Blockchain
with some Bitcoin

Jadi

Jadi

- Serious
- Not much serious

- Jadi.net
- (insta) jadijadinet
- (twtr) jadi
- (tlrgrm) jadinet

You

- Who
- Why?
- How?

- What is this class?

History 1/2

- Need
    - Exchange
    - Value
    - Coins
    - Notes
    - Bank Notes
    - Digital notes
- Prehistory (b coin and others)
    - Anonymity vs Double Spending vs centralized
    - A lot of tries, but all failed
    - You had to give money to get money

History 2/2

- Satoshi Nakamoto
- Why anonymous?
- Legends
- 2008 till now

lessons?

- Create a community
- Never Give Up!

This class

- BC vs BC
- Some math
- Some Programming
- Some Politics
- Some.. what else? You say!

Bitcoin

- Decentralized
- To make value, you need something scarce
- Some Programming
- Some Politics
- Some.. what else? You say!

Basics

- We need security
  - Is the coin genuine?
  - Is the history written on stone?
  - Does someone double spends?
  -
- Cryptography
  - Hashes
  - Digital signatures

Hash

- General Properties
  - Free input size
  - Specific output length
  - Efficiently Computable; O(n)
- Cryptographic hash
  - Collision resistance
    - Nobody can find collision
    - Even with Birthday Paradox
  - Hiding
    - One way
    - Used in commitments
  - Puzzle friendliness
    - Difficult to bruteforce
- Sha256
- Hash pointer: a pointer with a hash of data

Blocks

- TRX
- Timestamps
- Blocks are trxs, timestamps, previous hash and have a HASH
- Hash
  - Deterministic
  - One way
- Now lets create a blockchain

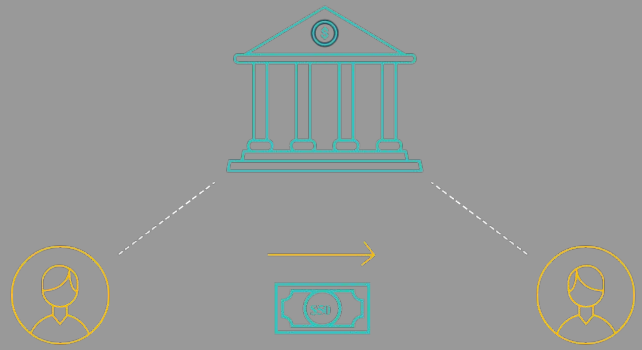
Signatures

- 1. Only you can sign but everyone can verify 2. Is on a specific document
- 1. (sk, pk) = GenKey(size) 2. Sig = (sk, msg) 3. IsValid = (pk, msg, sig)
- Bitcoin uses Elliptic CUrve Digital Signature Algorithm (ECDSA), strange choice by Satoshi
- pk is your identity
  - No need for a username
  - No need for authority
  - You address is the hash of your pk
  - You can create as much as pks you want, but people can connect the dots too

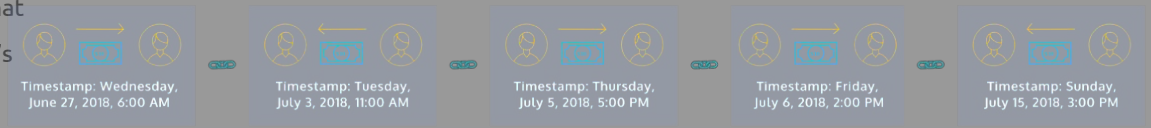
The blockchain is similar to a permanent book of records that keeps a log of all transactions that have taken place in chronological order.

Let's envision a bank transaction in which there are three parties: the sender, the bank, and the recipient. In order to ensure that there are no fraudulent transactions, the bank acts as the central authority between the parties.
The blockchain also logs transactions between senders and receivers, except there is no bank or central authority. Instead, the blockchain relies on a public network of computers to verify the transaction. The blockchain is just an accurate, and permanent record of all the transactions that have happened amongst the members in that blockchain's network. In this analogy, each block in the blockchain represents a transaction, and each transaction is connected to the prior transaction to form the entire connected blockchain.

What is a blockchain?



