Bitcoin and the Blockchain Technology

"On the Blockchain, no one knows you're a fridge" - Richard Brown

Summary

What? (Technology)

Why? (Ideology)

How? (Practicality)

Issues

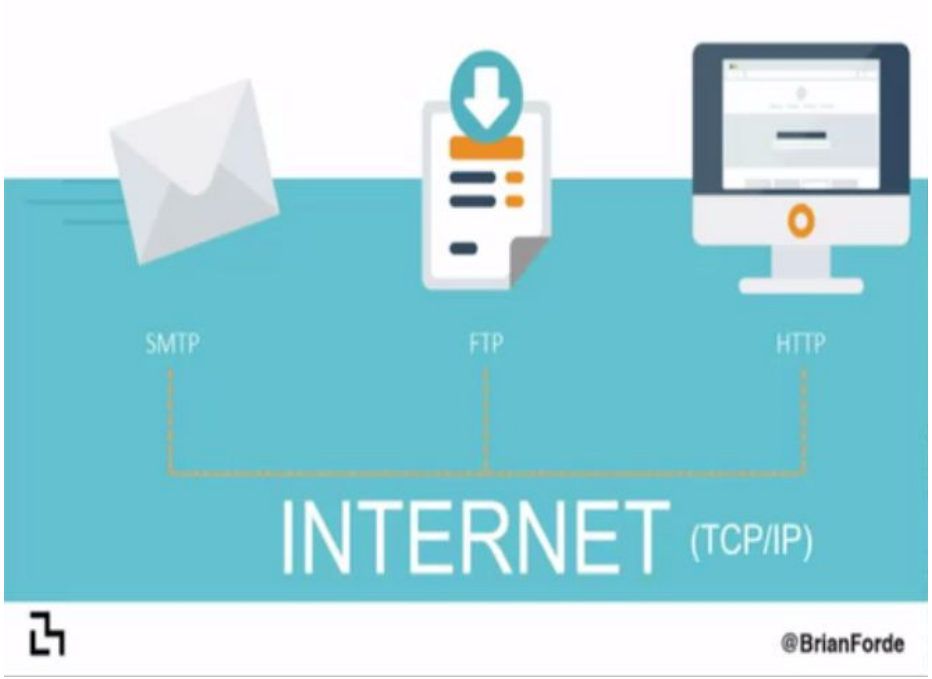
Use cases

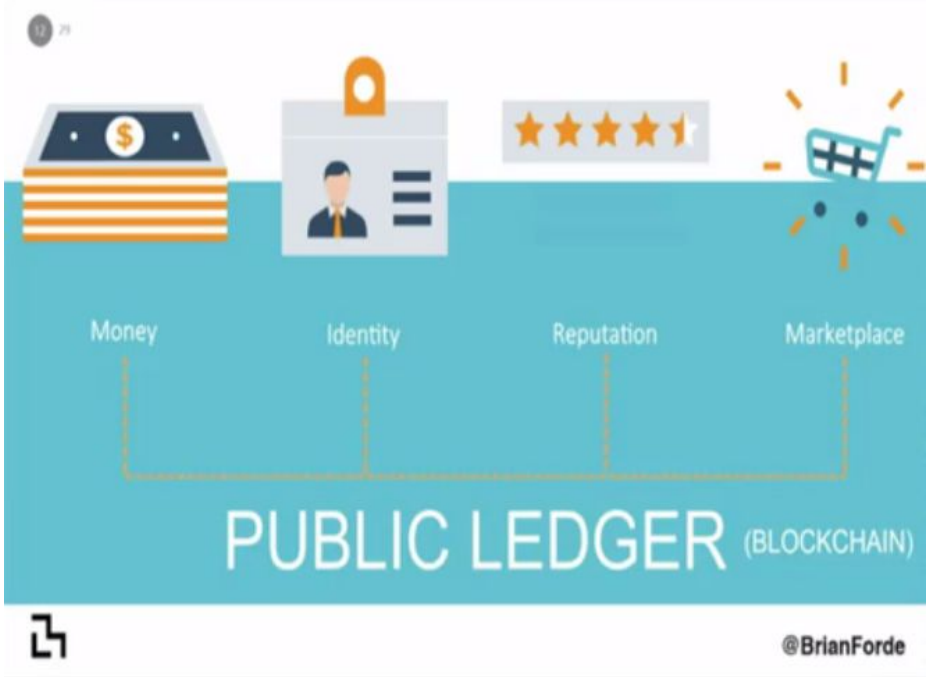
PART I: Technology

What is it?

How does it work?

Bitcoin is the Internet of Finance





Technological innovation

No new technology - a clever combination of existing technologies:

- Distributed Systems
- Peer-to-peer networks
- Hashing function
- Public-Private key **cryptography**
- **Cryptographic** signatures
- Elliptic curve **cryptography**

