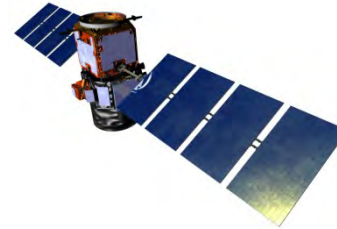




History and Concerns  
Innovation and Technology  
Analytics & Statistics  
New Services

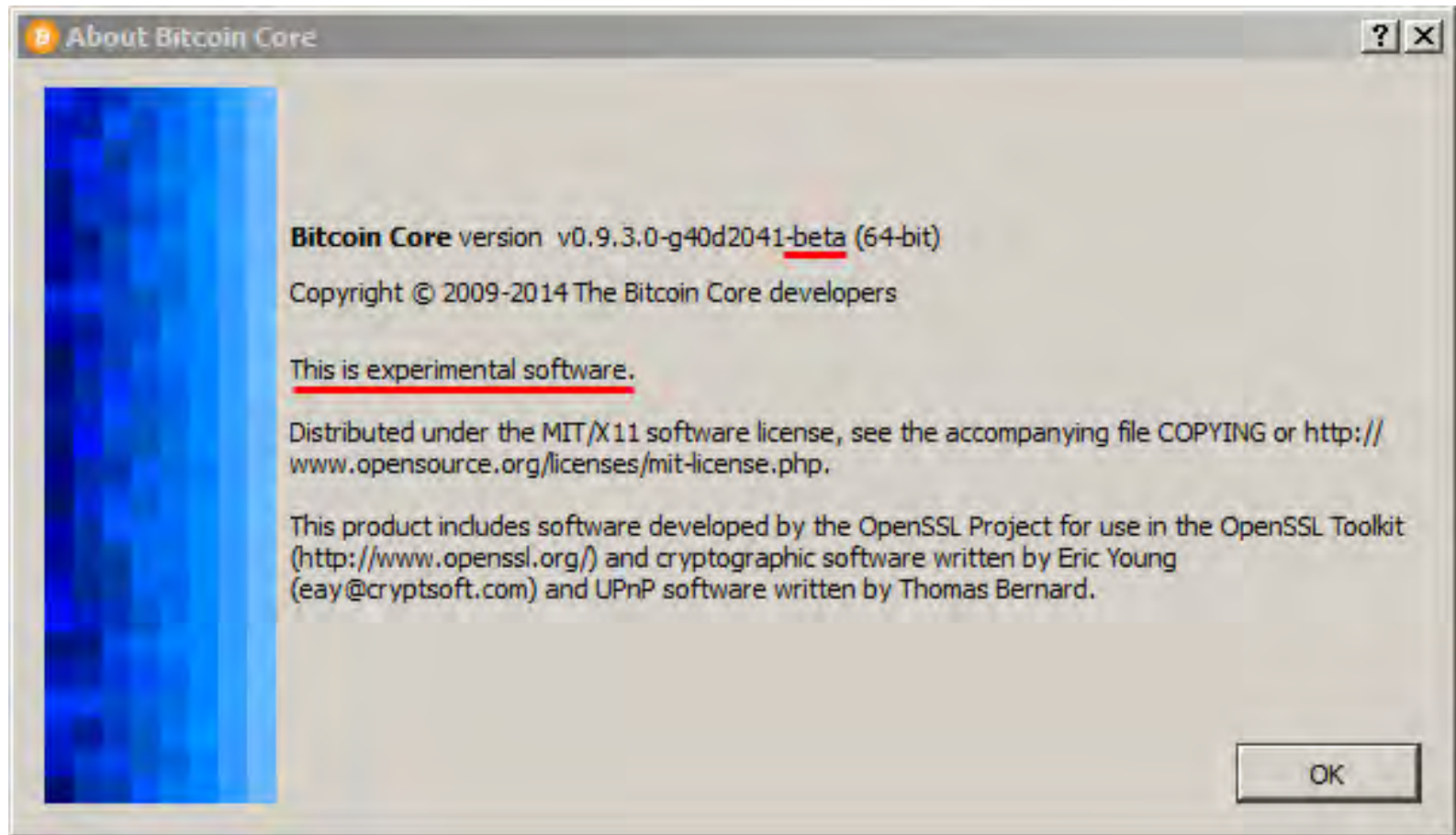
# About Me

**MUSE.AI**



<http://anton.io>  
@roldao

# Experimental Technology



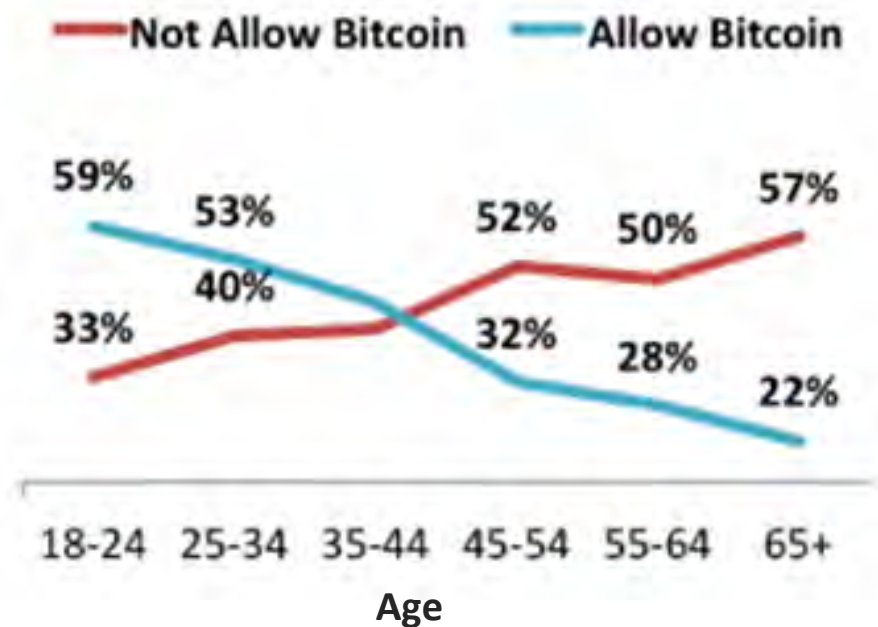
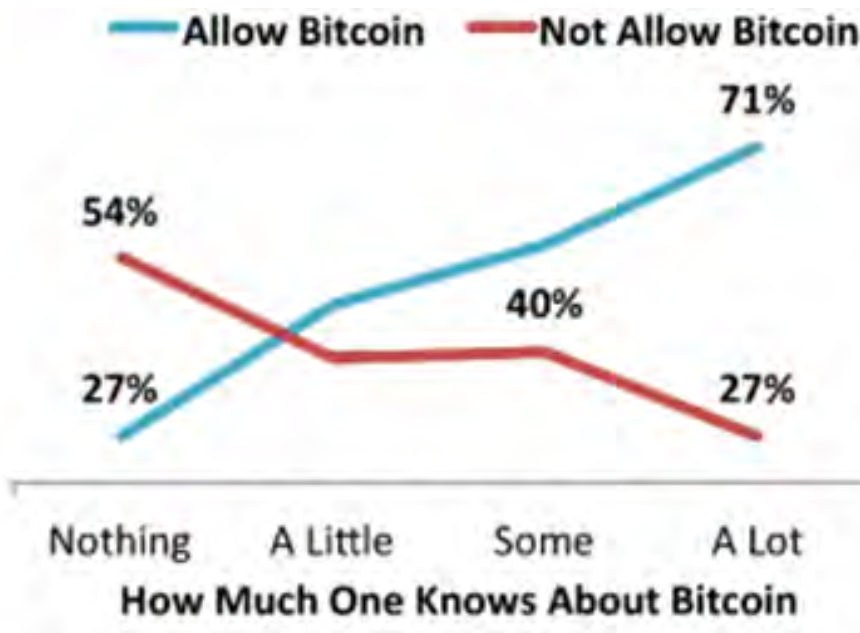
➤ \$6 billion experiment!!

# Brief History

- before – hashcash, eGold, b-money, ...
- 2008/Aug – bitcoin.org registered
- 2008/Oct – white paper published
- 2008/Nov – source code available
- 2009/Jan – genesis block mined (+9d to 1<sup>st</sup> transaction)
- 2009/Oct – 1<sup>st</sup> exchange rate: 1BTC = 0.0007639 USD
- 2010/Feb – 1<sup>st</sup> exchange is born (Bitcoin Market)
- 2010/May – 10,000 BTCs spent on pizza
- 2011/Apr – First put option sold (#bitcoin-otc)
- 2011/Jun – Bitcoin reaches \$10 on MtGox
- 2012/Jul – Bitcoin Start-up Incubator launched (BoostVC)
- 2013/Jul – Winklevoss Bitcoin Trust filed
- 2013/Aug – Texas judge ruled Bitcoin as Currency
- 2013 – BTC Ticker on all major business sites
- 2014 – Major corps accept Bitcoin (Dell, Expedia, MS, Time,..)
- 2015/Nov – EU Rules no VAT

# Knowledge vs. Public Perception

- Do you think the government should allow people to use Bitcoin to purchase goods and services or not?



