CSE446: Blockchain & Cryptocurrencies

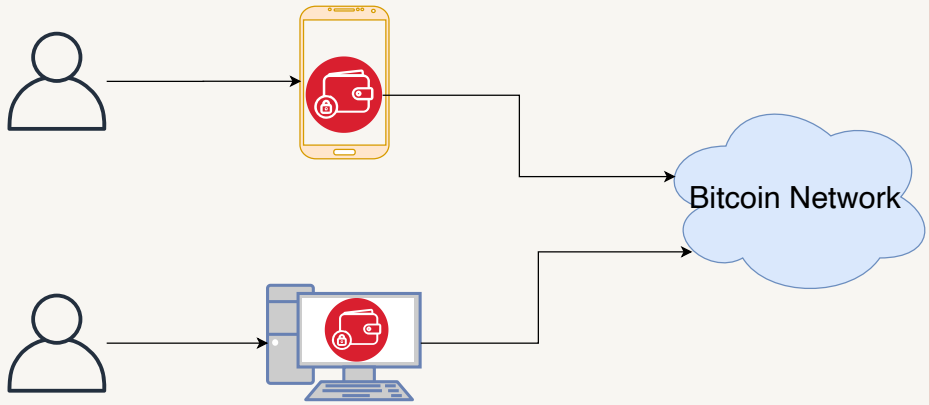
Lecture – 7: Bitcoin-2

Agenda

- Bitcoin components
  - Users
  - Node & Network

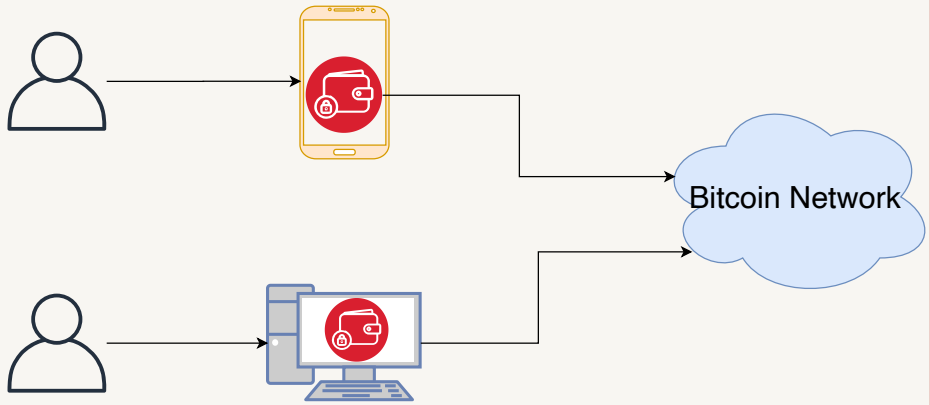
Bitcoin (hot) wallet

- A Bitcoin wallet is a collection of private keys
  - might be used to manage those keys and to make transactions on the Bitcoin network
- It is the entry point for any general users to interact with the bitcoin network
- Can be utilised in a PC, in any smart-device such as a mobile phone or tablet
- Also known as hot wallets as they are always connected to the network
- Examples: Exodus, Electrum, Mycelium



Bitcoin (hot) wallet

- Private keys are kept in encrypted (with a password) formats to ensure their security
- If password is forgotten, there is no way to recover funds attached to that private address
  - unlike other password enabled services, there is no account recovery option
- Strong usability issue
- Advantageous for daily trading or continuous usage
- Less secure (e.g. prone to malware attack)



