

# Introduction to Modern Cryptography

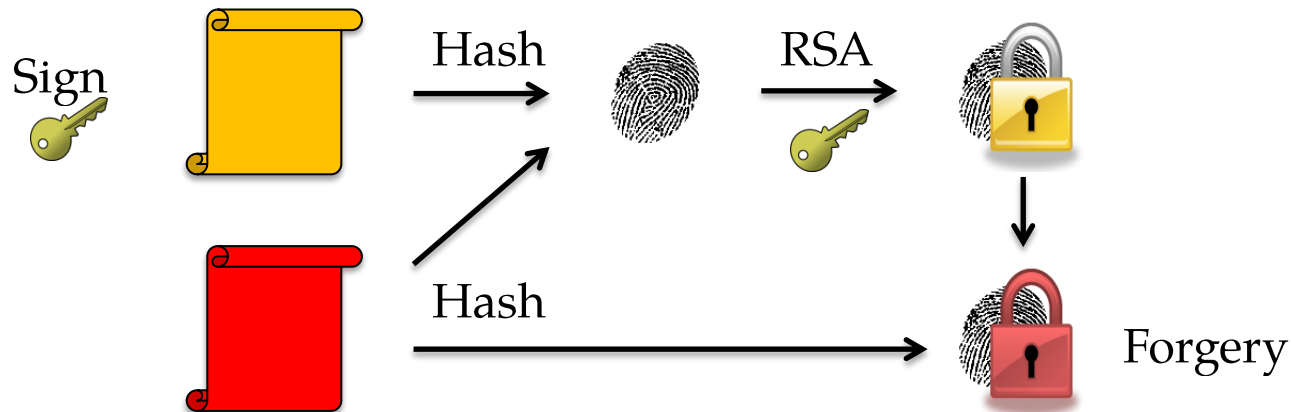
## Guest lecture on Bitcoin

dr.ir. Marc Stevens  
Cryptology Group  
Centrum Wiskunde & Informatica

<https://marc-stevens.nl/research>  
[marc@marc-stevens.nl](mailto:marc@marc-stevens.nl)

13-10-2014

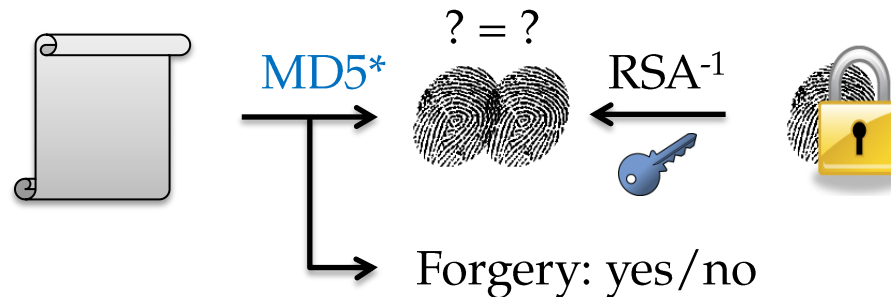
# My research: Cryptanalysis



Generate your own MD5 chosen-prefix collision attack  
in a day using Project HashClash:

<https://code.google.com/p/hashclash/>

# My research: Counter-cryptanalysis



Secure use of weak crypto primitives

Detect collision attacks

- Drop-in library interface
- Command line program

<http://marc-stevens.nl/research>

# Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org



**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. 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. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

