Peer production and Bitcoins.

Lasse Grinderslev Andersen

July 25th, 2014

Overview of this talk

- **Discovery and development of ’computability’**
  - In mathematics
  - In engineering
  - Important (early) breakthroughs
- Decentralization of production and the information economy
  - Industrial production
  - Peer production
- Bitcoins
  - Technical Details
  - Bitcoins in practice

Discovery & Development: Math

A general and vague notion of computability have been known for quite some time.. but:

1879 Freges publishes *Begrriffshrift*, invents predicate logic & isolates logical inferences.

1884 Freges publishes *Die Grundlagen der Arithmetik*, reduces aritmetik to logic.

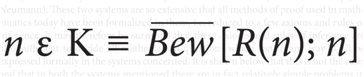
1910 Russell & Whitehead publishes *Principia Mathematica*, sougth to reduce mathematics to logic

Discovery & Development: Math

A general and vague notion of computability have been known for quite some time.. but:

1920 Hilbert states his metamathematics program: '*Formalize all of mathematics and prove it is consistent*'.

1931 Gödel proves its impossibility by reducing logic to arithmetic (by general recursive functions)

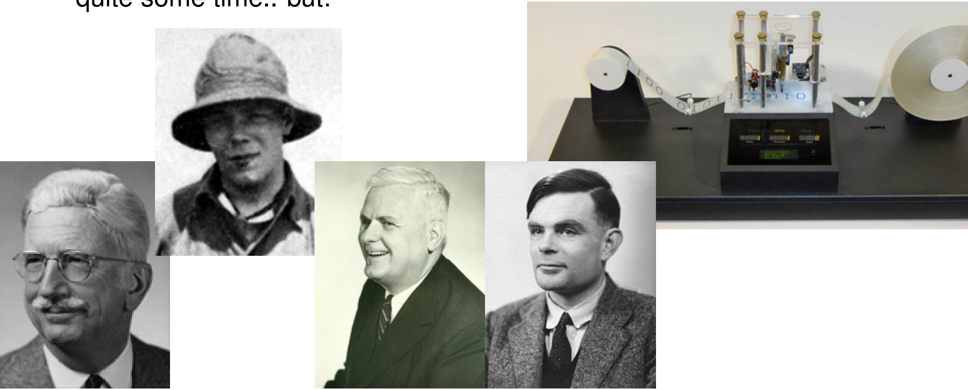


Neumann). These two systems are so extensive that all methods of proof used in math-
ematics today have been formalized in them, i.e. reduced to a few axioms and rules of
inference. It may therefore be surmised that these axioms and rules of inference are
also sufficient to decide all mathematical questions which can in any way at all be
expressed formally in the systems concerned. It is shown below that this is not the case
and that in both the systems mentioned there are in fact relatively simple problems in

$$n \, \varepsilon \, \mathrm{K} \equiv \overline{Bew}\,[R(n); n]$$

Discovery & Development: Math

A general and vague notion of computability have been known for quite some time.. but:



1936 Church and Turing independently showed there was no general solution to the Hilberts 'Decision Problem'

1939 Rosser proves equivalence: Churchs λ-calculus, Gödel + Herbrands recursive functions and Turings abstract machine

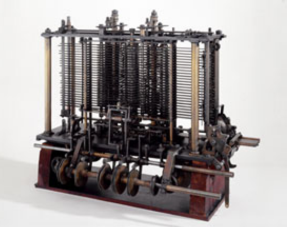
Discovery & Development: Math

Sum up: The formal notion of computability was about finding the largest class of machine-computable functions AND it was shown that logical inferences was among them!

Discovery & Development: Engineering

First Turing complete machines:

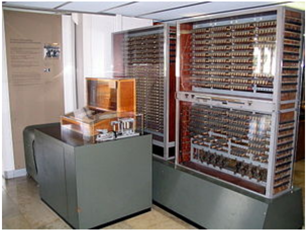
Name	Year	Comment
Analytical Engine (UK)	1837	Babbage made the drawings, never built
Zuse Z3 (DE)	1941	In principle TC, no branching!
ENIAC (US)	1946	Programming by cables.
Manchester Baby (UK)	1948	First stored program computer
UNIVAC (US)	1951	First 'mass produced' commerical compu



Discovery & Development: Engineering

First Turing complete machines:

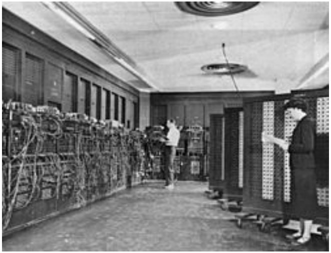
Name	Year	Comment
Analytical Engine (UK)	1837	Babbage made the drawings, never built
Zuse Z3 (DE)	1941	In principle TC, no branching!
ENIAC (US)	1946	Programming by cables.
Manchester Baby (UK)	1948	First stored program computer
UNIVAC (US)	1951	First 'mass produced' commerical compu

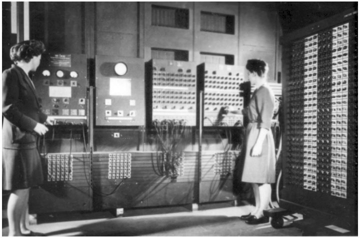


Discovery & Development: Engineering

First Turing complete machines:

Name	Year	Comment
Analytical Engine (UK)	1837	Babbage made the drawings, never built
Zuse Z3 (DE)	1941	In principle TC, no branching!
ENIAC (US)	1946	Programming by cables.
Manchester Baby (UK)	1948	First stored program computer
UNIVAC (US)	1951	First 'mass produced' commerical compu

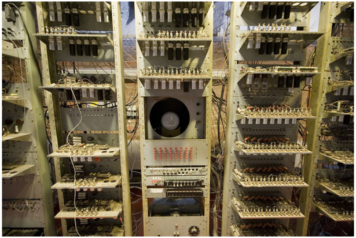




Discovery & Development: Engineering

First Turing complete machines:

Name	Year	Comment
Analytical Engine (UK)	1837	Babbage made the drawings, never built
Zuse Z3 (DE)	1941	In principle TC, no branching!
ENIAC (US)	1946	Programming by cables.
Manchester Baby (UK)	1948	First stored program computer
UNIVAC (US)	1951	First 'mass produced' commerical compu



Discovery & Development: Engineering

First Turing complete machines:

Name	Year	Comment
Analytical Engine (UK)	1837	Babbage made the drawings, never built
Zuse Z3 (DE)	1941	In principle TC, no branching!
ENIAC (US)	1946	Programming by cables.
Manchester Baby (UK)	1948	First stored program computer
UNIVAC (US)	1951	First 'mass produced' commerical comput

Discovery & Development: Engineering

First Turing complete machines:

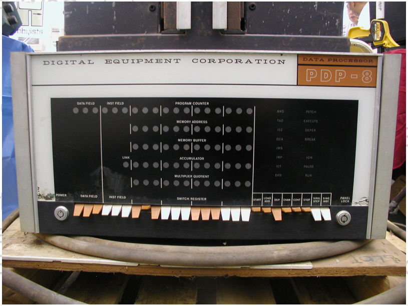
Name	Year	Comment
Analytical Engine (UK)	1837	Babbage made the drawings, never built
Zuse Z3 (DE)	1941	In principle TC, no branching!
ENIAC (US)	1946	Programming by cables.
Manchester Baby (UK)	1948	First stored program computer
UNIVAC (US)	1951	First 'mass produced' commerical compu

1945 Practice & theory joined:
First Draft of a Report on the EDVAC 'by' John von Neumann

Important breakthroughs

Fundamental decentralization & generativity of computability:

- ..of hardware
  - In the 1960s DEC introduces the mini-computer
  - Small-scale, new markets
  - Open specification, encouraging user modification/development
  - Mainframe ⇒ mini-computer ⇒ PC ⇒ smartphone
- ..of software
  - Open standards (IETF
  - Open source
- ..of communications
  - Networking ⇒ failure
  - In the beginning were BS, etc.
  - FidoNet, primitive rou
  - Internet, failure resista
  - Internet build on the 'E d, Clark, 1981)



Important breakthroughs

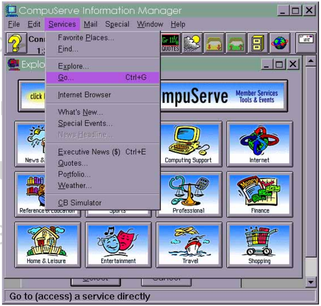
Fundamental decentralization & generativity of computability:

- ..of hardware
  - In the 1960s DEC introduces the mini-computer
  - Small-scale, new markets
  - Open specification, encouraging user modification/development
  - Mainframe ⇒ mini-computer ⇒ PC ⇒ smartphone
- ..of software
  - Open standards (IETF, W3C etc.)
  - Open source
- ..of communications
  - Networking ⇒ failure of Groschs law
  - In the beginning were 'online services': CompuServe, BBS, etc.
  - FidoNet, primitive routing
  - Internet, failure resistance ⇒ decentralized
  - Internet build on the 'End-to-End' principle (Saltzer, Reed, Clark, 1981)

Important breakthroughs

Fundamental decentralization & generativity of computability:

- ..of hardware
  - In the 1960s DEC introduc
  - Small-scale, new markets
  - Open specification, encou modification/development
  - Mainframe ⇒ mini-comput
- ..of software
  - Open standards (IETF, W3
  - Open source
- ..of communications
  - Networking ⇒ failure of Groschs law
  - In the beginning were 'online services': CompuServe, BBS, etc.
  - FidoNet, primitive routing
  - Internet, failure resistance ⇒ decentralized
  - Internet build on the 'End-to-End' principle (Saltzer, Reed, Clark, 1981)



Go to (access) a service directly

Important breakthroughs

Fundamental decentralization & generativity of computability:

2014 Turing Complete devices is cheap, fast, connected and comes in pocket sizes!

Overview of this talk

- Discovery and development of ’computability’
  - In mathematics
  - In engineering
  - Important (early) breakthroughs
- **Decentralization of production and the information economy**
  - Industrial production
  - Peer production
- Bitcoins
  - Technical Details
  - Bitcoins in practice

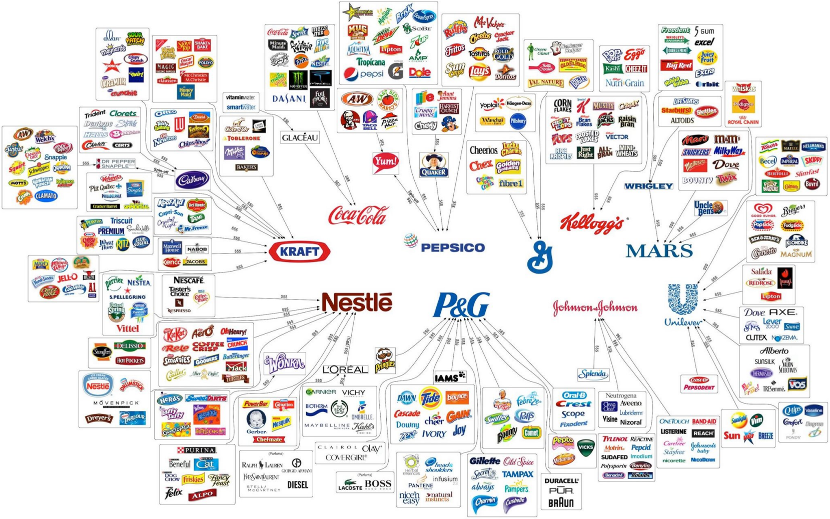
Industrial production

The industrial age have brought growth and prosperity, but..

