ownership transfer and is maintained in a distributed, peer to peer network of Bitcoin nodes.

Get your funds OUT of exchanges

- Avoid storing your cryptocurrencies with an **exchange**, even for a limited amount of time, it exposes you to many dangers. Storing funds in an exchange is similar to storing funds in a bank. It may sound safe but there is some exposure since a third party has control over your funds.
- Third-party risks include:
  - **Fraud** (your provider may not be so trusted after all),
  - **Security** (many providers have been victims of security attacks in the past),
  - **Financial health** (if you provider fails, your wealth may be lost, too).
- Use it only for day-to-day small amount transactions and enable **2-factor authentication** from the security settings.

Web Wallets

- **Least secure choice**, after exchanges

- Examples: *BitGo, Green Address, Coinbase, Xapo, BTC Wallet, Blockchain*
  - Web wallets store your private key(i.e. password) for you on their servers
  - May come by a mobile application or using your browser on a personal computer

  - Easy access to your coins from any device
  - Some of them are attached to exchanges and offer additional security such as offline storage – *Coinbase does both*

  - You are trusting a company not to steal your funds and disappear
  - You are trusting a company to keep your funds safe from attacks

Desktop Wallets

- Software downloaded and installed on a PC or laptop.
  - Complete control over your coins
  - No third-party is able to steal your coins.

- **Desktop wallets** can be **full nodes***(such as *Bitcoin Core*). i.e. the whole blockchain is downloaded on your computer and kept up to date, contributing to the maintenance of the decentralized Bitcoin network and its consensus by verifying transactions itself
  - Acceptable levels of control and protection, especially if private keys are **encrypted** with strong passphrases and regularly **backed up**.
  - More rewarding for hackers to target central servers to steal many people's coins than to target each individual's computer

  - Still a bit vulnerable to Internet attacks, such as **spying, malware or computer malfunctions. Do not let anyone steal or hack your computer.**
  - It takes ages to download and can be a hassle to keep update or synchronized with the rest of the network.
  - Regular users do not need to be full nodes as it reduces your hard drive capacity.

- **Desktop wallets** can be **lightweight** (such as *Electrum, see next page*): only a part (headers) of the Blockchain is downloaded – then connect to full nodes and only receive transactions that are needed for their operations.
  - All the advantages of a desktop wallet without the hassle of running a full node - less hard disk space and less bandwidth compared to a full node. Private key is held on your computer, meaning that you retain complete control.
  - Some (e.g. Jaxx) can hold a wide range of assets

  - Cannot verify transactions as it does not store a full copy of all transactions. Therefore must trust the third-party servers that they access the Bitcoin network and not a malicious third party which might spy your transactions.
  - Still a bit vulnerable to Internet attacks, such as **spying, malware or computer malfunctions. Do not let anyone steal or hack your computer.**

Lightweight Client - Electrum

- Electrum is one of the clients that enhances speed as the servers used are indexing the Bitcoin blockchain. Electrum has the following features:
  - It is available on Windows, MacOS, Linux and Android
  - It makes performing Bitcoin transactions quick and simple
  - It is free to download and is open source under the MIT license
  - It supports cold storage and multisig technology
- In addition, Electrum is easy to install:
  - Go to https://electrum.org/#download
  - Download the appropriate installer (Optional: you can verify the PGP signature)
  - Run the installer
  - Run the Electrum client 16

https://blog.coingate.com/2017/02/setup-electrum-guide/

Mobile Wallets

- Installed on a mobile device (examples: ***breadwallet*** **for iOS** and ***Coinomi*** **for Android**) – usually operate as a lightweight client or a web client
  - Portable, easy and comfortable - The smartphone’s camera scans the QR code of the receiver/merchant and transfers the coins.
  - Good for day-to-day transactions
  - If mobile device is lost or stolen the funds are not gone, backups can help you access your funds. **Backups** are required by most wallets.(usually a 12 word mnemonic phrase)
  - If the battery is too low, or the device is switched off the payments are affected.
  - Do not type your PIN when the device is visible to others and do not lose mobile & backup phrase
  - Choose secure-proven wallets. http://www.newsbtc.com/2017/06/11/anyone-can-extract-jaxx-wallet-mnemonic-seed-developers-will-not-fix-problem/

