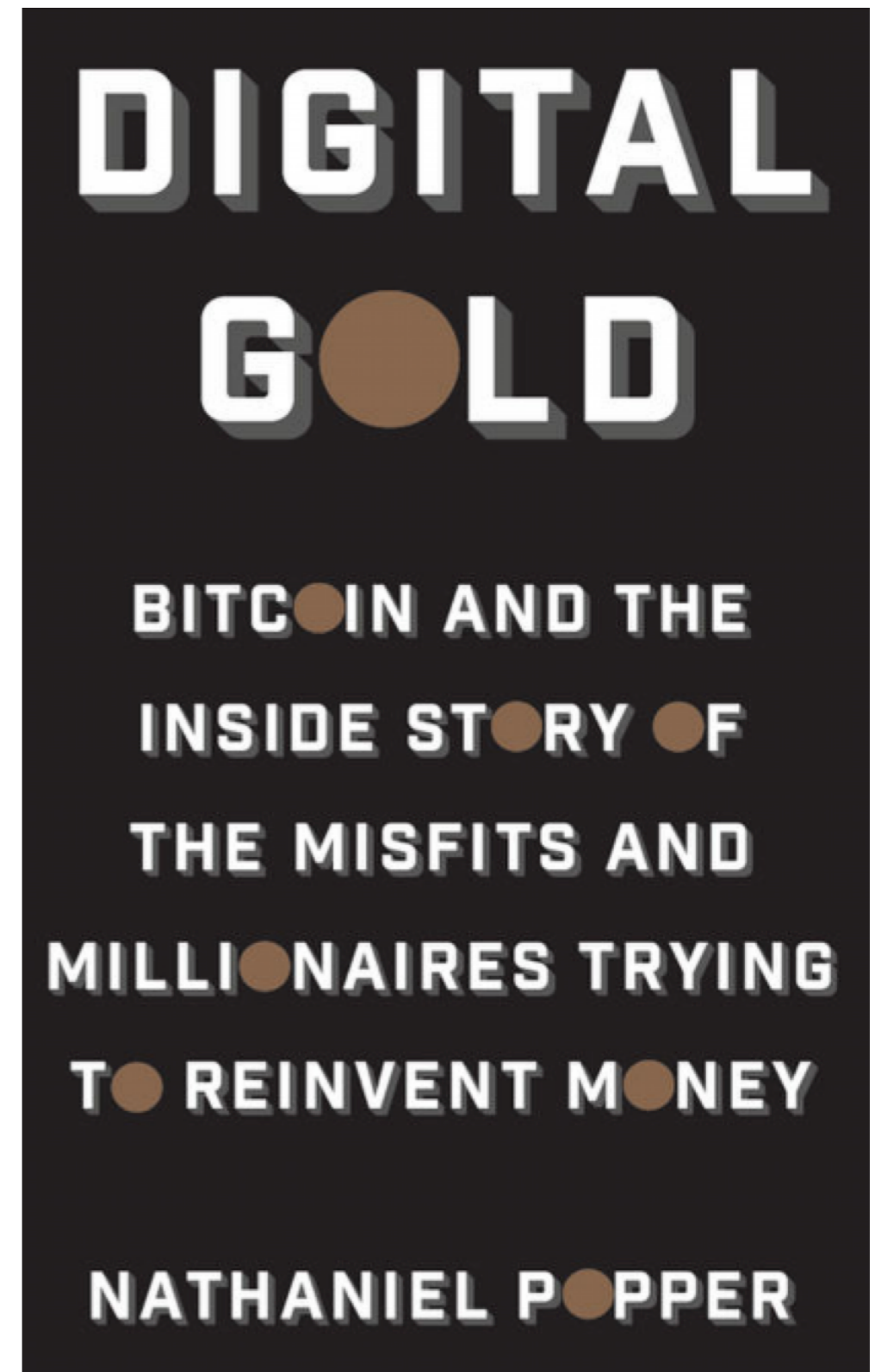
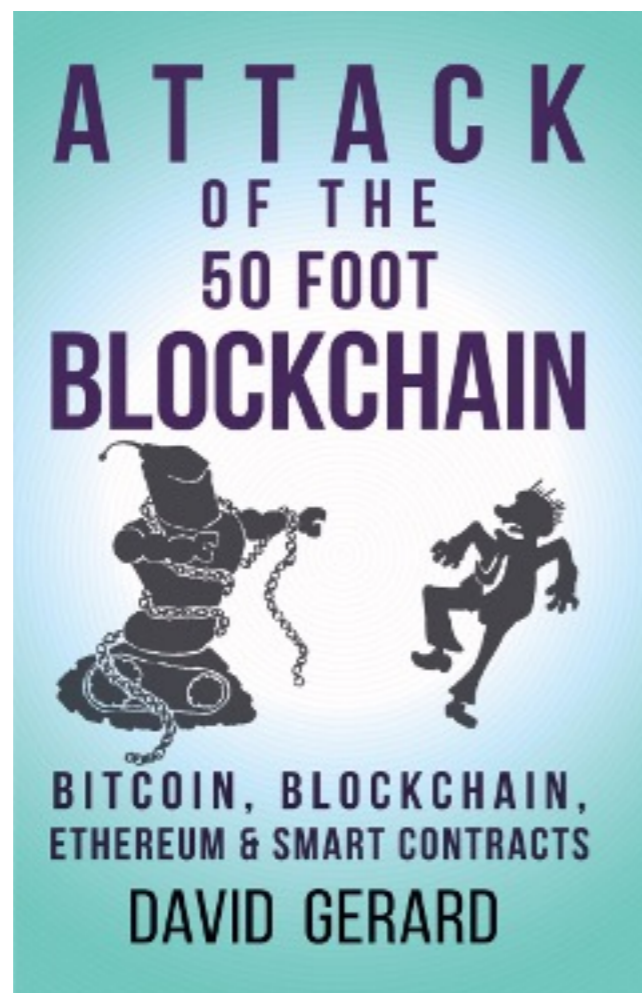
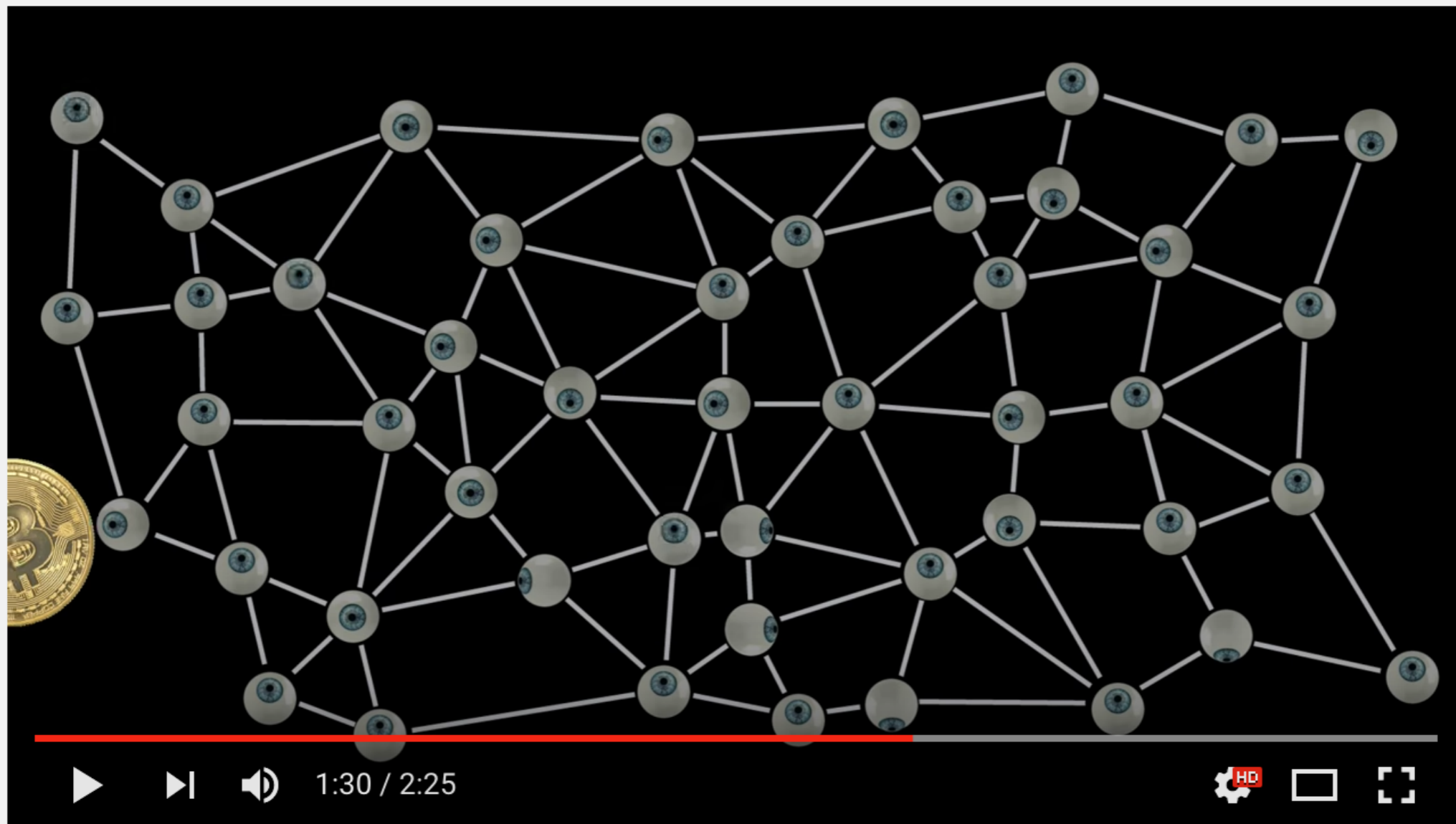


