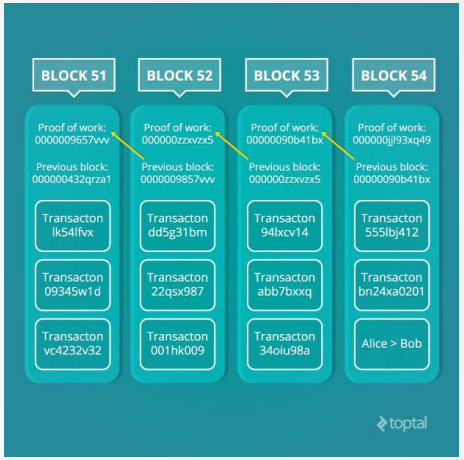
BITCOINS, BLOCKCHAINS AND BEYOND

Jelle Haandrikman

2017-02-07, Venlo-NL

@jhaand



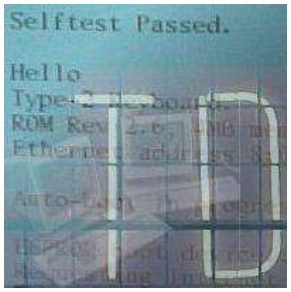
Available at: http://www.slideshare.net/jhaand/bitcoins-blockchains-and-beyond

Overview

- > Bitcoins: Dispel the hype and show possibilities for users
- > Blockchains: Explain the Technology for developers.
- > Beyond: What are others already doing with this new technology.

Note: If I'm going too fast: Ask questions.
At the end of each part: Room for discussion.

About me



IGT Systems

GXR

YS E-INT/ CH-INT

[@jhaand](https://twitter.com/jhaand)

E: jhaand@xs4all.nl

17DivS7Rc2JPs7oDf1FT3nn5XPF2idNPQ2

What makes Bitcoins interesting.

- The Euro and USD are doing fine for the most part for everyone. ;)
  But a lot of countries have big problems. (Greece, India, Argentina, China)
- 2 billion people lack good government services and/or have no bank.
- Incumbents accommodate their current methods to the internet.
  There exists no network like E-mail to handle money.
- Exponential/Sigmoid technologies go fast. (Once they get traction)
- Money in the bank becomes less valuable due to inflation.
- Transferring money across borders can be really painful and costly.
- Trends are to decentralize or globalize the way of doing business.
  Either go local or global.
- It feels like the internet in 1995.
- Open Source Software developers making money.
  FLOSS already does a lot of infrastructure, time to use code to offer services.

My personal introduction to Bitcoins

- Heard about it in 2009 via Slashdot and asked myself:

  “Why would you want to make your own money?”
- Then heard about the 2011 crash from 32 USD to 2.
- In January 2013 Bitcoin back to 20 EUR.

  “Hmmmm. Wasn’t this Bitcoin thing dead yet?”

  “Impossible, this can’t possibly work and I’ll find out why this can’t work.”
- “OK. The technology looks really solid but people remain skeptical. Looks like internet in 1995 and Linux in 1997. Let’s not skip this bandwagon this time.”
- “The central bank of the internet”

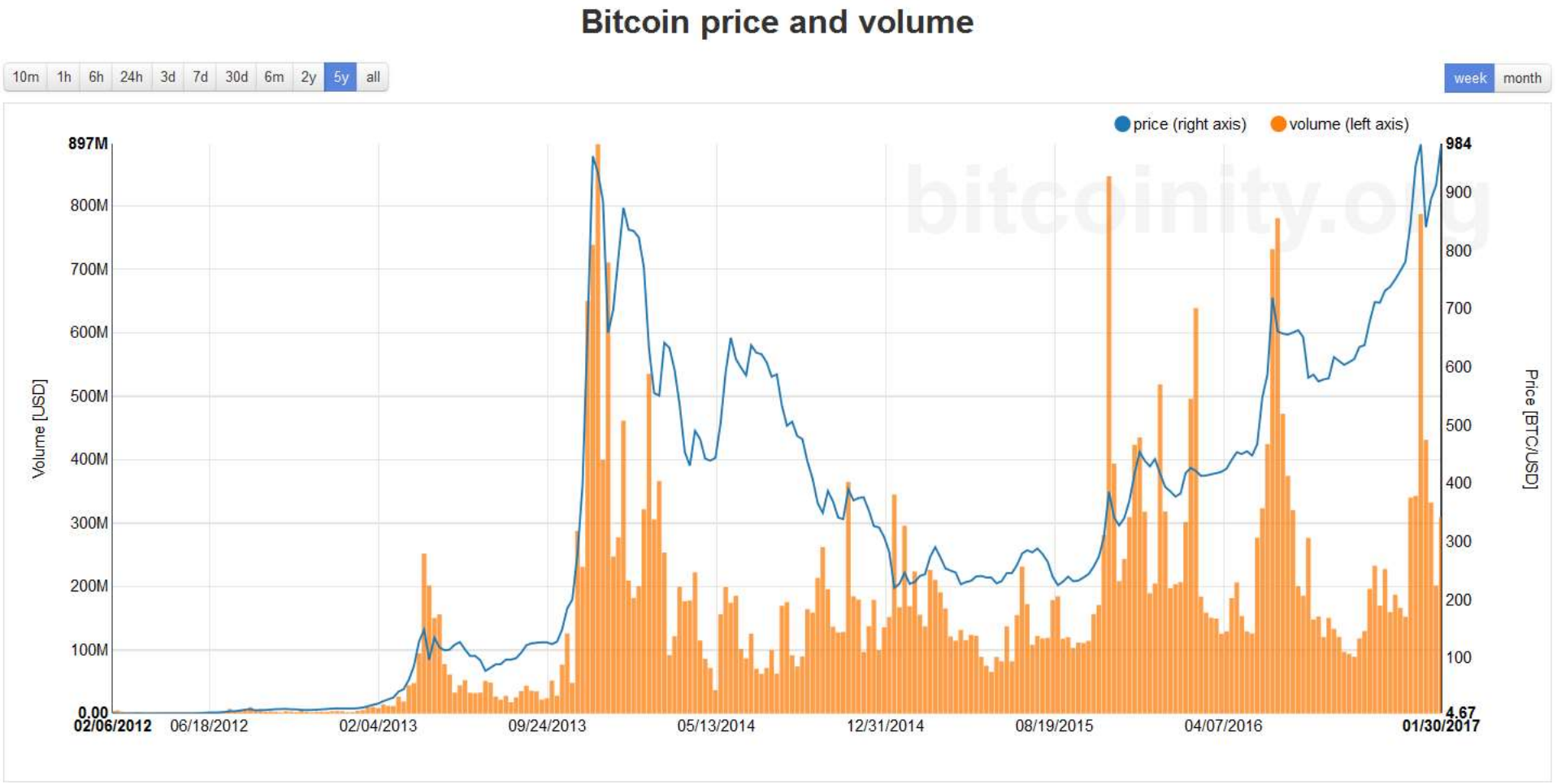
A MATRIX paying for dinner.

