Introduction to Bitcoin

Stefan Dziembowski

University of Warsaw

The First Greater Tel Aviv Area Symposium, 13.11.2014

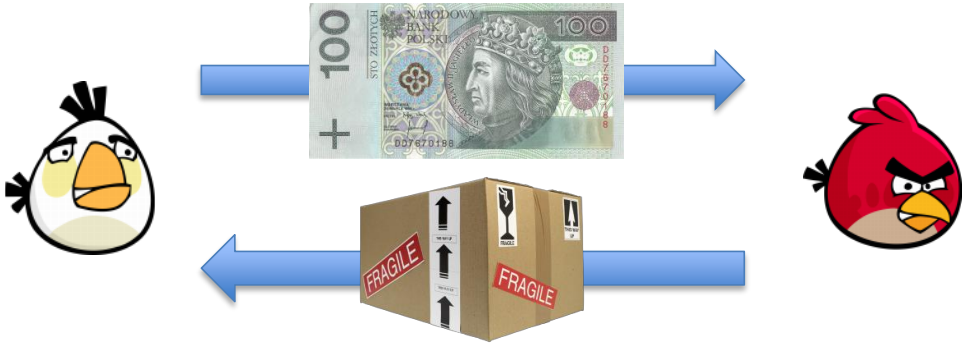
Outline

1. Introduction
2. Main design principles
3. Bitcoin's security?
4. Alternative ideas

Introduction

Digital vs. paper currencies

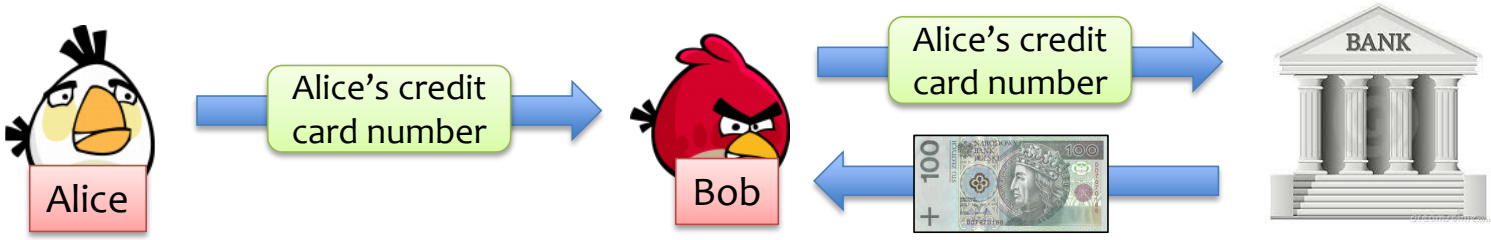
Paper:



Digital:

Very useful if  is also digital.

Traditional ways of paying “digitally”



PROBLEMS

1. **trusted server** for each transaction is needed (money doesn’t “circulate”),
2. high **transaction fees**,
3. **no anonymity**.

Bitcoin – a "digital analogue" of the paper money

A digital currency introduced by "Satoshi Nakamoto" in 2008.

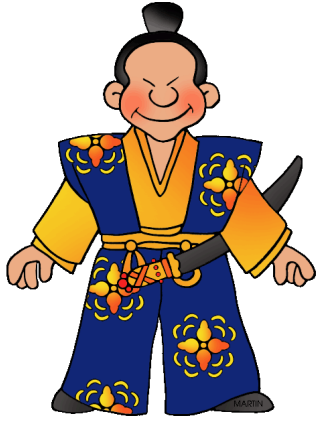
Based on the assumption that ``the majority of the computing power is honest".

currency unit: **Bitcoin (BTC) 1 BTC = 10^8 Satoshi**

as of 11.11.2014:

Market cap ≈ 4.9 billion USD

1 BTC ≈ 364 USD

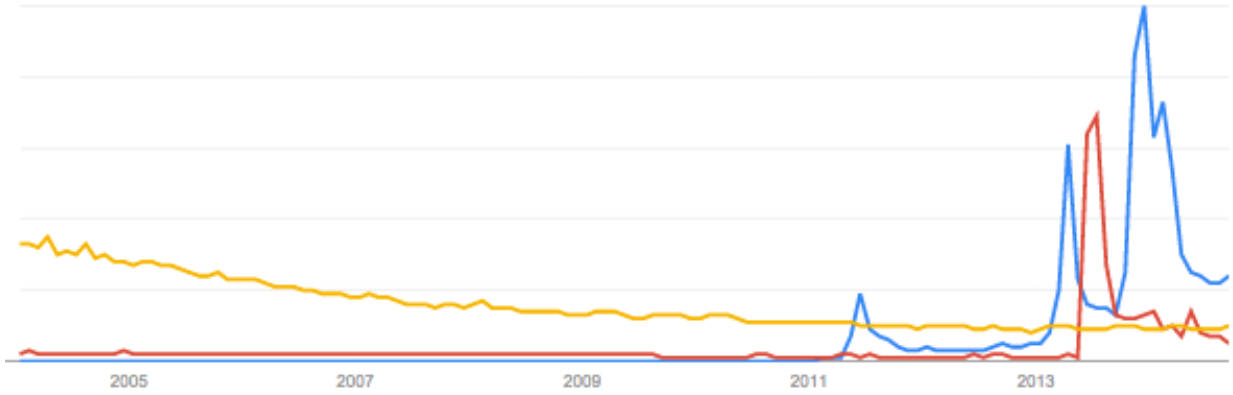


Probably one of the most discussed cryptographic technologies ever!

Topics

bitcoin	snowden	encryption
Search term	Search term	Search term

Interest over time



Bitcoin

in Bitcoin:

- no trusted server, money circulates
- low fees
- "pseudonymity"

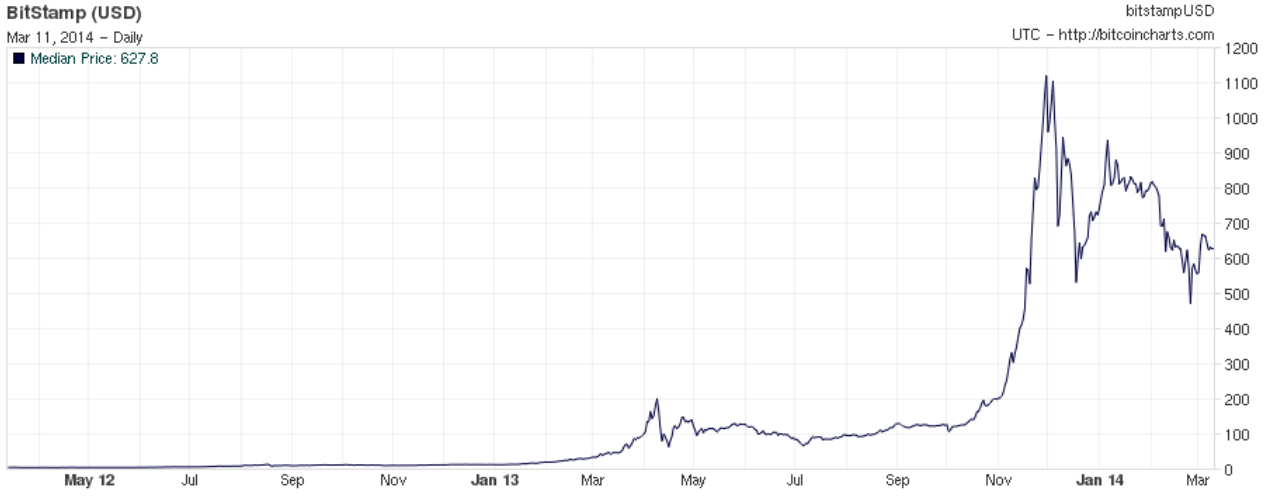
PROBLEMS WITH PREVIOUS APPROACHES

1. **trusted server** is needed (money doesn't "circulate"),
2. high **transaction fees,**
3. **no anonymity.**

“No trusted server”

nobody “**controls the money**”, and therefore:

- The amount of money that will ever be “printer” is fixed (to around 21 mln BTC) → **no inflation**
- The **exchange rate fluctuates**:



Really “no trusted server”?