Timestamp: Thursday, July 5, 2018, 5:00 PM



How blocks are created

- TRXs are added to the mempool
- When we have enough TRXs, it is called unconfirmed block
- We move to the next pool and will try to confirm the last block
- Announce our block and 51% should confirm (consensus)

- But what happens if someone tampers a block? ;)
- What happens if he recalculates other hashes too? ;)

Decentralized

1. Who maintains the ledger of transactions?
2. Who has authority over which transactions are valid?
3. Who creates new bitcoins?
4. Who determines how the rules of the system change?
5. How do bitcoins acquire exchange value?

Different levels, internet, SNMP, messaging (say Yahoo!)

Consensus

- Difficult or impossible in the presence of malicious; Byzantine Generals Problem
- But sometimes practice is better than theory :D especially in these two conditions:
    - We have incentives for good people
    - Random people will decide the next block
- Anonymous consensus is even more difficult
    - Sybil attack
    - Random choice

Implicit Consensus

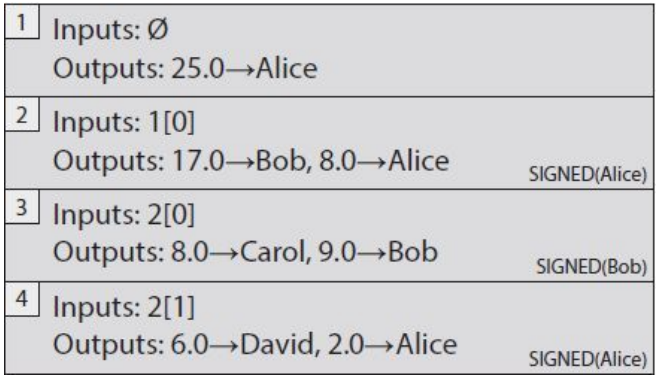
- In 5 steps
    a. New transactions are broadcast to all nodes.
    b. Each node collects new transactions into a block.
    c. In each round, a *random* node gets to broadcast its block.
    d. Other nodes accept the block only if all transactions in it are valid (unspent, valid signatures).
    e. Nodes express their acceptance of the block by including its hash in the next block they create.
- Lets review 3 main attacks: stealing bitcoins, DOS, Double Spend,

Mechanics of bitcoin

- How data is stored
- How network works
- Limitations

TRXs

- Account based? No
  - Common Idea: Jadi gave 15 to Zahra
  - very difficult to check the validity
- Ledger based? Yes
  - Saved TRXs with their input and output
  - Change address, because we have to consume the whole coins
- Scripting
- MultiSig



Bitcoin Network

- Peer to Peer
- TCP and random topology
- Anyone can download the client and join; EQUAL
    - You will need a seed note
    - Others will start to forget you if you are not active for 3 hours
- Flood or Gossip protocol. You tell the people you know, they check and pass if checks are passed
    - Latency can lead to different mempool, but mining will decide the ties (race condition)
- Around 10K full chain nodes are 24/7 active
- There are also simplified Payment Verification nodes (SPV) or lightweight nodes. These only contain headers, so only 100s of MBs instead of 100s of GBs

Bitcoin Limitations

- Created in 2009
- Each block is 1MB, each TRX is 250 bytes -> each block contain 4K TRX only
- One block every 10 minute -> 7 TPS! (VISA handels around 2K TPS and can handle 10K TPS peak)
- Cryptographic algorithm is ECDSA. Some believe this will be broken during bitcoins life span
- Solution? Soft and hard forks

so... there will be forks!


KEEP
CALM
AND
CARRY
ON

How to store

- availability, security, and convenience
- Wallets
  - Base 58 & QR Codes
  - Hot vs Cold storage (paper, brain, tamper resistance devices)
  - secret sharing (2 out of 2 R xor S), (2 out of N) points on axis, (N out of K): higher levels of formula (^2, ...)
  - banks : bank run, ponzi scheme, hack (Mt. Gox case), they need 3 to 10% liquidity
  - Online wallet/exchange (bank regulations, Proof of reserve, Proof of Liabilities)
  - Payment services
  - Currency (FIAT) exchanges (based on supply & demand)

