

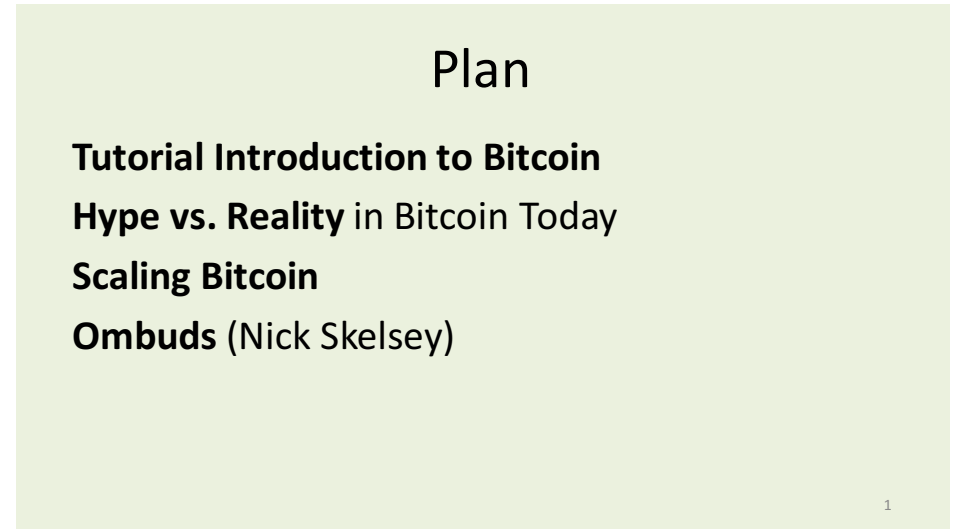
Trick or Treat?
*Bitcoin for Non-Believers,
Cryptocurrencies for
Cypherpunks*

David Evans
University of Virginia
www.cs.virginia.edu/evans
bitcoin-class.org

DC Area Crypto Day
All Hallows' Eve²
Johns Hopkins University

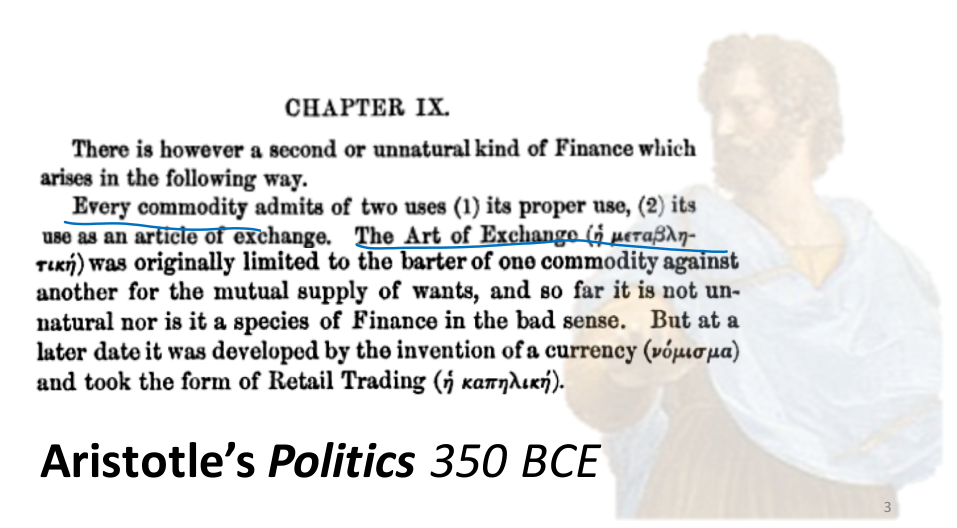


What is money?



Plan

- Tutorial Introduction to Bitcoin**
- Hype vs. Reality in Bitcoin Today**
- Scaling Bitcoin**
- Ombuds (Nick Skelsey)**



CHAPTER IX.

There is however a second or unnatural kind of Finance which arises in the following way.

Every commodity admits of two uses (1) its proper use, (2) its use as an article of exchange. The Art of Exchange (*ἡ μεταβλητικὴ*) was originally limited to the barter of one commodity against another for the mutual supply of wants, and so far it is not unnatural nor is it a species of Finance in the bad sense. But at a later date it was developed by the invention of a currency (*νόμισμα*) and took the form of Retail Trading (*ἡ καπηλική*).

Aristotle's *Politics* 350 BCE

Fiat Currency

fi·at

/'fiət, 'fē, ät/ ◀▶

noun

a formal authorization or proposition; a decree.

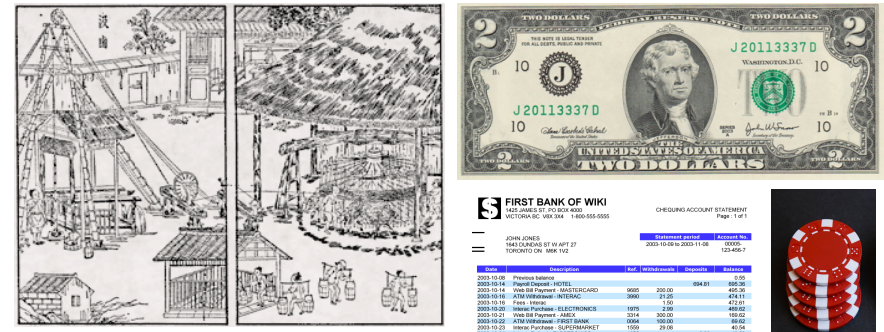
"adopting a legislative review program, rather than

synonyms: **decree, edict, order, command, comman-**
mandate, dictum, diktat

"a political union imposed through imper

• an arbitrary order.

