UNIVERSITY of NICOSIA

Session 4

Bitcoin in Practice – Part 1

Bitcoin clients, online wallets, cold storage, sending, & receiving

DFIN 511: Introduction to Digital Currencies

Session 4: Objectives

Objectives

- An overview of how exchanges and wallets work
- Get an introduction on Bitcoin clients
- Search and analyze Bitcoin transactions via online explorers such as https://www.blockchain.com/explorer
- Learn about the concepts of 'hot' and 'cold' storage

Session 4: Objectives

1. Exchanges and Crypto ATMs
2. Bitcoin/Crypto Wallets
3. Clients
4. Wallet Protection
5. Conclusions
6. Further Reading

Session 4: Bitcoin in Practice

1. Exchanges and Crypto ATMs

Cryptocurrency Exchanges

Exchanges are one of the typical ways that beginners can acquire bitcoin and other cryptocurrencies. There are hundreds of cryptocurrency exchanges, but there are some things to look out for before joining one:

Fees:

- Deposit and withdraw fees vary from exchange to exchange and may be impacted by their coin management practices. These details should be available on the exchange's website.

Cryptocurrencies supported:

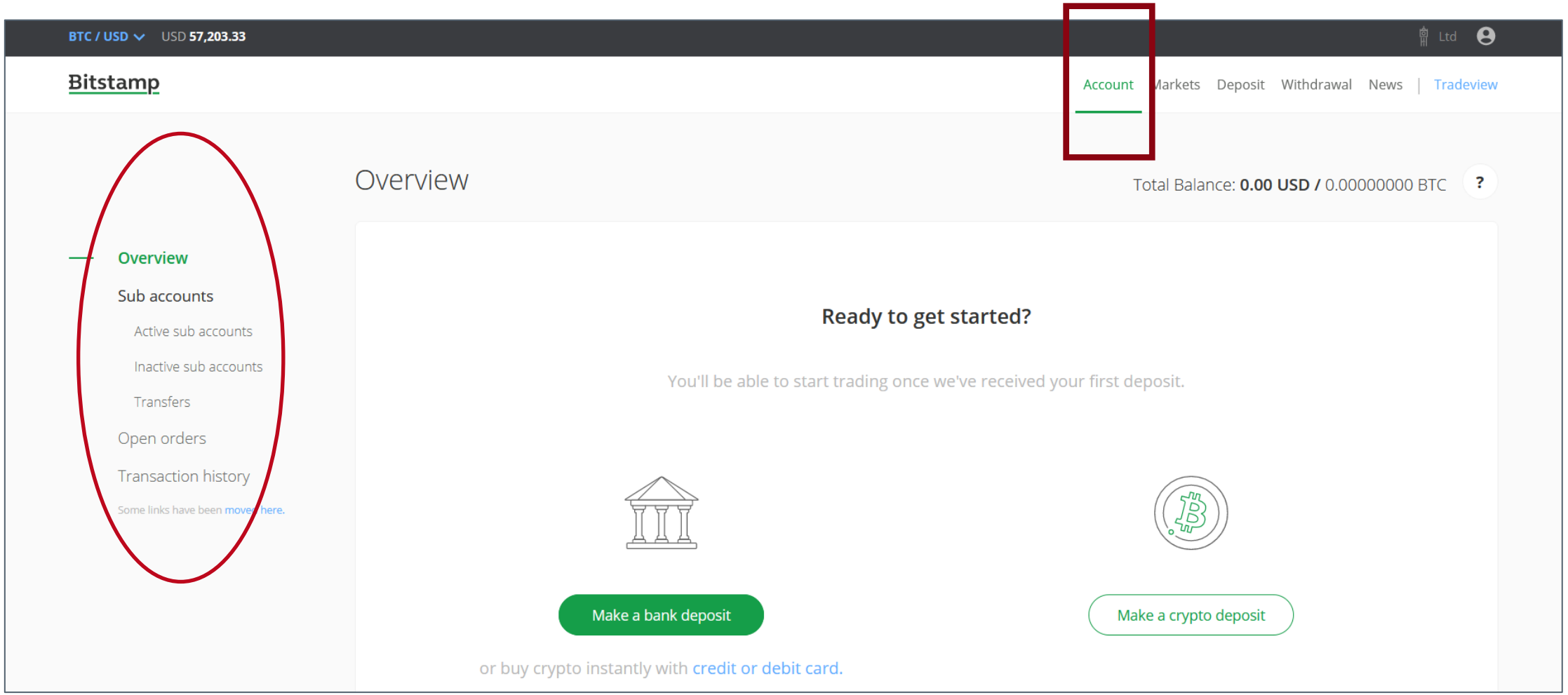
- These exchanges tend to offer buy / sell services for bitcoin by default; if you are interested in other cryptocurrencies, check whether the ones you seek are supported (ex. Ether, Monero, Zcash, etc).

Reputation:

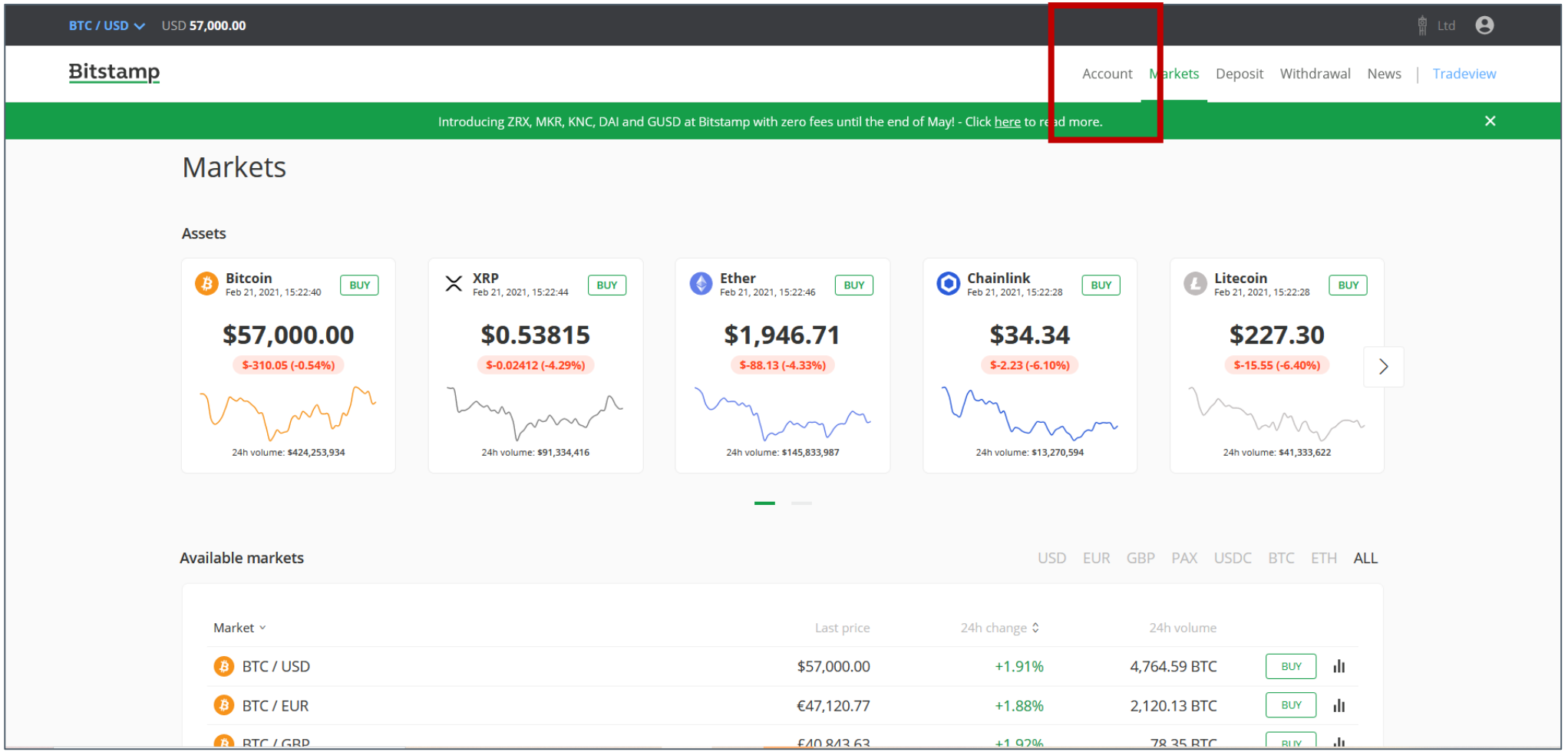
- Make sure to read user reviews, forums, and other social media to learn more about an exchange before trusting them with your money and personal information.

See various exchanges ranked by trade volume here: https://coinmarketcap.com/rankings/exchanges/

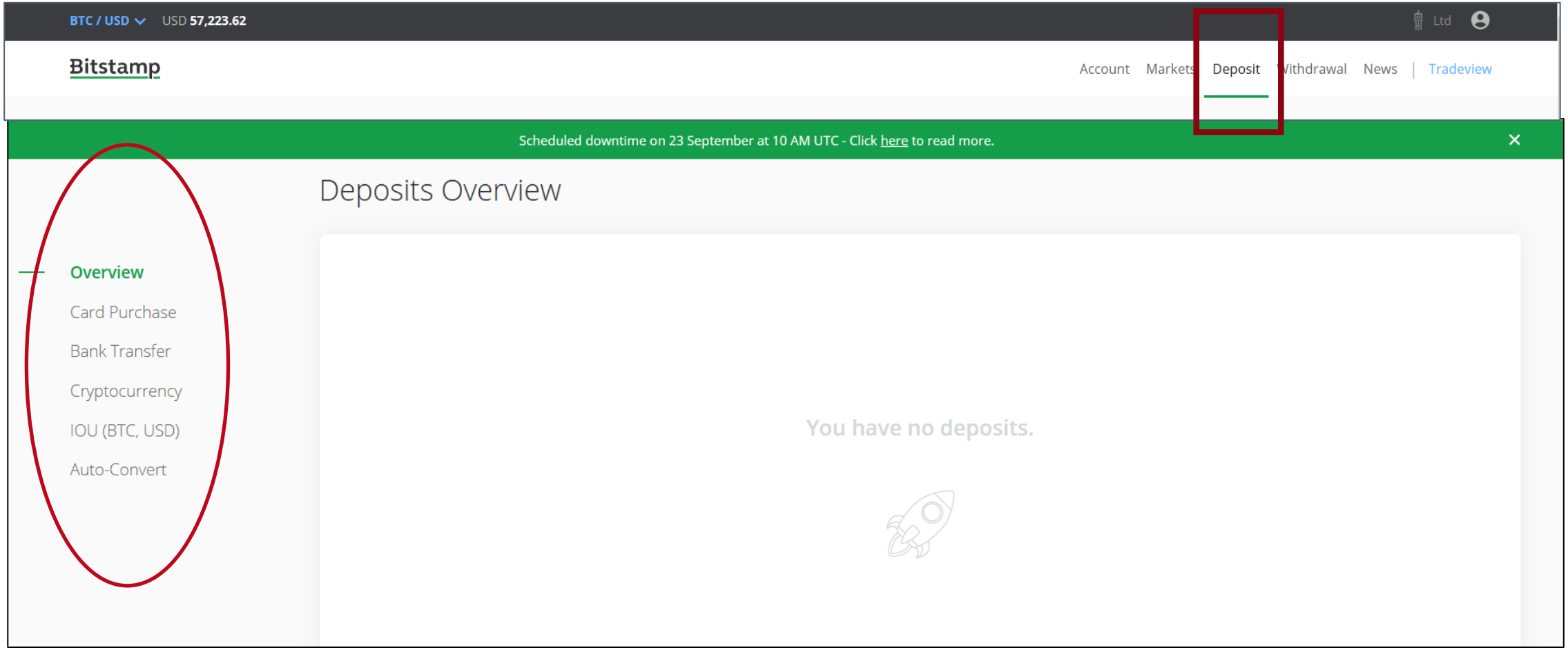
Example – Bitstamp exchange: “Account” Tab