# Bitcoin and Blockchains



Updated 8-19-21

What's a Blockchain?



## Understand the Blockchain in Two Minutes

# Live Online Blockchain Demo

The screenshot shows a web browser window with the URL <https://anders.com/blockchain/blockchain.html>. The page title is "Blockchain Demo". The navigation menu includes "Hash", "Block", "Blockchain", "Distributed", "Tokens", and "Coinbase". The main content area is titled "Blockchain" and displays three blocks in a sequence.

Block #	Nonce	Data	Prev Hash	Hash
1	5692	Sam paid Sally 1 coin	00000000000000000000000000000000	0000a0a54a0bd9d8830a83608aca14c09
2	2564	Sue paid Sally 2 coins	0000a0a54a0bd9d8830a83608aca14c09	0000d50ae9450e4a706877ee92c8cea69
3	7174	Joe paid Sue 3 coins	0000d50ae9450e4a706877ee92c8cea69	0000b3b98b7208dfef33e7

Each block has a "Mine" button at the bottom.

Link Blockchain 10

Bitcoin

# Why Should Anyone Care?

- **Bitcoin** itself is not very attractive
  - Scams
  - Pyramid schemes
  - High-risk investment
  - Money laundering

# My Evolving Position



**Sam Bowne** @sambowne · 7 Apr 2015

To teach kids about **Bitcoin**, give them **piggy** banks. 6 months later smash them, steal the money, and laugh.



607



506



**Sam Bowne** @sambowne · May 24

My previous **contempt** towards **cryptocurrencies** was uninformed. Now I understand them better: they deserve far more **contempt**.



1



9



# Why Does Bitcoin Have Any Value?

- Three killer apps
  - Silk Road (purchase illegal things)
  - Ransomware (must pay in Bitcoin)
  - Economies with high inflation (like Argentina)
- 2017: **Speculation**



# 7% of all Bitcoins Stolen



CoinDesk's BPI illustrated bitcoin's dramatic drop in value following the emergence of the rumours.

FEBRUARY 25, 2014

**MT GOX  
ALLEGEDLY LOSES  
\$350 MILLION IN  
BITCOIN (744,400  
BTC)**

Speculation mounts following the publication of a leaked report, which states enormous losses and indicates the exchange will close amid its attempts to rebrand.

ROBERT MCMILLAN BUSINESS 03.03.14 6:30 AM

# THE INSIDE STORY OF MT. GOX, BITCOIN'S \$460 MILLION DISASTER



# Bitcoin Price Chart



- What is the real value of a bitcoin?