"the appraisal dropped the value from \$75,000 to
bureaucratic fiat"



With a strong enough army, anything can be a fiat currency

Centralized Digital Currency



Trusted Bank

Account No.	Owner's Identify	Value
3022493	Alice	2033.23
3022494	Bob	85733.03
3022495	Colleen	24331.77
3022496	Dave	0.01 24000

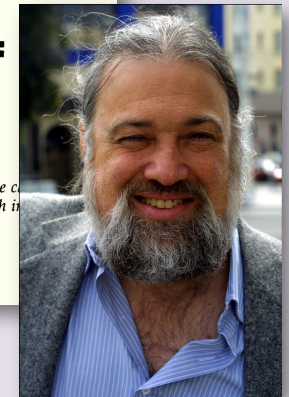
ARTICLES

SECURITY WITHOUT IDENTIFICATION: TRANSACTION SYSTEMS TO MAKE BIG BROTHER OBSOLETE

The large-scale automated transaction systems of the near future could be designed to protect the privacy and maintain the security of both individuals and organizations.

DAVID CHAUM

Communications of the ACM
October 1985



ARTICLES

SECURITY & TRANSACTIONS: THE BIG BROTHER

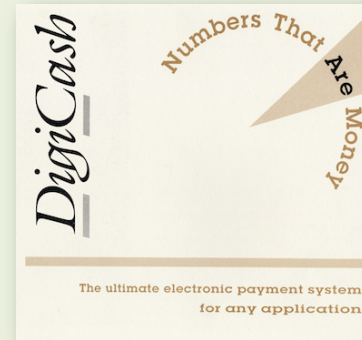
The large design and org

DAVID CHAUM

Communications of the ACM
October 1985

Computerization is robbing individuals of the ability to monitor and control the ways information about them is used. As organizations in both the private and the public sectors routinely exchange such information, individuals have no way of knowing if the information is inaccurate, obsolete, or otherwise inappropriate. The foundation is being laid for a dossier society, in which computers could be used to infer individuals' life-styles, habits, whereabouts, and associations from data collected in ordinary consumer transactions. Uncertainty about whether data will remain secure against abuse by those maintaining or tapping it can have a "chilling effect," causing people to alter their observable activities. As computerization becomes more pervasive, the potential for these problems will grow dramatically.

First Wave Cryptocurrency



David Chaum

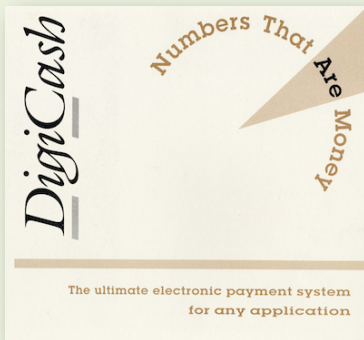
WIRED

E-Money (That's What I Want)

The killer application for electronic networks isn't video-on-demand. It's going to hit you where it really matters - in your wallet. It's not only going to revolutionize the Net, it will change the global economy.
By Steven Levy



First Wave Cryptocurrency



David Chaum

WIRED

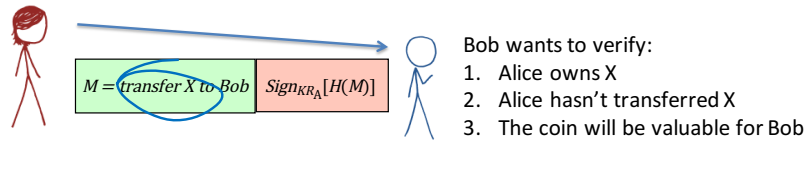
E-Money (That's What I Want)

The killer application for electronic networks isn't video-on-demand. It's going to hit you where it really matters - in your wallet. It's not only going to revolutionize the Net, it will change the global economy.
By Steven Levy