4. Cold storage – Hardware and Paper wallets

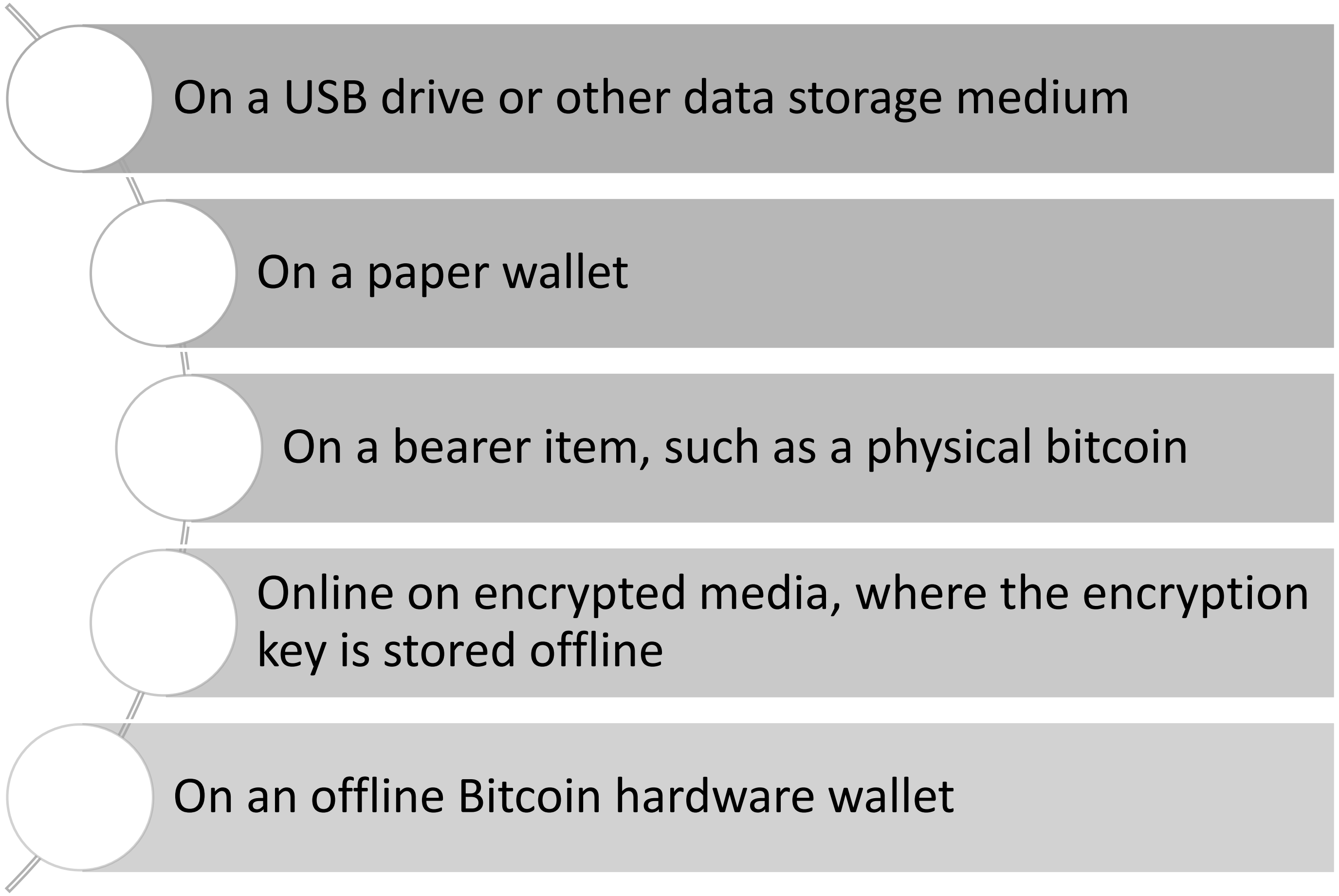
Cold and Colder Storage

“Cold storage in the context of Bitcoin refers to keeping a reserve of bitcoins offline”

(from the Bitcoin Wiki)