www.mauldineconomics.com/editorial/the-bitcoin-bubble-explained-in-4-charts#



**MAULDIN**  
ECONOMICS

*It's Time to Get Real About Your Investments*

Home

Articles & Commentary

Our Publications

About Us

Editorial

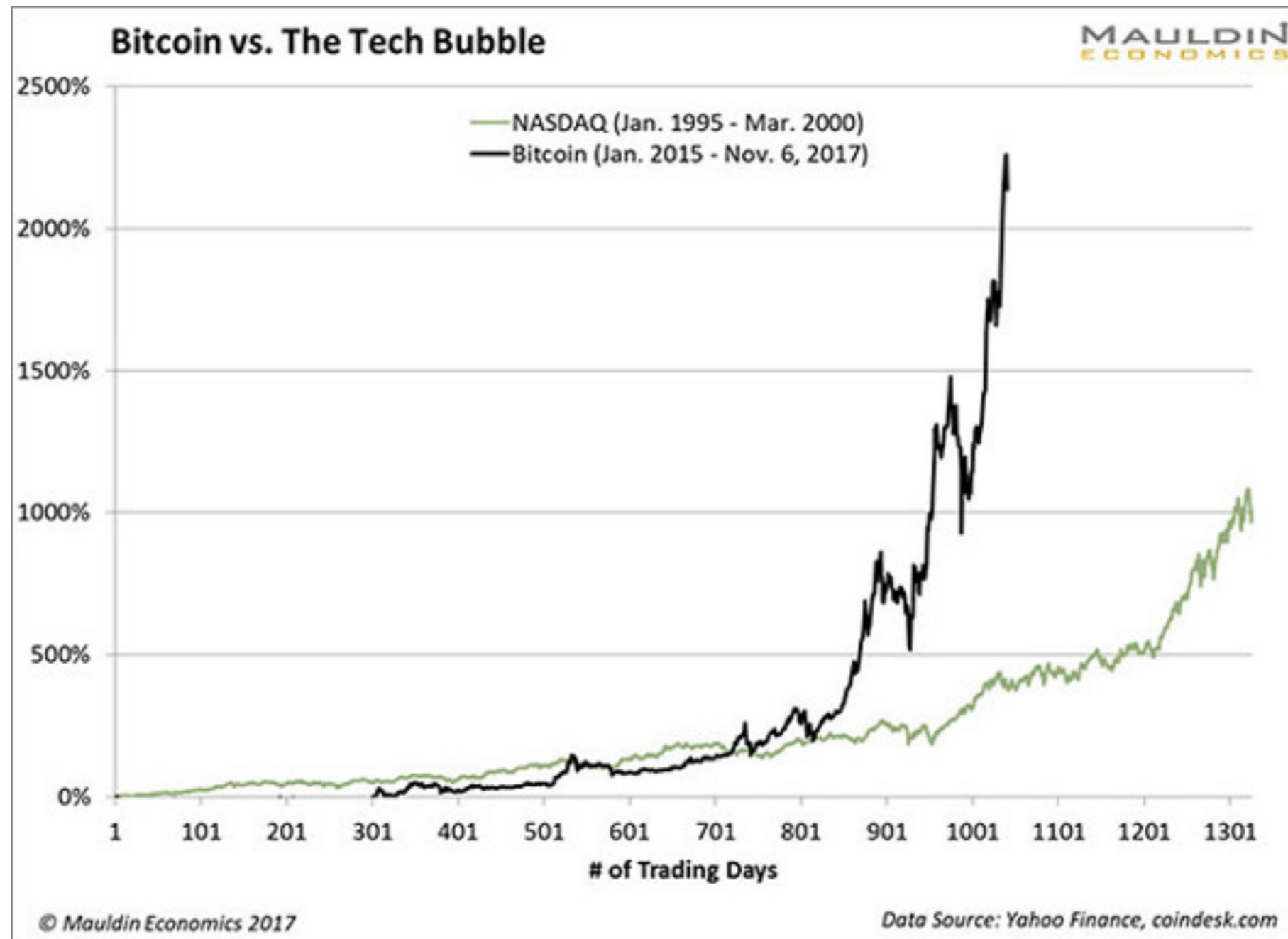
---

## The Bitcoin Bubble Explained in 4 Charts

NOVEMBER 13, 2017

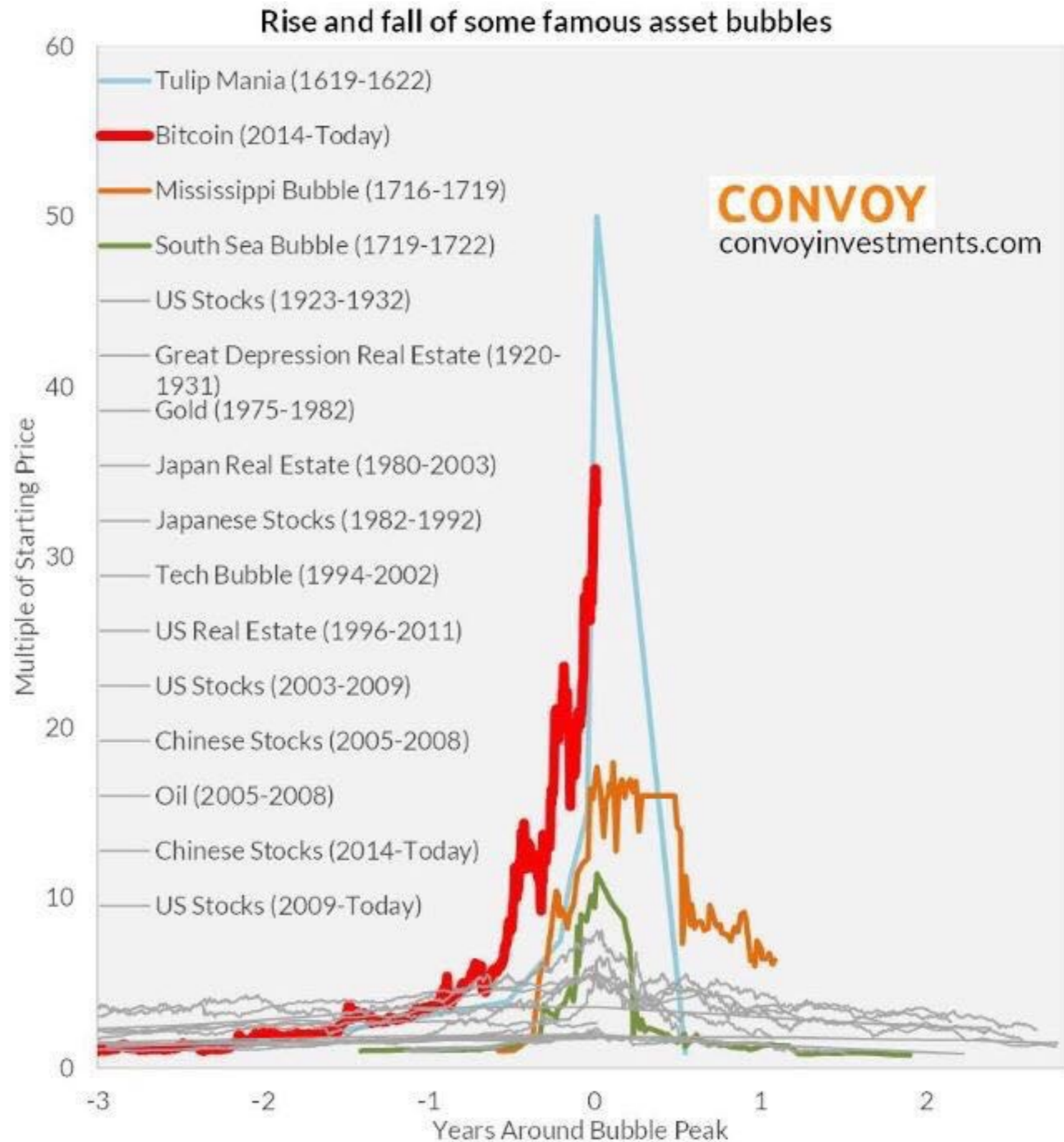
BY JAKE WEBER

# Bitcoin Rose Faster than the DotCom Bubble



In 1637, a single tulip bulb sold for more than the cost of a large mansion

<http://www.bbc.com/culture/story/20160419-tulip-mania-the-flowers-that-cost-more-than-houses>





*This part of my life, this part right here,  
this part is called "being stupid"*

[https://en.wikiquote.org/wiki/The\\_Pursuit\\_of\\_Happyness](https://en.wikiquote.org/wiki/The_Pursuit_of_Happyness)