Bankrupt, 1998

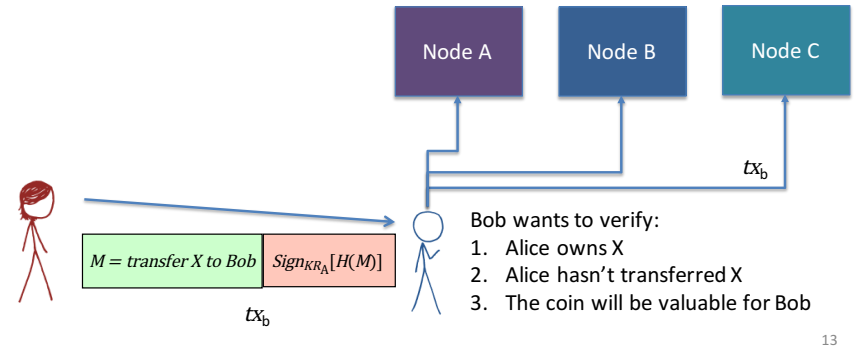


Double Spending Challenge

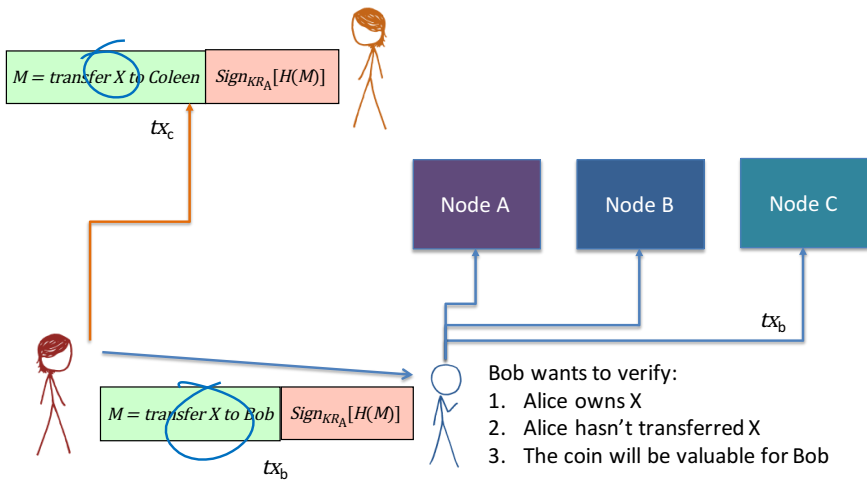


12

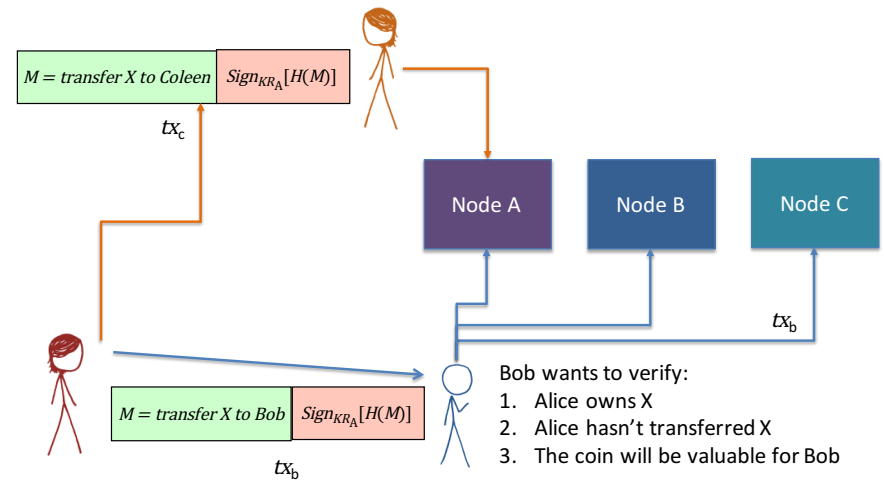
Double Spending Challenge



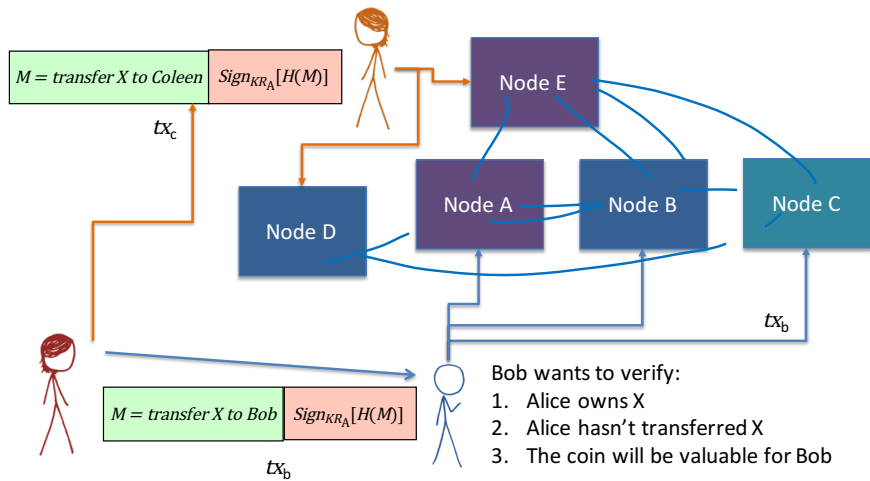
13



14



15



16

Satoshi's Solution

Bitcoin P2P e-cash paper

Satoshi Nakamoto [satoshi at vistamail.com](mailto:satoshi@vistamail.com)
 Fri Oct 31 14:10:00 EDT 2008

- Previous message: [Fw: SHA-3 lounge](#)
- Messages sorted by: [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

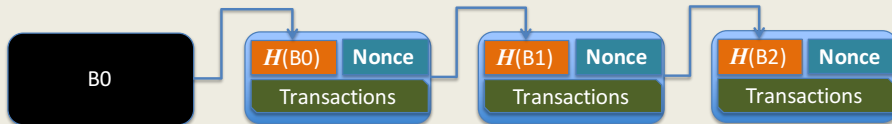
The paper is available at:
<http://www.bitcoin.org/bitcoin.pdf>

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution.

Blockchain



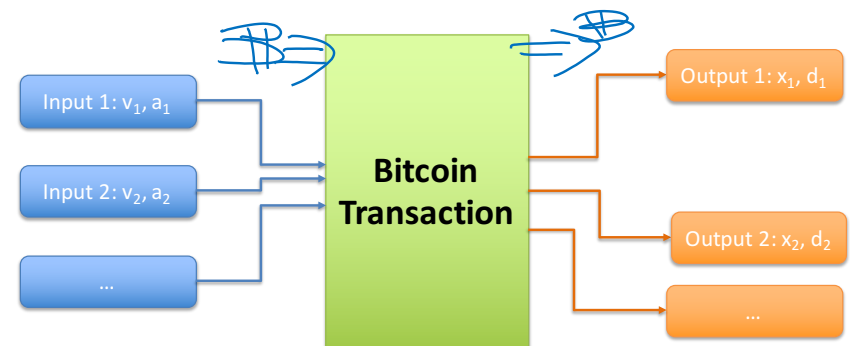
Distributed ledger maintained by network of untrusted nodes

Blocks added require proof-of-work

Node's agree to consensus: longest (most difficult) chain

Incentives designed to encourage network nodes to:
Validate and record transactions
Spend effort on extending consensus chain