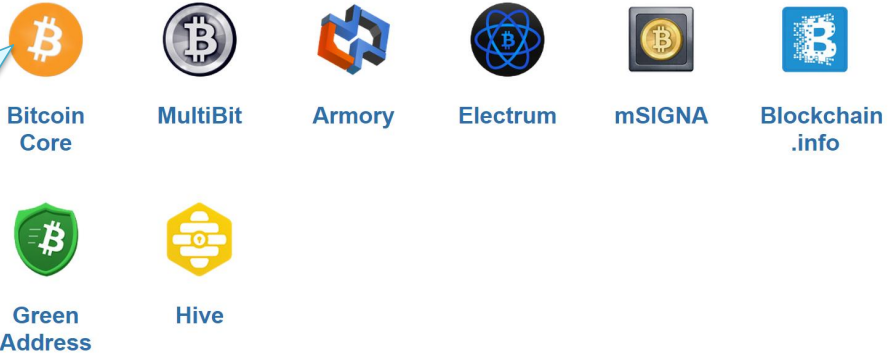
The client software is written by people who are in power to change the system.

For example, this is the list of “desktop clients”:

The most popular client.

(open source)

The developers: Wladimir J. van der Laan, Gavin Andresen, Jeff Garzi, Gregory Maxwell, Pieter Wuille



Bitcoin ≈ “real money”?

Bitcoin value comes from the fact that:

“people expect that other people will accept it in the future.”

enthusiasts:

It’s like all the other currencies

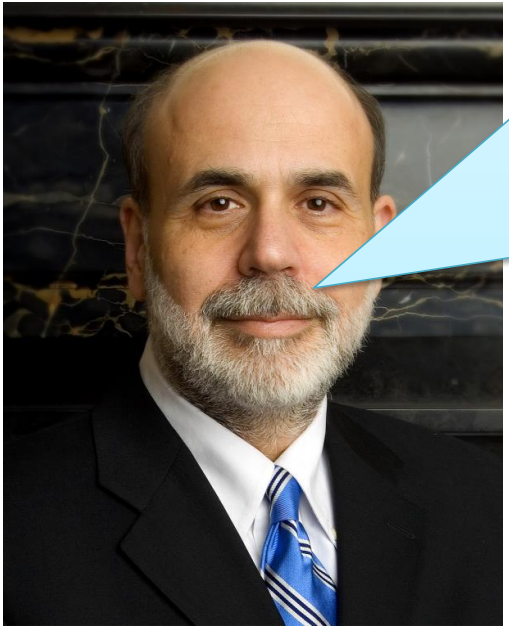
sceptics:

It’s a Ponzi scheme

P. Krugman

A. Greenspan

Some economists are more positive



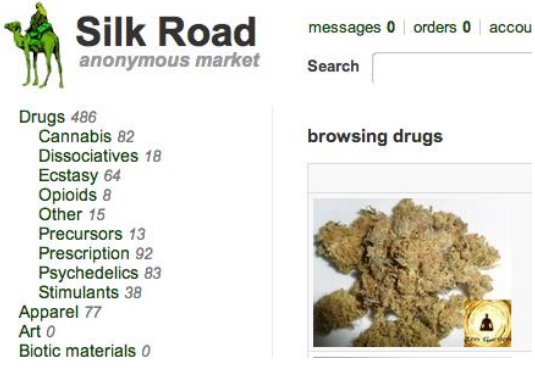
Ben Bernanke

While these types of innovations **may pose risks** related to law enforcement and supervisory matters, there are also areas in which they may hold long-term promise, particularly if the innovations **promote a faster, more secure and more efficient payment system**.

Why did Bitcoin become so popular (1/2)?

- Ideological reasons (crypto-anarchism).

- Good timing (in 2008 the "quantitative easing" in the US started).



- Seeming anonymity (anonymous enough for trading illegal goods?)

Why did Bitcoin become so popular (2/2)?

- Low transaction fees.
- Hype?
- Very popular in some non-democratic countries (until the government forbids to use it).

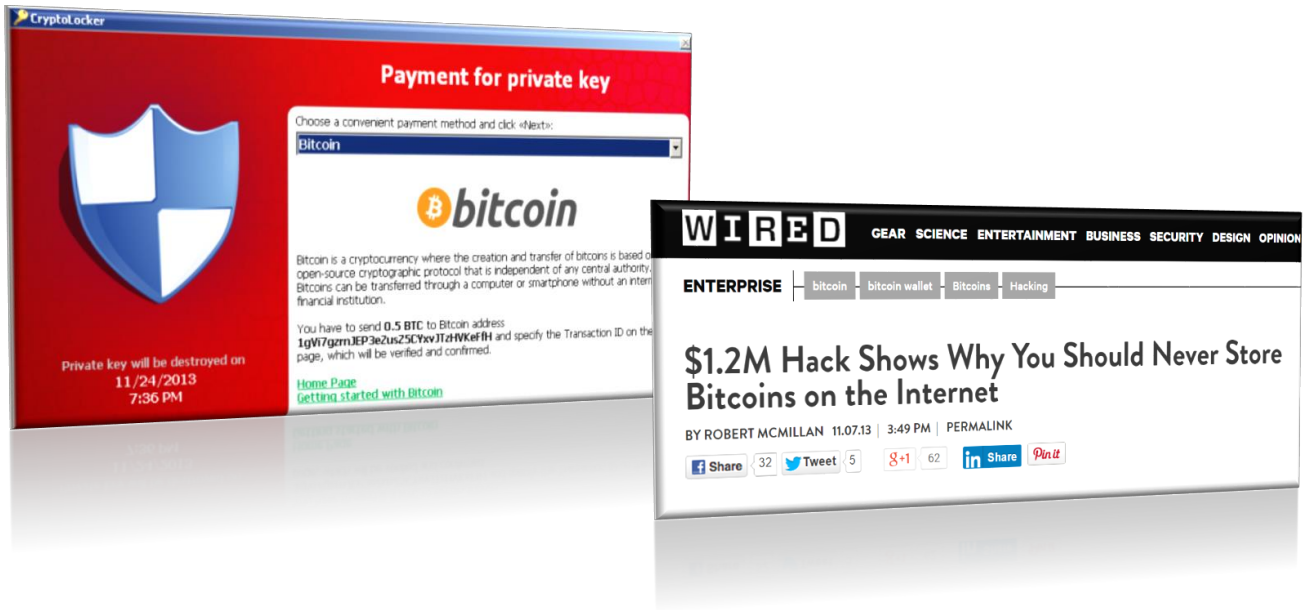
Downsides of decentralization (1/2)

There are no “regulators”…

MtGox (handling **70%** of all Bitcoin transactions) shut down on **Feb 2014** reporting 850,000 bitcoins (≈ **450 million USD**) stolen.

Downsides of decentralization (2/2)

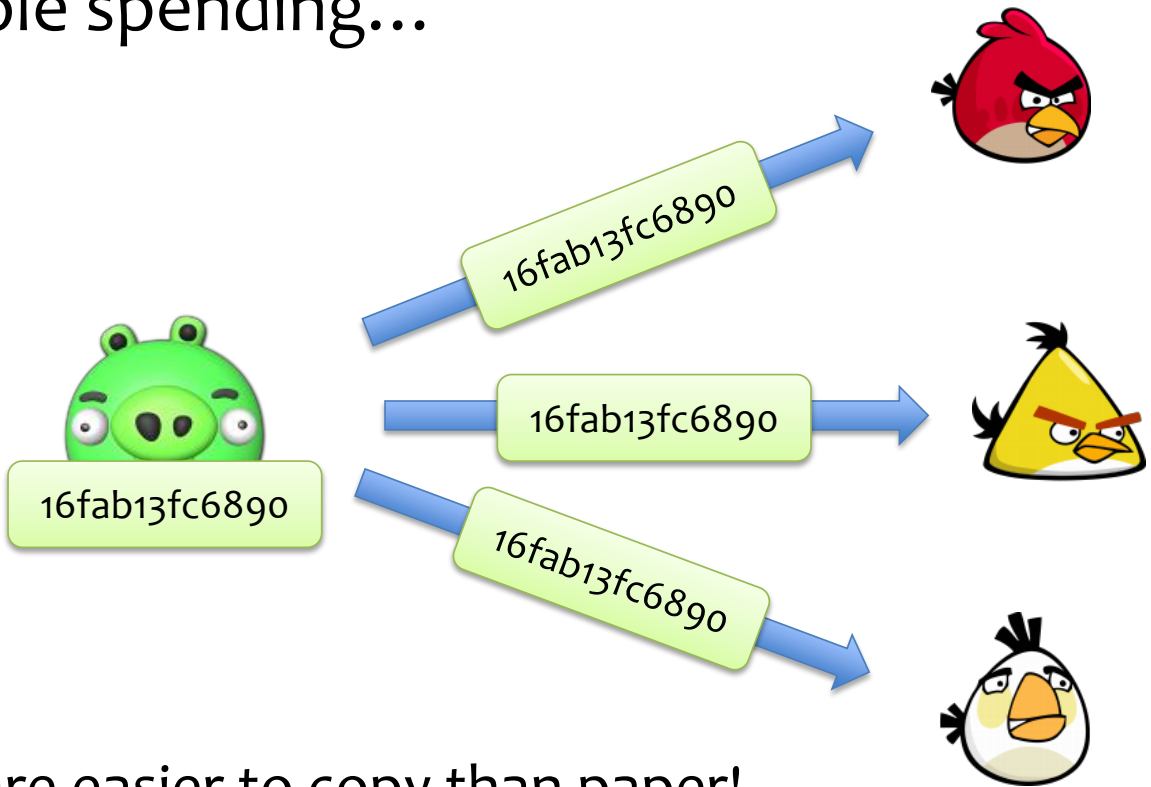
Nobody can reverse transactions, so finally **hackers have good reasons to break into personal computers.**



Main design principles

Main problem with the digital money

Double spending…



Bits are easier to copy than paper!