- Keeping your private keys offline is arguably one the best ways to protect them.
- This can happen in a number of ways, depending on whether the medium of key storage comes into contact with the Internet or other connected devices.
- **“True cold storage”** means that the private keys have never been on a networked computer or device, i.e. they have been **generated offline and without intermediaries.** The signing of outgoing transactions (signed with those keys) also **occurs offline**. This method is more common for long-term storage of large funds that you will not be sending out very frequently, as it is generally impractical for everyday use. You can still safely use the addresses to send bitcoins to them, as well as to check their balances.
- **“Conventional cold storage”** usually refers to an offline medium for storing bitcoins that only goes online to sign transactions. This is an intermediate security step that is more practical, **but might still expose the keys to threats.**

Cold Storage



On a USB drive or other data storage medium

On a paper wallet

On a bearer item, such as a physical bitcoin

Online on encrypted media, where the encryption key is stored offline

On an offline Bitcoin hardware wallet

Hardware Wallets

- Act as a safe lockbox. Examples: (Trezor, Ledger Nano)

  - Provide extra security and fault tolerance as they are not connected anywhere and cannot be hacked like a computer
  - Private keys generated, stored within the device and never leave the device
  - Transactions signed within a PIN protected external device – does not need to be imported to software
  - **Backups** are required by most wallets.(usually a 12 word mnemonic phrase)

  - Less convenience than desktop and mobile wallets
  - Make sure you do not lose both the device and the mnemonic phrase
  - Price – Also make sure you buy from original stores to avoid the danger of a compromised shipment

An interesting comparison between most wallet types and a hardware wallet like Trezor, can be found here.

Paper Wallets

“A paper wallet is a mechanism for storing bitcoins offline as a physical document or object that can be secured.

Paper wallets are generally created by printing a brand new public address and private key onto paper, and then sending bitcoins from a "live" wallet to the printed wallet's public address for safekeeping.”

(from the Bitcoin Wiki)

A **“paper wallet”** consists of two components:

- The public address, which has to be available to anyone that wants to send bitcoins to you
- The private key, which is the key you need in order to use, spend your own bitcoins

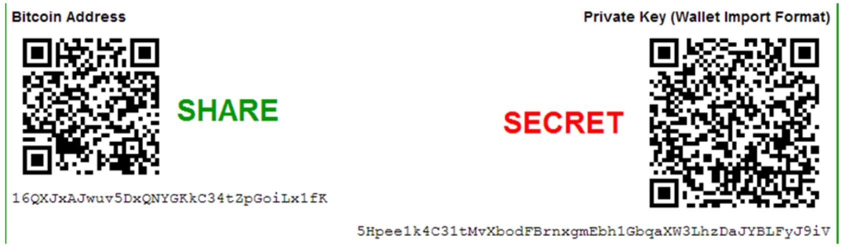
Paper Wallets

- Documents that contain pairs of public and private keys. Must be stored on a safe place, make at least 2 copies.
  - Maximum protection from cyber-attacks/hardware failures/operating system errors/breakdowns etc.
  - Ideal for long term storage of funds or gifts
  - Easily generated, printed

  - Loss, theft, paper degrading, destruction e.g. water
  - Must be imported to software at some time, unlike hardware wallets
  - When withdrawing part of your funds, you risk losing the remaining balance, because of the way Bitcoin treats change in transactions. For details, see this discussion. https://www.reddit.com/r/Bitcoin/comments/1c9xr7/psa_using_paper_wallets_understanding_change/

  Tip: always check your balances online before storing or destroying a paper wallet.
- Make sure you are working offline when generating a paper wallet!
- Use multiple paper wallets; i.e. generate a different wallet for expenses that you pay using bitcoins, and use different ones for long term storage of bitcoins

1KezyKE3zKYesKttaEsUQBSb76q3swdZuX
PUBLIC ADDRESS
bitcoin
DEPOSIT / VERIFY
1KezyKE3zKYesKttaEsUQBSb76q3swdZuX
PRIVATE KEY / WITHDRAW



Bitcoin Address

16QXJxAJwuv5DxQNYGKkC34tZpGoiLx1fK

Private Key (Wallet Import Format)