Mayday and Murs – Bitcoin Beezy

Bitcoin in a nutshell.

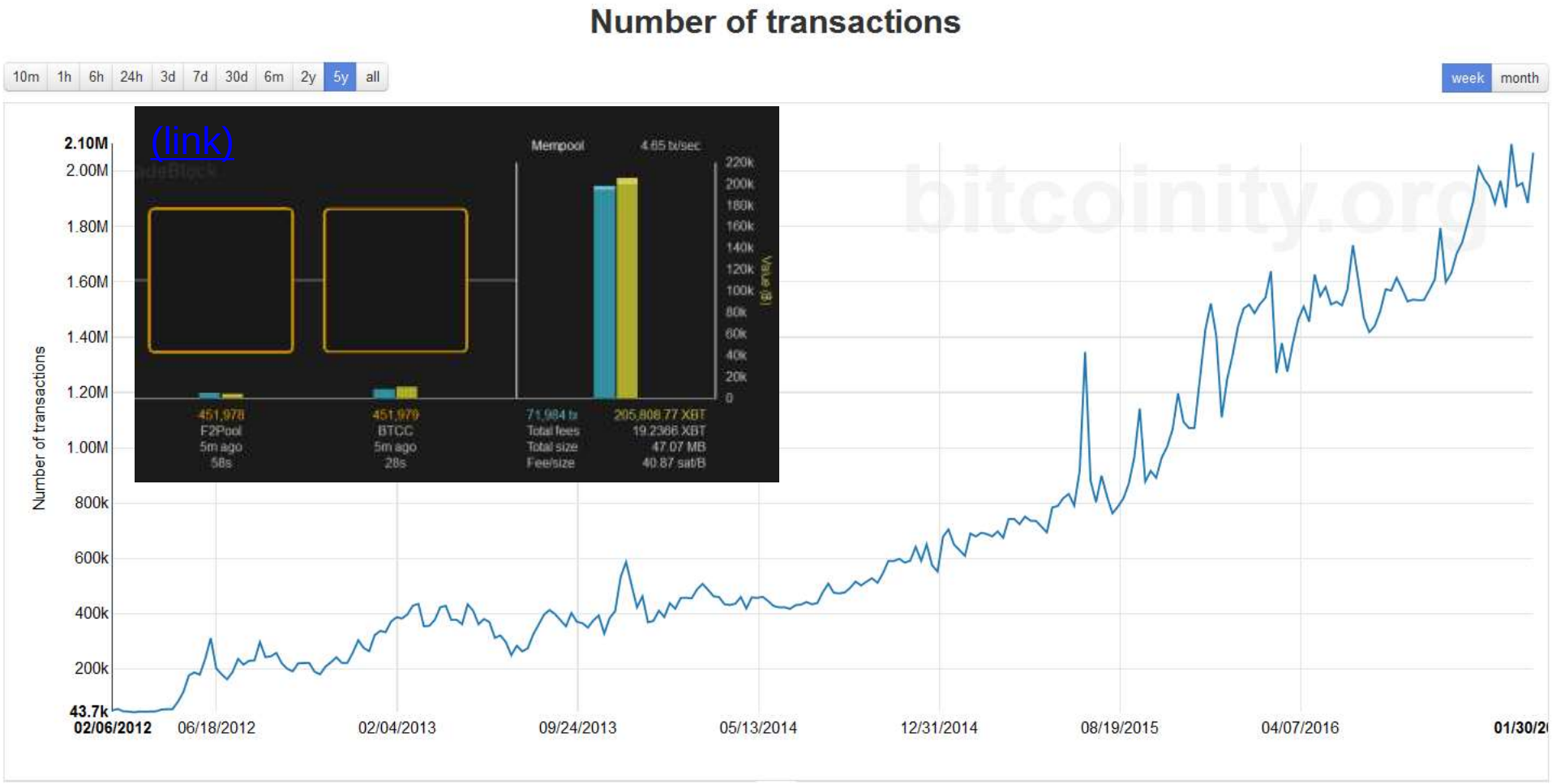
- Global payment network that operates without trust to transmit any amount of Bitcoin for 0.25 EUR via a public ledger, underwritten and secured by miners every 10 minutes.
- Introduced by a pseudonym “Satoshi Nakamoto” in 2008 via his paper:
  “Bitcoin: A Peer-to-Peer Electronic Cash System”
- Collaborated on the OSS project until mid 2010 and then vanished.
- Available amount currently: 16.1 million BTC
- Current rating: 980.13 EUR (@kraken, 2017-02-07T17:33)
- Total capitalization: 15.8 $x10^9$ EUR
- Every 10 minutes 12.5 new Bitcoins created.
- Speed of creation halved every 4 years. Ends with 21 million BTC in 2140
- Software organized via Bitcoin foundation
- Quantities:
  - 1.00: Bitcoin
  - 10^{-3}: mBit
  - 10^{-6}: bits
  - 10^{-8}: Satoshi
- Standard fee per transaction: 0.25 mBtc (0.25 EUR) (minimum 0.1 mBtc)