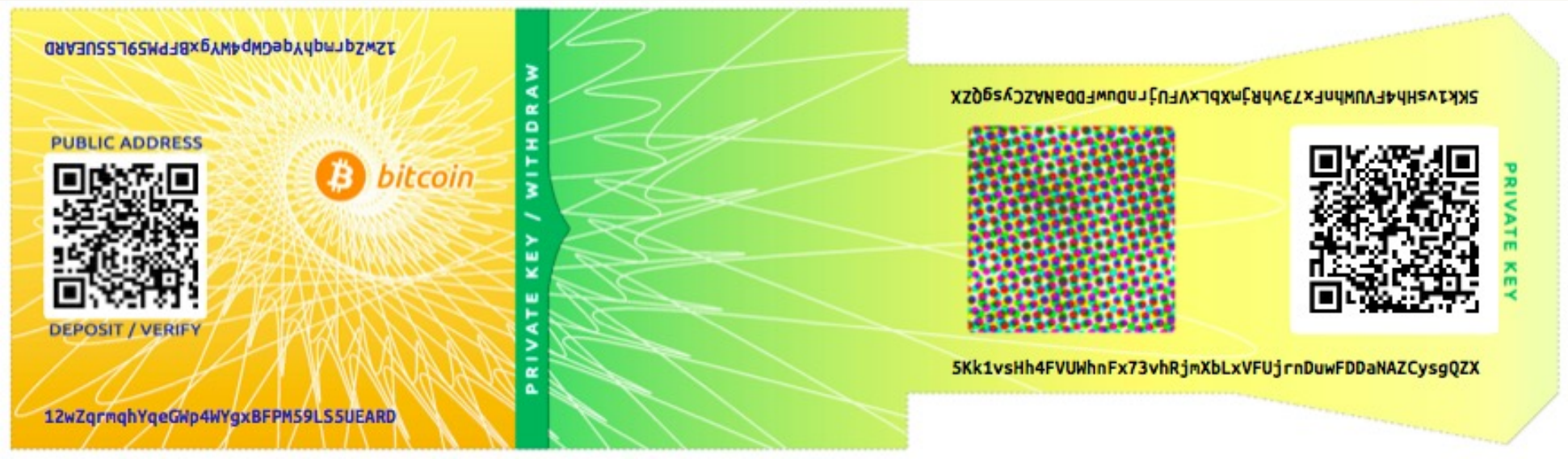
Cold wallet: paper wallet/cold wallet

- Paper wallets are bitcoin private keys printed on paper
  - might include the corresponding bitcoin address for convenience, but this is not necessary because it can be derived from the private key
- They are a very effective way to create backups or offline bitcoin storage, also known as *cold storage/wallet*

Cold wallet: paper wallet/cold wallet

- As a backup mechanism, a paper wallet can provide security
  - against the loss of key due to a computer mishap such as a hard-drive failure, theft, or accidental deletion
  - store it offline in a secret & secure place, even in a bank vault
- As a "cold storage" mechanism, if the paper wallet keys are generated offline
  - never stored on a computer system
- Hence, they are much more secure against hackers, keyloggers, and other online computer threats

Cold wallet: paper wallet/cold wallet



https://raw.githubusercontent.com/bitcoinbook/bitcoinbook/develop/images/mbc2_0410.png

Hardware wallet

- A **hardware wallet** is a special type of bitcoin wallet which stores the user's private keys in a secure hardware device
- They have major advantages over standard software wallets:
  - private keys are often stored in a protected area of a microcontroller, and cannot be transferred out of the device in plaintext
  - immune to computer viruses that steal from software wallets
  - can be used securely and interactively, as opposed to a paper wallet which must be imported to software at some point
  - much of the time, the software is open source, allowing a user to validate the entire operation of the device