5Hpee1k4C31tMvXbodFBrnxgmEbh1GbqaXW3LhzDaJYBLFyJ9iV

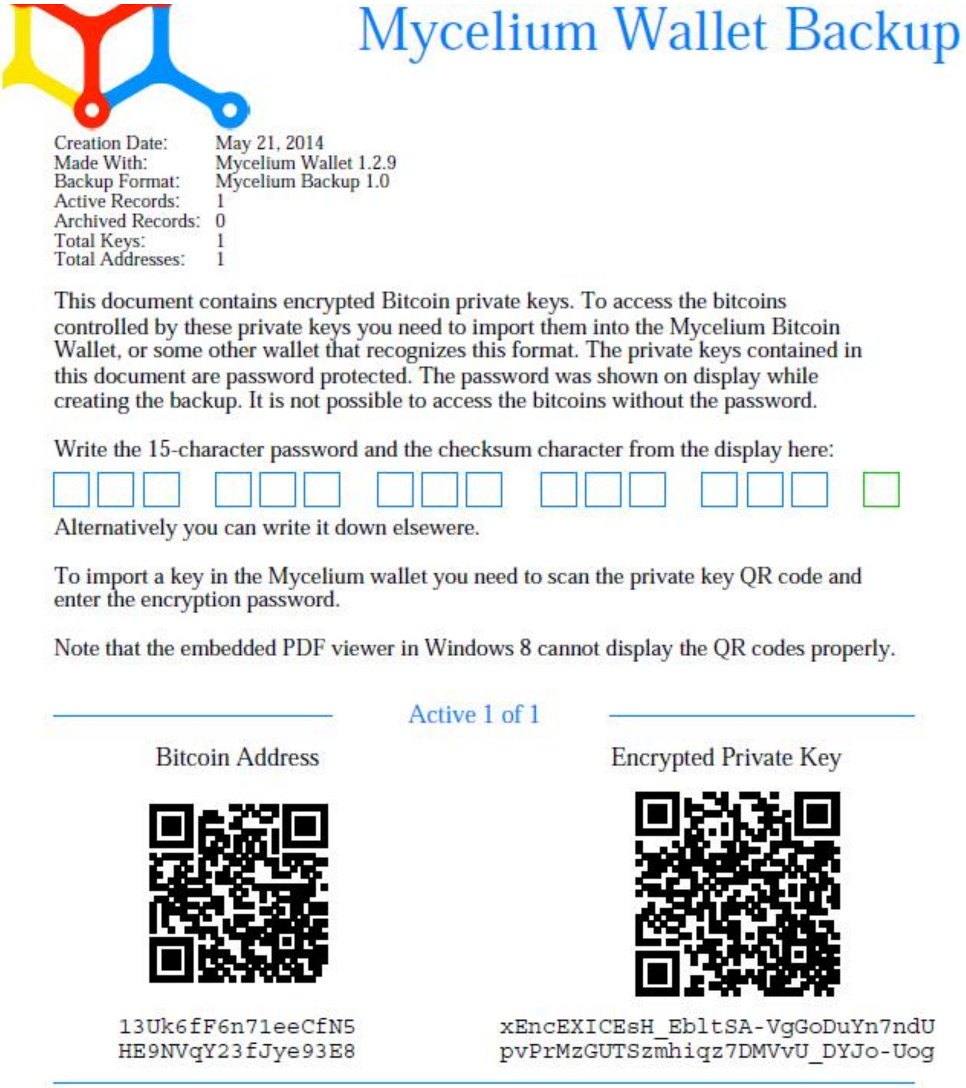
Paper Wallets

- An encrypted paper wallet should appear as on the right (generated here using the Mycelium Android wallet). We can share this wallet freely, since the private keys are encrypted.

- Only the owner of bitcoins (who knows the password) can decrypt the wallet and gain access to the private keys. This paper wallet can also be used to receive bitcoins by scanning the QR code shown bottom-left (i.e. the public address).

- A copy of this presentation can also be used as a backup by its owner in case all other copies have been destroyed!

- Newer users of Mycelium also have access to HD accounts, which provide additional features (BIP 32/44 and 39) and use **Seed phrases** instead of passwords.



