# Bitcoin

## GNU Generation

Axel Angel

EPFL

April 2013

# Table of Contents

1. Introduction
2. Details
3. Outro

Bitcoin is a *digital* P2P **decentralized** chaotic maybe-illegal free-as-in-free-software *cyberpunk* **hype** cool rebel next-gen bubble[1] EXPERIMENTAL alternative *volatile* underground anonymous cryptographic potential currency

[1] but don't told anyone

Bitcoin was created for a money without intermediates. Third parties:

- Cost
- Have trust problems
- Can revert transactions (e.g.: non-reversible services)
- Single-point of failure

## Subjects

Bitcoin is:

- Decentralized (double spending)
- Cryptographic (SHA, ECDSA)
- Emerging (speculation)
- Open-source (and free)

Figure: Bitcoin logo

Overview:

- Avoid double-spending, all transactions are publicly announced.
- Majority of nodes witness transactions order
- Block of chains

Issuing: First transaction of mined block is self-reward.
$\Rightarrow$ Incentive to play by rules

Proof-of-work:

- SHA-256
- Target with adaptive difficulty (moving average)
- Block: (prev block hash, nonce, [ Tx, . . . ])

cannot be changed unless redoing work

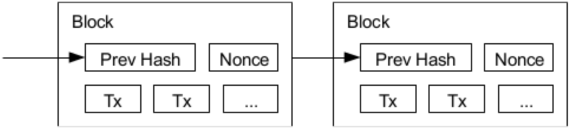


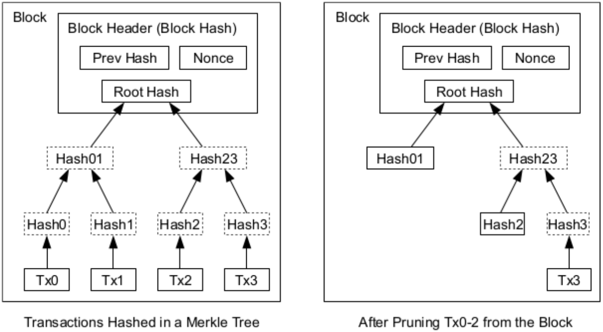
Figure: Blocks chain

Network:

(1) Transactions broadcast
(2) Nodes collect them into block
(3) Nodes mine
(4) When new block, broadcast
(5) Nodes check validity and mine next block if OK

Merkle Tree: Transactions in a Merkle Tree allows:

- Partial verification
- Keep only block header



Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

Figure: Merkle tree of a block

## Transactions and privacy

Transactions and privacy:

- Transaction is [ in ], [ out ] and in/out amount
- Privacy not main goal (public, multi-inputs)
- Can be anonymous

Script in transactions: Stack-based and simple language describe how owner can spend. Words: true/false, if/else, arithmetic, strings, crypto General case:

- Public key of destination + signature with this key

Other cases:

- Multi-signature (*n* among *m*)
- Can add messages (OP_DROP)
- Bounty for hard problems/puzzles?

```
scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash>
              OP_EQUALVERIFY OP_CHECKSIG
scriptSig: <sig> <pubKey>
```

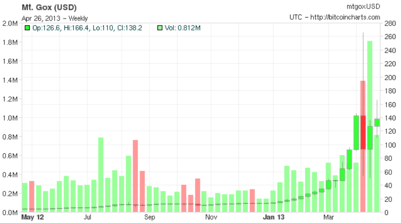
Mining:

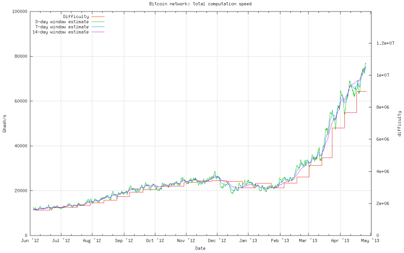
| Technology | Period | Speed | Example | Watts |
|---|---|---|---|---|
| CPU | 2009-2010 | 52 Mhash/s | Xeon x5690 | 170W |
| GPU | 2010-2011 | 825 Mhash/s | ATI 7970 | 214W |
| FPGA | 2011-2012 | 860 Mhash/s | ZTEX | 50W |
| ASIC | 2013+ | 10 Ghash/s | Block Erupter | 83W |

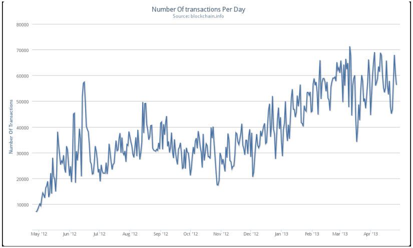
Current mining speed: 69'570 Ghash/s (883 Peta-FLOPS)

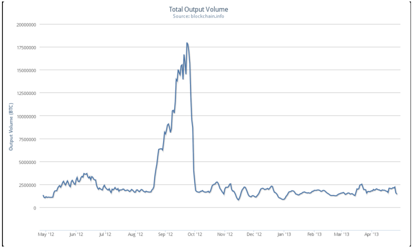
Mining details: Like a lottery. The SHA hash of block must be lower than the 256-bit target string (increment nonce): first to find wins. Probability to win per attempt: $2.59 \times 10^{-17}$.

## Because we love graphs


Mt. Gox (USD)
Apr 26, 2013 – Weekly
mtgoxUSD
UTC – http://bitcoincharts.com


Bitcoin network: total computation speed


Number Of transactions Per Day
Source: blockchain.info


Total Output Volume
Source: blockchain.info

## Conclusion

Do a useless conclusion now