It has been a rocky ride getting here.



Source:http://bitcoinity.org

It looks like 2013, but this times it's different.



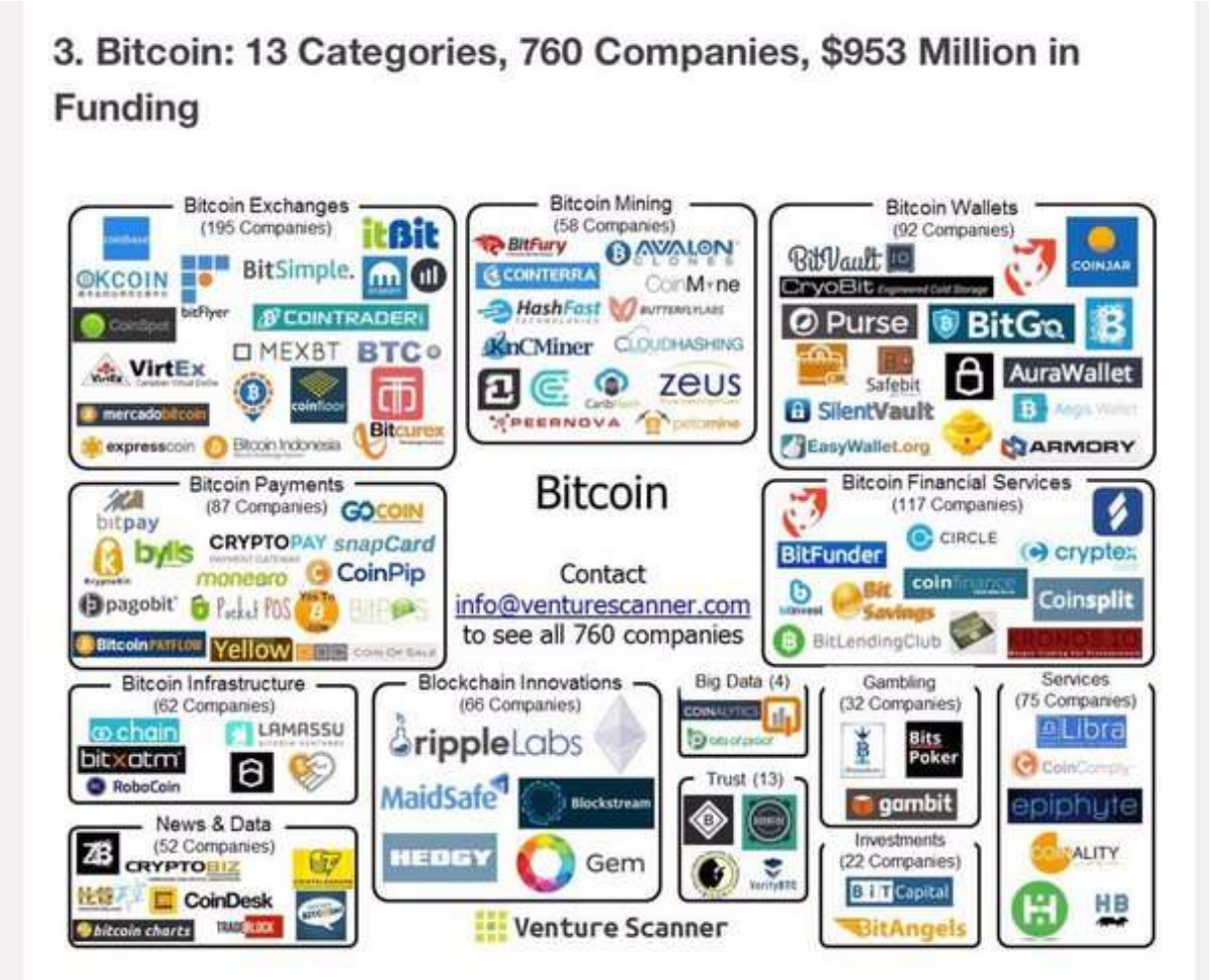
Source:http://bitcoinity.org

Along the way a lot of interesting new stuff and humor in an open source software kind of way.