- **Assumption:** We are inherently selfish! ⇒ top-down institutions, material incentives, market-based approaches to everything

Industrial production

- **Centralization: Bigger is better**
  - High initial cost
  - Aggressive marketing

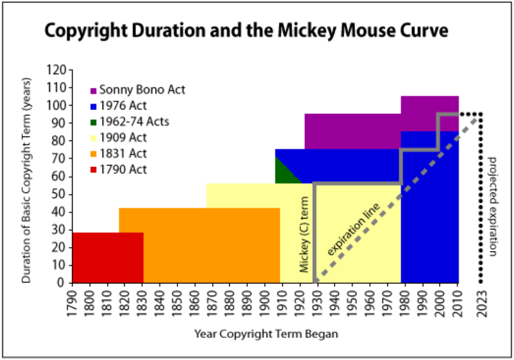


Industrial production

- One-to-many relationship between producers and consumers
- Lowest denominator

Industrial production

- Increased barrier of entry in politics
  ⇒ need money from $BigCorp
- Strengthened Intellectual Property rights
- Lobbying/Regulatory Capture



Industrial production

Industrial/free market capitalistic production does seem to have some general bad sideeffects...

Peer production

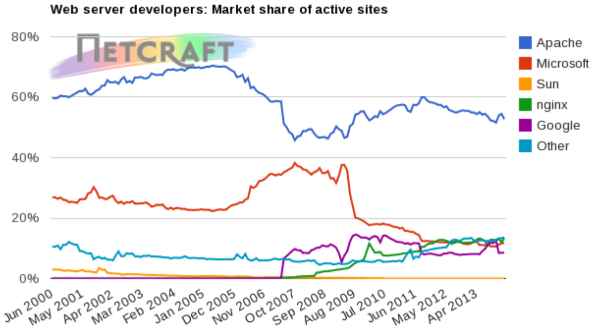
Properties of new (commons-based) peer production

- **Assumption:** We enjoy autonomy, cooperating and find meaning & value in creating for others

Peer production

Properties of new (commons-based) peer production

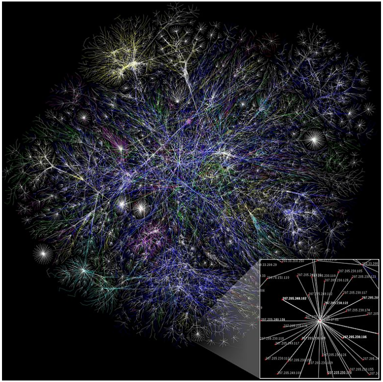
- Decentralized:
  - Production: Wikipedia, Amazon, Google, GNU/Linux, **Apache**, (FOSS), etc. etc.
  - *Resiliant* non-SPF platforms: Bittorrent, Bitcoins, Tor, HTTP, the **Internet**



Peer production

Properties of new (commons-based) peer production

- Decentralized:
  - Production: Wikipedia, Amazon, Google, GNU/Linux, **Apache**, (FOSS), etc. etc.
  - *Resiliant* non-SPF platforms: Bittorrent, Bitcoins, Tor, HTTP, the **Internet**



Peer production

Properties of new (commons-based) peer production

- Commons (Creative commons, GPL etc.)
- Modular (SETI@home, NASA Mars Mapping)
- Low barrier of entry
- Many-to-many communication and free information sharing (blogosphere, slashdot, youtube)
- Less aggressive income & Crowdsourcing/crowdfunding (kickstarter, indiegogo)

Peer production

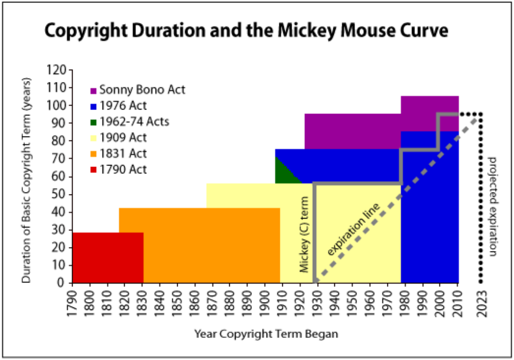
Properties of new (commons-based) peer production

Relying on a generative platform: Network & Devices

Gatekeeping

The open generative ecology under pressure by gatekeepers:

- Strengthens IP laws
- Control of computability: Thethered appliances & Vendor lock-in
- Paywalls (wtf scientists?!)
- Software patents
- Destro



Gatekeeping

The open generative ecology under pressure by gatekeepers:

- Strengthens IP laws
- Control of computability: Thethered appliances & Vendor lock-in
- Paywalls (wtf scientists?!)
- Software patents
- Destroying net-neutrality

Gatekeeping

The open generative ecology under pressure by gatekeepers:

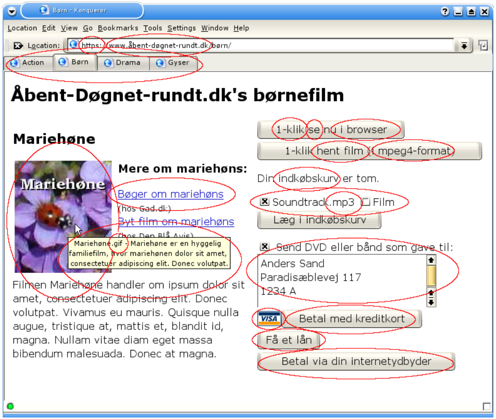
- Strengthens IP laws
- Control of computability: Thethered appliances & Vendor lock-in
- Paywalls (wtf scientists?!)
- Software patents
- Destroying net-neutrality

NON SOLUS
LSEVIER

Gatekeeping

The open generative ecology under pressure by gatekeepers:

- Strengthens IP laws
- Control of computability: Thethered appliances & Vendor lock-in
- Paywalls (wtf scientists?!)
- Software patents
- Destroying net-neutral


Børn - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location: https://www.åbent-døgnet-rundt.dk/børn/
Action
Børn
Drama
Gyser
1-klik se nu i browser
1-klik hent film i mpeg4-format
Læg i indkøbskurv
Betal med kreditkort
Få et lån
Betal via din internetydbyder

Åbent-Døgnet-rundt.dk's børnefilm

Mariehøne

Mere om mariehøns:

Bøger om mariehøns
(hos Gad.dk)

Byt film om mariehøns
(hos Den Blå Avis)

Mariehøne.gif - Mariehøne er en hyggelig familiefilm, hvor mariehønen dolor sit amet, consectetuer adipiscing elit. Donec volutpat.