# Media Coverage





# Concerns - Ponzi Scheme / Tulip Mania



# Confusing Media Circus



# Concerns - Conspiracy Theories



# Concerns - Illicit Activities / Drugs

# Concerns - Legal Framework



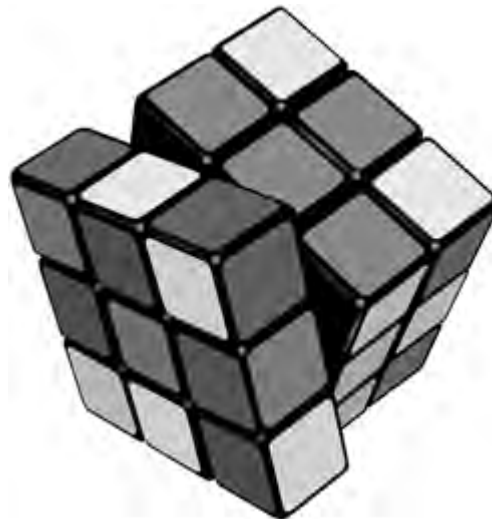
*“The Federal Reserve simply does not have authority to supervise or regulate bitcoin in any way.” – Janet Yellen*

# Concerns - Others

A word cloud of concerns related to Bitcoin 2.0. The words are arranged in a roughly triangular shape, with 'NotReversibleKeyLoss' at the top and 'VolatileTrust' at the bottom. The words are in various shades of gray and sizes, with some being bold and others regular. The concerns listed include: NotReversibleKeyLoss, ComplexMaths, NotPhysical, LimitedSupply, NoAccountability, Bitcoin2.0, MoneyLaundering, Misinformation, BrokenSHA256, SlowTransactions, Scalablility, BrokenECDSA, NotaCurrency, NoTaxes, Hackers, NoInflation, and VolatileTrust.

NotReversibleKeyLoss  
ComplexMaths NotPhysical  
LimitedSupply NoAccountability Bitcoin2.0  
MoneyLaundering Misinformation  
BrokenSHA256 SlowTransactions  
Scalablility BrokenECDSA NotaCurrency  
NoTaxes Hackers NoInflation  
VolatileTrust

# The Problem



# The Bitcoin Solution Allows:

- Creation of digital assets / tokens
- Proof of ownership
- Transfer of ownership
- Uniqueness of ownership
- Creation of accounts at will
- Direct exchange between participants without a third party!!



# Other Related Aspects:

- Micro-payments\*
- Payment freedom
- Frictionless transactions
- No central point of failure
- Public and transparent ledger
- Fast transactions across borders
- No central point of manipulation
- No risk of physical possession/loss
- Well understood and mathematical
- The gold standard in crypto-currencies
- Very low fees, some times even zero fees
- Anyone/Thing can open/close an account
- Human2Human/Machine2H/H2M/M2M Business
- ...



\*currently, with some important limitations.

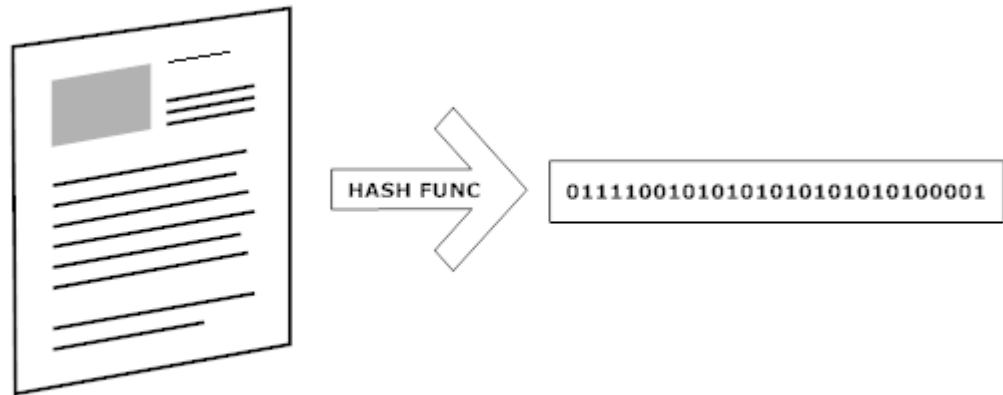


# How Does Bitcoin Work?



# Key Concepts – Hashes 1/2

## ➤ Hashing functions



```
In [1]: 2**256
```

```
Out[1]: 115792089237316195423570985008687907853269984665640564039457584007913129639936L
```

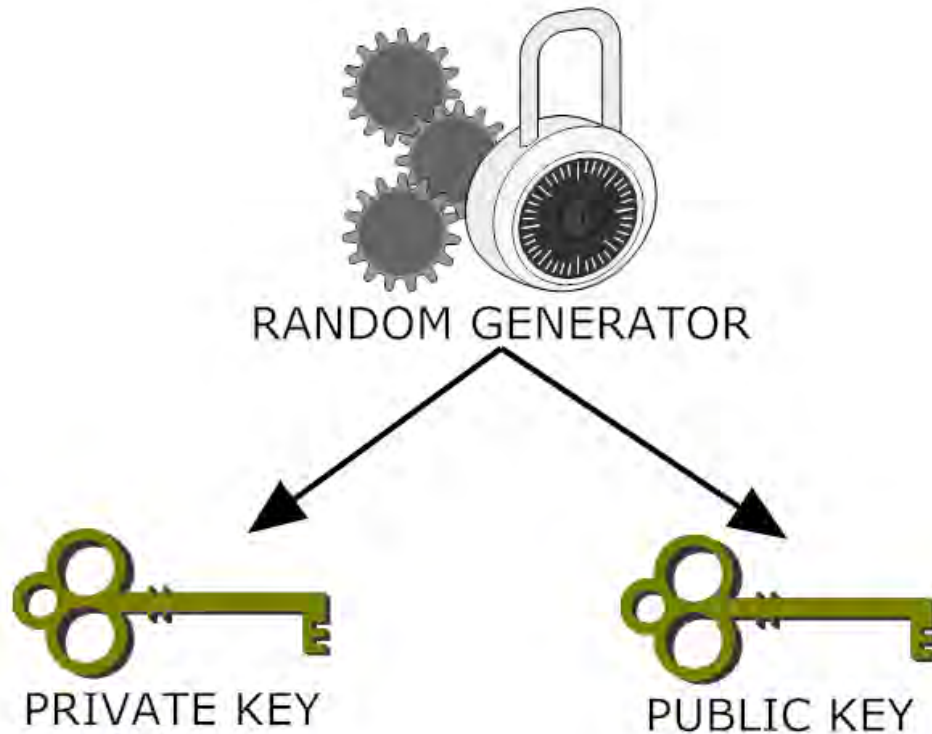
```
In [2]: import hashlib  
sha256 = hashlib.sha256()  
sha256.update("")  
sha256.hexdigest()
```

```
Out[2]: 'e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855'
```

# Key Concepts – Hashes 2/2

- Obfuscating passwords (*e.g.* /etc/shadow)
- Cyclic Redundancy Checks (*e.g.* md5 on downloaded files)
- Verification of file authenticity (*e.g.* kernel source code)
- Compression of data (*e.g.* deduplication on git / ZFS/ ...)
- Bucketing data (*e.g.* database sharding)
- ...
- Integrity of chain of events (*e.g.* merkle root / blockchain)
- Calibrating compute power for Proof of Work!
- Proof of prior existence without disclosure

# Key Concepts – Digital Signature Algorithms



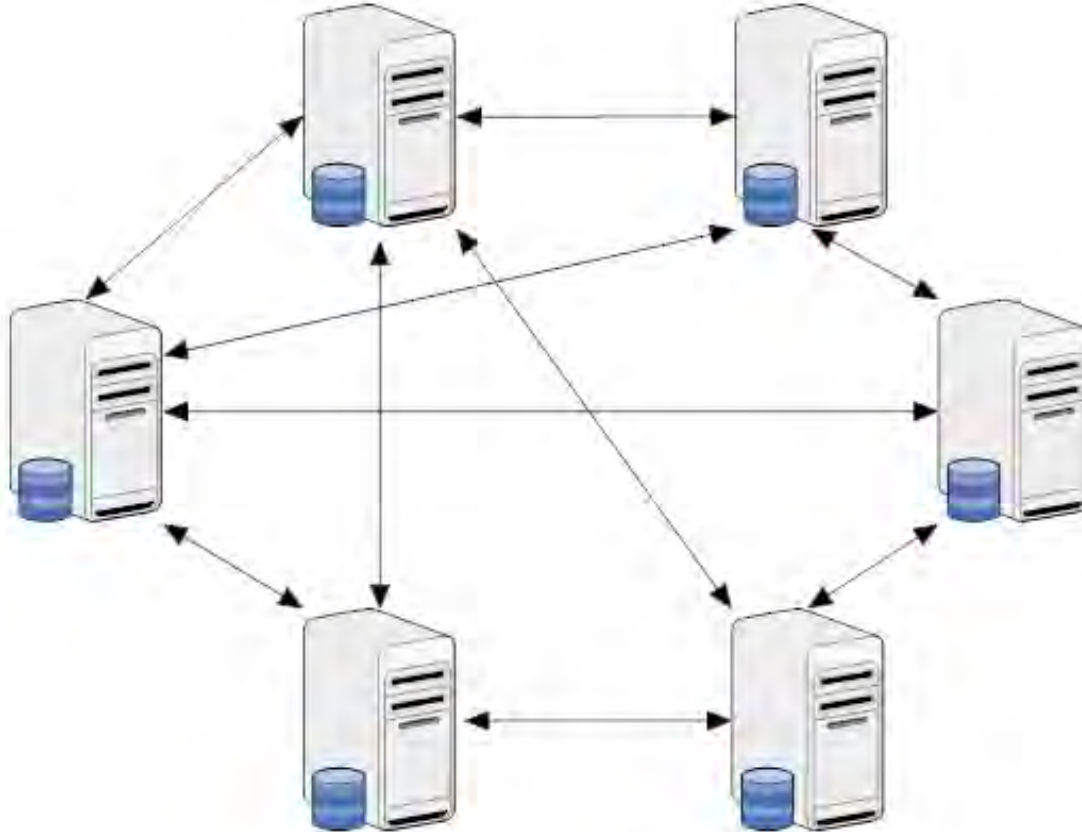
# Key Concepts – Public Ledger

Time	Account	Inputs	Outputs	Balance
1	addr1	20	-	20
2	addr2	100	-	100
3	addr1	-	10	10
4	addr1	20	-	30
5	addr2	-	100	0
6	addr2	2	-	2
7	addr3	5	-	5
8	addr3	2	4	3
9	addr1	5	-	35
...	...	...	...	...