18



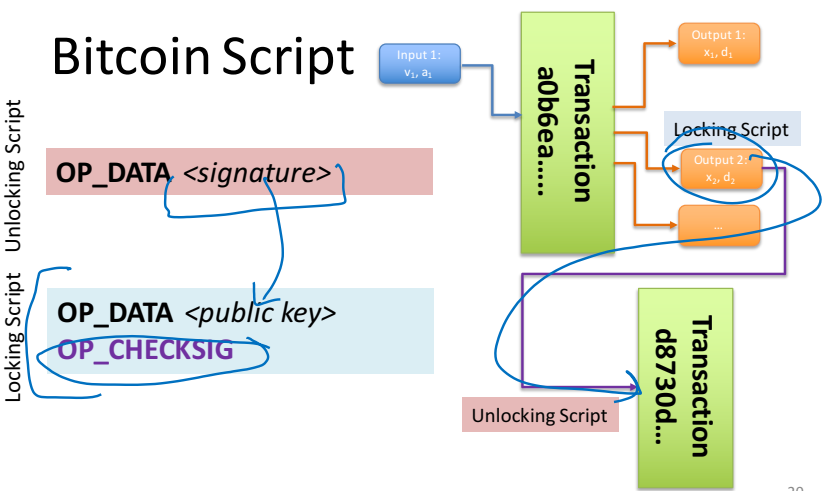
$$\text{transaction fees} = \text{sum}(\text{input values}) - \text{sum}(\text{output values})$$

(must be non-negative for valid transaction)

19

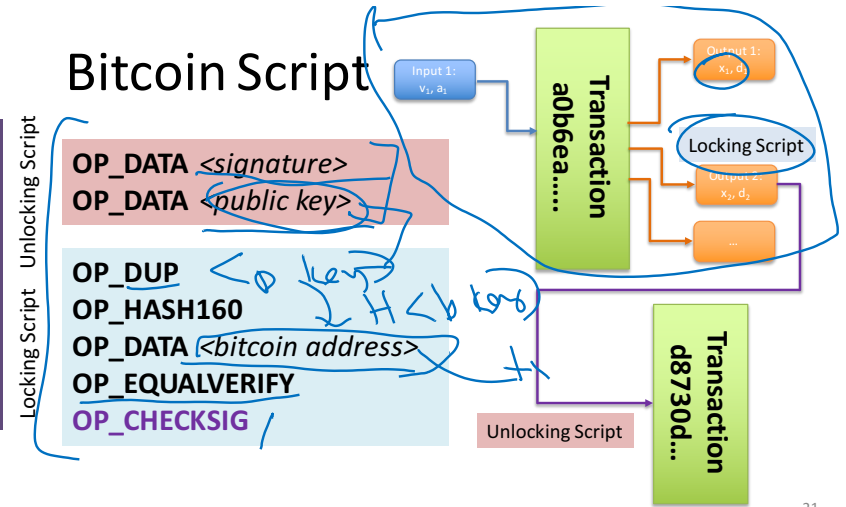
If Bitcoin Address were just public key

Bitcoin Script



Bitcoin Address = H(public key)

Bitcoin Script



OP_RETURN (until July 2010)

<https://github.com/bitcoin/bitcoin/blob/v0.1.5/script.cpp#L170>

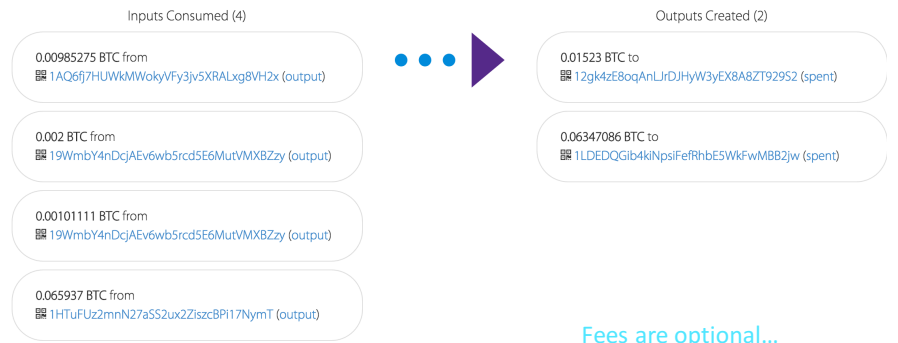
```

170     case OP_RETURN:
171     {
172         pc = pend;
173     }
break;

```

Universal Unlocking Script!
OP_DATA 1
OP_RETURN

Example Transaction



Transaction View information about a bitcoin transaction

3a1b9e330d32fe1ee42f8e66420d22be978bbe0dc5862f17da9027c9be118c4

17dxM1cdeXPL1-ZNJDAPwU2C4H9XV5VqR (50,000 BTC - Output)
 19H4PcYpCw@FUh5J1pna5B9w9z2ar1cQ4 (50,000 BTC - Output)
 1Lfd5wWnU7Hk3Kp8v54f6TMD1CaHq1Y (50,000 BTC - Output)
 15c9gw9EU7BsdZvFhEcdvQDZv1hH26Zos (50,000 BTC - Output)
 1FbaQntU2BAWYzvaRf9SmLEDMEUwPvG1 (50,000 BTC - Output)
 1MyGxTelWmjNkYBf85JPKL5vnhTRU7Hd (50,000 BTC - Output)
 14yXkRDM6E1Bbm7DMnuv1PKUk8K65J4y (50,000 BTC - Output)
 191sZn1o7WZ1baNqUmRow6RPp293gbeLW (42,000 BTC - Output)
 1Q4EpJ6eaXDV1mEhX7JgusBUGN4GBcM5v (50,000 BTC - Output)