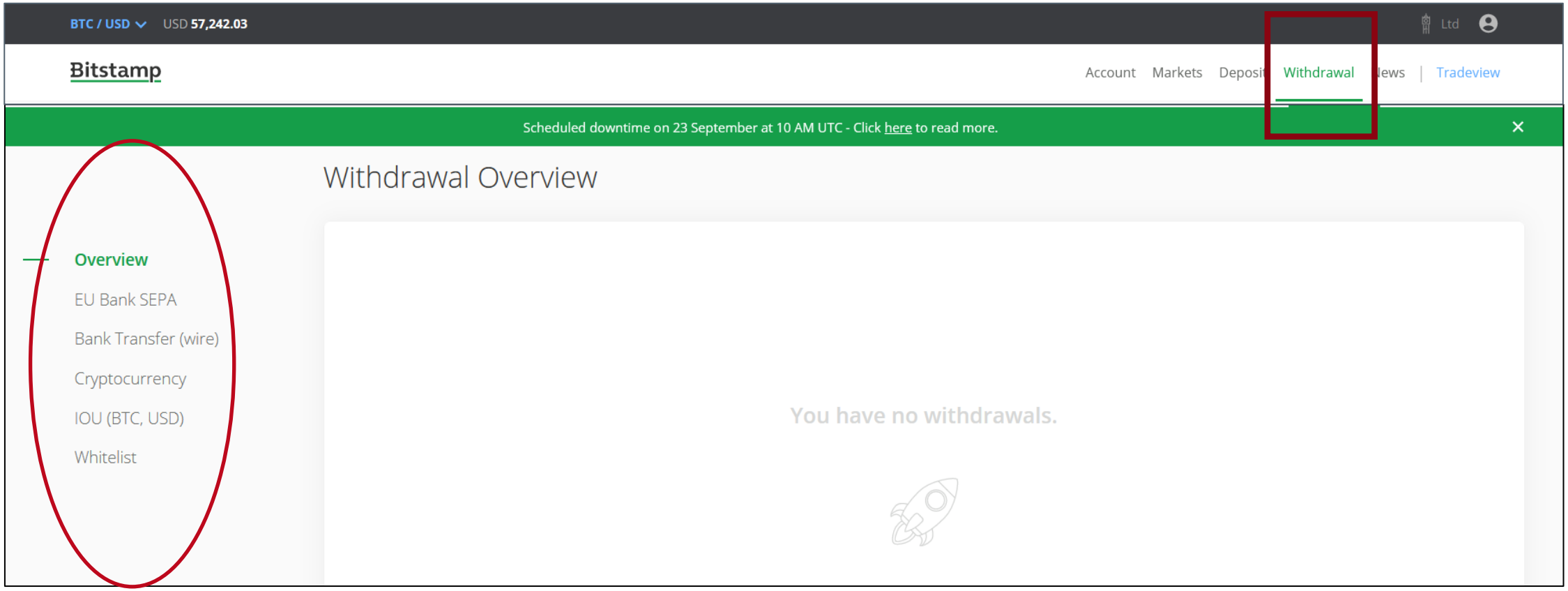
"Markets" Tab



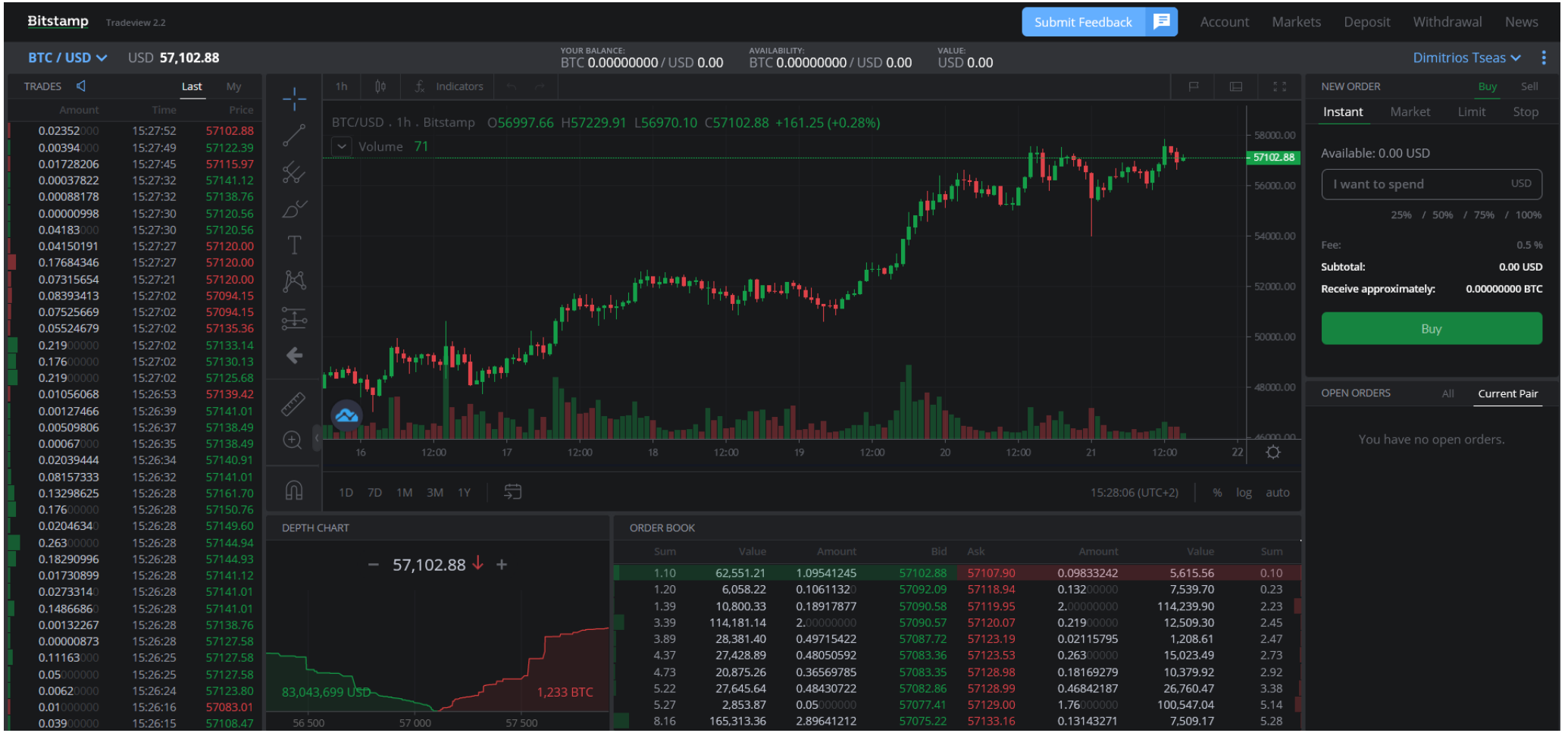
“Deposits” Tab



"Withdrawal" Tab



“Tradeview” Tab



Bitcoin ATMs

According to Coin ATM Radar, as of September 2020, there were more than 10,000 ATMs in 71 countries around the world. As of September 2021, there are now more than 25,000 ATMs in 74 countries. Some of them support Lightning and cryptocurrencies other than bitcoin as well.

Two types of Bitcoin ATMs:

- **One-way:** Only fiat-to-crypto trades are supported, i.e. you can only buy bitcoin
- **Two way:** Both fiat-to-crypto and crypto-to-fiat trades are supported, i.e. you can buy and sell bitcoin

Bitcoin ATMs

Two-way Bitcoin ATMs are becoming popular and have started increasing in numbers.

The ATM provider can take between 1-10% in commission, spread, and transaction fees.

The price of an ATM depends on factors like the number of cryptocurrencies supported and how many bank notes it can hold. They are typically sold for around $9,000 - $13,000.

SumoATM v.2

Genesis1

Satoshi2

BATMThree M+

Bitcoin ATMs

Buy Process	Sell Process
Choose “Buy bitcoin," enter amount.	Choose “Sell bitcoin," enter amount.
Provide mobile number (if required); receive SMS code and enter it.	Provide mobile number (if required); receive SMS code and enter it.
Scan ID document (if required).	Scan ID document (if required).
