# the bitcoin protocol

some interesting tid-bits

Stop me with any questions, this is meant to be a discussion. No one really understands this technology fully! (unsolved problems galore…)

*sorry if that offended anyone!

# how does bitcoin work on the protocol level?

- On a high level we have three important concepts:
  - 1) Transactions
  - 2) Mining
  - 3) Blocks

# I will talk about

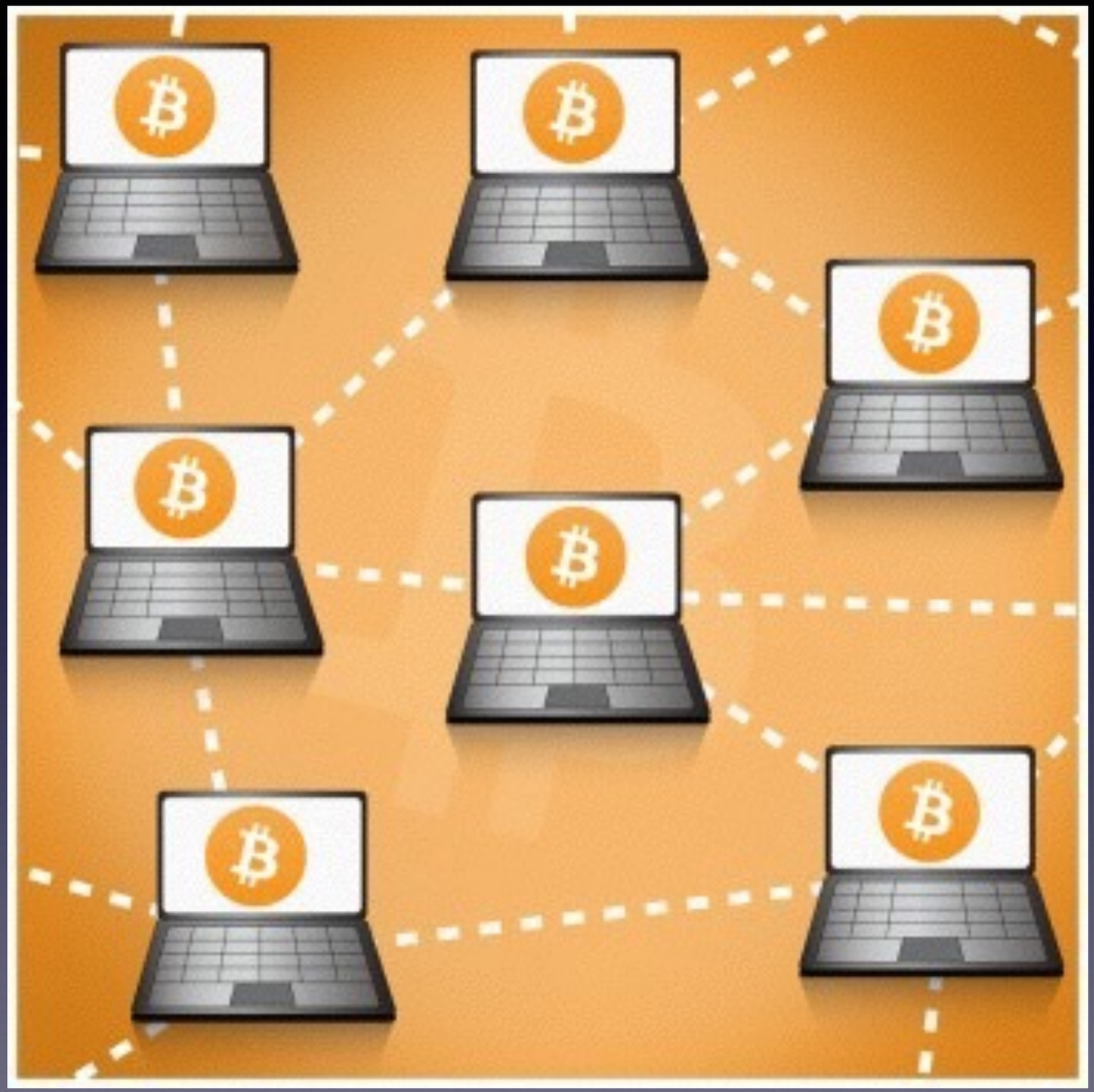
- Transactions mostly, and some blocks

# How does an exchange of money work?

- How does paying a friend work?
- How does a system like Visa work?
- How is bitcoin different from something like Visa?

# Bitcoin works by propagating transactions on a peer-to-peer network

- Instead of posting a transaction to a single company's server (a la Visa), you send your transaction to peer nodes
- Peers then send your transaction to other peers!



# Transactions

- Fundamental unit of exchange in bitcoin
- Think about each a Bitcoin transaction as giving somebody a bill that cannot be counterfeited, nor be invalidated! (As good as gold… ha.)

# What makes a transaction?

- It must be atomic. This means that it either happens, or it does not.
- Transaction outputs can only be spent once. They are non-refundable. What does this mean?

# Non-refundable

- Why is this important?
- If they are refundable, who decides how to refund it? Imagine a situation where you have acquired a stolen $100 bill (legally). Should the owner be able to claim that from you?

