# bitcoin

And Relevant API’s
By Andrew Malta

# High Level Overview of Bitcoin

- An online payment method protocol
- Decentralized
- Anonymous
- Transparent
- Awesome

# What is a Bitcoin?

- This is a bitcoin: 4ffa1e10f374f76cb95c19d4cb69d1f61383a4c12e7edaa882404c5ca1e3459a
- Well sort of … it is a fraction of one ... for someone!
- I can use this to pay people under one condition.
- Bitcoins don’t really exist. They are just an illusion.

# Whose Bitcoin is it?

- Whoever knows the secret!
- Bitcoin is based on public/private key cryptography
- These keys are stored in something called a Wallet
- A wallet can have 1 or more of these public/private key pairs.

# Public Addresses and Private Keys

- Public Address (26 - 35 alphanumeric characters)

    ie) **1PXpMRcLyzckVVvBuNG2vo4CHcZvsbwa36**

    -This is public because you can share it with everyone.

- Private Key ( A very large number, usually 2^256 bit number)

    ie) **L4Ev3G95ngpqy3C8qiX88rH91NDD9CabxV2zkjYQzQt9pU1S9bCU**

    -Whoever knows this can spend any and all of your Bitcoin.

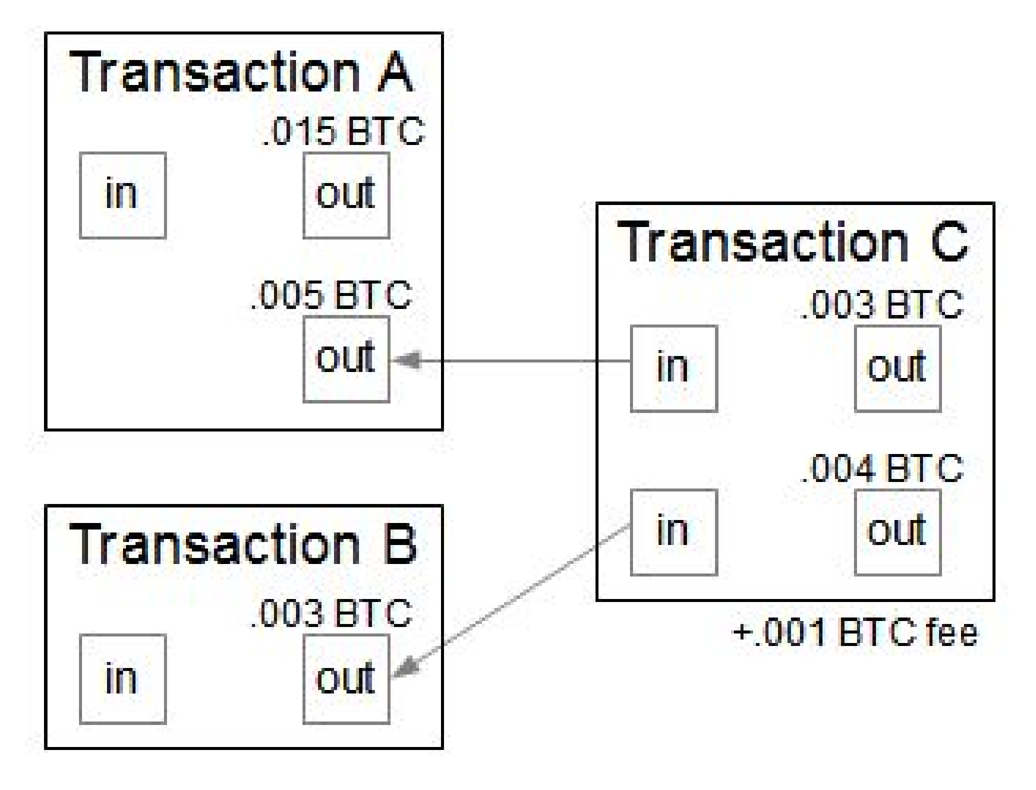
# How do I get an address?

- They can be generated randomly
- You can choose to seed this random number generator. (brainwallet)
- You can store bitcoin in your brain
- www.bitaddress.org is great!

# Transactions

- 4ffa1e10f374f76cb95c19d4cb69d1f61383a4c12e7edaa882404c5ca1e3459a
- Fundamentally (simplified a little):

  1) Inputs:  Old transactions in which I was an ouput.
- 2) Outputs:  The addresses I wish to send bitcoin to.
- 3) Amount:  How much bitcoin am I sending to each output.