All Transactions



# Key Concepts – P2P Networks



# Key Concepts – “Script” Language



- Non-Turing complete (*i.e.* no loops)
- Stack-based
- Forth-like syntax (*e.g.* hint of the creators age!)
- Each stack evaluates to True or False
- Allows embedding of data (*e.g.* messages)
- Built-in cryptographic and hashing functions (*e.g.* SHA256, RIP160)
- Allow for non-trivial conditions such as multi-signature, etc.

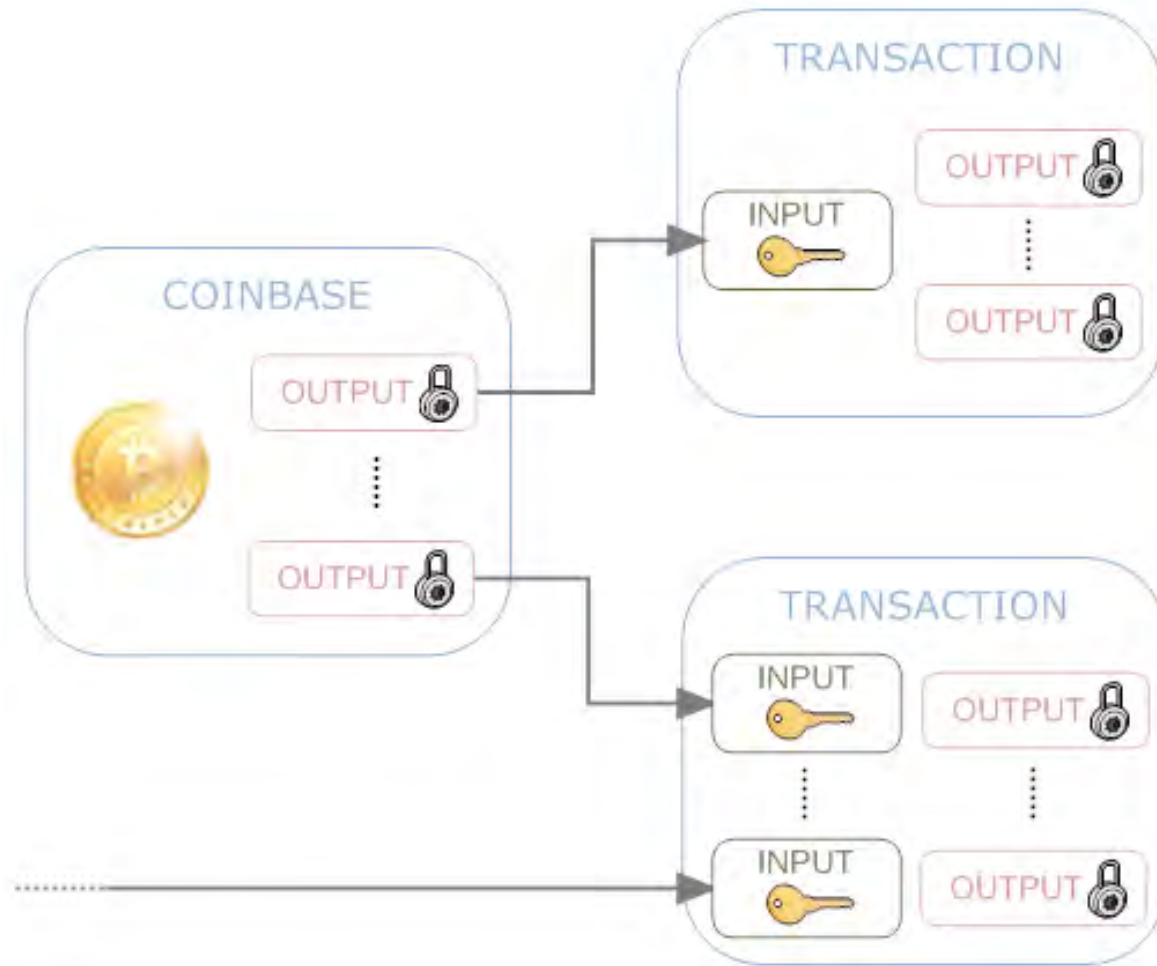


# Key Concepts – Network Effects & Game Theory

- Interests are aligned for everyone to cooperate
- Positive Network effects
- Only valuable if intact
- Need to cooperate to keep its value
- 51% Attacks benefit no-one
- ...