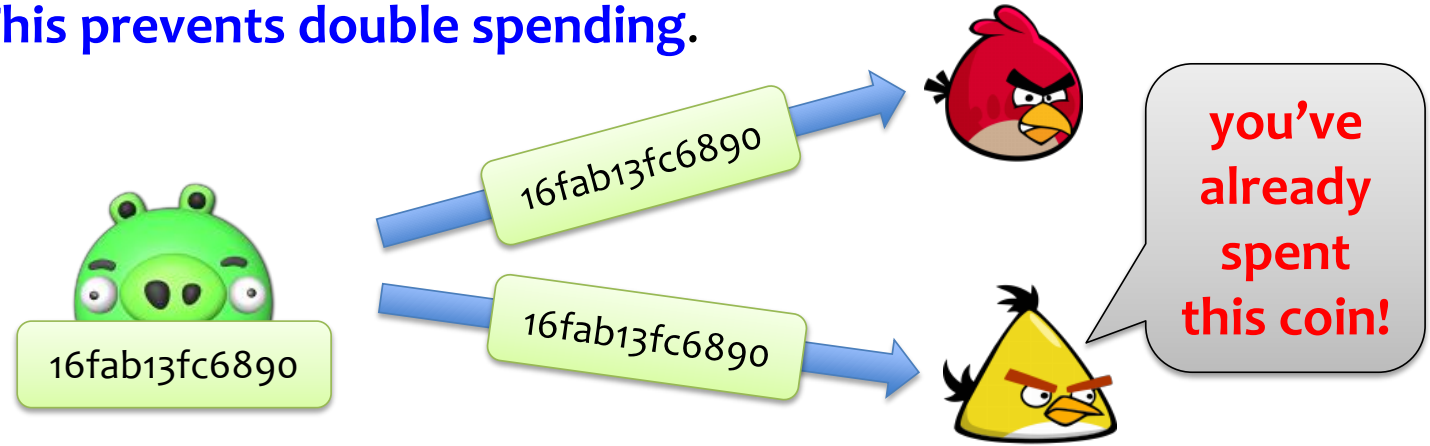
Bitcoin idea (simplified):

The users emulate a **public trusted bulletin-board** containing a list of transactions.

A transaction is of a form:

"User $\mathbf{P_1}$ transfers a coin #16fab13fc6890 to user $\mathbf{P_2}$"

This prevents double spending.

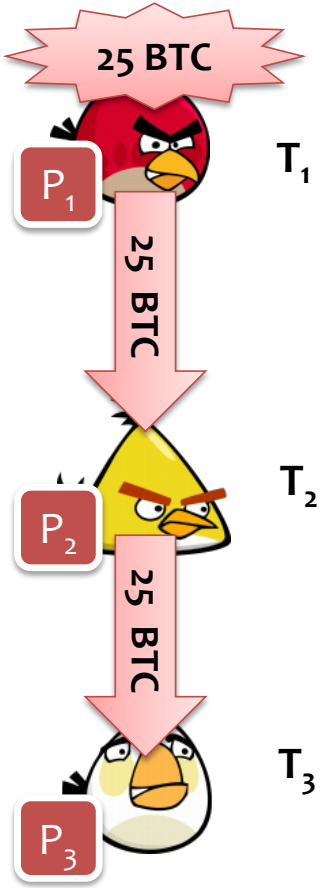


User identification

We use the digital signature schemes.

The users are identified by their public keys.

Transaction syntax – simplified view



in the "mining process"

We say that **T_3 redeems T_2**

T_1 = (User P_1 creates **25 BTC**)

$[T_2]$

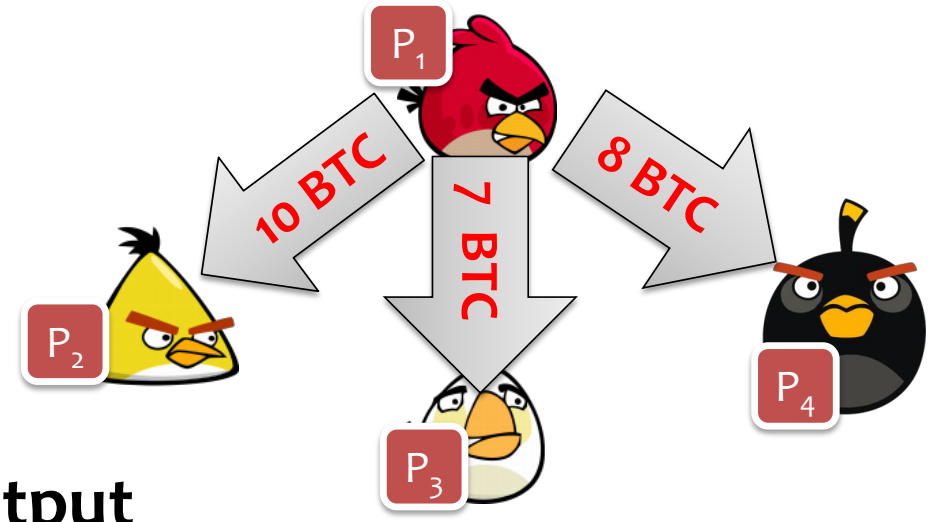
"value of T_2"

T_2 = (User P_1 sends **25 BTC** from T_1 to P_2 **signature of P_1 on $[T_2]$**)

$[T_3]$

T_3 = (User P_2 sends **25 BTC** from T_2 to P_3 **signature of P_2 on $[T_3]$**)

How to “divide money”?

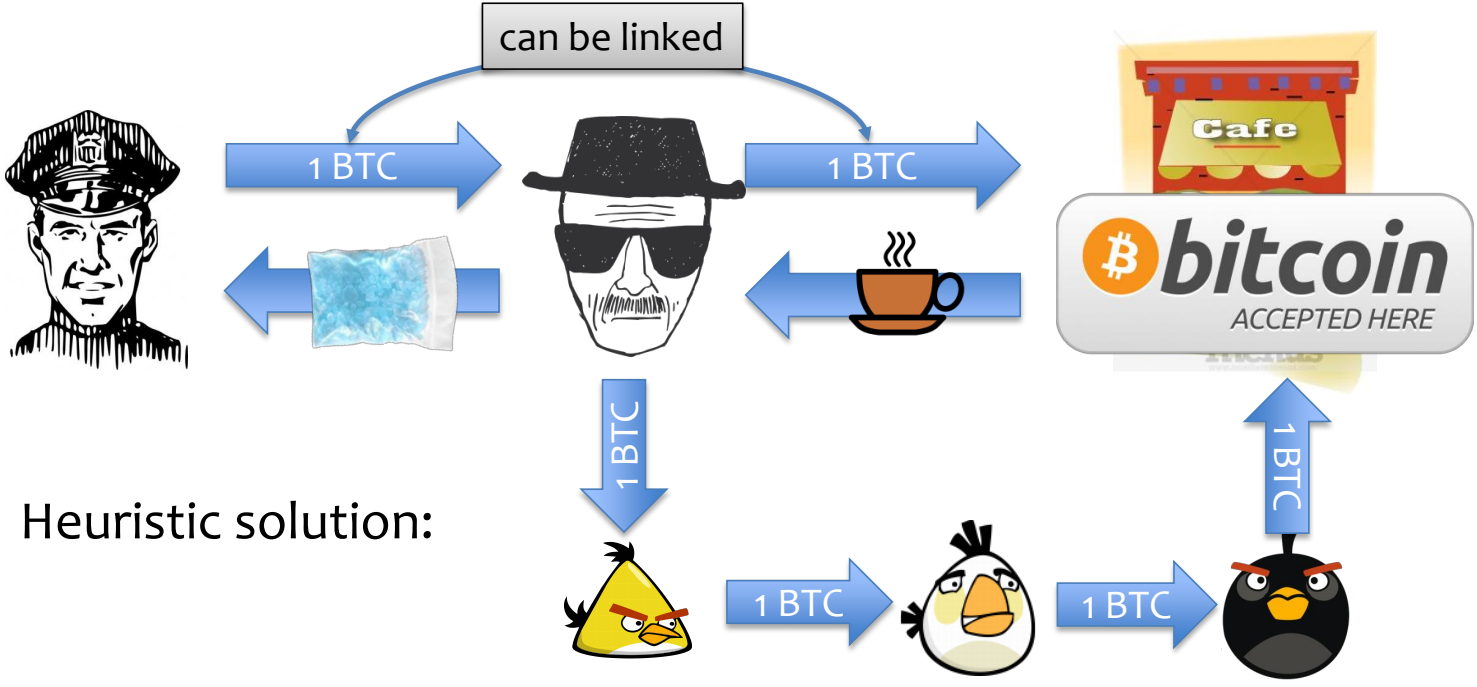


Multi-output transactions:

$[T_2]$

$T_2 =$ (User P_1 sends **10 BTC** from T_1 to user P_2, User P_1 sends **7 BTC** from T_1 to user P_3, User P_1 sends **8 BTC** from T_1 to user P_4) **signature of P_1 on $[T_2]$**

Anonymity?

