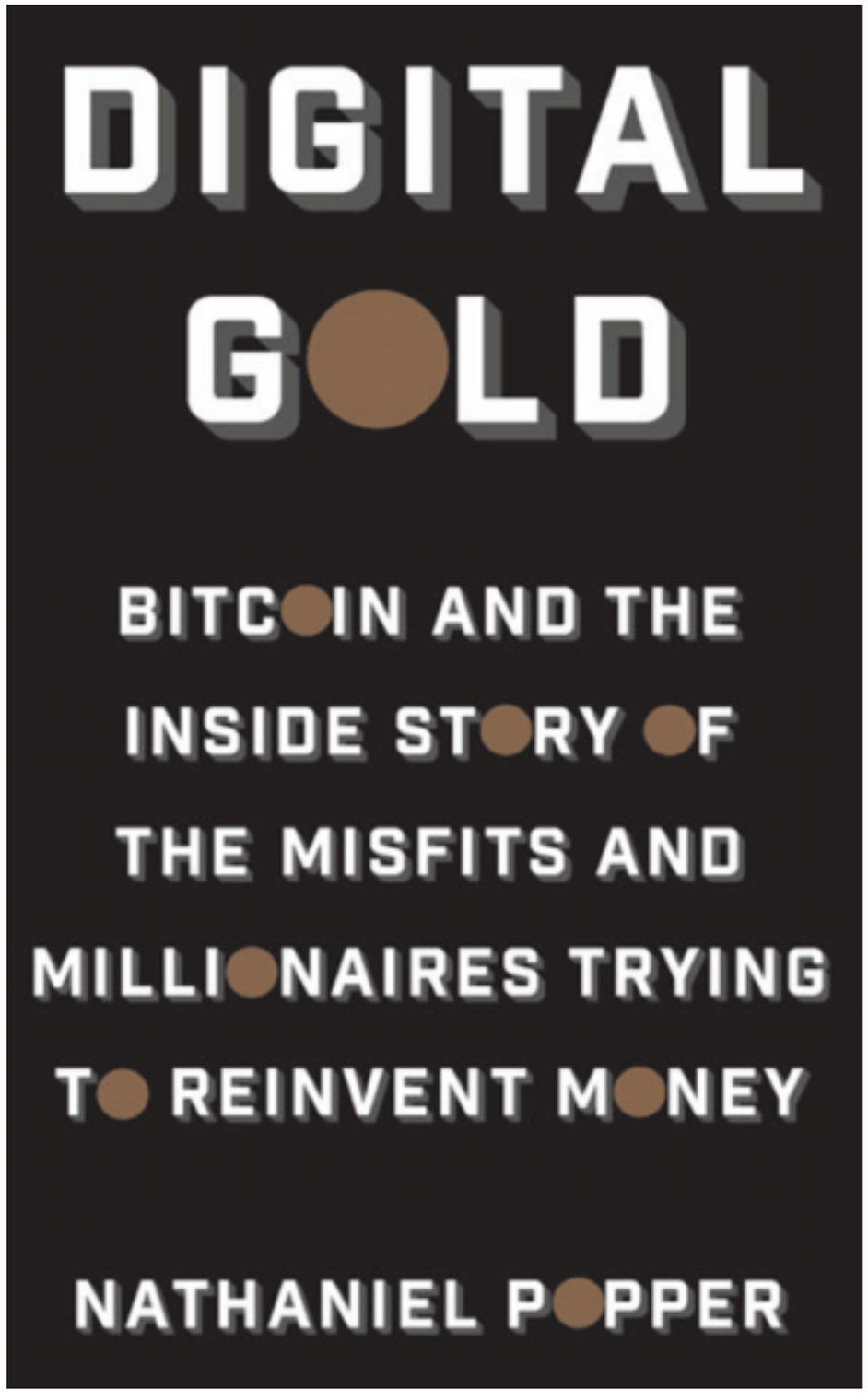
# Bitcoin and Blockchains




yearup

Updated 12-19-2017

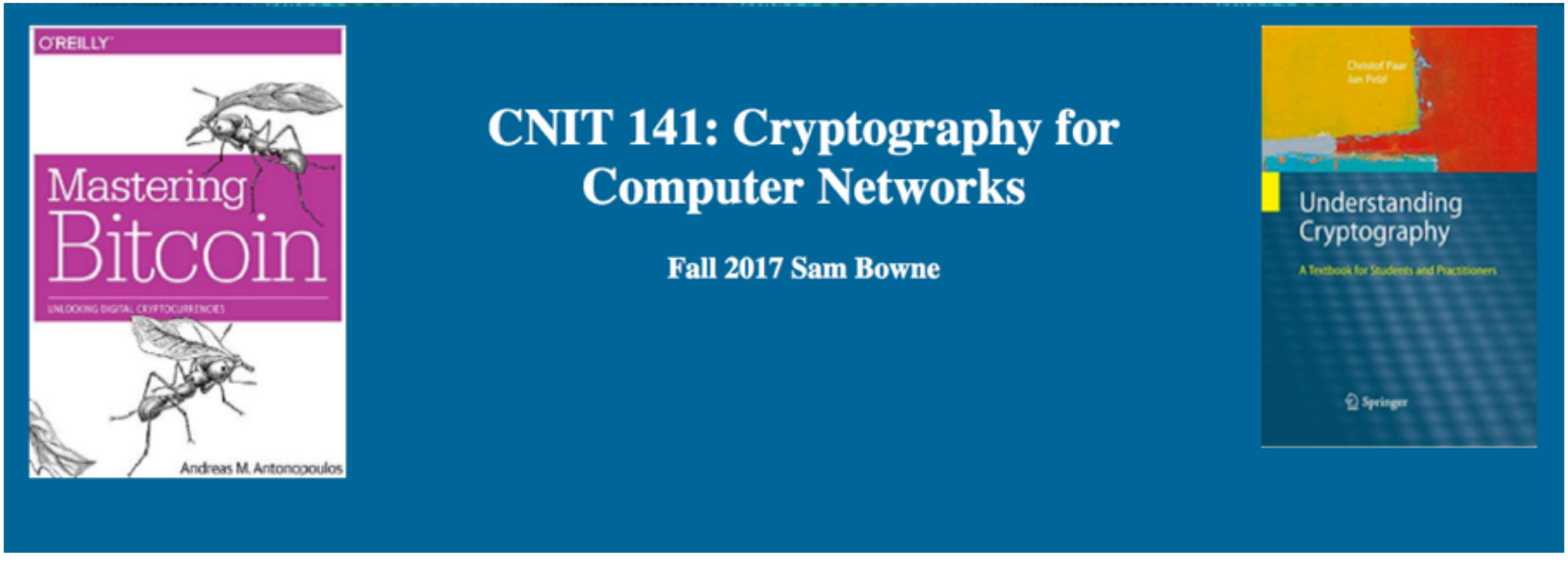
# Me

**Sam Bowne**

@sambowne

I teach security and hacking at City College San Francisco.

# Class


O'REILLY
Mastering
Bitcoin
UNLOCKING DIGITAL CRYPTOCURRENCIES
Andreas M. Antonopoulos
CNIT 141: Cryptography for
Computer Networks
Fall 2017 Sam Bowne
Christof Paar
Jan Pelzl
Understanding
Cryptography
A Textbook for Students and Practitioners
Springer