## 1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need.



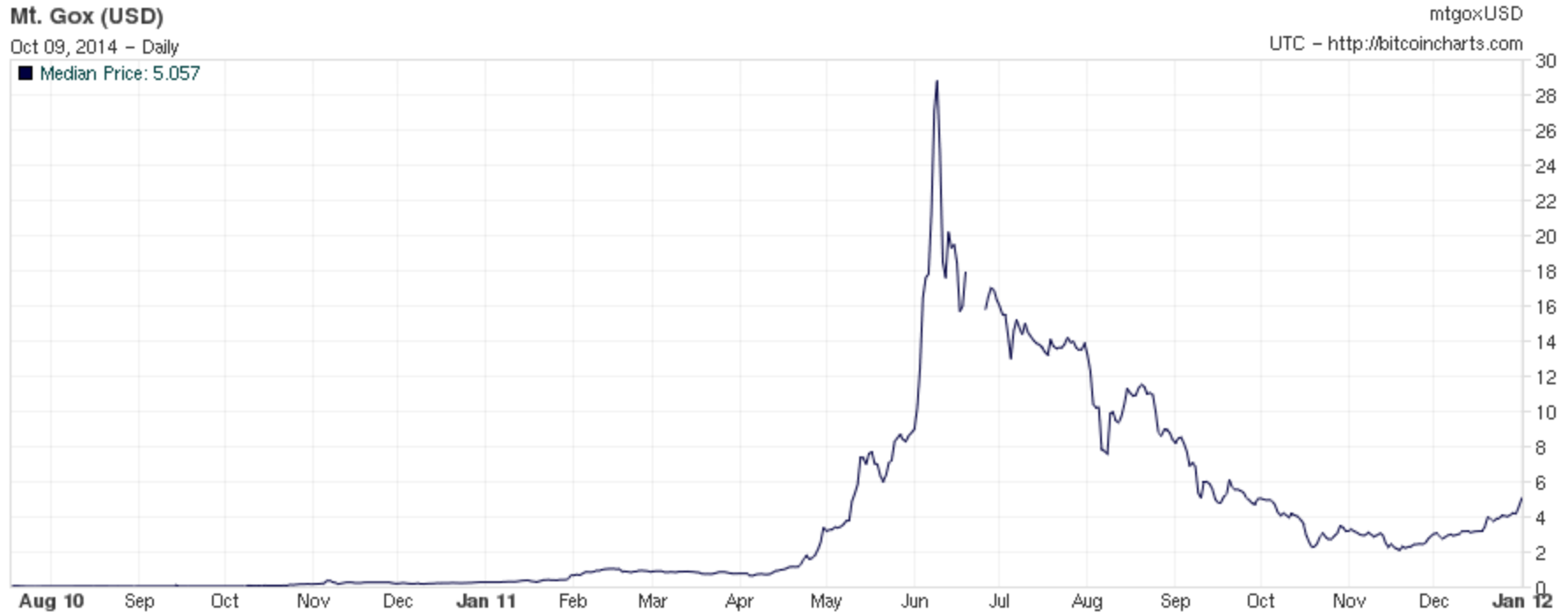
- First viable decentralized digital currency
- Money? Asset?
- VS,EU: virtual currency
- Price very volatile: no stable store of value
- Grand experiment