The world according to Bitcoin

- Entrepreneurs all over the world
- Miners, gamblers and money hiders in China.
- Silicon Valley has VC money invested in 2016.
- Local sellers and interest in countries with most the infrastructure.
- Remittance to Philippines and Africa.
- Opportunities in countries with good education but bad institutions and or failing currencies. (South America, Cyprus, Greece, Ukraine)
- Europe:
  - Somewhere in-between
  - Good institutions
  - Good technology
  - Good Financial knowledge

And now the serious investors are now pouring in.



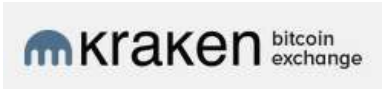
2017 will prove a make it or break it year for Bitcoin.

Paying with Bitcoin

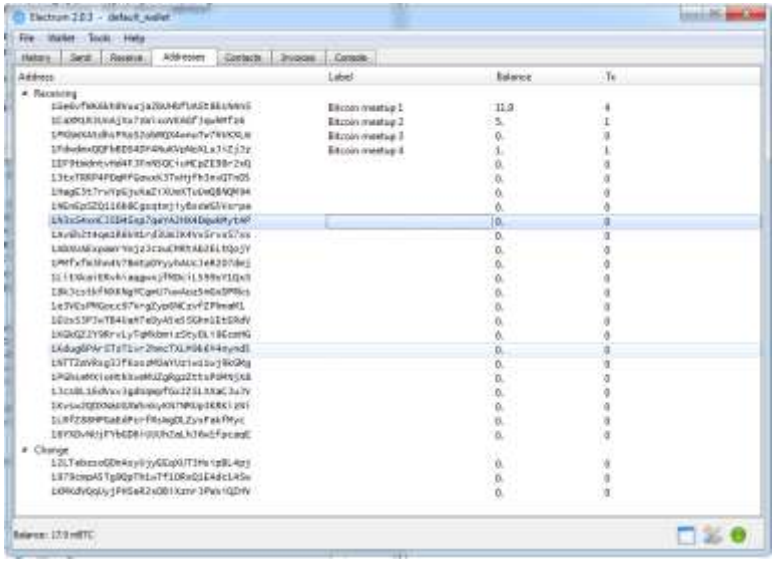
- What can you pay:
  - Get fast food: Thuisbezorgd.nl
  - OEMs: Microsoft.com, Overstock, etc.
  - Charities (Nepal, Philippines)
  - Games (Steam and in-game)
  - Local resellers (Arnhem Bitcoincity, The Hague)
  - Items not for sale using normal means:
    - Darknet items (Silkroad V x.x)
    - Order Persian shoes from Iran
    - Grey economy, medicines
    - Support (blogs Wikileaks, Ross Ulbrich)
  - Tipping (demo) (view)

Getting Bitcoins

- Via Exchanges: Bitcoin.de, Kraken.com, Bitonic.nl
- Local resellers: Local bitcoin, Mycelium local trader
- Mining (not profitable anymore)
- Trading
- Get paid in bitcoin
- Install machines that get paid in bitcoin.
  IoT services, vending machines, autonomous taxi's, AirBnB automatic check-in
- Stealing, ransomware (warning: BTC is pseudonomous, people will find you)
- Transfer them to your machine at home.



Tooling



Note: Don't install Bitcoin core as wallet.
It downloads the whole Blockchain. (45.6 GiB)
The wallet MultibitHD is now deemed unsafe.

- Manage your bitcoins:
  - At the exchange.
  - On your computer (Electrum)
  - On your Mobile (Mycelium)
  - On a paper wallet
  - On a hardware wallet (Trezor)
  - BIP 0032 HD wallet (12 words on a sheet)
- Be your own bank. So make sure you get the security OK.
- Also your administration for taxes needs to be in order.

Trading / Investing in Bitcoins

- Since there is no regulation, except the algorithm and the miners mining, expect a lot of volatility.
- Investing: Buy and hold. (Buy the dips)
- Trading, expect volatility:
  - Exchanges get hacked and people get scammed.
  - There's no oversight. (AFM, SEC, etc….)
  - Large players move the market.
  - Literature from 1920's seems to hold up quite good. ☺
  - Fundamentals: Regulations, Payment possibilities, transaction volume, legislation in different countries and sentiment.
  - Introducing a deflationary currency into a fiat inflationary world looks like an interesting experiment.
  - Follow /u/ibankbtc on reddit. (**@ibankbitcoins**)
- Sites:
  bitcoinwisdom.com
  bitcoincharts.com
  blockchain.info
  Cryptowat.ch

Risks of Bitcoins.