What is Bitcoin: https://www.youtube.com/watch?v=Gc2en3nHxA4

Building Blocks

Bitcoin software - open-source application implementing the bitcoin protocol

Peer-to-peer network - decentralized network of nodes running the software

Blockchain - decentralized database of transactions

Bitcoin token - decentralized digital currency

Bitcoin address - cryptographic key pair

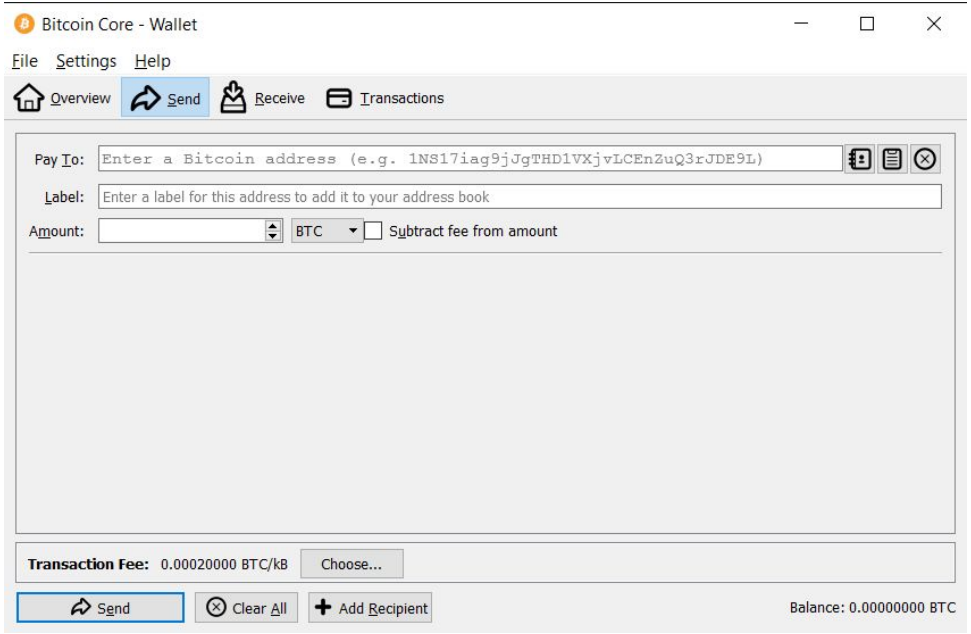
Bitcoin wallet - where you keep your keys

Bitcoin software

Your **interface** to the Bitcoin ecosystem

Open-source:
https://github.com/bitcoin/bitcoin

Your **vote** on the bitcoin protocol



https://coin.dance/nodes

Bitcoin Wallets and Address

Bitcoins are not “stored” anywhere. There are no “accounts”.

- Public address: “receive” bitcoins (transactions outputs)
- Private address: prove bitcoin ownership, sign messages

Related to cryptographic **public/private key pair** - mathematically linked.
Derived using *Elliptic Curve Digital Signature Algorithm (ECDSA).*

Can have multiple public addresses corresponding to one private address

Wallet seed: guarded rated nephew violin semifinal egotistic aloof zigzags raking rhythm reef justice rated ….

Transactions

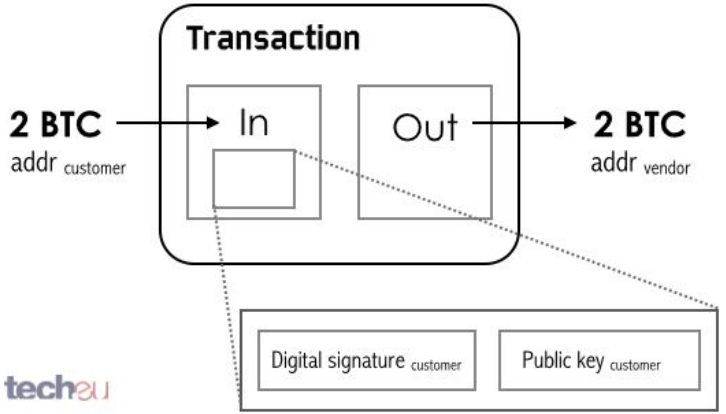
http://cryptograffiti.info/#4573

A transaction is a **message** containing:

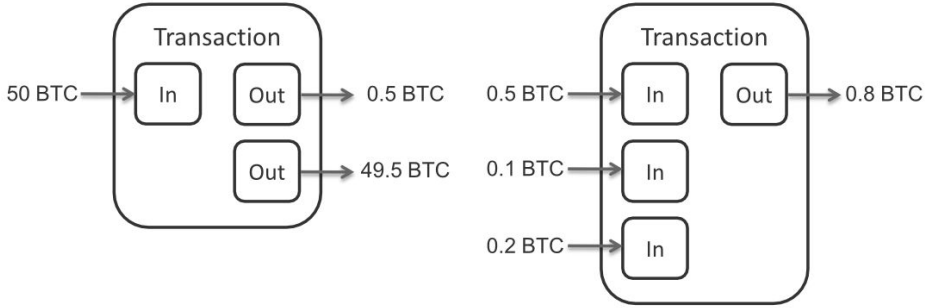
- output(s): btc amount to a public address
- input(s): output of previous transaction to a public address
- (optionally) data: 80 bytes of data

Transfer of bitcoin ownership
from inputs to outputs

How many bitcoins I own?
The total value of all unspent
transaction outputs that I can prove I own



Transactions



Your message **broadcasted** to the network:

- Input: In block 1 someone transferred ownership of 50BTC to public address X
  - Signature: I hereby prove I own public address X by signing that unspent output from block 1 with the private key corresponding to X
- Output: I now transfer ownership of 0.5BTC to public address Y and 49.5BTC to Z.
  - Anyone who can prove ownership of these public addresses can spend these amounts.

Nodes in the network verify your message:

- Is the referenced transaction in block 1 valid?
- Does the signature correspond to public address X?