https://www.ledgerwallet.com/images/products/lns/ledger-nano-s-fold-medium.png

https://en.bitcoin.it/w/images/en/d/de/Trezor-tx.jpg

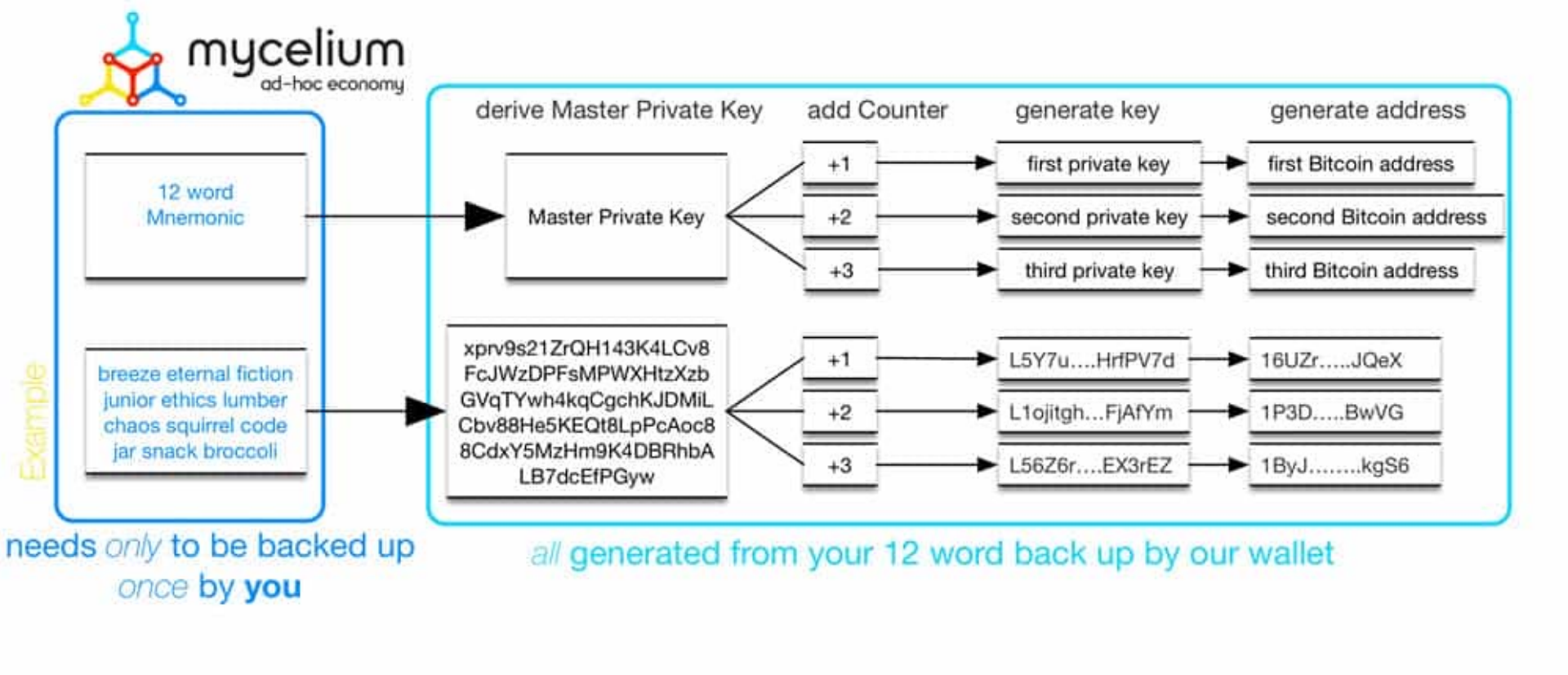
HD wallet

- A Hierarchical Deterministic (HD) is a key creation and transfer protocol which allows creating child keys from a parent key in a hierarchical way
  - Wallets using the HD protocol are called HD wallets
  - The single starting parent key is known as a seed
- The seed allows a user to easily back up and restore a wallet without needing any other information

HD wallet

- Seeds are typically serialised into human-readable words in a **Mnemonic** phrase
- A mnemonic phrase, mnemonic recovery phrase or mnemonic seed is a list of words which store all the information needed to recover a Bitcoin wallet
- Such Mnemonic words must be stored securely and must never be typed on any website