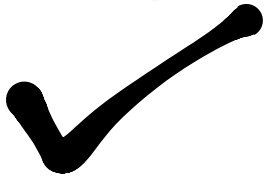


Heuristic solution:

Can sometimes be de-anonymized:
[Meiklejohn et al. **A fistful of bitcoins: characterizing payments among men with no names,** 2013]

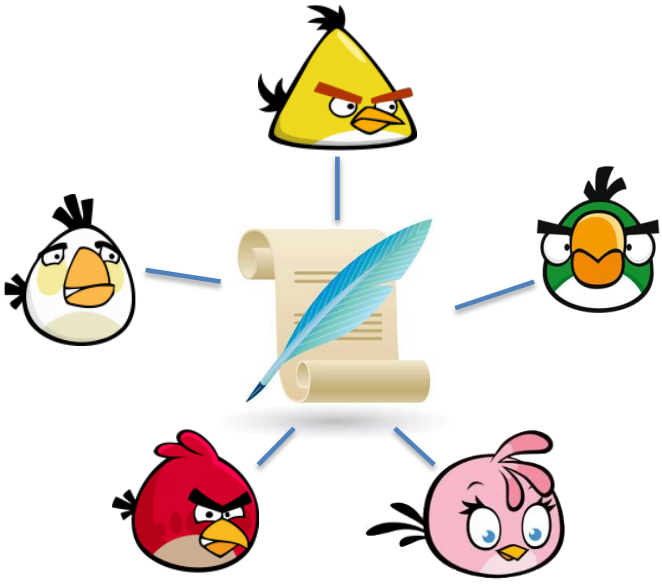
What needs to be discussed

1. How is the **trusted bulletin-board** maintained?
2. How are the users identified?
3. Where does the money come from?
4. What is the syntax of the transactions?

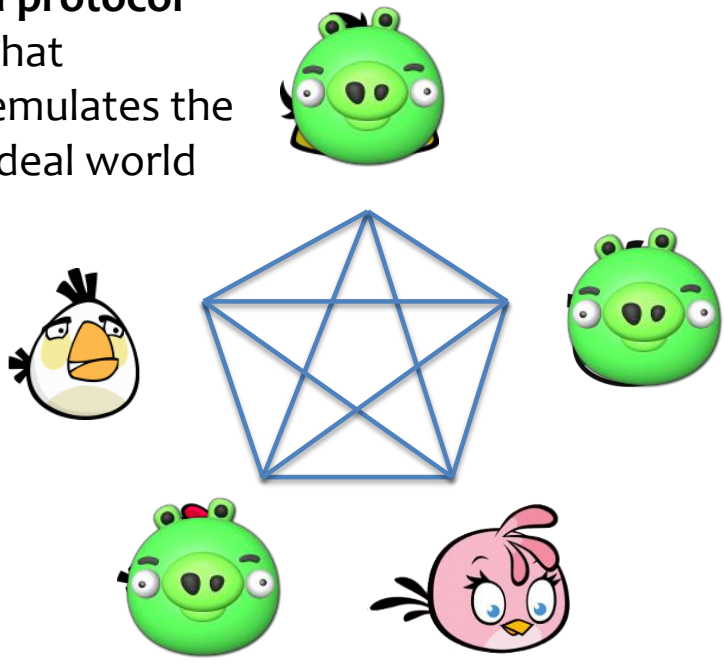


Trusted bulletin-board emulation

the "ideal" world



a **protocol** that emulates the ideal world



Main difficulty: Some parties can cheat.

Classical result: simulation is possible if the "majority is honest".

For example for **5** players we can tolerate at most **2** "cheaters".

Problem

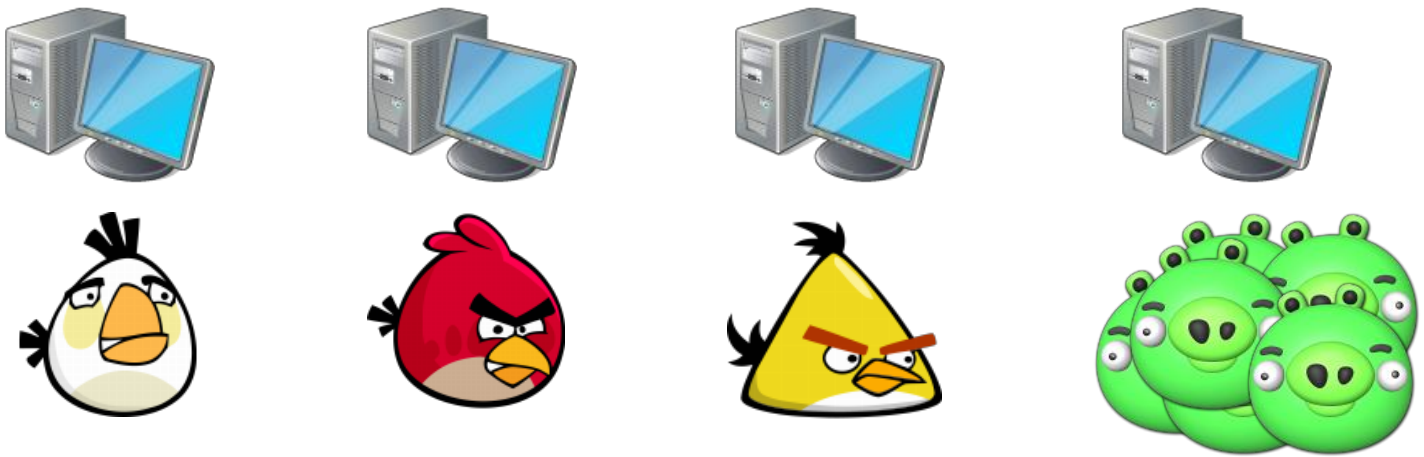
How to define "**majority**" in
a situation where
everybody can join the network?

The Bitcoin solution

Define the “majority” as

the majority of the computing power

Now creating multiple identities does not help!



How is this verified?

Main idea:

- use **Proofs of Work**
- **incentivize** honest users to constantly participate in the process

The honest users can use their **idle CPU cycles**.

Nowadays: often done on **dedicated hardware**.

A simple hash-based PoW

H -- a hash function whose computation takes time **TIME(H)**

random **x**

Prover
finds **s** such that
H(s,x) starts with **n** zeros (in binary)

