CMSC 398F
Week #5
Wallets & Anonymity

Announcements

- We decided not to release Quiz 4
- Project #1 will be be released after class
- Join the class Piazza!
  - piazza.com/umd/fall2022/cmsc398f

From Last Week

- Bitcoin transactions are scripts that transfer bitcoin from one account to another.
- Bitcoin addresses are derived from public keys (RIPEMD-160), which are derived from private keys (using ECDSA).
- The wallet address is a shorter representation of the public key's final part and usually has a length of 160 bits.
- From a technical perspective, transactions are sent and received from an address. One encrypts, exports, backs up, and imports from a wallet.

Wallets

- Most Bitcoin users don’t have the entire the entire blockchain downloaded, and doesn't need any fancy functionality
- All they have is a wallet to help manage their keys, and they can send and receive Bitcoin to anyone else on the network.
- Wallets come in many shapes and sizes, they can be hosted on the web, your computer, or can even be physical

What is a crypto wallet?

- Crypto wallets store your private keys, keeping your crypto safe and accessible. They also allow you to send, receive, and spend cryptocurrencies like Bitcoin and Ethereum.
- Unlike a normal wallet, which can hold actual cash, crypto wallets technically don’t store your crypto. Your holdings live on the blockchain, but can only be accessed using a private key. Your keys prove your ownership of your digital money and allow you to make transactions.

Keys

- When you send from a Blockchain wallet, the transaction is signed with your private key (without actually disclosing it), which indicates to the entire network that you have the authority to transfer the funds on the address you're sending from.
- The security of this system comes from the one-way street that is getting from the private key to the public address.
- Not possible to derive the public key from the address; likewise, it is impossible to derive the private key from the public key.

What do Wallets Do?

- A wallet is composed of several public and private keys
- The program uses the public key to generate a unique BTC address
- Someone else can send BTC to this address
    - Private key should never be shared with anyone: it is used to sign new transactions and lets you access your funds
    - Can also be used to generate the public key and BTC address
- Modern wallets use a ‘seed phrase’
    - Used to generate multiple unique private keys
    - Works like a root key

Hot vs. Cold Wallets

- We generally distinguish wallets in two different ways
    - Hot wallets are connected to the internet
        - Software Wallets
    - Cold wallets are not connected to the internet
        - Hardware Wallets
        - Paper Wallets

Software Wallets (Hot)

- Web wallets, Desktop wallets, and mobile wallets
  - Web wallets use a web interface (think Coinbase, Binance, etc.)
  - Desktop wallets need to be downloaded and executed locally on your machine
  - Mobile wallets are similar to Desktop wallets

Hardware Wallets (Cold)

- Physical, electronic devices that use RNG to generate public and private keys.
- These keys are stored physically in the device itself
- Inconvenient for traders and frequent users.

Paper Wallets (Cold)

- Piece of paper on which blockchain address and private key is printed out on
- Presents numerous flaws, making it highly discouraged.
  - You cannot send partial funds
- bitaddress.org

Online Wallets

- Exchanges (such as Coinbase or Binance) will usually create a wallet for you when you sign up for the site, so you can just trade cryptocurrency instantly on the network
    - Convenience is key!
- For exchanges that carry many types of cryptocurrency, it’s also very easy to convert between cryptocurrencies
- Biggest con: security
- Historically, exchanges have been hacked many times — if your private keys are being stored by the exchange, than anyone who steals it can now steal all of your money

Lite Wallets or Lightweight Wallets

- Many cryptocurrencies have wallet software that you can download on your computer
    - It checks in with certain nodes to gather information when you want to spend money
- These wallets store private keys on your computer
- Biggest advantage to lite wallets is increased security — all of your coins are stored in your hands, not with an exchange
- However, if your laptop gets compromised for any reason, your coins may still be stolen
    - And if you wipe/lose your laptop on accident, then you’ve potentially lost your coins!