If you already have a Bitcoin wallet, generate a bitcoin address and have the machine scan the QR code in your wallet.	The ATM will provide a QR code / address to send bitcoin to; open your bitcoin wallet and scan it.
If you don't already have a Bitcoin wallet, install one on your device or have the machine print a temporary paper wallet (if available). Follow previous step.	Authorise the bitcoin transaction from your wallet to the ATM.
Insert cash and wait for processing.	If the ATM requires zero confirmations, then you will receive bank notes from the machine immediately. Otherwise, you will receive a printed receipt and need to wait for at least one confirmation (around 10 minutes).
Get receipt on paper or via email.	Once the transaction is confirmed, scan the QR code from your receipt into the ATM and you should receive bank notes.

Session 4: Bitcoin in Practice

2. Bitcoin/Crypto Wallets

Bitcoin/Crypto Wallet Types

You may choose a wallet based on what best suits your needs. In this session, we will explore various types of wallets and clients:

- Web
- Desktop
- Mobile
- Hardware
- Paper

Learn More: See No. 1 in further reading for a Trezor wallet comparison.

Wallets and clients can be chosen based on a number of criteria:

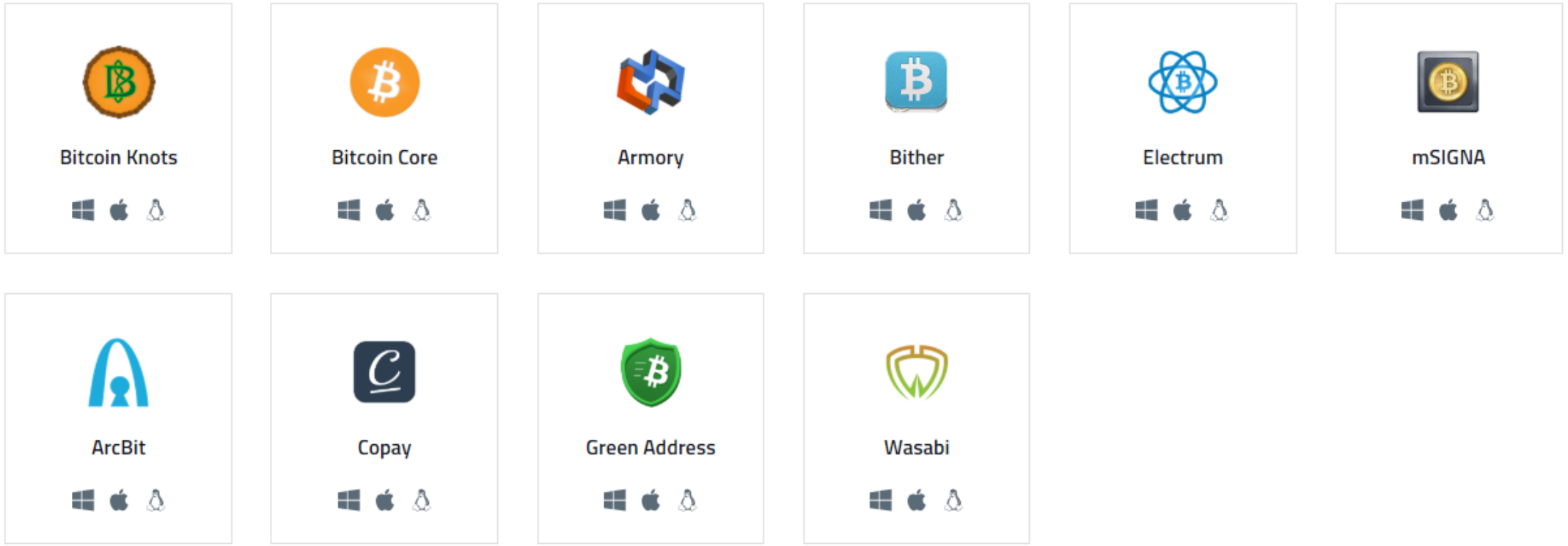
- How much bitcoin is being used / stored
- IT proficiency (beginner vs. expert)
- Type of device
- Occasional use vs. everyday use
- Security and privacy concerns
- Cryptocurrencies being used
- Type and complexity of transactions

