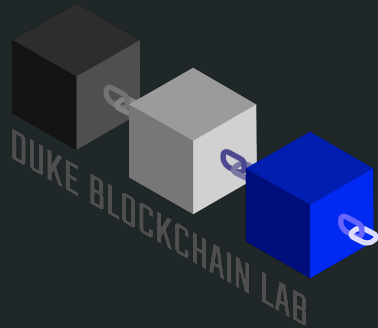


What is Bitcoin?

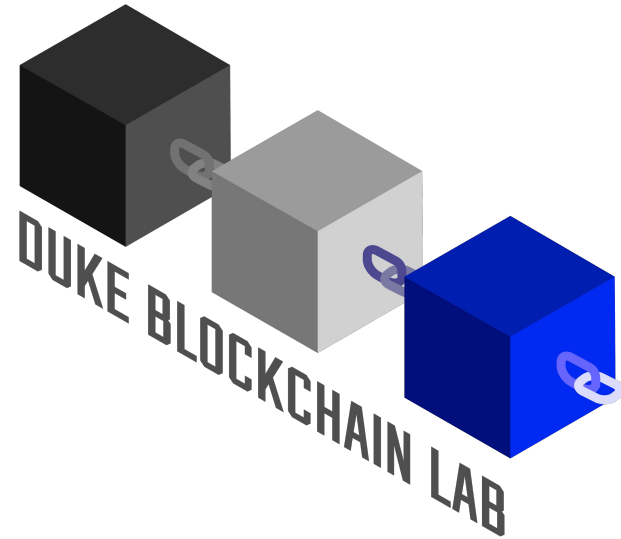
Why should I care?

David Zarge
Duke University
February 13, 2018



About the Duke Blockchain Lab

- **Education:** Lecture Series, House course, Ethereum crash course, Cryptocurrency Investment Group (CIG), etc.
- **Industry:** Outside speakers, recruiting pipeline, mentorship
- **Incubation:** Support for blockchain based projects



Today

What is Bitcoin?

- Brief overview of history, technical concepts, key players
- Using Bitcoin: Buying, hodling, and using cryptocurrency

Why should you care

- Defining value and money
- Importance of blockchain and cryptocurrency

History

Phase 1: Jan 2009-Early 2011 (0->1)

Phase 2: Early 2011-Mid 2013 (1->200)

Phase 3: Mid 2013-late 2016 (1200->300-->700)

Phase 4: Early 2017-Now (700-->19000->6000-->?)

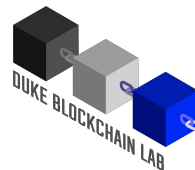
2008: Bitcoin Begins



- Satoshi Nakamoto and the Genesis Block (Jan 2009)
 - White paper, "Bitcoin: A Peer-to-Peer Electronic Cash System"

The [raw hex version](#) of the Genesis block looks like:

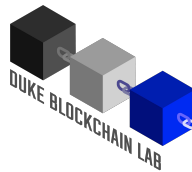
```
00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000001 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E ....;fiyz{.²zÇ,>
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA gv.a.È.Ã`SQ2:Ÿ.ª
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C K."J)«_IyŸ...¬+|
00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 .....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D .....ÿÿÿÿM.ÿÿ..
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F ..EThe Times 03/
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C Jan/2009 Chancel
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 lor on brink of
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 second bailout f
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 or banksÿÿÿÿ..ð.
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 *....CA.gšÿ"pUH'
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6 .gñ|q0•.\\ö"(à9.¡
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4 ybàè.ad†Iö¿?LI8Ä
00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 ÓU.â.Ã.p†8M+ø..W
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 ŠLp+kñ._~....
```



Excerpt from Bitcoin Whitepaper

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...

