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

- 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”

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.

Agenda

1. Bitcoin wallets
2. Bitcoin clients
3. Sending and receiving bitcoins
4. Cold storage
5. Paper wallets
6. Conclusions
7. Further Reading

1. Bitcoin wallets

Bitcoin 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 an exchange site), **they are not actually yours**, as seen in the case of MtGox, which discontinued operations in February 2014.*

Bitcoin 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.

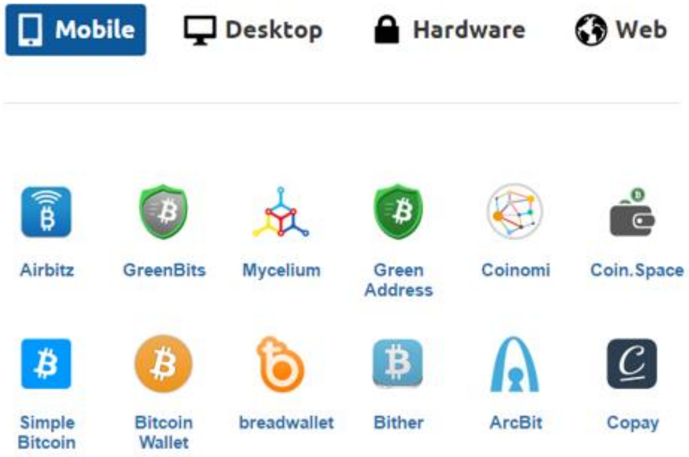
A wallet is simply a collection of addresses and the keys that unlock the funds within*.*

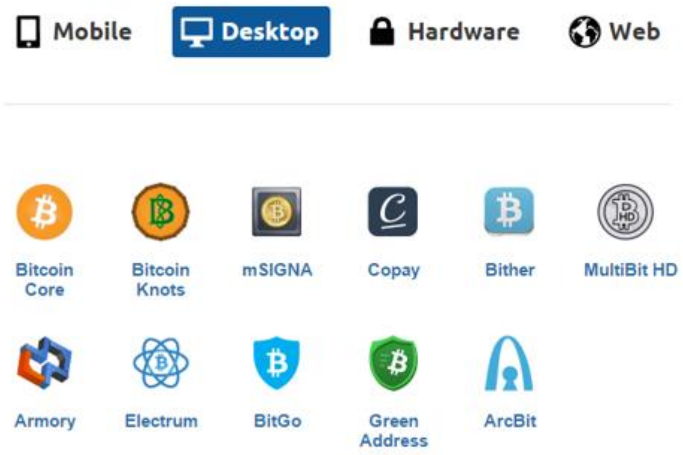
There is practically no limit to the number of addresses a user can create."

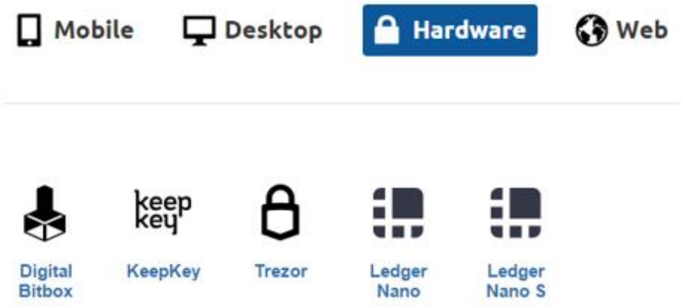
(from Antonopoulos, Mastering Bitcoin)

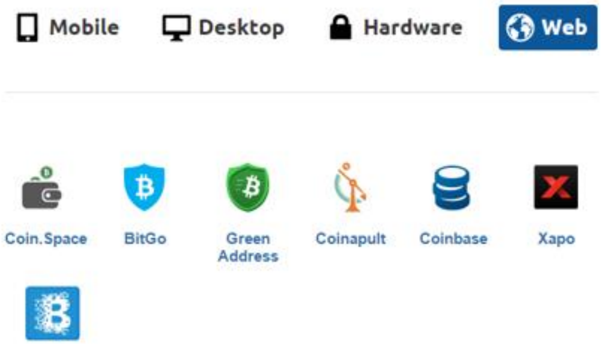
Bitcoin wallets

Today, there are lots of different wallet solutions, allowing users to choose what best suits them, for example:









https://bitcoin.org/en/choose-your-wallet and https://www.bitcoin.com/choose-your-wallet

2. Bitcoin clients

Bitcoin clients

- There are different types of Bitcoin clients:
  - Full client
  - Web client
  - Lightweight client
  - Mobile client

Image source: bitcoinargentina.org

Bitcoin clients

The terms Bitcoin "*wallet*" and "*client*" are sometimes used interchangeably. However, for this course we are going to 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

There are several types of 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 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.

