Crypto News?

Wallets

Recall last week

- Bitcoin transactions are scripts that transfer bitcoin from one address to another
- Bitcoin addresses are derived from public keys (using RIPEMD-160), which are themselves derived from private keys (using ECDSA)
- Bitcoin private keys can be hard to keep track of
- Bitcoin transaction scripts are not easy or user-friendly to create or issue to the network

How do you keep track of your bitcoin addresses?

- Most people use a **wallet**
- It would be very complicated and non-user friendly if you had to do everything we talked about last week yourself
- Wallets effectively keep track of all of this and do it for you, so you only worry about sending and receiving bitcoin
- Wallets can generate new addresses for you
    - Keeps track of all of your private keys so you don’t lose them
    - Usually instantiated using a seed, so you can recover your “passwords” — recall last week

How do you issue transactions to the network?

- Wallets not only keep track of private keys and addresses, but they can also create well-formed transactions
  - Some wallets only support P2PKH transactions, but others also support P2SH Multisig as well
- Wallets can generate signatures on your behalf so you can issue your transactions
- If you have multiple addresses that contain bitcoin, your wallet can keep track of the total Bitcoin for you and **batch** your transactions
  - Why would batching be useful?

What kinds of wallets exist? What are the pros and cons of each?

- Online Wallets
- Lite Wallets
- Node Wallets
- Hardware Wallets
- Paper Wallets

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 exchange
- A major pro of online wallets is convenience — it's very easy (and fast) to log on to Coinbase and send your coins wherever you want
- 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

- Many cryptocurrencies have wallet software that you can download on your computer, and it checks in with a node/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 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 on Bitcoin’s network are responsible for gathering and verifying transactions, and then passing them to miners for inclusion in a block
- Nodes store Bitcoin’s UTXO pool
    - Between the UTXO pool and the blockchain, running a node can be quite space-intensive; for this reason, most people don’t run nodes on their laptop, but rather a desktop computer in a set location such as their home
- Carries same risk as lite wallets

Hardware Wallets

- Some form of hardware that holds your private keys and plugs into your computer when you want to actually spend your coins
- Hardware wallets usually need to interact with some form of software in order to send transactions
- Hardware wallets **only** deliver a signature to the computer — this means that even on a compromised computer, you can make safe transactions
- This makes for even higher security
    - What happens if you lose your hardware wallet?

Paper Wallets

- These “wallets” are simply private/public key pairs written down on a piece of paper; these wallets are the hardest to use
- When you want to spend money, you’ll have to input your private key into a website/software to create the transaction
    - YOU SHOULD **ALWAYS** SPEND THE ENTIRE BALANCE IF YOU DO THIS
- Paper wallets are the most secure type of wallet — no electronics involved, so you can just lock your paper in a safe
    - The Winklevoss twins use a paper wallet to protect their massive amounts of bitcoin
- Biggest con — if the paper is destroyed, there is no protection to get it back unless you wrote it down somewhere else
- If you don’t spend your entire balance, your coins may be **severely** compromised

Deterministic Wallets

- We’ve talked about how you can lose your coins if you lose your lite, node, or hardware wallets
- In practice, most of these wallets have a protection against that — they are **deterministic**
- Deterministic wallets are instantiated with a **seed** — some information that is used to then create every private key that you own
- As long as you do not lose your seed, you can lose your wallet and just instantiate a new one with the same seed
    - This will recreate every private key you previously had, so you don’t lose any coins

Deterministic Wallets

- What types of deterministic wallets are there?
- String Deterministic
  - User chooses some string, say “ILoveBitcoin”
  - Addresses created by hashing string with a counter (i.e., Hash(“ILoveBitcoin1”), Hash(“ILoveBitcoin2”), Hash(“ILoveBitcoin3”), ..., Hash(“ILoveBitcoinN”))
- Hierarchical Deterministic (HD)
  - Seed is a random 128-bit value presented as a set of 12 strings to the user (i.e., “weight district loophole tape honey vivid fabric abstract bear face champion saturation”)
  - Each address is a point picked out of a mathematically complex function
- HD wallets tend to be more secure than string deterministic wallets

Summary

- Bitcoin addresses and transactions are hard to keep track of accurately as a user
- Wallets can take care of all of this for you
- Several types, but each carries their pros and cons
- When picking between the type of wallet to use, user mostly has to balance security with ease of use

Project 2

- Project 2 will be out tonight, and is due at 11:59 PM on 10/12 (deadline is 11:59 on 10/15)
- In this project, you will act as a node that receives and has to verify transactions
- You will have to verify signatures and create new UTXOs, as well as keep track of and update the UTXO pool as you verify transactions
- We highly recommend using Eclipse or IntelliJ for this project, as the setup and overhead is a bit more complex than the last project for running tests

Questions?