Mycelium Wallet Backup

Creation Date:	May 21, 2014
Made With:	Mycelium Wallet 1.2.9
Backup Format:	Mycelium Backup 1.0
Active Records:	1
Archived Records:	0
Total Keys:	1
Total Addresses:	1

This document contains encrypted Bitcoin private keys. To access the bitcoins controlled by these private keys you need to import them into the Mycelium Bitcoin Wallet, or some other wallet that recognizes this format. The private keys contained in this document are password protected. The password was shown on display while creating the backup. It is not possible to access the bitcoins without the password.

Write the 15-character password and the checksum character from the display here:

□□□ □□□ □□□ □□□ □□□ □

Alternatively you can write it down elsewere.

To import a key in the Mycelium wallet you need to scan the private key QR code and enter the encryption password.

Note that the embedded PDF viewer in Windows 8 cannot display the QR codes properly.

Active 1 of 1

Bitcoin Address

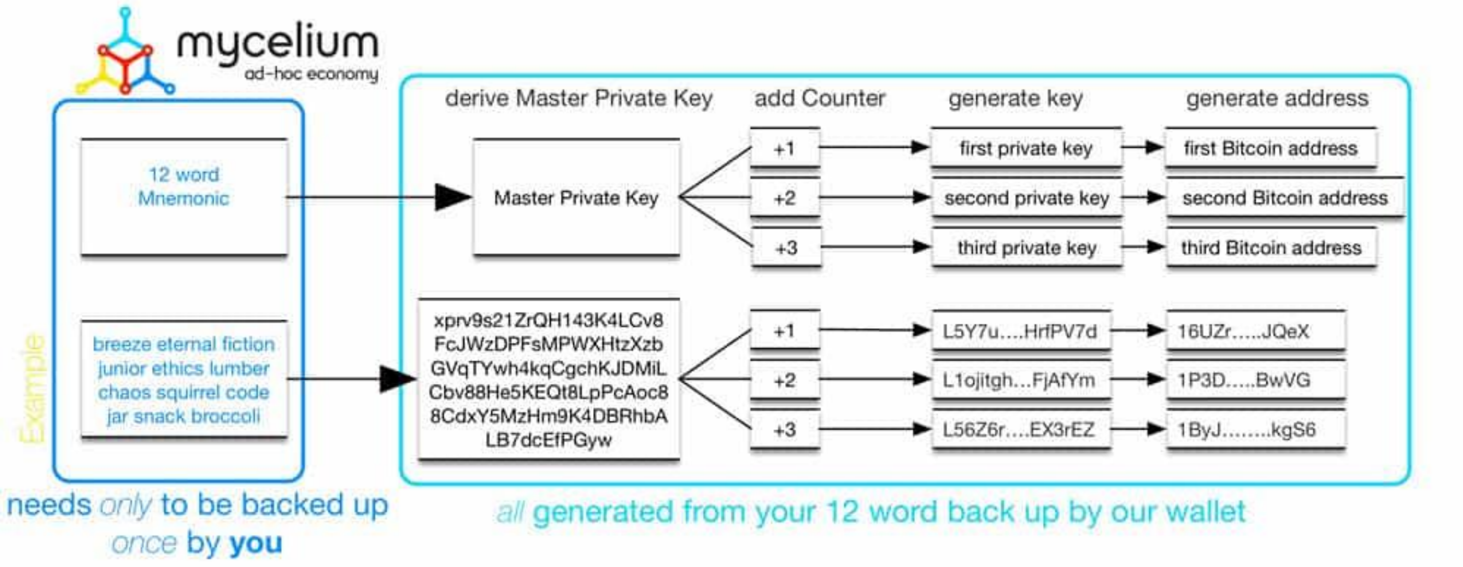
13Uk6fF6n71eeCfN5
HE9NVqY23fJye93E8

Encrypted Private Key

xEncEXICEsH_EbltSA-VgGoDuYn7ndU
pvPrMzGUTSzmhiqz7DMVvU_DYJo-Uog

Hierarchical Deterministic (HD) Wallets

- HD wallets allow the pattern of public/private keys to be generated by only backing up the wallet (e.g. via the 12 world mnemonic) once. The backing up is mandatory.
- New addresses are derived hierarchically and sequentially from a single master seed.
- HD wallets generate a hierarchical tree-like structure of keys which start from the seed master key based on BIP 32. When you restore an HD wallet using the seed key, the wallet goes ahead and drives all the private keys of the tree using BIP 32.
- Since this mechanism allows many receiving addresses to be generated, it enhances more privacy.
- Examples include the majority of wallets like Coinomi, Mycelium, Jaxx, Electrum and all the hardware wallets.



