Cryptocurrencies

Aggelos Kiayias

Historical:

- Stage 1 : barter

Commodity Money

grain

- Stage 2, some goods are elevated into money.

shells

gold

pepper

Standard Coins

- 700 BC, in Greece, first known standardized coins. (~ concurrently India, China)

Athens 10 drachma coin: ~450 BC

Paper money

- Bank issues notes which is representative of value (but has almost no intrinsic value).
- Gold standard: the bank notes are in some direct correspondence with gold stored in the bank.

Plastic Money

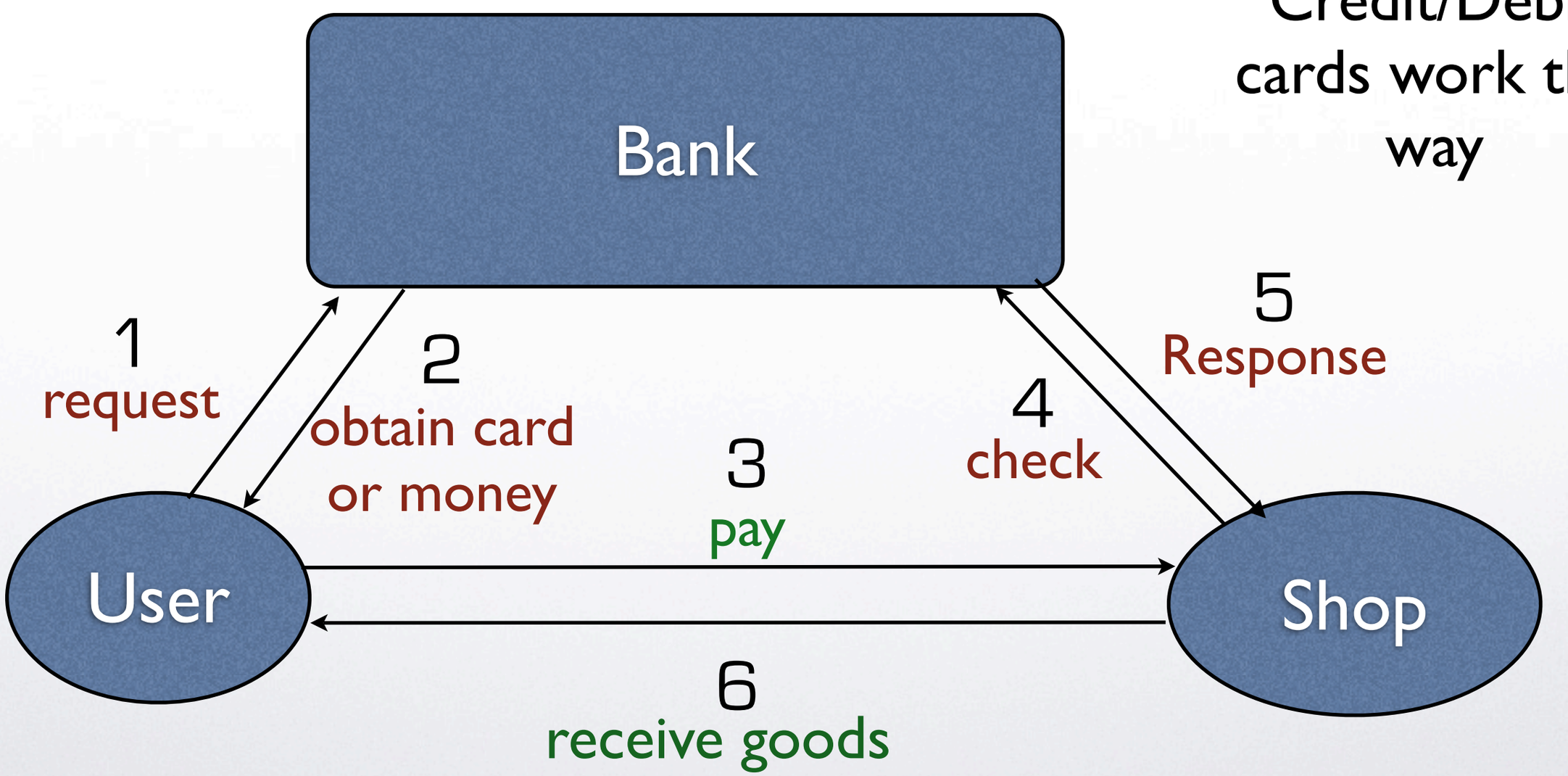
- Bank issues card with account information
- Possible security features:
  - smartcard: integrated circuit that may execute cryptographic operations.
- Card can be used to authorize transactions to/from account.