# MtGox trading started July 2010



20BTC for 1\$

# Bubble of June 2011



Peak of 33\$ at June 9

Crashes to almost 2\$

# Bubble of April 2013

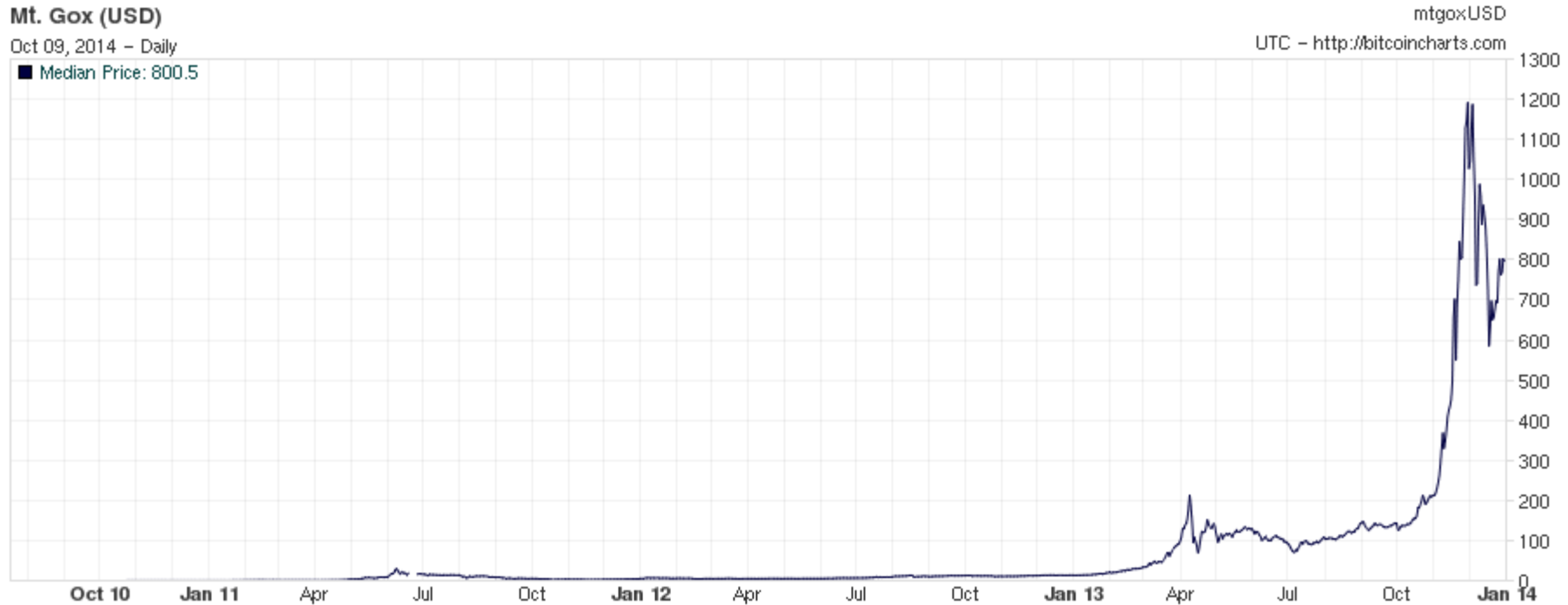


Peak of 266\$ at April 9

Crashes to 70\$



# Bubble of December 2013



Peak of 1200\$ at December 4

Crashes to 600\$

# MtGox shut down Feb 24 2014

BTC withdrawals stopped Feb 7

All withdrawals stopped Feb 17



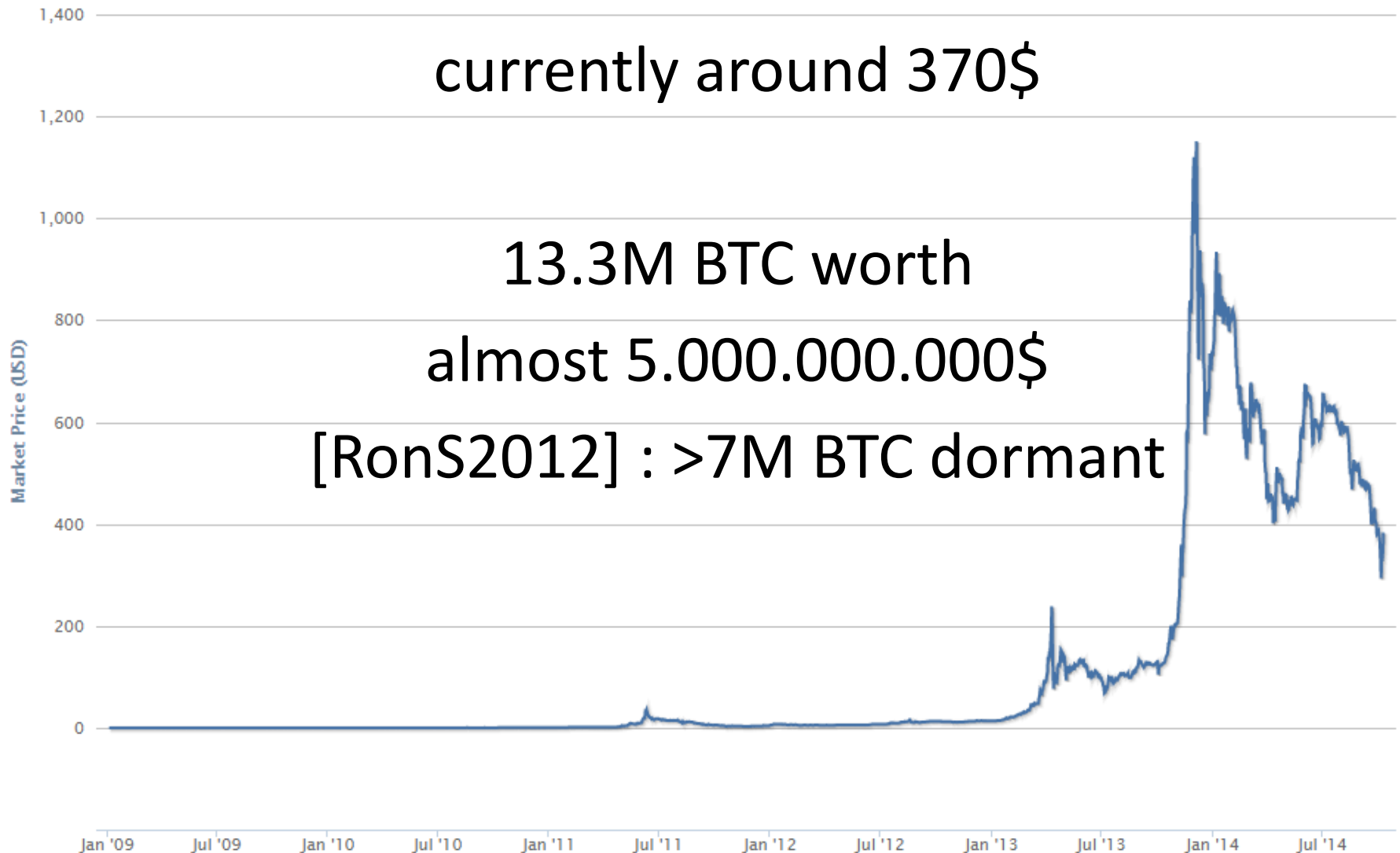
Claimed loss of >850.000 BTC due to 'transaction malleability'  
[DeckerW2014]: at most 8000BTC lost  
due to transaction malleability up to Feb 7

Market Price (USD)  
Source: blockchain.info

currently around 370\$

13.3M BTC worth  
almost 5.000.000.000\$

[RonS2012] : >7M BTC dormant



# Bitcoin protocol

- Maintains public ledger of transactions
- Decentralized
  - Entirely run on P2P-network of untrusted parties