→ 1Hzpk4eXTbrAfmH2noWkrqx06wH6qncd - (Spent) 17,757.57575758 BTC
 1eHhgWbVqu8YhwMQPhQ668HPjT1pvZGSP - (Spent) 424,242.42424242 BTC

442,000 BTC

Summary		Inputs and Outputs	
Size	1698 (bytes)	Total Input	442,000 BTC
Received Time	2011-06-23 06:50:15	Total Output	442,000 BTC
Included In Blocks	132749 (2011-06-23 06:50:15 + 0 minutes)	Fees	0.00 BTC
Confirmations	248416 Confirmations	Estimated BTC Transacted	424,242.42424242 BTC

24

Exhibit B

SEALED BY COURT ORDER

ORIGINAL FILED

UNITED STATES DISTRICT COURT
Northern District of California

Richard W. McKing
Carl Mark Force II, et al

Case No. 8-15-70370

CRIMINAL COMPLAINT

MEJ

TECHNOLOGY

Former U.S. Agents Charged for Bitcoin Theft During Silk Road Probe

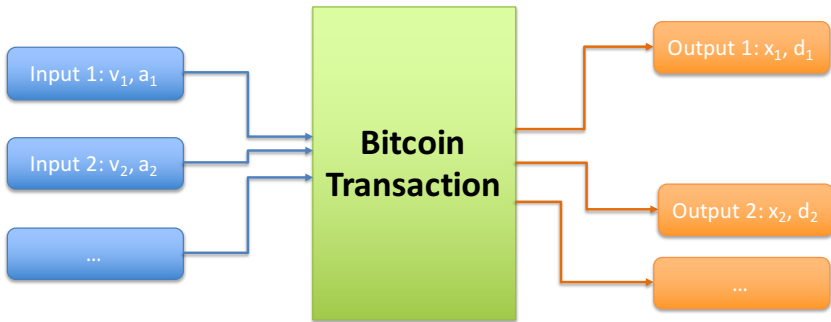
By REUTERS MARCH 30, 2015 2:02 PM EDT.

(Reuters) - The U.S. Justice Department announced charges on Monday against two former federal agents accused of stealing the digital currency bitcoin during the investigation of the underground drug marketplace Silk Road.

Carl Force, a former Drug Enforcement Administration agent, and Shaun Bridges, a special agent with the Secret Service, were charged in a criminal complaint filed in San Francisco federal court with offenses including wire fraud and money laundering.

All times are UTC (Coordinated Universal Time)

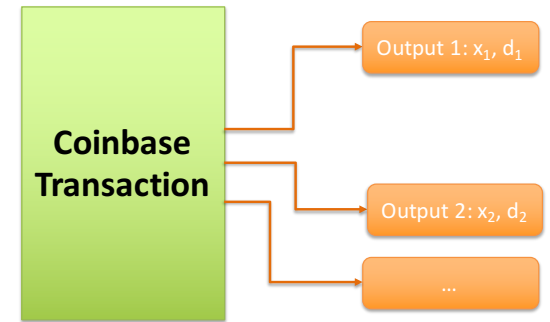
25



transaction fees = sum(input values) – sum(output values)
 (must be non-negative for valid transaction)

How is new bitcoin created?

26



sum(output values) ≤ sum(transaction fees) + mining reward

$$\text{mining reward} = \frac{50 \text{ BTC}}{2^{\text{floor}(\text{block number} / 210,000)}}$$

27

Block #381166

BlockHash 00

Summary

Number Of Transactions	1218	Difficulty	62253982449.76082
Height	381166 (Mainchain)	Bits	1811a954
Block Reward	25 BTC	Size (bytes)	692196
Timestamp	Oct 29, 2015 11:14:13 PM	Version	3
Merkle Root	a89ab0a78cf1125851b8088actab9...	Nonce	620980862
Previous Block	381165		

Transactions

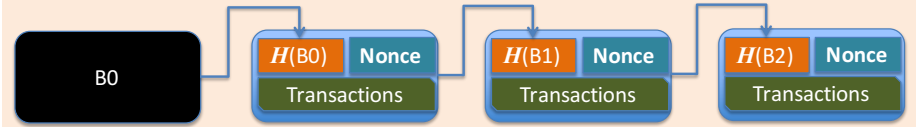
81606678cd9071582792a1dd6fb852d3c4a82cd4c7fd02a4d0f5db207060370a mined Oct 29, 2015 11:14:13 PM

No Inputs (Newly Generated Coins) > 152f1muMCNa7gpXYhYAQ61hxEGacmncB 25.23965915 BTC (U)

1 CONFIRMATIONS 25.23965915 BTC

28

Bitcoin's Proof-of-Work



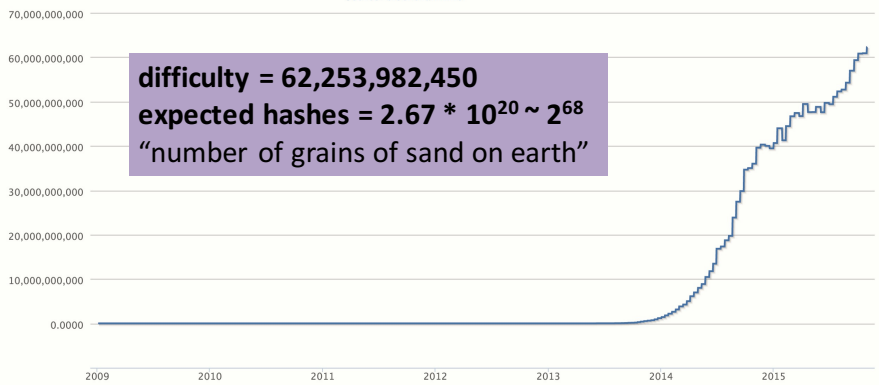
Find a nonce x such that:

$$\text{SHA-256}(\text{SHA-256}(r \parallel x)) < T/d$$

r = header includes $H(\text{previous block})$
 root of Merkle tree of transactions