# Website

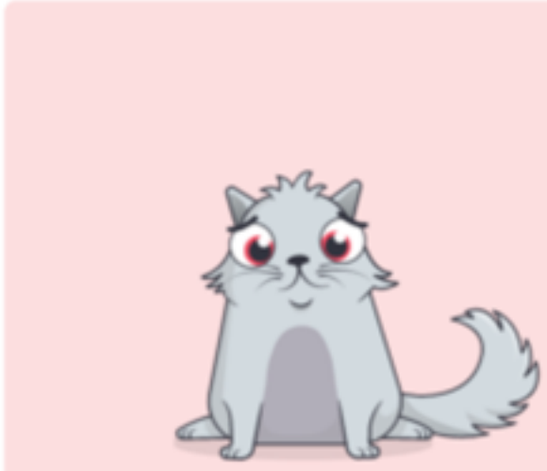
https://samsclass.info

YearUp, 12:30, 80 Sutter Street, San Francisco

Tue, Dec 19, 2017

Slides · Key

Cryptokitties Project



Ethereum

**Kitty 294354 · Gen 19**

Slow

Bitcoin

**Kitty 160236 · Gen 8**

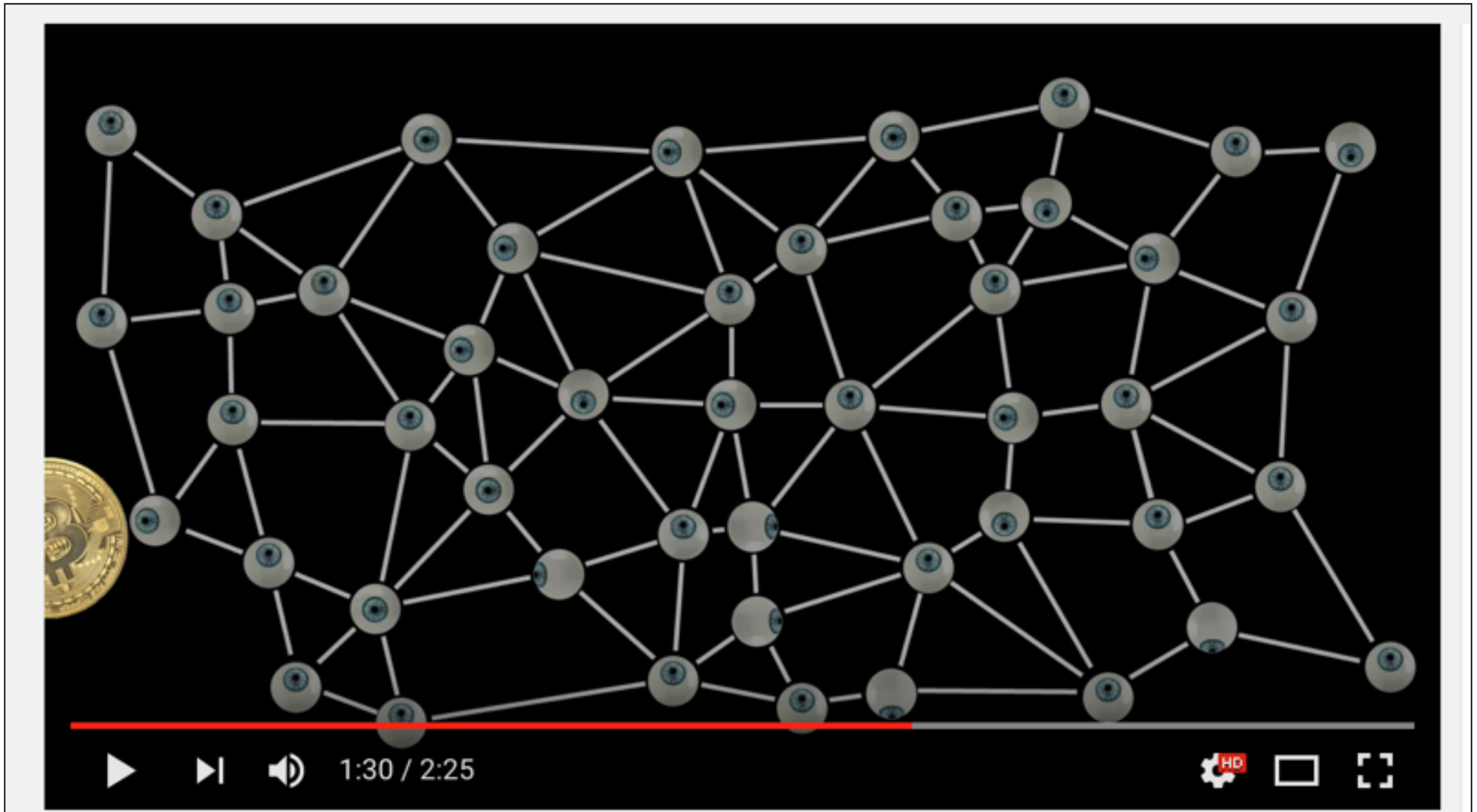
Plodding

IOTA

**Kitty 241311 · Gen 20**

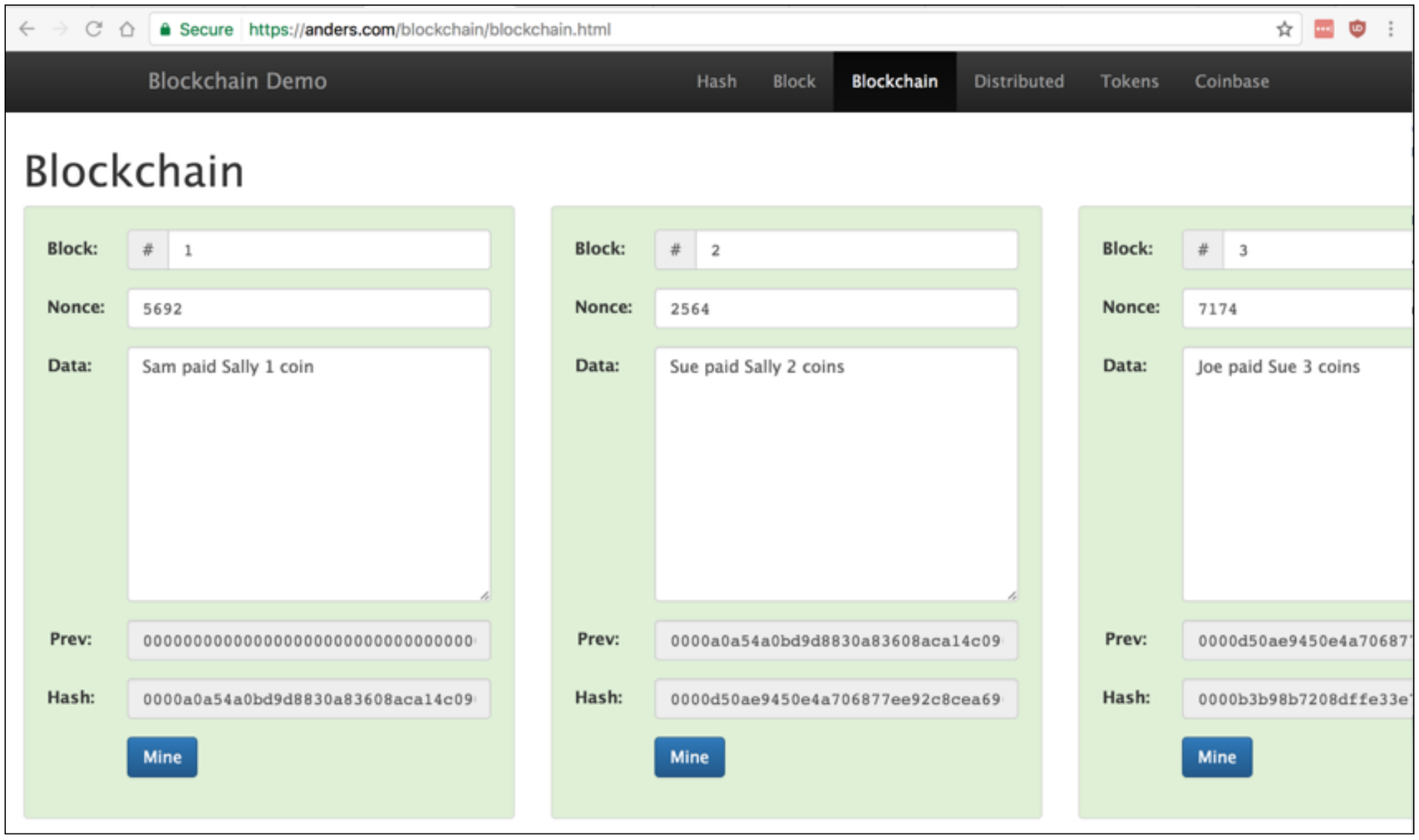
Slow

# What's a Blockchain?




Understand the Blockchain in Two Minutes

# Live Online Blockchain Demo




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

# 0.75% of all Bitcoins Stolen

## *Bitcoin Plunges After Hacking of Exchange in Hong Kong*

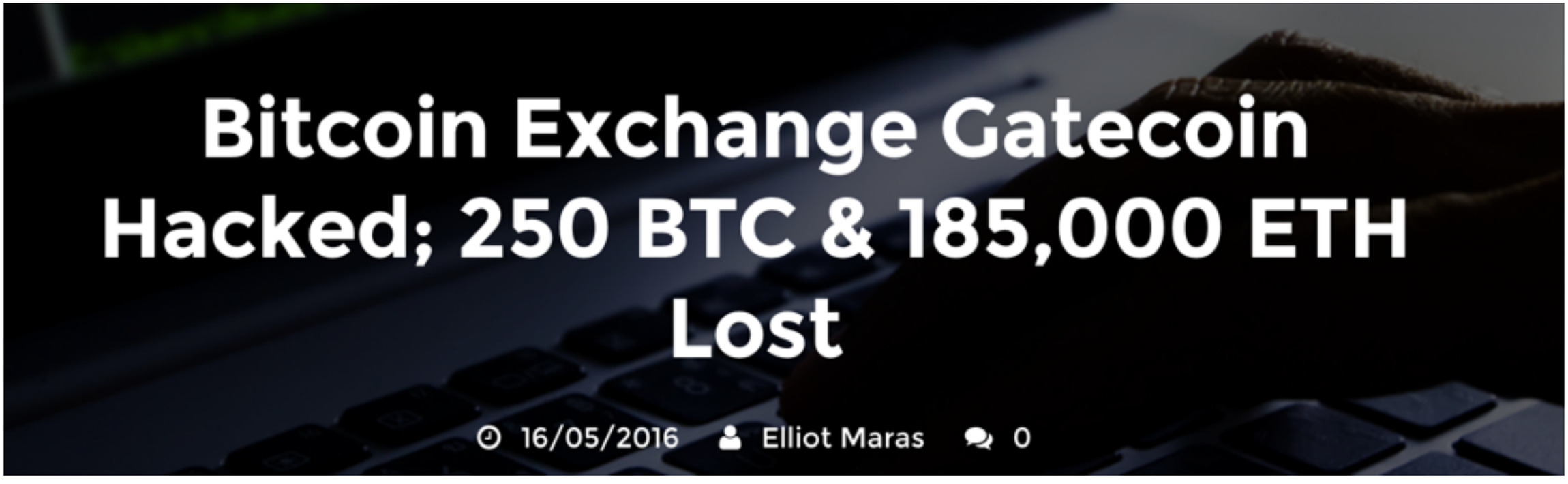
By AMIE TSANG AUG. 3, 2016

## The Bitfinex Bitcoin Hack:

## One of the world's largest bitcoin exchanges lost $65 million in a hack

# Details of $5 Million Bitstamp Hack Revealed

Stan Higgins | Published on July 1, 2015 at 22:45 BST



# Suspected multi-million dollar Bitcoin pyramid scheme shuts down, investors revolt

By Adrianne Jeffries on August 27, 2012 03:43 pm Email @adrjeffries

# Bitcoin exchange BitFloor shuttered after virtual heist

Nearly a quarter million dollars worth of the peer-to-peer currency was stolen by accessing unencrypted backup wallet keys.

Internet

September 4, 2012

# Cryptsy Hacked: Bitcoin Worth $USD 6 Million Stolen

*By Ali Raza* on January 18, 2016 *Email* *@hackread* CYBER ATTACKS HACKING NEWS MALWARE

**The hacker inserted a Trojan malware into Cryptsy's code so that he could access precious information and transfer cyber currencies.**

# Bitcoin site Inputs.io loses £1m after hackers strike twice

Inputs.io, run by a developer known as TradeFortress, waits two weeks to report loss of 4,100 Bitcoins in two separate hacks to its customers

# Danish Bitcoin exchange BIPS hacked and 1,295 Bitcoins worth $1 Million Stolen

Monday, November 25, 2013 Swati Khandelwal

# $4.1 Million goes missing as Chinese bitcoin trading platform GBL vanishes

Kadhim Shubber (@kadhimshubber) | Published on November 11, 2013 at 17:15 BST

# Largest Bitcoin Heists Before 2014

## Critical (≥10 k฿)

| Rank | Name | Time | Severity |
|---|---|---|---|
| 1 | Bitcoin Savings and Trust | 2011–2012 | est. 263024 ฿ |
| 2 | Silk Road Seizure | October 2013 | 171955.09292687 ฿ |
| 3 | MyBitcoin Theft | July 2011 | 78739.58205388 ฿ |
| 4 | Linode Hacks | March 2012 | l.b. 46653.46630495 ฿ |
| 5 | July 2012 Bitcoinica Theft | July 2012 | 40000.00000000 ฿ |
| 6* | May 2012 Bitcoinica Hack | May 2012<br>Unresolved as of December 2012 | 18547.66867623 ฿<br>39000 ฿ total impact |
| 7 | Allinvain Theft | June 2011 | 25000.01000000 ฿ |
| 8 | Tony Silk Road Scam | April 2012 | est. 30000 ฿ |
| 9 | Bitfloor Theft | September 2012 | u.b. 24086.17219307 ฿ |
| 10 | *Bitomat.pl Loss* | August 2011 | est. 17000 ฿ |

* Rank includes pass-through impact

# Poloniex Loses 12.3% of its Bitcoins in Latest Bitcoin Exchange Hack

Pete Rizzo (@pete_rizzo_) | Published on March 5, 2014 at 20:11 BST

# Secret Service Agent Gets Six-Year Sentence for Bitcoin Theft

Stan Higgins | Published on December 7, 2015 at 21:42 BST

# Bitcoin Price History

# Bitcoin Prices in 2017

- From $1000 to $17000 in one year
- What real value has increased this year?

