Bitcoin

pancake <pancake@nopcode.org>
@trufae

What

What is bitcoin?

- p2p cryptocurrency (sha256 + ecdsa)
- coins generated decentralized (no inflation)
- public, free and opensource
- anonymous and community driven

Variants

All crypto currencies are based on bitcoin code base

Namecoins

- Used to register .bit domain names

Litecoins

- Cheap bitcoins (bitcoin is gold, litecoins is silver)

Freicoin (see later)

- Fork of bitcoin to implement pruning and demurrage

Freicoin

This project created by the Occupy WallStreet movement.
This is: two NASA devs and a photographer/designer aims to create a fork of bitcoin featuring:

- opensource + easy for new users
- official exchange site
- bittorrent transfers of blockchain
- blockchain pruning (reduce size of blockchain)
- demurrage (% of each address is distributed)

```
http://www.indiegogo.com/freicoin
http://www.freicoin.org/
```

When: History

Project released in 2008 by "Satoshi Nakamoto"

```
https://en.bitcoin.it/wiki/History
```

The author disappeared after 2 years of discussing stuff in the forums. Lot of mistery in the origin.

Always used anonymous communication channels and perfect english. Satoshi means ’wise’ in japanese.

```
http://observer.com/2011/06/bit-omoney-whos-behind-the-bitcoin-bubble/
```

Who uses bitcoins?

- People paying for VPNs, proxys or hostings.
- Sending money to other country with no taxes
- Speculators and brokers
- Hackers and cryptopunks
- Poker, lotteries and other gambling sites
- Illegal stuff like drugs or weapons (srsly?)

Darknet

Lot of criticism has been imposed on btc as being used by mafias and drug dealers in order to scape from banking system and being untraceable.

That is not true at all, bitcoin is used mainly for trading and speculation, and there are much more ilegal transactions using dollars and euros than in bitcoins.

Remember: In bitcoin everything is public.

Anonymous?

How anonymous is something public?

Bear in mind that IPs are tracked, bitcoin addresses can be connected to users (twitter profiles, donation websites..)

```
http://blockexplorer.com/
```

Here is a guy writing tools to analyze the blockchain and make bitcoin a little less anonymous. This is good as long as it is possible :) and can be used to track stoled money.

```
http://toolongdidntread.com/
http://blockchain.info/tree/5484758
```

Why use bitcoins?

- To securely buy stuff on the internets
- To break the visa/paypal monopoly
- Accepting donations
- For pure technical interest
- To learn economy or cryptography
- For fun

Free money!

How to get bitcoins

- exchange (mtgox.com bitcoin.com.es localbitcoins.com)
- gambling (sealwithclubs.eu minefield.bitcoinlab.org)
- lottery (satoshidice.com)
- poker (bitcoipoker.org sealwithclubs.eu)
- bets (betsofbitco.in)
- works (bitcoinerr.com)
- mining (50btc.com bitpenny.com bitcoinpool.com)
- stocks (glbse.com)
- donations (coinad.com freebitcoins.appspot.com)
- ads (anonymousads.com)
- stealing (pwning banks or wallets)

Where to use it?

- donations (wikileaks, software, orgs, movies, ..)
- coindl.com (open store)
- ezines (bitcoinmagazine.net coineer.com ..)
- exchange sites (gold, time bank, ..)
- stores (bitcoindeals, giftcards, ..)

How to use it?

- client
  - official: bitcoind: shell, gui, api
  - online: instawallet.org blockchain.info/wallet
  - light: electrum, multibit

- addresses
  - user defined local name (alias)
  - address is the pubkey
  - generated in local with 0 balance
  - create one for each input address
  - no personal data asociated

- transfers (with fee, no return)

Transfers

How it works

- wallet
- addresses
- blockchain (4GB)
- payment (transfers)
- mining (pool, merged, solo)

Wallet

wallet.dat is the storage for your addresses

- db4 format
- private and public keys
- related transactions
- supports aliases for addresses

Advanced clients for managing the wallet

```
http://bitcoinarmory.com/
https://github.com/radare/bitcointools
```

Online wallets

```
https://instawallet.org
https://blockchain.info/wallet/
```

Addresses

In Bitcoin, an address is not like a bank account or a credit card number. A bitcoin address is not linked to any personal information.