29

Difficulty
 Source: blockchain.info



30

Actual Bitcoin Block

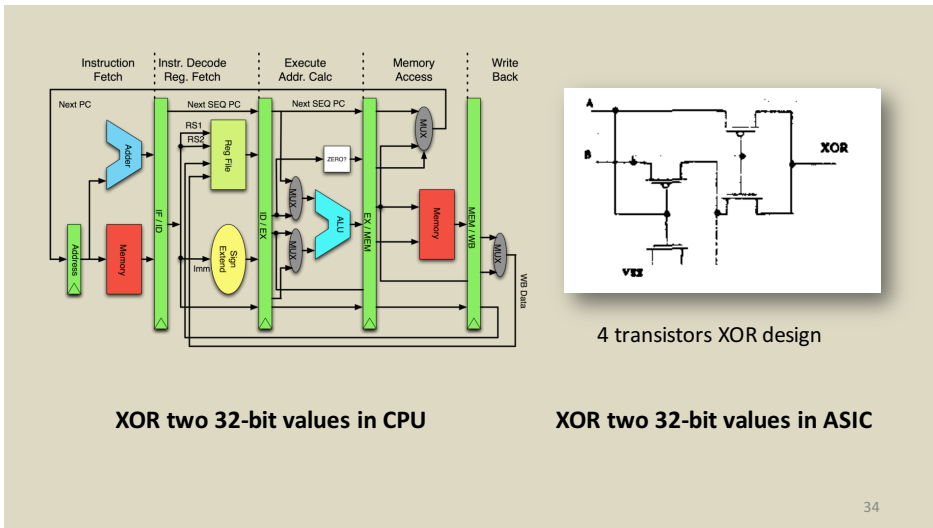
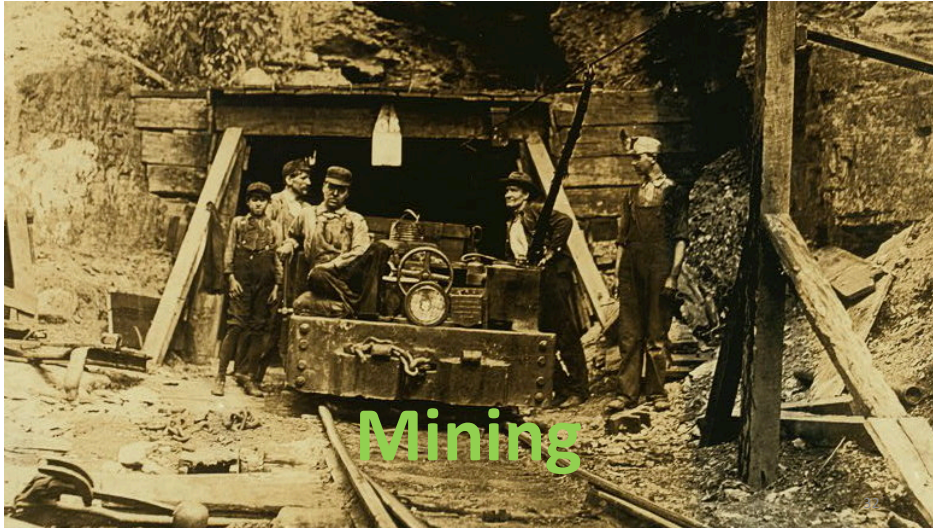
Block Headers

Block headers are sent in a headers packet in response to a getheaders message.

Field	Size	Description	Data type	Comments
version	4	Block version information, based upon the software version creating this block	uint32_t	
prev_block	32	The hash value of the previous block this particular block references	char[32]	
merkle_root	32	The reference to a Merkle tree collection which is a hash of all transactions related to this block	char[32]	
timestamp	4	A timestamp recording when this block was created (Will overflow in 2106 ^[2])	uint32_t	
bits	4	The calculated difficulty target being used for this block	uint32_t	
nonce	4	The nonce used to generate this block... to allow variations of the header and compute different hashes	uint32_t	
txn_count	1	Number of transaction entries, this value is always 0	var_int	

https://en.bitcoin.it/wiki/Protocol_documentation#Block_Headers

31




ASIC https://en.bitcoin.it/wiki/Mining_hardware_comparison

Be sure to research any of these vendors and machines intensely before spending any money.

Product	Advertised Mhash/s	Mhash/J	Mhash/s/\$	Watts	Price (USD)	Currently shipping	Comm ports	Dev-friendly
AntMiner S1 [1]	180,000	500	800	360	299[2]	Discontinued	Ethernet	GPL infringement
AntMiner S2 [3]	1,000,000	900	442	1100	2259	Discontinued	Ethernet	GPL infringement
AntMiner S3 [4]	441,000	1300	1154	340	382[2]	Discontinued	Ethernet	GPL infringement
AntMiner S4 [5]	2,000,000	1429	1429	1400	1400	Discontinued	Ethernet	GPL infringement
AntMiner S5 [6]	1,155,000	1957	3121	590	370	Discontinued	Ethernet	GPL infringement
AntMiner S5+ [7]	7,722,000	2247	3347	3,436	2,307	Yes	Ethernet	GPL infringement
AntMiner S7 [8]	4,860,000	4000	2666	1,210	1,823	No	Ethernet	GPL infringement

BITMAIN Products Auctions Support News About Us



AntMiner S5+ Batch 1
 Speed: 7.722TH/S
 Weight: 11 kg
 Price: 2307 USD (10.016 BTC)
 Sold Out

0


Description

BITMAIN ANTMINER S5+: The New Standard

Bitmain is proud to introduce our newest iteration of AntMiner, the S5+. This model is comprised of three hashing modules, each of which is approximately the same form factor as the S5, with the addition of an extra hashing board located in the middle of each module. The new design squeezes 144 BM1384 chips into the same area that the S5 fit only 60 chips into.