- ‘Byzantine fault tolerant’
  - Claimed secure with (dis)appearing and malicious parties up to some limits
- First solution to “Double Spending”
  - Transactions become final and agreed upon by all (honest) parties

# BTC

- Amounts in BTC up to 8 decimals  
*satoshi* = 0.00000001 BTC
- Total amount of BTC fixed in protocol
  - New BTC ‘freely’ given away in ‘lottery’ (mining)
  - On avg. 50 new BTC every 10 min. in first 4 years
  - Then 25 for the next 4 years, etc.
  - Total limited to 21M BTC
  - Currently: 13.3M BTC

# Bitcoin address

- Based on Elliptic Curve *secp256k1*
- Account: (PrivKey, PubKey)



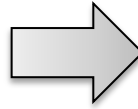
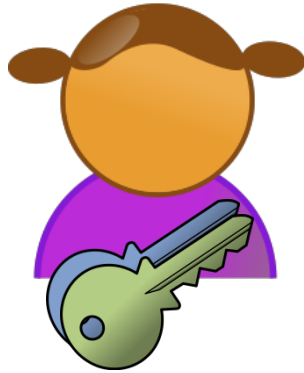
- Bitcoin address:



= Base58(RIPEMD160(SHA256(PubKey)))

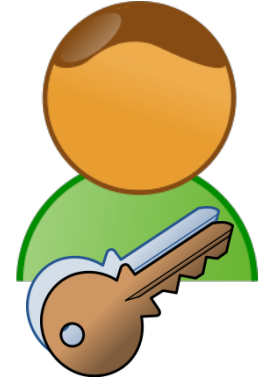
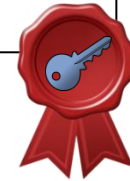
E.g.: *37k7toV1Nv4DfmQbmZ8KuZDQCYK9x5KpzP*