# Bitcoin and Ethereum vs Visa and PayPal – Transactions per second

Bitcoin – 3 to 4 transactions per second

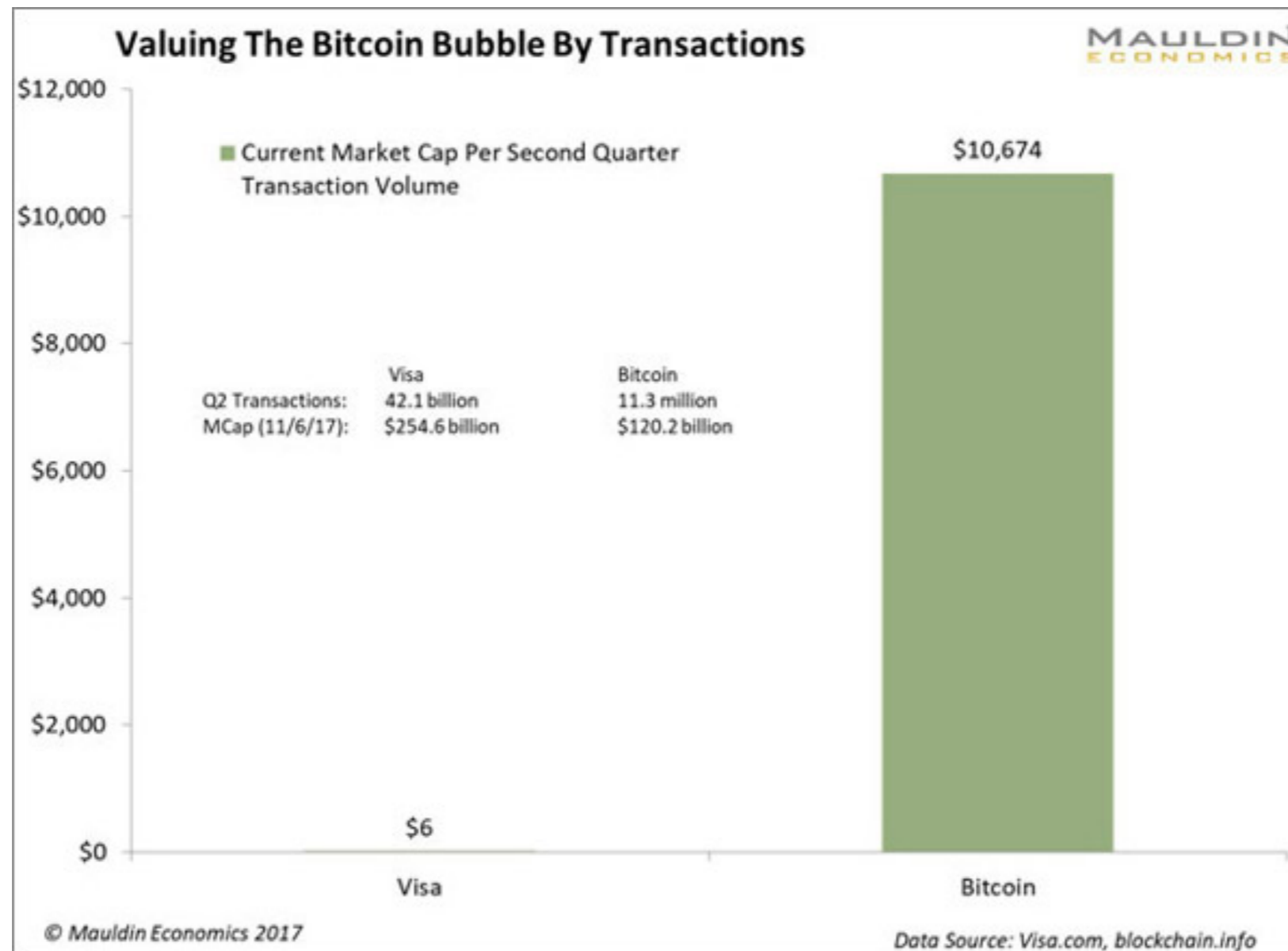
Ethereum – 20 transactions per second

PayPal – 193 transactions per second average

Visa – 1,667 transaction per second

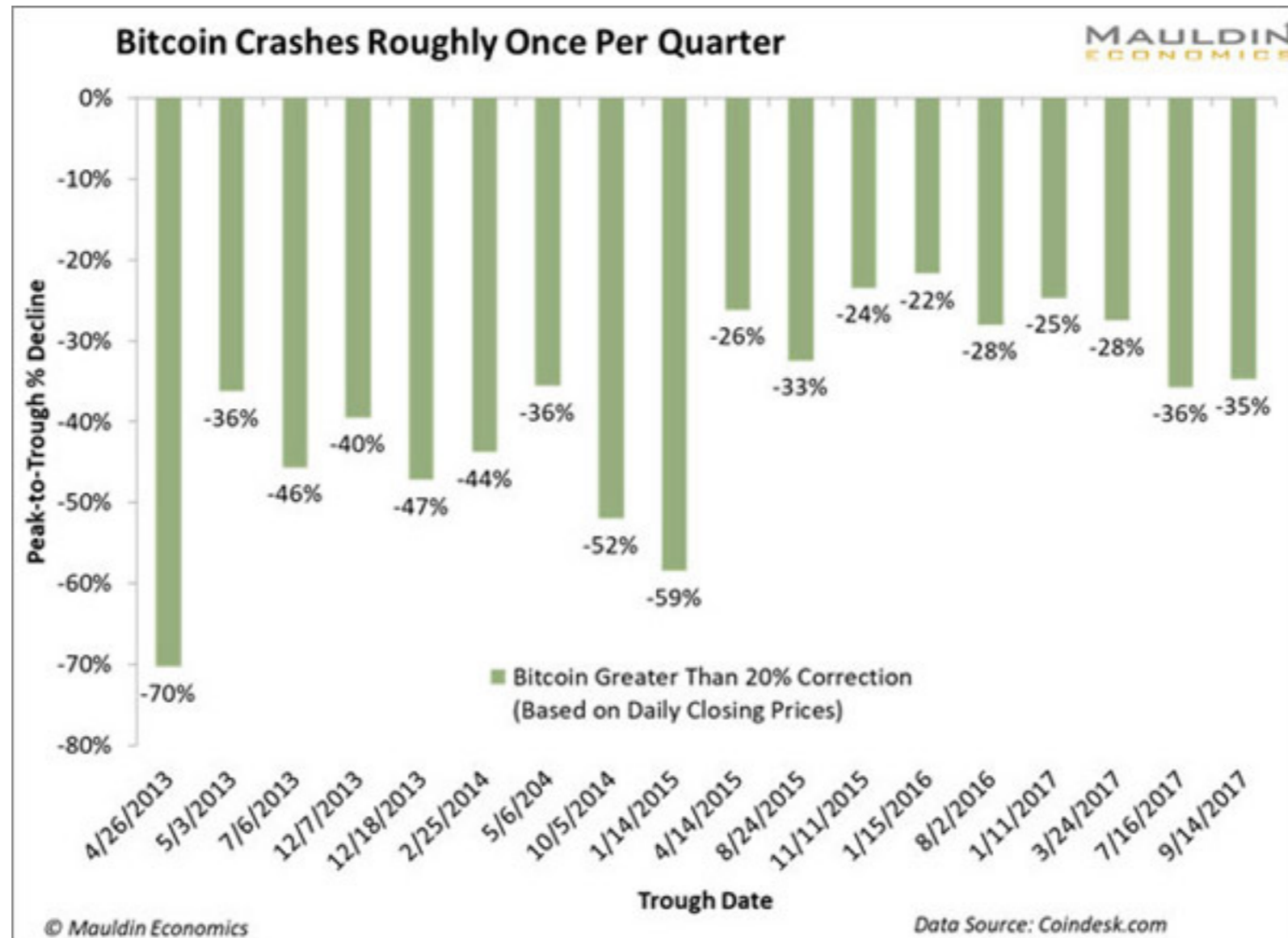


# Is Bitcoin a Means of Exchange?

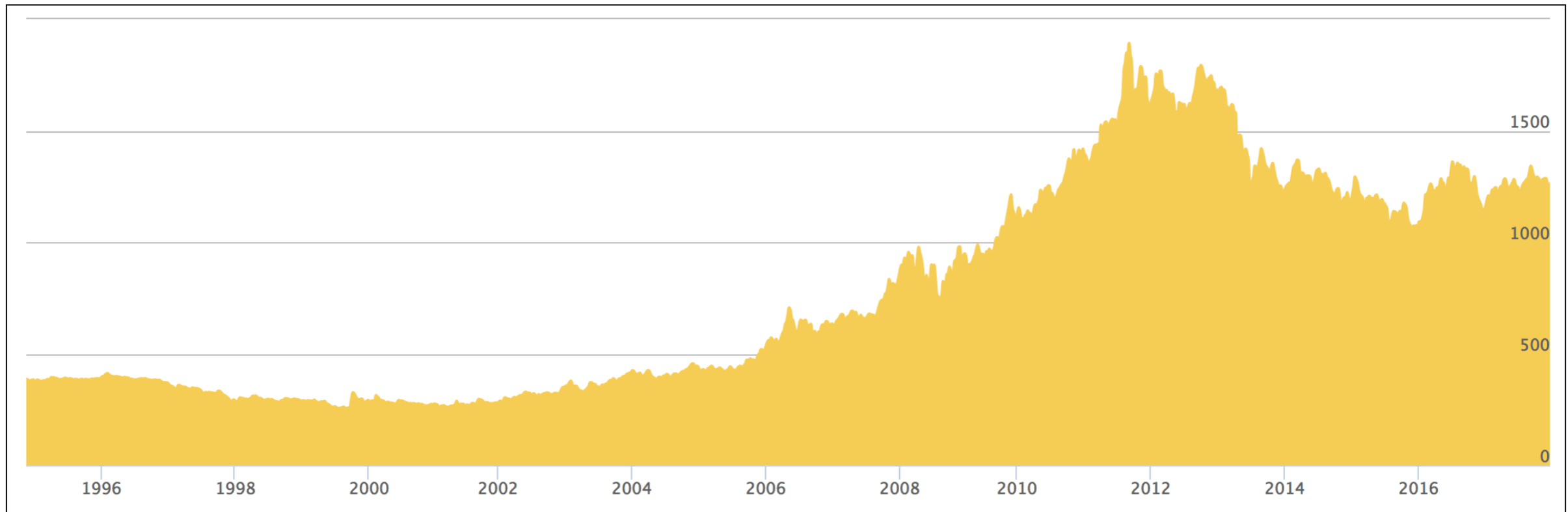


- Visa is valued at \$6 per transaction