Shipping will be within 72 hours after receiving full payment.

BITMAIN Products Auctions Support News About Us



AntMiner S5+ Batch 1
 Speed: 7.722TH/S

Comparison

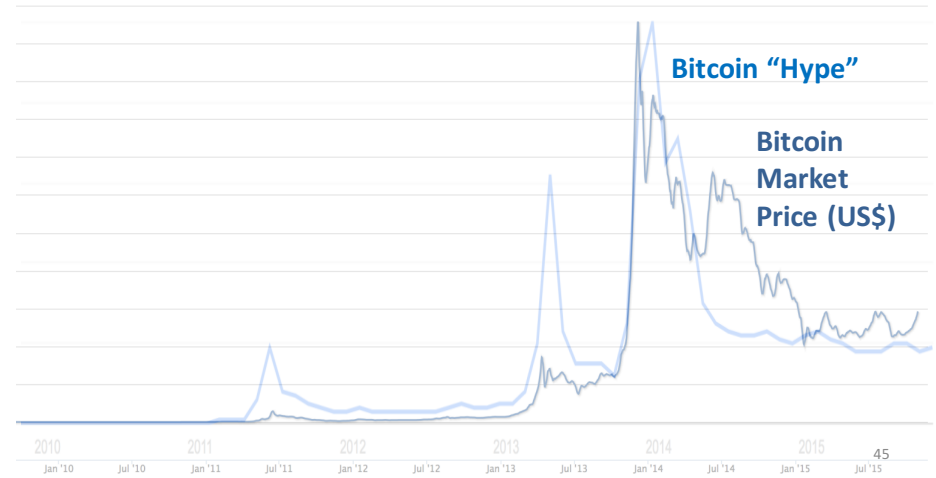
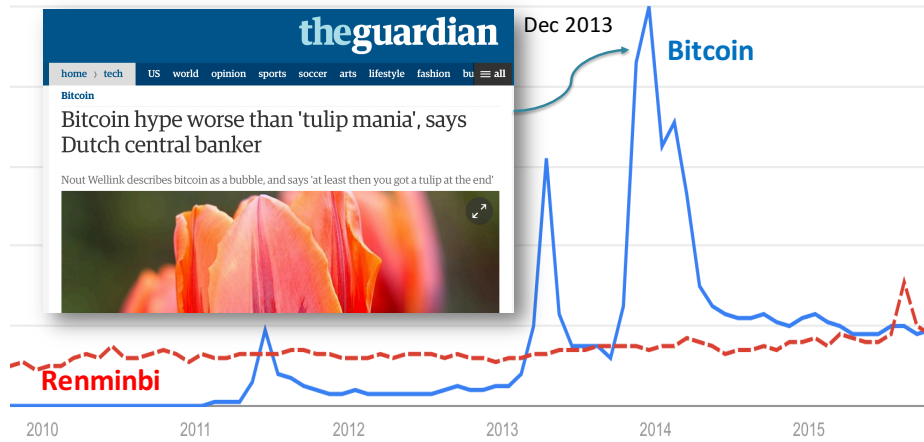
	AntMiner S4+	AntMiner S5	AntMiner S5+
Chip	204x BM1382	60x BM1384	432x BM1384
Hashrate	2570GH/s	1155GH/s	7722GH/s
Power Draw	1500W	590W	3436W
Power Efficiency	0.58J/GH	0.51J/GH	0.445J/GH
Dimensions(mm)	432*442*133	298*137*155	275*372*155
Weight(boxed)	14.4kg	3.5kg	11kg

144 BM1384 chips into the same area that the S5 fit only 60 chips into.

Shipping will be within 72 hours after receiving full payment.



Google Trends



Reality Check

Bitcoin "Market Capitalization" = Number of Bitcoins × Market Price
= 14,777,800 × \$314 = **\$4.64B**



What does a \$4.64B Market Cap company look like?

VCA is the leading provider of pet health care services in the country.

VCA is the leading provider of pet health care services in the country with a nationwide clinical laboratory system and over 600 free-standing animal hospitals in 41 U.S. states and Canada. [More...](#)

You are considering selling your hospital? See what options VCA offers you. [More...](#)

Investor Relations
WOOF
NASDAQ Symbol

NASDAQ: WOOF
Market Cap: \$4.4B
Average daily trading: \$35M

Bitcoin
Market Cap: \$4.6B
Average daily transactions: \$50M (?)
Average daily US\$ exchange value: \$3M

© 2015 VCA Inc.
VCA White Corporation has moved to [vcaig](#)

48

Can Bitcoin Scale?