Find the wallet that's right for you: https://bitcoin.org/en/choose-your-wallet

For a list of bitcoin-only wallets, see here.

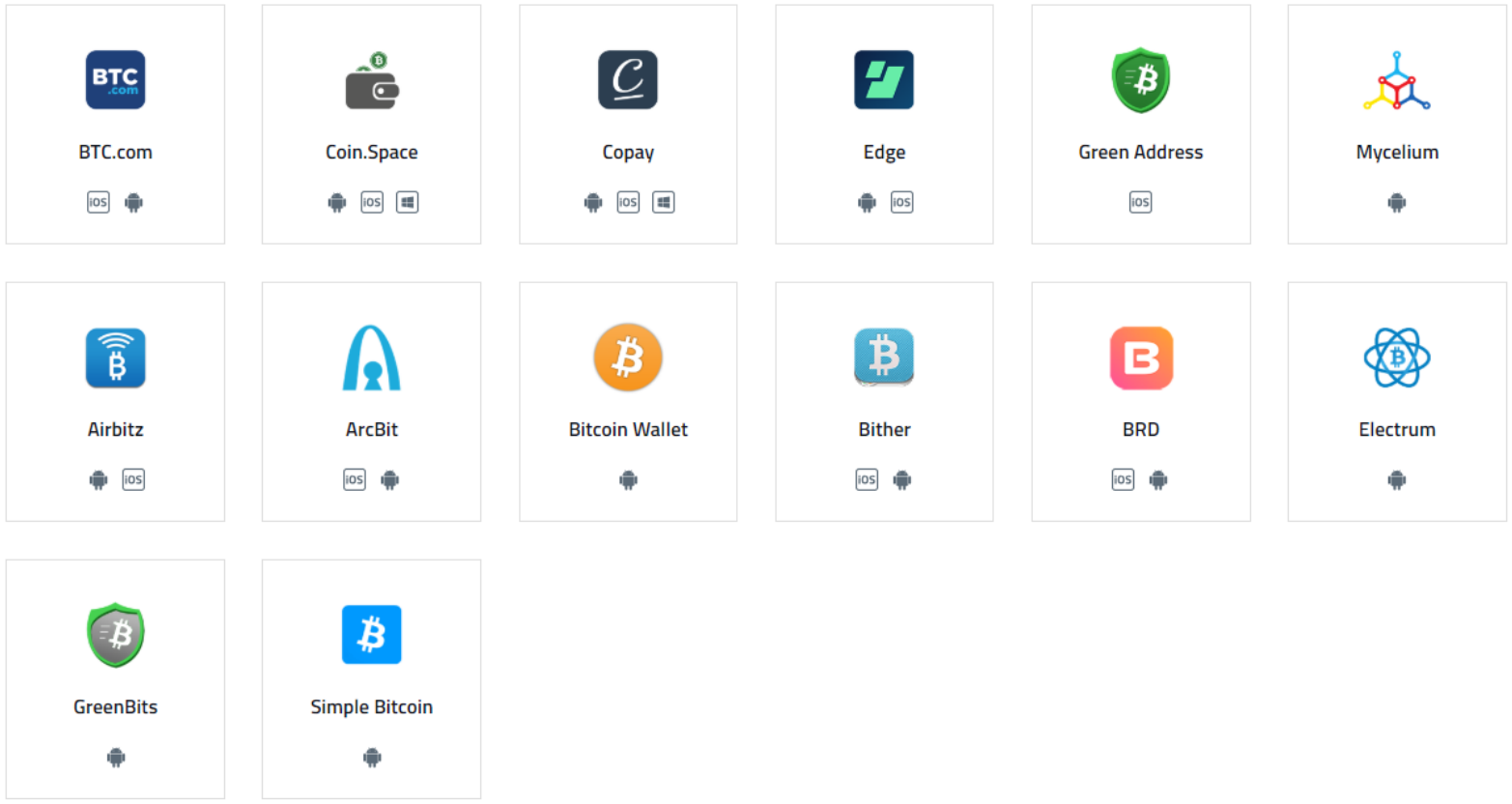
Bitcoin/Crypto Wallet Types (Indicative)

Desktop Wallets:



Bitcoin/Crypto Wallet Types (Indicative)

Mobile Wallets:



Bitcoin/Crypto Wallet Types (Indicative)

Hardware Wallets:

KeepKey

Ledger Nano S

Trezor

BitBox

Bitcoin/Crypto Wallet Types

> *"A wallet is software that holds all your addresses. Use it to send bitcoins and manage your keys."*
>
> *Antonopoulos, A. M. "Mastering Bitcoin Second Edition: Programming the Open Blockchain", (2018),* https://github.com/bitcoinbook/bitcoinbook/blob/develop/glossary.asciidoc

- As outlined in Session 3, bitcoin ownership is established through digital keys and signatures.
- Ideally, keys should be generated locally on the user's desktop, laptop, smartphone, or special-purpose hardware device. Users can access and manage keys through a variety of wallet software. "Possession of the key that can sign a transaction is the only prerequisite to spending bitcoin, putting the control entirely in the hands of each user."
- Keep in mind that if you **don't** know who generates your private keys, where they are stored, or if someone else has them (such as in the case of a custodial exchange), they are not actually yours. The case of Mt.Gox, which discontinued operations in February 2014, is a well-known example of this lesson.