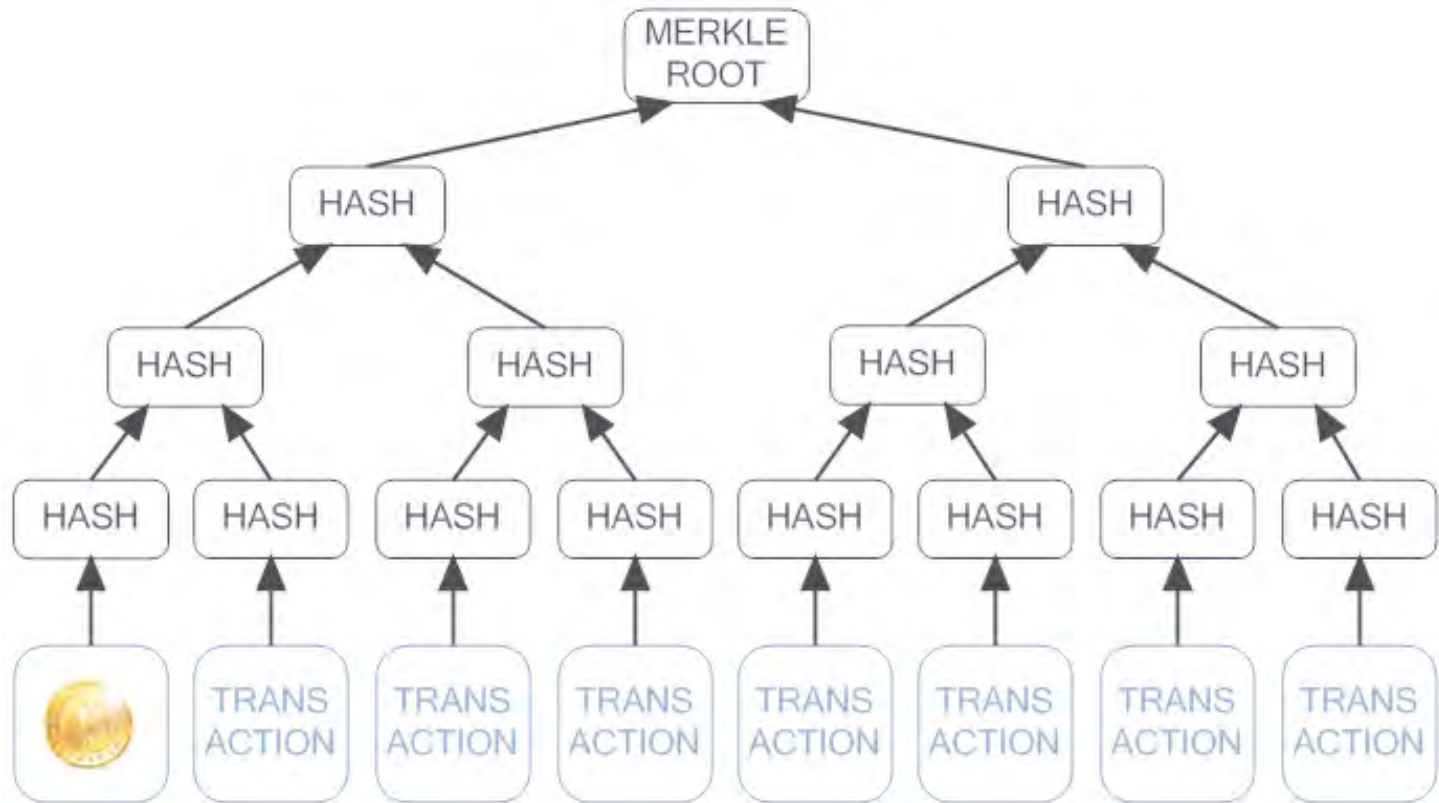
# Details – Transactions 1/2



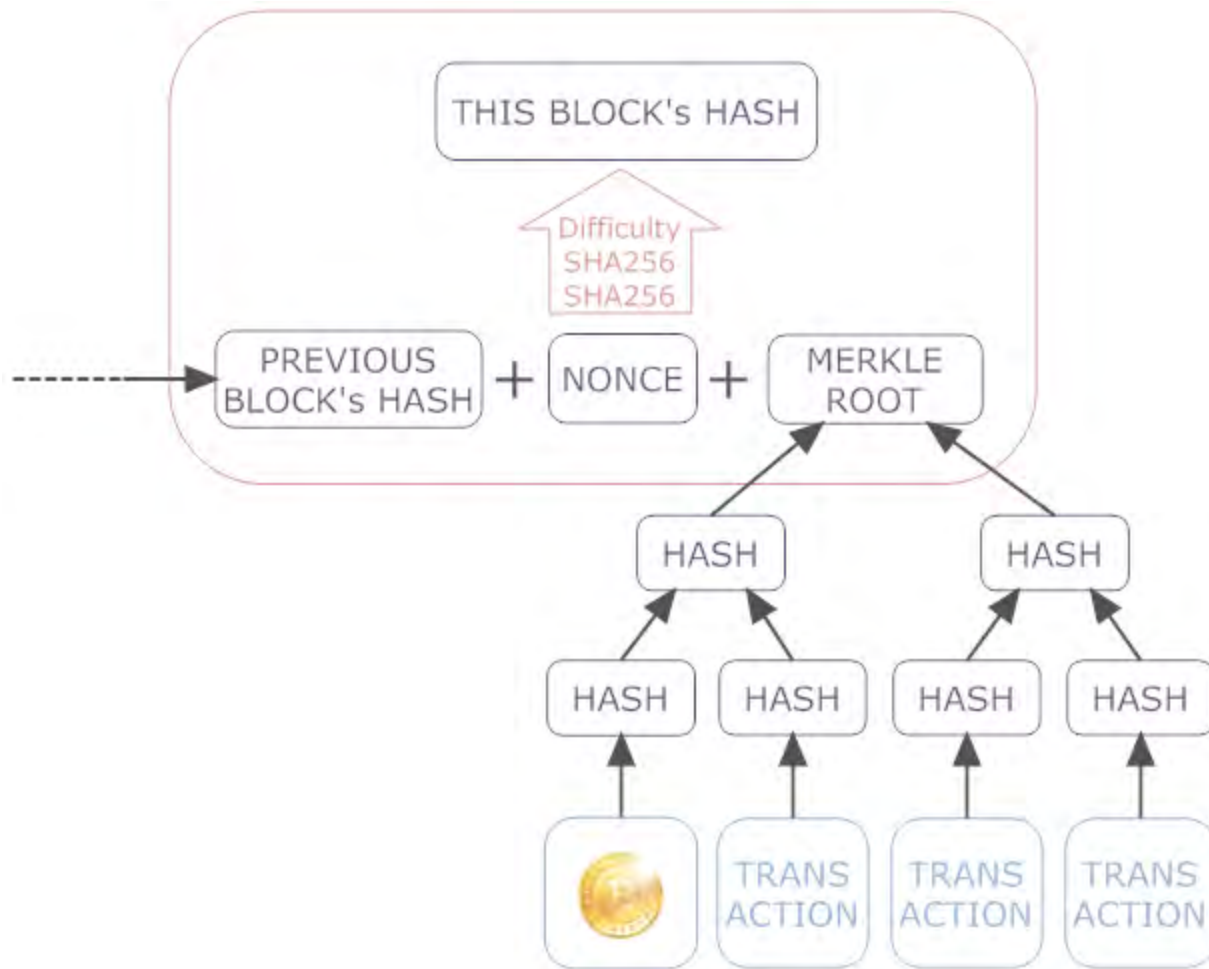
# Details – Transactions 2/2

- 2 types: Coinbase, and Standard
- Outputs typically “lock” coins to the owner of some key
- Can embed messages (*e.g.* timestamp)
- Coinbase
  - 1<sup>st</sup> transaction of a mined block
  - Brings coins into existence
  - Allows miners to claim mining fees
- Standard
  - Outputs cannot exceed inputs
  - Excess Inputs will be added to Coinbase as mining reward
  - Chain of transactions necessarily begins at a Coinbase

# Details - Storing Transactions



# Details – Block 1/3



# Details – Block 2/3

- 1<sup>st</sup> block is named genesis
- All other blocks reference previously mined block
- System calibrates difficulty to mine one every ~10mins
- At the beginning, each block generated 50 BTCs
- Every 210,000 blocks (~4 years) this value halves
- Currently at 25 BTCs/block