<https://bitcoin.org/bitcoin.pdf>

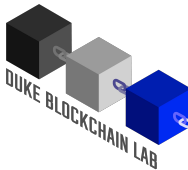


The Original Vision (Oct 2008)

- 21 million bitcoins
in circulation
- Initial reward:
50 BTC per block
- Cut reward in half
every 210,000
blocks, or ~4 years

Bitcoin: A Peer-to-Peer Electronic Cash System

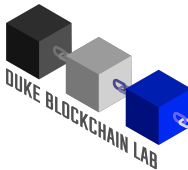
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org




2008: Bitcoin Begins





- Satoshi Nakamoto and the Genesis Block (Jan 2009)
 - White paper, "Bitcoin: A Peer-to-Peer Electronic Cash System"
- Early growth, adoption, and the dark web
- Mt. Gox, rise and fall of the first major exchange
- Explosive growth, legitimacy, and eventual competition in the cryptocurrency space




10,000 BTC Pizza

 Author Topic: Pizza for bitcoins? (Read 651169 times)

laszlo
Full Member


Activity: 199


 **Pizza for bitcoins?**
May 18, 2010, 12:35:20 AM
#1

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

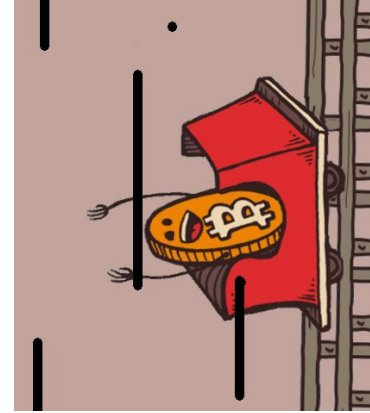
BC: 157fRqAKrDyGHR1Bx3yDxeMv8Rh45aUet

What Happened in 2017: Bitcoin



What Happened in 2017

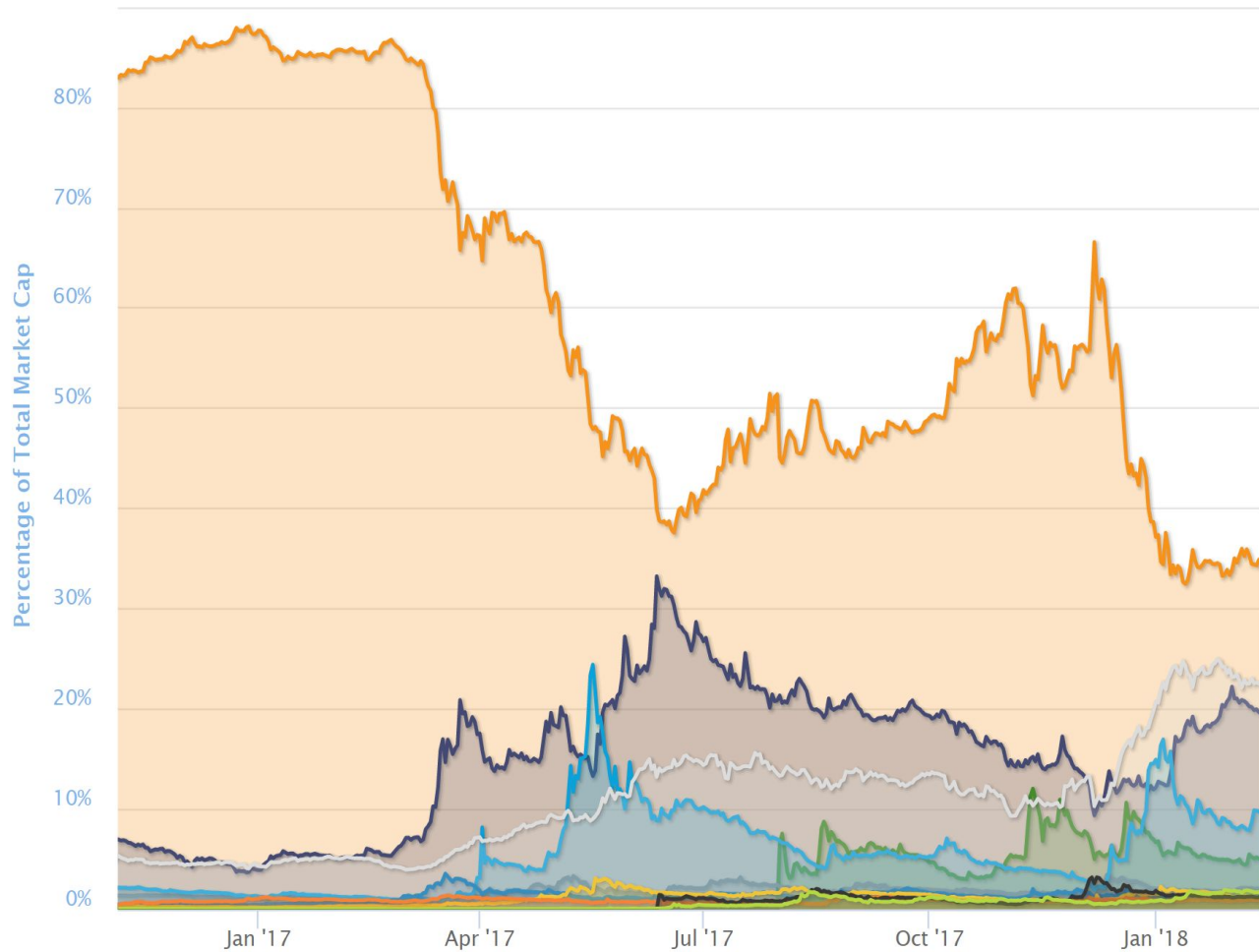
- Price explosion
- Mainstream Attention
 - Institutional Investors
 - Increased government scrutiny
- Cryptocurrency and ICO craze