http://bitbonkers.com/

You need to *convince* the network of the bitcoins you control

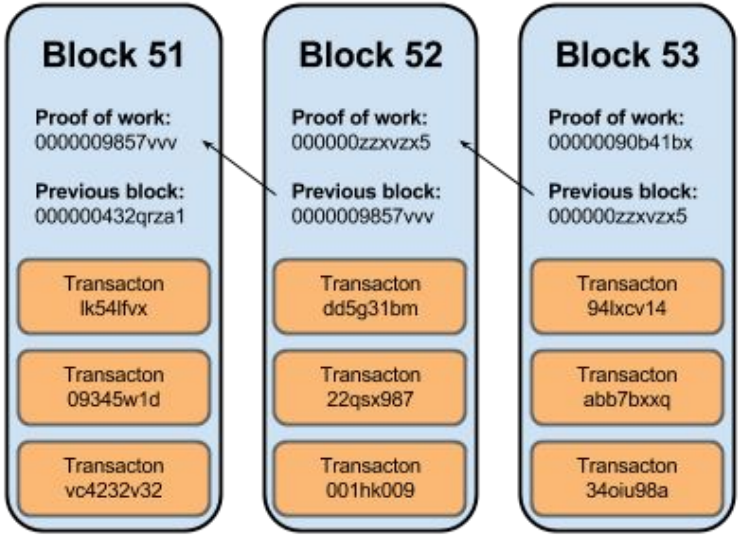
Blockchain

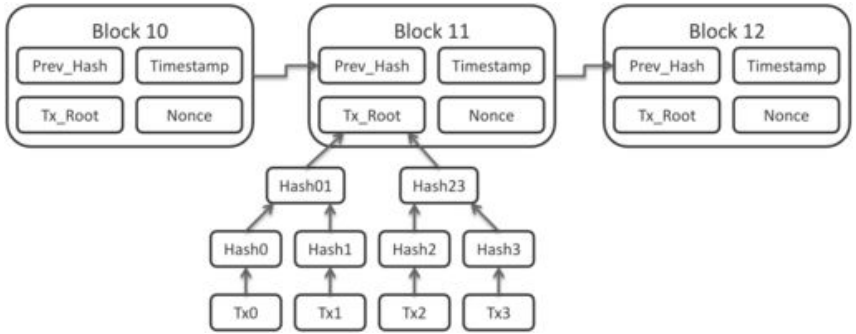
Broadcasted transactions are gathered in a “block”.

Blocks are “mined” and appended to the blockchain.

Public distributed immutable **ledger** of transactions.

Each block “points” to the previous one.





Mining

Who gets to write the next block? How to select one node in the whole peer-to-peer network? - achieving decentralized consensus

Proof-of-work protocol for decentralized consensus:

1. Miners solve mathematically hard puzzle (takes ~10 minutes to solve)
2. The first one to find the solution announces it to the network
3. Gets to write the next block
4. Generates new Bitcoins as a reward

One block “mined” every ~10 minutes. Reward halves every 4 years.

Summary on Technology

A **peer-to-peer network** of nodes running the **Bitcoin software** and protocol

Transfer ownership of Bitcoins using **public/private key pairs**

Transactions are recorded in the **blockchain** decentralized public ledger

Miners secure the ledger and generate **Bitcoin tokens** as a reward

Bitcoin is a payment system based on cryptographic proof, instead of trust.

https://blockchain.info/

PART II: Ideology

What problems it solves?

Why should we care?

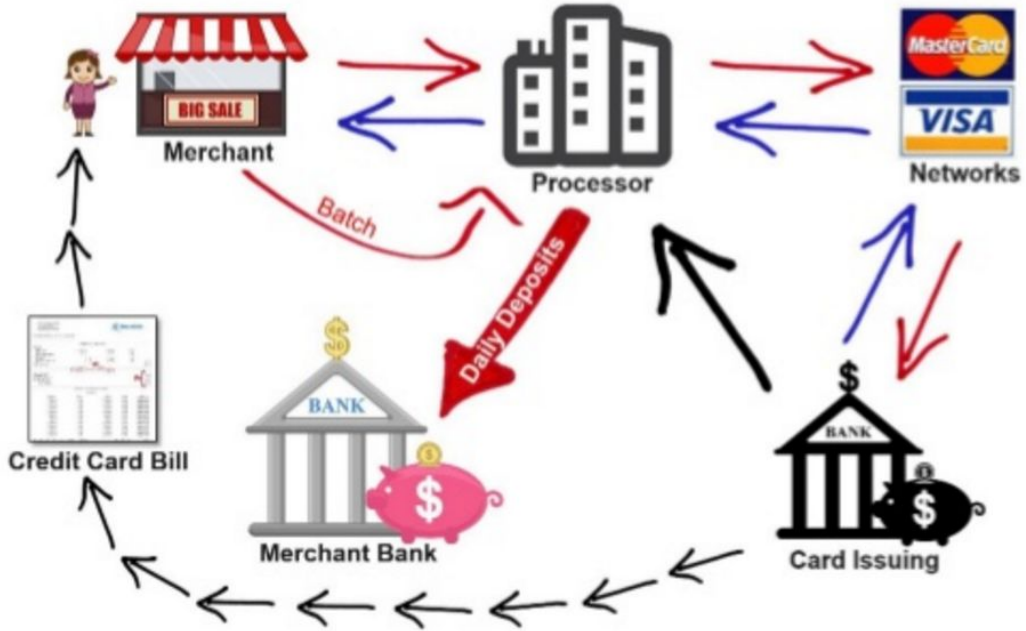
Middlemen have power

The poorer the country, the higher the fees

Digital cash = digital message (email)