- PrivKey used to sign outgoing transactions
- Wallet: many (PrivKey, PubKey)

# Transactions



I, , pay BC #13107 to 



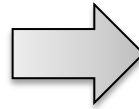
# Transactions



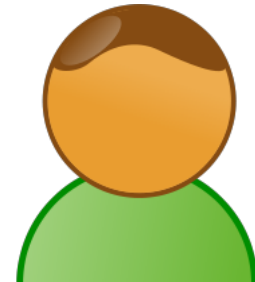
~~transaction #213  
to Alice: 1BTC~~

transaction #354  
to Alice: 2BTC

transaction #903  
to Alice: 22BTC



Transaction #903  
I, Alice, pay from transaction #213  
- 1BTC to Bob  
- 22BTC to Alice



transaction #903  
to Bob: 1BTC

transaction id = hash content

Account balance:

*total balance of unspent  
incoming transactions*

source transaction must be  
spent completely

multiple source transactions

multiple beneficiaries

script language

more complex payment and  
transaction models

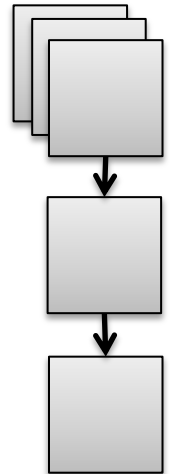
also non-transactions:

store arbitrary (short) data  
in Blockchain



# Public ledger

- Complete public record of all transactions
- Stored in *Blockchain*:
  - Sequence of valid *Blocks*
  - Each valid Block contains:
    - ID (hash) of preceding block
    - Valid transactions
    - Proof of work: global effort, ‘lottery’ between participants
    - Reward: fixed number of new BTC awarded to winner
  - New valid Block added every 10 min. on avg.



# Mining

- Mining: generating POW to extend Blockchain
- Search for solution:

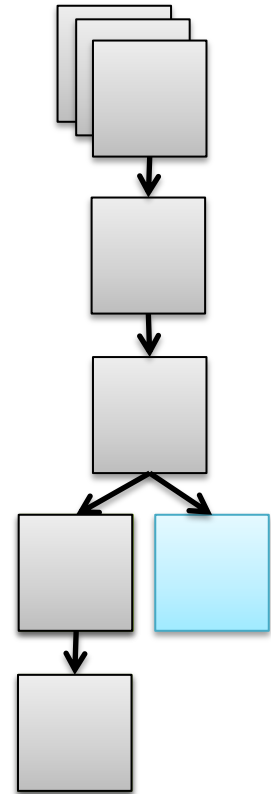
$$\text{SHA256}(\text{Block} \mid \text{Nonce}) < D$$

Random guess succeeds with probability  $D/2^{256}$

- Variable difficulty enforced such that on average 1 solution per 10 minutes is found
- Global Lottery: # tickets = # SHA256/10min
- Winner gets new BTC awarded
- Incentive to prevent single malicious party with majority in hashing power

