Bitcoin

pancake <pancake@nopcode.org>

@trufae

Introduction

What is bitcoin?

- Bitcoin is a cryptocurrency
- Free and OpenSource
- Everything is public
- Based on P2P (bootstrapped on IRC)
- Descentralized trust
- Uses sha256 and ECDSA crypto
- A currency value depends on trust

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

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-bubbl

Wallet

The wallet is the storage for your addresses

- db4 format
- private and public keys
- all 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/
```

Banks

Online wallets are like banks. They own your private and public keys and allow you to make transfers.

This is useful for new users, and to use it from mobile phones. No taxes or fees imposed.

When compromised, if not designed properly you can loose all your money.

```
https://bitcointalk.org/index.php?topic=93074.0
```

SCAM

There are several known cases of scam around the bitcoin, take care about what you do with your money and read carefully every comment on the internet, understand how it works.

There have been fake bank sites, fake hacks that involve transactions, etc.. they just want to stole your money.

Beware!

Using bitcoin

There are different kind of ways to use bitcoin

Online wallets
- priv/pub stored on remote server

Standard client
- Requires the full blockchain (~2GB)
- Wallet can be encrypted
- jsonrpc api to interact with wallet and network

Light clients
- unsafe, fast, useful for mobiles

Addresses

In Bitcoin, an address is not like a bank account or a credit card number. A bitcoin address does not identifies a single person.

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

Bruteforcing addresses

Use vanitygen to create addresses containing a string

:)

Vanitygen:

```
git clone git://github.com/samr7/vanitygen.git
```

For more information on bitcoin addresses see:

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

Transfers

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

Transactions that contain a fee are priorized by miners, so they are validated before others.

A transfer is confirmed when it has been validated at least 6 times.

~15m with fees
~3h without fees

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

Using the daemon

The bitcoind (the official daemon) can export its functionality as a JSON−RPC api.

You can run bitcoind [command] [arguments]

Edit your ~/.bitcoin/bitcoind.conf to set user/pass for rpc

```
bitcoind validateaddress 1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v
```

Ads

There are several sites that allow you to create ads or put them in your site and get bitcoins

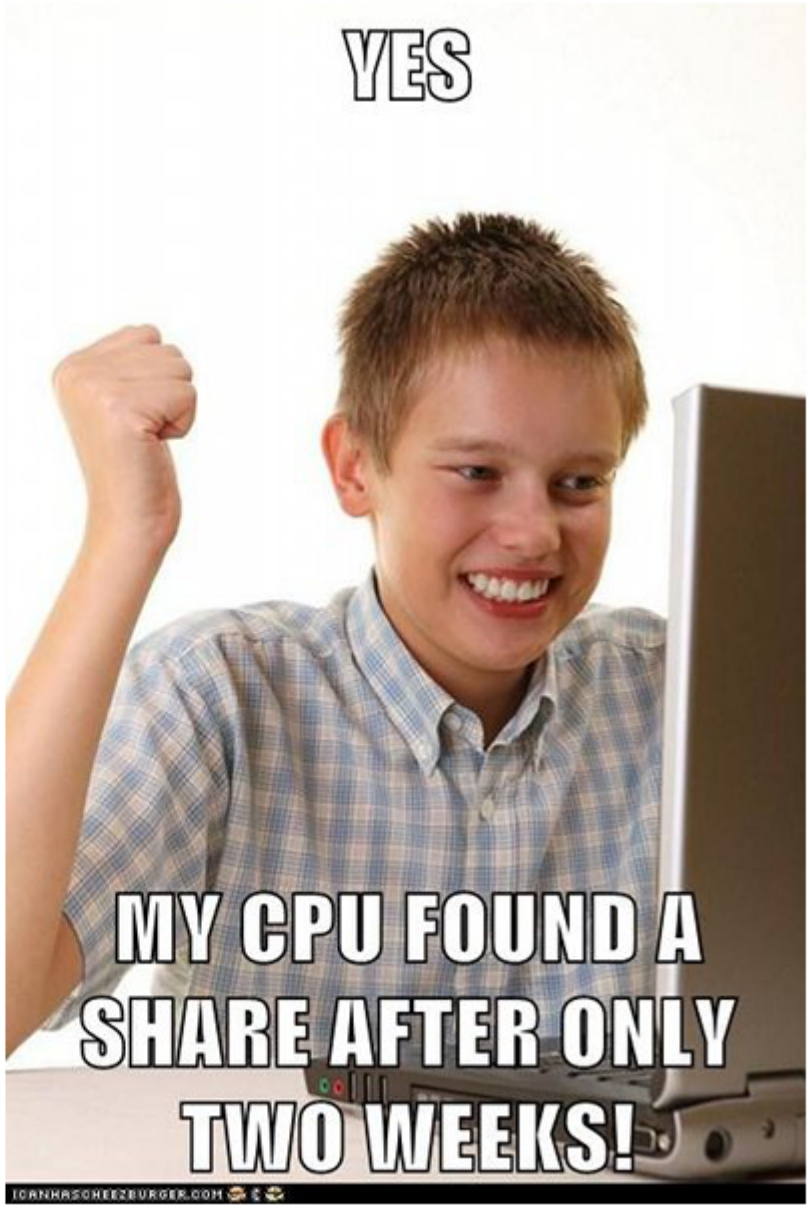
```
http://www.anonymousads.com
```

This is similar to GoogleAds, but without censorship or personal information required. The setup is purely anonymous
and requires no login to administrate.

Other site:

```
http://bitcoinpyramid.com/ads
```

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

- Network power measured in TH/s
- Each block is reward of 50btc
- Difficulty depends on network power
- 51% security

Mining pools

Types of mining:

- PPS (pay per share)
- PPLNS (pay per N last shares in round)
- Proportional
- DGM (double geometric method)

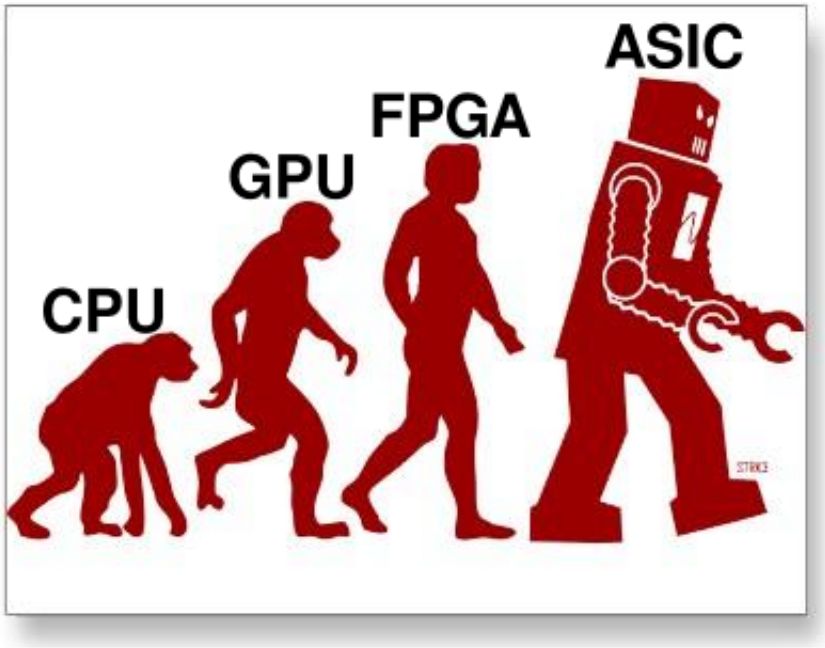
Public pools:

- BitcoinPool
- 50btc (pps)
- BTC Guild (pps)

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)



Mining difficulty

The difficulty to find a valid share depends on the current network power. Network difficulty is recalculated every 24h and all clients must be syncronized in order to accept a share.

Those shares are grouped in a block which is rewarded when resolved.

Current network hashing power is about 16.000 GH/s.
A block is solved every ~10 minutes.

Coins?

Casascius are physical bitcoins made of brass or gold, designed to be used in real life by collectors or exchanges.

https://www.casascius.com/

Free coins!

Those sites aim to promote the use of bitcoin by giving bitcoins for free:

Faucet (google account required)

```
http://freebitcoins.appspot.com/
```

Bitcoins every 24h (0.0001btc)

```
http://dailybitcoins.org/
http://www.coinad.com/
```

Games, ads, surveys..

```
http://www.freedigitalmoney.com/
```

Trading

There is trading services also in bitcoin

- GLBSE is the most famous

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

- Create an IPO is 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

Gambling

There are bets, lotteries, games...

- SatoshiDice

```
http://www.satoshidice.com/
```

- MineSwap

```
http://minefield.bitcoinlab.org
```

- Bets of Bitcoin

```
http://betsofbitco.in/
```

- Poker

```
http://www.bitcoinpoker.org/
https://sealswithclubs.eu/
```

Magazines

Some of the online and paper based bitcoin zines:

```
http://bitcoinmagazine.net/
http://www.coineer.com/
```

Youtube is full of tutorials and

```
http://www.youtube.com/results?search_query=bitcoin
```

The bitcoin show

```
http://onlyonetv.com/2011/08/the-bitcoin-show-podcast-episode-035/
```

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
```

Where to buy stuff?

There are several places where you can buy stuff in btc

Peer to peer shop service

```
https://www.coindl.com/
```

An index of many stores accepting bitcoins

```
http://bitcoindeals.com/
```

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.

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.

Security

For security reasons is better to move your money to new accounts every N days.

If the >50% of network power uses a new algorithm can win the official network and create new branch in blockchain.

Real clients will never accept such nodes as long as they do not complain to bitcoin rules.

Keep your private keys in a secure place. Use them only when you need to create a transfer

Do not use online wallets to store lot of money.

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
- bittorrent transfers of blockchain
- blockchain pruning (reduce size of blockchain)
- easy to bootstrap by new users
- exchange site
- demurrage (% of each address is distributed)

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

Other links

Blockchain Charts

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

Nice introduction

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

Forums

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

ktxby

Questions.. anyone?