Questions

Blockchain Basics

Q: What does it mean that blockchains are decentralized? **A:** If we abstract the blockchain to be a list of records, decentralization can be understood as the storing of the list in more than one place.

Q: What are key benefits of decentralization? **A:** (1) With no central entity holding records, there is less risk of corruption and tampering. In other words, the network of nodes does not have to trust any single entity. (2) There is no central point of failure. If records were kept on a single computer, the health of that machine would be solely responsible for the safety and persistence of the records. If that machine was to entirely break, the records would be gone forever. In contrast, if the records were repeated across many machines, any one system failing would not result in a loss of the records. (3) Transparency is a feature of decentralization. Because the records are kept in many places, there are many "eyes" verifying the integrity of the records. (4) Certain use cases benefit in greater optimization. Consider a server serving files to clients. The clients closest to the server would experience the best performance; as you move further away, the service would grow slower. If these servers were instead dispersed evenly, there is a better chance the client would be close to a server and not experience a deteriorated service.

Q: What is the double-spending problem and how does blockchain solve it? **A:** Digital records are easily duplicated or tampered with, which has historically rendered digital currencies unreliable. Without a way to confidently verify the history of transactions, past attempts of digital currencies were susceptible to being "spent twice"—meaning users were able to spend money that they didn't actually have. However, since blockchain links the blocks using cryptographic proof, a network of people can confidently agree on the history of transaction and thus be sure that no money is "spent twice."

Q: What are the functions of a crypto wallet? **A:** A crypto wallet needs to be able to generate valid keys/addresses, safely store the keys, and construct, sign, and broadcast transactions.

Keys and Addresses

Q: What does it mean for a child key to be "hardened"? Why would we use a hardened child key over a non-hardened?

A: Hardened Keys are a type of BIP32 derivation, denoted by an apostrophe in the derivation path (ex: m / 44' / 0' / 1' / 1 / 0). When a Child Key is "hardened", it removes the link to a parent public key. Hardened Keys are more safe and secure, as an attacker cannot recover the parent private key if the child key has been compromised.