- Bitcoin over \$10,000 per transaction

# Is Bitcoin a Store of Value?

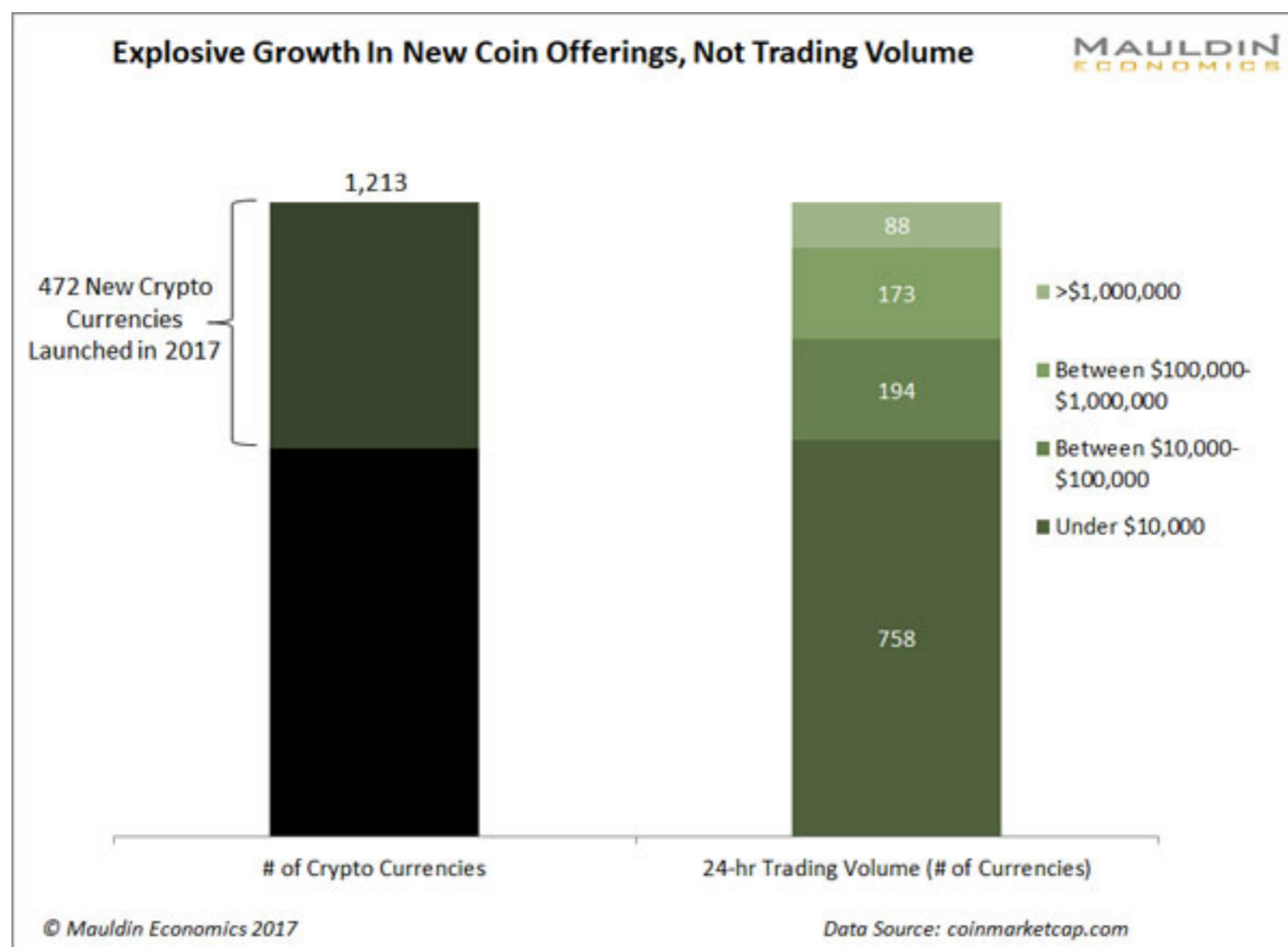


# Gold is the Classic Store of Value



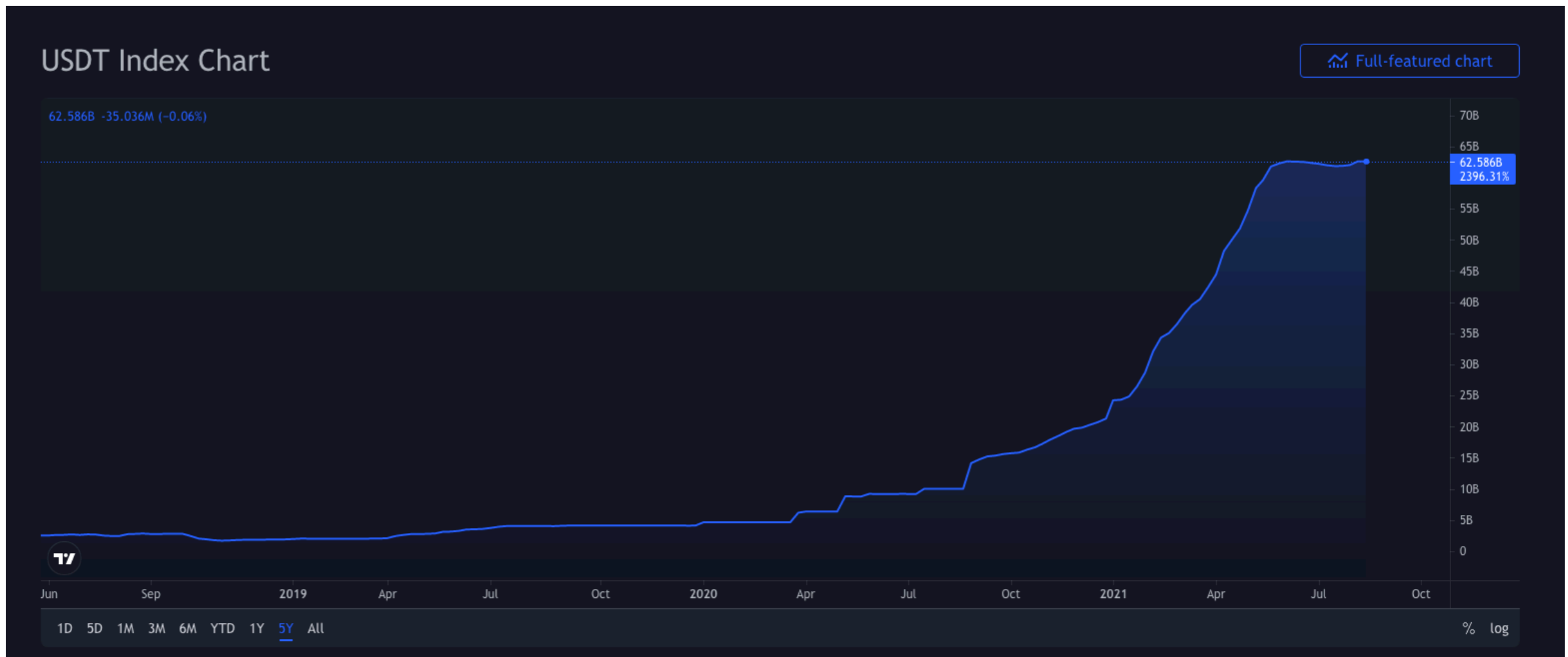
<https://www.moneymetals.com/precious-metals-charts/gold-price>

# Initial Coin Offerings (ICO)



...only 20 of the currencies are actually being used for something other than trading. The rest are purely speculative trading instruments.