$74 billion

Middlemen always take a cut

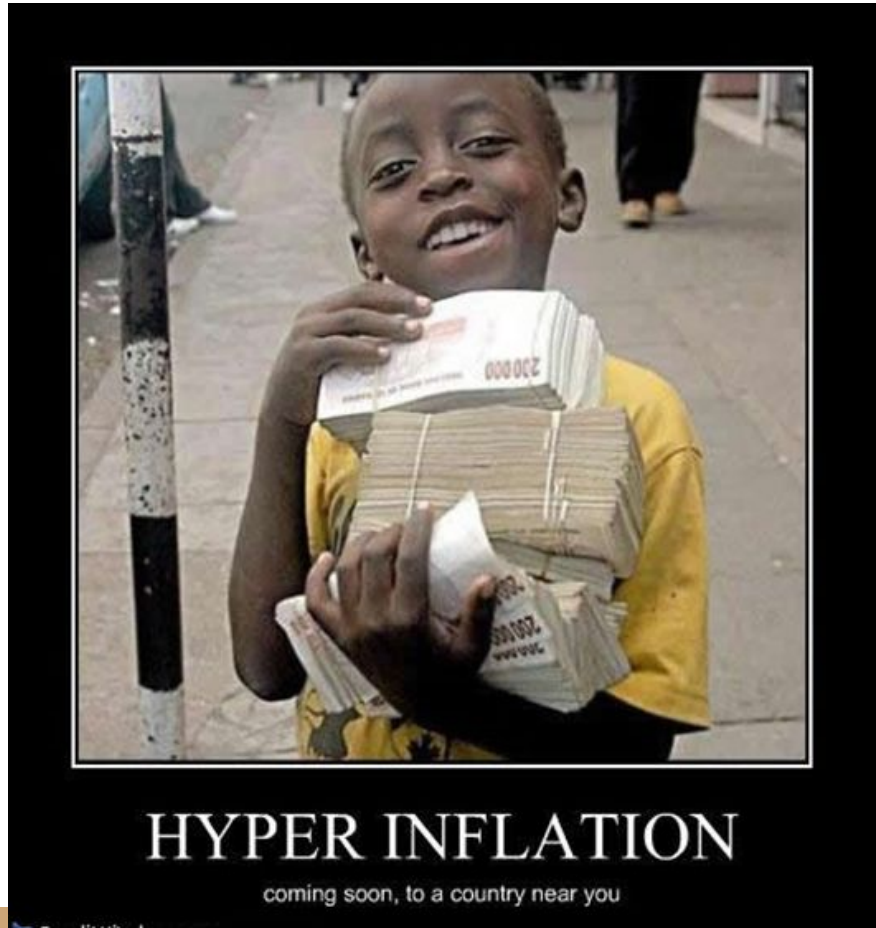


Impose censorship

Transfer to/from Euro zone costs 20 euro!

Governments take populations hostage

Zimbabwe: currency less valuable than the paper it is printed on



Venezuela: The wealth of people is decreasing with 180% a year

Your bank controls your money

Banks impose withdrawal limits

Cyprus →

Banks apply retroactive measures

Belgium →

Tienduizenden spaarders krijgen plots extra taks

Door een extra taks die de regering sinds kort heft op een reeks beleggingsfondsen, zagen tienduizenden spaarders gisteren plots geld van hun rekening gaan. Ze kochten enkele jaren geleden een bepaald type beleggingsfondsen, omdat de meerwaarden daarop belastingvrij waren. Maar de regering veranderde die regel, en voerde voor al die fondsen vorige zomer toch een taks in, met terugwerkende kracht, vanaf 1 juli 2008. En nu pas heeft BNP Paribas zijn computers zo kunnen programmeren dat het bedrag geïnd kan worden. Bij Test-Aankoop liepen al honderden klachten binnen.

(bm)

> 11

Banks seize money from dormant accounts

UK → 15y

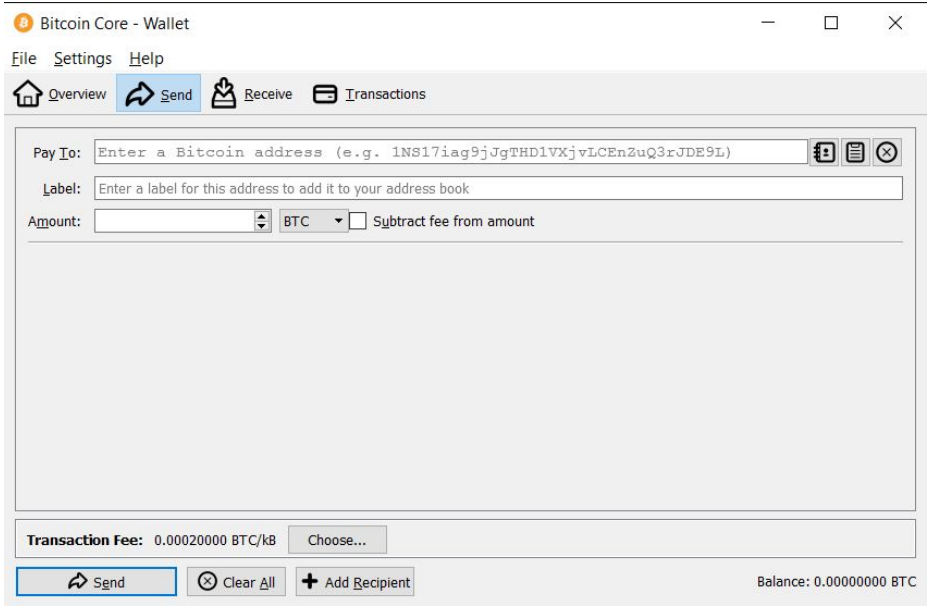
Japan → 10y

Australia → 3y

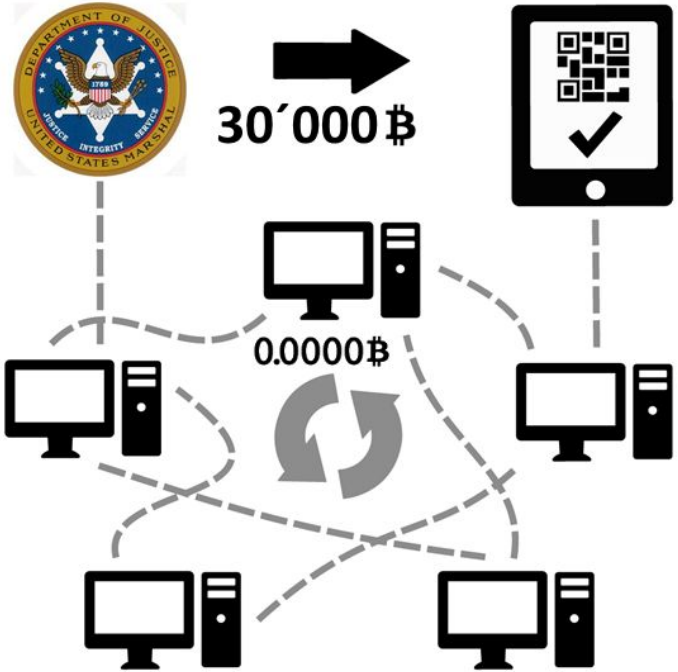
US → 1y

Belgium → ??

