Blockchain Lecture Notes

- Some stats
    - 582 billion USD: value of remittances sent out of US each year
    - T-3: total time securities to take (silly clearing houses)
    - 25% percent of fee that goes to Uber for each ride
    - 100% of revenue that goes to Facebook, Google, for your data
- Create a world without a middleman
- Background Technology
    - Hashing
        - “Summarizes” data
        - Can’t unsummarized
        - Any change to data results in total different output.
    - Digital Signatures
        - Can’t just use the mouse to sign a trackpad because copy
        - Public key cryptography
            - Private key - signature pen
            - Public key - database used to check the signature
        - Links some message
- Bitcoin Ecosystem
    - Two Parties
        - Users
            - I control 1 bitcoin
            - I create a transaction
            - From, to, value, signed
            - Use private key
            - Broadcast transaction to bitcoin network
        - Miners
            - Group t1,t2,t3,t4 transactions into a block (T)
            - Miners see transactions
            - Create “blocks” that hold transaction
            - Send blocks to each other
            - How do they create blocks?
        - You can only build on one block, points to previous block
        - How do Miners provide security?
            - Making blocks requires energy
                - High cost of attacking the network
            - Recursive bootstripping
        - Making a block creates Bitcoin
- Attacks
    - 51% Miner Attack

-
    -
        - Create two blockchains at the same time
        - Spend money in one, do not spend money in the other
        - Buy a coffee on one blockchain, don’t buy a coffee on the other
        - Recreation of history, make a longer chain with an alternate version of history
        - if this is bigger then other chains, then that chain is the correct one
    - Miner Censorship
        - “I don’t want to buy coffee!” -some miners
        - Don’t include your transactions in a block

- Ethereum!
    - Has extra piece of data
        - Write code on it
    - Also a block chain
        - Different than Bitcoin
            - Different users, miners, blockchain
            - Bitcoin 2.9
    - Smart Contracts
        - Not smart
        - Not contracts (maybe in some cases)
        - Programs that can hold and control money (code)
    - Example
        - Automated payroll system
    - Is this interesting?
        - Yes -> parts of firms can be replaced
        - No -> volatility, can be worth a lot or a little
    - Make new cryptocurrency on top of existing blockchain
    - General purpose blockchain
- Cryptoeconomics
    - Definition
        - Using of in procotcol defined incentives to build systems with some set of desired properties
- Zero Knowledge Proofs
    - Create a transaction privately with mathematical proof
- P+epsilon attack
- Innovative protocols
- tinyurl.com/develop-smart-contacts
- pennblockchain.com
- github.com/penn-blockchain
    - simple storage