# Tether Market Capitalization

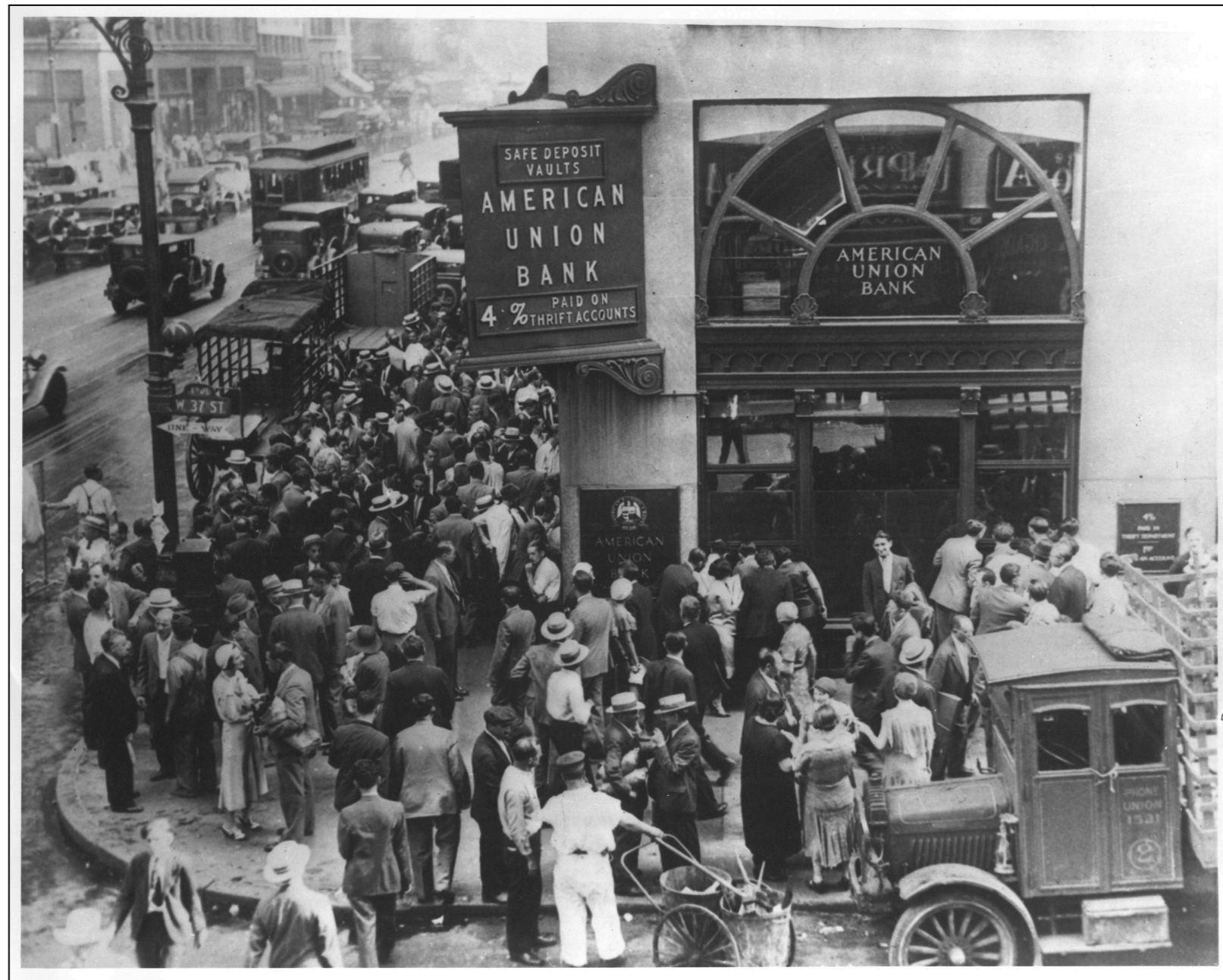


Constantly issuing more to push Bitcoin price up

Actual cash reserves are 3%

<https://davidgerard.co.uk/blockchain/2021/05/13/tether-publishes-two-pie-charts-of-its-reserves/>

# 1929 Bank Run



Ethereum

# Smart Contracts

- Programs that run on the Ethereum blockchain
- A company can be run by a program, and have no physical location
- Advocates expected to be exempt from all laws and taxes



# The DAO, The Hack, The Soft Fork and The Hard Fork



6 comments



Antonio Madeira



28 Sep 2017



37.36 K



## Digital Autonomous Organization (DAO)

- Started with \$150 M investment
- Launched in May, 2016
- Security concerns were raised but ignored
- On June 18, a hacker stole \$70 M

# Ethereum Enthusiasts Determine Their DAO After A Successful Hard Fork



As of 12:00pm GMT yesterday, a majority of Ethereum Network miners agreed to fork the Ethereum blockchain in order to refund Ether that was hacked from the DAO (Decentralized Autonomous Organization). Now the Ethereum community must choose their DAO ("a way" in Chinese) with which coin they will support.

# We spoke to the vigilante hackers who stole \$85 million in ether to save it

- "White-Hat Hackers" stole **rescued** the remaining Ether from the DAO to pressure Ethereum into forking
- Reportedly, the funds were returned later

# July - Oct, 2017

## Hacker Uses A Simple Trick to Steal \$7 Million Worth of Ethereum Within 3 Minutes

 Monday, July 17, 2017  Mohit Kumar

## Hacker Steals \$8.4 Million in Ethereum (4th Heist In A Month)

 Monday, July 24, 2017  Swati Khandelwal

## Warning: Enigma Hacked; Over \$470,000 in Ethereum Stolen So Far

 Sunday, August 20, 2017  Mohit Kumar

## EtherParty Breach: Another Ethereum ICO Gets Hacked

 Tuesday, October 03, 2017  Mohit Kumar

# parity

technologies ltd

Parity Technologies would like to allow its users and supporters to make a financial contribution to help it in its mission: developing the fastest and most secure way of interacting with the Ethereum network.

# Biggest Hack In History Freezes \$156M In Tech Funds, Damaging Some Entertainment Startups

by [Bruce Haring](#)

November 11, 2017 11:37am

[Parity Technologies](#) was the victim of the hack. The company manages a network of digital wallets which hold tokens that can be sold as needed by their owners and turned into cash. Earlier this week, a hacker breached one of the wallets and subsequently wiped out its contents, including a code library. That resulted in other wallets in the blockchain being frozen. Parity said today that 587 wallets containing 513,774.16 in ether, the digital coin associated with the ethereum blockchain, have been frozen.

Parity has been reaching out to owners of the affected wallets, but, as yet, **has not found a solution to unblocking the wallets and freeing the frozen funds.** “We are endeavoring to find a solution as soon as possible,” said a statement from Jutta Steiner, the company founder. The situation was called “a learning opportunity” for the company, “albeit a painful one.”