s

Verifier
checks if
H(s,x) starts with **n** zeros

salt | "hardness parameter

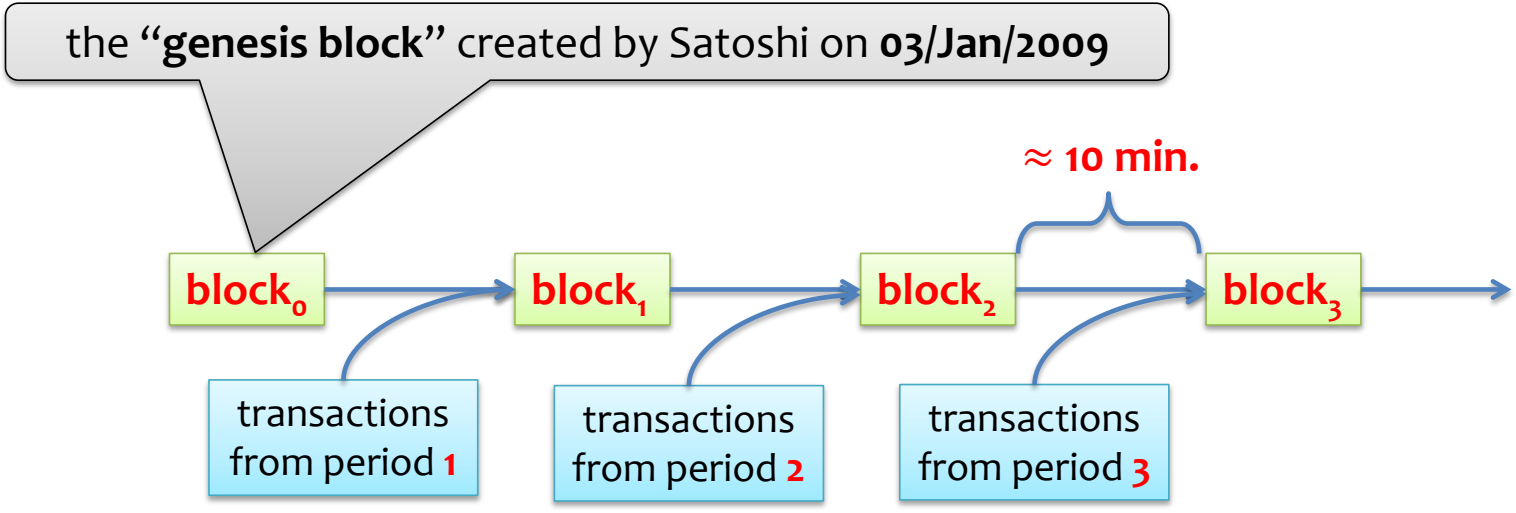
takes time $2^n \cdot$ **TIME(H)**

takes time **TIME(H)**

Main idea

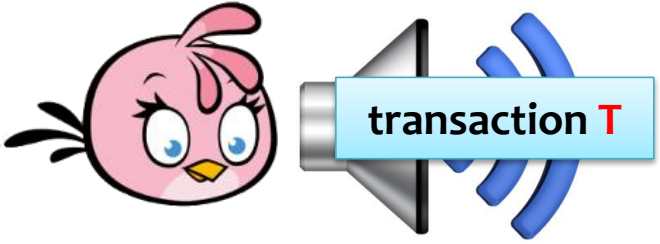
The users participating in the scheme are called the "miners".

They maintain a chain of blocks:



How to post on the board

Just broadcast (over the internet) your transaction to the miners.



And hope they will **add it to the next block.**

the miners are incentivized to do it.

Main principles

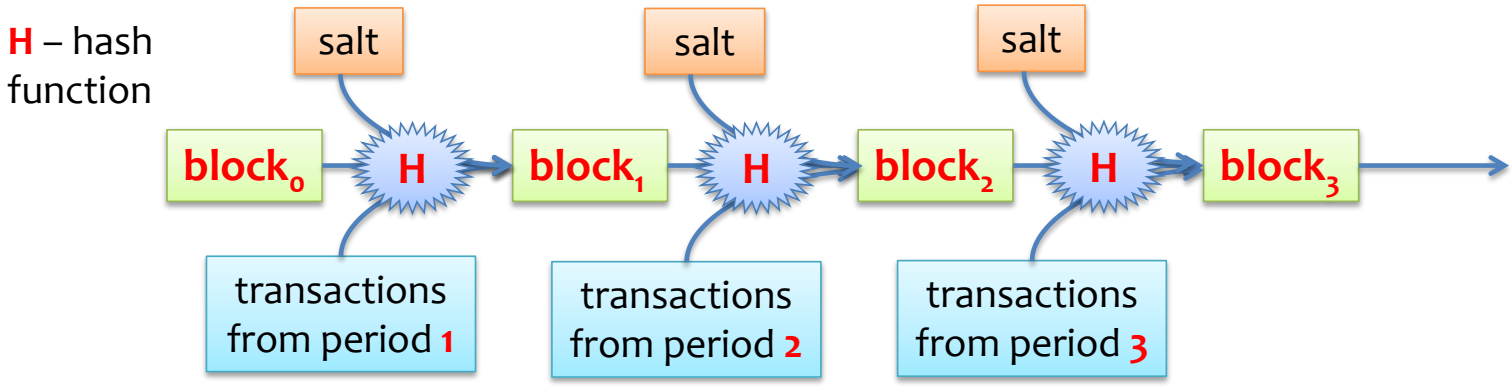
1. It is **computationally hard** to extend the chain.

2. Once a miner finds an extension he **broadcasts it to everybody**.

3. The users will always accept "**the longest chain**" as the valid one.

the system incentivizes them to do it

How are the PoWs used?



Main idea: to extend it one needs to find **salt** such that

H(salt, block$_i$,transactions) starts with some number **n** of **zeros**

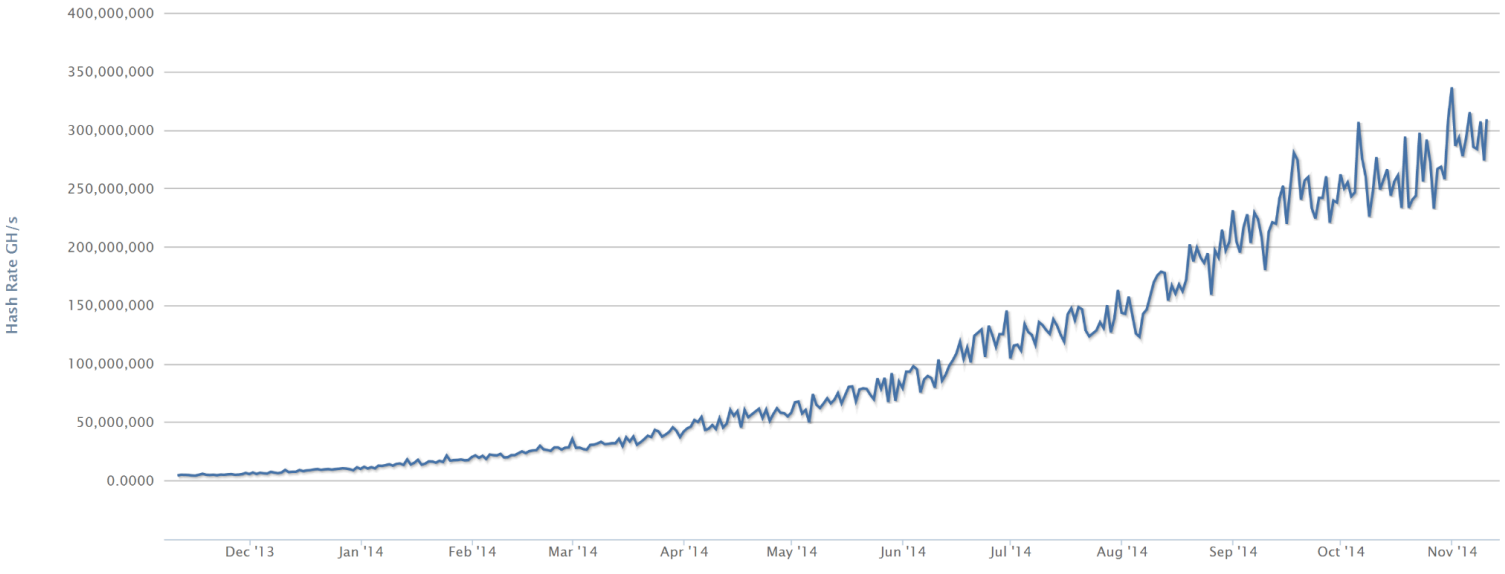
The hardness parameter is periodically changed

- The computing power of the miners **changes**.
- The miners should generate the new block **each 10 minutes** (on average).
- Therefore the hardness parameter **is periodically adjusted** to the mining power
- This happens once each **2016 blocks**.
- For example the block generated on 2014-03-17 18:52:10 looked like this:

```
000000000000000006d8733e03fa9f5e5
2ec912fa82c9adfed09fbca9563cb4ce
```

“Hashrate” = number of hashes computed per second

total hashrate:



Note:

Nov 05 2014 : 283,494,086 GH/s

Nov 05 2013 : 3,657,378 GH/s

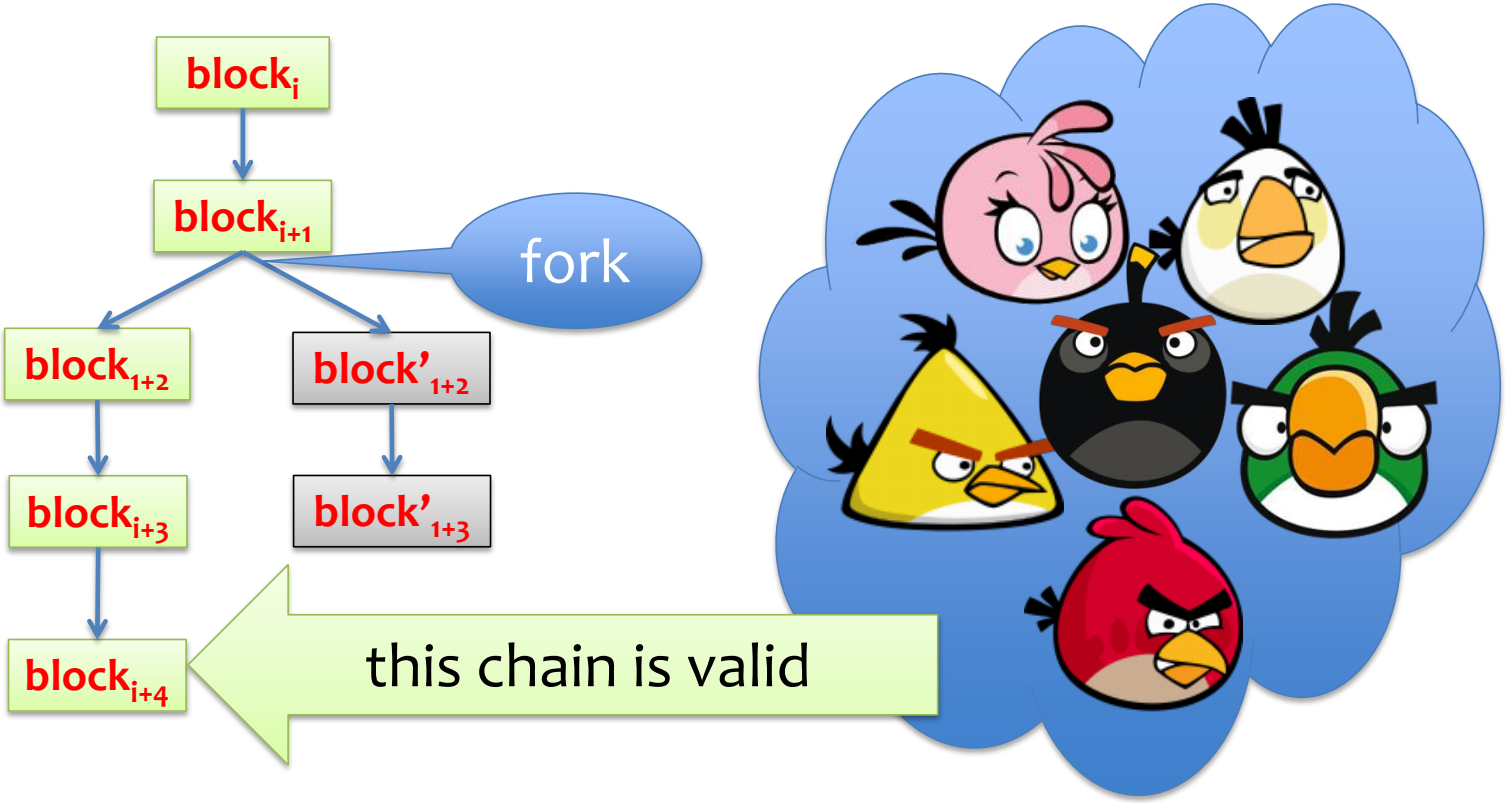
$\approx 2^{58}$ hash / second

How it looks in real life

291061	109adb5479...	2014-03-17 18:49:11
291060	418788ad79...	2014-03-17 18:44:35
291059	675b86077a...	2014-03-17 18:34:59
291058	ebce6837fa...	2014-03-17 18:29:34
291057	ee7453e6d0...	2014-03-17 17:47:28
291056	d2c08a5ee9...	2014-03-17 17:26:21

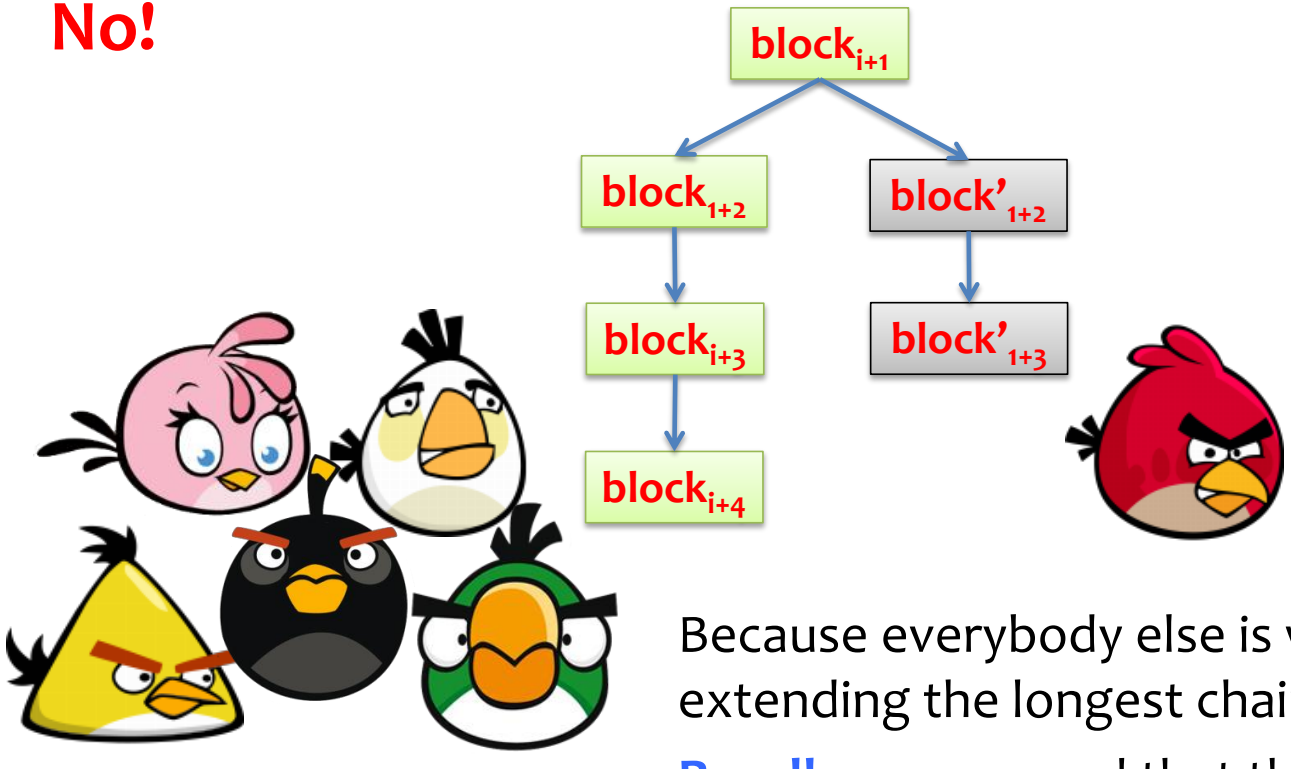
What if there is a “fork”?

The “**longest**” chain counts.



Does it make sense to "work" on a shorter chain?

No!



Because everybody else is working on extending the longest chain.

Recall: we assumed that the majority follows the protocol.

How are the miners incentivized to participate in this game?

Short answer: they are paid (in Bitcoins) for this.

We will discuss it in detail later…

What needs to be discussed

1. How is the **trusted bulletin-board** maintained?
2. How are the users identified?
3. Where does the money come from?
4. What is the syntax of the transactions?

Where does the money come from?