Online payment systems

- How do you prevent double-spending?

Centralized Systems

Credit/Debit cards work this way



Cryptocurrency Principles

- Trust Distribution: no entity controls the minting of money.
- Scarcity: there may be a limited amount of money.
- Difficulty: minting requires effort. *Cryptographic guarantee.*
- Verifiability: transactions are indisputable.
- Efficiency and Scalability.
- Pseudonymity/Anonymity/Traceability: ability or inability to track or classify transactions.

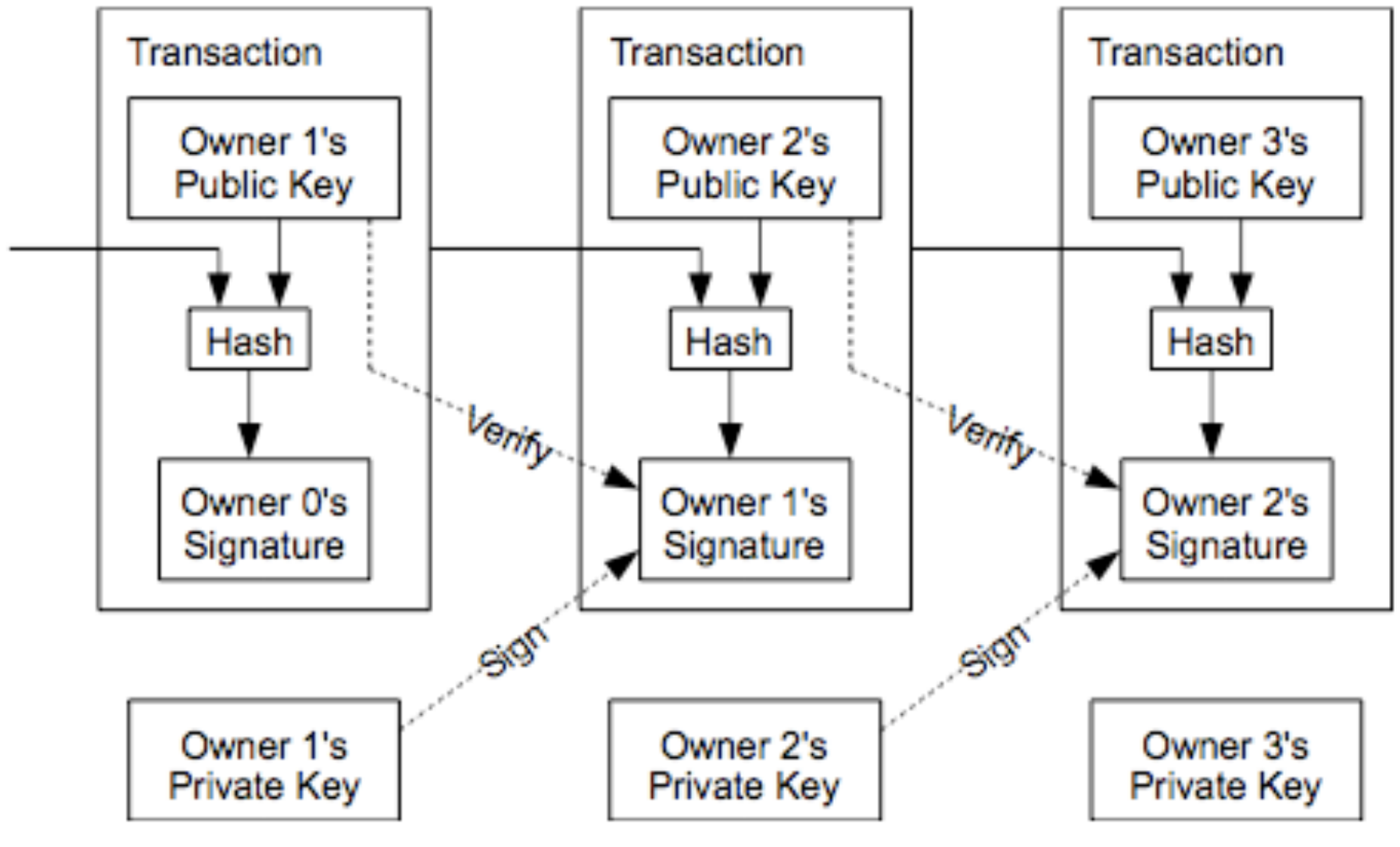
Bitcoin

- Bitcoin P2P network starts on Jan 2009.
- Relies on proofs of work.
- It distributively maintains a public ledger that keeps track of all transactions.
- Pseudonymous.
- Fixed amount of bitcoin (~21M).

Bitcoin vs. $


BitStamp (USD)
May 22, 2015 – Daily
Op:235, Hi:237.2, Lo:234.8, Cl:234.8
Vol: 3.127K
bitstampUSD