# Whats does a transaction look like?

- It’s just data. This data is sent over the network in JSON form (Javascript Object Notation)
- http://explorer.chain.com/transactions/bc44bf4ce6bf358a9e7cc75fffa8fcac5195b1025cbbf87bf99908b7d74b3210

# Ok ok. Seems pretty normal.

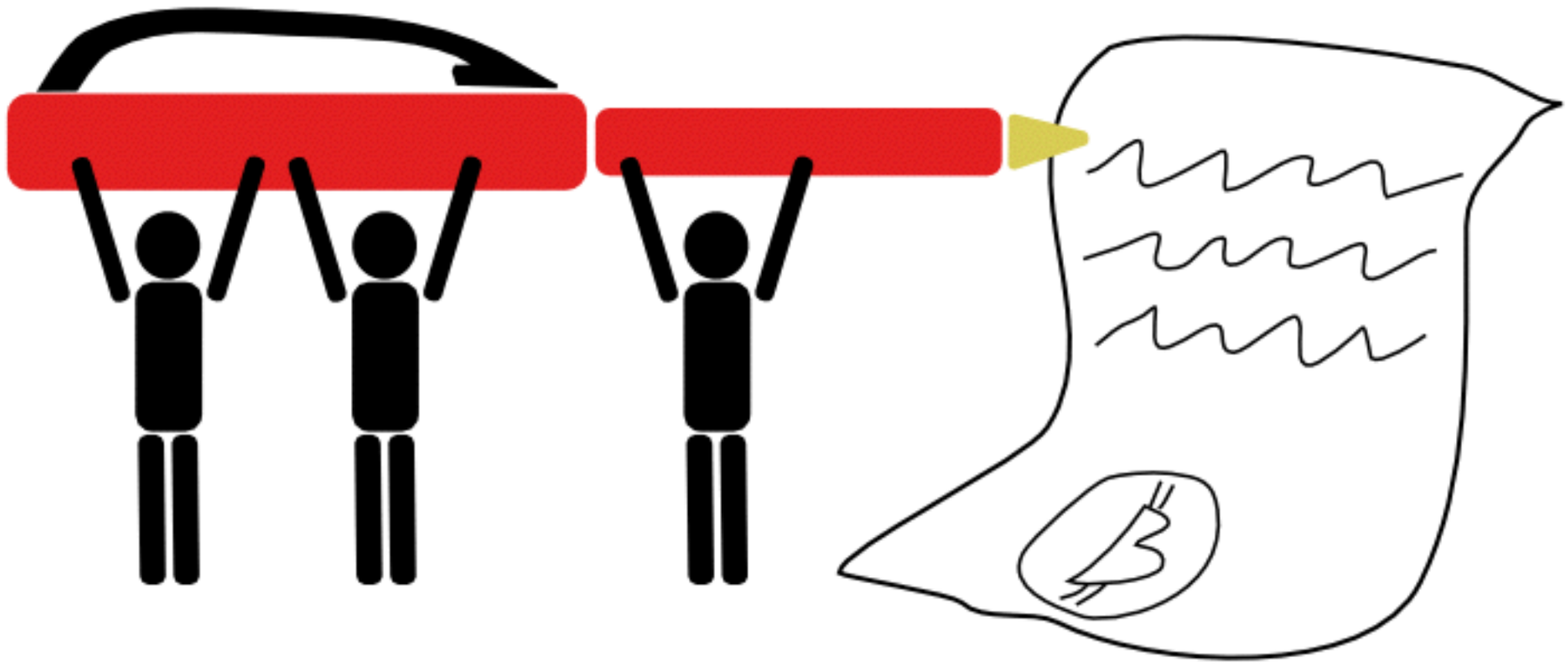
- What is so cool about this transaction?
- Who has experience in programming?

# Addresses can be programmed!

- A bitcoin wallet require a script in order to spend from an address
- You could write a script which allows ANYONE to spend from the wallet (giveaway?)
- You could write a script that requires 2 of 3 people to sign the transaction…

# Multi-sig transactions

- This allows for powerful financial tools
- Imagine you wanted to setup a wallet with a friend, that required both of you to sign off on a transaction
- What about a trust-less system for contracts?



This is a real live bitcoin transaction.

Not really, but hey.

# Bitcoin Bookie

- This was an idea we implemented for a hackathon 2 weeks ago in Vegas, it is a app where you can bet on fantasy sports and not trust a bookie.
- It allows for 3 people to create a wallet together that requires 2 signatures to spend the bitcoin
- Imagine you wanted to send money to a long lost relative at some point in time: you could do this without ever “giving” anyone else possession of your bitcoin

# NLOCKTIME

- “nLockTime is a parameter that can be attached to a transaction, that mandates a minimal time (specified in either unix time or block height), that before this time, the transaction cannot be accepted into a block.”

- With this, you can set up payment schemes which are time dependent! Once again, this does not require a lawyer or someone to enforce this protocol, its built in!

# Why should you be excited about Bitcoin?

- It, in essence, is just a more intelligent way of the most basic form of human exchange. Transaction.
- By allowing for programmable transactions, we are creating a new technological and financial sector.

# Questions?

# Some ideas for the hackathon


- Sentinel wallets web app which detect if someone has hacked your computer
- A w