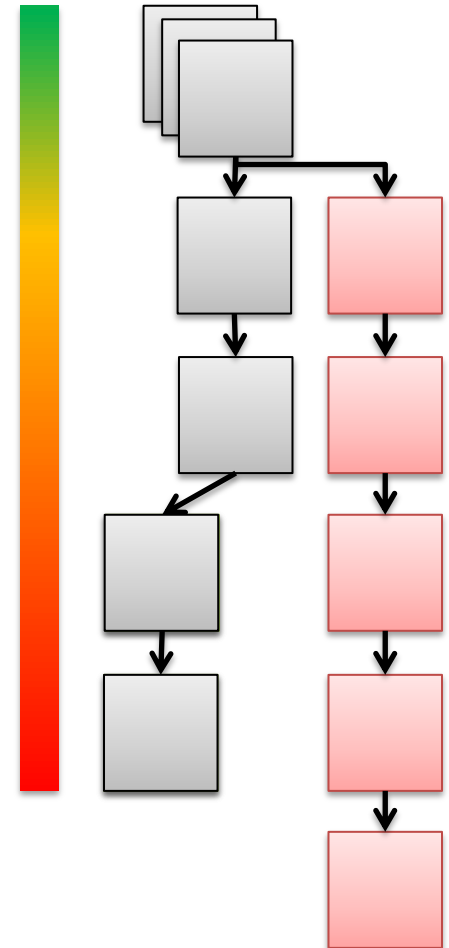
# Blockchain fork

- Each node running bitcoin protocol maintains a private version of the Blockchain
- Near-simultaneous solution may cause a 'fork'
  - Honest nodes in the network maintaining different Blockchains
  - Each try to extend its own version
  - Fork resolved by choosing Longest Blockchain, until then both are maintained in network
- More serious 'complete forks' caused by software incompatibilities (e.g., March 2013)



# Security

- Adapting chain is a race against the rest
- Majority hashing power:  
clearly insecure
- No majority:  
security of a block claimed to grow  
exponentially in # succeeding blocks
- Individual transactions secured by  
digital signatures
  - Requires unforgeability of signatures



# Security aspects

- Wallet
