Bitcoin

- Private Key: L2X6r6cVAY7Ji5svGoCjEWW1oMfW6rTbpDBGhssGoWP9DdXMF7c1

- Public Key: 1A6vdRLNbaWT4PyhgXRxZ3BGR5WVYfzXBk

Bitcoin

- To generate a valid transaction:
  - Create a tx output with an amount of BTC <= the amount of inputs you have
  - Using your private key, generate a digital signature to add to the tx
  - Because the tx info will be different every time, so will the digital signature; they are not reusable

- Digital Signature Math:
  - Elliptic curve digital signature algorithm

Bitcoin

Account Balances

- No “account balances” are kept by the Bitcoin protocol
  - Ownership of funds is verified by links to previous txs (UTXO Model)

- In order to send a valid tx, a user must reference previous tx where they received BTC (inputs).

Bitcoin

- Essentially all BTC txs are linked to previous txs

- How can we trust previous tx?
  - We don’t need to, their inputs can be checked too
  - If we run a full node client, the first thing necessary to allow the software to work, is to download the entire history all the way back to the first tx

Bitcoin

- All inputs must be spent in their entirety
  - If you receive an input larger than an output you'd like to spend, you need to send the remaining amount to yourself as change

- An input can only be used once, and after that is considered spent
  - This eliminates "double spend" potential

Bitcoin

Complex Txs

- Bitcoin has a scripting language that allows for more complex txs
  - MultiSig
  - TimeLock
  - Escrow

- Not without risk!
  - 2600+ BTC were lost in 2011 due to improperly generated address

Bitcoin

Bitcoin is not anonymous

- Bitcoin is pseudonymous; users have a static identifier (public key), that is not necessarily linked to their identity

- If proper internet security is applied, minimal personal info will be revealed

Bitcoin

Hierarchical Deterministic Wallets

- Standard software for cold storage wallets
  - Generates a new receive address for every tx

- This allows for obfuscation of identity because wallet addresses are only used one time

Bitcoin

Public/Private Key Creation

- The “trustless” nature of the protocol does not require any permission to “create”, or generate a pub/priv key pair

- Offline software can do so, using a random function to generate the keys

Bitcoin

Generating Key Pairs

- Because of the very high number of possible addresses, one can generate it at random and a collision is very unlikely (however possible)

- Total number of possible addresses: (1.46 x 10^48 || 2^160)

Analogy: Total # of grains of sand on earth = 7, 500, 000, 000, 000, 000, 000

Bitcoin

Recap

- Digital Signature
  - Creates a value that can only be produced by the owner of the funds (holder of the private key) using cryptography

- Referenced Txs
  - All possible txs will have to be link to previous txs going back the entire history of the chain

Bitcoin

Potential Security Vulnerability: Tx Ordering

- Because txs are passed among multiple nodes on the network, there's no guarantee that the order in which they are received is the in which they were created
- To combat this, txs are grouped into blocks which are then considered to be executed at the same time (regardless of when the tx was broadcast)
- Txs exist in 2 discrete states: Unconfirmed, Confirmed

Bitcoin

Generating a New Block

- Because any node can suggest a block to the network, how does the network decide which suggestion to pick?