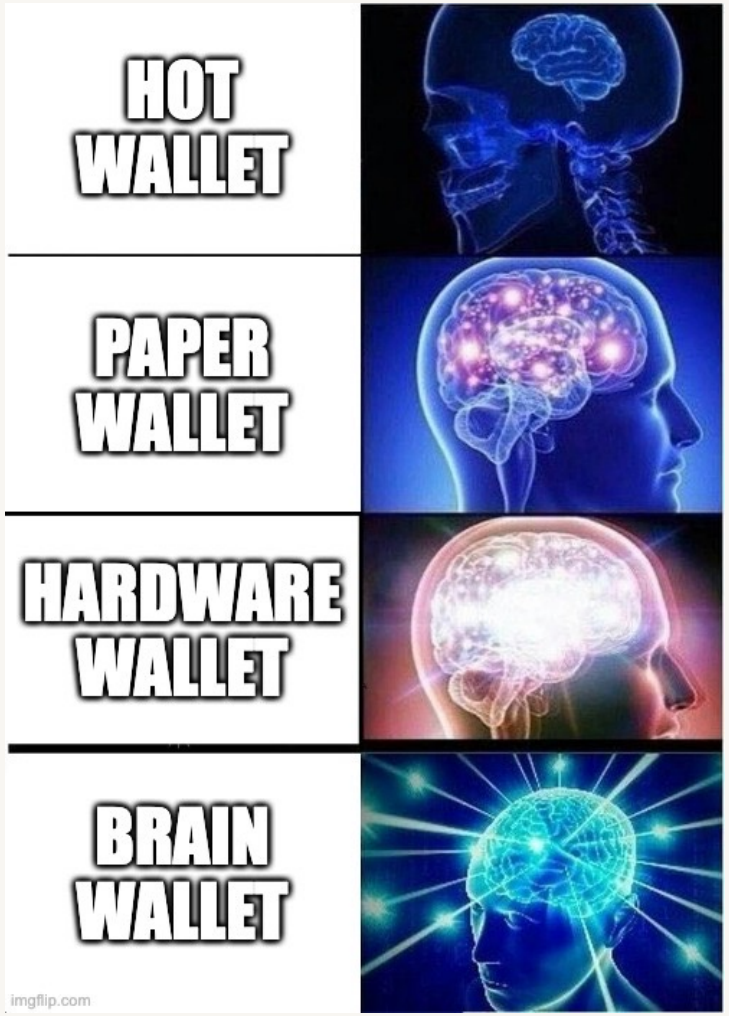
HD wallet



https://coinsutra.com/wp-content/uploads/2017/07/HD_Wallets.jpg

Brain wallet

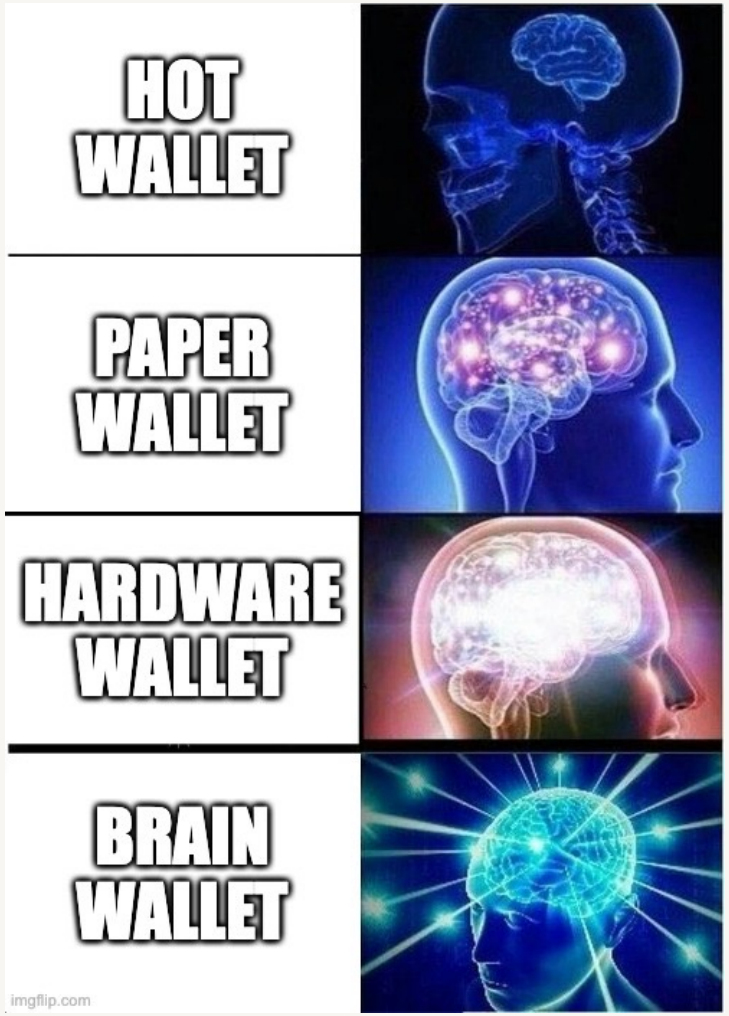
- A brain wallet refers to the concept of storing Bitcoin’s private key in one's own mind by memorising a seed phrase
- If the seed is not recorded anywhere, the Bitcoins can be thought of as being held only in the mind of the owner
- If a brain wallet is forgotten or the person dies or is permanently incapacitated, the Bitcoins are lost forever
- Using memory techniques allow them to be memorised and recalled easily