A miner who finds a new block gets a "reward" in **BTC**:

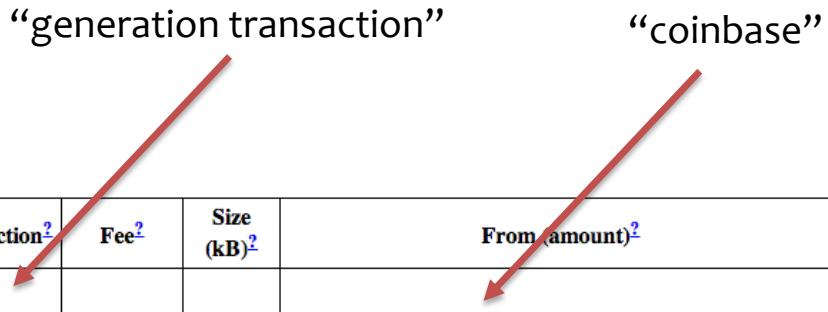
≈ 4 years

- for the first **210,000** blocks: **50 BTC**
- for the next **210,000** blocks: **25 BTC** ← current reward
- for the next **210,000** blocks: **12.5 BTC**,

and so on…

Note: **$210{,}000 \cdot (50 + 25 + 12.5 + \cdots) \rightarrow 21{,}000{,}000$**

This is how it looks in detail



Transaction[?]	Fee[?]	Size (kB)[?]	From (amount)[?]	To (amount)[?]
0ac34c9949...	0	0.173	Generation: 25 + 0.05974785 total fees	1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY: 25.05974785
2055f19a51...	0.0002	0.259	1Kpv8JEcWLhUqi4q8dnrwxiaZPKL4KUoeR: 179.9998	1HCukLGfkCfKCryXT73hj2SyVAC9kzRGkC: 105 15zBXYeXbtJ5xs48arouP7BHQu4AQ5xfZa: 74.9996
66815aff01...	0.001	0.258	1dice6DPtUMBpWgv8i4pG8HMjXv9qDJWN: 0.35	15GPjviasjMD8QJvMTs5qYsB8wtQLQGBtP: 0.00175 1HZHBnH2FbHNWieMxAh4xBPfgfuxW15UPt: 0.34725

More details

Each block contains a transaction that **transfers the reward** to the miner.

Advantages:

1. It provides **incentives** to be a miner.
2. It also makes the miners interested in **broadcasting new block** asap.

this view was challenged in a recent paper:
Ittay Eyal, Emin Gun Sirer
Majority is not Enough: Bitcoin Mining is Vulnerable
(we will discuss it later)

Bitcoin’s security?

Possible attack goals

- **double spending**,
- get **more money from mining** than you should,
- "**short selling**" – bet that the price of BTC will drop and then destroy the system (to make the price of BTC go to zero),
- someone (government?) interested in **shutting Bitcoin down**…

Note: this can be done e.g. by a spectacular fork that lasts just for a few hours…

What we do (not) know about Bitcoin's security?

1. Technical errors 
2. Features/problems
3. Conceptual errors
4. Potential threats

Some notable cases of **programming errors**

- a block *74638* (**Aug 2010**) contained a transaction with **two outputs summing to over 184 billion BTC** – this was because of an **integer overflow** in Bitcoin software

  (solved by a software update and a "manual fork")
  one double spending observed (worth 10.000 USD).

- a **fork** at block *225430* (**March 2013**) caused by an **error in the software update** of Bitcoin Core
  (lasted 6 hours, solved by reverting to an older version of the software)

Moral: nothing can be really "completely distributed".
Sometimes human intervention is needed…

What we do (not) know about Bitcoin's security?

1. Technical errors
2. Features/problems 
3. Conceptual errors
4. Potential threats

Hardware mining

History of mining:

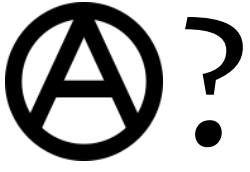
CPU → GPU → FPGA → ASIC

Bitcoin double SHA256 ASIC mining hardware

Product	Advertised Mhash/s	Mhash/J	Mhash/s/$	Watts	Price (USD)	Currently shipping
Achilles Labs AM-850 [1]	850,000	1478	1223	575	695	Discontinued
Achilles Labs AM-1700 [2]	1,700,000	1581	1553	1075	1095	Yes
Achilles Labs AM-3400 [3]	3,400,000	1581	1794	2150	1895	Yes
Achilles Labs AM-6000 [4]	6,000,000	1579	2073	3800	2895	Yes
AntMiner S1 [5]	180,000	500	800	360	299[6]	Discontinued
AntMiner S2 [7]	1,000,000	900	442	1100	2259	Discontinued
AntMiner S3 [8]	441,000	1300	1154	340	382[6]	Yes
AntMiner S4 [9]	2,000,000	1429	1429	1400	1400	Yes

Drawbacks of the hardware mining

1. Makes the whole process ``**non-democratic**''.



2. Easier to attack by **very powerful adversary**?

3. **Excludes some applications** (mining a as "micropayment").

Advantages of the hardware mining

- Security against **botnets**.
- Makes the miners interested in the **long-term stability** of the system.

How "long term"?

Remember that the total hashrate went up almost **100x** over the last year…

Mining pools

Miners create cartels called

the mining pools

This allows them to reduce the variance of their income.

Note:

The **total hashrate** of the Bitcoin system as of 5.11.2014

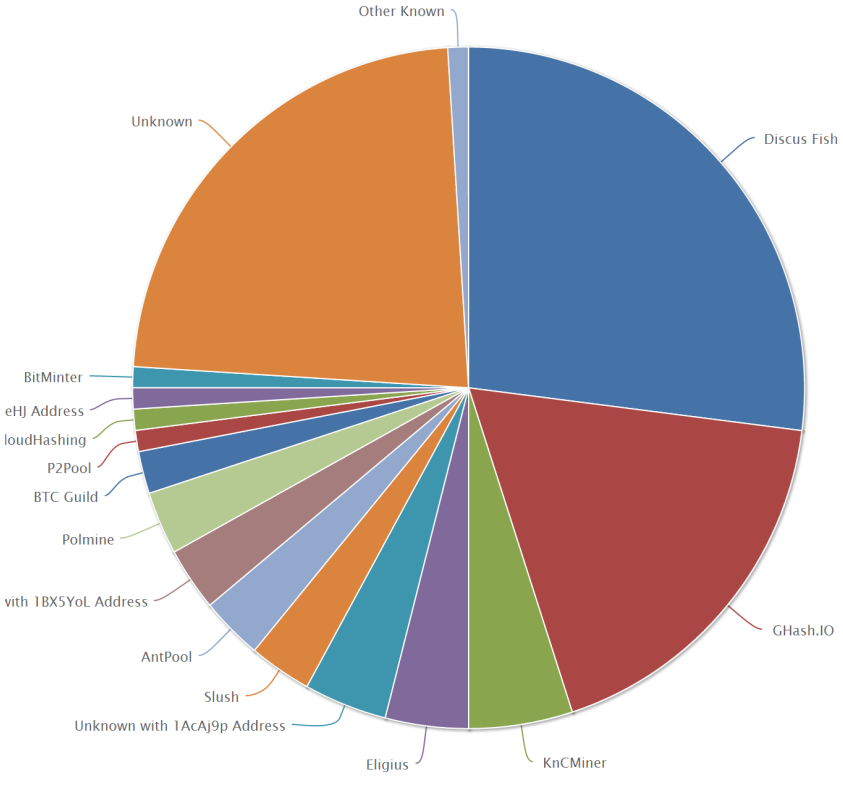
number of blocks in 1 year

$$\frac{283{,}494{,}086 \text{ GHash / s}}{1{,}700 \text{ GHash / s}} \approx 166{,}761 = 3.17 \cdot (365 \cdot 24 \cdot 6)$$

The **hashrate of the Achilles Labs AM-1700 miner** (1095 USD)

The user has to wait on average over **3 years** to mine a block
(**even if the difficulty does not increase**!)

Popular mining pools



The general picture

The mining pool is **operated centrally**.

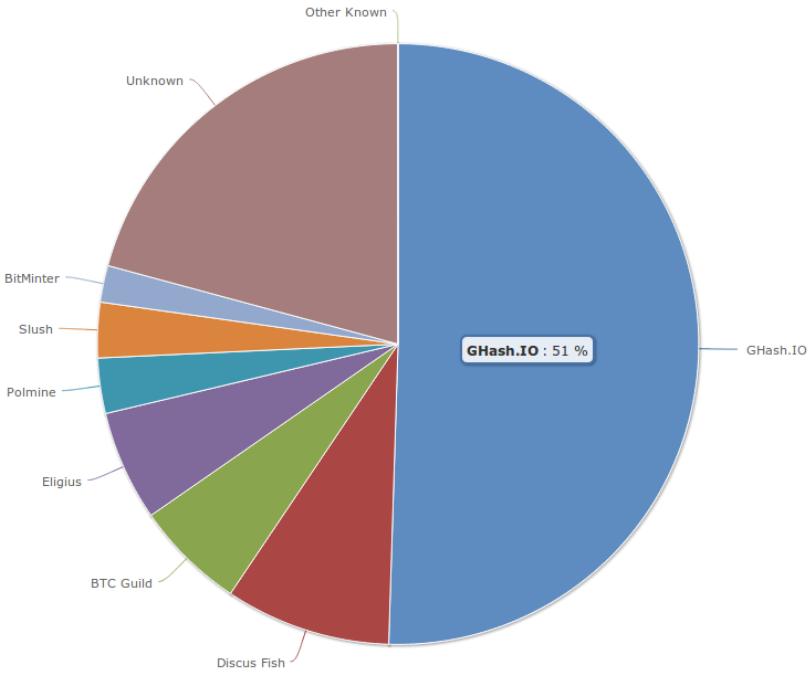
Some of the mining pools **charge fees for their services**.