UTC – http://bitcoincharts.com
140K
130K
120K
110K
100K
90K
80K
70K
60K
50K
40K
30K
20K
10K
0K
1200
1100
1000
900
800
700
600
500
400
300
200
100
0
Oct 11
Jan 12
Apr
Jul
Oct
Jan 13
Apr
Jul
Oct
Jan 14
Apr
Jul
Oct
Jan 15
Apr

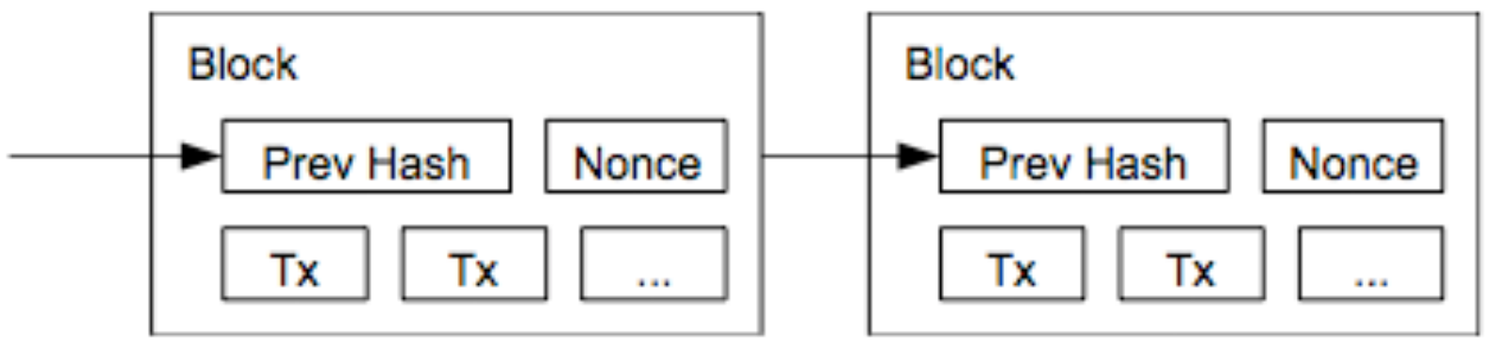
BitCoins



Transferring ownership of an asset

Bitcoin Transaction Blocks

Distributively maintains the transaction history



Generating a valid block requires a *proof of work*.

SHA256(Block) should satisfy a certain constraint
(e.g., starts with 0000000)

Transaction

Short link: http://blockexplorer.com/t/8n65mn2mCM

Hash[?]: cd3b641faa72bab1ea12ef5579dff58d57ee3858a5179bef3e2cc28da826752f
Appeared in block 281220 (2014-01-18 23:28:56)
Number of inputs[?]: 1 (Jump to inputs)
Total BTC in[?]: 0.6874
Number of outputs: 2 (Jump to outputs)
Total BTC out[?]: 0.6374
Size[?]: 226 bytes
Fee[?]: 0.05
Raw transaction[?]