Be your own bank



Direct transfer of value. Optional fees

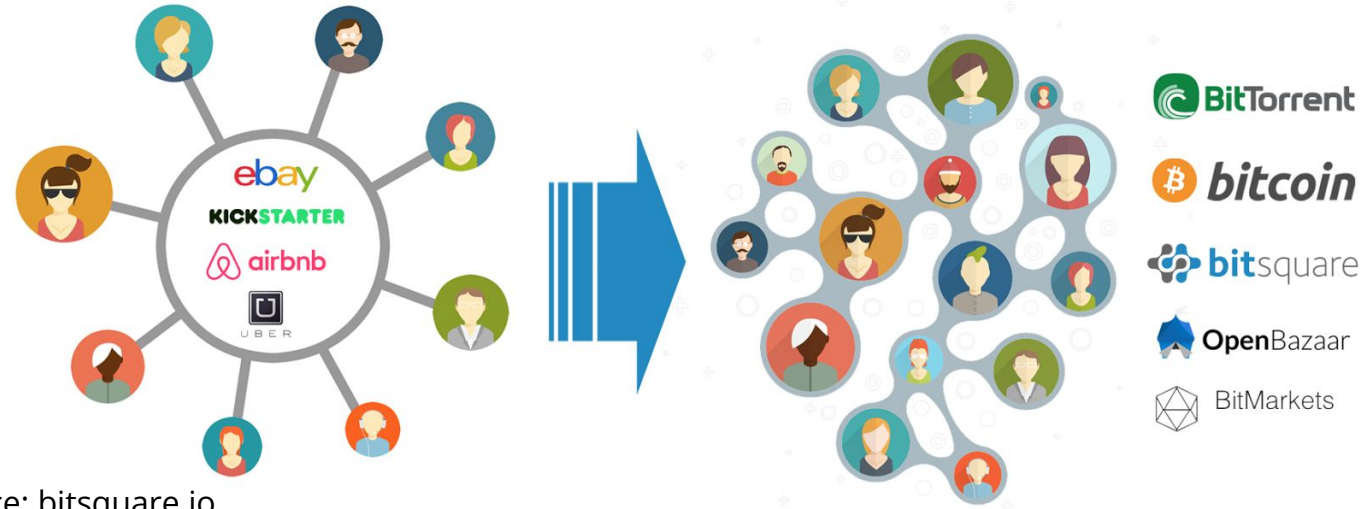


Technology for independence

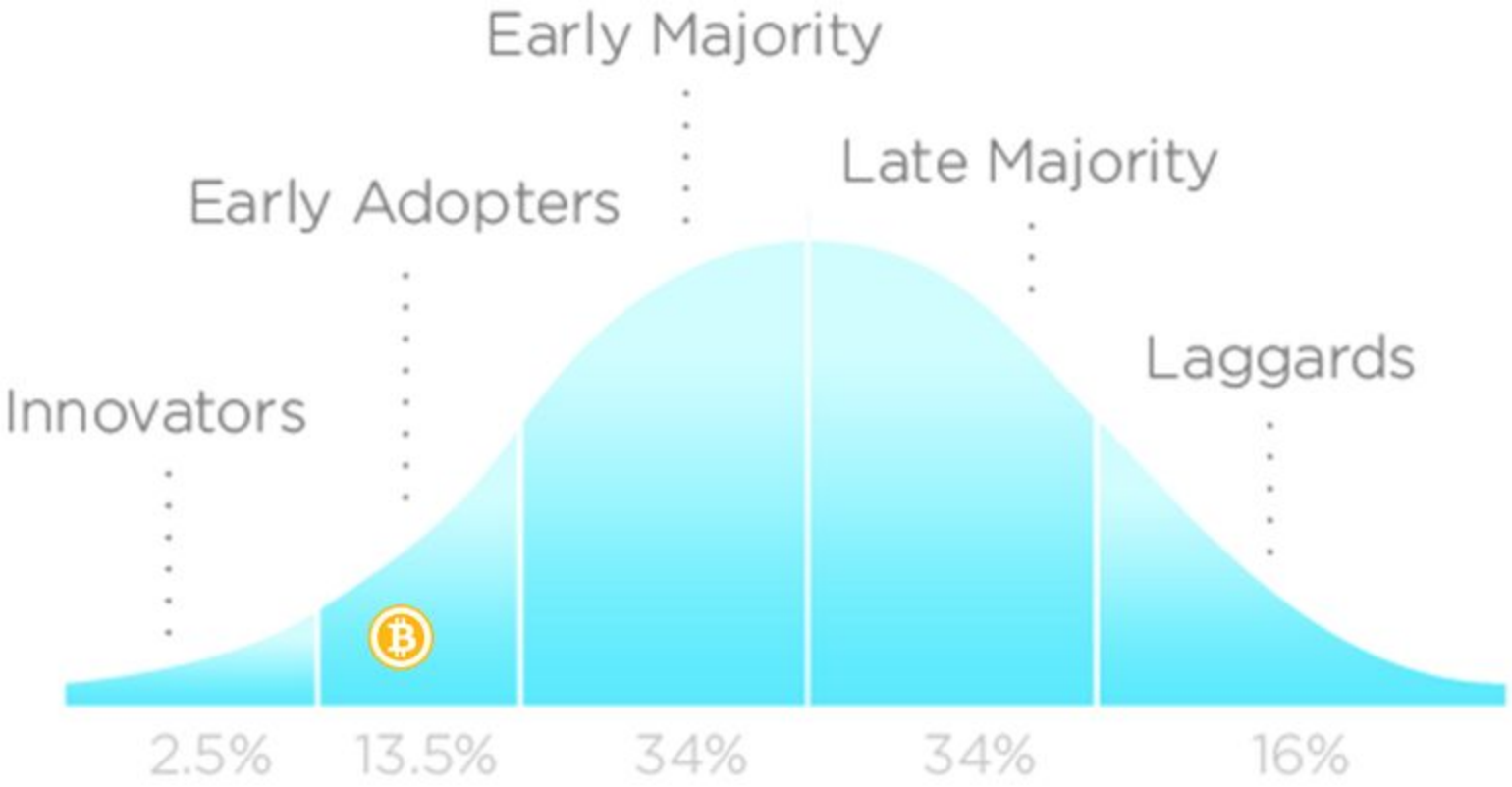
Permissionless innovation

Anyone can pay anyone or create anything without asking permission

Enabling true P2P economy



source: bitsquare.io



INNOVATION ADOPTION LIFECYCLE

Summary - Bitcoin ideology

disintermediation - allows direct transfer of value
empowerment - gives financial power and freedom
independence - you decide what happens with your money