Filmen Mariehøne handler om ipsum dolor sit amet, consectetuer adipiscing elit. Donec volutpat. Vivamus eu mauris. Quisque nulla augue, tristique at, mattis et, blandit id, magna. Nullam vitae diam eget massa bibendum malesuada. Donec at magna.

Din indkøbskurv er tom.

☒ Soundtrack.mp3 ☐ Film

☒ Send DVD eller bånd som gave til:

Anders Sand
Paradisæblevej 117
1234 A

Gatekeeping

The open generative ecology under pressure by gatekeepers:

- Strengthens IP laws
- Control of computability: Thethered appliances & Vendor lock-in
- Paywalls (wtf scientists?!)
- Software patents **Beware, the patent trolls are coming!**
- Destroying net-neutrality

Gatekeeping

The open generative ecology under pressure by gatekeepers:

- Strengthens IP laws
- Control of computability: Thethered appliances & Vendor lock-in
- Paywalls (wtf scientists?!)
- Software patents
- Destroying net-neutrality

FEDERAL COMMUNICATIONS COMMISSION

Overview of this talk

- What bitcoins is and how it works
- Present state of bitcoins
- Myth & facts
- Perspectives

Introduction

’That’s the kind of society I want to build. I want a guarantee – with physics and mathematics, not with laws – that we can give ourselves real privacy of personal communications.’

- John Gilmore

Introduction

- In 2010 Visa/MasterCard handled 85% of all credit card transactions
- In 2005 Visa and MasterCard earned 30 billion $ in ’interchange fees’
- Centralized control/surveillance on the flow of money: MasterCard blocked payment to Wikileaks, PayPal blocking payment to cyberlockers
- Paypal: 3% receiving tranasction fee
- PayPal and MasterCard actively try to block bitcoin related bussineses

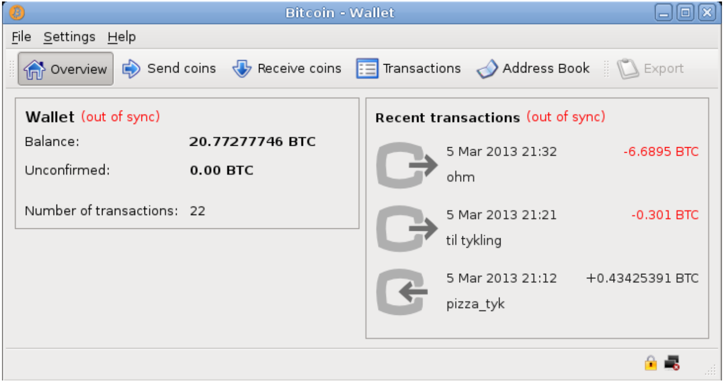
Introduction

- In 2010 Visa/MasterCard handled 85% of all credit card transactions
- In 2005 Visa and MasterCard earned 30 billion $ in 'interchange fees'
- Centralized control/surveillance on the flow of money: MasterCard blocked payment to Wikileaks, PayPal blocking payment to cyberlockers
- Paypal: 3% receiving tranasction fee
- PayPal and MasterCard actively try to block bitcoin related bussineses

...and the of course the entire post-Snowden mass-surveillance world!

What is bitcoins

- 2009: Invented by ’Satoshi Nakamoto’ and described in his/her *Bitcoin: A Peer-to-Peer Electronic Cash System*
- Made reference implementation... and disappeared!
- Open source!



Wallet (out of sync)

Balance: **20.77277746 BTC**

Unconfirmed: **0.00 BTC**

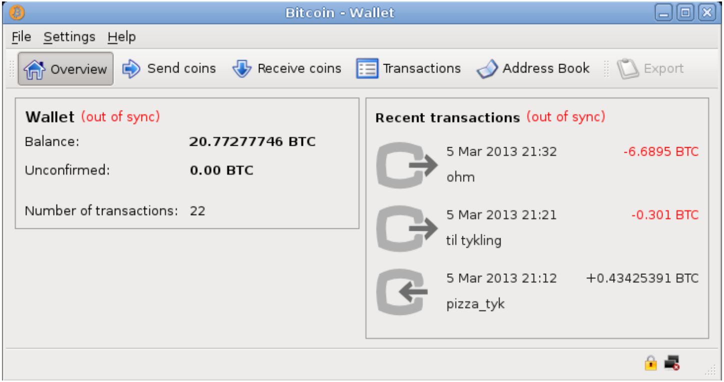
Number of transactions: 22

Recent transactions (out of sync)

5 Mar 2013 21:32 ohm	-6.6895 BTC
5 Mar 2013 21:21 til tykling	-0.301 BTC
5 Mar 2013 21:12 pizza_tyk	+0.43425391 BTC

What is bitcoins

- 2009: Invented by 'Satoshi Nakamoto' and described in his/her *Bitcoin: A Peer-to-Peer Electronic Cash System*
- Made reference implementation... and disappeared!
- Open source!



Wallet (out of sync)

Balance: 20.77277746 BTC

Unconfirmed: 0.00 BTC

Number of transactions: 22

Recent transactions (out of sync)

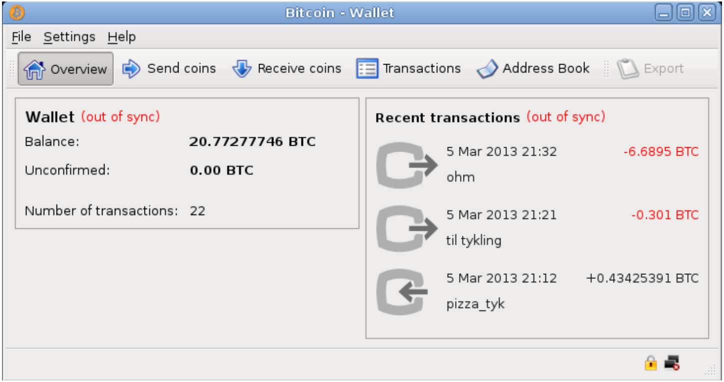
5 Mar 2013 21:32 -6.6895 BTC
ohm

5 Mar 2013 21:21 -0.301 BTC
til tykling

5 Mar 2013 21:12 +0.43425391 BTC
pizza_tyk

What is bitcoins

- 2009: Invented by ’Satoshi Nakamoto’ and described in his/her *Bitcoin: A Peer-to-Peer Electronic Cash System*
- Made reference implementation... and disappeared!
- Open source!