https://i.imgflip.com/6x41nq.jpg

Brain wallet

- Private keys will be generated from a seed => random words known as passphrase
- Use the passphrase to generate a private key
  - E.g. hashing the passphrase
- Then generate the public key from the private key using a standard algorithm
- The passphrase needs to be securely created, otherwise an adversary could easily guess
- If the passphrase is long, it will be difficult to memorise

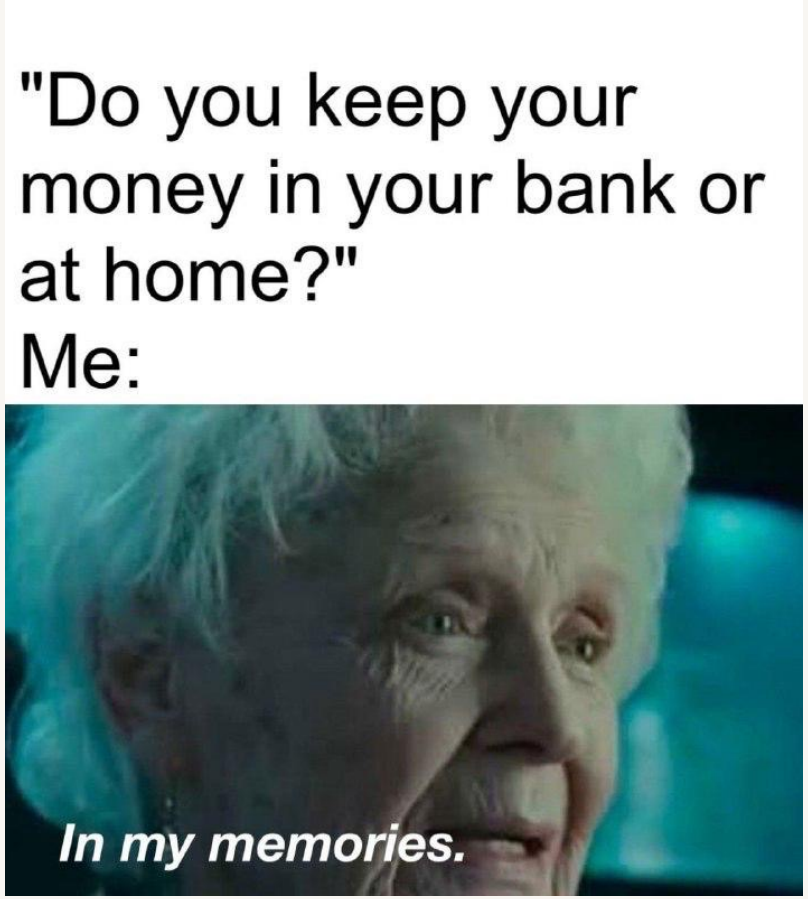


https://i.imgflip.com/6x41nq.jpg

Brain wallet

- To memorise a seed with this method you must invent a story which hits the words as "keynotes”
- Let the key phrases are the following
  - witch collapse practice feed shame open despair creek road again ice least
- “Imagine going through a room and seeing your sister dressed as a **witch**, playing the jenga boardgame until the tower **collapses** and so on”

Brain wallet



Custodial wallet

- Let other people / companies store your bitcoins / cryptocurrencies for you
- No access to the private key, coins can only be used through a certain interface / website
- Very common within most exchanges
    - The money is sent to the exchange, the account on the platform has now a new balance which can be traded or paid out
- However: Very dangerous!
- Many exchanges got hacked, users lost their funds. Be careful!


THANK YOU
QUESTIONS?