Inputs[?]

Previous output (index)[?]	Amount[?]	From address[?]	Type[?]	ScriptSig[?]
5a6ac66824cc...:1	0.6874	1DCBnn9NDmY76pj4KhoxKVvCbfq1H5d1vk	Address	3045022100cc8363ab2545232fa99fd63eacfb2c 03e431e7cc0e60896ccba0409e2c68903bd143c

Outputs[?]

Index[?]	Redeemed at input[?]	Amount[?]	To address[?]	Type[?]	ScriptPubKey[?]
0	Not yet redeemed	0.292	1JMnjTW9XAd6kNs27zoPyEyQ2TW2FDabq3	Address	OP_DUP OP_HASH160 be68a1fa3e1e2cf6311c92935e0597ac83bd86b8 OP_EQUALVERIFY OP_CHECKSIG
1	Not yet redeemed	0.3454	16qpcjHx4UsvWsbTrhjREGNHQShACeCUf	Address	OP_DUP OP_HASH160 011ad5602f426e550aaddd8c8cab61f818f34329 OP_EQUALVERIFY OP_CHECKSIG

From http://blockexplorer.com

Block 281220?

Short link: http://blockexplorer.com/b/281220

Hash?: 0000000000000000137167c3a9b843035ad75418bba5f4f3bde661be5a955f6aa

Previous block?: 0000000000000000257a8157e5c2948b5511822640f53e2799a443ad5ec4a94a9

Time?: 2014-01-18 23:28:56

Difficulty?: 1 789 546 951.05324 ("Bits"?: 19026666)

Transactions?: 174

Total BTC?: 1625.59780063

Size?: 89.664 kilobytes

Merkle root?: 9f3efc5d2433864dae18148c88d9c2ab58e094baaa78615845c3641e123c0e3a

Nonce?: 3102274478

Raw block?

Transactions

Transaction?	Fee?	Size (kB)?	From (amount)?	To (amount)?
4197bfa3a6...	0	0.168	Generation: 25 + 0.08187781 total fees	18d3HV2bm94UyY4a9DrPfoZ17sXuiDQq2B: 25.08187781
cd3b641faa...	0.05	0.226	1DCBnn9NDmY76pj4KhoxKVvCbfq1H5d1vk: 0.6874	1JMnjTW9XAd6kNs27zoPyEyQ2TW2FDabq3: 0.292 16qpcjHx4UsvWsbTrhjREGNHQShACeCUf: 0.3454
6c2fcab612...	0.001	0.258	1JVZM5XqDULZce6yGqR9u435YmfWjqbg8w: 1	1GPyn2UfrvnZi3BjBoKSb9byfMbJKx6yeN: 0.97318037 18meAufCoMuLp1wjG7L27oP183odtn3EKL: 0.02581963
ef8118a3ef...	0.0005	0.223	15v1YuQSerr5T27JKCNmDgQRHaNwfUnGn9: 0.01	16NwGDZ4LQzQZQfC25nK4VwGJXXJuDcSn2: 0.0095
2009870a11...	0.0005	0.226	1Hk7t7kqoiA9c2Q3bJBa3JTrsNkQ2AFdDq: 441.8540463	1JnpeePZ7XL9JLEqRh1KpZ7cUZPGSPTx7g: 441.8046463 12o5SgJWUGXuPr1MSeRqSM9s9ijMPKh33b: 0.0489

