Recitation 24 — Bitcoin

Overview

- Bitcoin provides a decentralized electronic currency so that users don't have to trust a centralized bank
- Transactions are recorded on the "blockchain", a special type of log that is broadcast to all participants.

Components of Bitcoin

The blogpost that accompanied this recitation is a great resource; below is just an outline

- Public keys: used in lieu of personally-identifying names
- For A to spend a coin with B: A takes the hash of the previous transaction, along with B's public-key (effectively their name), and signs that.
    - Including the hash of the previous transaction lets us order the transactions; signing the transaction means only A can transfer its coins.
- Consensus:
    - Possible problem: A could spend a coin with B at the same time C spends a coin with D, both add that to the previous transaction. Which is correct? We need some form of consensus
        - Note that this problem is not malicious in nature; all parties are acting honestly here.
    - Second possible problem: Solutions that require (say) a majority of components to agree on a sequence of transactions are open to "Sybil Attacks", where a malicious user creates multiple identities to verify false transactions.
    - Solution: Bitcoin uses proofs-of-work to verify transactions. As users continue to add to each fork of the blockchain, eventually one will win out and become longer; that's the accepted sequence of transactions.
        - Con: Takes a long time for a transaction to be fully verified! Also, environmental impact (below)

Discussion

- Lots of talk these days about Bitcoin's impact on the environment, especially given the amount of energy required to perform the proofs of work.
- How anonymous is Bitcoin?
- How usable is it?
- What are the connections to other areas of 6.1800?
    - Many: logging, consensus, encryption, hashing, signatures, integrity, …