- Slow: With 1 MiB blocks per 10 minutes, only 7 transactions/second possible.
- The network might be decentralized, but other stakeholders are not:
  - Miners: Most operations in China
  - Developers only a small core of people divided in 2 camps.
  - ASIC miners come from small batch of OEM's and the ASIC's themselves via TSMC.
- Developments last 2 years show: If the risk becomes too great, the exchange rates tanks. → Things get solved.
  - 51 % attack
  - Bugs. (Blockchain fork 2013-03-(11/12) version 0.8 vs 0.7) (link)
  - MTGox
  - Block size debate. (still ongoing -> Bitcoin Core, Bitcoin Unlimited)
- Regulations, banning, taxes, KYC/AML
- Other crypto currencies might take over.
- The protocol, network and core client works good. Interfacing to the real world causes a lot of problems.
- Security remains key: 2FA, passwords, hide wallets, backups, etc.
  protect against: theft, fire, natural disasters, etc.

Bitcoins: References

- Bitcoin.org (+ intro video)
- Original Bitcoin paper. (8 pages)
- Documentaries:
  - The rise and rise of bitcoin (link)
  - Morgan Spurlock Inside Man – Bitcoin (link)
  - Tegenlicht: Het bitcoin evangelie (link)
- Youtube:
  - Andreas M. Antonopoulos educates Senate of Canada about Bitcoin (Oct 8, ENG) (link)
  - Joe Rogan Experience #844 - Andreas Antonopoulos (link)
- Reddit: /r/btc /r/bitcoinmarkets (/r/bitcoin)
- Twitter: @coindesk @bitcoin @tuurdemeester @aantonop @AaronvanW @rogerver
- Left out: HD wallets + Multi-signature transactions

Blockchains

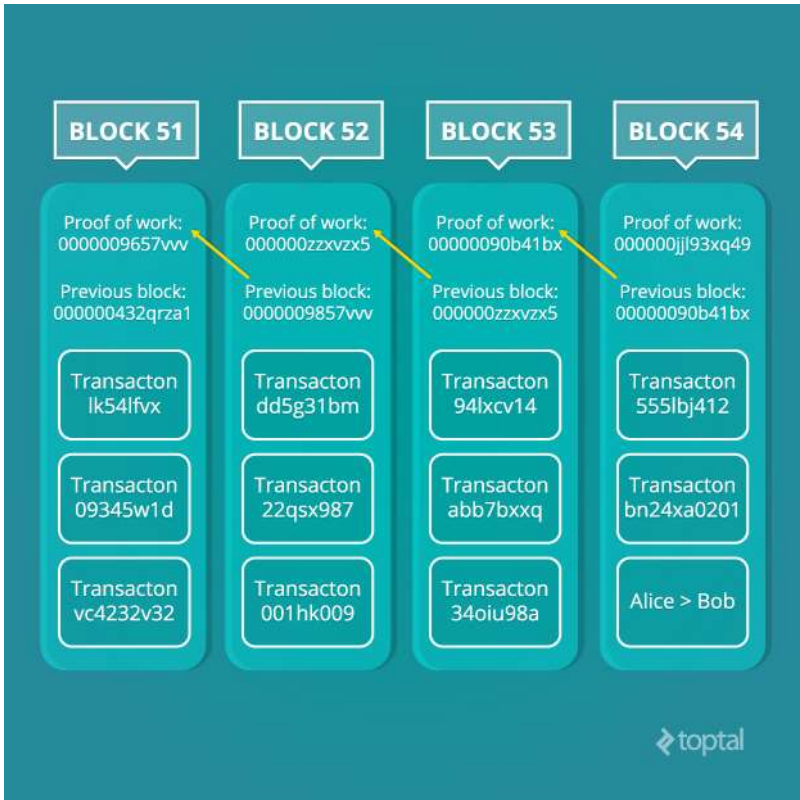
- Basics for:

  Making sure we have a definitive global record of all transactions.
- How does Bitcoin actually work?
- Starters: Every Public address has a corresponding secret private address
  - Public: For receiving and viewing the contents
  - Secret: For sending Bitcoin somewhere else.
- Transactions are distributed to the whole network.
- Transactions are recorded in a distributed ledger/journal, called the Blockchain.
  - If you want to know the balance, check all the transactions to that address.
- A miner underwrites the transactions on average every 10 minutes.