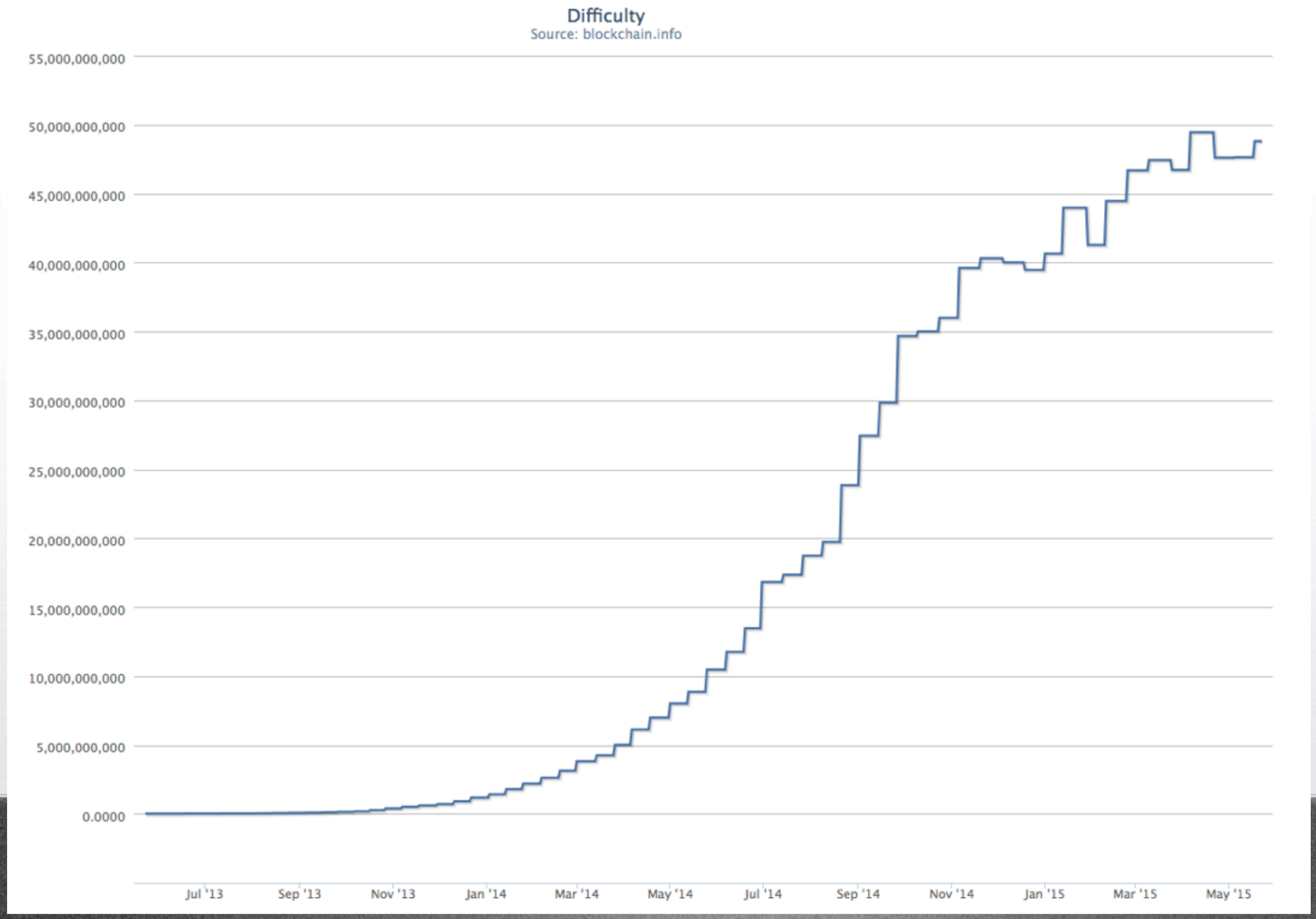
Block Difficulty

- The difficulty level determines how hard it is to mine blocks.
- The difficulty is adjusted every 2016 blocks based on the time it took to find these blocks.
- Desired rate: 1 block per 10 minutes. Therefore 2016 blocks would have to take 2 weeks.
- Difficulty *D* should be calculated as a proportion of how much over or under 2 weeks it took to calculate 2016 blocks.

Adjusting Difficulty

- Difficulty level 1: (<u>32</u> 0's|| <u>16</u> 1's || <u>208</u> 0's) = *A* ← First block has to hash below this
- Difficulty level *D* would have as target (*A*/*D*)
- Expected number of hashes to find a block with difficulty *D* is equal to $$\frac{2^{256}}{A/D} = \frac{D \cdot 2^{48}}{2^{32}-1} = H$$
- Next *D* is calculated: let *H* be the average number of hashes the network computes in 10 min (over the previous 2016 blocks). Solve for D.