https://coinsutra.com/hd-wallets-deterministic-wallet/

Secure your wallet, no matter what type it is!

- Some ways of securing your wallet include:
  - Avoiding (if possible) the use of online services. When using web clients that generate private keys for you, it is most advisable to save that page and generate the private keys offline. You can use a site like www.bitaddress.org for generating private keys (offline) and printing a BIP38 encrypted paper wallet from it.
  - If using several wallets, some wallets can be used for everyday use (e.g. smaller expenses) and some for storing large quantities of bitcoins; the remaining wallets can be stored offline as paper wallets.
  - Backing up your wallets regularly, following the 3-2-1 rule (3 copies, 2 mediums, 1 off-site)
  - Encrypting your wallet. Most services that provide paper wallet creation commonly allow for an encryption method. An added measure would be to split the keys in an “m of n” manner like Shamir's secret sharing scheme (SSSS). “m” copies out of “n” must be used together to synthesize the full private keys, while individual copies cannot be compromised, even if they are exposed.

- **Finally, always keep your Bitcoin software up to date!**

4. Conclusions

Conclusions

- The Bitcoin client is an end-user software that provides access to the Bitcoin network.
- Each Bitcoin wallet stores keys and signs Bitcoin transactions.
- Full clients maintain the entire Bitcoin ledger (i.e. transaction history) and, are therefore able to verify transactions.
- Lightweight clients do not store the blockchain locally and are therefore unable to verify transactions; instead they must rely on third-party servers.
- Securing bitcoins may involve cold storage (e.g. using USB flash drives, offline hardware wallets, paper wallets, etc.) and wallet encryption.

Conclusions

- Both novice and experienced users should pay attention to securing their digital wealth.
- Proper measures of protection require significant investments in time and care.
- **Important tips:**
  - **Select an exchange which suits your needs**
  - **Do not keep funds with the exchange**
  - **Select one or more types of wallets which suit your needs.**
  - **At least a hardware wallet is essential if you own a significant amount of cryptocurrency funds.**
  - **Encrypt your wallet (Encryption is provided as standard in most wallets and must be used at all times –even for small balances. Encrypting basically means choosing a password that provides access to your funds). NEVER FORGET YOUR PASSWORD**
  - **Backup your wallet (Also a process offered by all wallet types)**
- The next session will discuss full clients, transaction processing and mining in Bitcoin.

5. Further Reading

Further Reading

On wallets comparison:

- Satoshi Labs

http://doc.satoshilabs.com/trezor-faq/_images/compared_to.png

On wallet protection:

- Securing your wallet: Practical advice from bitcoin.org

https://bitcoin.org/en/secure-your-wallet

- How to store your Bitcoins: An overview of wallet types by Coindesk

http://www.coindesk.com/information/how-to-store-your-bitcoins/

- Securing your Digital Wealth – Andreas Vlachos on IFXEXPO Conference

https://www.youtube.com/watch?v=uJpQGGD49zw

On hardware wallets:

- Hardware wallets - Coindesk

https://www.hongkiat.com/blog/setup-trezor-beginner/

https://www.coindesk.com/ledger-to-ledger-hardware-wallet-integrates-with-decentralized-exchange/

Some wallet best practices:

- https://www.cryptocoinsnews.com/bitcoin-wallet-security-best-practices/

On multi-sig: (not presented in this session but good to know)

- Multisignature - Wikipedia

https://en.bitcoin.it/wiki/Multisignature

UNIVERSITY of NICOSIA

Questions?

Contact us:

Twitter: @mscdigital
Course Support: digitalcurrency@unic.ac.cy
IT & Live Session support: dl.it@unic.ac.cy