What Happened in 2017: Crypto Market Cap



What Happened in 2017: Dominance



How does it work?



How does it work?

- Blockchain
- Key players:
 - Miners
 - Users
 - Developers
 - Exchanges

FAQ

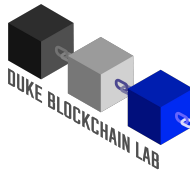
How do I get it?

Where do I keep it?

How do I use it? Can I buy stuff?

Who controls it?

Should I buy?



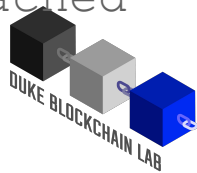
Mining

What is it?

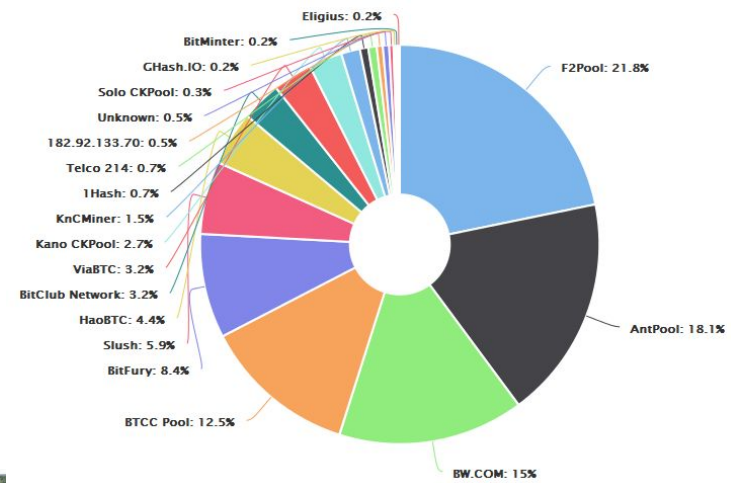
- Secures Bitcoin blockchain
- Adds new Bitcoins to the economy

How does it work?

