Lecture 3 - Centralized and Decentralized Cryptocurrencies

Rylan Schaeffer and Vincent Yang

April 18, 2016

Note: This lecture is based on Princeton University's BTC-Tech: Bitcoin and Cryptocurrency Technologies Spring 2015 course.

Agenda

- Final Project
  - Rudimentary cryptocurrency
  - Groups vs. Pairs vs. Single
  - Report on some study/article about Bitcoin/Cryptocurrencies
  - Other ideas
- Homework 3
- Why decentralize?
- Problems to solve/How proof of work solves them
- Mining/Motivations/Why it's important (Proof of work)
- Shortest vs. Longest blockchain
- Double spending
- 51% attacker

Centralization vs. Decentralization

Centralized Banking

- Centralize: to concentrate under a single authority
- Centralized banking means there is a single institution that manages supply, inflation, and interest.
- Cryptocurrency has to satisfy:
  - Mathematically complex (to avoid fraud and hacker attacks)
  - Preserve user anonymity without being a conduit for tax evasion, money laundering, etc.
  - Decentralized but with *adequate consumer safeguards and protection* - reason will be introduced

Advantages to Centralization

- Automation:

  Easily manage a large number of keys e.g. Mastercard Europe

  Maintain secure infrastructure and improve operations/efficiency
- Centralized Monitoring:

  Record everything that happens easily; brings transparency
- Centralized Policy
- Easily update and track keys
- Easily update cryptographic schemes - swap out algorithms

CentralizedCoin

- I can generate coins, and give them unique ID's. I also sign these coins.
- I can pass them to anyone else - I sign the transaction; recipient can prove it's valid because it has my signature.
- Recipient can sign to pass to someone else.
- Chain of hash pointers can be used to follow it back. = verify
- Double Spending Problem
- Only I can write on the chain - everything has to pass through me
- This is centralized; how do you trust me?

Centralized Cryptocurrencies

- E-Gold (1996)
  - Operated by Gold and Silver Reserve inc
  - Let users open an account denominated in gold; could make instant transfers
  - Grew to 5 million accounts; processing over 2 billion a year
  - "e-Gold Special Purpose Trust" - actually held the gold; could see gold bars with serial numbers per acct.
  - Hackers used flaws in Microsoft Windows OS's and phishing to compromise millions of e-gold accounts
  - People thought it was *anonymous*, but really it was *pseudonymous*. Law enforcement identified many.
  - Ponzi schemes via. eBay
  - Patriot Act, after Sept 11, made operating a money transmitter business without a state money transmitter license a federal crime.
  - Taken down 2007-2013; inability to provide reliable user identification and cut off illegal activity
  - PayPal has done a better job, but still has to deal with the same problems.
  - KYC - process of verifying clients' identity
- DigiCash by Chaum 1990

  - Store money as data on your computer
  - Transfer anonymously
  - Lacked decentralization; the company's servers were used
  - Went bankrupt in 1998

- Can be shut down by gov. at any time

Decentralized Cryptocurrencies

- Decentralization is not all or nothing

  Partially decentralized - SMTP (email)

- How does Bitcoin deal with Decentralization?

  Problems to address, since it's no longer centralized

  1. Who maintains ledger of transactions?
  2. Who determines which transactions are valid/invalid?
  3. Who creates new coins
  4. Who chooses when rules change

Distributed Consensus (Solves 1 and 2)

- Paxos - Method for consensus
- All good nodes agree on the same value (proposed by a good node)

  A good node is one that is being honest

- How it works:
  - All nodes have a sequence of blocks of transactions they have reached consensus on; order is important
  - Each node has a set of outstanding transactions - this solves the problem where not all nodes are aware of all transactions.
  - Each transaction is broadcast to all
  - Doesn't matter if transactions are left out - they get included in the next block.
  - A random node gets to broadcast its block per round
  - Other nodes accept only if valid, and show through including block in hash for next block.
  - Paxos is a Two Phase Commit (2PC): Coordinator suggests value to all nodes, Coordinator (on receiving enough yes's), says value is final - Update. (Problem of falling coordinator is solve by everyone being able).

    Two phases are called *Voting Phase* and *Commit Phase*.

- Consensus without identity - Block Chain
  - Solution: Proof of Work (explanation next)
  - Bitcoin nodes don't have identity; pseudonymity vs. anonymity
  - Implicit Consensus: Random node picks next block in the chain, and other nodes vote by extending or ignoring.

    Implicit because implied though not plainly expressed

- Byzantine Generals: How to make a safe decision while communicating with other parties over an insecure network

  Example: 500 - split into 5 groups. 300 defending. 1 group corrupt.