Tricky part: how to prevent cheating by miners? How to reward the miners?

(see Meni Rosenfeld: *Analysis of Bitcoin Pooled Mining Reward Systems*)

June 2014

Ghash.io got > 50% of the total hashpower.



Then this percentage went down…

Observation

What we were promised:

“distributed currency independent from the central banks”

What we got (in June 2014):

“currency controlled by a single company”…

What is really our security assumption?

1. No cartel controls the majority of the computing power,
   or
2. The majority of participants is **100%** honest.

"As long as a **majority** of CPU power is controlled by nodes that are **not cooperating** to attack the network, they'll generate the longest chain and outpace attackers"

?

we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly **becomes computationally impractical for an attacker** to change **if honest nodes control a majority of CPU power**

In order for the Bitcoin to work we need a following (**strong**) assumption:

The majority behaves honestly even if it has incentives not to do so.

Is it realistic?

enthusiast:

Yes, since the majority is interested in maintaining the system

sceptics:

No, since this is not how capitalism works…
(e.g.: *tragedy of the commons*)

Another risk

Why not to **rent** the hashpower to perform the attack?

Conjecture

Maybe the only **reason why nobody broke Bitcoin yet** is that there is no good way to short-sell BTC?

What we do (not) know about Bitcoin's security?

1. Technical errors
2. Features/problems
3. Conceptual errors 
4. Potential threats

Selfish mining

Ittay Eyal, Emin Gun Sirer
Majority is not Enough: Bitcoin Mining is Vulnerable

basic idea: when you mine a new block keep it to yourself.

We explain it with some simplifying assumptions.

What happens when there is a fork?

Bitcoin specification:

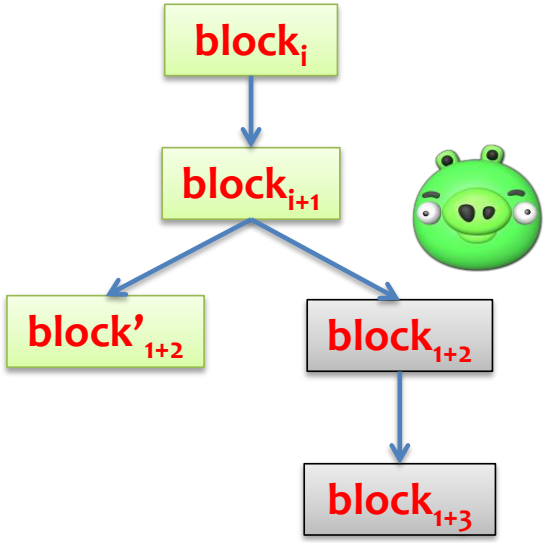
> "from two blocks of equal length mine on the first one that you received".

Assume that the adversary is always first (e.g. he puts a lot of "fake nodes" that act as sensors).

Assume that the adversary does not broadcast the new block that he found (and mines on it "privately").

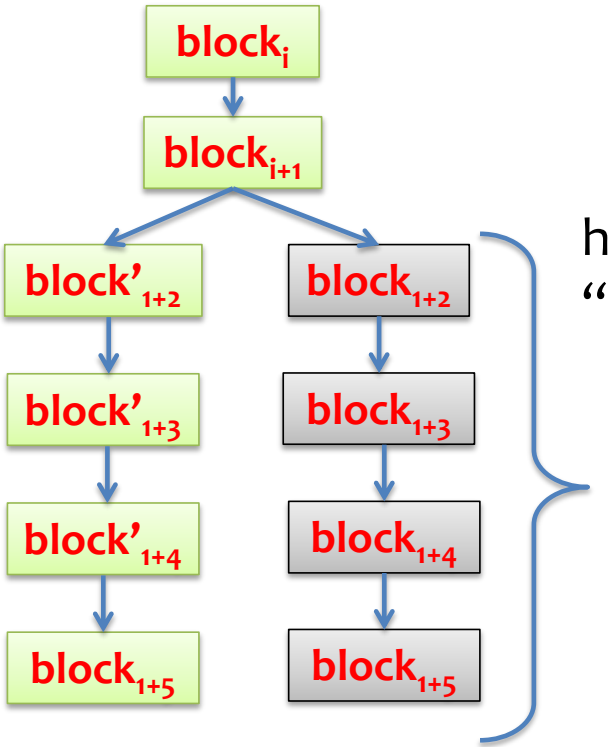
Two things can happen:

1. the **adversary** manages to extend his "private block chain" by one more block, or
2. the "**honest users**" manage to find an alternative extension.



In this case the **adversary** quickly publishes his block so he looses nothing

If the adversary is lucky then he obtains advantage over the honest miners.



he publishes his chain if the "public chain" equalizes with it

the reward for these blocks goes to him

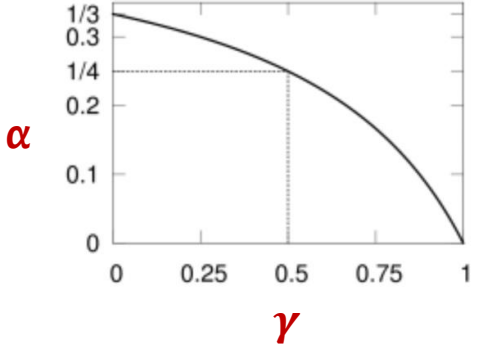
Note: this works even if the adversary has minority of computing power.

The assumption that "the adversary is always first" may look unrealistic.

Eyal and Sir show a modification of this strategy that works **without this assumption**.

- γ – **probability that the honest users choose adversary's block**
- α – **fraction of adversary's computing power**

Their strategy works as long as $\alpha > \frac{1-\gamma}{3-2\gamma}$



Another clever attack

Lear Bahack **Theoretical Bitcoin Attacks with less than Half of the Computational Power**

The "*Difficulty Raising Attack*" – exploits the way the difficulty is adjusted in Bitcoin.

What we do (not) know about Bitcoin's security?

1. Technical errors
2. Features/problems
3. Conceptual errors
4. Potential threats

Alternative ideas

Litecoin

Released in **Oct 2011** by Charles Lee.

Uses **scrypt** hash function introduced in:

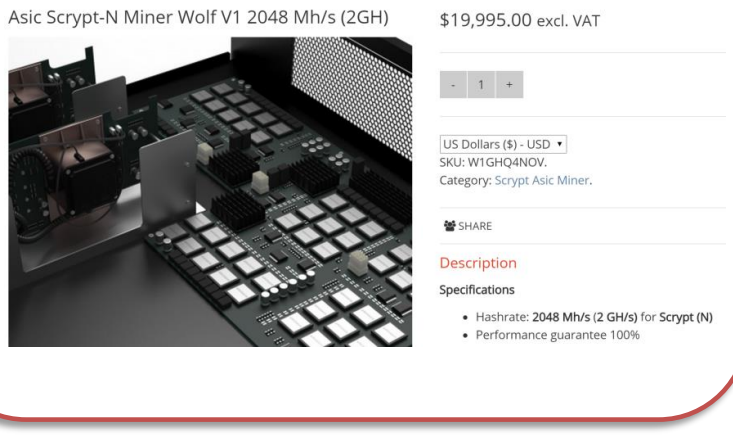
> Colin Percival, **Stronger Key Derivation via Sequential Memory-Hard Functions**, 2009.

Idea: **scrypt** is memory-hard, so there should be no hardware-mining.

as of 11.11.2014:

> **Market cap** ≈ 124 million USD
> **1 BTC** ≈ 3.68 USD

really?



Proofs of Stake

The “voting power” depends on how much money one has.

Justification: people who have the money are naturally interested in the stability of the currency.

Currencies: BlackCoin, Peercoin, NXT,

Also has some problems…

Proofs of Space

Replace **work** by **disk space**.

S. Dziembowski, S. Faust, V. Kolmogorov, K. Pietrzak, **Proofs of Space**.

Main advantages:

– no "dedicated hardware",

– less energy wasted ("**greener**").

Problem: hard to construct (only ***interactive*** **Proofs of Space** are known)

Preventing mining pool creation

Idea: help the mining pool members to cheat.

Andrew Miller, Elaine Shi, and Jonathan Katz. **Non-outsourceable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions.** June 2014

Conclusion

1. People want “cryptocurrencies”.
2. Bitcoin has some **important weaknesses**, new ideas are needed.
3. Tricky **security model**.
4. Bitcoin ideas that are interesting on their own:
   a) **consensus based on the PoW**
   b) generalized **transaction format**

Thank you!