  - Has to be protected against loss (hardware failure)
  - Has to be protected against theft (physical or online)
  - Many examples
    - E.g., Nov'13: hard drive with 7500BTC thrown away
    - E.g., Jun'11: Theft of 25.000 BTC due unattended PC
    - Various online wallet websites hacked
    - Aug'13: Low entropy PrivKeys generated by Android Apps guessed by attackers

# Security aspects

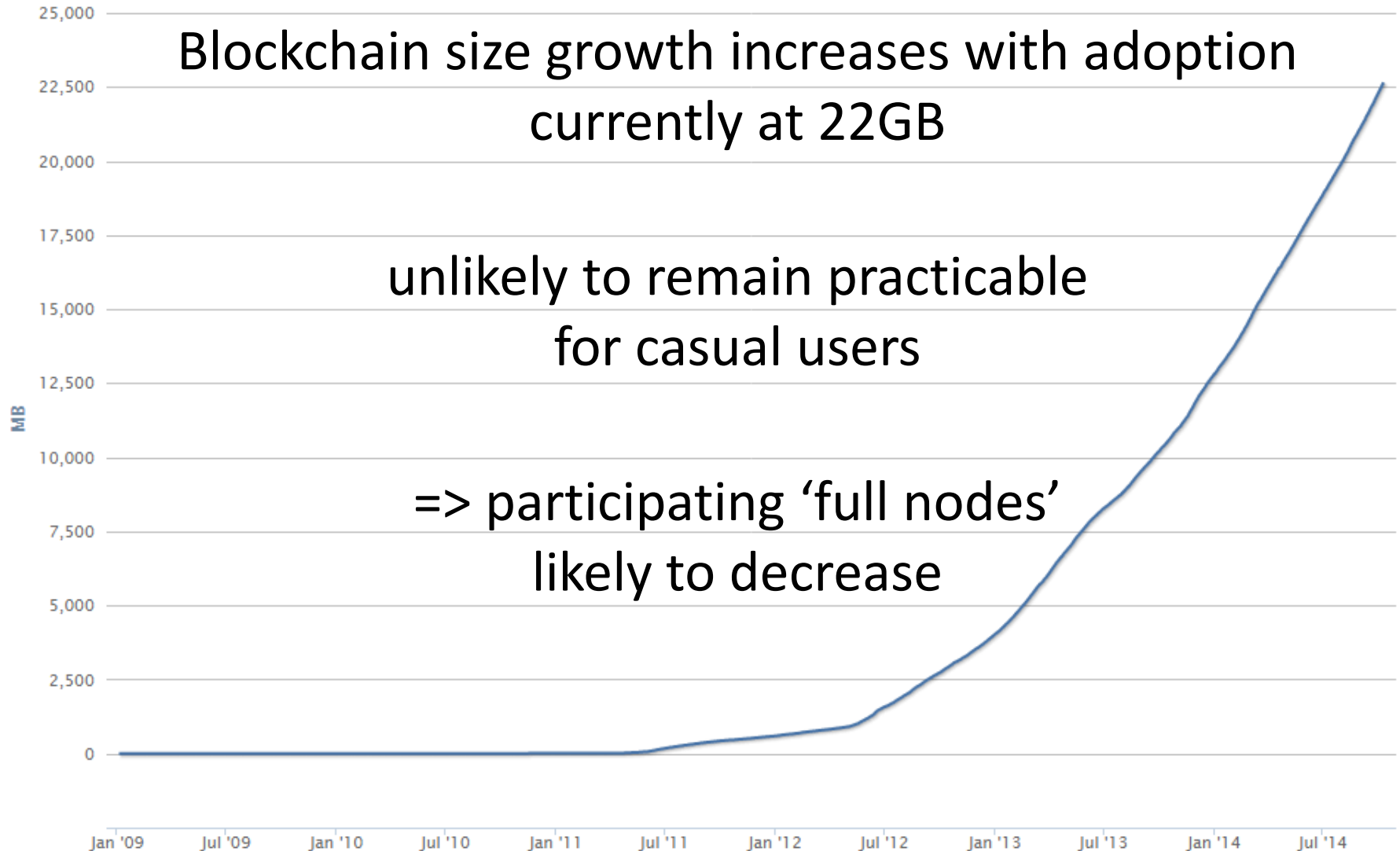
- Public Ledger
  - Transactions final
  - No cash-backs or refunds in case of loss or theft
  - No fake bitcoins
  - Not anonymous: bitcoin address are pseudonyms
  - Completely transparent: all transactions public for ever
    - Transaction graph can be used to link addresses to entities, track malicious movements, thefts etc.  
See, e.g., [RonShamir2012]
  - Scalability due to blockchain size growth?