August 12, 2021  
8:17 PM PDT  
Last Updated 6 days ago

## Technology

# Explainer: How hackers stole and returned \$600 mln in tokens from Poly Network

4 minute read

By Gertrude Chavez-dreyfuss and Michelle Price

## 'Dogecoin is money': Check Elon Musk's message amid crypto rally



Elon Musk

---

1 min read . Updated: 26 Jul 2021, 02:14 PM IST



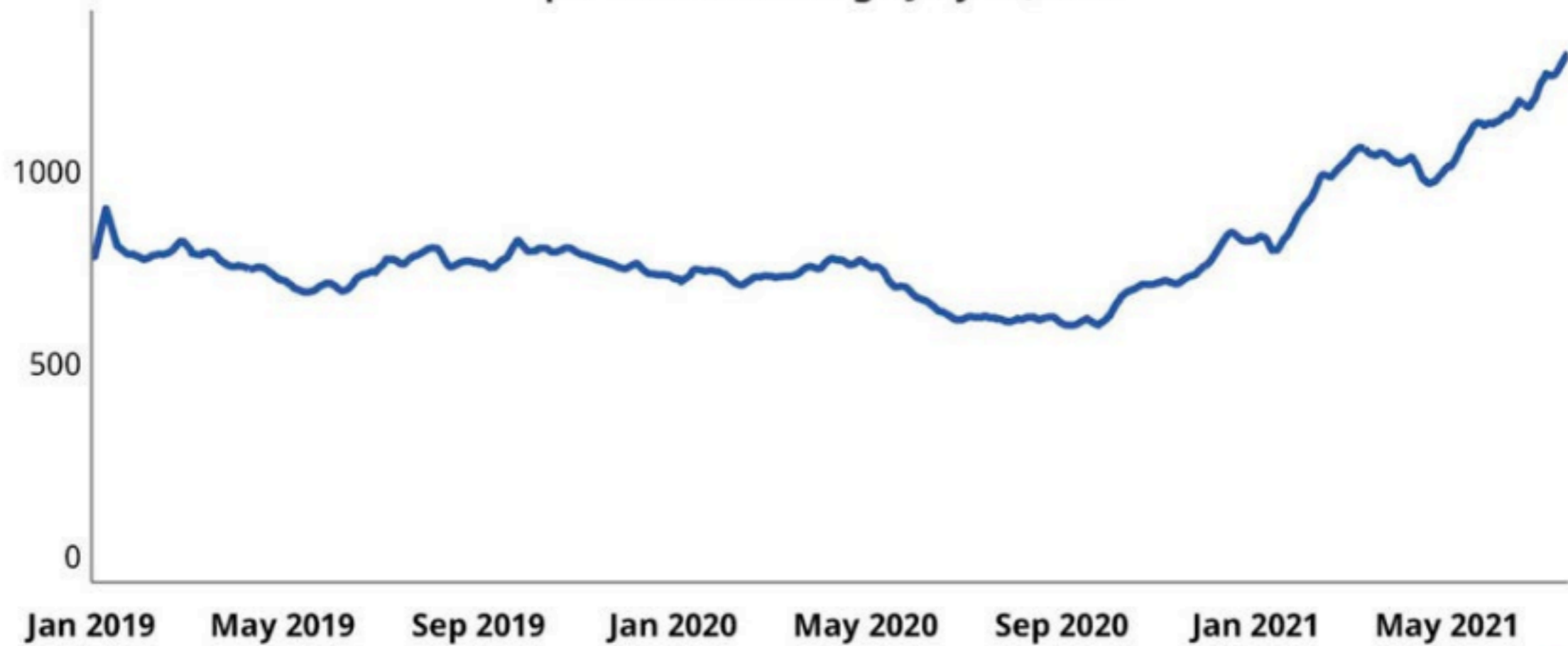
# Blockchains

# Blockchains

- The technology behind Bitcoin
- Everyone has a copy of the complete ledger
- Very difficult to lie or cheat
- Enables business dealings with people you don't trust
- No trusted central authority
  - Bank, government, regulator, ...

# Crypto and blockchain job postings on the rise

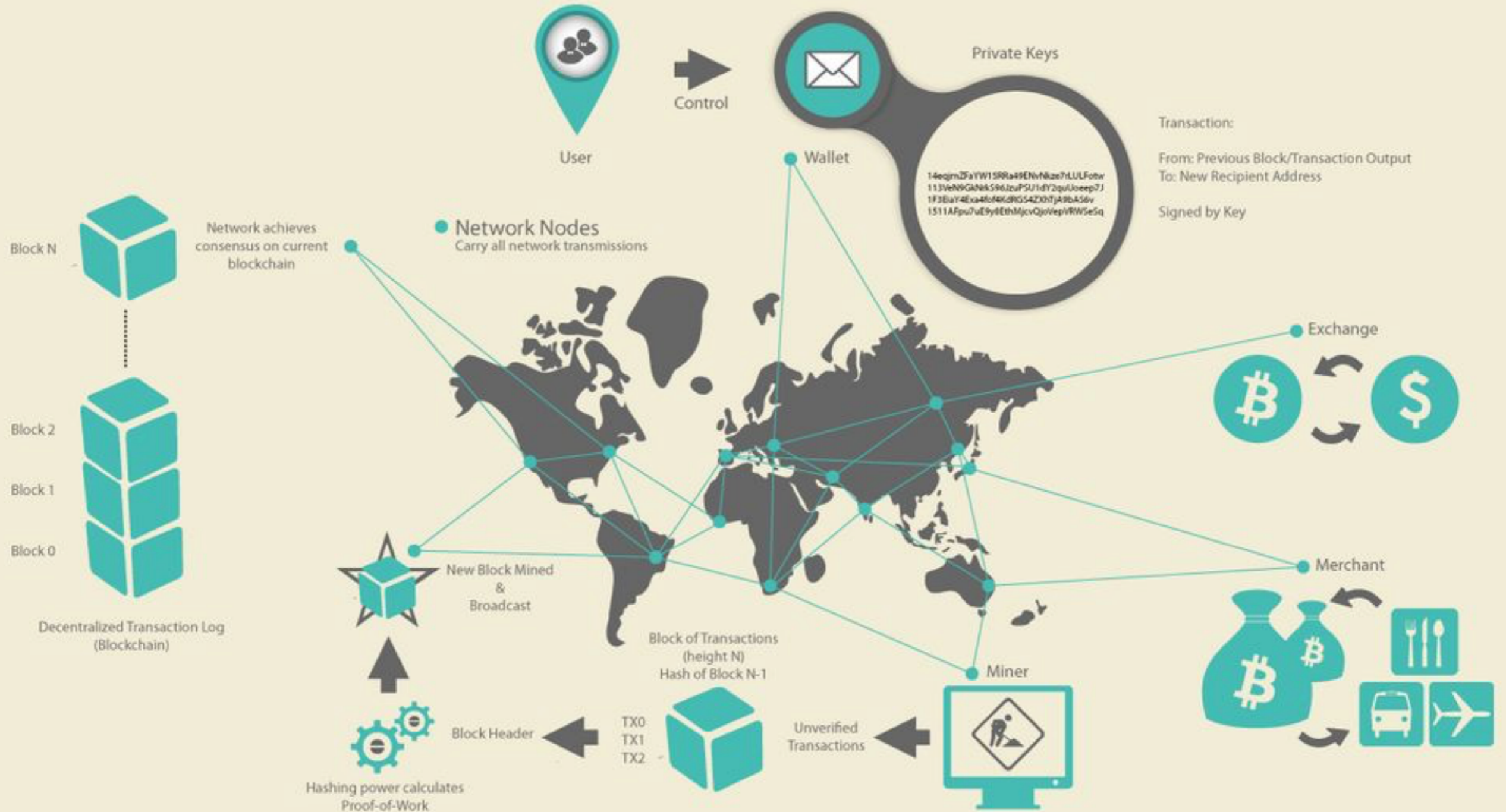
Share of crypto and blockchain job postings  
per million through July 16, 2021