They are generated in local and you can create as much as you want.

A bitcoin address are:

- first char must be 1 or 3
- 33 or 34 characters
- numbers and upper/lowercase letters
- except O/0 and I/l (to prevent visual ambiguity)
- validation requires crypto

Blockchain

The blockchain is the storage for all the transactions verified by the network.

It’s syncronized and verified by all the nodes in the network.

Nowadays is 4GB. Storage and network usage is a problem for mobile bitcoin clients.

Transfers

Money is transfered from a single source address to one or many destination addresses.

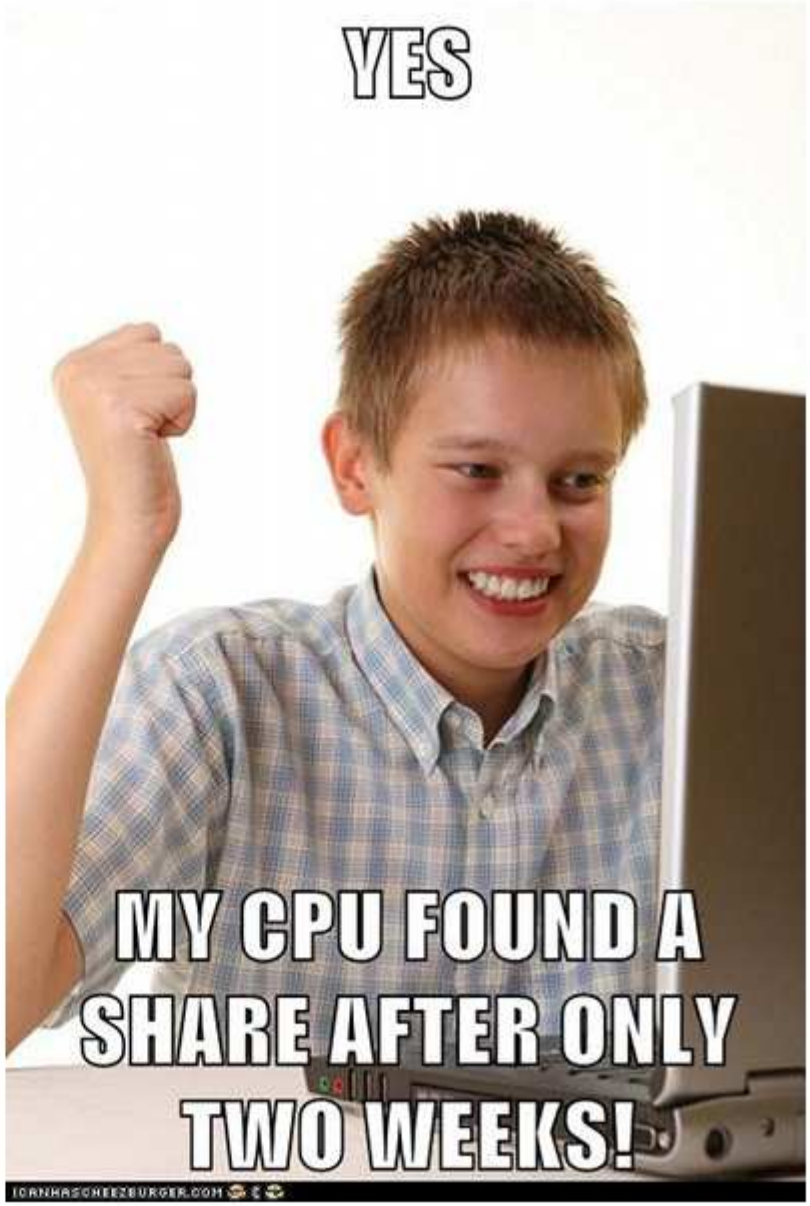
Transfers are sent to the network in order to verify it, when it gets 6 validations it is considered as confirmed.