Bitcoin Mining

- What is the task? Finding a valid block, less than 2^68 nonces will work
- Difficulty changes every 2016 blocks
- Hardware (CPU (20M), GPU (200M), FPGA(1G), ASIC(14G))
- Energy consumption
    - Thermodynamic Limits (Landauer's principle: each bit $kT \ln 2$ joules)
    - Repurposing energy!
    - Electricity into cash
- Pools
    - Syndicate idea
    - Anti cheat
    - 51% GHash

Mining Attacks

- Forking Attack (Spending and then mining the previous block)
- Forking via Bribery (clever idea? Run a pool with loss of revenue, or give tips in blocks!)
- Block Withholding Attacks = Selfish Mining
- Blacklisting or Punitive Forking (announcing that you won't work on a chain if it contains blah blah)
- Feather Forking (just like punitive forking but just for a short period of time)

Future? Moving toward mining based on TRX Fees

Anonymity

- Anonymous = without name
- Anonymous vs pseudo-anonymous (reddit vs 4chan) vs unlikability
- In bitcoin, you don’t have a real name but you have an address
- Side channels (big data)
- It is difficult to reach Unlikability because receiver sees the senders address
- Why anonymity is needed?
    - To reach the traditional privacy we had
    - To reach a new level of privacy
        - Salary, class fees, paying subcontractors will reveal business plans
        - It is difficult to exchange fiat with cryptocurrency, laundering is difficult
- TOR sample

deanonymyzation

- Check wikileaks donation page
- When creating TRXs, we are joining coins: most of the time shared spending is evidence of joint control of the different input addresses
- Attacks
  - Clustering
  - Direct trx with one person
  - Service providers, exchanges, fiat money
  - Carelessness; say posting your address to a forum for donations
  - Network layer: sudden connection to a lot of bitcoin nodes and a TRX is created there. 2011 black hat -> use TOR

Deanonymyzation defences

- Stealth addresses: g^x is the public key and the wallet address is $H(g^x)$, so bob will publish g^x , alice will choose r, calculate g^{xr} and do the trx to that and inform bob about r
- Mixing: if you want anonymity, use an intermediary
  - Online Wallets (do not promise, they know a lot!)
  - Dedicated mixing services (you have to trust)
  - Decentralized mixing (better anonymity, no theft based on protocol, no need to wait or trust an agent)
    - CoinJoin (people participate in Inputs)
    - Merge Avoidance (Target provides many Outputs for one TRX)
    - ZeroCoin and Zerocash
    - Check https://bitcoin.org/en/payment-processing-guide#introduction

Consensus

- About…
  - Rules
    - Programmers
    - Stakeholders (minser, investors, merchants, payment services)
    - Sample? bip-0148
  - Coin values
  - History of the blockchain
- Rule book? Software. Discussion? BIPs
- Other pressures? Governments…

Alternates 1/2

- Essential Puzzle Requirements
  - Quick to verify
  - Adjustable Difficulty
  - Progress free / Memoryless

(Proportional chance)

- ASIC resistance puzzles (one-CPU-one-vote)
  - Memory hard
    - Equihash (ZCash)
    - Scrypt (litecoin)
  - X11

```
1 def scrypt(N, seed):
2     V = [0] * N // initialize memory buffer of length N

    // Fill up memory buffer with pseudorandom data
3   V[0] = seed
4   for i = 1 to N:
5      V[i] = SHA-256(V[i-1])

    // Access memory buffer in a pseudorandom order
6   X = SHA-256(V[N-1])
7   for i = 1 to N:
8      j = X % N // Choose a random index based on X
9      X = SHA-256(X ^ V[j]) // Update X based on this index

10   return X
```

Alternates 2/2

- Proof of useful work (SETI, Folding, Prime search)
- Proof of storage (Permacoin, BurstCoin)
- Nonoutsourcable
    - Rewarding sabotage
    - We can change the puzzle from “find a block whose hash is below a certain target” to “find a block for which the hash of *a signature* on the block is below a certain target.” This signature must be computed using the same public key used in the coinbase transaction.
- Proof of stake or virtual mining (PeerCoin based on coinage and sha256, DASH is mixed X11/POS)

Finish!