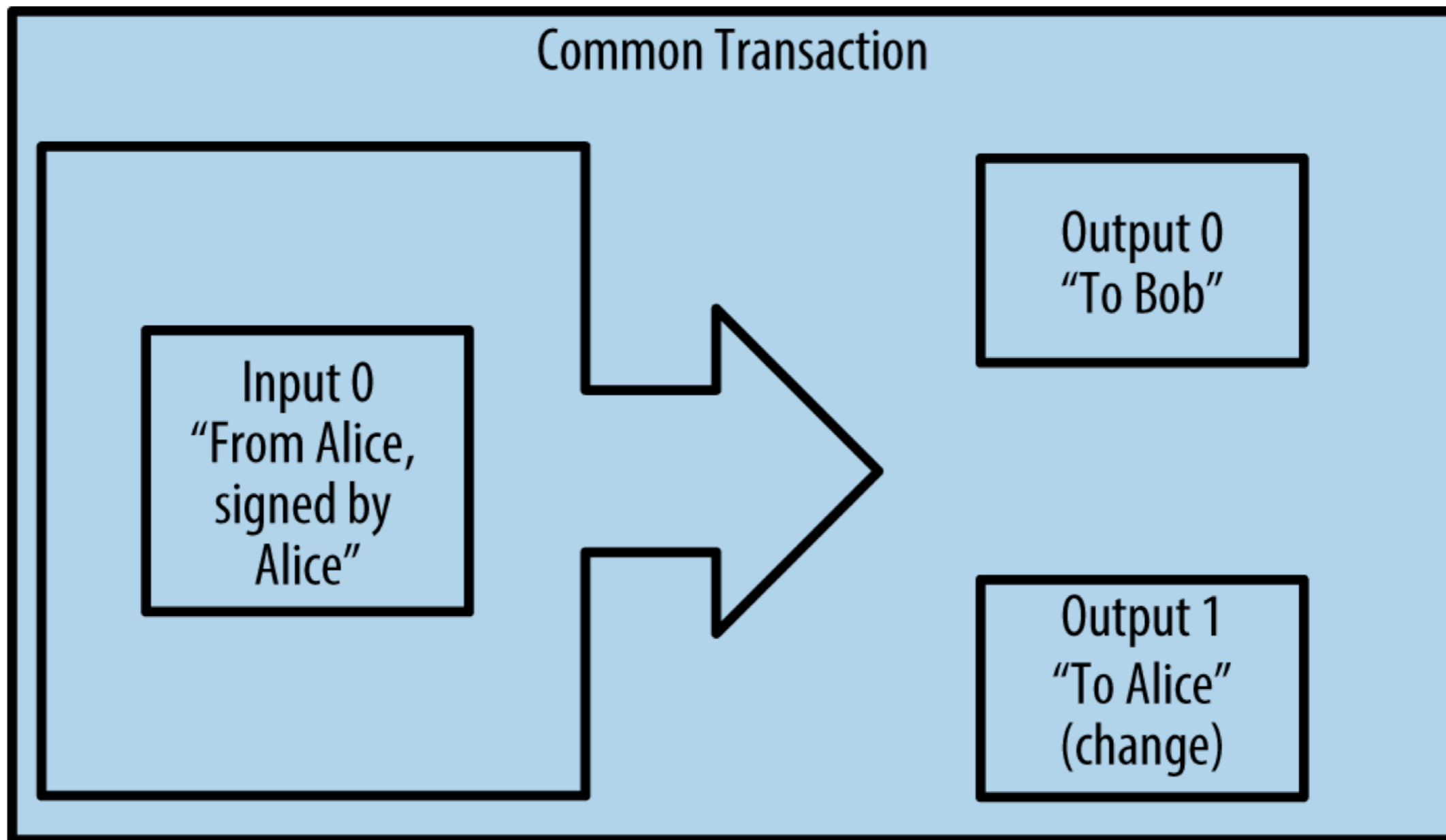


Source: Indeed. Data is 7 day moving avg.



# How Bitcoin Works





*Figure 2-5. Most common transaction*

# How Bitcoin Works

- Blocks are signed by miners with a SHA-256(SHA-256(block)) hash
- The hash must start with 69 bits of zero
- Difficulty is adjusted to keep the time between successes near 10 min.
- This makes forging signatures very difficult
- Miners get an award (currently 25 bitcoins) plus transaction fees
  - [Link Bitcoin 8](#)

# Bitcoin's Importance

- Bitcoin is a real-world test of blockchain technology
- A bunch of rebels, criminals, scammers, and suckers
- Demonstrated how well blockchains work
- AND THEY WORK

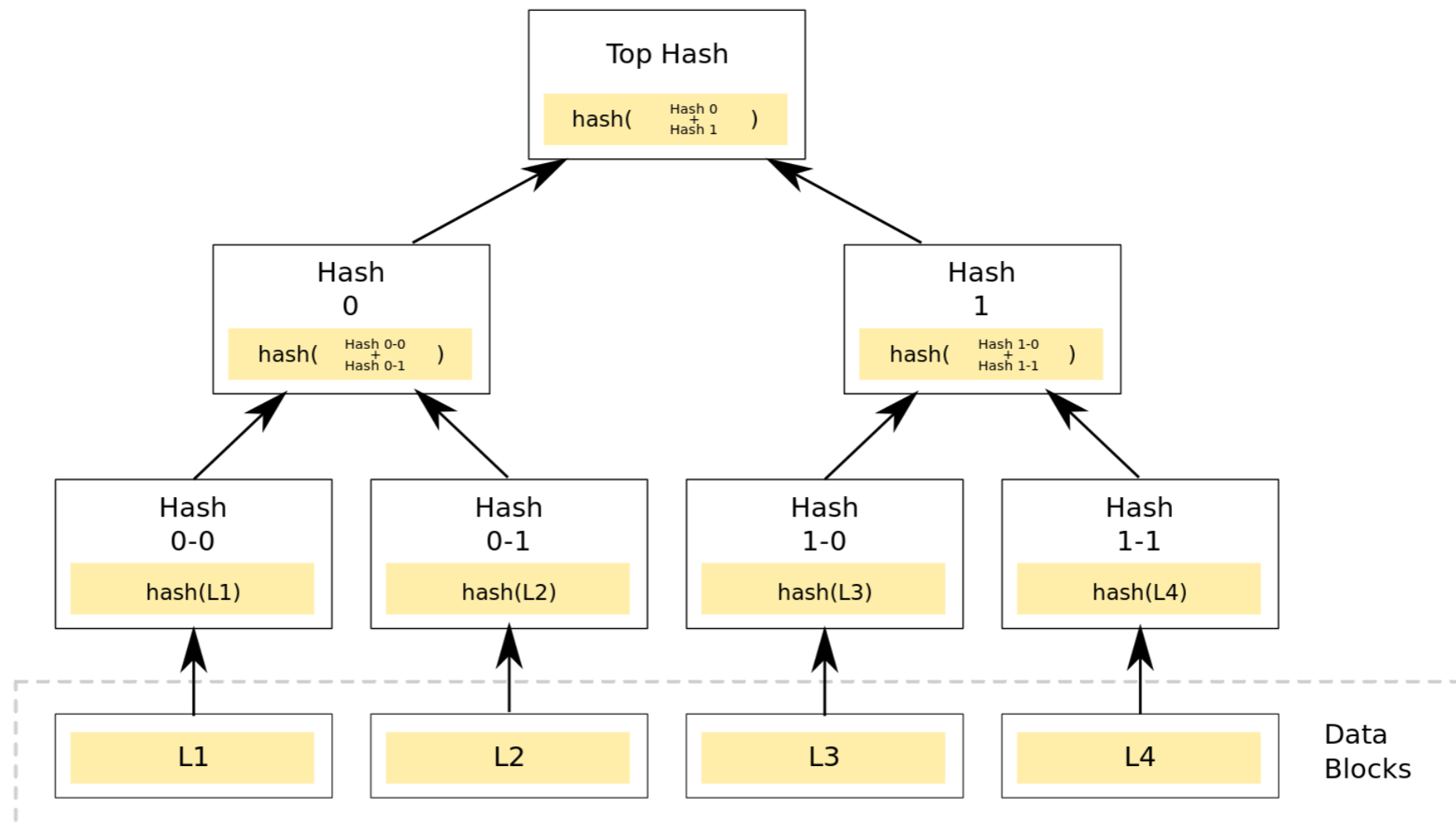
# History

- "Satoshi Nakamoto" invented and launched Bitcoin on Jan. 3, 2009
- A response to the 2008 financial crisis
- Fiat money without any bank or government controlling it



# Merkle Tree

- Designed to "allow efficient and secure verification of large data structures" -- Link Bitcoin 2



# Block

- A **block** is a public ledger of all bitcoin **transactions**
- Every computer running the full bitcoin software has a copy of the entire blockchain
- Every 10 minutes, the Bitcoin transactions are gathered together into a **block** and finalized by **miners** with **proof of work**
  - A hash value that's very difficult to compute, but easy to verify
- Each mined block produces 25 new bitcoins (soon this value will halve)

# Genesis Block


Blockchain Luxembourg S.A.R.L [LU] <https://blockchain.info/tx/4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b>

**BLOCKCHAIN** info Home Charts Stats Markets API Wallet Search English


## Transaction

View information about a bitcoin transaction



[4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b](#)

No Inputs (Newly Generated Coins)  [1A1zP1eP5QGefi2...](#) (Genesis of Bitcoin [🔗](#)) - (Unspent) 50 BTC

50 BTC

Summary	
Size	204 (bytes)
Received Time	2009-01-03 18:15:05
Reward From Block	0
Scripts	<a href="#">Hide scripts &amp; coinbase</a>
Relayed by IP 	<a href="#">0.0.0.0 (whois)</a>
Visualize	<a href="#">View Tree Chart</a>

### CoinBase

04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73  
(decoded)   The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

# Decoding the Coinbase

```
Untitled
0 04FFFF00 1D010445 54686520 54696D65 73203033  ~ ~  EThe Times 03
20 2F4A616E 2F323030 39204368 616E6365 6C6C6F72 /Jan/2009 Chancellor
40 206F6E20 6272696E 6B206F66 20736563 6F6E6420  on brink of second
60 6261696C 6F757420 666F7220 62616E6B 73  bailout for banks
```