Miners: Proof of Work

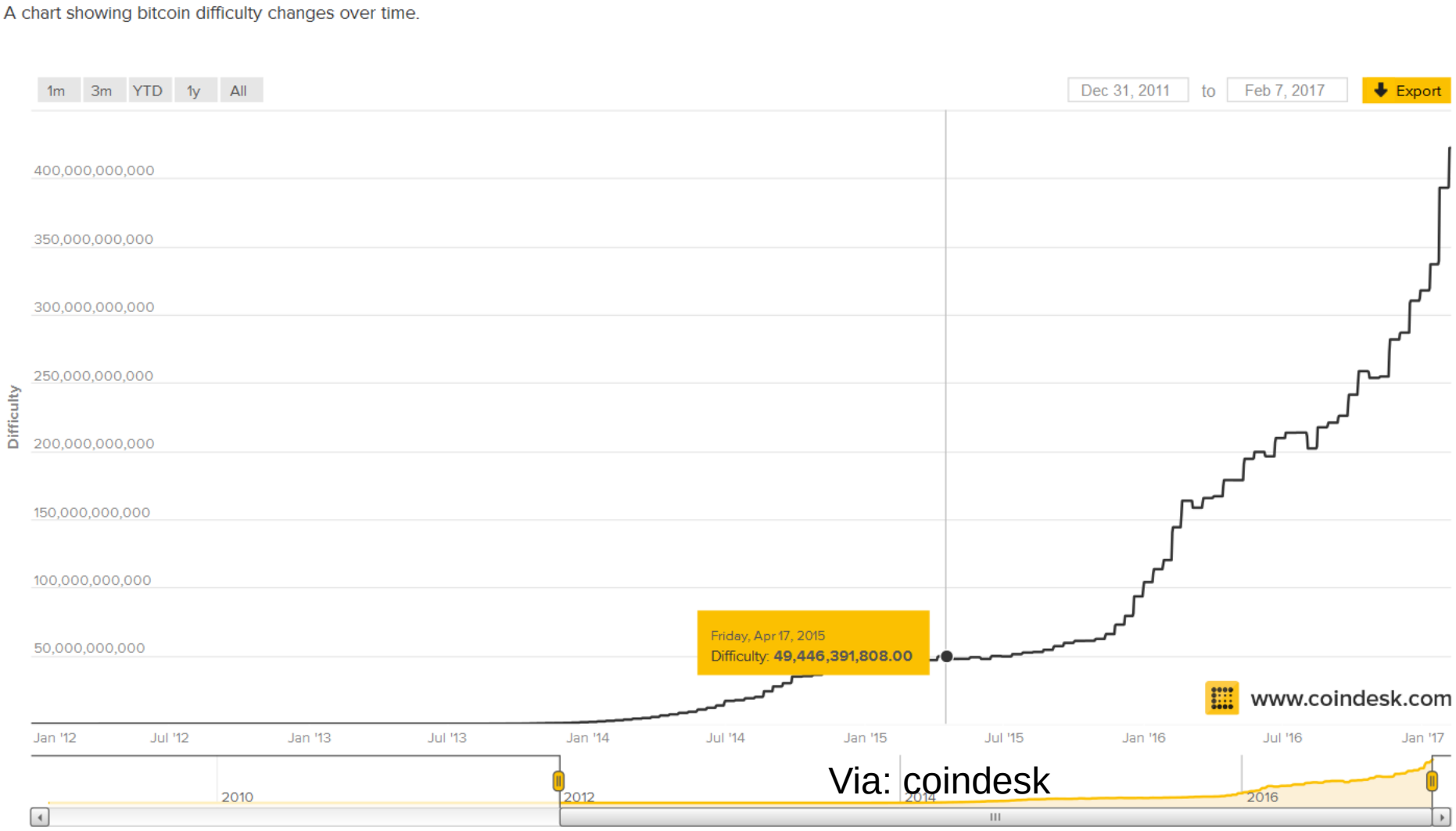
Inspect the blocks: here and here

- Miners:
  - Record all the transactions,
  - Try to find the answer to a difficult math problem first.
  - Based on all recorded transactions and the outcome of the last mined block
  - The miner that solves it first:
    - Wins 12.5 BTC +
    - Transaction fee's for a block.
    - Distributes the winning block
    - Starts mining the next block.
  - Miners compete to win the next block every 10 minutes.
  - With extra computing power:
  - Change difficulty after 2016 blocks.
  - This is just a way to construct a global, secure, trustless, non-reversible, high available, transactional journal/database.



Blockchain difficulty

> Thus the incentive to mine rises when BTC prices rise and power costs fall.



Via: coindesk

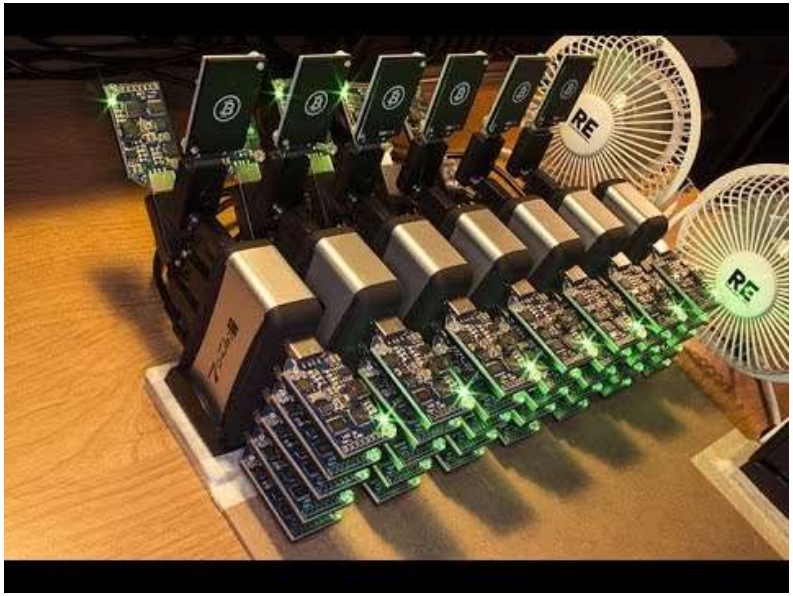
Mining in the old world (2010)

Started as a hobby.