Bitcoin - Wallet
File Settings Help
Overview Send coins Receive coins Transactions Address Book Export

Wallet (out of sync)

Balance: **20.77277746 BTC**

Unconfirmed: **0.00 BTC**

Number of transactions: 22

Recent transactions (out of sync)

5 Mar 2013 21:32 -6.6895 BTC
ohm

5 Mar 2013 21:21 -0.301 BTC
til tykling

5 Mar 2013 21:12 +0.43425391 BTC
pizza_tyk

How does bitcoins work?

- Wallets/accounts etc. is represented by a string of digits:
  `1GBZ1imm9Fkcfa7EPbQ4dy7QeZb7wH7yGX`
  This is also the public key (in 'human readable form')
- When Alice sends bitcoins to Bob she broadcasts to the network: '**I am sending x BTC to Bob**'
  ...and sign it with her private key.
- The network validates Alices message with her public key and insert it into a **block** the **blockchain**.

How does bitcoins work?

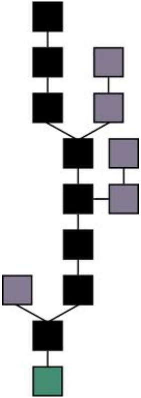
- Wallets/accounts etc. is represented by a string of digits: `1GBZ1imm9Fkcfa7EPbQ4dy7QeZb7wH7yGX`
  This is also the public key (in 'human readable form')
- When Alice sends bitcoins to Bob she broadcasts to the network: '**I am sending x BTC to Bob**'
  ...and sign it with her private key.
- The network validates Alices message with her public key and insert it into a **block** the **blockchain**.

How does bitcoins work?

- Wallets/accounts etc. is represented by a string of digits: `1GBZ1imm9Fkcfa7EPbQ4dy7QeZb7wH7yGX`
  This is also the public key (in 'human readable form')
- When Alice sends bitcoins to Bob she broadcasts to the network: '**I am sending x BTC to Bob**'
  ...and sign it with her private key.
- The network validates Alices message with her public key and insert it into a **block** the **blockchain.**

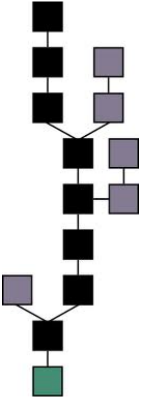
How bitcoin works: The Blockchain

- The blockchain is composed of blocks
- Blocks contains all valid transactions created since last block - defines the truth!
- A decentralized way of dealing with 'double spending'
- Blocks is generated by proof-of-work and is called mining



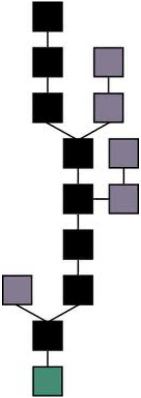
How bitcoin works: The Blockchain

- The blockchain is composed of blocks
- Blocks contains all valid transactions created since last block - defines the truth!
- A decentralized way of dealing with 'double spending'
- Blocks is generated by proof-of-work and is called mining



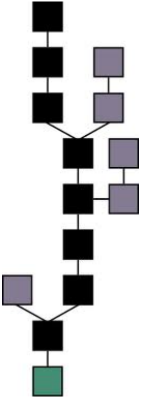
How bitcoin works: The Blockchain

- The blockchain is composed of blocks
- Blocks contains all valid transactions created since last block - defines the truth!
- A decentralized way of dealing with ’double spending’
- Blocks is generated by proof-of-work and is called mining



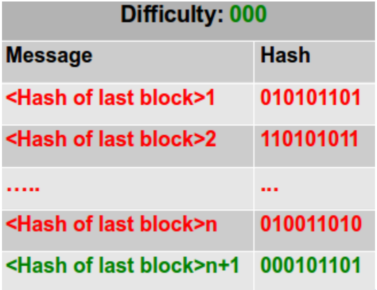
How bitcoin works: The Blockchain

- The blockchain is composed of blocks
- Blocks contains all valid transactions created since last block - defines the truth!
- A decentralized way of dealing with 'double spending'
- Blocks is generated by proof-of-work and is called mining



How bitcoin works: The Blockchain

- Nodes can compete in finding blocks
- A block is found when an 'appropriate' hash is generated
- Solution-checking easy
- Other nodes approve a block by trying to find the next block
- Block-difficulty adjusts every 2016 blocks (14 days)
- Reward of 25 btc for a block *atm.* (max. $21 * 10^6$ BTC)
- Block-reward halves every 210,000 blocks (4years)

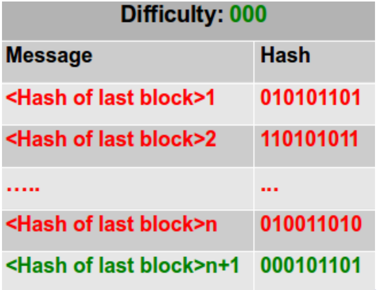


Difficulty: 000

Message	Hash
<Hash of last block>1	010101101
<Hash of last block>2	110101011
…..	...
<Hash of last block>n	010011010
<Hash of last block>n+1	000101101

How bitcoin works: The Blockchain

- Nodes can compete in finding blocks
- A block is found when an ’appropriate’ hash is generated
- Solution-checking easy
- Other nodes approve a block by trying to find the next block
- Block-difficulty adjusts every 2016 blocks (14 days)
- Reward of 25 btc for a block *atm.* (max. $21 * 10^6$ BTC)
- Block-reward halves every 210,000 blocks (4years)