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

MAULDIN ECONOMICS

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



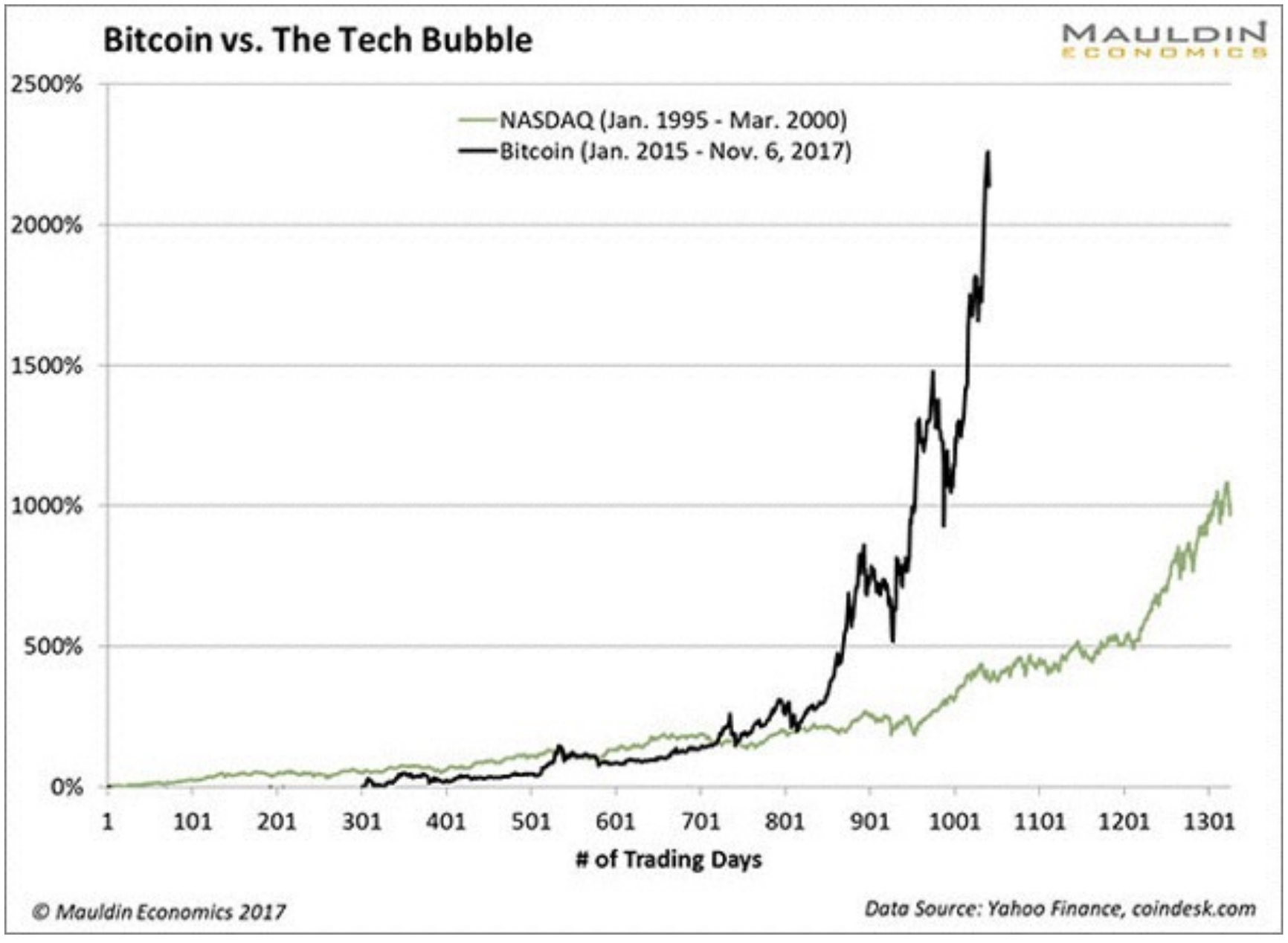
Editorial

# The Bitcoin Bubble Explained in 4 Charts

NOVEMBER 13, 2017

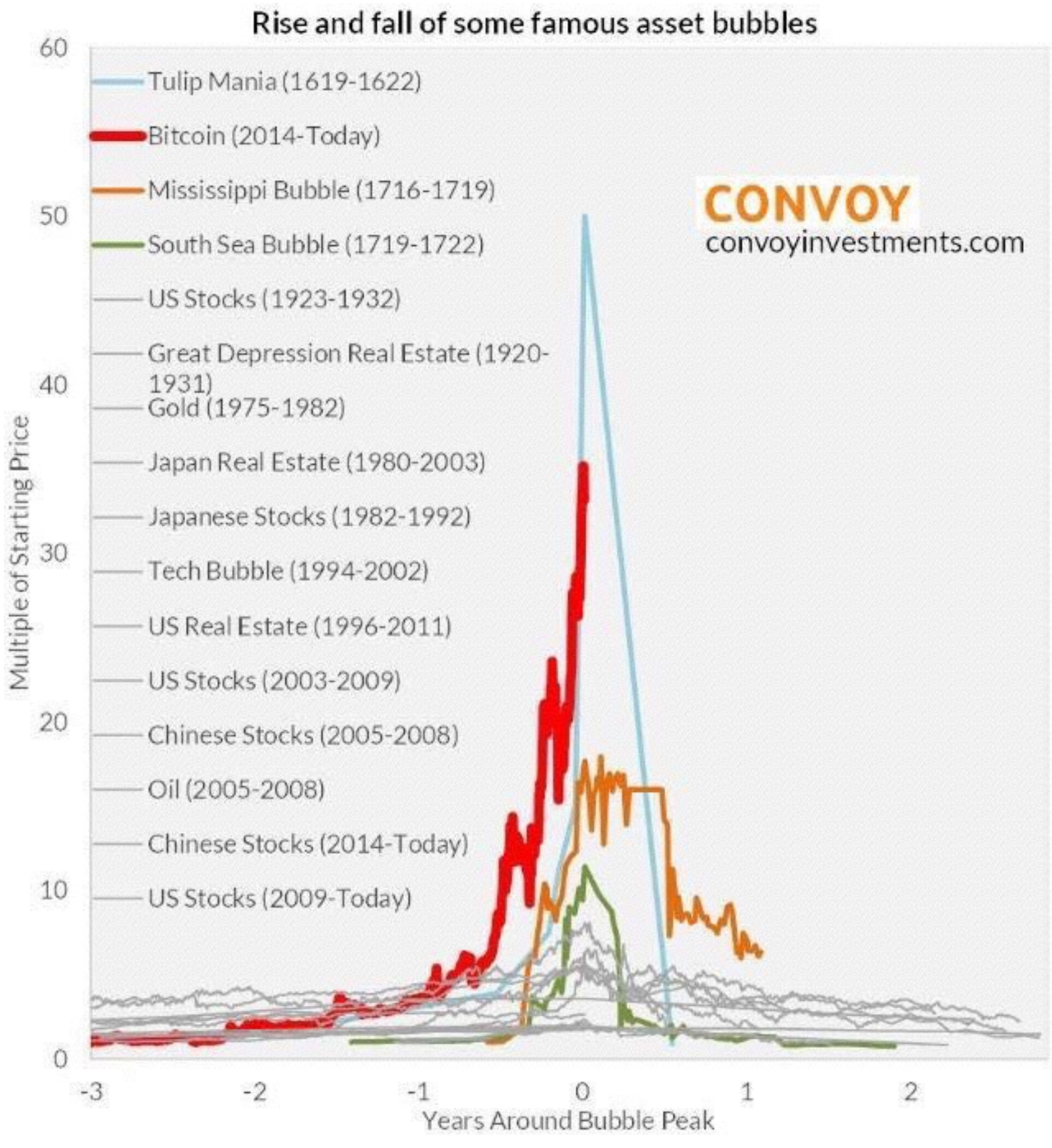
BY JAKE WEBER

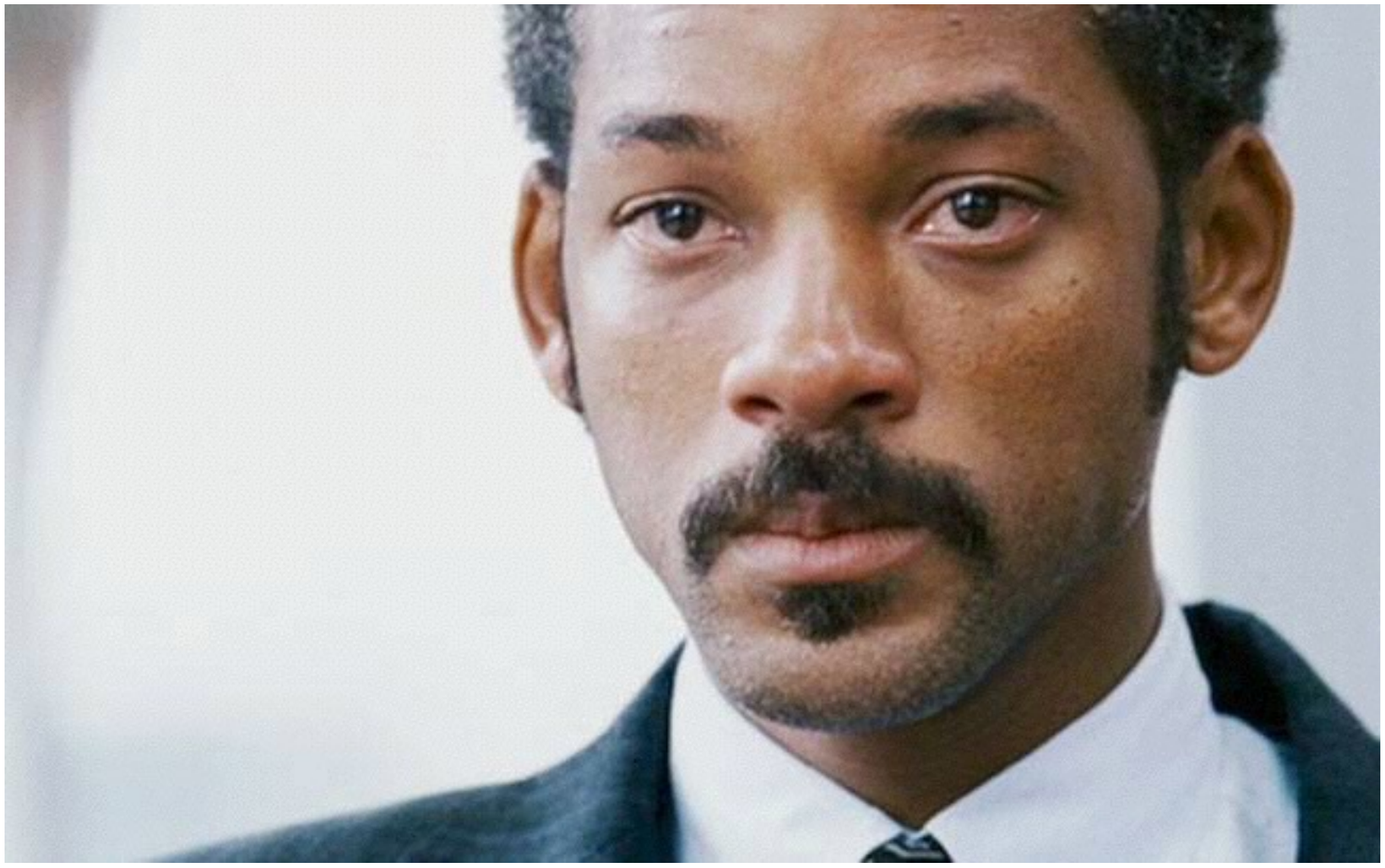
# Bitcoin Rose Faster than the DotCom Bubble



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

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

Bitcoin – 3 to 4 transactions per second

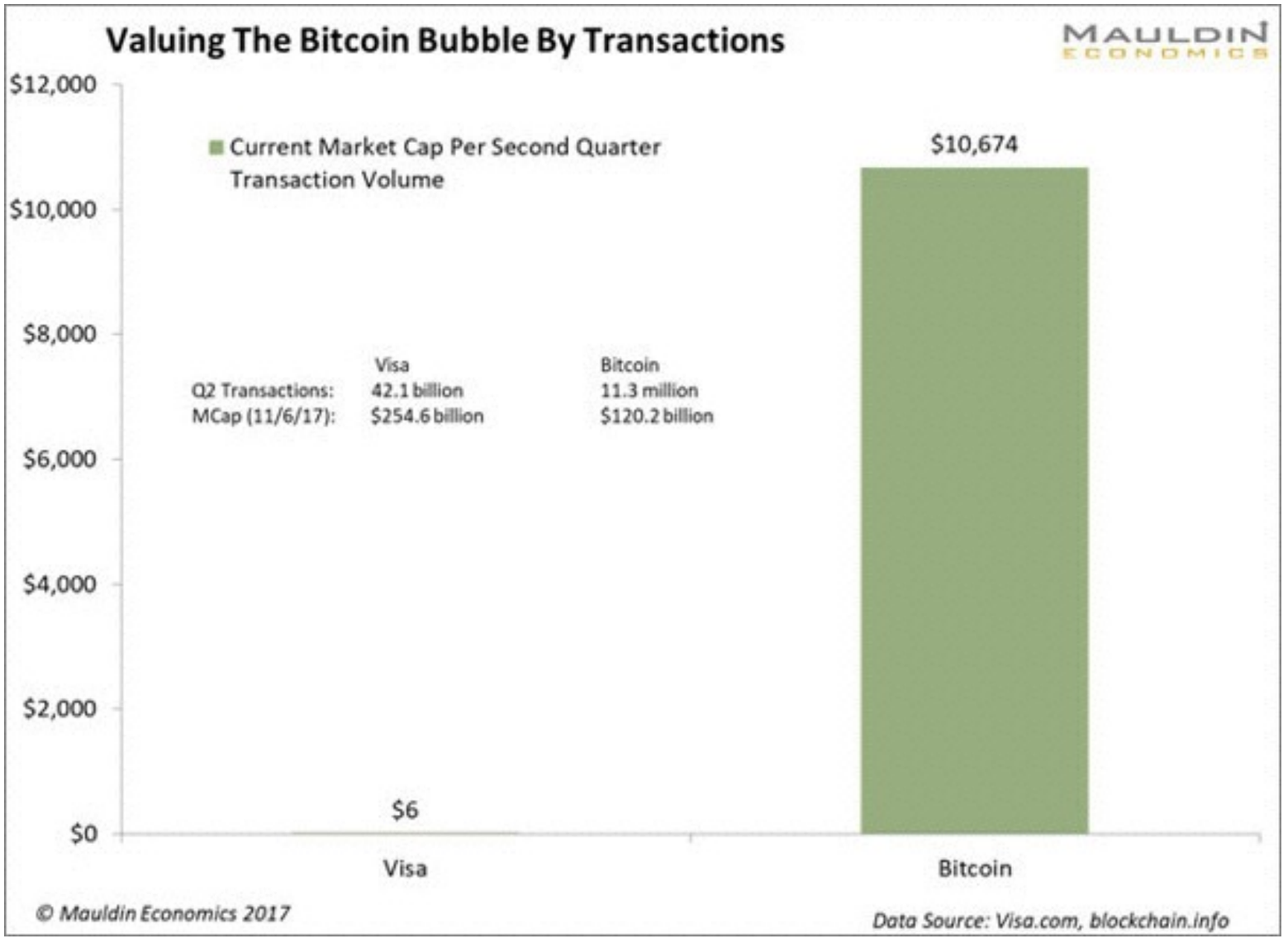
Ethereum – 20 transactions per second

PayPal – 193 transactions per second average

Visa – 1,667 transaction per second

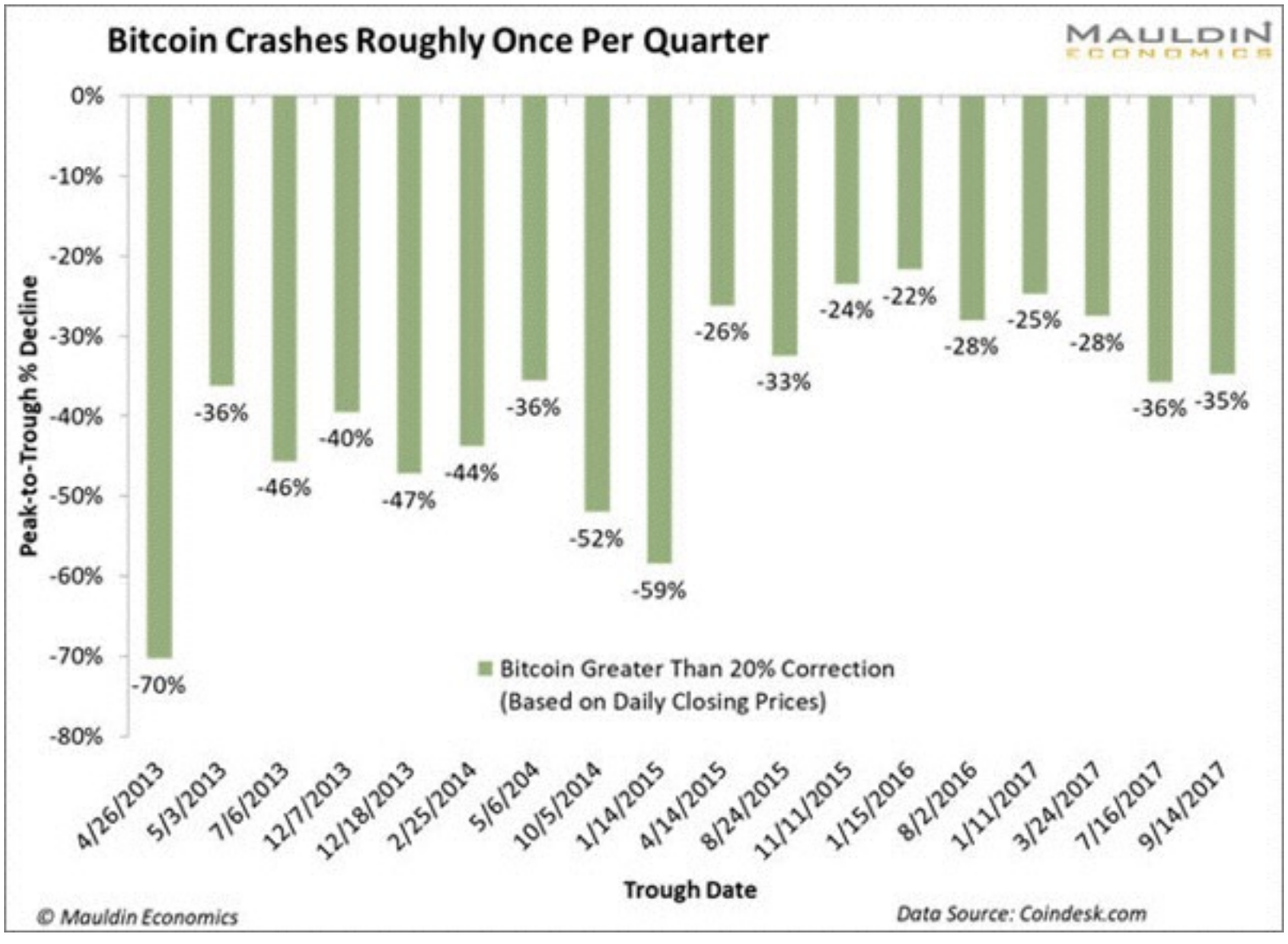
www.altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/