- Block size is currently fixed at 1 MB\*
- 1 MB translates to ~7 Transactions per Second

\*Bitcoin XT – includes patches to upgrade to 8 MB once 75% are voting to change from 2016.

# Details – Computing a Block Hash

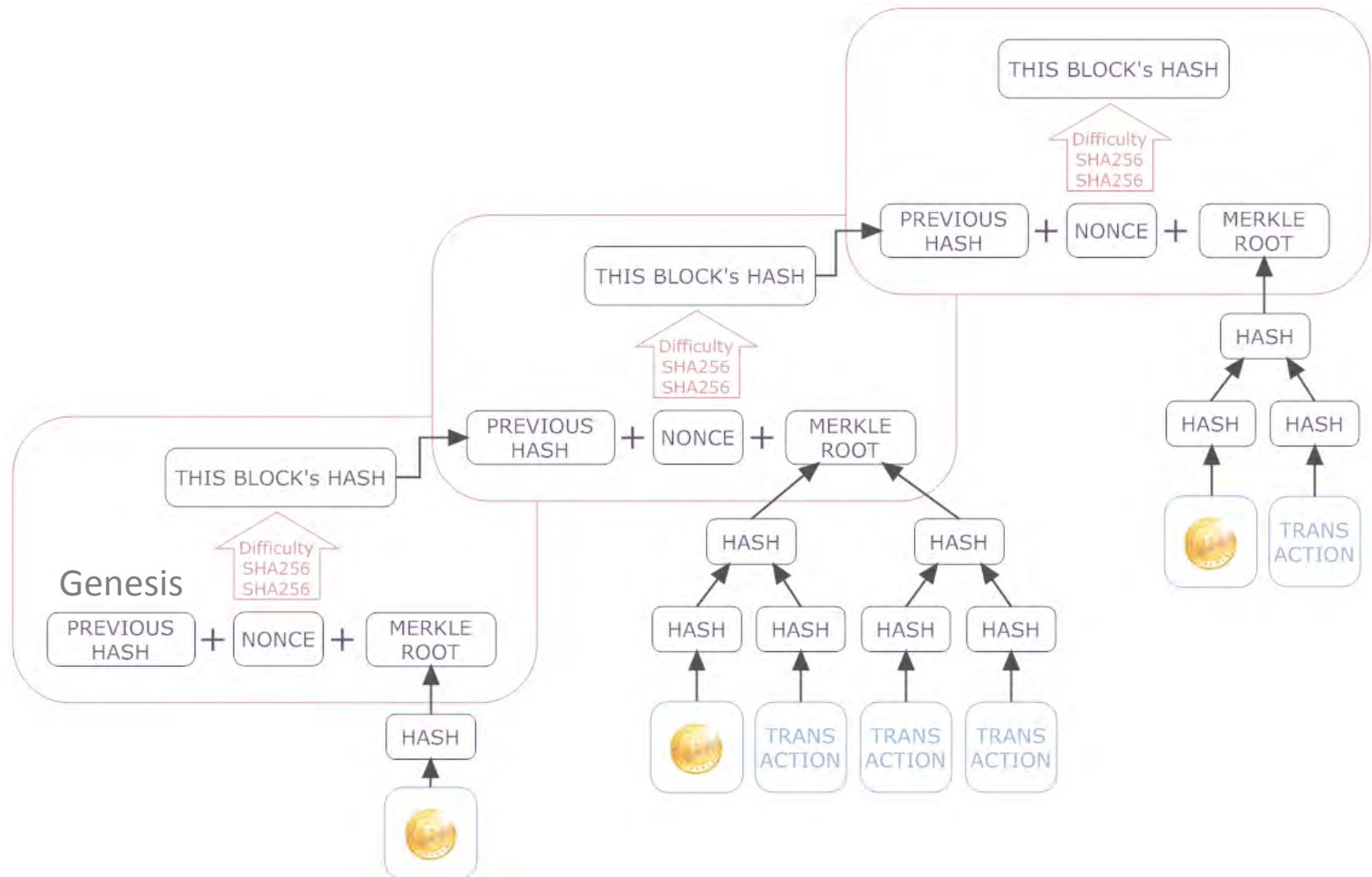
```
In [1]: from hashlib import sha256
# Block 288888
hex_next_block = (
    # Version
    "02000000" +
    # Prev block
    "d5776392209a5211166c137c6645b0c07610c64bff39a3350000000000000000" +
    # Merkle root
    "adf3233d0c6de7739cd3c9c3ebc8f0513831e935f49d637ead4afcf9c1b622cd" +
    # Time
    "ecee1553" +
    # Difficulty
    "26200119" +
    # Nonce
    "6a14f276"
)
bin_next_block = hex_next_block.decode('hex')
hash = sha256(sha256(bin_next_block).digest()).digest()
hash[::-1].encode('hex_codec')
```

```
Out[1]: '00000000000000000a456b9cd160ccfaf4d6b7341dc9aae04f98e5120fa5a73a3'
```

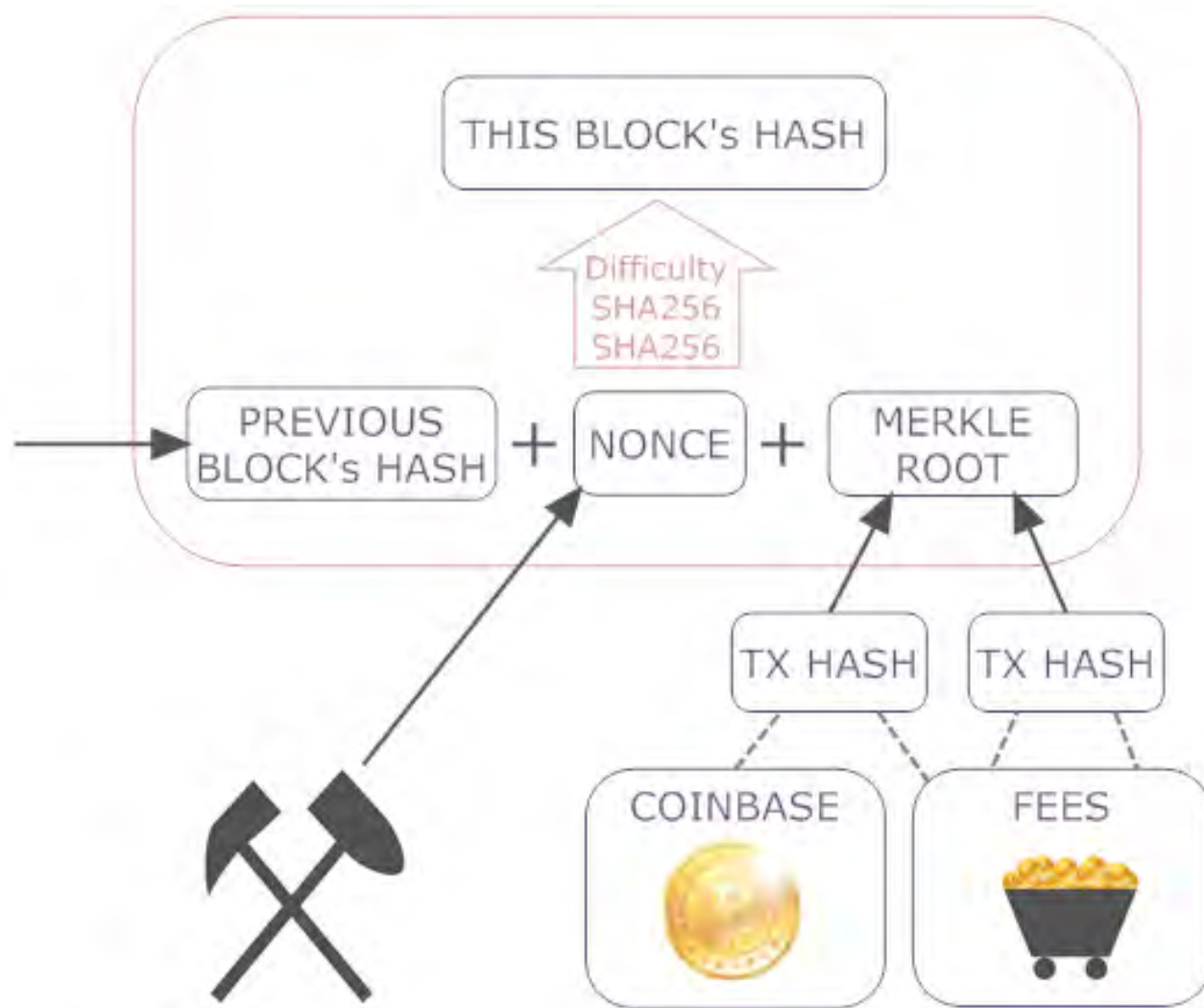
<https://blockchain.info/block-height/288888>