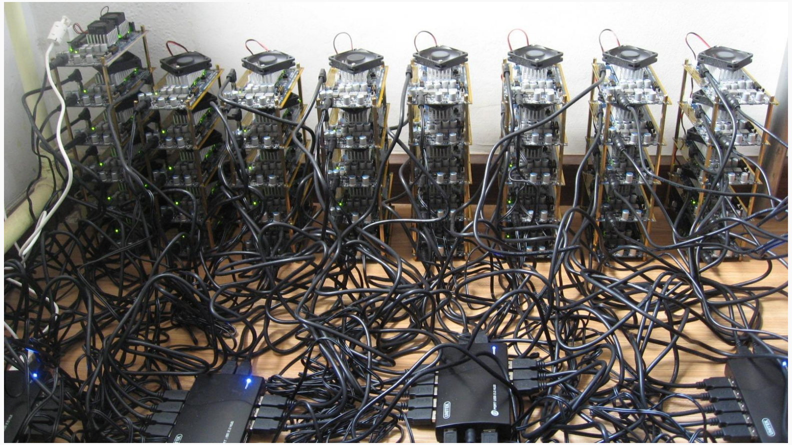

Transaction A
.015 BTC
in
out
.005 BTC
out
Transaction C
.003 BTC
in
out
.004 BTC
in
out
+.001 BTC fee
Transaction B
.003 BTC
in
out

# How do I get bitcoin?

- Elect to be paid for a good or service in bitcoin
- Faucet
- Buy bitcoin with fiat currency
- Mine

# Mining Bitcoin?

- Spend computational power to achieve some goal.
- Compete against other miners.
- Hashing the transactions of the network + nonce
- Solving a “Block” gets you the coins.



coinbase

BitGo

chain

# Relevant Services and APIs

BLOCKCHAIN

coinprism

bitpay

BLOCKCYPHER

# Blockchain API Providers

- Blockchain.info, Blockcypher, Chain, etc.
- Provide JSON REST endpoints
- Rate limit throttling
- They do a lot of work so you don’t have to.

# Popular Wallets

- Online:  Bitgo, Electrum, CoinBase, etc.
- Offline: Multibit, Coinomi, Microsoft Office (just joking please don’t do this)
- Store your keys
- Create, sign, and propagate transactions
- Offline wallets will sync to the bitcoin network.

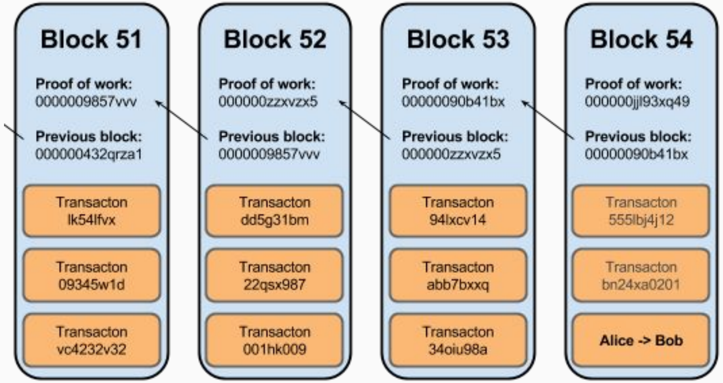
# Merchant Services

- Bitpay, Coinbase, Coinify, etc.
- Allow merchants (online and not) to accept bitcoin.
- Really important for the future of bitcoin.

# Blockchain

# Bitcoin Blockchain

- The “Public Ledger” that bitcoin relies on.
- It is decentralized!
- Completely transparent to everyone.
- Permanent



# Dread Pirate Roberts Transaction

https://blockchain.info/tx/e7db5246a810cb76e53314fe51d2a60f5609bb51d37a4df105356efc286c6c67

- Txid courtesy of the Wired, article “Read the Transcript of Silk Road’s Boss Ordering 5 Assassinations”
- Example of why the DHS likes bitcoin!

# Amazing Potential

- Extremely simple but really powerful.
- Lots of applications outside of Bitcoin
- Colored Coins, Proof of Ownership, etc!

# Colored Coins

- What if you could trade anything you wanted with the bitcoin protocol?
- https://www.youtube.com/watch?v=fmFjmvwPGKU
- If this interests you, check out Coin Prism or Chromaway.

# Other Applications

- Stopping jewelry theft!
- Distributed Loans.
- Distributed cloud storage
- Transparent Voting
- So much More

# Questions

If you think of any after, send me an email.

andrew.malta@yale.edu