Mining with new developments around 2011/2013

FPGA's

ASIC's



Professional Mining (present day)

Hobby has no chance.

An enormous bitcoin mine went up in flames, affecting the entire network

A large bitcoin mining facility in Thailand went up in flames this week, destroying the five-megawatt operation and disrupting the crypto-currency's entire network.

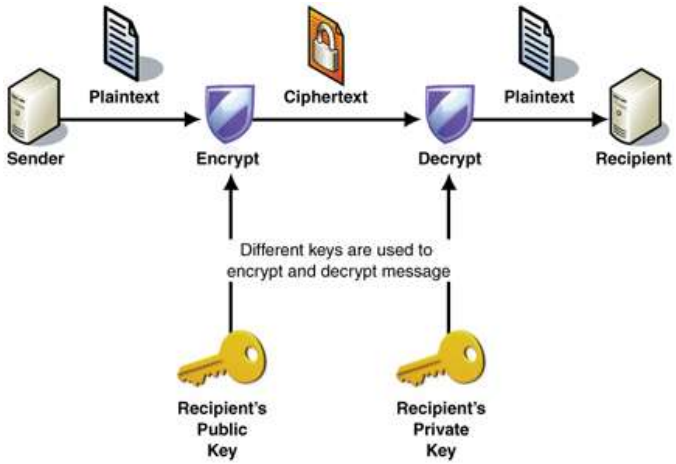
Src: qz.com

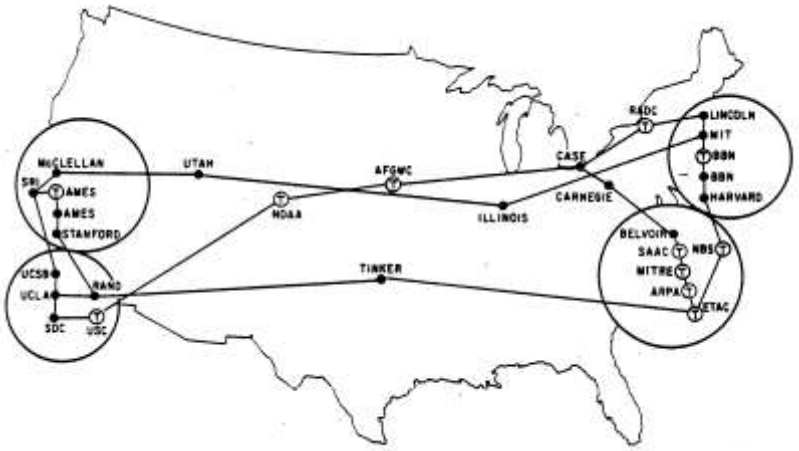
Where did Blockchains come from?

- Combination of modern crypto technology from around 2004.
- Using surplus military technology
  - Databases
  - Networks
  - Asymmetrical Cryptography

"Do we want to allow a means of communication between two people which even *in extremis,* with a signed warrant from the home secretary personally, that we cannot read? … My answer to that question is no, we must not. The first duty of any government is to keep our country and our people safe."

David Cameron





What are the variations on what we've seen?

- Block size
- Time per block
- Number of coins
- More privacy
- Store other information than money.
- Encryption Algorithm used.
- Federated vs. Decentralized
- Proof of Work vs. Proof of Stake
- Time of Genesis block.
  (arriving late to the party)

Thus resulting in 200+ alt-coins.

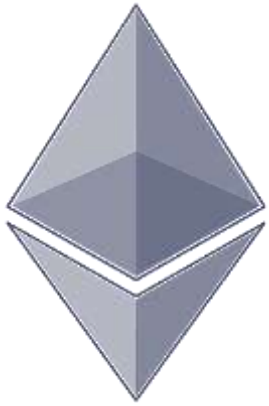
Blockchains: References

- Blockchain Technology Explained: Powering Bitcoin (link)
- Primer on Elliptic curve cryptography (link)
- Bitcoin Unlimited (link)
- Bitcoin Core development (link)
- Twitter: **@gavinandresen** **@petertoddbtc**
- Mastering Bitcoin – Andrea M. Antonopoulos (book)

Beyond

- Now Finally possible to create network native, global, resilient databases.
- Uses:
  - Futures, Bonds, Options, etc.
  - Collaboration between local parties without institutions.
  - Decentralized storage (blockchain + crypto + bittorrent) storj.io IPFS
  - Decentralized computer (Ethereum on next slide)
  - Store calibration data of your newly shipped Machine
    - (Device History Record)
  - UL / CE Certification library with test records
  - Proof of Identity
  - Register elections
  - Register records across parties. (e.g. align booking of plane, hotel and car)
  - Big Data (with internet dating as example)