Bitcoin difficulty



current difficulty $\approx 2^{67}$

LiteCoin

- Similar to bitcoin but
  - block is mined every ~ 2.5 minutes
  - it employs *scrypt* as the proof of work scheme (rather than "SHA256 <")
- scrypt is designed to be much harder to optimize in ASIC / FPGA (contrary to SHA256).

ZeroCoin

- In bitcoin/*coin it is possible to link all transactions and “follow the money”
- Zerocoin uses more complex cryptographic techniques than bitcoin to make transactions unlinkable.
- It still maintains the integrity of the ledger through the use of zero-knowledge proofs.

From http://coinmarketcap.com

4.07.14

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Market Cap Graph (7d)
1	Bitcoin	$ 8,193,829,645	$ 631.31	12,979,050 BTC	$ 22,725,573	-2.91 %	
2	Litecoin	$ 235,225,979	$ 7.87	29,888,304 LTC	$ 1,803,307	-2.55 %	
3	Nxt	$ 58,277,169	$ 0.058277	999,996,993 NXT*	$ 216,563	-6.00 %	
4	Darkcoin	$ 34,369,317	$ 7.74	4,439,097 DRK	$ 498,320	+4.23 %	
5	Peercoin	$ 32,997,592	$ 1.53	21,532,213 PPC	$ 184,192	-6.52 %	
6	Ripple	$ 25,442,200	$ 0.003254	7,817,888,647 XRP*	$ 220,676	-4.60 %	
7	Dogecoin	$ 19,861,471	$ 0.000232	85,680,831,277 DOGE	$ 446,985	+5.53 %	
8	Namecoin	$ 17,495,607	$ 1.91	9,183,032 NMC	$ 181,992	-4.82 %	
9	Mastercoin	$ 11,100,923	$ 19.71	563,162 MSC*	$ 362	+7.19 %	
10	BlackCoin	$ 9,640,912	$ 0.129263	74,583,439 BC*	$ 42,749	-1.99 %	

22.05.15

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$ 3,349,186,008	$ 236.05	14,188,400 BTC	$ 16,084,100	0.41 %	
2	Ripple	$ 210,567,404	$ 0.006599	31,908,551,587 XRP *	$ 198,354	0.24 %	
3	Litecoin	$ 61,554,304	$ 1.57	39,239,054 LTC	$ 1,766,290	7.25 %	
4	Dash	$ 15,369,081	$ 2.85	5,387,745 DASH	$ 45,793	-1.64 %	
5	Stellar	$ 13,890,789	$ 0.002872	4,837,097,306 STR *	$ 18,666	2.86 %	
6	Dogecoin	$ 13,677,392	$ 0.000137	99,498,716,423 DOGE	$ 184,472	5.07 %	
7	BitShares	$ 13,327,218	$ 0.005306	2,511,953,117 BTS *	$ 330,042	30.24 %	
8	Nxt	$ 11,357,267	$ 0.011357	999,997,096 NXT *	$ 59,742	2.62 %	
9	BanxShares	$ 8,231,356	$ 1.44	5,708,331 BANX *	$ 13,793	0.55 %	
10	MaidSafeCoin	$ 8,076,793	$ 0.017847	452,552,412 MAID *	$ 6,746	4.68 %	

Bitcoin can be more than a payment system

- Distributed consensus mechanism that works without identity infrastructure. May be used for:
  - Any kind of registry (e.g., land registry - case of Honduras land title registry http://in.reuters.com/article/2015/05/15/usa-honduras-technology-idINKBN0O01V720150515)
  - Document time stamping services.
  - Any computation between parties that requires some accountability.

Ethereum

- A ledger where *smart contracts* can also receive and generate transactions.

Here is the implementation of a "Bank" in Ethereum:

```
def init():
    self.storage[msg.sender] = 10000
def code():
    to = msg.data[0]
    from = msg.sender
    value = msg.data[1]
    if self.storage[from] >= value:
        self.storage[from] = self.storage[from]  - value
        self.storage[to] = self.storage[to] + value
```