Bitcoin

Tom Anderson

Bitcoin

- Network of bitcoin peers (servers) run by volunteers
- Peers are not trusted: may be greedy or corrupt
- Each peer knows about all bitcoins and transactions
- Transaction (sender -> receiver):
  - sender sends transaction info to some peers
  - peers check that bitcoin hasn't already been spent
  - peers flood transaction to all other peers
  - receiver checks that lots of peers have seen transaction

Purses

- Instead of discrete coins, aggregate into purse
- Purse
  - Controlled by a public key (only owner can spend)
  - Aggregate value = sum over history of in/outs
  - Peers check remaining balance > transfer
  - Peers only accept valid transfers
- Newly minted coins go into a single purse

Block Chain

- Block
  - Hash of previous block (no undo)
  - Set of transaction (transfer)
  - Assignment of newly minted coins to purse
  - Nonce st SHA of block < threshold
- Transaction
  - ID of source of funds (unspent transaction)
  - Amount to be transferred
  - Public key of new owner
  - Signed by owner of source of funds

Example

- 0.1 Bitcoin owned by Jialin (who received it in payment from Ellis)
- T7: pub(Jialin), hash(T6), 0.1 BT, sig(Ellis)
- Jialin buys a hamburger from Doug
- Doug gives Jialin a public key (bitcoin "address")
  - Perhaps create a new address just for this purchase
- Jialin creates a new transaction and signs it
- T8: pub(Doug), hash(T7), 0.1 BT, sig(Jialin)

Example

- T8: pub(Doug), hash(T7), 0.1 BT, sig(Jialin)
- Jialin sends T8 to bitcoin peers; peers flood
- Honest peers verify that
  - hash(T7) contains enough value
  - T8's sig() corresponds to T7's pub()
- Peer finds valid nonce for block containing T8
- Broadcasts nonce to other peers
- Next block will contain hash of block with T8

Double Spending

Suppose Jialin creates two transactions spending the same bitcoin balance

- Jialin->Doug, Jialin->Tom

How long should Doug wait before giving Jialin the hamburger?

Until Doug sees Jialin flood the transaction to many peers?

Double Spending

How long should Doug wait before giving Jialin the hamburger?

Until Doug sees Jialin flood the transaction to many peers?

- not in the chain, Jialin might flood conflicting xaction

Until Doug sees one peer with chain containing xaction?

Double Spending

How long should Doug wait before giving Jialin the hamburger?

Until Doug sees Jialin flood the transaction to many peers?

- not in the chain, Jialin might flood conflicting xaction

Until Doug sees one peer with chain containing xaction?

- maybe that peer is corrupt, in league with Jialin

Until Doug sees lots of peers with chain containing xaction?

Double Spending

How long should Doug wait before giving Jialin the hamburger?

Until Doug sees Jialin flood the transaction to many peers?

- not in the chain, Jialin might flood conflicting xaction

Until Doug sees one peer with chain containing xaction?

- maybe that peer is corrupt, in league with Jialin

Until Doug sees lots of peers with chain containing xaction?

- risky -- some other chain may win
- perhaps that chain won't have transaction

Until Doug sees chain with multiple blocks after transaction?

- slim chance attacker can catch up

Reward

- Solution is broadcast to every replica; what keeps replicas from stealing the solution?
- Every replica works on a slightly different puzzle
- Ellis works on:
  - SHA(previous hash, mint coin and give it to Ellis, set of transactions, nonce) < target
- Jialin works on:
  - SHA(previous hash, mint coin and give it to Jialin, set of transactions, nonce) < target

When Nonce is Found

Replicas have a choice:

- Ignore the answer and continue to try to find another one
- Take the answer as a given and work on the next puzzle.

Which should it choose?

- If more than half of the computational power chooses (b), replica should choose (b)

Who Wins?

- If two nodes find the nonce at about the same time, who wins?
- Depends on solution to the next puzzle!
- Everyone has an incentive to work on chain that others will work on
  - If next solution uses A's solution, A wins
  - If next solution uses B's solution, B wins
- In practice, choose the nonce that is less likely (smaller)

Who Wins?

- Replicas have an incentive to prevent others from announcing their solutions
- DoS attacks
  - flood replica with traffic so TCP connections fail
- BGP prefix hijacking
  - Internet is shortest path routing, without security
  - Announce your network has shorter path to target replica, then don't deliver the traffic

Mining Groups

- Reward is (very) sporadic: if 1M replicas search for hash, each will win once every few decades.
- Pool resources: pay nodes to look for solutions
- If Doug is a coordinator, ask replicas to:
  - SHA(previous hash, mint coin for Doug, msg, nonce)
- Why would anyone do this for Doug?
  - Small reward for incremental proof of work
  - Ex: hand out 0.001 bitcoin for nonces with 60 zeros

Serial Numbers Revisited

- Proof of work solves how we create new coins
  - Every 10 minutes, another reward
- What about inflation?
  - Reward decreases by 2x every few years
  - Increasing number of coins in circulation
  - Fixed total number of coins (93% of total already mined)
- Do miners stop working when reward stops?

Theory of Money

- Why do bitcoins have value?
- Why does gold?
- Why does cash?
- Why does Facebook or Google stock?

Who Wins?

- Bitcoin founder(s) performed early mining
  - Reserved 1M Bitcoins for their own use = $2B
  - But haven't spent them (bitcoin log is public)
  - Is it possible for them to sell?
  - Backlog equal to 18 months of mining (!)

Transaction Reward

- When a replica receives a request what should it do?
  - Ignore it?
  - Add it to the next batch?
  - Forward it?

Transaction Reward

- When a replica receives a request what should it do?
  - Ignore it?
  - Add it to the next batch?
  - Forward it?
- Transactions can have multiple outputs
  - Main payment to recipient
  - Side payment to the winning miner

Private Exchanges

- Bitcoin
  - can only perform a few operations per second
  - performs operations slowly (minutes to confirm)
  - No accountability if seller reneges
- Private exchanges/escrow
  - Both parties trust exchange
  - Execute operations on internal account record
  - Exports internal account to cash or public bitcoin
- How is this different from a bank?

Bitcoin and Other Cryptocurrencies

- Bitcoin is not the only electronic cash standard
- Zerocoin
  - Better anonymity (money laundering)
- Ethereum
  - Better scripting (create new types of coins)
- Ripple
  - Public blockchain, but with stable price

Bitcoin Discussion

- Where does value of a Bitcoin come from?
- How long will SHA-256 last?
- How do we make changes to the protocol?
- Is Bitcoin anonymous? Linkability
- Is Bitcoin ethical? Ransomware
- Private exchanges and security
- Non-reversible (vs. credit cards)
- Attacks: mining monopolies, BGP route hijacks, …