# Is Bitcoin a Means of Enchange?

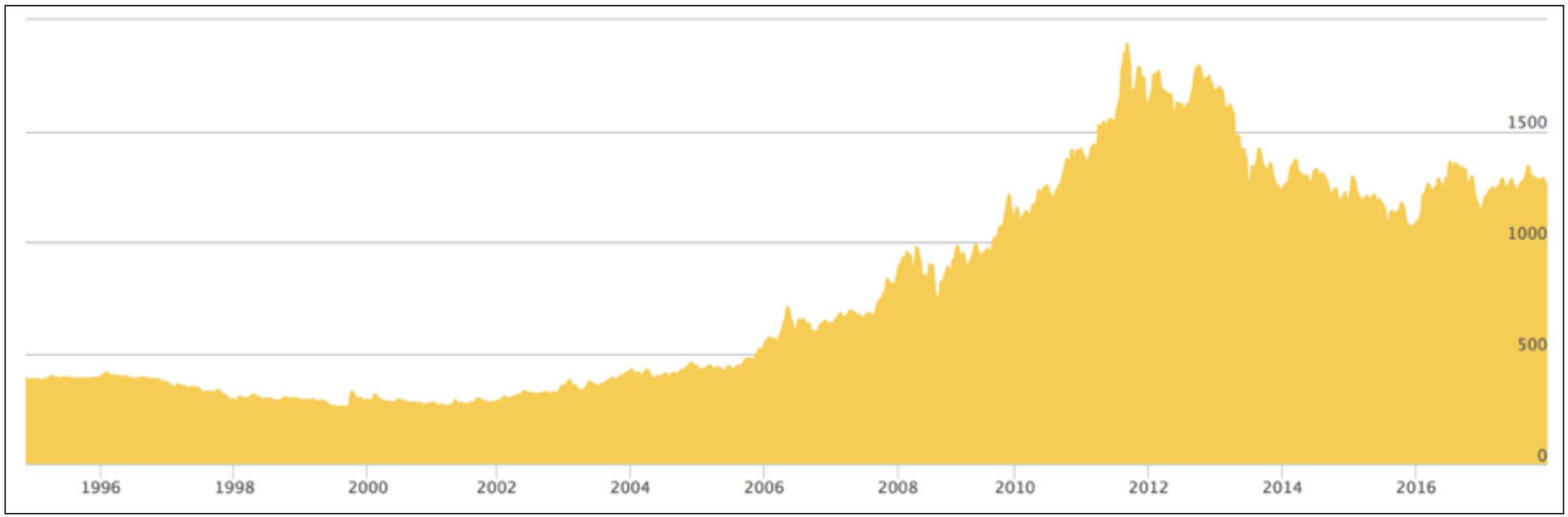



- Visa is valued at $6 per transaction
- Bitcoin over $10,000 per transaction

# Is Bitcoin a Store of Value?

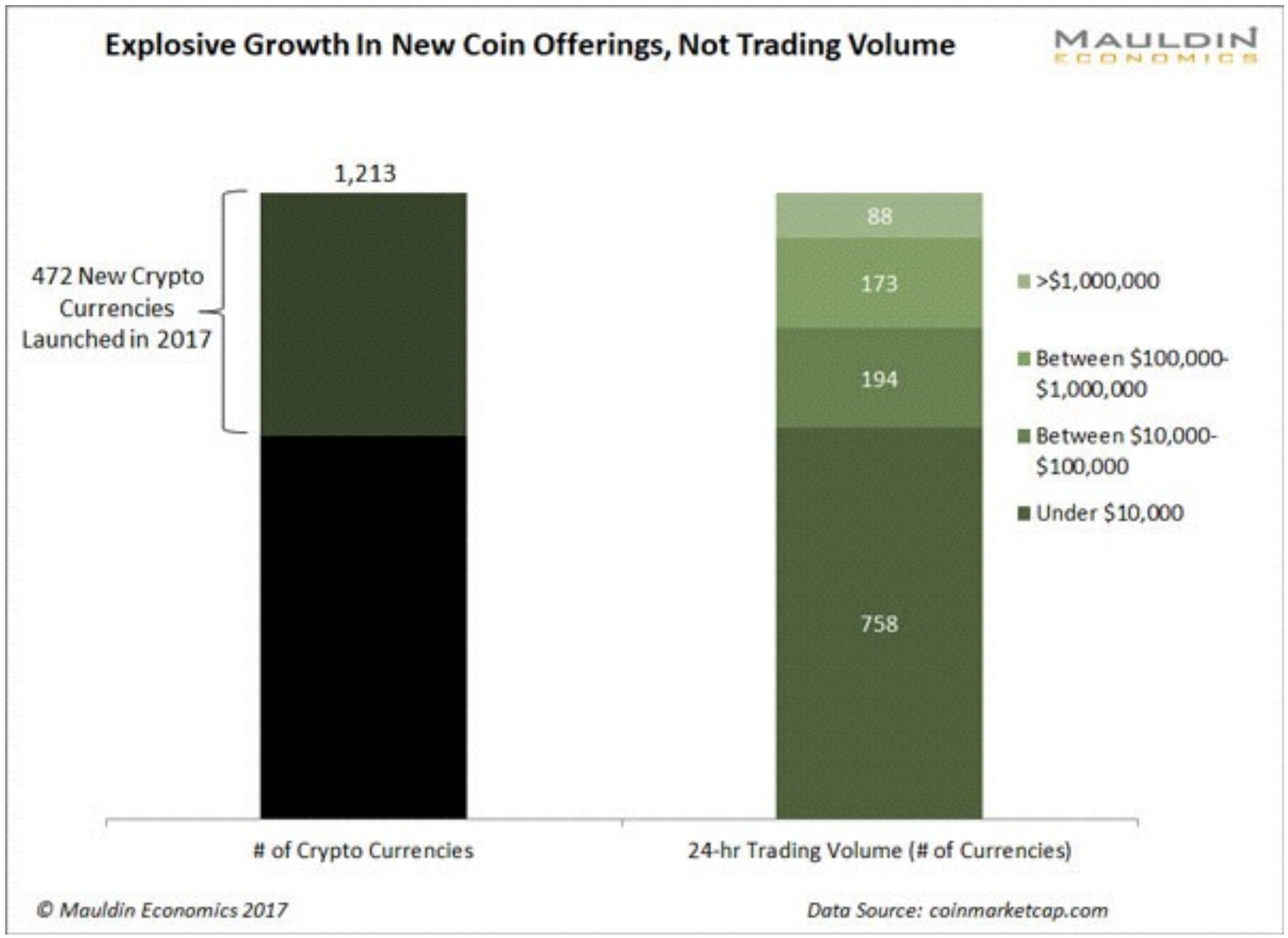


# Gold is the Classic Store of Value




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

# Initial Coin Offerings (ICO)



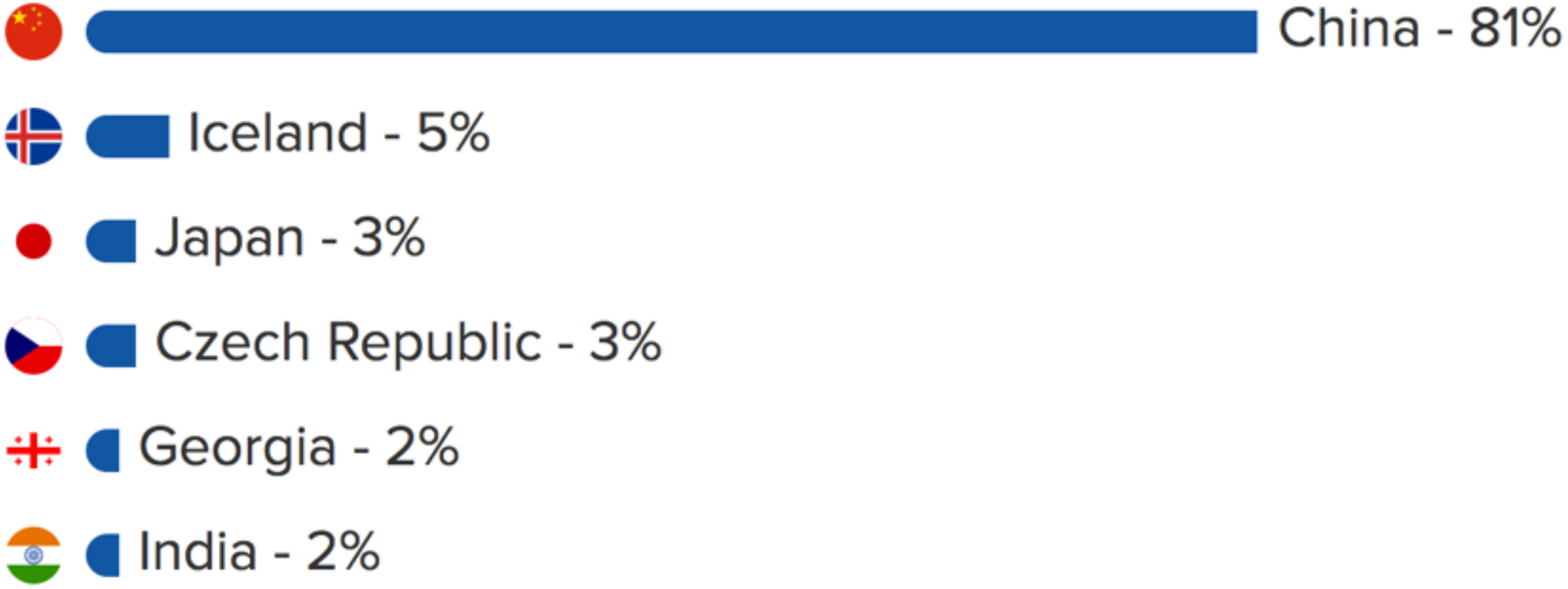

...only 20 of the currencies are actually being used for something other than trading. The rest are purely speculative trading instruments.