  Give example then consider: Must wait 10 minutes to give message, and must embed all past messages in your own.

  Work is hard, but easy to check if it's been done.

  Blockchain is important because it is a way of representing the truth, without any one gatekeeper.

  Chosen node chooses what the next block is; voting is by what is extended by the others
  Source: `http://www.dugcampbell.com/byzantine-generals-problem/`
- Works because difficult (impossible) to subvert.
- "Zero confirmation transaction" is a bad idea.
- The more confirmations, the better the choice. Bitcoin uses 6.

The Solution: Proof of work:

- Select nodes in proportion to computational power
- *Give example of leading 0's*
- Difficult to compute
- Puzzle Friendliness: No solving strategy for finding $H(k|x) = y$ is better than trying random values of x.
- Motivation to subvert the process (picking a hopefully honest node), so reward honest nodes
- Use bitcoins to incentivize honest nodes - mining. Reward only if it becomes legitimate transaction
- Every 210,000 blocks (4 years), block reward is cut in half. Geometric sum - 21 million bitcoins
- Nonce published as part of the block.
- Proof of work details
  - Mining: Hash function with nonce appended to beginning (ex: 0's)
  - HashCash - with SHA-256 (used twice)
  - Less than some value
  - Items used: version, prevBlockHash, merkleRoot, timestamp, bits, nonce
  - Selecting nodes based on processing power/proportional
  - Hash puzzles - to make blocks, it needs to find a nonce where
  - $H(nonce \mid\mid prev\_hash \mid\mid tx \mid\mid tx \mid\mid ... \mid\mid tx) \ < \ target$
  - Nonce: Random number that is only used once
  - Hash puzzle properties: difficult, parameterizable cost (10 minutes variable target), trivial to verify
  - 10 minutes: reduce inefficiency from having many blocks
  - $meantimetonextblock = \frac{10minutes}{fraction\ of\ hash\ power}$
  - proof of stake - proportion to ownership of currency (used in other cryptocurrencies)
  - http://www.righto.com/2014/09/mining-bitcoin-with-pencil-and-paper.html
- Incentives: Solves 3

- Can't penalize, but can reward nodes for working correctly.
- *Incentive 1*: Block Reward (25 BTC, halves every 4 years). (Solves 3)

  21 million max - block reward is how new coins are created; run out in 2140.
- *Incentive 2*: Transaction Fee

  Incentive to have your transaction verified
- Remaining problems:

  How to pick random node

  How to avoid free-for-all rewards

• The miner gains if reward > cost

  reward = block reward + tx fees

  mining cost = hardware cost + operating costs

• Aspects of decentralization in Bitcoin

  - Peer to peer network, open to anyone, low barrier for entry
  - Mining is open to everyone
  - Updates to software - core developers trusted by the community who have a lot of power (Solve Problem 4)

• New Problems from being Decentralized and Attacks:

  - Fischer-Lynch-Paterson: concensus impossible with a single faulty node.
    solved with 6 blocks

    Can't penalize those who try to double spend, since there's no way to tell
  - Blocks have a tendency to extend the block they hear about first
  - Orphan Block
  - Latency, not all nodes connected, internet connection, malicious nodes
  - Attacks:
  - Stealing - even if Alice gets to decide the next block, she can't steal because she has to create a valid transaction; can't forge signatures
  - Denial of Service - even if Alice never validates Bob's transactions, an honest node will eventually do so.
  - Double Spend - DRAW DIAGRAM
    Say Alice pays Bob, and an honest node broadcasts this. Bob accepts that he's been paid. Alice then gets to broadcast her own transaction. She then makes a block with the *prevBlock* hash as the one before her payment to Bob. Only one of these blocks will be accepted.
  - Sybil attack

    Can't gain more power by having more accounts

    Satoshi's original paper had 1 cpu = 1 vote
  - Zero-confirmation transaction

    Bob gives Alice product before transaction has been verified

    6 blocks; double spend probability goes down exponentially

    Never a 100% guarantee

• Solves the problem of not trusting a central authority - Problem 4

• 51% attacker

  1. CANNOT Steal Bitcoin
  2. CANNOT change block reward
  3. Suppress transactions
  4. Destroy confidence in Bitcoin

Changing the rules

- Two types of changes - soft forks; hard forks

  Soft forks are forward compatible; new rules are subset of old rules. Only applied if over 51% agree.

  Hard forks are backward compatible; old rules are subset of new rules. Everyone needs to upgrade to new.

Source: `http://people.dsv.su.se/~matei/courses/IK2001_SJE/Chaum90.pdf`
Source: `http://blog.koehntopp.de/uploads/Chaum.BlindSigForPayment.1982.PDF`