net neutrality - does not discriminate source, destination, amount, type, ...
open access - anyone can participate
permissionless - no need to ask for approval
resilient - you can’t kill decentralized currencies
trustless - open-source, publicly auditable
censorship proof- freedom of association
programmable - create complex financial tools

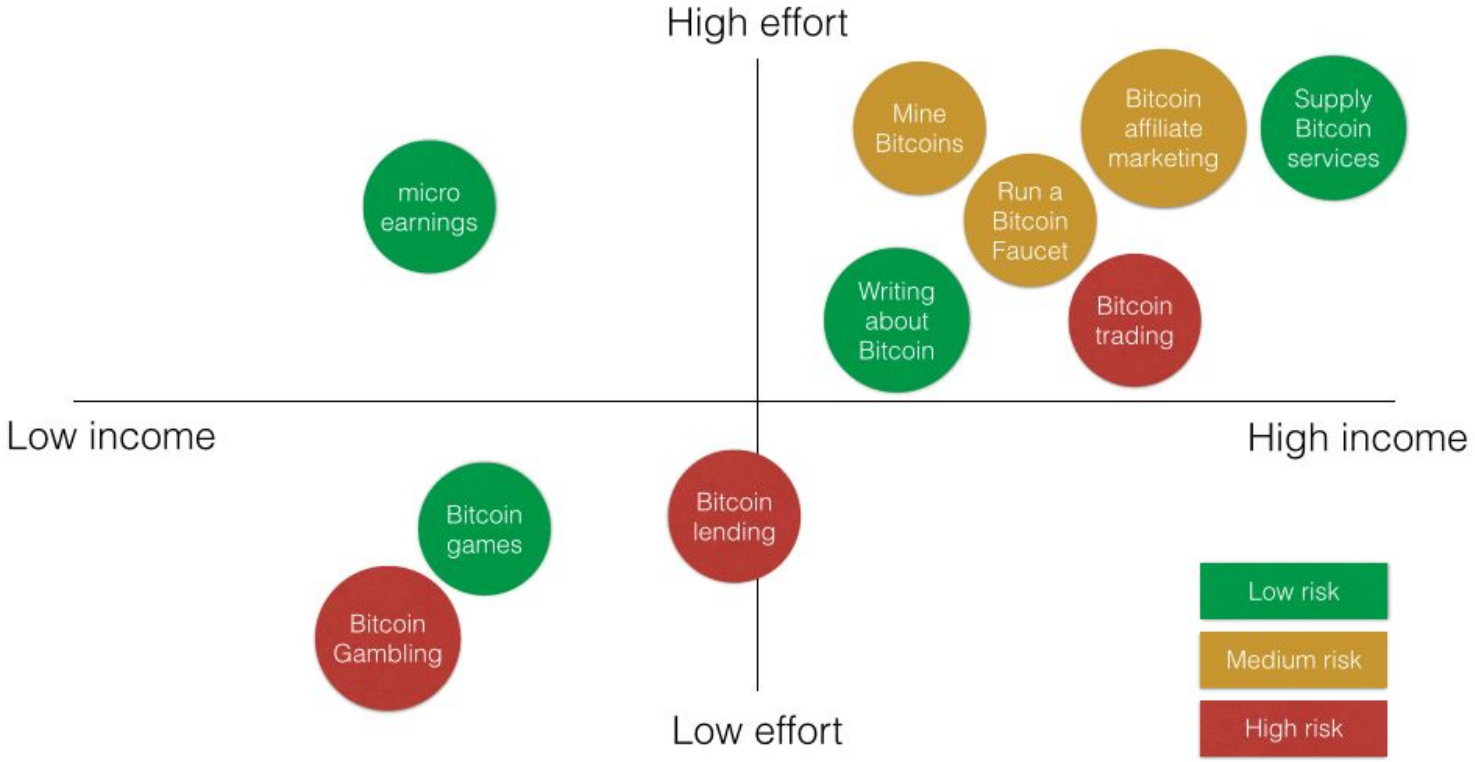
PART III: Practicality

How to get it?

How to store it?

Where to spend it?

How do I get bitcoins?



