1. Incentives build robustness in **BitTorrent**
2. **Bitcoin**: A Peer-to-Peer Electronic Cash System

1. Cohen
2. Nakamoto

Course announcements

- **Project presentations** schedule finalized
  - 12m talk + 5m Q/A
  - Time must be split evenly between all group members
- **Project report+code** due December 11th by 6PM PT
  - **Report** as pdf via email. Instructions on homepage:
    - *https://www.cs.ubc.ca/~bestchai/teaching/cs538b_2020w1/final-report.html*
  - **Code** as link to a public repository, or a private repo shared with my GitHub id *bestchai*

BitTorrent and BitCoin

- Breakout discussion:
  - **Why** were these systems successfully adopted?

BitTorrent adoption

- Why was BitTorrent successfully adopted?
- *Something people want*: efficient file sharing and **free** access to files they want
- *Easy to use*: simple interface for both file sharers and those downloading the file.
- Simple algorithm = developer friendly
- At the time (early 2000s): bandwidth is a problem, scalable services were rare
- *Scalable* P2P design: easy to add more people to a swarm **(+ the more peers you add, the better the system gets)**
- No centralization = no regulation = rampant illegality = popular! Great for censor-avoidance
- Not that you can't figure out who is who, but it's painful to send take-down notices to 10^6+ people (NATs help with anonymization) + countries/enforcement may not actually care
- Centralized tracker, but can have many of them! — easy to run a tracker: lightweight peer lookup operation pushed to tracker (connectivity metadata); heavy-weight operation to peers (data)
- Incentive-based design ~ fair(?); difficult to mis-use (or to cheat)

BitCoin adoption

- Why was BitCoin successfully adopted?
- Targeted something people needed: digital money; easy concept ~ coins = money
- Incentivized participation with mining ~ *“make free money!”*
- Gradient in mining difficulty: the more people care, the more competition for mining, the more advances in mining “rigs” => mining data centres
- 2008 (reminder: financial crisis) — **timely** to-market; people searching for alternatives to the centralized banking infrastructure
- Finite number of BitCoins can be created = prevents currency inflation (more convincing e-currency)
- **The more miners participate, the more robust the network (to attacks)**
- Designed with few assumptions about **future** power of computers (GPUs/ASICs) ~ **PoW difficulty is set to a constant time rate**
- “Pretty good privacy” — identity separated from the public key on the chain (minimal information for authentication)
- Trading BitCoin — expand reach, but also adds vulnerability to the overall network
- Ali Stage 1: first adopters (anarchists, security/p2p/crypto/criminal experts)
- Ali Stage 2: those who are incentivized by money (e.g., speculators)
- Stage 3: established institutions (mutual funds, ETFs, …)

Bit[Torrent|Coin] adoption

- Why were these systems successfully adopted?

- Adoption curve: initial adoption is driven by “first adopters” != regular (eventual) users

- Dangers of popularity (more attacks, more scrutiny):

  - BitTorrent: authority take-down

  - BitCoin: Mining competition, regulation, attacks

  - Rise of vulnerabilities through pernicious **intermediaries** (those who want to benefit on the way to the protocol/system): malware (bittorrent), brokers/ exchanges (bitcoin; *Quadriga*)

- Different models of scalability

  - **Sharding** into swarms with BitTorrent = more efficient/better

  - A single large (bigger is better) public network = better for cryptocurrencies (security and verifiability/transparency of the blockchain); forking = bad

BitTorrent

- File sharing; create a swarm with a tracker per file
- Break a file into blocks
- Tracker to hand out nodes to peers
- Peers download blocks and exchange them among each other
- Peers incentivized by tit-for-tat
    - You want a bloc (part of a file), you are *forced* to share another block (exploitation)
    - Optimistic unchoke: chance to explore potential peers (exploration)
        - Want: better peers! Peers that will reciprocate (if you are in their top-k list) — finding your niche
        - Global efficiency (~pareto) — you want to globally match peers optimally
            - In reality, BitTorrent is highly sub-optimal
        - Classic balance between explore and exploit
- Lookup / how peers find swarm (.torrent file -> tracker) *out of band*
    - Peer downloads a .torrent file, which includes tracker IP:port and list of block hashes
    - Peer connects to tracker, which gives it peers to connect to
    - The .torrent file is impossible to authenticate content
- Huge contrast with previous systems: focused exclusively on *lookup*
- BitTorrent focus is on efficiency of the file sharing (imagine WWW without a search engine)

BitCoin

- PoW with mining for implementing BFT
  - Highly energy inefficient (compute useless hashes)
  - Finite supply of coins; PoW adjusts; eventually transaction fees are the only incentive to mining
  - Txn validation = wait until some number of blocks follow the block containing the txn (typically 5, for a validation of 6)
- Blockchain: linked chain (difficult to beat)
- Longest chain for resolving concurrency issues
- Icentivize mining: Coinbase transactions due to mining create new coins + txn fees (incentive inclusion of txns in the blocks)
- Transactions are a set of inputs/outputs (chain of transactions lead to coinable or genesis)
- P2P system with no structure: flooding for disseminating txns and blocks
- Bitcoin script language (not Turing complete, stack-based) => smart contracts (Ethereum innovation)
- Efficient storage of transactions with Merkle trees: payment verification
- Fairly centralized development team ; decentralized decision on deployment (miners/others decide which version they get to run) => disagreement in deployment leads to forks (expensive conflict resolution mechanism)
  - Substantial fragmentation in the crypto space (forks: bitcoin cash; alt coins (build on codebase): ripple…)
- Privacy through anonymization
- **Transactions irreversible: if you buy it… you buy it :-) No process for dispute resolution (this is fairly expensive)**

Next: Hyperledger

- Public blockchain (BitCoin) => *Private blockchain* (hyperledger)
    - A very popular “private” blockchain system
    - BFT adoption in the enterprise via blockchains
    - Why *blockchain* and not e.g., *PBFT*?
- Our last paper! (Next week is for project presentations)