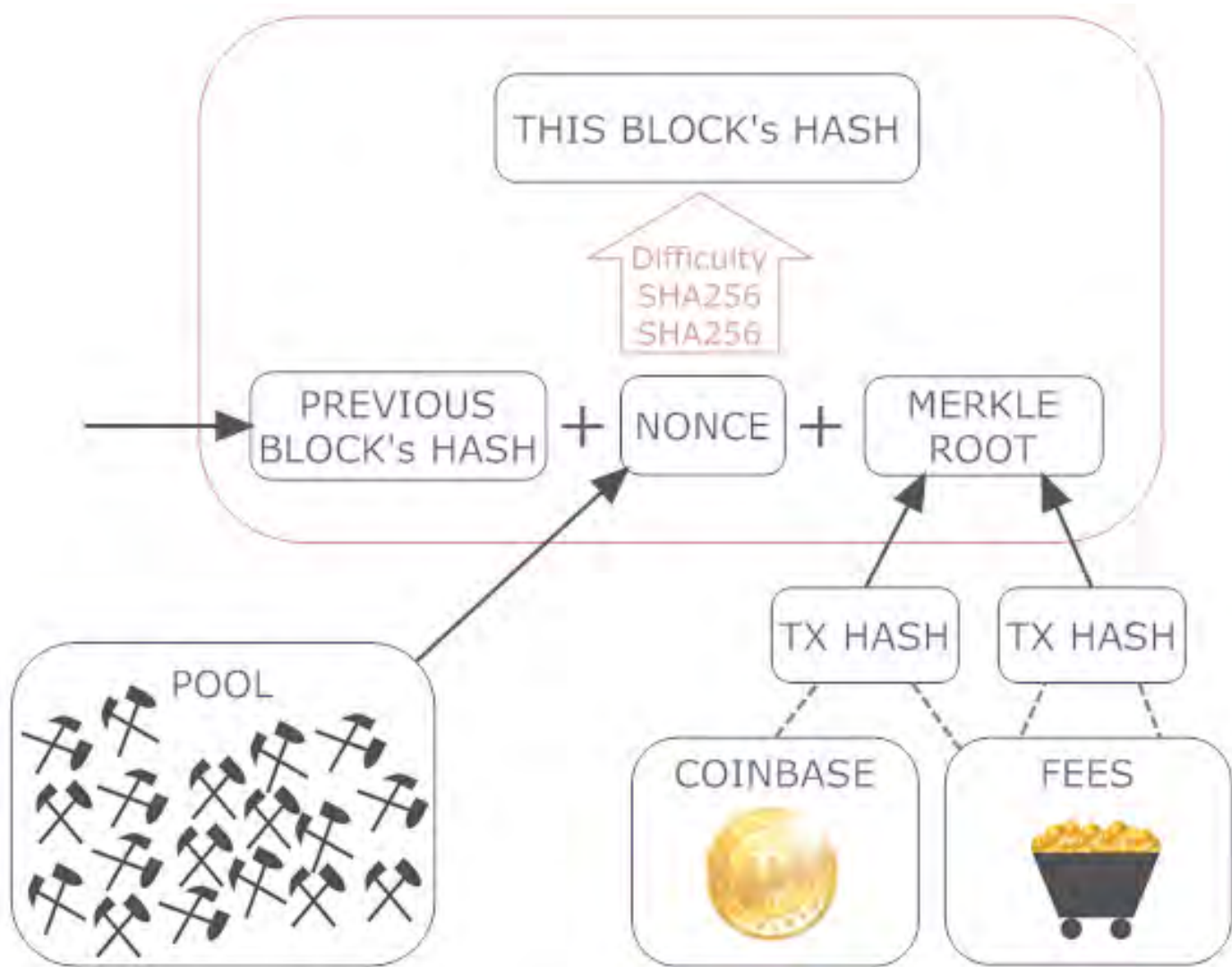
# Details - Blockchain



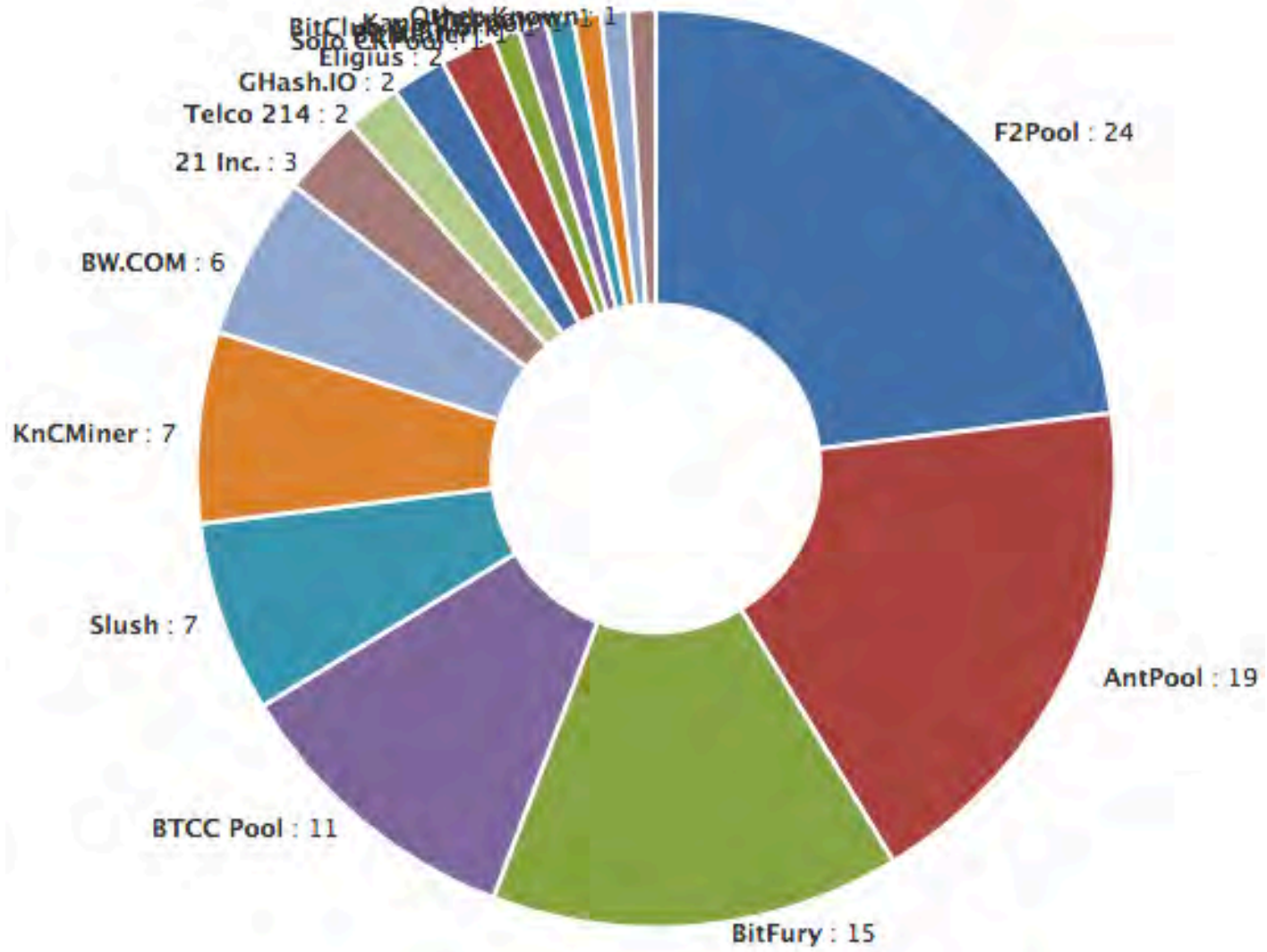
# Mining



# Mining - Pools

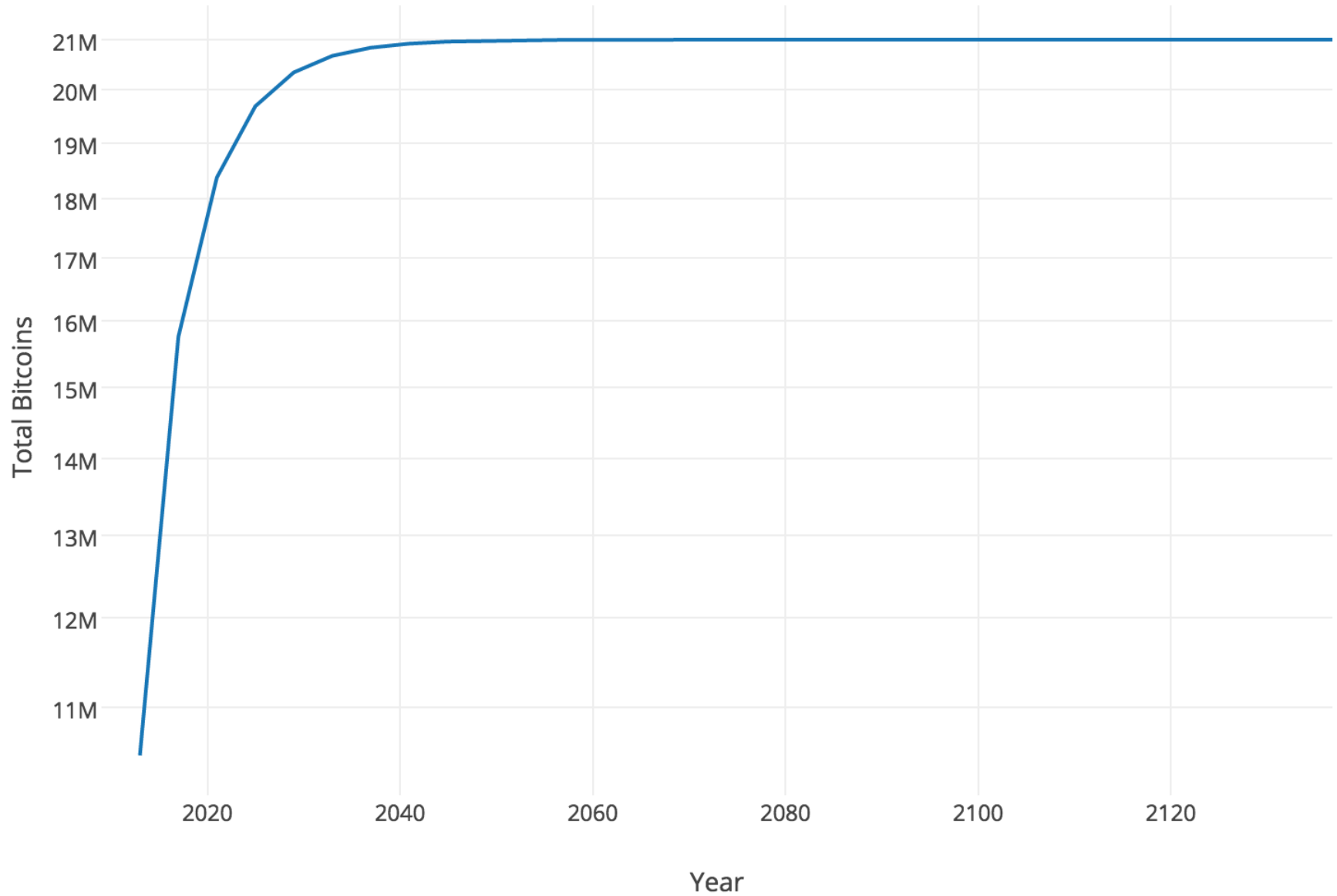


# Mining – Pools Contribution



source: <https://blockchain.info/pools>

# Bitcoin Mining



# Mining Fees and Rewards

- Miners are incentivized in two ways: Fees and Rewards
- Fees are discretionary amounts set by the sender
- Rewards are given at the discovery of each block
  - (until 2136-10-11 10:15:05)
- Transaction may be free if
  - Less than 1kB
  - Outputs >0.01 BTCs
  - Priority is large enough
- each additional 1k should include a fee of 0.1mBTCs

Source: [https://en.bitcoin.it/wiki/Transaction\\_fees](https://en.bitcoin.it/wiki/Transaction_fees)

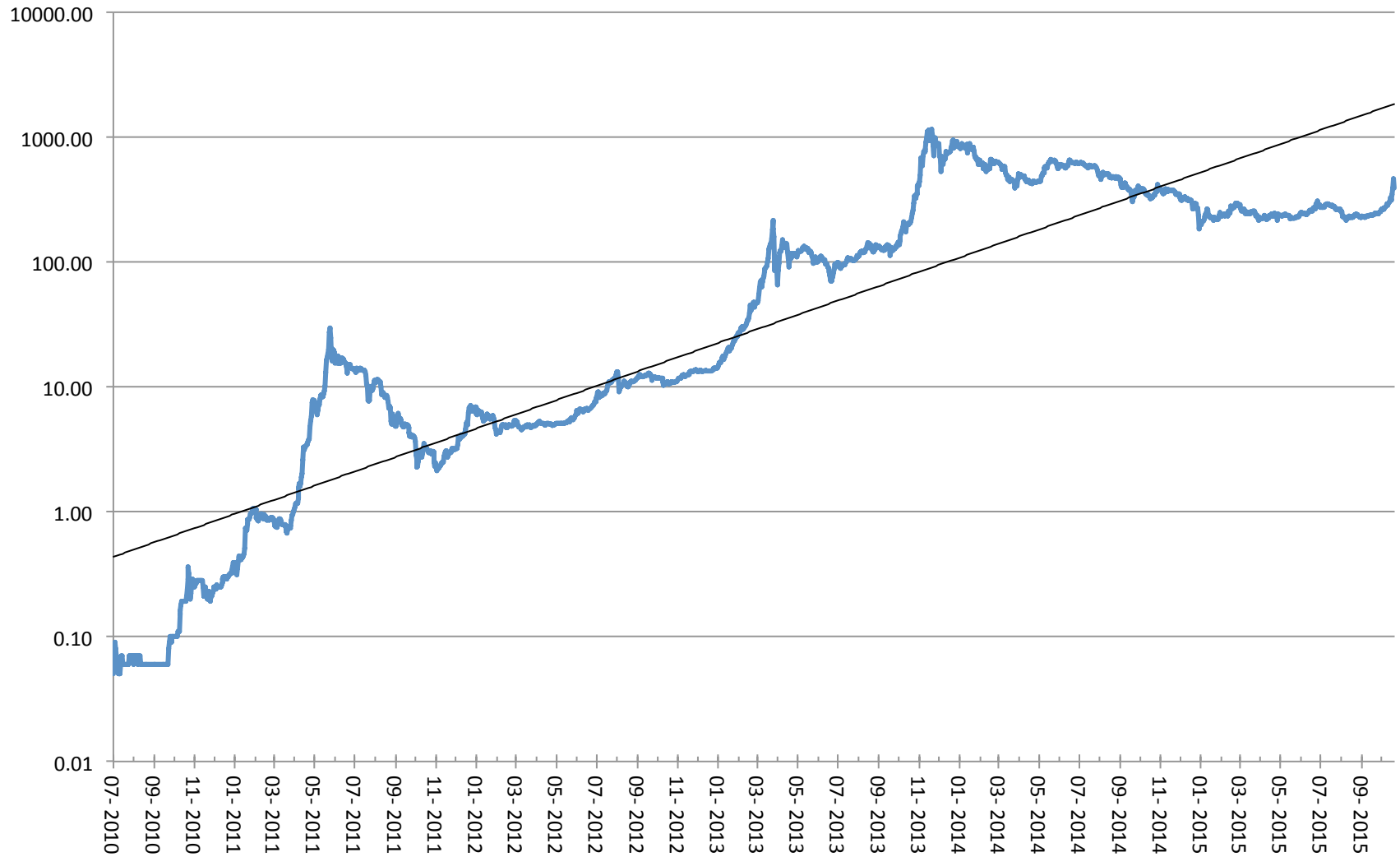
# Analytics & Statistics





# Price Evolution

## BTC/USD



# Discovering Bitcoin's Fair Price?

- $1 \text{ Bitcoin} = f_{\text{cost}}(\text{Energy} + \text{Equipment} + \dots)$ 
  - Hardware performance varies widely
  - Energy depends on country
  - Difficulty level
- Other Interesting questions
  - How will diminishing coinbases affect fees?
  - Will mining make energy generation more efficient or more expensive for day-to-day use?
  - Will mining drive innovation for faster and cheaper electronics or make high-end chips more expensive?

# Mining Efficiency



CPU  
>1Mh/s  
~5khps/W



GPGPU  
>1Gh/s  
~2Mhps/W



FPGA  
>1Gh/s  
~10Mhps/W



ASIC  
>10Gh/s  
~235Mhps/W

400x

5x

32x

64000x

source: [https://en.bitcoin.it/wiki/Mining\\_hardware\\_comparison](https://en.bitcoin.it/wiki/Mining_hardware_comparison)