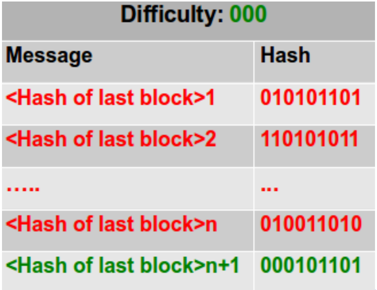


Difficulty: 000

Message	Hash
<Hash of last block>1	010101101
<Hash of last block>2	110101011
…..	...
<Hash of last block>n	010011010
<Hash of last block>n+1	000101101

How bitcoin works: The Blockchain

- Nodes can compete in finding blocks
- A block is found when an ’appropriate’ hash is generated
- Solution-checking easy
- Other nodes approve a block by trying to find the next block
- Block-difficulty adjusts every 2016 blocks (14 days)
- Reward of 25 btc for a block *atm.* (max. $21 * 10^{6}$ BTC)
- Block-reward halves every 210,000 blocks (4years)

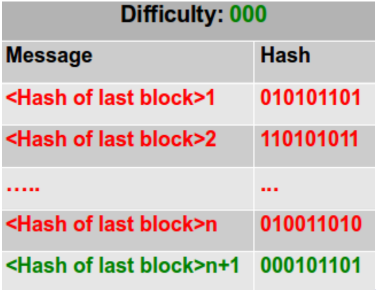


Difficulty: 000

Message	Hash
<Hash of last block>1	010101101
<Hash of last block>2	110101011
…..	...
<Hash of last block>n	010011010
<Hash of last block>n+1	000101101

How bitcoin works: The Blockchain

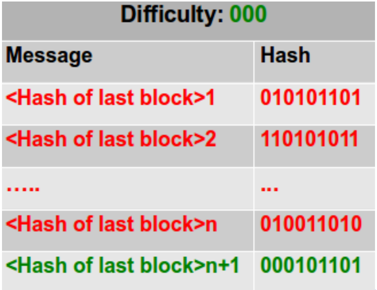
- Nodes can compete in finding blocks
- A block is found when an ’appropriate’ hash is generated
- Solution-checking easy
- Other nodes approve a block by trying to find the next block
- Block-difficulty adjusts every 2016 blocks (14 days)
- Reward of 25 btc for a block *atm.* (max. $21 * 10^6$ BTC)
- Block-reward halves every 210,000 blocks (4years)



Difficulty: 000	
Message	**Hash**
<Hash of last block>1	010101101
<Hash of last block>2	110101011
.....	...
<Hash of last block>n	010011010
<Hash of last block>n+1	000101101

How bitcoin works: The Blockchain

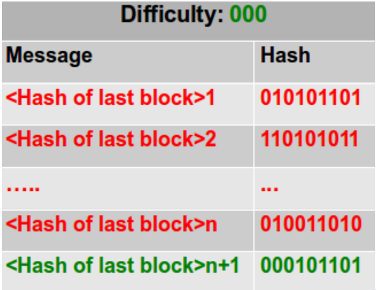
- Nodes can compete in finding blocks
- A block is found when an 'appropriate' hash is generated
- Solution-checking easy
- Other nodes approve a block by trying to find the next block
- Block-difficulty adjusts every 2016 blocks (14 days)
- Reward of 25 btc for a block *atm.* (max. $21 * 10^6$ BTC)
- Block-reward halves every 210,000 blocks (4years)



Difficulty: 000	
Message	Hash
<Hash of last block>1	010101101
<Hash of last block>2	110101011
.....	...
<Hash of last block>n	010011010
<Hash of last block>n+1	000101101

How bitcoin works: The Blockchain

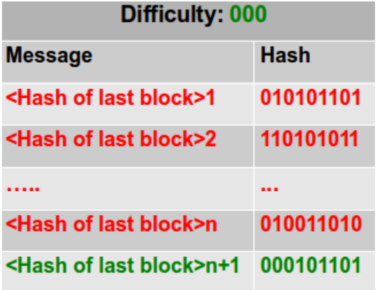
- Nodes can compete in finding blocks
- A block is found when an ’appropriate’ hash is generated
- Solution-checking easy
- Other nodes approve a block by trying to find the next block
- Block-difficulty adjusts every 2016 blocks (14 days)
- Reward of 25 btc for a block *atm.* (max. $21 * 10^6$ BTC)
- Block-reward halves every 210,000 blocks (4years)



Difficulty: 000	
Message	Hash
<Hash of last block>1	010101101
<Hash of last block>2	110101011
.....	...
<Hash of last block>n	010011010
<Hash of last block>n+1	000101101

How bitcoin works: The Blockchain

- Nodes can compete in finding blocks
- A block is found when an 'appropriate' hash is generated
- Solution-checking easy
- Other nodes approve a block by trying to find the next block
- Block-difficulty adjusts every 2016 blocks (14 days)
- Reward of 25 btc for a block *atm.* (max. $21 * 10^6$ BTC)
- Block-reward halves every 210,000 blocks (4years)

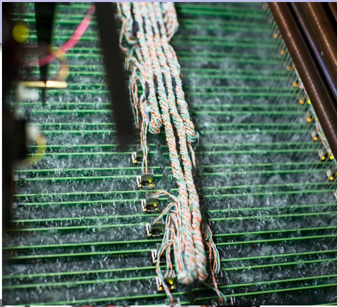


Difficulty: 000	
Message	**Hash**
<Hash of last block>1	010101101
<Hash of last block>2	110101011
…..	...
<Hash of last block>n	010011010
<Hash of last block>n+1	000101101

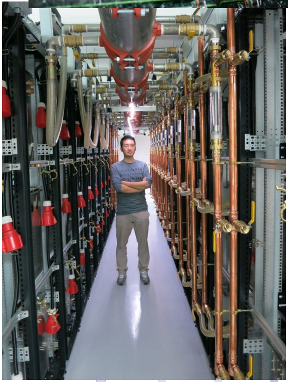
Present state of mining

- In the beginning it was all only CPUs
- Then came GPU-mining
- Then came FPGA-mining
- Then came ASIC miners
- Upcoming: Rent ASIC-miners
- ... next Intel, Nvidida & AMD?