Blockchain Size  
Source: blockchain.info

Blockchain size growth increases with adoption  
currently at 22GB

unlikely to remain practicable  
for casual users

=> participating 'full nodes'  
likely to decrease



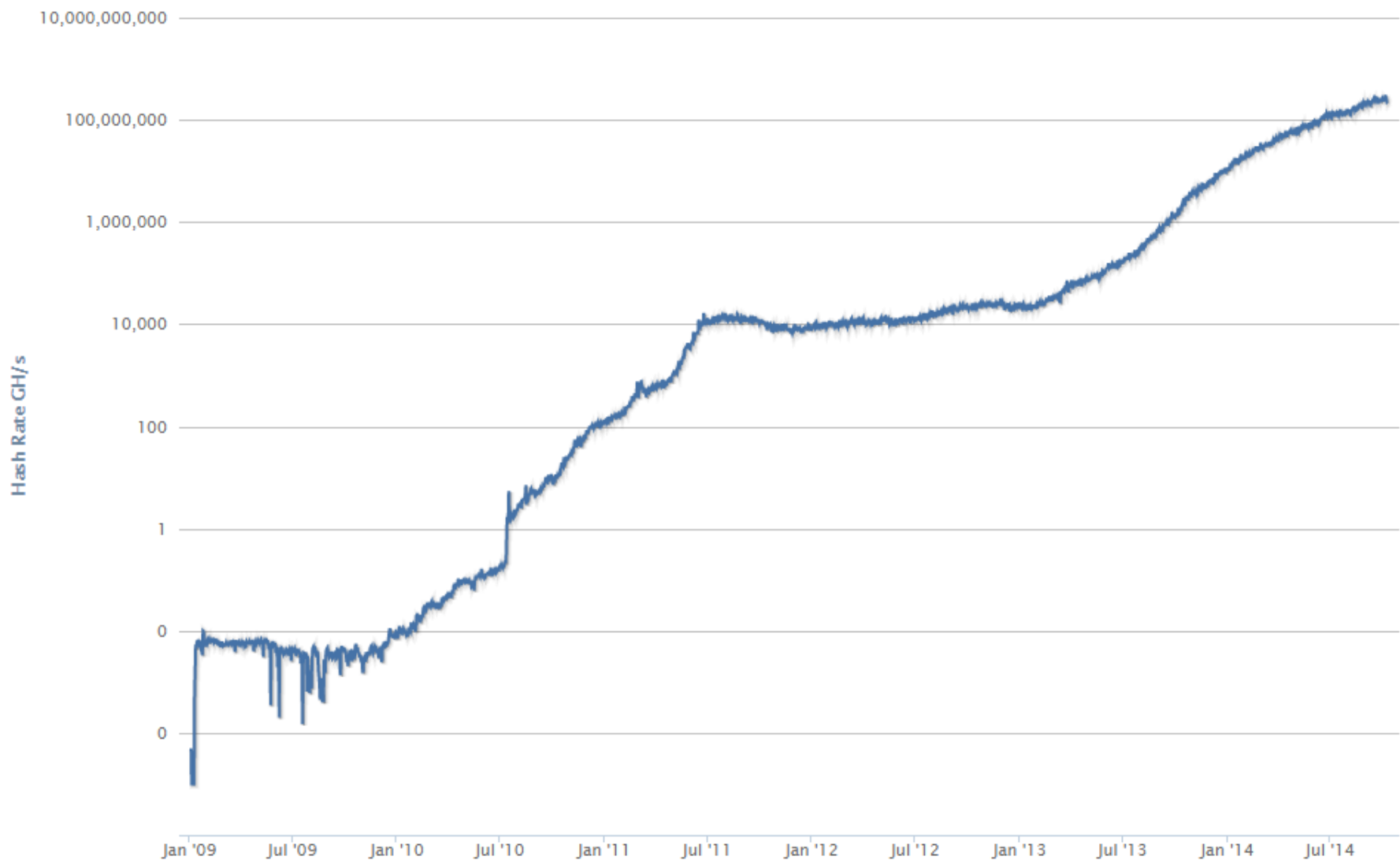
# Security aspects

- Mining
  - Race in hashing power
    - 2009-2010: mostly CPU
    - 2011: mostly GPU
    - 2012: FPGAs
    - 2013-: ASICs



## Hash Rate

Source: [blockchain.info](https://blockchain.info)



# Security aspects

- Mining
  - Bitcoin provides insights on computing power scales
  - Total computing power dedicated to Bitcoin:
    - $2^{58}$  SHA-256s per second
    - $2^{82.9}$  SHA-256s per year
  - Clearly allows to violate 80-bit security
  - What if used to break ...
    - SHA-1: brute force collision search in 2 months  
or 36 collisions in 1 year
    - RSA-1024: factor approx. 128 RSA 1024-bit keys per year

# Security aspects

- Mining
  - Selfish mining
    - Violate protocol to achieve higher chance in lottery
    - Various strategies depending on connectivity to network
    - High connectivity strategy:
      1. When you find a solution, do not share immediately
      2. Keep others working at shorter chain: lost computations
      3. When detecting another solution, “rush” in and overwhelm network with your solution
    - Low connectivity strategy (less rewarding):
      1. Privately try to extend chain
      2. When honest miners gain in, publish your longer chain

# Security aspects

- Mining
  - Adverse effects 10-min BTC rewards
    - Stealing computational power (e.g., malware, misuse company property)
    - Mining specialized: in hands of the few
    - Near-majority mining pools
      - Majority can easily be reached by malicious pact between 2 owners of near-majority pools
      - Participants can become unwitting accomplices

# Security aspects

- Post-Quantum security
  - ECC PrivKeys efficiently breakable
  - However, PubKey hidden until 1st transaction
  - Small exploit time window  
IF each bitcoin address used only once
  - 370.000.000\$-challenge
    - First transactions did use PubKey as address
    - >1M BTC remains in very old wallets (e.g., Satoshi)
    - 370.000.000\$-challenge to break *secp256k1*
  - Used Crypto (e.g., Lattice based)  
can be upgraded in clients,  
probably causes complete fork