Bitcoin clients

There are several types of Bitcoin clients:

- 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.

- 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.

A “Key” Choice

Having your keys stored locally or remotely (i.e. on a third-party’s server) is a question that depends on your Bitcoin wallet and client choice. Bear in mind that, the security of your funds also heavily depends on this choice, thus your decision must be made carefully. Below we examine some of the pros and cons of storing your wallet locally or remotely.

Locally: If your computer is compromised by a hacker, if it crashes (and you have no backups), or if you forget your passwords, your private keys (and bitcoins) will most probably be lost forever! However, if you take reasonable steps to avoid intrusion or exposure, your keys will be reasonably safe and protected from third-party failure or intent. In this case, you exchange convenience for increased security.

Remotely: If the third-party exchange’s security is compromised, or if they act maliciously, your bitcoins will most probably be lost forever! Bitcoin exchanges are not Banks. Most will provide a method of changing your passwords if you forget them, and employ security experts and suitable infrastructure, so you will not have to worry about taking extensive security measures. However, third-party exchanges are more likely targets for intruders, and if compromised, they could steal your bitcoins. In this case you exchange security for increased convenience.

Bitcoin clients – web client

Let’s see a short demo. It will show how to create a web wallet. This is the easiest way to start using Bitcoin. We highly recommend that everyone creates at least one web wallet.

Click on the video to continue :

This is a time to start using Bitcoin. The easiest way is to create online wallet. There are many ways. We are goint to use Blockchain.

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

(https://multibit.org/)

3. Sending and Receiving bitcoins

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: https://99bitcoins.com/top-10-bitcoin-faucets/.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

- When first created, a Bitcoin wallet is empty.

In order to receive some bitcoins we have to inform the sender about your wallet’s Bitcoin address, just like we would provide our email address to someone who wants to send us an email. To send bitcoins e.g. when using a desktop client, a sender can just copy and paste the receiver’s address:

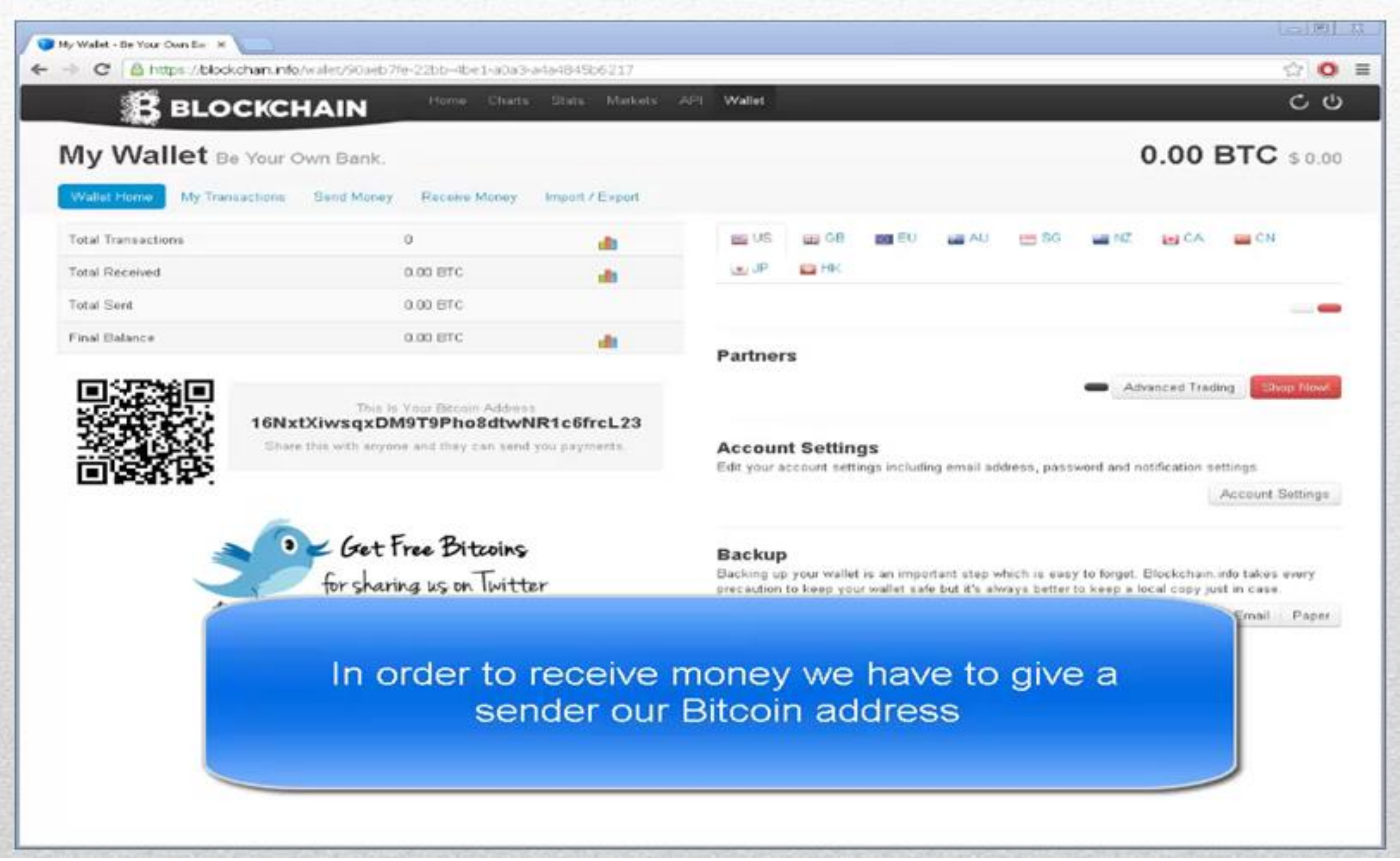
16NxtXiwsqxDM9T9Pho8dtwNR1c6frcL23

- If the sender is using a mobile client, it could be more convenient to scan the relevant QR code:

- For example, we will send a few mBits (1/1000 BTC) to our new wallet.

Sending and Receiving bitcoins

Click on the video to continue:



My Wallet Be Your Own Bank.

0.00 BTC $ 0.00

Total Transactions	0
Total Received	0.00 BTC
Total Sent	0.00 BTC
Final Balance	0.00 BTC

This Is Your Bitcoin Address

16NxtXiwsqxDM9T9Pho8dtwNR1c6frcL23

Share this with anyone and they can send you payments.

Partners

Account Settings

Edit your account settings including email address, password and notification settings.

Backup

Backing up your wallet is an important step which is easy to forget. Blockchain.info takes every precaution to keep your wallet safe but it's always better to keep a local copy just in case.

In order to receive money we have to give a sender our Bitcoin address

Image source https://news.bitcoin.com

Sending and Receiving bitcoins

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.

4. Cold storage

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

Methods of cold storage include keeping bitcoins:

- 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

Hardware wallets like the Trezor, provide extra security and fault tolerance against compromised computers or untrusted connections. They accomplish this by having the private keys generated, stored and the transactions signed within a PIN protected external device. You can also backup your keys in encrypted paper wallets in case the device is destroyed.

Even if your computer is compromised, you can deny signing any transactions you don't recognize and your PIN is protected from keyloggers as it doesn't leave the device.

Others devices available are the HW.1 and Ledger nano hardware wallets, providing a cheaper, simpler and more practical alternative to Trezor, but with slightly limited security features. It may be more convenient to think of these devices, as a safe (Trezor) and a lockbox (HW.1 and Ledger nano) in terms or price, convenience and security.

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

5. Paper wallets

Paper wallet

"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 wallet

- Why do you need a paper wallet? You may use a paper wallet to:
  - Protect against hackers’ attacks / lack of security when transactions take place online
  - Protect against fatal software / operating system errors / break downs
  - Ensure long-term, offline storage and absolute ownership of your private keys
  - Give the paper wallet, with the bitcoins, as a gift :)

- Obvious drawback:
  - A paper wallet is a tangible asset, thus it is more vulnerable to theft. As with cash, to be able to use/spend your coins you must make sure that you keep the paper wallet physically secure (and/or otherwise encrypted)

- Best practices:
  - 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

More here: https://en.bitcoin.it/wiki/How_to_set_up_a_secure_offline_savings_wallet