Buy bitcoins on exchanges

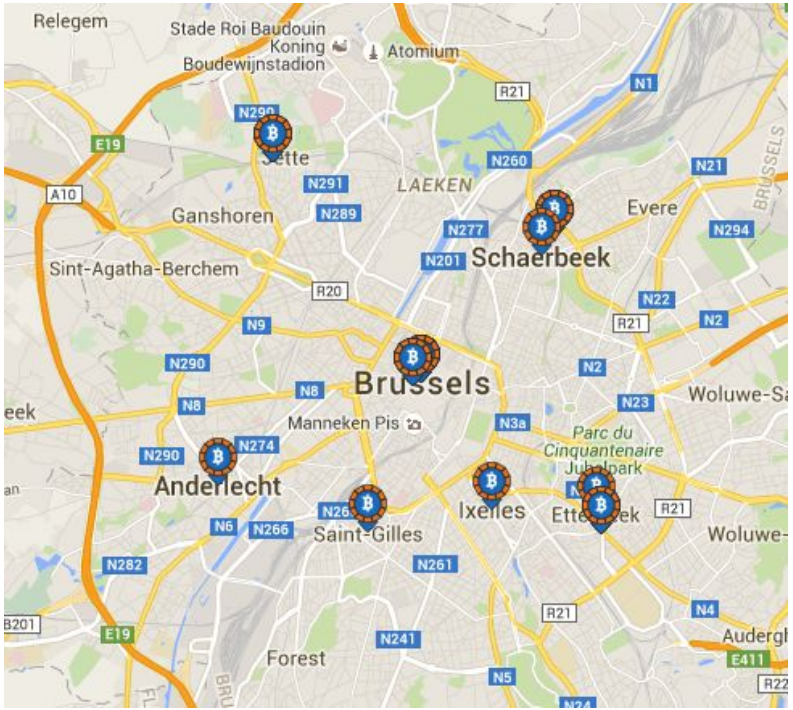
bitsquare

The decentralized bitcoin exchange

bitsquare.io

LocalBitcoins.com

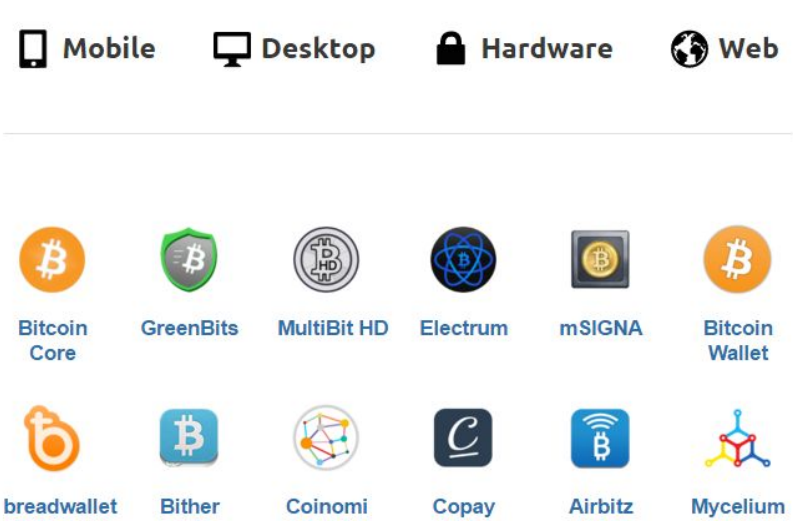
Bringing Bitcoin Everywhere



How do I store my bitcoins?

www.bitaddress.org

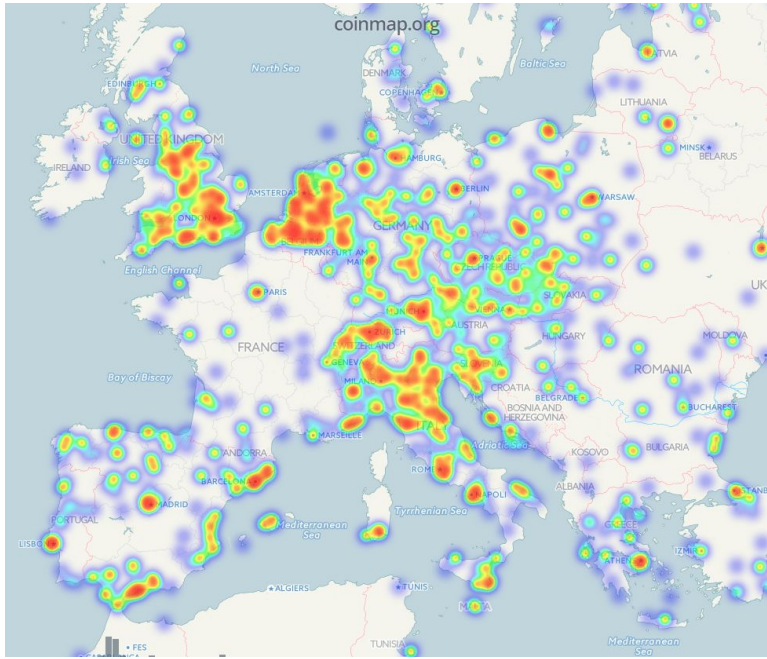
1. Create a wallet
   a. online (web service)
   b. offline (software)
   c. offline (hardware)



2. Keep your wallet safe
   a. stored online
   b. stored on computer
   c. stored offline

Where to spend my bitcoins?