# FPGA Spaghetti Monster

source: <http://www.bitcoinminingrigs.com/>

# Professionalized Mining

# Hash Rates

Source: blockchain.info

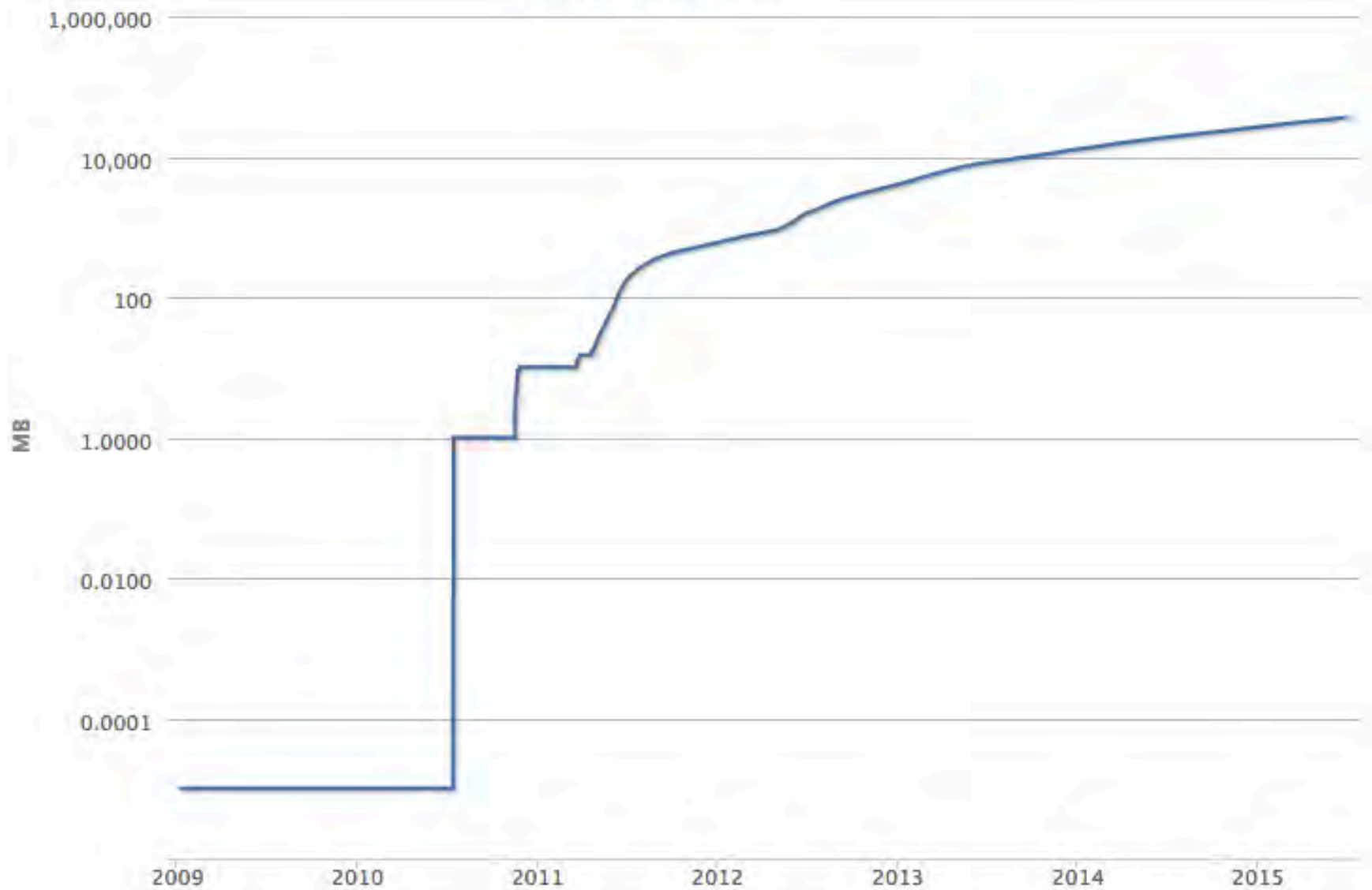


# Difficulty Rates



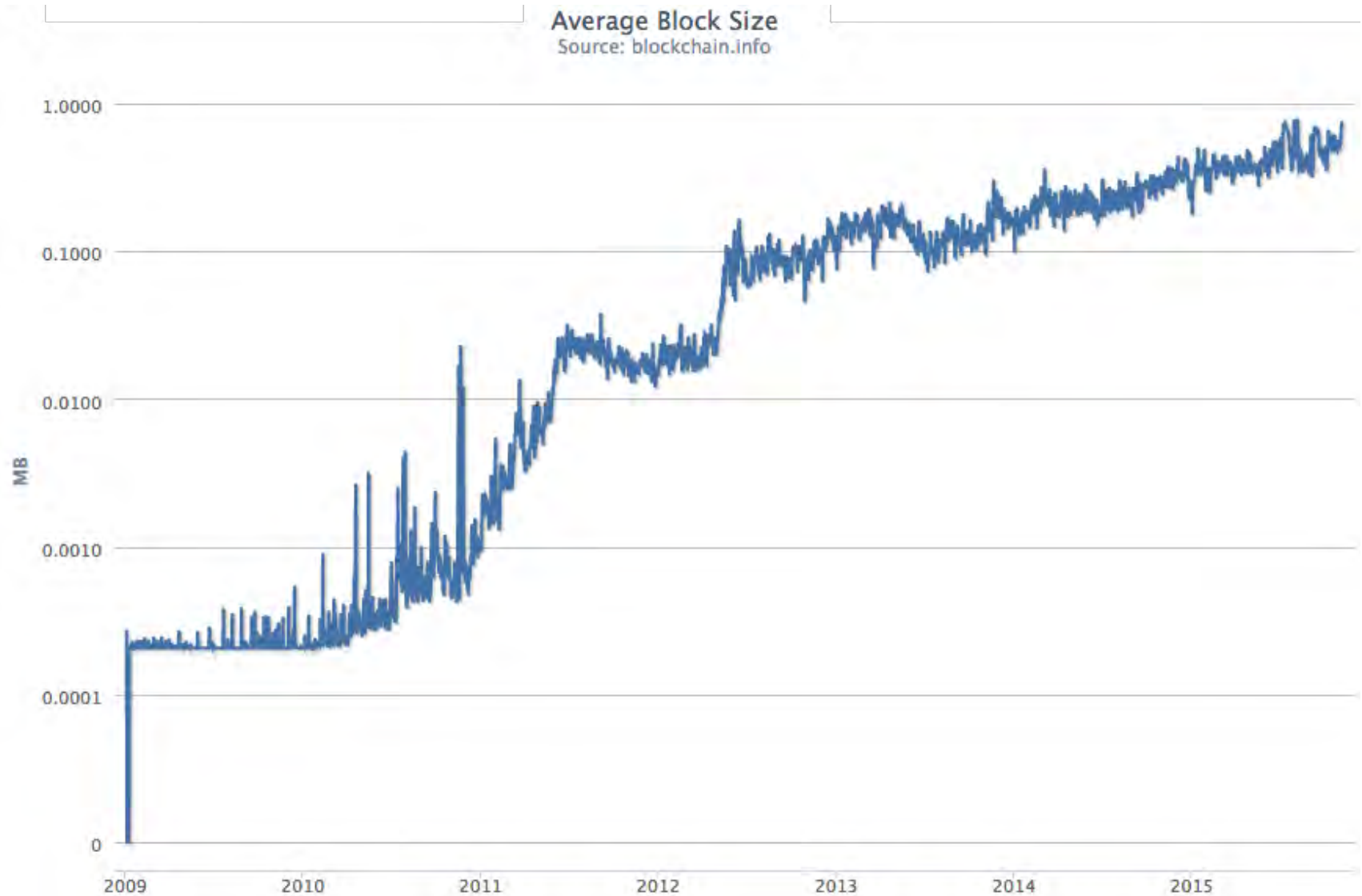
# Ledger Storage

Source: blockchain.info







# Average Block Size



# Blockchain Browsers

 **BLOCKCHAIN**

Home Charts Stats Markets API Wallet



## Home

Welcome to Blockchain [More...](#)

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
<a href="#">289599</a>	3 minutes	23	33,071.56 mBTC	<a href="#">Eligius</a>	11.80
<a href="#">289598</a>	3 minutes	361	466,711.86 mBTC	<a href="#">Slush</a>	187.56
<a href="#">289597</a>	< 1 minute	64	1,042,265.53 mBTC	<a href="#">109.72.66.244</a>	52.21
<a href="#">289596</a>	11 minutes	110	466,894.30 mBTC	<a href="#">BTC Guild</a>	96.82
<a href="#">289595</a>	13 minutes	91	540,007.66 mBTC	<a href="#">GHash.IO</a>	56.44
<a href="#">289594</a>	14 minutes	159	1,312,066.81 mBTC	<a href="#">BTC Guild</a>	96.83

### Latest Transactions

<a href="#">9630322bf5...</a> ( <a href="#">SatoshiBONES</a> 62.5pct)	< 1 minute	3.48751 mBTC
<a href="#">30aefa292f2...</a> ( <a href="#">SatoshiBONES</a> 62.5pct)	< 1 minute	36.82881 mBTC

### Search

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address..

