

Lecture 3 - Centralized and Decentralized Cryptocurrencies

Rylan Schaeffer and Vincent Yang

April 6, 2016

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

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)
 - Decentralized but with *adequate consumer safeguards and protection*
 - Preserve user anonymity without being a conduit for tax evasion, money laundering, etc.

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
- Liberty Reserve
 - Shut down, also by Patriot Act, in May 2013.
- E-Gold and Liberty Reserve were popularly used for money laundering and shut down
- Can be shut down by the government at any time
- 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

Decentralized Cryptocurrencies

- Decentralization is not all or nothing
 - Partially decentralized - SMTP (email)
- Bitcoin and Decentralization
 - How does Bitcoin deal with decentralization?
 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
5. How do bitcoins gain value

Consensus (distributed consensus)

Distributed consensus protocol: two properties

1. Must end with all nodes in agreement, and value has to have been generated by honest node
2. When someone wants to make a transaction, the person broadcasts to the nodes that make up the network.

There is no requirement for the recipient to be on the network

Must come to consensus on which transactions were broadcast in what order

Each node has:

1. Single, global ledger that each node has a copy of
2. Pool of transactions that have been received but not verified (varies from node to node)

- How do nodes come to consensus?

At regular intervals, every node proposes its own pool to be next block

Consensus protocol with each node's input as its own block

If this protocol succeeds, then a valid block will be chosen - it doesn't matter how many people propose this block

Doesn't matter if transactions get left out; they could just be in the next block

- Problems:

Latency, not all nodes connected, internet connection, malicious nodes

Global time does not exist

- Byzantine Generals

- Paxos

Makes compromises - never produces inconsistent result, but under rare conditions, protocol can get stuck

- How Bitcoin breaks traditional assumptions

Works better in practice than in theory - no accurate model yet exists

Only solves problems in currency context due to incentives(not distributed databases, which is where the problem originated)

Embraces randomness - consensus happens over an hour, nodes can't be certain of what's in/out; the odds just change exponentially

- Block Chain

- Consensus without identity

- Sybil attack

Can't gain more power by having more accounts

Satoshi's original paper had 1 cpu = 1 vote

- Implicit Consensus:

Chosen node chooses what the next block is; voting is by what is extended by the others

- Bitcoin consensus algorithm (simplified)

1. New transactions broadcast to all nodes

2. Each node collects transactions
 3. Random node gets to broadcast its block per round
 4. Other nodes accept only if valid
 5. Nodes show acceptance through including block in hash for next block
- Attacks
 - Stealing - even if Alice gets to decide next block, she can't steal because she has to create 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 - Say Alice pays Bob, and an honest node broadcasts this. and Bob accepts that he's been paid. Alice then gets to broadcast her own transaction. She then makes a block with the `emphprevBlock` hash as the one before her payment to Bob. Only one of these blocks will be accepted.
 - Blocks have a tendency to extend the block they hear about first
 - Orphan Block
 - Zero-confirmation transaction
 - Bob gives Alice product before transaction has been verified
 - 6 blocks; double spend probability goes down exponentially
 - Never a 100% guarantee
- Incentives/Proof of work
 - Motivation to subvert the process (picking a hopefully honest node), so reward honest nodes
 - HashCash - with SHA-256
 - Can't penalize those who try to double spend, since there's no way to tell
 - 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
 - Incentives Part 2 - Transaction fees
 - Incentive to have your transaction verified
 - New Problems With Incentives
 - Random node
 - Everyone wants to run nodes for rewards
 - Sybil nodes to subvert process
 - Solution: proof of work
 - Proof of work
 - Selecting nodes based on processing power/proportional
 - Hopefully not monopolized
 - proof of stake - proportion to ownership of currency (used in other cryptocurrencies)
 - Hash puzzles - to make blocks, it needs to find a nonce where
$$H(\text{nonce} || \text{prev_hash} || \text{tx} || \text{tx} || \dots || \text{tx}) < \text{target}$$
 - 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
 - $$\text{meantimetonextblock} = \frac{10\text{minutes}}{\text{fraction of hash power}}$$
 - The miner gains if reward \geq cost
 - reward = block reward + tx fees
 - mining cost = hardware cost + operating costs

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>