- Each valid block must contain the answer to a special mathematical problem

Bitcoin

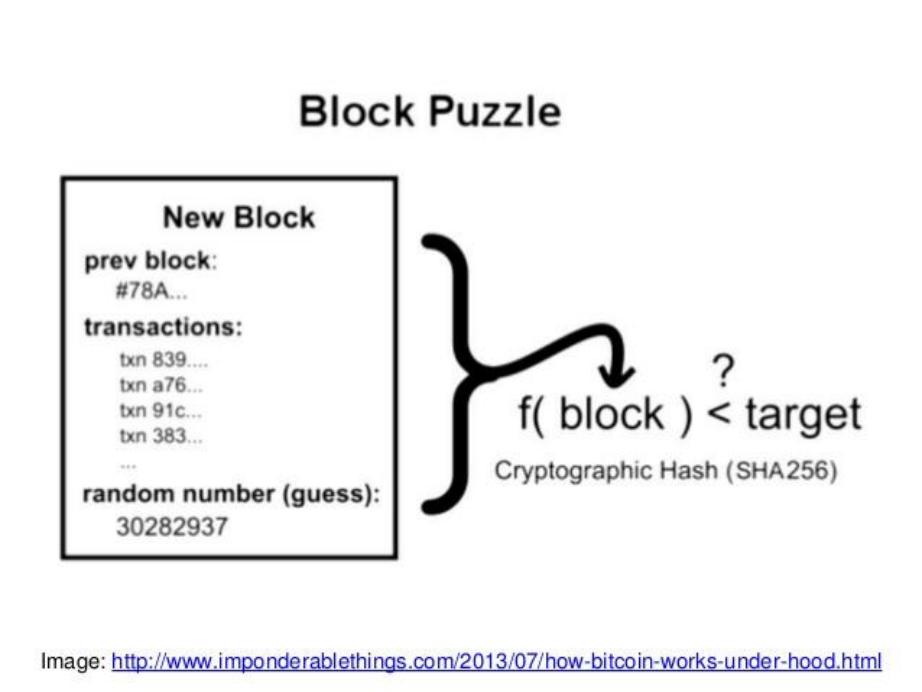

Image: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Bitcoin

- Bitcoin uses the SHA256 hash function

- https://passwordsgenerator.net/sha256-hash-generator/

Bitcoin

- Because the output cannot be reverse computed even the most powerful computer are reduced to guessing

- The computers take all of the information required in the block (txs, previous hash, timestamp, etc...) and find the missing nonce that gives the required number of leading 0s.

Bitcoin

- The Bitcoin network is designed to confirm new blocks every 10 minutes

- In order to maintain this schedule, the network difficulty is assessed every 2016 blocks (roughly 2 weeks), and adjusted if needed

- The difficulty of the network is increased or decreased by the amount of leading 0s required

Bitcoin

- In the rare occasion that a block is solved simultaneously by more than 1 miner, the nodes use the block they received first

- The tie becomes broken when the next block gets solved. The rule is that nodes will always switch to the longest chain available

- Miners must always be mining for the chain with the most “work”

Bitcoin

- If a tx is included in one of the shorter chains, it will eventually return to the Mempool as an unconfirmed tx

- The current precedent for mining pools solving multiple blocks is 6, so it is standard to wait for 6 confirmations to consider a mined tx secure

Bitcoin

Mining and 51% Attacks

- What if an attacker has lots of computer equipment to attack the network?
    - If the attacker has 50% of the network mining power, they would still only have a 50% chance of solving a block before the rest of the network
    - This makes attacking the network very expensive with only a small possible benefit

Bitcoin

Mining and 51% Attacks

- Because of all of the work done to find the blockhash of previous txs, if someone were to try to invalidate a block further back in the chain, they would have to do all of the “work” to solve the blocks up to the present

Bitcoin

Blockchain 101 - A Visual Demo

- https://www.youtube.com/watch?v=_160oMzblY8

The interactive version is available here:

- http://anders.com/blockchain/

Bitcoin

Bitcoin Generation - The Coinbase

- In order to create incentives for miners to contribute computational work to the network, the miner who solves a block receives a block reward

- This coinbase tx is given as an input to that user’s address

Bitcoin

- The block reward can be seen as a temporary subsidy, provided by the protocol to create financial incentives to bring the network to scale, as well as distribute the tokens in a slow, predictable means

- Total BTC in circulation: 17, 572, 100

- Date scheduled for last BTC to be mined: 2140

Bitcoin

- Block reward at instantiation of protocol : 50BTC

- Around November 2012 reward was reduced to 25

- Around July 2016 reward was reduced to 12.5

Bitcoin

- Miners also receive all of the tx fees in the block they solve

- The protocol has been designed with the intention that once it meets its intended scale, the block reward subsidy will no longer be required, and the tx fees will be enough to incentivize mining

- Tx fees are decided by market economics. During December 2017, BTC tx fees reached as high as $50USD

Bitcoin

Mining Pools

- To flatten the variance of mining, many miners join mining pools which distribute mining rewards proportional to computation contributed

- These pools can be large, which can be problematic and undermine the ethos of decentralisation that the network was built on