Present state of mining

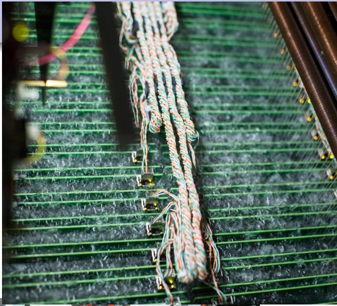


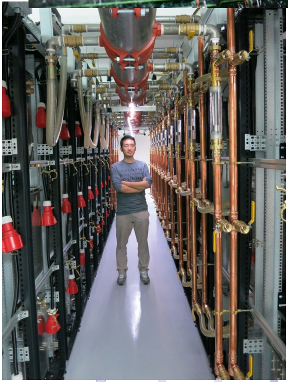
- In the beginning it was all only CPUs
- Then came GPU-mining
- Then came FPGA-mining
- Then came ASIC miners
- Upcoming: Rent ASIC-miners
- ... next Intel, Nvidida & AMD?



Present state of mining

- In the beginning it was all only CPUs
- Then came GPU-mining
- Then came FPGA-mining
- Then came ASIC miners
- Upcoming: Rent ASIC-miners
- ... next Intel, Nvidida & AMD?



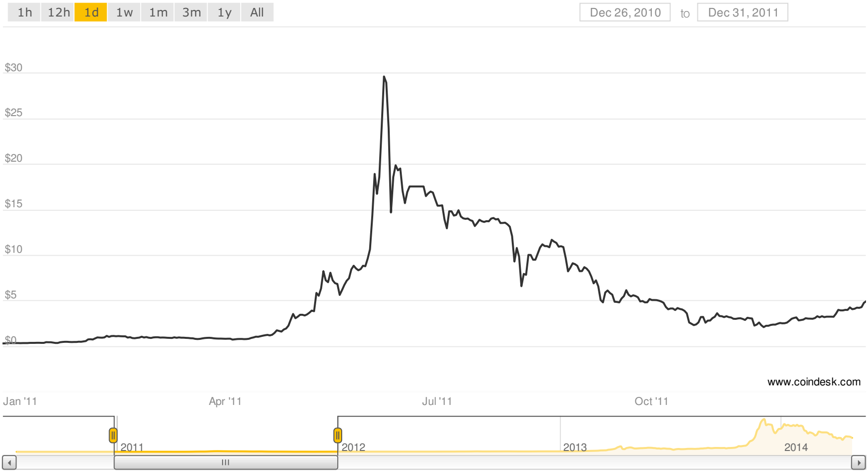


Present state of bitcoins

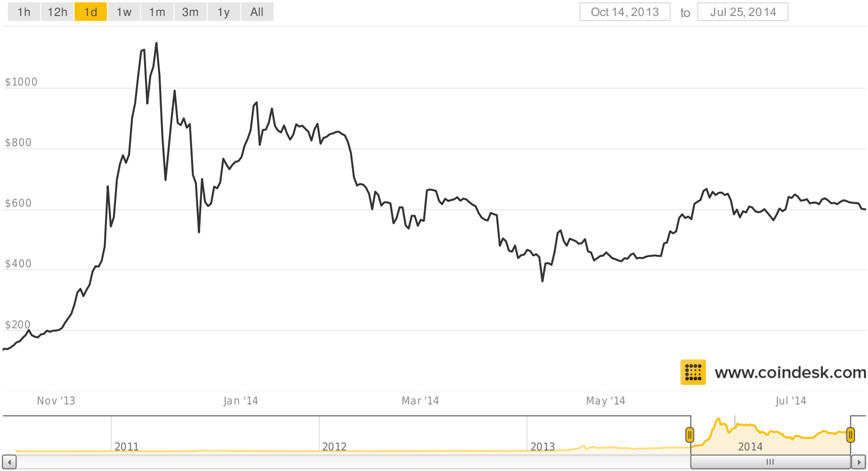
	01-03-2012	16-12-2013	29-04-204
Total BTC amount	8,461,000	12,125,000	12,702,000
Price USD	$4.9	$794	$451
Tradingvolume (30d)	$6,769,500	$101,632,000	$ 815,761,000
Hashrate [THash/ExaFLOPS]	11/0.137	7,175/91	56,572/718

	Today!
Total BTC amount	13,060,000
Price USD	$597
Tradingvolume (30d)	$966,508,000
Hashrate [THash/ExaFLOPS]	134,454/1667

Oh, the bubbles! I



Oh, the bubbles! II



Recent notable events

- Dell ($56.94 billion), Dish Network ($13.9 billion) and NewEgg($2.5billion) accept bitcoin
- Mt.Gox filed for bankruptcy
- $100 million VC in 2013, $64.2 million so far in 2014 ($200 million estimated)
- 35+ Bitcoin atms 10+ countries, debit cards etc.
- Variety of altcoins more or less departed from bitcoin protocol
- Silk Road takedown
- Attention of regulators
- China!

Myth, facts and in between

- **Myth**: Bitcoins is anonymous, impossible to regulate!
- **Myth**: Criminal heaven
- **Myth**: It's a Ponzi-scheme, TULIPCRAZE!!11one
- **Objection** :Bitcoin is not real money, it has no **real** value compared to normal currency

Myth, facts and in between

- **Myth**: Bitcoins is anonymous, impossible to regulate!
  Fact: It's complicated!
  Much more privacy-oriented than other electronical money
- **Myth**: Criminal heaven
- **Myth**: It's a Ponzi-scheme, TULIPCRAZE!!11one
- **Objection** :Bitcoin is not real money, it has no **real** value compared to normal currency

Myth, facts and in between

- **Myth**: Bitcoins is anonymous, impossible to regulate!
  Fact: It's complicated!
  Much more privacy-oriented than other electronical money
- **Myth**: Criminal heaven
- **Myth**: It's a Ponzi-scheme, TULIPCRAZE!!11one
- **Objection** :Bitcoin is not real money, it has no **real** value compared to normal currency