- https://coinmap.org
- Mobile Vikings
- Pizza.be
- Microsoft, Dell, Expedia
- Donations – bloggers, charities, community
- Services – usebitcoins.info; bitcoinget.com
- Things – Purse.io, overstock.com



Practical example

The first one to claim the private key can transfer the money.

https://blockchain.info/

Public address:
1JquFrmLzAEc6k538Egi5VQtu9P1fYK8VL

Private address:
Ky6YfyChFUfiSg6yoVebamLdmxkQk1nQyL34rsYzQZWXRXYfYbxC

Steps:

1. Install a wallet app
   a. e.g. Mycelium, GreenBits, etc.
   b. it creates a wallet for you
2. Sweep private key
   a. in Mycelium -> “Cold Storage”
   b. In Greenbits -> “Sweep”
3. Transfer funds away to your new wallet
4. Never ever use the wallet on this screen again

Summary

1. Inform yourself first! – bitcoin.org (Website), en.bitcoin.it (Wiki)
2. Create wallet securely – bitaddress.org, software wallet
3. Start with small amounts
4. Keep wallet safe

Issues

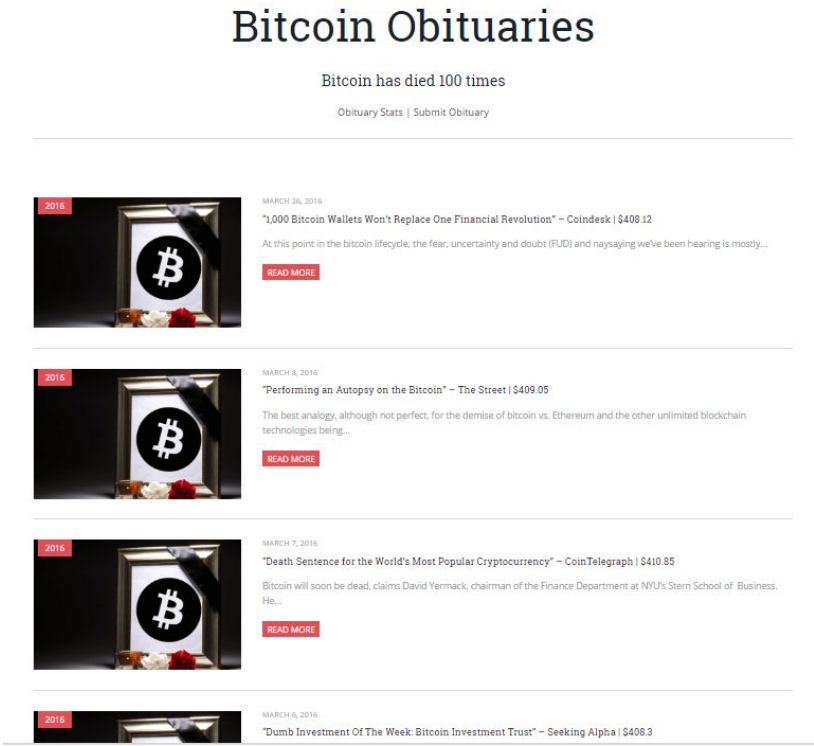
Some form of centralization

Energy consumption

Complex to grasp

No “customer support”

Negative press



Blockchain Use cases (present)

Currency - medium of exchange, store of value, unit of account

Remittance - transfer of value across currencies and without middlemen (e.g. Rebit, Abra)

Decentralized database - each computer keeps a local copy of the entire database. Resilient file storage. (e.g. StorJ)

Proving ownership of digital goods - sign digital goods with private key, everyone can verify using public key (e.g. Ascribe, BitProof, UProov)

Timestamping of documents - send a document as a blockchain transaction, which is timestamped

Digital identity - digital identity signed by private key

Transparent voting - vote by publicly sending a digital token that you own, or delegate your vote by transferring ownership of that token

Blockchain Use cases (present)

Crowdfunding without escrow - multisignature wallet collects micro donations and sends them only if the target amount has been reached by a given time (e.g. Lighthouse app)

Provably fair gambling - open source, no “backstage” manipulations (SathoshiDice)

Micropayments - pay per second in video streaming (e.g. streamium.io), pay per minute of consumption in smart grids, micro-donations without overhead (e.g. ChangeTip)

Decentralized markets - currency/goods/prediction markets without trusted central party. (e.g. Bitsquare, OpenBazaar, Augur)

Transparent supply chain - tracing the origins and histories of products (e.g. Provenance)

Smart contracts, Decentralized Autonomous Organizations, Synergetic Cooperations, etc.

Blockchain Use cases (in development)

P2P trading - trade goods/services directly between peers (e.g. energy in Brooklyn Microgrid)

Tamper-resistant storage - police body camera videos stored on a Blockchain to ensure that video evidence has not been tampered with, and verify where and when the video is taken.

Transparent performance monitoring - making sure funds from the federal government are spent well by local governments. dynamic performance monitoring, rather than a static annual report.

Decentralized login security - login granted if user identified by >50% of participating computers

Transfer of ownership of physical goods (car, home,...) - ownership of a digital token grants access to device/home. Transfer ownership by transferring token.

Payment in IoT - devices can pay to each other without mediator

> **"#InternetOfThings is when the toaster mines Bitcoins to pay off its gambling debts to the fridge"** - Andrew Miller (Twitter)

https://www.youtube.com/watch?v=j23HnORQXvs

Ethereum as Bitcoin v2.0

Solidity - a programming language for the blockchain

Smart contract - program that lives on the blockchain; publicly auditable open-source decentralized application (ĐApp)

Decentralized Autonomous Organization (ĐAO) - a self-governing transparent organization with incorruptible business rules; able to formalise multilateral relationships or transactions

Everyone can reliably expect the programmed instructions to be consistently and securely executed

http://dapps.ethercasts.com/

Pointers

Starting point - www.bitcoin.org, https://en.bitcoin.it

Coursera free online course - https://www.coursera.org/course/bitcointech

Andreas Antonopoulos - book, youtube videos

Antonopoulos, Andreas. *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", 2014.

Bitcoin original paper - https://bitcoin.org/bitcoin.pdf

Nakamoto, Satoshi. *Bitcoin: A peer-to-peer electronic cash system*, 2008.

bitcoin.org