Bitcoin/Crypto Wallet Types

“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.”

Antonopoulos, A. M., "Mastering Bitcoin Second Edition: Programming the Open Blockchain" (2018), https://github.com/bitcoinbook/bitcoinbook

Session 4: Bitcoin in Practice

3. Clients

There are different types of Bitcoin clients:

1. Full client versus lightweight client
2. Desktop client
3. Web client
4. 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 broadcasts outgoing transactions to peer nodes.

Read more about clients vs wallets: 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 stored locally.
- Anyone in the world can run a full node. There are more than 12,600 public nodes operating across 96 countries *(Aug 28, 2021).*
- A **Lightweight client** stores the user's wallet but relies on third-party owned servers for accessing the network and learning information about the blockchain. This client does not store a full copy of the blockchain 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.

Read more about clients vs wallets: http://bitcoin.stackexchange.com/questions/20487/whats-the-difference-between-a-bitcoin-client-and-wallet

Bitcoin Clients

- A **Web client** is accessed through a web browser and stores the user's wallet locally in the browser or on a server owned by a third-party. This can be similar to webmail, in that it usually relies entirely on a third-party server. Some web clients are just an interface for a custodial service (e.g. Coinbase) where the private keys are stored; others (e.g. greenaddress.io) store the private keys encrypted, and 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.

Session 4: Bitcoin in Practice

4. Wallet Protection

Sending and Receiving Bitcoin

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

1. **Offer a service or product for bitcoin**. Many businesses and individuals already accept bitcoin.
2. **Accept bitcoin as a donation** e.g. if you run a charity, such as BitGive and Bitcoin Water Project.
3. **Purchase bitcoin through an exchange** at the current market price. A very comprehensive list of Bitcoin exchanges, categorized by country, can be found here. Identity verification is usually required before you can deposit/withdraw fiat and buy/sell bitcoin or other cryptocurrencies. Thus, opening and verifying the account might take some time.

Sending and Receiving Bitcoin/Cryptocurrencies

- When you first open a Bitcoin / cryptocurrency wallet, it is empty.
- In order to receive bitcoin or any other cryptocurrency, you need to provide the sender with an address from your wallet, just like you would provide your email address to someone who wants to send an email.
- To send bitcoin, the 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 provide a QR code instead.
- When a transaction is confirmed, it is included in the public ledger, i.e. the blockchain, and becomes part of Bitcoin history.
- Each transaction corresponds to a chain of ownership transfer and is maintained in a distributed, peer-to-peer network of nodes.

DO NOT SEND MONEY TO THIS ADDRESS

Get your funds OUT of exchanges

Avoid storing your cryptocurrencies with an exchange, for longer than is necessary, as it can expose you to many risks. Storing bitcoin in an exchange is similar to storing dollars or euros in a bank: a third party has control over your funds.

Third-party risks include:

- **Fraud** (your provider may not be so trustworthy after all),
- **Security** (many providers have been victims of cyberattacks in the past),
- **Privacy** (if your provider collects sensitive personal data, you could be at risk of identity theft and other targeted attacks)

Don't store significant amounts for the long-term on custodial exchanges. Make sure to enable some form of (non SMS-based) two-factor authentication in the account settings.

Learn More: You can find reading lists here and here on securing your wallet(s).

Web Wallets

After exchanges, **web wallets are the least secure choice and are not recommended**:

- Web wallets often store your private key for you on their servers
- They can be used through a mobile application or browser on your personal computer

Web Wallets: Pros & Cons

✓ Easy access to your coins from any device

✓ Third party takes the responsibility for your funds

× You are trusting a company not to steal your funds and disappear

× You are trusting a company to keep your funds safe from attacks

× High risk of phishing attacks, easy to redirect people to the wrong website and steal their password.

Desktop Wallets – Full Nodes

Desktop Wallet Features

- Software downloaded and installed on a PC or laptop.
- The Bitcoin Core desktop full client comes with a bitcoin wallet.

Desktop Wallets Pros & Cons:

✓ Contributing to the maintenance of the decentralized Bitcoin network

✓ Full control and protection, especially if private keys are encrypted with strong passphrases and regularly backed up

✓ Harder to target each individual user's computer than to compromise custodial services storing the funds of thousands or millions of users.

× General-purpose computers are vulnerable to malware, malfunctions, and are attractive for thieves.

× It may take days to download and synchronize, with noticeable bandwidth and disk space requirements.

× Often have advanced features and functionality that are confusing for beginners.

Desktop Wallets – Lightweight

Desktop wallets can be **lightweight** (such as *Electrum, see next page*): only a small portion of the blockchain (headers of blocks) is downloaded; the client relies on other full nodes to verify transactions, and will only receive transactions that are relevant to its wallet.

Lightweight Desktop Wallet Pros & Cons:

- ✓ 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 keys are stored locally on your computer, meaning that you retain complete control.
- ✓ Some can manage a wide range of coins and tokens.
- x Cannot verify transactions as it does not store a full copy of the blockchain. You must trust third-party servers to access and receive information about the Bitcoin network. A malicious third party might spy your transactions.
- x General-purpose computers are vulnerable to malware malfunctions and are attractive targets for thieves.