- Miner works to solve a problem...**Proof of work**
- If the solution is valid-> The new block is mined, the solver is given Bitcoin reward (currently 12.5 BTC)
- Incentive to include transactions in blocks: fees attached



Modern Mining



Exchanges

BITFINEX 

coinbase

 **GDAX**

 **BINANCE**

BITTREX

 **GEMINI**

Wallets

Hardware:

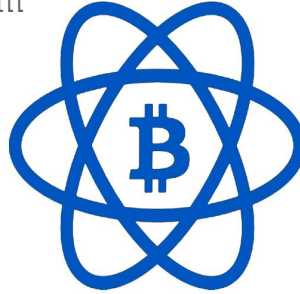
Desktop:

Mobile:

Ledger



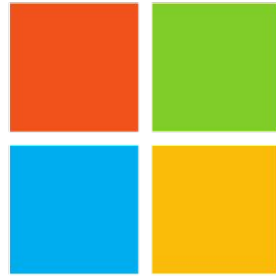
Electrum



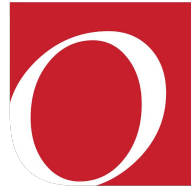
Trezor



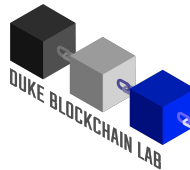
Merchants



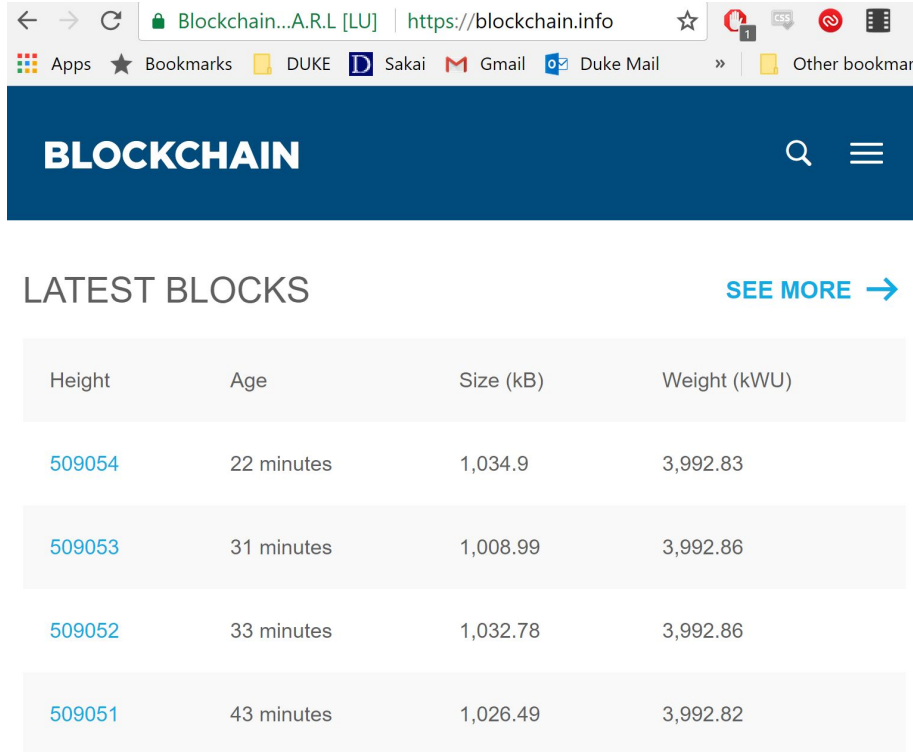
WIKIPEDIA
The Free Encyclopedia



overstock™

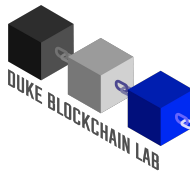


Bitcoin's Blockchain...more next week!



The screenshot shows a web browser window with the address bar displaying "Blockchain...A.R.L [LU] | https://blockchain.info". The browser's bookmark bar includes "Apps", "Bookmarks", "DUKE", "Sakai", "Gmail", "Duke Mail", and "Other bookmar". The website header is dark blue with the word "BLOCKCHAIN" in white, a search icon, and a menu icon. Below the header, the section "LATEST BLOCKS" is displayed with a "SEE MORE" link and a right-pointing arrow. A table follows, listing the latest blocks with columns for Height, Age, Size (kB), and Weight (kWU).