Transactions that contain a fee are priorized by miners.

~15m with fees
~3h without fees

That is a problem for in−place payments (restaurants..)

Mining


YES
MY CPU FOUND A SHARE AFTER ONLY TWO WEEKS!
ICANHASCHEEZBURGER.COM

Mining

Consists in taking a group of transfers and find a hash prefixed by N zeros and push it to the network

- N zeros is the difficulty level
- Difficulty depends on network power (adaptative)
- Network power measured in TH/s
- Each block rewards 50btc (25btc by the end of 2012)
- Difficulty depends on network power
- Merged / Pooled / Solo mining
- 51% security

Pooled mining

A pool is a server that constructs a block and send it to the miners in order to find a hash that matches the difficulty.

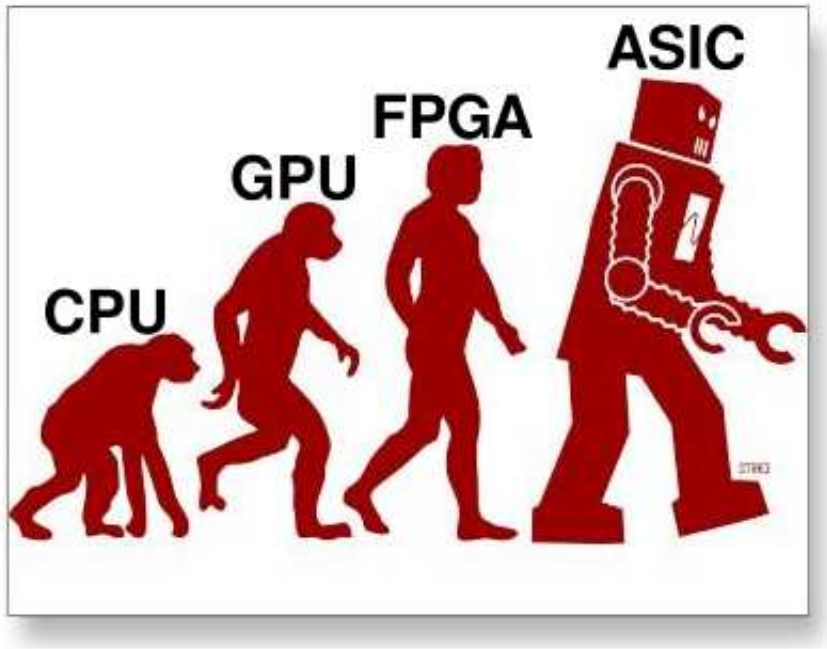
if (hash > D && < SN) rewards ("share")

- Proportional (high variance)
- Pay per share (0.18 mBTC)
- Pay per last shares
- DGM (double geometric method)

https://en.bitcoin.it/wiki/Comparison_of_mining_pools

Mining hardware

- JS/Java (cool for xss)
- CPU (i5 = ~6MH/s)
- GPU (~60MH/s)
- FPGA (less power consumption)
- ASIC (>4GH/s, little power consumtpion)



Trading

GLBSE is the most famous trading site:

```
https://glbse.com/
```

- Create an IPO costs about 8btc
- All realtime data is free

You can also buy/sell bitcoins. MtGOX is the #1 site

- Defines the exchange price of btc/dollar/euro
- Lot of verifications (ID, CC, photo..) to avoid fraud

BugCoin (toy project)

A bugtracker written in NodeJS that interacts with a bitcoind using a remote agent which periodcally connects to the webservice in order to perform sensitive tasks.

```
git clone git://github.com/radare/bugcoin.git
```

Running online demo at:

```
http://bugcoin.nodester.com/
```

Still work in progress, contribs are welcome.

FMI

Blockchain Charts

```
http://blockchain.info/charts
```

Nice introduction

```
http://bitcoinme.com/
```

Forums

```
https://bitcointalk.org
```

Youtube is full of tutorials

```
http://www.youtube.com/results?search_query=bitcoin
http://onlyonetv.com/2011/08/the-bitcoin-show-podcast-episode-035/
```

The End

Questions.. anyone?