Lightweight Client - Electrum

Electrum has the following:

- Available on Windows, MacOS, Linux and Android under the MIT license.
- It makes performing Bitcoin transactions quick and simple.
- It supports cold storage and multisig features.

In addition, Electrum is easy to install:

- Go to https://electrum.org/#download
- Download the appropriate installer. (Optional: you can verify the PGP signature: to check that the software packages you downloaded are authentic and were not maliciously modified in transit.)
- Run the installer.
- Run the Electrum client.

https://blog.coingate.com/2017/02/setup-electrum-guide/
https://www.pcgamer.com/how-to-set-up-an-electrum-bitcoin-wallet

https://medium.com/@ecurrencyhodler/how-to-setup-a-multiparty-3-of-5-multisig-wallet-using-electrum-126835c3da69

Mobile Wallets

Installed on a mobile device (examples: ***Copay, BRD*** **for iOS** and **Mycelium, *Coinomi* for Android**) – usually operate as a lightweight client or a web client.

Mobile Wallets Pros & Cons:

- ✓ Portable, easy and comfortable - The smartphone's camera scans QR codes of receivers / merchants
- ✓ Good for day-to-day transactions
- ✓ If your mobile device is lost or stolen, the funds are not gone as long as you have made a proper backup. Most mobile wallets require making backups upon setup (usually a 12-word mnemonic phrase).
- × Harder to run with / as a full client (though many wallets have been adding support for this recently).
- × When in the presence of others or cameras, take care that your PINs and other sensitive wallet info is not visible.
- × Take care to secure your mobile device and accounts against popular attacks such as SIM-swaps.

Cold Storage

- 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 can be connected to the internet or other devices.
- **Cold storage** refers to using an offline medium for storing bitcoin private keys, i.e. a device that is not connected to the internet, at least most of the time. This method is more common for the long-term storage of large sums that do not need to be accessed or used regularly. Today the most popular medium for this is hardware wallets.
- **'Deep' cold storage** refers to a method of cold storage where private keys are generated entirely offline, sign transactions offline, and are stored on a device that is not / has never been connected to the internet. A device which has been modified to remove networking features and used under various isolation techniques is known as 'airgapped.'

Cold Storage

- On a USB drive or other data storage medium
- On a paper wallet
- On a bearer item, such as a bitcoin
- Online on encrypted media, where the encryption key is stored offline
- On an offline Bitcoin hardware wallet

Hardware Wallets

Hardware wallets are special-purpose devices. Examples: (Trezor, Ledger Nano, ColdCard)

Hardware Wallet Pros and Cons:

- ✓ Security through isolation (less complex than a general purpose computer, therefore less vulnerable to common attacks)
- ✓ Private keys generated and stored locally, controlled by the user
- ✓ PIN protection for accessing the keys and sending transactions in wallet interface
- ✓ Backups are required by most of these wallets during the setup process; recorded on paper or metal (usually as a 12 to 24 word mnemonic phrase)
- × Price
- × Less convenient than mobile wallets for day-to-day transactions
- × Do not lose both the device and the backup mnemonic phrase
- × Beware buying from third-party resellers rather than the manufacturer

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

Learn More: You can find here a further reading list to learn more about hardware wallets.

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 can be shared with anyone who wants to send bitcoin to you.
- The private key, which you need in order to spend the bitcoin.

Paper Wallets

Paper wallets are no longer recommended! Many paper wallet generators have been compromised and they are difficult to use properly.

Documents that contain pairs of public and private keys. Must be stored on a safe place. Recommended to make at least two copies. Always generate paper wallets offline!

Paper Wallets Pros & Cons:

✓ Protection from cyber-attacks or hardware failures. Can be generated offline.

✓ Ideal for long-term storage of funds and gifts

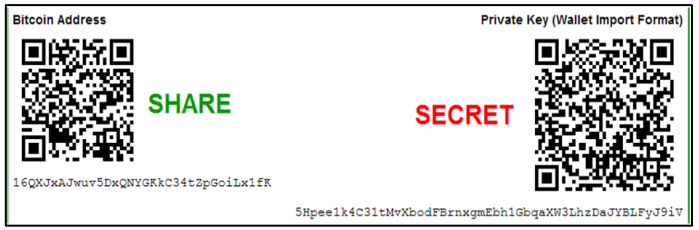
× Loss, theft, destruction (water, fire)

× Must be imported to software at some time, unlike hardware wallets

× Must specify the change address when spending a part of the funds or else you risk losing the remaining balance, because of the way Bitcoin treats change in transactions.

Paper wallets are no longer recommended! Many paper wallet generators have been compromised and they are difficult to use properly.