Height	Age	Size (kB)	Weight (kWU)
509054	22 minutes	1,034.9	3,992.83
509053	31 minutes	1,008.99	3,992.86
509052	33 minutes	1,032.78	3,992.86
509051	43 minutes	1,026.49	3,992.82



Bitcoin's Blockchain: A distributed ledger

Transaction View information about a bitcoin transaction

9bd661eeaab955a92e3f111aaee9d9b817f534196372c525b180e7e611c4f020

1JP7kktGGtC5gin1D7c5SmusDjbqddkrwe (\$ 199.17 - Output)



1Fm9izRLn5nDWQfGPxXLxpGTNLLiiQzFmz - (Unspent)

\$ 194.23

2 Confirmations

\$ 194.23

Summary

Size 192 (bytes)

Weight 768

Received Time 2018-02-13 22:09:45

Included In Blocks [509055](#) (2018-02-13 22:16:30 + 7 minutes)

Confirmations 2 Confirmations

Visualize [View Tree Chart](#)

Inputs and Outputs

Total Input \$ 199.17

Total Output \$ 194.23

Fees \$ 4.93

Fee per byte 300 sat/B

Fee per weight unit 75 sat/WU

Estimated BTC Transacted \$ 194.23

Scripts [Hide scripts & coinbase](#)

What defines value?

What defines value?

Why are these so expensive?

- Real-estate
- Cars
- Jewelry
- Precious metals
- Artwork

What is currency? Why does it have value?

What is currency? Why does it have value?

Money/Currency:

- Medium of exchange
- Store of value
- Unit of account

Value:

- Trust in economy and government
- Stability

Alternative Store of Value / Hedge

Why are precious metals (i.e. gold) valuable?

Alternative Store of Value/ Hedge

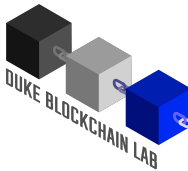
Why are precious metals/gold valuable?

- Scarcity, durability, (sometimes) utility
- Gold market: \$7 Trillion global market

Macroeconomic Factors Driving Bitcoin demand:

- Demonetization in India and Venezuela
- Trump, Brexit, and global instability

Oppressive, authoritarian governments-> **how can I keep my money safe from the government seizure and changes in the political climate?**



Traits of Money	Gold	Fiat (US Dollar)	Crypto (Bitcoin)
Fungible <i>(Interchangeable)</i>	High	High	High
Non-Consumable	High	High	High
Portability	Moderate	High	High
Durable	High	Moderate	High
Highly Divisible	Moderate	Moderate	High
Secure <i>(Cannot be counterfeited)</i>	Moderate	Moderate	High
Easily Transactable	Low	High	High
Scarce <i>(Predictable Supply)</i>	Moderate	Low	High
Sovereign <i>(Government Issued)</i>	Low	High	Low
Decentralized	Low	Low	High
Smart <i>(Programmable)</i>	Low	Low	High

International Transactions

- Peer-Peer
 - Remittance market: **\$500B**, 230M participants
 - Western Union, Moneygram, etc
- Bank-Bank
 - Blockchain could offer improvements for both domestic and int'l txns
 - Ripple (XRP)



Clearing and Settlement

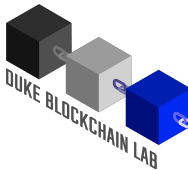
ACH - Could reduce txn time from day(s) to instantaneous

SWIFT - Processes \$5 Trillion/day, showcased a proof-of-concept using blockchain technology

12 January 2017

SWIFT explores blockchain as part of its global payments innovation initiative

Deloitte: Blockchain Systems Could Rival ACH Network By 2025



All this hype, but one thing we haven't addressed...

WHAT IS THE CASE AGAINST BITCOIN?

WHAT IS THE CASE AGAINST BITCOIN?

- Security
- Fees
- Mining
- **Scalability**
- Volatility
- Governance
- Early adopter ownership

Next week...

Understanding Blockchain