# Cryptocurrency Infographic

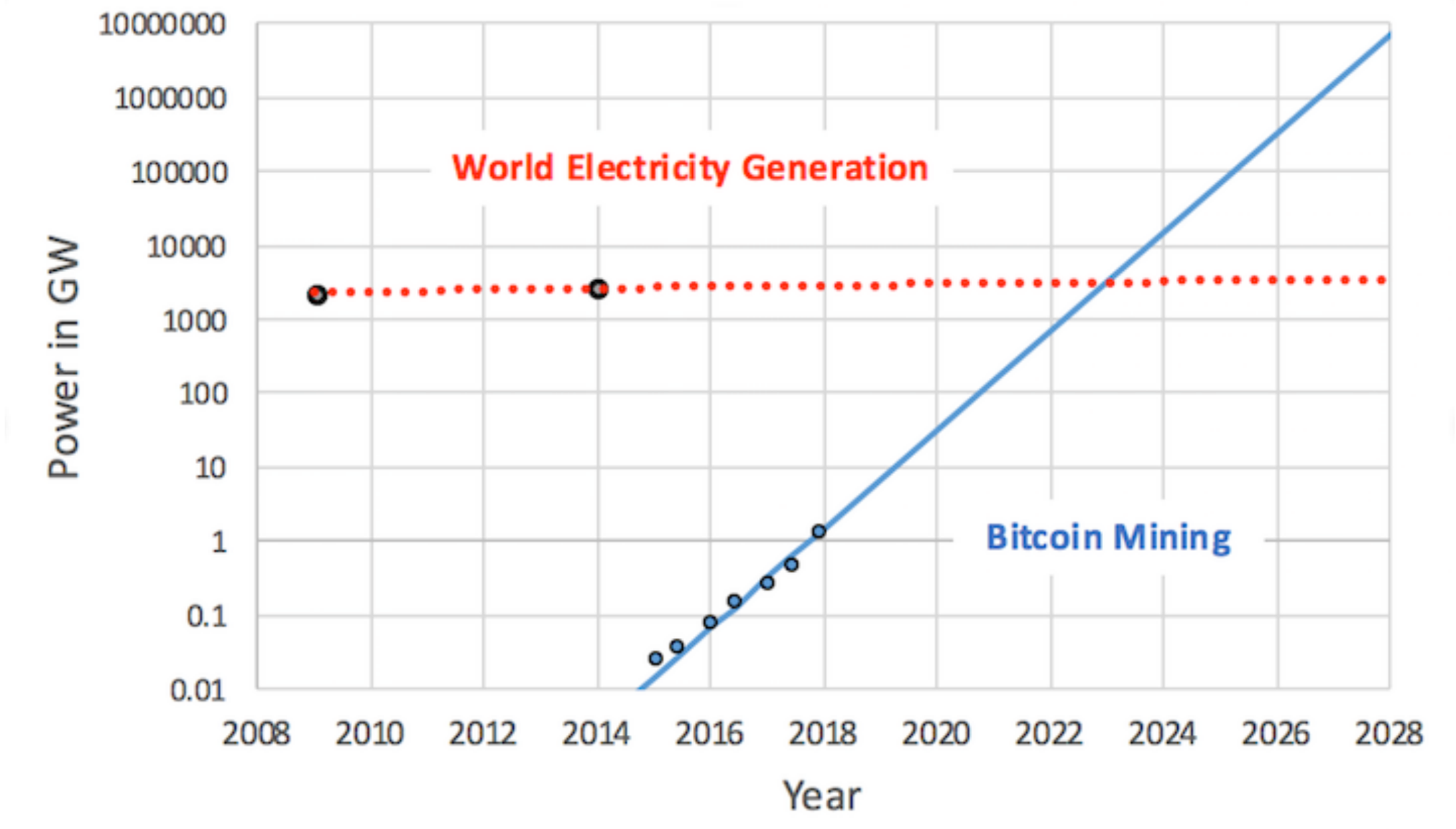
https://youtu.be/Gq_bjaI0NTo

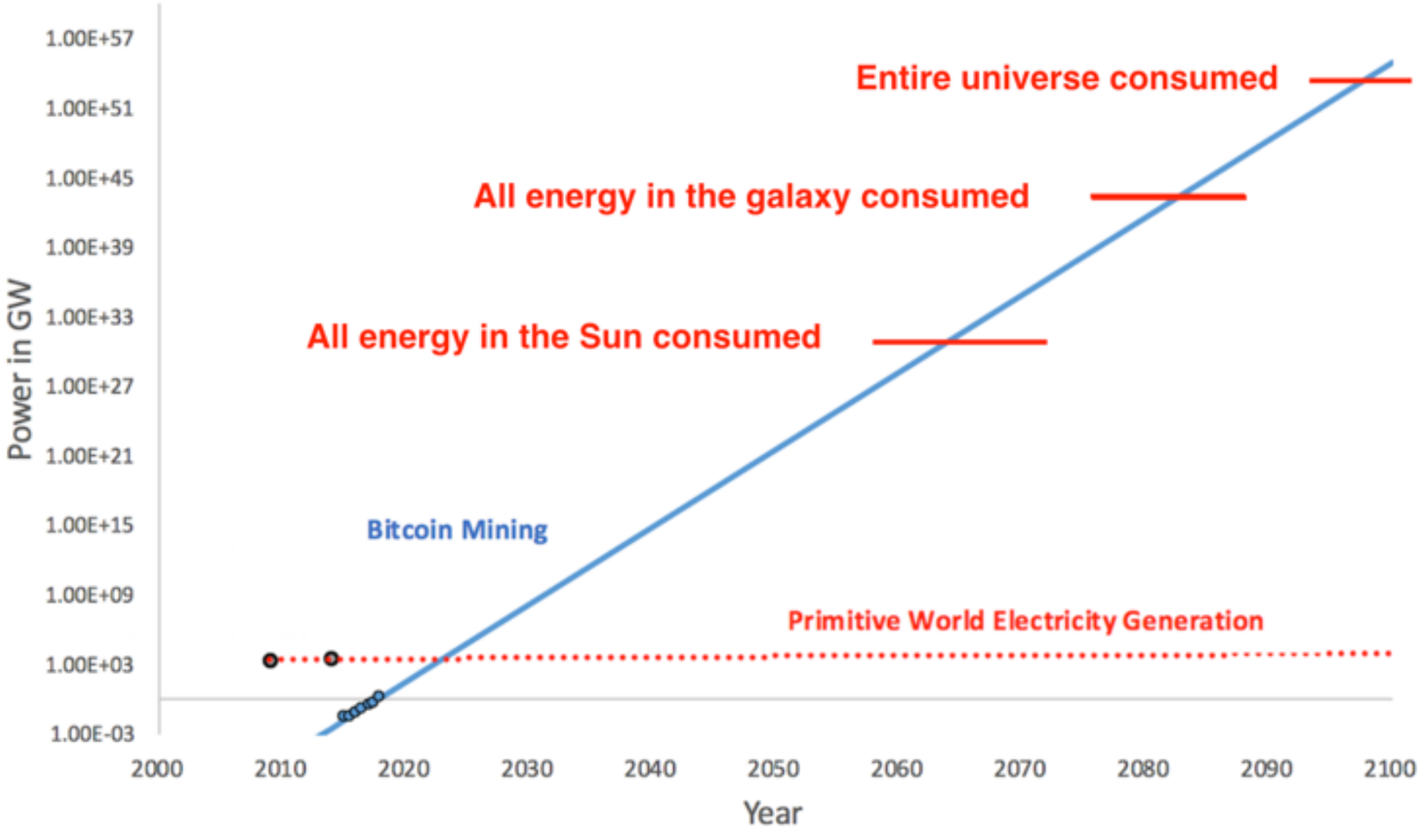
# Bitcoin Mining Pools

Jordan Tuwiner Last updated July 13, 2017



# Bitcoin Power Consumption




Entire universe consumed
All energy in the galaxy consumed
All energy in the Sun consumed
Bitcoin Mining
Primitive World Electricity Generation
Power in GW
1.00E+57
1.00E+51
1.00E+45
1.00E+39
1.00E+33
1.00E+27
1.00E+21
1.00E+15
1.00E+09
1.00E+03
1.00E-03
2000
2010
2020
2030
2040
2050
2060
2070
2080
2090
2100
Year

# 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

# 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

https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/

# 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

mashable.com/2017/07/26/ethereum-stolen-white-hat-group-rescued/#Czl1YnISSPqz

# 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."

deadline.com/2017/11/big-hack-freezes-156m-in-funds-damaging-some-entertainment-startups-1202206411/

# Blockchains

THE WALL STREET JOURNAL.

# Blockchain Experts, a Rare Breed, May Demand Big Bucks

By KIM S. NASH

May 12, 2016 5:48 pm ET

0 COMMENTS

Lamar Wilson, chief executive of blockchain startup Fluent, said he tried to hire two blockchain engineers early this year and that they told him, separately, they had offers from different Wall Street firms for jobs that paid $250,000 in salary.

# Blockchain jobs continue to explode, offer salary premiums

Blockchain development is the second-hottest skill in the job market today, growing more than 200% since this time last year.

By Lucas Mearian

Senior Reporter, Computerworld | DEC 15, 2017 10:25 AM PT

# Quarterly Skills Index

## The top 20 fastest-growing skills, Q3 2017

### 1 ROBOTICS

Develop machines that can substitute for humans such as opening doors or making a cup of coffee.

### 2 BLOCKCHAIN

A Distributed Ledger Technology (DTL) that verifies and records Bitcoin transactions.

### 3 BITCOIN

A cryptocurrency and peer-to-peer digital payment system that aims to remove friction from transactions.

### 4 PENETRATION TESTING

Test computer systems, networks and web apps to find vulnerabilities.

### 5 REACT.JS

A JavaScript library for building user interfaces.

### 6 AMAZON WEB SERVICE LAMBDA

Run code without provisioning or managing servers and pay only for the compute time you consume.

### ADDITIONAL SKILLS

7 Augmented Reality

8 Deep Learning

9 Instagram Marketing

10 Final Cut Pro X

11 Swift Development

12 AngularJS Development

13 Salesforce

14 Vulnerability Assessment

15 Natural Language Processing

16 HubSpot Marketing

17 Machine Learning

18 Objective-C Development

19 Learning Management System (LMS)

20 jQuery Development

upwork™

# 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, ...

www.cloudpro.co.uk/it-infrastructure/6086/microsoft-launches-project-bletchley-blockchain-framev

# Microsoft launches Project Bletchley blockchain framework

WRITTEN BY
Clare Hopping

News

17 Jun, 2016

## The project will outline Microsoft's plans for creating an open, modular blockchain fabric powered by Azure

Microsoft has announced its commitment to creating an open, modular blockchain fabric in the cloud with Project Bletchley.

Following the launch Microsoft Azure Blockchain as a Service (BaaS) at the tail end of last year, Microsoft has been looking for ways to build the offering and creating an entire framework around it is just the way to do it, Microsoft said.

# Ethereum Blockchain as a Service now on Azure

Posted on November 9, 2015

Marley Gray, Director, BizDev & Strategy, Cloud and Enterprise

Microsoft and ConsenSys are partnering to offer Ethereum Blockchain as a Service (EBaaS) on Microsoft Azure so Enterprise clients and developers can have a single click cloud based blockchain developer environment. The initial offering contains two tools that allow for rapid development of SmartContract based applications: Ether.Camp - An integrated developer environment, and BlockApps - a private, semi-private Ethereum blockchain environment, can deploy into the public Ethereum environment.

ETH BaaS
Ethereum Blockchain as a Service

# Hands On With Linq, Nasdaq's Private Markets Blockchain Project

Pete Rizzo (@pete_rizzo_) | Published on November 21, 2015 at 14:57 BST

FEATURE

675 229 21 446 41

Business Software

# Santander unveils first UK blockchain for international money transfers

Money transfer pilot scheme rolled out to staff aims to speed up and simplify transactions

John Leonard

@_JohnLeonard

26 May 2016

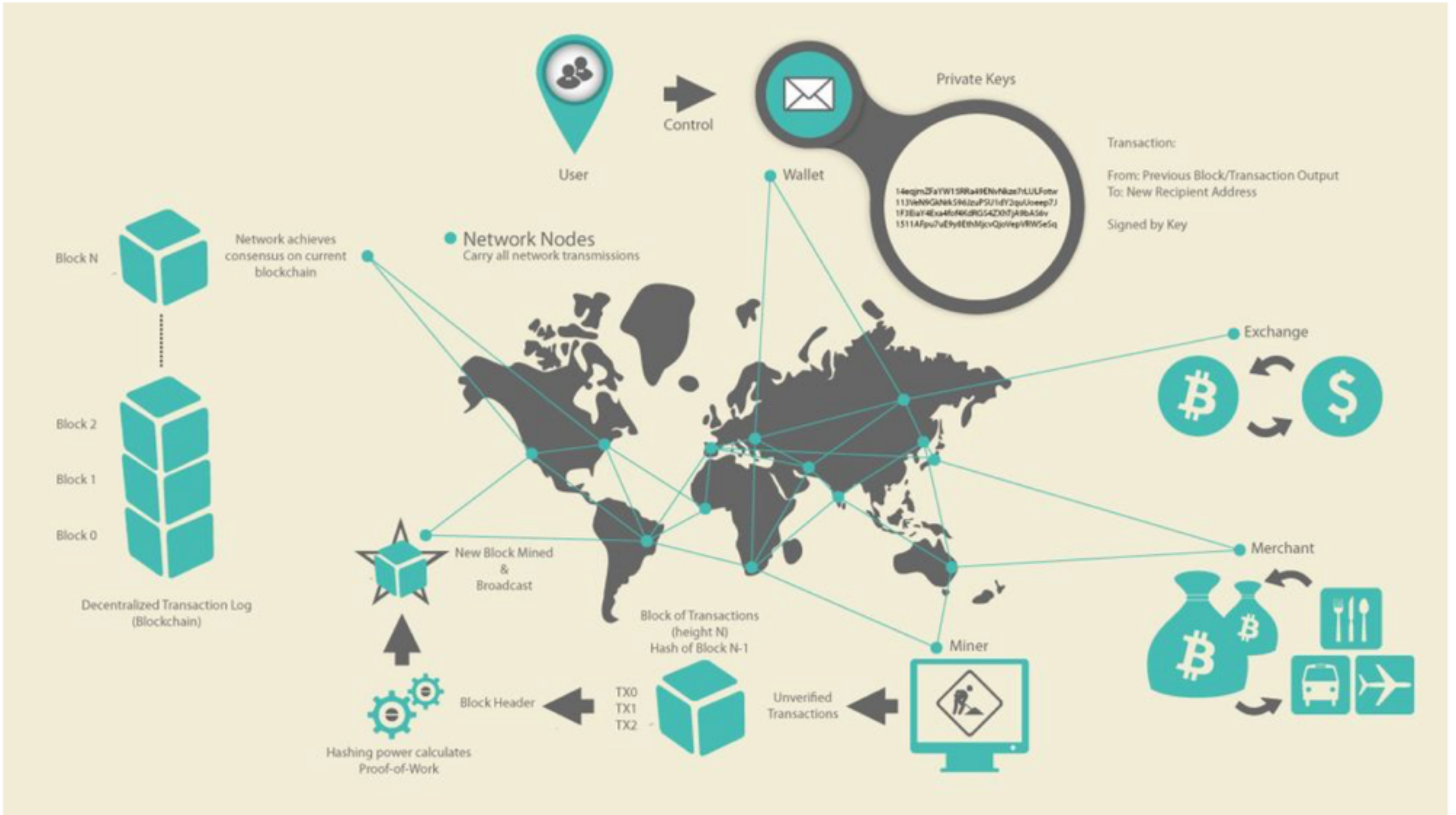
0 Comments

# Sydney Stock Exchange Developing Blockchain Trading System

Stan Higgins | Published on May 19, 2016 at 16:30 BST

As reported by the *Sydney Morning Herald*, the Sydney Stock Exchange (SSX) will initially look to facilitate the trade of private stocks, but will eventually open the system up to publicly traded stocks as well. The project brings to mind Linq, the blockchain project developed by securities exchange operator Nasdaq in partnership with blockchain startup Chain.