Public vs. Private Keys

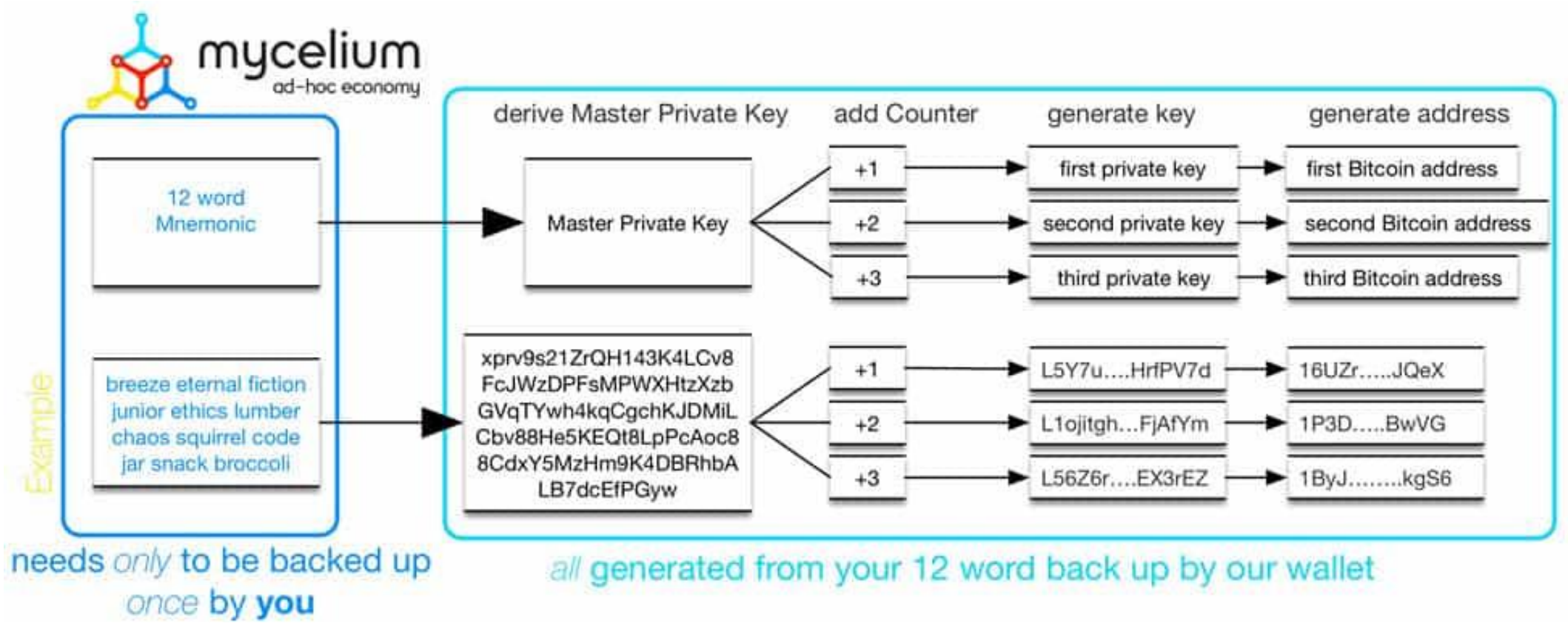


Hierarchical Deterministic (HD) Wallets

- Based on BIP 32, HD wallets generate a hierarchical tree-like structure of keys from a single master seed.
- When you restore an HD wallet using the seed, the wallet can derive all "child" private keys and addresses.
- Since this mechanism allows many receiving addresses to be generated, it reduces address reuse and therefore enhances privacy.
- Examples of HD wallets include Coinomi, Mycelium, Jaxx, Electrum, and all the hardware wallets.

- **Read more about HD Wallets:** https://coinsutra.com/hd-wallets-deterministic-wallet/

Hierarchical Deterministic (HD) Wallets



Secure your wallet, no matter what type it is!

Some ways of securing your wallet include:

- Avoiding (if possible) the use of online services or devices to generate private keys.
- Use different types of wallets for different purposes and amounts. For example, you may use a mobile wallet for small everyday purchases, whereas your long-term savings are kept on a hardware wallet.
- Create backups of all your wallets and occasionally test recovering them to your device(s). Make sure that they are stored in a safe and secure place.
- Encrypt your wallet with a passphrase -- even if someone steals your mnemonic seed, they won't be able to access your coins without the passphrase!
- Do **NOT** split your mnemonic seed words and store them in different places, as such practices generally increase the chances of accidental loss. Instead, you can use multisig or the more experimental Shamir's secret sharing scheme (SSSS).

Finally, in general, make sure to use the most up-to-date versions of software on your devices. Otherwise you may miss important security patches!

Session 4: Bitcoin in Practice

5. Conclusions

Conclusions

- There are many types of clients that provide access to the Bitcoin network. Full clients download, verify, and store the entire transaction history. Lightweight clients only store and verify a small portion of the blockchain; they must rely on a full client, often provided by third parties, to receive and broadcast transactions.
- Bitcoin wallets store and manage keys for signing transactions. The word" wallet" is misleading as it does not actually “hold” the bitcoin. The ownership of bitcoin is recorded on the blockchain.
- It is best to generate and store bitcoin private keys offline, known as 'cold' storage. A passphrase can be applied for added security. General-purpose, internet-connected devices have a larger attack surface than a special-purpose, offline device.

Conclusions

- Both novice and experienced users should pay attention to securing their digital wealth. Proper measures of protection may require significant investments in time and care.
- **Important tips:**
  - **Select an exchange which suits your needs**
  - **Do not keep funds long-term 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 with a passphrase. This is an optional step for some wallets. NEVER FORGET YOUR PASSPHRASE, as your mnemonic seed will not be enough to recover those funds."**
  - **Create backups of your wallets (often a required step during setup).**

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

Session 4: Bitcoin in Practice

6. Further Reading

Conclusions

On wallets comparison:

1. Satoshi Labs

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

On wallet protection:

2. Securing your wallet: Practical advice from bitcoin.org

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

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

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

4. Securing your Digital Wealth – Andreas Vlachos on IFXEXPO Conference

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

Conclusions

On hardware wallets:

5. Hardware wallets

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

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

https://medium.com/shapeshift-stories/hardware-wallets-make-a-comeback-thanks-to-the-new-shapeshift-1ab16c0df419

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

6. Multisignature - Wikipedia

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

Conclusions

On additional features:

7. New Exchange Features – Bitcoin Magazine

https://bitcoinmagazine.com/articles/with-new-exchange-features-wallets-arent-just-for-storing-bitcoin-anymore

https://www.exodus.io/

https://cointelegraph.com/news/consumer-electronics-giant-htc-announces-bitcoin-full-node-on-exodus-1s-smartphone

UNIVERSITY of NICOSIA

Questions?

Contact Us:

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