49

<https://github.com/bitcoin/bitcoin/blob/master/src/consensus/consensus.h>

```

1 // Copyright (c) 2009-2010 Satoshi Nakamoto
2 // Copyright (c) 2009-2014 The Bitcoin Core developers
3 // Distributed under the MIT software license, see the accompanying
4 // file COPYING or http://www.opensource.org/licenses/mit-license.php.
5
6 #ifndef BITCOIN_CONSENSUS_CONSENSUS_H
7 #define BITCOIN_CONSENSUS_CONSENSUS_H
8
9 /** The maximum allowed size for a serialized block, in bytes (network rule) */
10 static const unsigned int MAX_BLOCK_SIZE = 1000000;
11 /** The maximum allowed number of signature check operations in a block (network rule) */
12 static const unsigned int MAX_BLOCK_SIGOPS = MAX_BLOCK_SIZE/50;
13 /** Coinbase transaction outputs can only be spent after this number of new blocks (network rule) */
14 static const int COINBASE_MATURITY = 100;
15

```

50

```

2632 bool CheckBlock(const CBlock& block, CValidationState& state, bool fCheckPOW, bool fCheckMerkleRoot)
2633 {
2634     // These are checks that are independent of context.
2635
2636     if (block.fChecked)
2637         return true;
2638
2639     // Check that the header is valid (particularly PoW). This is mostly
2640     // redundant with the call in AcceptBlockHeader.
2641     if (!CheckBlockHeader(block, state, fCheckPOW))
2642         return false;
2643
2644     // Check the merkle root.
2645     if (fCheckMerkleRoot) {
2646         bool mutated;
2647         uint256 hashMerkleRoot2 = block.ComputeMerkleRoot(&mutated);
2648         if (block.hashMerkleRoot != hashMerkleRoot2)
2649             return state.DoS(100, error("CheckBlock(): hashMerkleRoot mismatch"),
2650                 REJECT_INVALID, "bad-txnmkroot", true);
2651
2652         // Check for merkle tree malleability (CVE-2012-2459): repeating sequences
2653         // of transactions in a block without affecting the merkle root of a block,
2654         // while still invalidating it.
2655         if (mutated)
2656             return state.DoS(100, error("CheckBlock(): duplicate transaction"),
2657                 REJECT_INVALID, "bad-txns-duplicate", true);
2658     }
2659 }

```

<https://github.com/bitcoin/bitcoin/blob/master/src/main.cpp>

51

```

2632 bool CheckBlock(const CBlock& block, CValidationState& state, bool fCheckPOW, bool fCheckMerkleRoot)
2633 {
2634     // These are checks that are independent of context.
2635
2636     if (block.fChecked)
2637         return true;
2663
2664     // Size limits
2665     if (block.vtx.empty() || block.vtx.size() > MAX_BLOCK_SIZE || ::GetSerializeSize(block, SER_NETWORK, PROTOCOL_VERSION) > MAX
2666         return state.Dos(100, error("CheckBlock(): size limits failed"),
2667             REJECT_INVALID, "bad-blk-length");
2668
2669     // First transaction must be coinbase, the rest must not be
2670     if (block.vtx.empty() || !block.vtx[0].IsCoinBase())
2671         return state.Dos(100, error("CheckBlock(): first tx is not coinbase"),
2672             REJECT_INVALID, "bad-cb-missing");
2673     for (unsigned int i = 1; i < block.vtx.size(); i++)
2674         if (block.vtx[i].IsCoinBase())
2675             return state.Dos(100, error("CheckBlock(): more than one coinbase"),
2676                 REJECT_INVALID, "bad-cb-multiple");
2677
2678     // Check transactions
2679     BOOST_FOREACH(const CTransaction& tx, block.vtx)
2680         if (!CheckTransaction(tx, state))
2681             return error("CheckBlock(): CheckTransaction of %s failed with %s",

```

<https://github.com/bitcoin/bitcoin/blob/master/src/main.cpp>

Scale Today

Block Size = 1MB

Typical transaction size ~ 500 Bytes

Maximum of ~2000 transactions per block / 10 minutes

So, about 3-4 transactions per second


Scale Today

Block Size = 1MB

Typical transaction size ~ 500 Bytes

Maximum of ~2000 transactions per block / 10 minutes

So, about 3-4 transactions per second

\$1B / day = 

Cost to control bitcoin (assuming other miners are "rational"):

value per block-minute = \$7500/10 minutes ~ \$750/minute ~ \$1M/day
to increase to **\$1B/day** with current transaction rate:

\$3472 fee per transaction (without losing transactions)

or **33 Billion transactions per day** (with current \$0.03 fee)

Scale Today

Block Size = 1MB

Typical transaction size ~ 500 Bytes

Maximum of ~2000 transactions per block / 10 minutes

So, about 3-4 transactions per second

Transactions per Day

VISA: 300M

Interbank: 100M

Cost to control bitcoin (assuming other miners are "rational"):

value per block-minute = \$7500/10 minutes ~ \$750/minute ~ \$1M/day
to increase to **\$1B/day** with current transaction rate:

\$3472 fee per transaction (without losing transactions)

or **33 Billion transactions per day** (with current \$0.03 fee)

Cash is the single biggest opportunity

Visa Inc. Developed Markets (2012)



Visa Inc. Emerging Markets (2012)



Note: PCE defined as Purchase PCE (does not include non-financial transactions); excludes Europe
Source: PCE growth from Oxford Economics (Nominal \$); all other data from Euromonitor Merchant Segment Survey estimates, 2013

12 | Visa Investor Day

Transactions per Day

VISA: 300M
Interbank: 100M
Cash: 20B? ≈S

“rational”):
\$750/minute ~ \$1M/day
on rate:
g transactions)
ent \$0.03 fee)

56

Scale Today

Block Size = 1MB

Typical transaction size ~ 500 Bytes

Maximum of ~2000 transactions per

So, about 3-4 transactions per second

Transactions per Day

VISA: 300M
Interbank: 100M
Cash: 20B? ≈S

Facebook Likes: 4.5B

SMS Messages: 25B

WhatsApp Msg: 50B

Cost to control bitcoin (assuming other miners are
value per block-minute = \$7500/10 minutes ~ \$750/minute ~ \$1M/day
to increase to \$1B/day with current transaction rate:

\$3472 fee per transaction (without losing transactions)

or **33 Billion transactions per day** (with current \$0.03 fee)

57



Ombuds

Distributed microblogging