Node Wallets

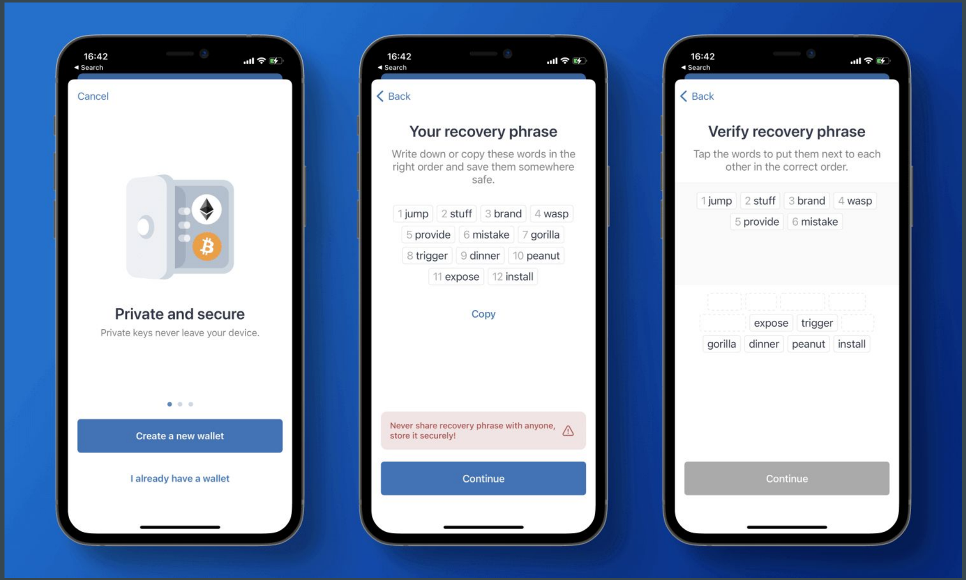
- Node wallets are similar to light wallets, but they keep entire blockchain locally and act as a node; no need to check in to gather info before spending
- Running a node on your computer provides support for the network, and contributes to keeping your funds safe
- Nodes store Bitcoin's UTXO pool
- Carries same risk as lite wallets

Multisig Wallet

- Adds another layer of security
- Can utilize multiple signatures to sign for an outgoing transaction
- Several keys can can generate a signature
- Although multi-sig technology existed long before the arrival of crypto, it's most often associated with the advent of Bitcoin

Recovery Phrase: Master Key

- A recovery phrase (sometimes known as a seed phrase) is a series of words generated by your cryptocurrency wallet that gives you access to the crypto associated with that wallet.
- The seed phrase can be said to be a crypto wallet's master key.
- For example, when a hardware wallet and lost or deleted wallet from the computer, it can easily create a new wallet and use the seed phrase, which will recover cryptocurrencies held in the wallet.



Private and secure

Private keys never leave your device.

Your recovery phrase

Write down or copy these words in the right order and save them somewhere safe.

1 jump 2 stuff 3 brand 4 wasp
5 provide 6 mistake 7 gorilla
8 trigger 9 dinner 10 peanut
11 expose 12 install

Never share recovery phrase with anyone, store it securely!

Verify recovery phrase

Tap the words to put them next to each other in the correct order.

1 jump 2 stuff 3 brand 4 wasp
5 provide 6 mistake

expose trigger
gorilla dinner peanut install

Recovery Phrase

- Every blockchain wallet generates a seed phrase of 12 to 24 words during the setup process and instructs the user to record all the words in order. The words are chosen at random from a word list. Many wallets use the BIP39 standard, which has a list of 2,048 words.
- To use a seed phrase with a wallet, select the option to restore using a recovery phrase. The wallet will prompt you to enter your seed phrase in order. After you've correctly entered the seed phrase, you'll have your crypto in your wallet.

Recovery Phrase vs Private Key

- Blockchain wallets generate public keys and private keys.
- A public key can be shared with other parties and is used for receiving transactions, similar to an account number.
- A wallet address is a hashed version of this public key. A private key is the wallet owner's key and is used for authorizing transactions, like a PIN.
- Each time the wallet generates a wallet address that the owner can use to receive crypto, it also generates new public and private keys associated with that address. Private keys are derived from the wallet's seed phrase.

Metamask Demo