Search

- Blockchain
- Block Explorer
- BTCLook

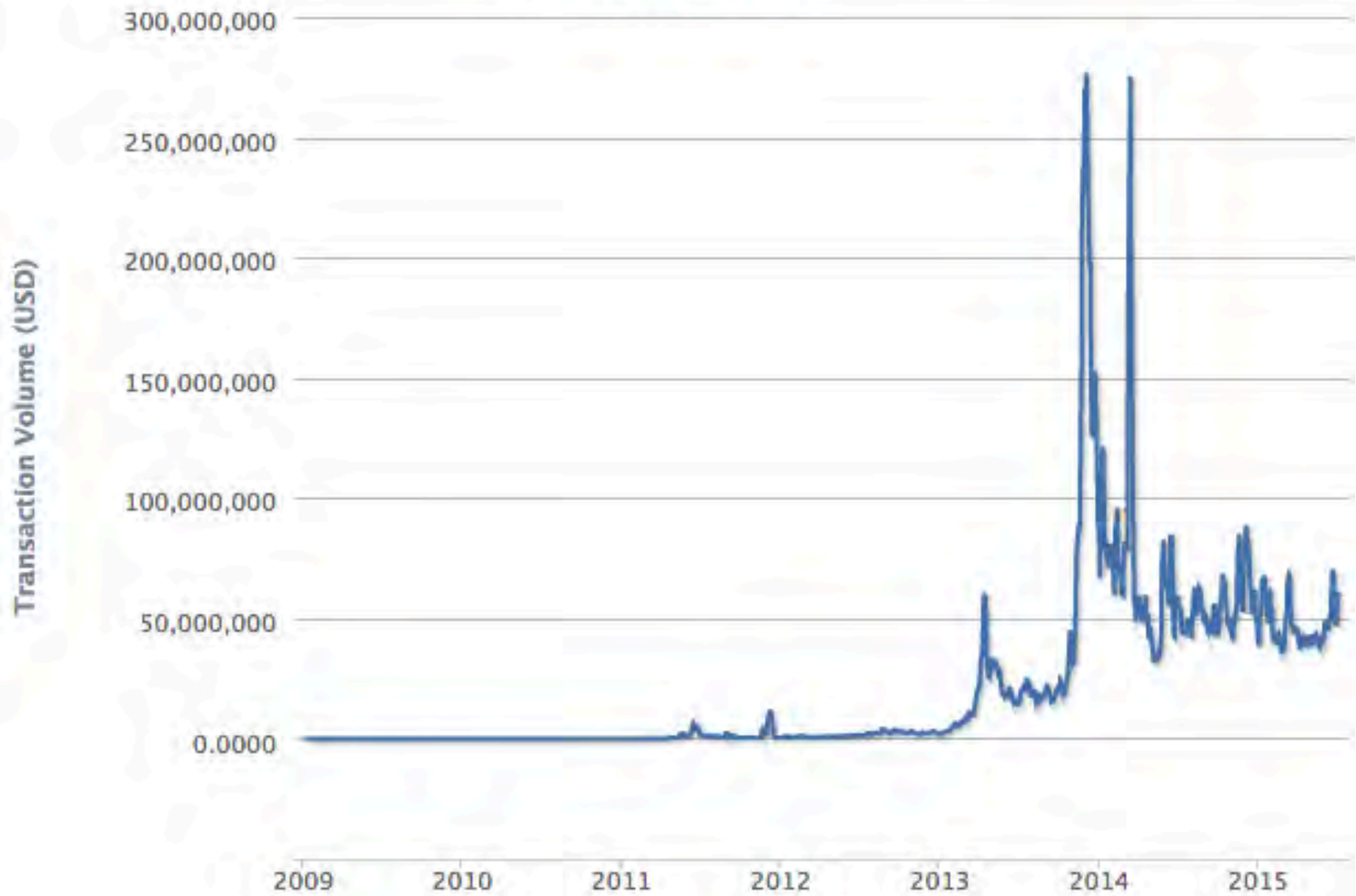
- Biteasy
- Blockr.io

# Current Statistics (05.Nov.2015)

➤ Total blocks	382,187
➤ Time between blocks	9.11 (minutes)
➤ Terahashes/s	354,753
➤ PetaFLOPS	5,920,057 (1 <sup>st</sup> top500 ~x100)
➤ Average transactions/h	8125
➤ Average fees/h	1.575 BTCs / 630 USD + ~10000 USD (coinbases)
➤ Bitcoins mined	
➤ Market cap	14,804,274 BTCs (70%) 5,834,808,906 USD 7,743,170,444 EUR 3,926,537,858 GBP

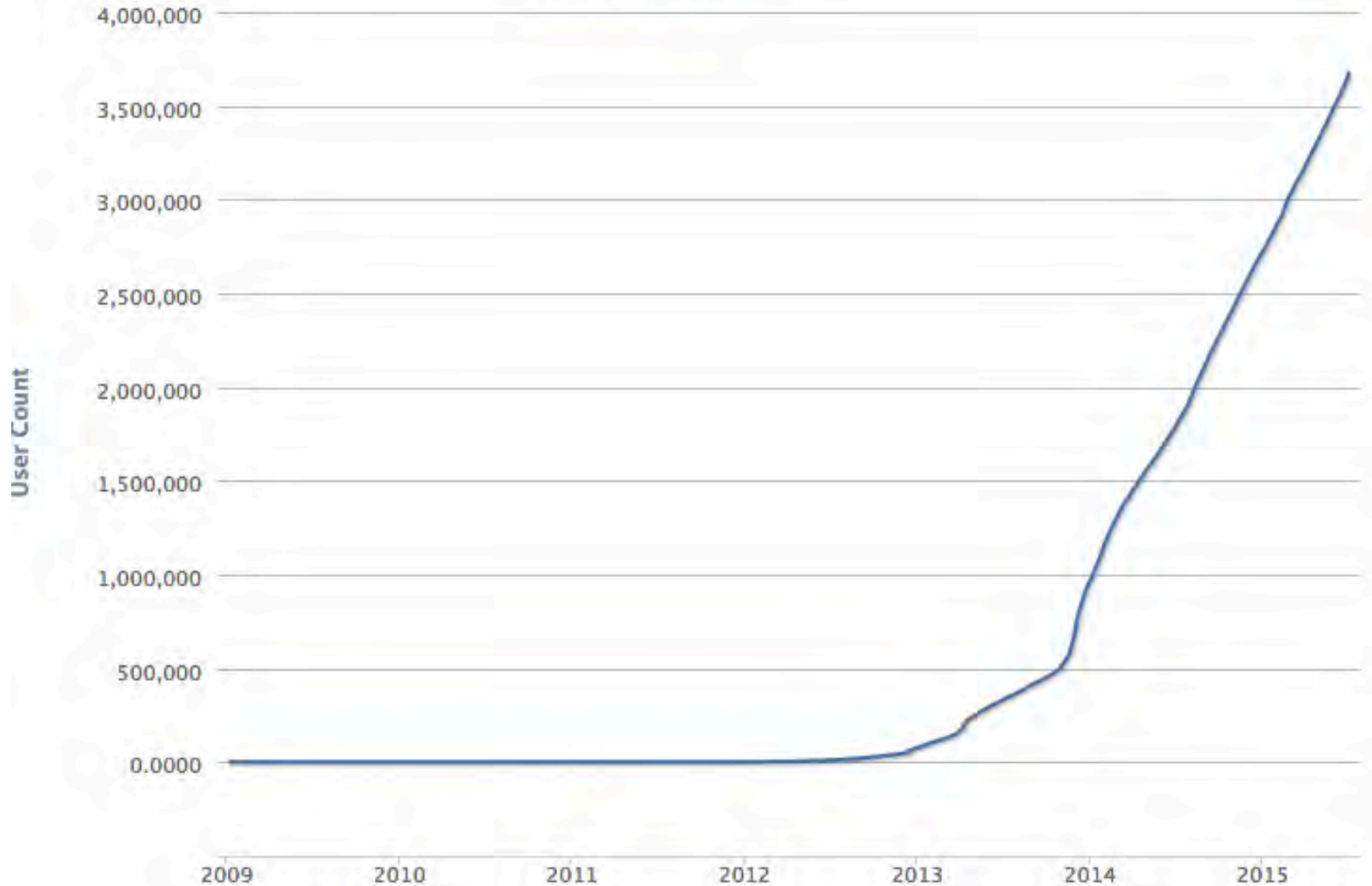
# Transaction Volumes

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



# Wallet Statistics

Source: blockchain.info



# Open Source Libraries and Resources

# Some Bitcoin Reference Sites

- Main source of information  
<https://en.bitcoin.it/>
- News  
<http://www.coindesk.com/>
- Historical data  
<http://winkdex.com/>
- Forum  
<https://bitcointalk.org/>
- Bitcoin explorer and Wallet  
<https://blockchain.info/>
- Twitter  
[@BitcoinByte](#)  
[@BitcoinMagazine](#)  
[@LetsTalkBitcoin](#)  
[@petertoddbtc](#)  
[@jgarzik](#)

# Some Bitcoin Libs/Apps

- Source code of reference Bitcoin client  
[github/bitcoin/bitcoin](https://github.com/bitcoin/bitcoin)
- RPC-based library – not maintained anymore  
[github/laanwj/bitcoin-python](https://github.com/laanwj/bitcoin-python)
- Low-level library does follows the bitcoin core  
[github/petertodd/python-bitcoinlib](https://github.com/petertodd/python-bitcoinlib)
- Alternative to main client - relies on original net stack  
[github/etotheipi/BitcoinArmory](https://github.com/etotheipi/BitcoinArmory)
- Out-dated but had great tools for dumping data out of db  
[github/gavinandresen/bitcointools](https://github.com/gavinandresen/bitcointools)
- Trading application with SMSs alerts  
[github/skylarweaver/Bitcoin-Trader](https://github.com/skylarweaver/Bitcoin-Trader)
- Simple ticker that collects data from multiple exchanges  
[github/rgho/bitcoin\\_prices\\_python](https://github.com/rgho/bitcoin_prices_python)
- Blockchain explorer  
[github/bitcoin-abe/bitcoin-abe](https://github.com/bitcoin-abe/bitcoin-abe)
- Automated arbitrage trading application  
[github/maxme/bitcoin-arbitrage](https://github.com/maxme/bitcoin-arbitrage)



# Generating a Custom Address

```
In [1]: # https://github.com/cdecker/pycoin
from pycoin import wallet
import random

while True:
    seed = hex(random.randint(0, 2**126))[2:-1]
    master = wallet.Wallet.from_master_secret(seed)
    addr = master.bitcoin_address()
    if addr[1:3].lower() == 'py':
        print 'Found key'
        print '    Seed:', seed
        print '  Address:', addr
        print '  PrivKey:', master.wif()
        break
```

Found key

Seed: 22605df3c42c63c26ca3f217bf5aacc7

Address: 1PyFVWBEY5JeDNwGwaq6gAPQLmpTikd2y5

PrivKey: KxHhPATrad6vvSK5Yg8DNMo9EhREUxiBDicLvoRiVDsy2tvZH6EN

# New Services



# New Services Enabled

- Zero/Low commission betting (WinCoins)
- Music made of transactions (Listen to Bitcoins)
- Smart contracts (Ethereum)
- Time stamping (Btproof)
- Micro-donations (Laybit)
- Tracking places of tension (Fiatleak)
- Virtual IPOs / Stock Market / Derivatives (mpex.co)
- Arbitrage between fiat and crypto currencies (btcarb)
- Machines that work for own profit/upgrades
  - e.g. self driving cars / delivery drones
- ... many many others ...



Thank you  
Have a cryptic day!

<http://anton.io>  
@roldao