# How Bitcoin Works



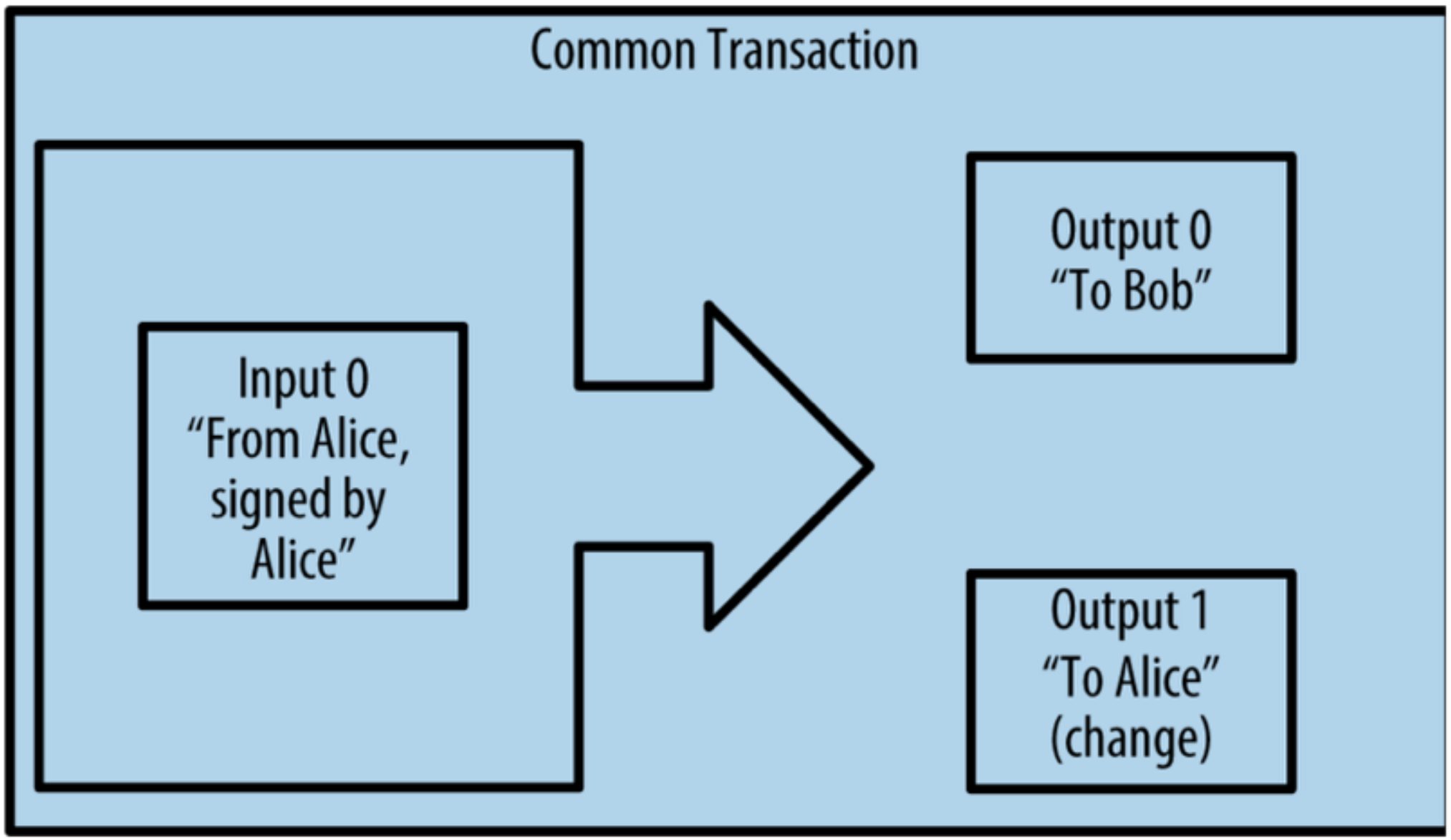



*Figure 2-5. Most common transaction*

# 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

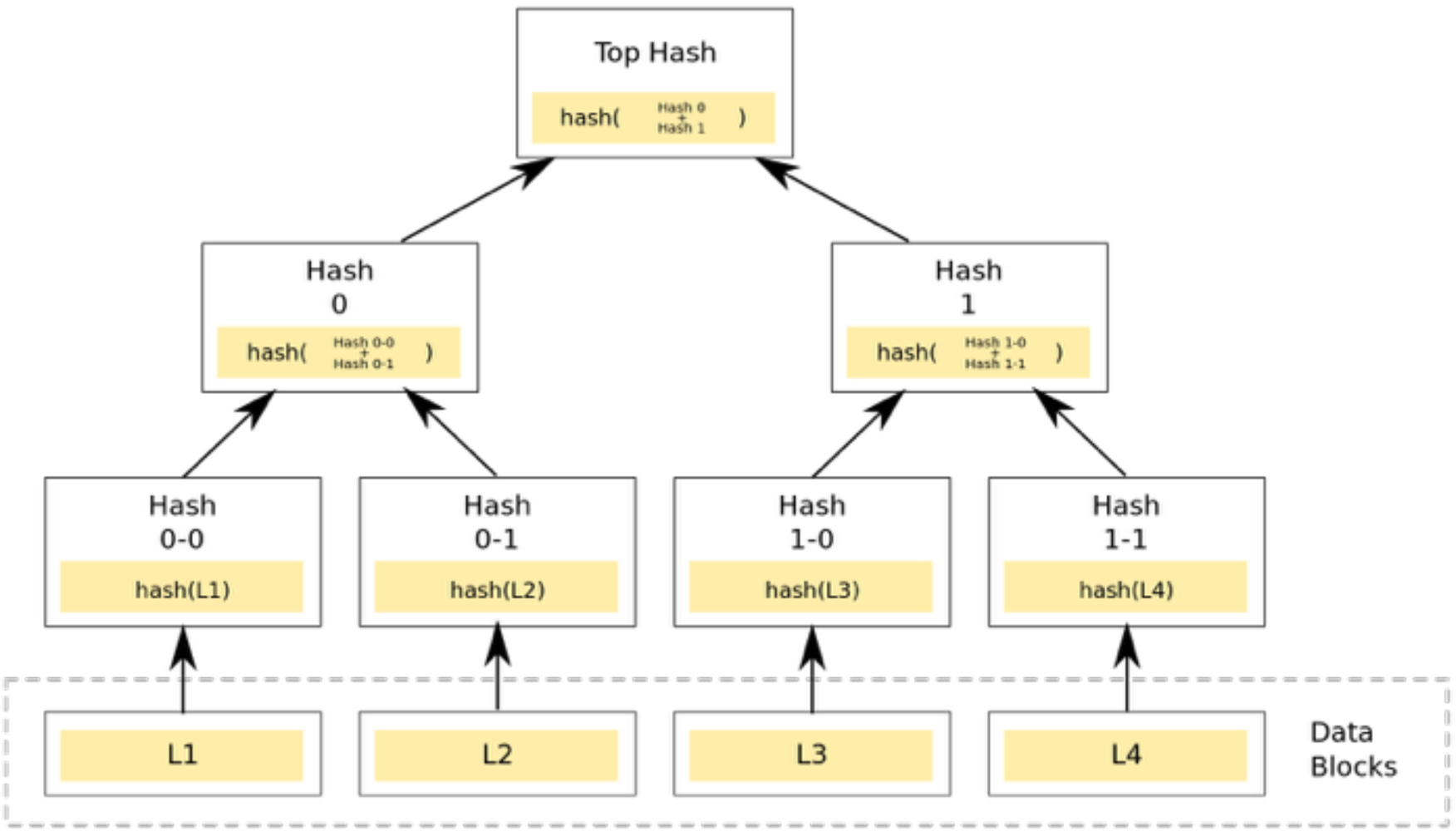
- "Satoshi Nakamoto" invented and launched Bitcoin on Jan. 3, 2009

- A response to the 2008 financial crisis

- Fiat money without any bank or government controlling it

# Merkle Tree

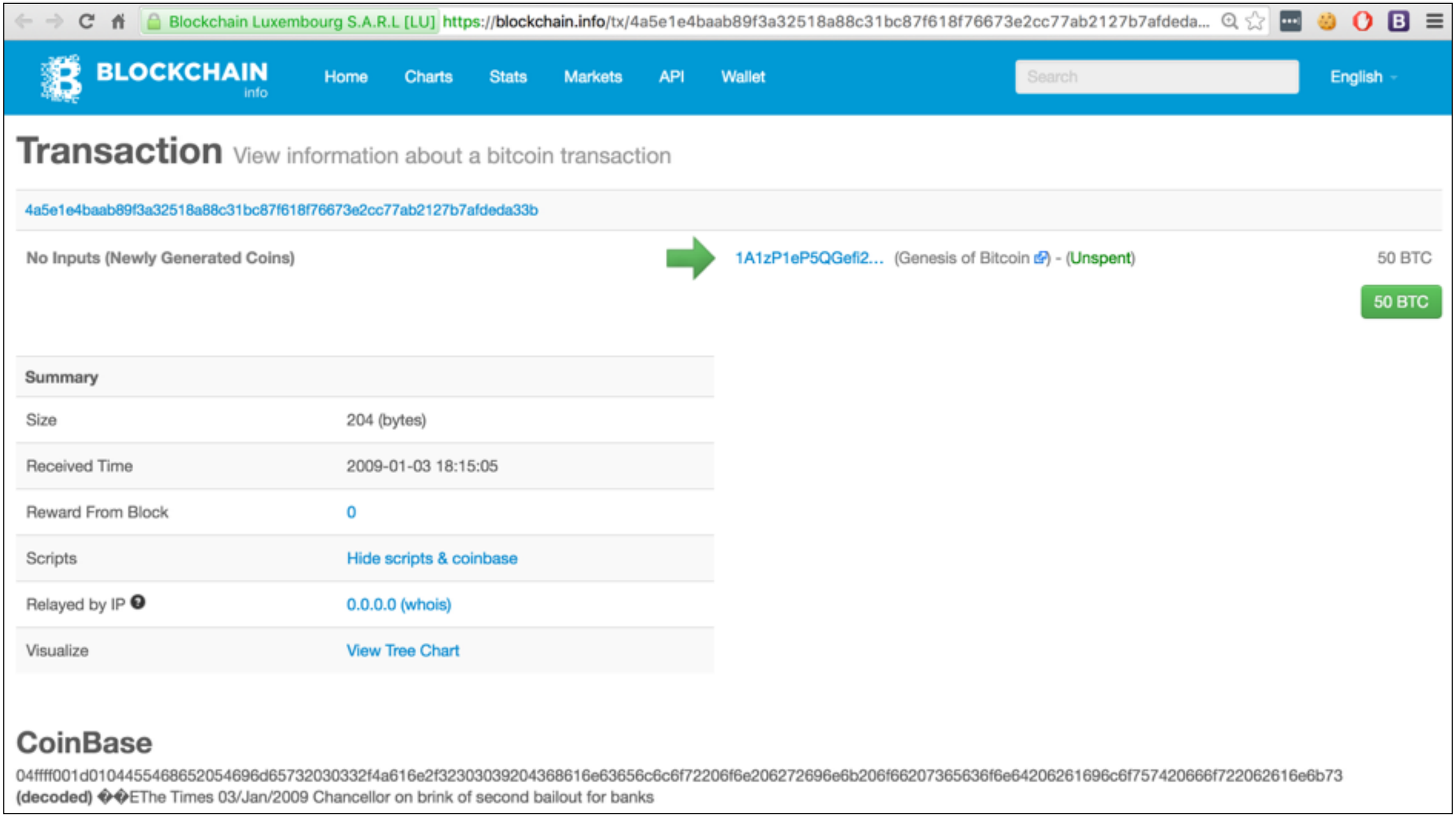
- Designed to "allow efficient and secure verification of large data structures" -- Link Bitcoin 2



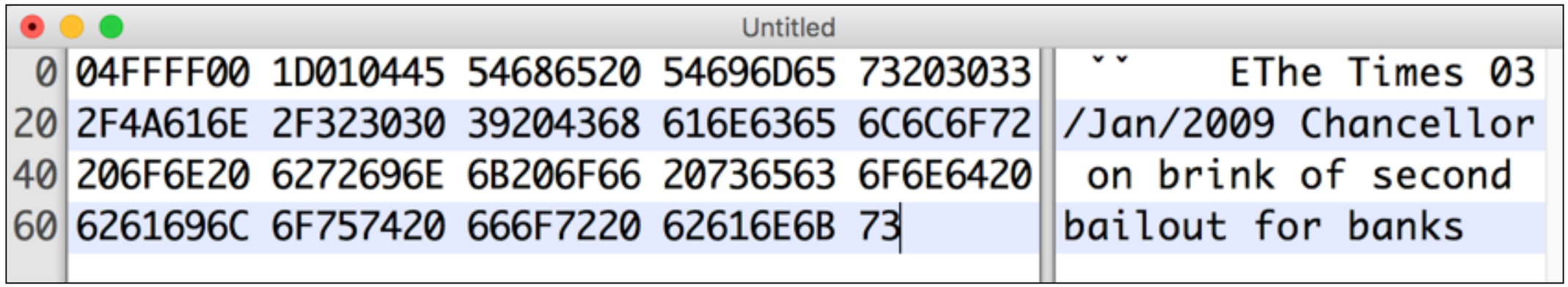
# Block

- 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)