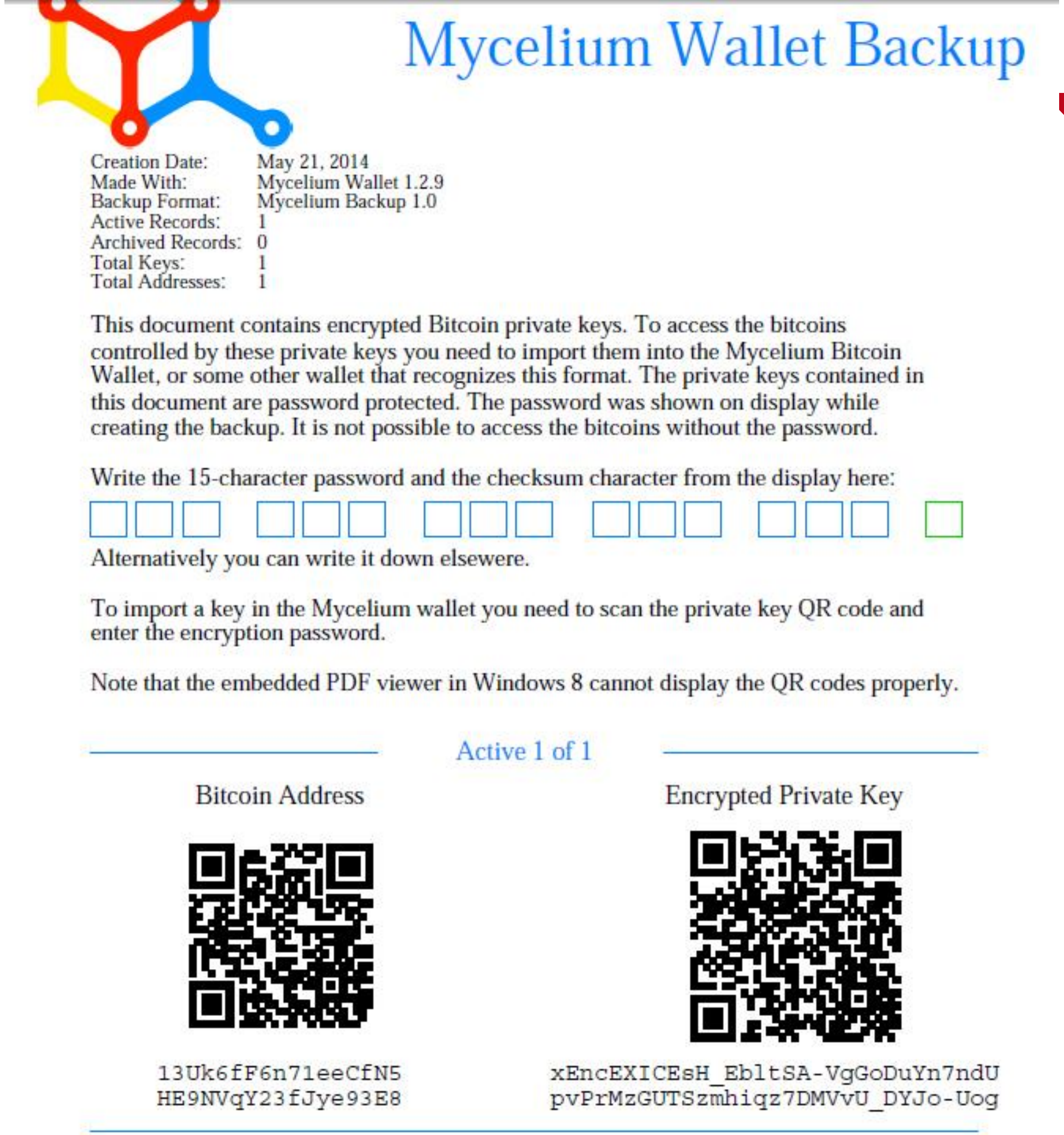
Secure your wallet

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!

Sending and Receiving bitcoins



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	Encrypted Private Key
13Uk6fF6n71eeCfN5 HE9NVqY23fJye93E8	xEncEXICEsH_EbltSA-VgGoDuYn7ndU pvPrMzGUTSzmhiqz7DMVvU_DYJo-Uog

An encrypted paper wallet should appear as on the left (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.

5. 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.
- The next session will discuss full clients, transaction processing and mining in Bitcoin.

6. Further Reading

Some Further Reading

- **Bitcoin: A Peer-to-Peer Electronic Cash System**, Satoshi Nakamoto https://bitcoin.org/bitcoin.pdf
  (Satoshi Nakamoto's original Bitcoin paper)
- **Mastering Bitcoin**, Andreas M. Antonopoulos, https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf
  (A text book introducing Bitcoin though storytelling)
- **Bitcoin Wiki** https://en.bitcoin.it/
- Blockchain.info http://blockchain.info/
- Choose your Bitcoin wallet https://bitcoin.org/en/choose-your-wallet
- Electrum https://electrum.org/#home
- BitGo https://www.bitgo.com/
- Green Address https://greenaddress.it/en/
- Bitcoin.org (securing your wallets) https://bitcoin.org/en/secure-your-wallet
- 99bitcoins.com (wallet reviews) https://99bitcoins.com/best-bitcoin-wallet-2015-bitcoin-wallets-comparison-review/
- Some wallet best practices https://www.cryptocoinsnews.com/bitcoin-wallet-security-best-practices/

UNIVERSITY *of* NICOSIA

Questions?

Contact us:

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