Myth, facts and in between

- **Myth**: Bitcoins is anonymous, impossible to regulate!
  Fact: It's complicated!
  Much more privacy-oriented than other electronical money
- **Myth**: Criminal heaven
  Fact: They're in heaven already: Estimated $10 trillion dollar black market economoy.
  What about cash?
  Bitcoin can survive a ban, bitcoins only for criminals?
- **Myth**: It's a Ponzi-scheme, TULIPCRAZE!!11one

- **Objection** :Bitcoin is not real money, it has no **real** value compared to normal currency

Myth, facts and in between

- **Myth**: Bitcoins is anonymous, impossible to regulate!
  Fact: It's complicated!
  Much more privacy-oriented than other electronical money
- **Myth**: Criminal heaven
  Fact: They're in heaven already: Estimated $10 trillion dollar black market economoy.
  What about cash?
  Bitcoin can survive a ban, bitcoins only for criminals?
- **Myth**: It's a Ponzi-scheme, TULIPCRAZE!!11one
- **Objection** :Bitcoin is not real money, it has no **real** value compared to normal currency

Myth, facts and in between

- **Myth**: Bitcoins is anonymous, impossible to regulate!
  Fact: It's complicated!
  Much more privacy-oriented than other electronical money
- **Myth**: Criminal heaven
  Fact: They're in heaven already: Estimated $10 trillion dollar black market economoy.
  What about cash?
  Bitcoin can survive a ban, bitcoins only for criminals?
- **Myth**: It's a Ponzi-scheme, TULIPCRAZE!!11one
  Fact: Not **store of value** but **medium of exchange**: buy and spend quickly
  Bitcoin protocol will not be visible to the masses. Liquidity problems is annnoying at worst, not devastating
- **Objection** :Bitcoin is not real money, it has no **real** value compared to normal currency

Myth, facts and in between

- **Myth**: Bitcoins is anonymous, impossible to regulate!
  Fact: It's complicated!
  Much more privacy-oriented than other electronical money
- **Myth**: Criminal heaven
  Fact: They're in heaven already: Estimated $10 trillion dollar black market economoy.
  What about cash?
  Bitcoin can survive a ban, bitcoins only for criminals?
- **Myth**: It's a Ponzi-scheme, TULIPCRAZE!!11one
  Fact: Not **store of value** but **medium of exchange**: buy and spend quickly
  Bitcoin protocol will not be visible to the masses. Liquidity problems is annnoying at worst, not devastating
- **Objection** :Bitcoin is not real money, it has no **real** value compared to normal currency

Myth, facts and in between

- **Myth**: Bitcoins is anonymous, impossible to regulate!
  Fact: It's complicated!
  Much more privacy-oriented than other electronical money
- **Myth**: Criminal heaven
  Fact: They're in heaven already: Estimated $10 trillion dollar black market economoy.
  What about cash?
  Bitcoin can survive a ban, bitcoins only for criminals?
- **Myth**: It's a Ponzi-scheme, TULIPCRAZE!!11one
  Fact: Not **store of value** but **medium of exchange**: buy and spend quickly
  Bitcoin protocol will not be visible to the masses. Liquidity problems is annnoying at worst, not devastating
- **Objection** :Bitcoin is not real money, it has no **real** value compared to normal currency
  Answer It has value because it is generative, fast, global, decentralized & secure.
  Value only needs to be > 0

Myth, facts and in between

- **Myth**: Bitcoins is anonymous, impossible to regulate!
  Fact: It's complicated!
  Much more privacy-oriented than other electronical money
- **Myth**: Criminal heaven
  Fact: They're in heaven already: Estimated $10 trillion dollar black market economoy.
  What about cash?
  Bitcoin can survive a ban, bitcoins only for criminals?
- **Myth**: It's a Ponzi-scheme, TULIPCRAZE!!11one
  Fact: Not **store of value** but **medium of exchange**: buy and spend quickly
  Bitcoin protocol will not be visible to the masses. Liquidity problems is annnoying at worst, not devastating
- **Objection** :Bitcoin is not real money, it has no **real** value compared to normal currency
  Answer It has value because it is generative, fast, global, decentralized & secure.
  Value only needs to be > 0

...the future of bitcoins is unkown since the technology is so new.

Also unkown to economists!

TODO for the bitcoin community

- **Improve code in protocol layer**
- Enhance privacy in the protocol layer
- Enhance security in content layer (seems like first lessons learned)
- Enhance usability: For laymen, merchants etc. MUCH have happened!
- Improve legal status (Not a currency in DK)

Perspectives on bitcoins

- **Generative** technology that ’lowers the playing field’: Everybody can innovate!
- Threatens existing payment processors
- Improves privacy in present the present mass-surveillance world
- Potential to catalyze peer-production of e.g. knowledge and culture

Perspectives on bitcoins

- **Generative** technology that 'lowers the playing field': Everybody can innovate!
- Threatens existing payment processors
- Improves privacy in present the present mass-surveillance world
- Potential to catalyze peer-production of e.g. knowledge and culture

Perspectives on bitcoins

- **Generative** technology that 'lowers the playing field': Everybody can innovate!
- Threatens existing payment processors
- Improves privacy in present the present mass-surveillance world
- Potential to catalyze peer-production of e.g. knowledge and culture

Perspectives on bitcoins

- **Generative** technology that ’lowers the playing field’: Everybody can innovate!
- Threatens existing payment processors
- Improves privacy in present the present mass-surveillance world
- Potential to catalyze peer-production of e.g. knowledge and culture

Perspectives on bitcoins

- **Generative** technology that ’lowers the playing field’: Everybody can innovate!
- Threatens existing payment processors
- Improves privacy in present the present mass-surveillance world
- Potential to catalyze peer-production of e.g. knowledge and culture

Catalysing the ’networked information economy’ ?

Thank you for your attention!
https://stripe.com/blog/bitcoin-the-stripe-perspective