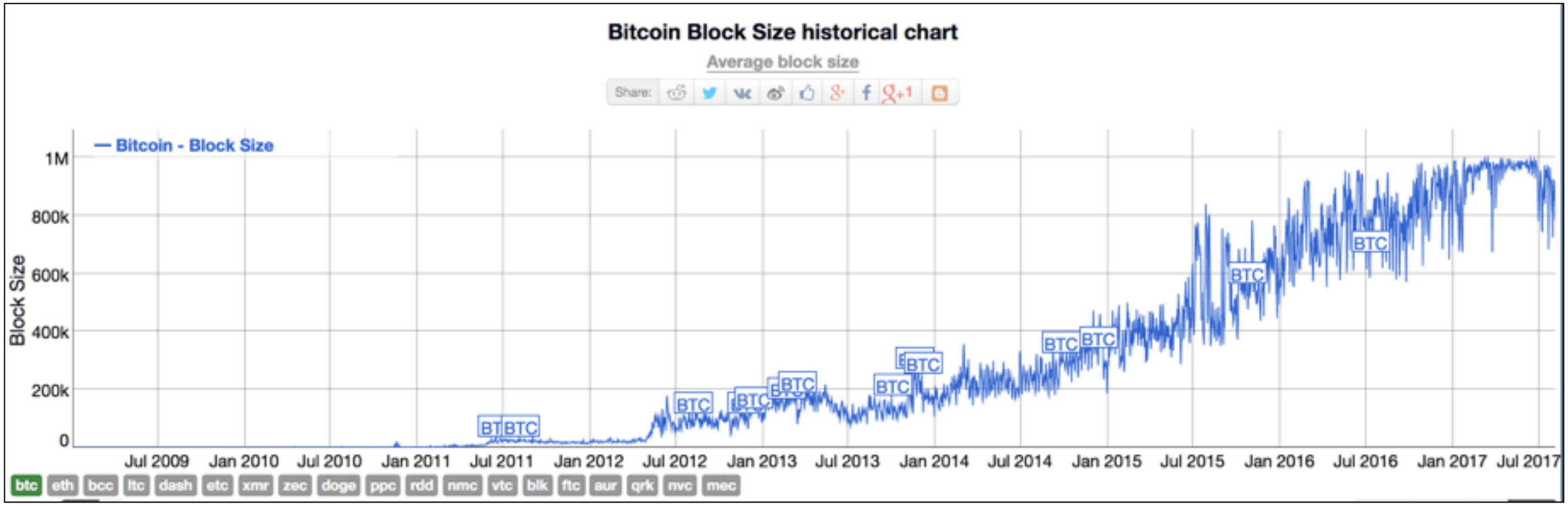
# Genesis Block



# Decoding the Coinbase



# Bitcoin's Block Size Limit




- Bitcoin has reached its limit of transactions per block
  - Link Bitcoin 24

# Bitcoin Forked in Aug, 2017

**Why was a fork necessary to create Bitcoin Cash?**
The legacy Bitcoin code had a maximum limit of 1MB of data per block, or about 3 transactions per second. Although technically simple to raise this limit, the community could not reach a consensus, even after years of debate.

**Was the 1 MB blocksize causing problems for Bitcoin?**
Yes, In 2017, capacity hit the 'invisible wall'. Fees skyrocketed, and Bitcoin became unreliable, with some users unable to get their transactions confirmed, even after days of waiting.

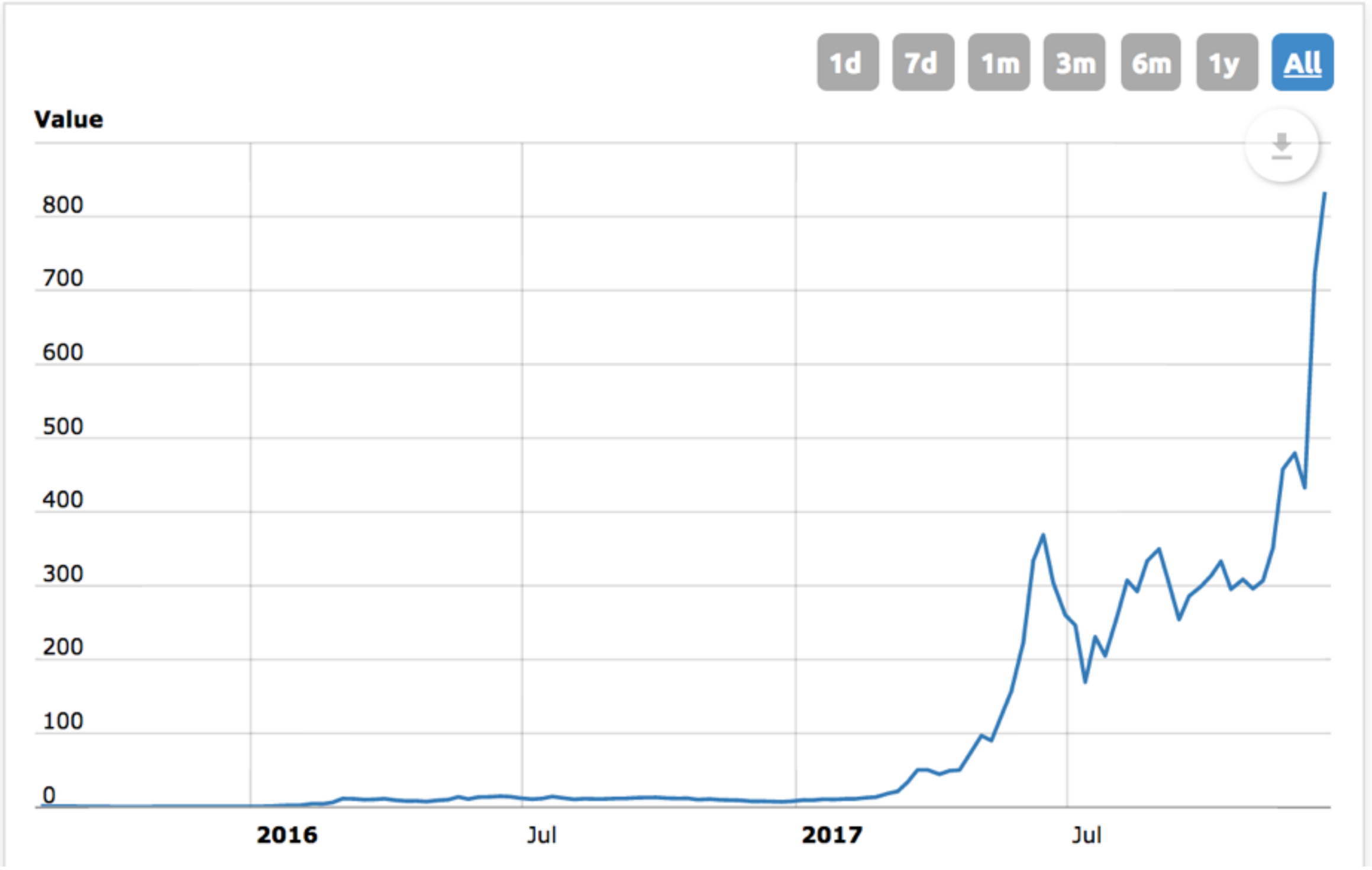
Bitcoin stopped growing. Many users, merchants, businesses and investors abandoned Bitcoin. Its marketshare among other cryptocurrencies quickly plummeted from 95% to 40%.

**Does Bitcoin Cash fix these problems?**
Yes. Bitcoin Cash immediately raises the blocksize limit to 8MB as part of a massive on-chain scaling approach. There will be ample capacity for everyone's transactions.

Low fees and fast confirmations will resume with Bitcoin Cash. The network will be allowed to grow again. Users, merchants, businesses, and investors will return.

# Bitcoincash Charts

# Ethereum Charts



# Iota Charts

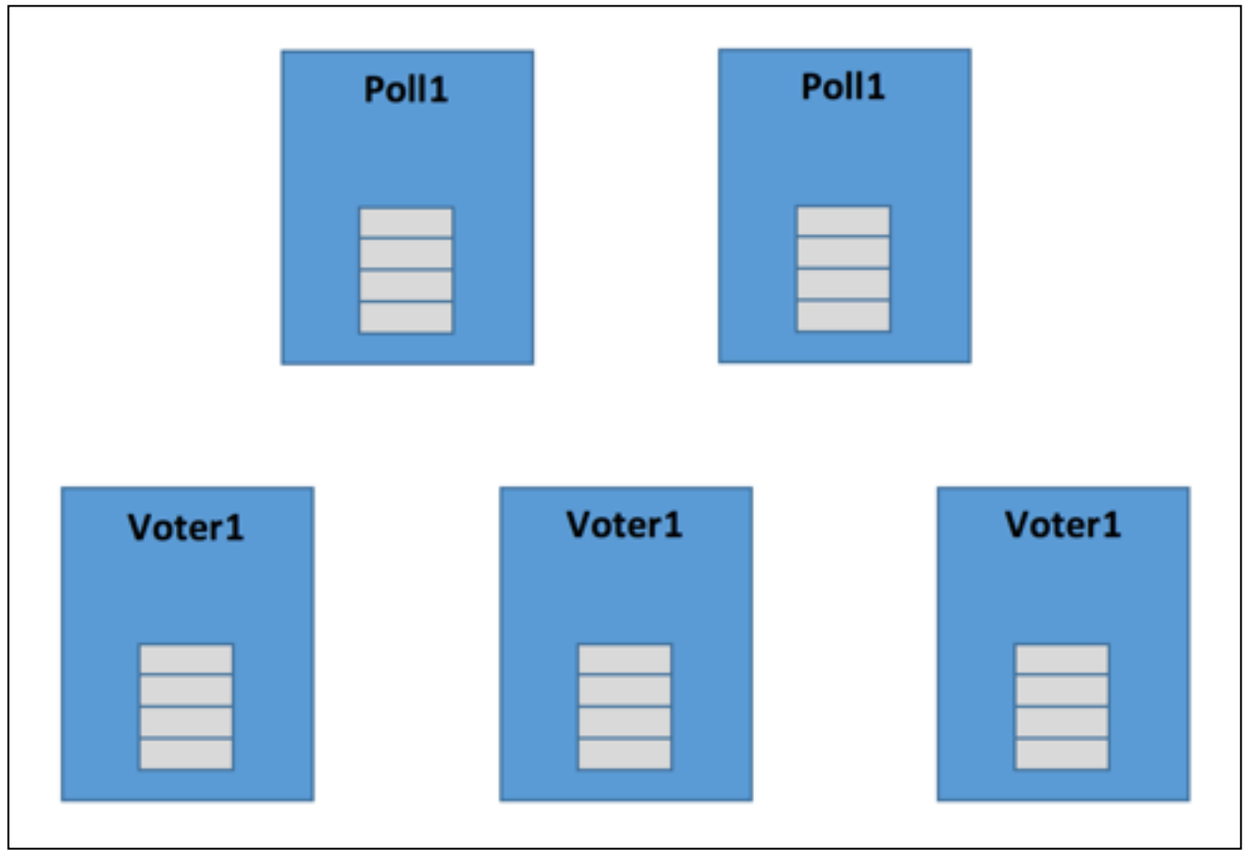
# Blockchain Voting

# Blockchain Voting

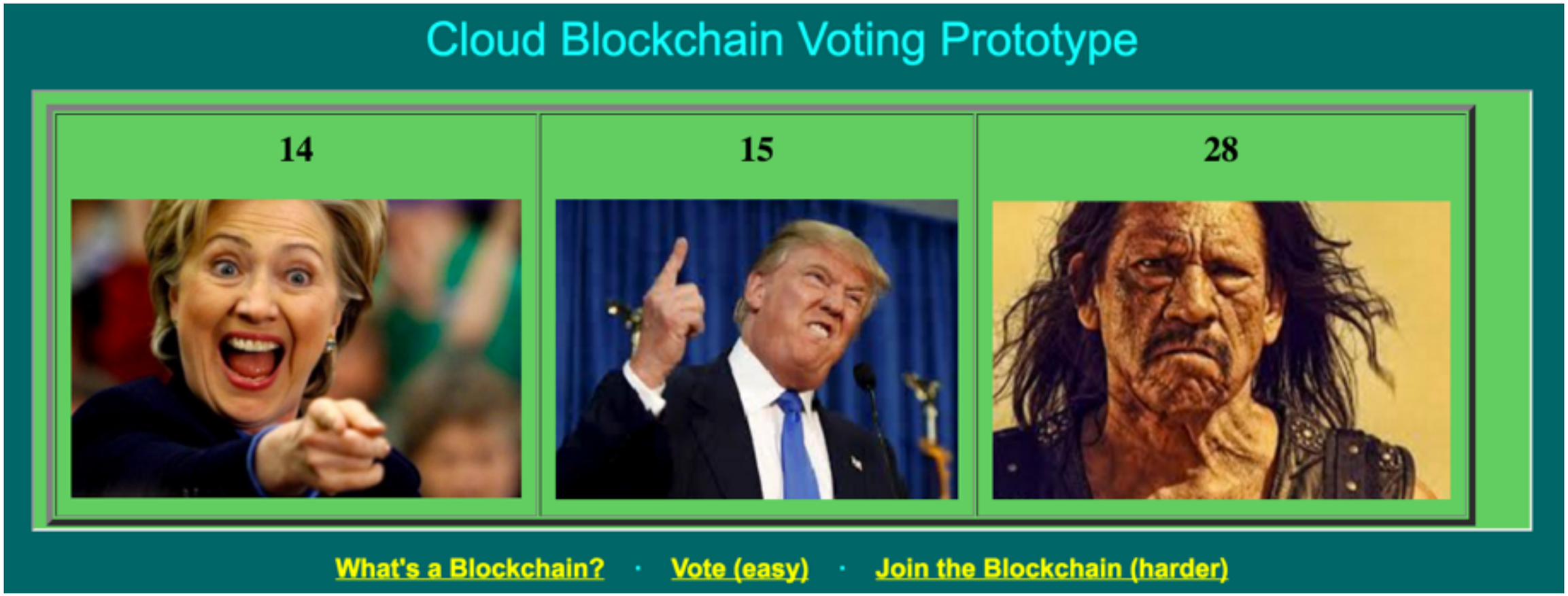
- Every stakeholder has the complete blockchain