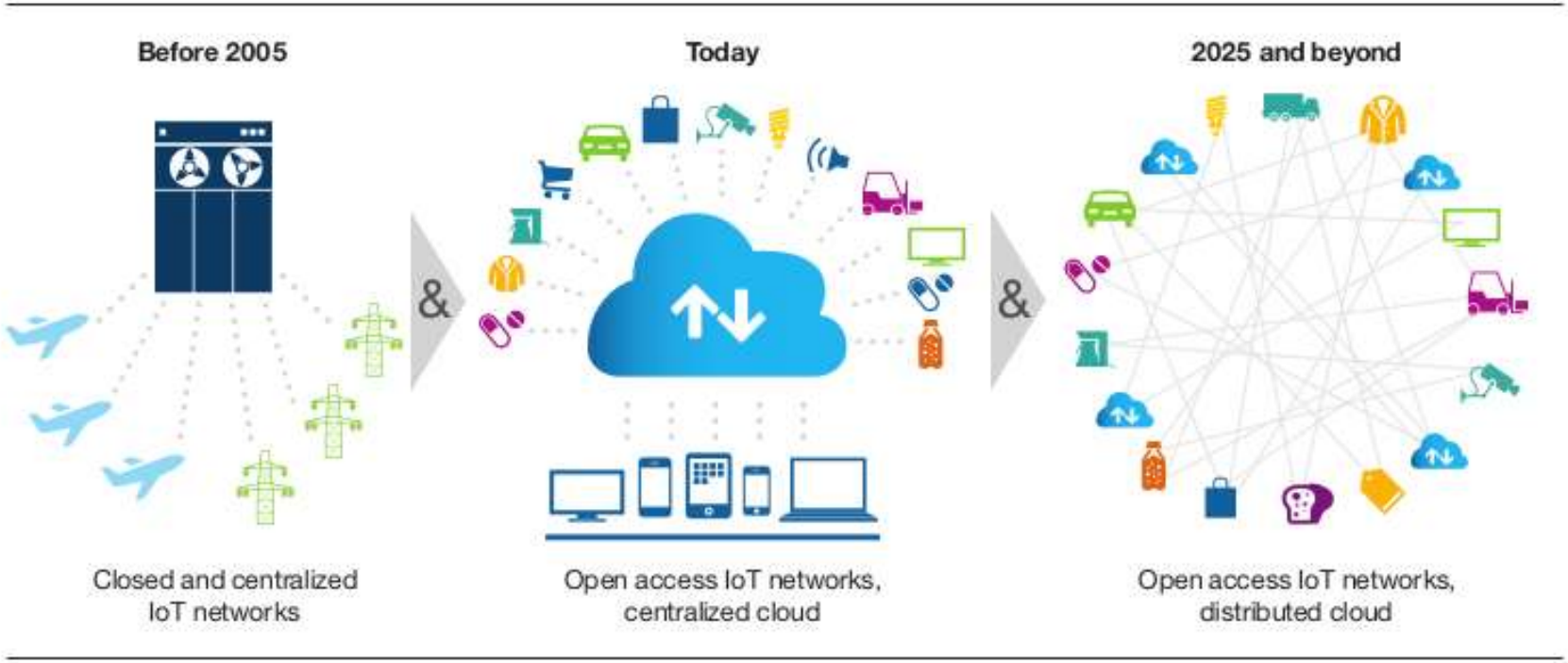
Ethereum



- Permanent smart contracts on a global blockchain
- Small programs (size of VB macros) that can be executed.
- The world computer (video)
- Usage for:
  - Crowdsourcing
  - Contracts
  - Auctions, etc.

IoT powered by blockchain technology

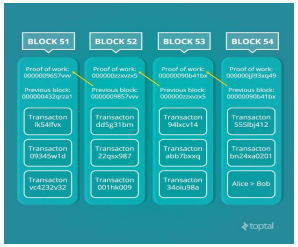
- Making Back-end for Iot permanent remains a big challenge.
  - Go for really big players /silo's (Amazon) (inflexible)
  - Or roll your own and keep it small. (needs a human touch)
- IBM and Samsung work on a new decentralized platform: (ADEPT) (Autonomous Decentralized Peer-to-Peer Telemetry



Beyond: References

- Vitalik Buterin on Singularity 1-on-1 (link)
- CoinScrum and Proof of Work: Tools for the Future - Vinay Gupta (yt-link)
- Vinay Gupta – Singapore Talk (yt link)
- Dr. Gavin Wood - DEVCON1: Ethereum for Dummies (yt link)
- http://ethereum.org
- FTP016: Vitalik Buterin on Ethereum and The Decentralized Future (link)
- From cypherpunk to blockchains & Wtf is Ethereum really? - Redecentralize 2015 (yt-link)
- Economist article: The trust machine (link)
- Twitter: @leashless @ReggieMiddleton @pmarca @ethereumproject @gavofyork @VitalikButerin

Conclusions:



- **Bitcoin:** Good solid technology and useable today. But the rest of the world is still adapting.
- **Blockchains:** New way to bring databases to the internet and increase frictionless collaboration between parties.
- **Beyond:** People are making solutions that are global, decentralized, permanent. Mechanizing services in an open source way for people that could not be served.
- **Timeline:** This feels like the internet in 1996.
- **Overall:** Blockchains brings computer democracy to the internet.
  But don't quit your day job yet without a solid plan.

- Thank you for attention.

- Twitter: @jhaand
- E-mail: jhaand@xs4all.nl

Tips: 17DivS7Rc2JPs7oDf1FT3nn5XPF2idNPQ2