- Voters can verify that their voted were counted

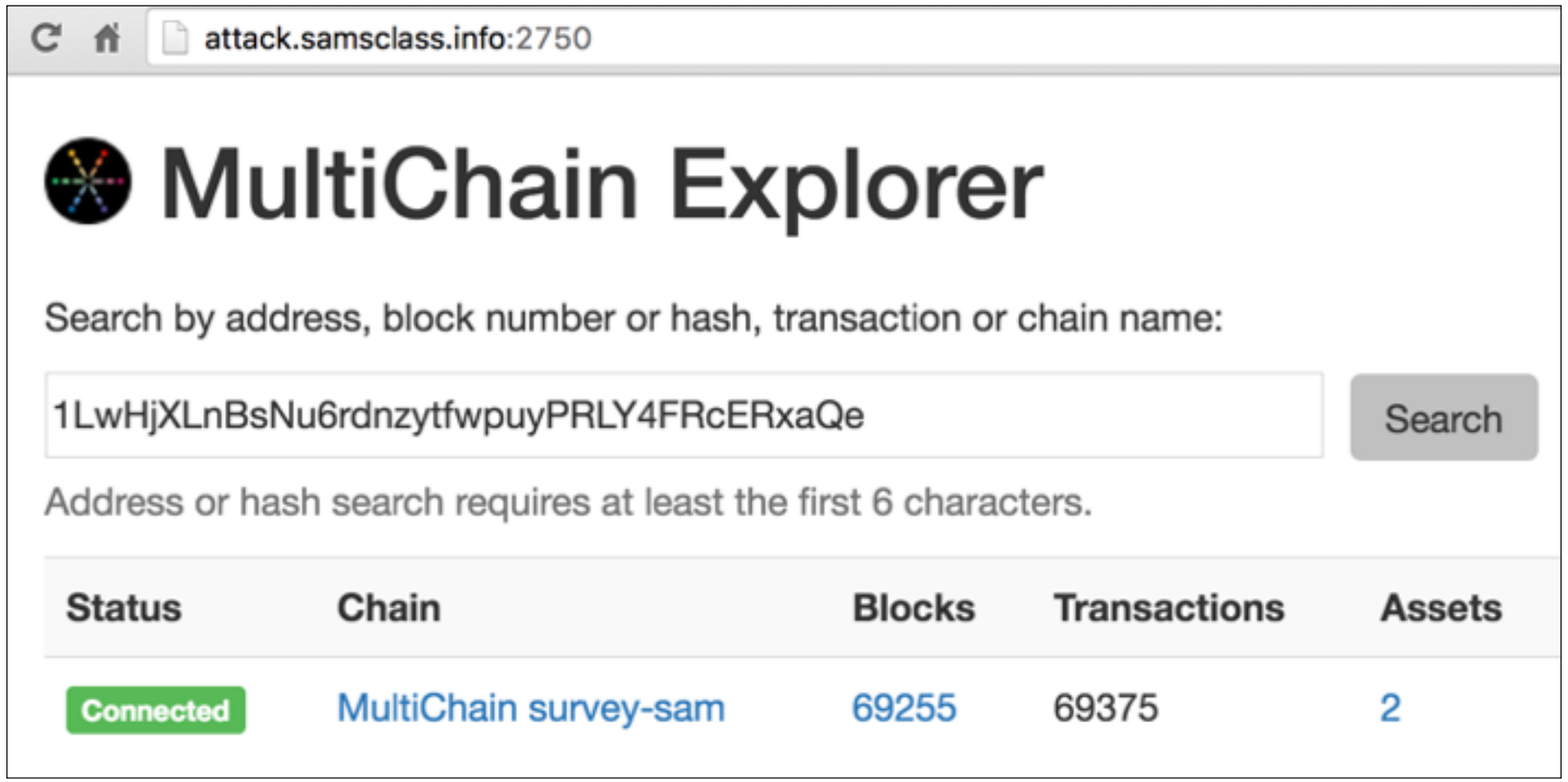
- Anyone can verify the totals at any time

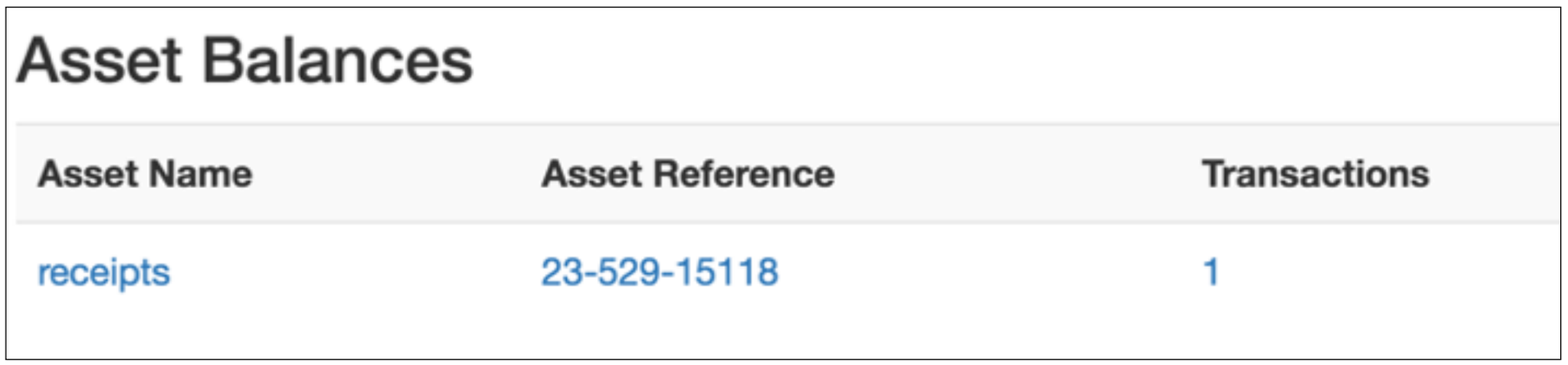


# People Voted



# Verify that Your Vote was Counted



# Verify Vote Totals

## Address
## 14kuyh5KmxuVRog5LWDgFAMSAcDcBScfUtFuD1

### Permissions

### Asset Balances

| Asset Name | Asset Reference | Transactions | Raw Units | Balance |
|---|---|---|---|---|
| receipts | 23-529-15118 | 45 | 2986 | 2986 |
| token | 23-265-53281 | 14 | 14 | 14 |

- Much hype about security
- Obviously they know nothing about security
- They don't care to hear criticism either

# Cryptokitties

Secure | https://www.cryptokitties.co

CryptoKitties

My Kitties Marketplace Invite

# Collectible. Breedable. Adorable.

Collect and breed digital cats.

Start meow

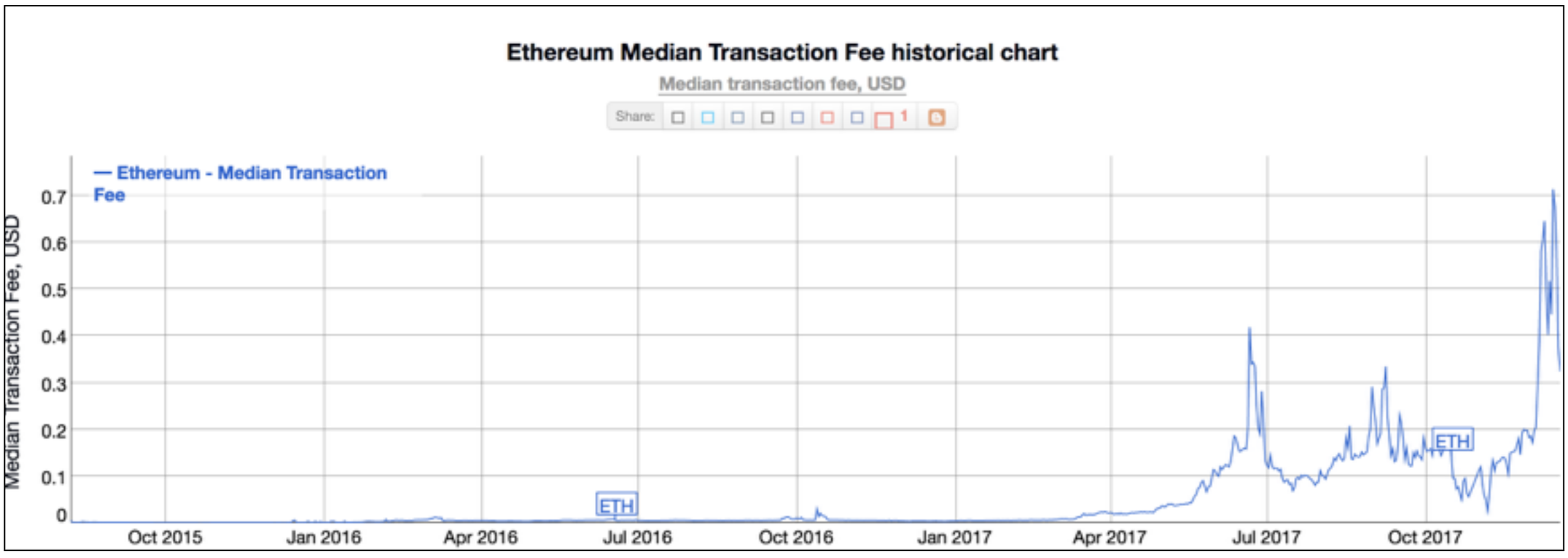
# How Crypto-Kitties Disrupted the Ethereum Network

https://hackernoon.com/how-crypto-kitties-disrupted-the-ethereum-network-845c22aa1e6e

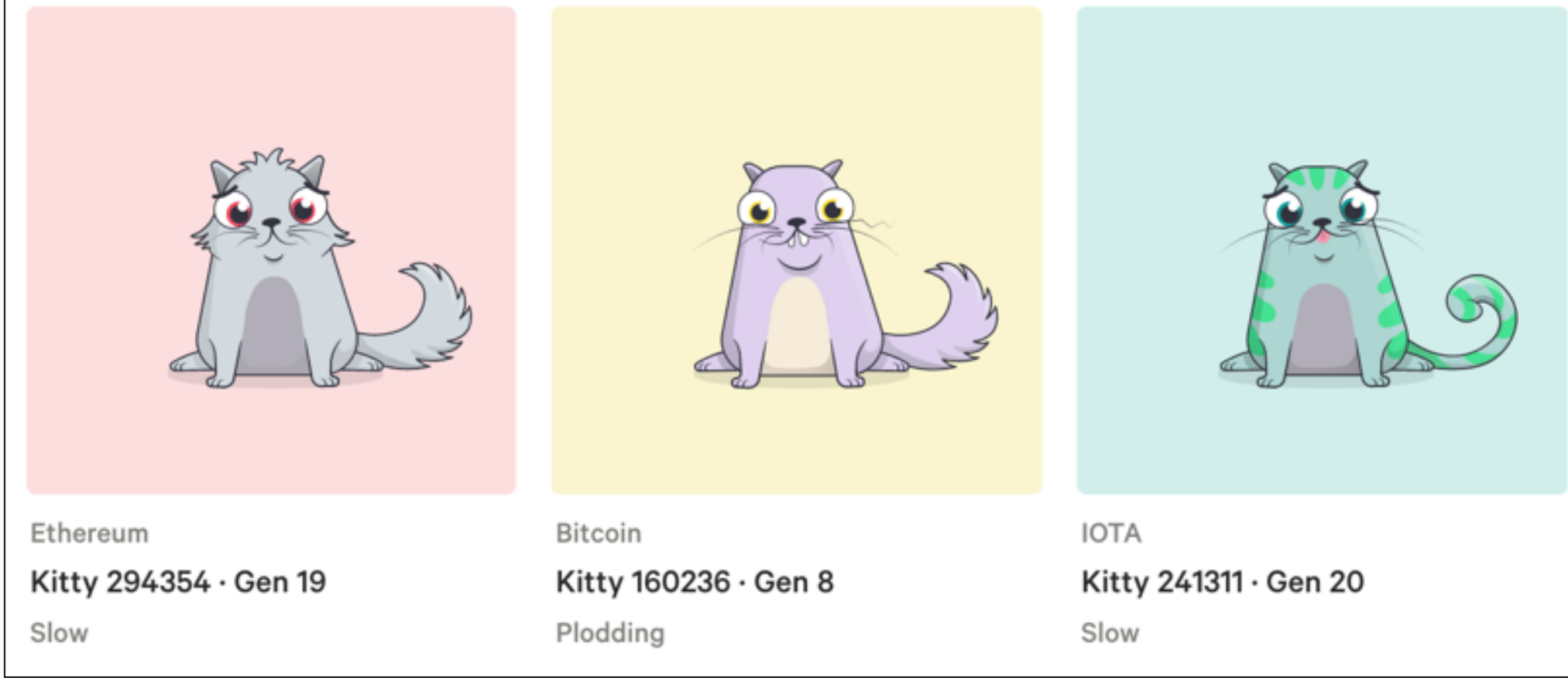
**What's the Impact on Ethereum?—Significant Volume**

The Crypto-Kittie app applies the Ethereum blockchain to create a public, shared history of Crypto-Kitties. Crypto-Kitties make up over 20 percent of all Ethereum computations and the app is Ethereum's most popular by far, with users having spent over $3 million total on breeding alongside buying and selling the game related items. In addition, an average cat currently trades for above $100 worth of ether.

https://bitinfocharts.com/comparison/ethereum-median_transaction_fee.html



# Contest



Ethereum

**Kitty 294354 · Gen 19**

Slow

Bitcoin

**Kitty 160236 · Gen 8**

Plodding

IOTA

**Kitty 241311 · Gen 20**

Slow

Kahoot!