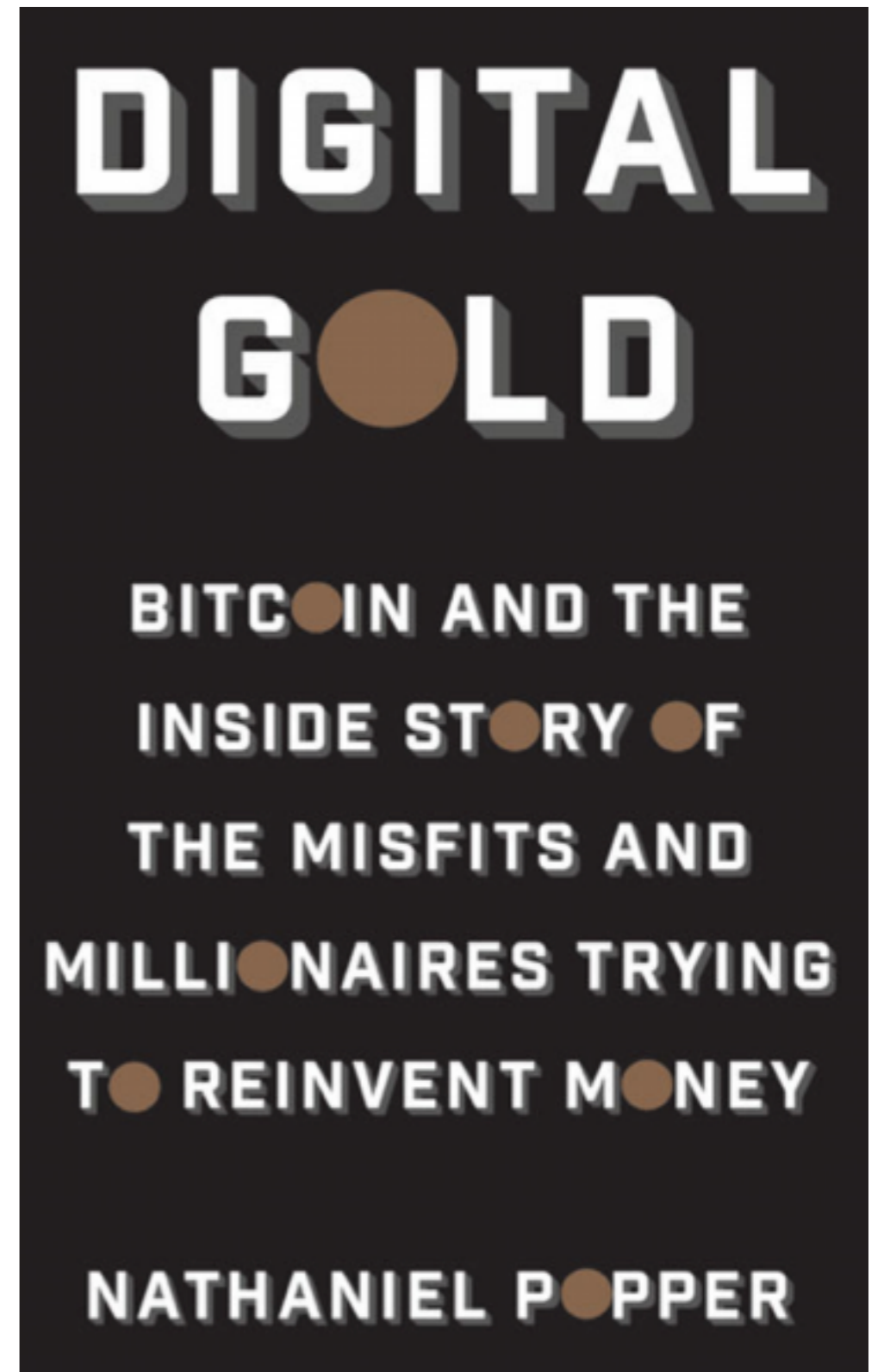
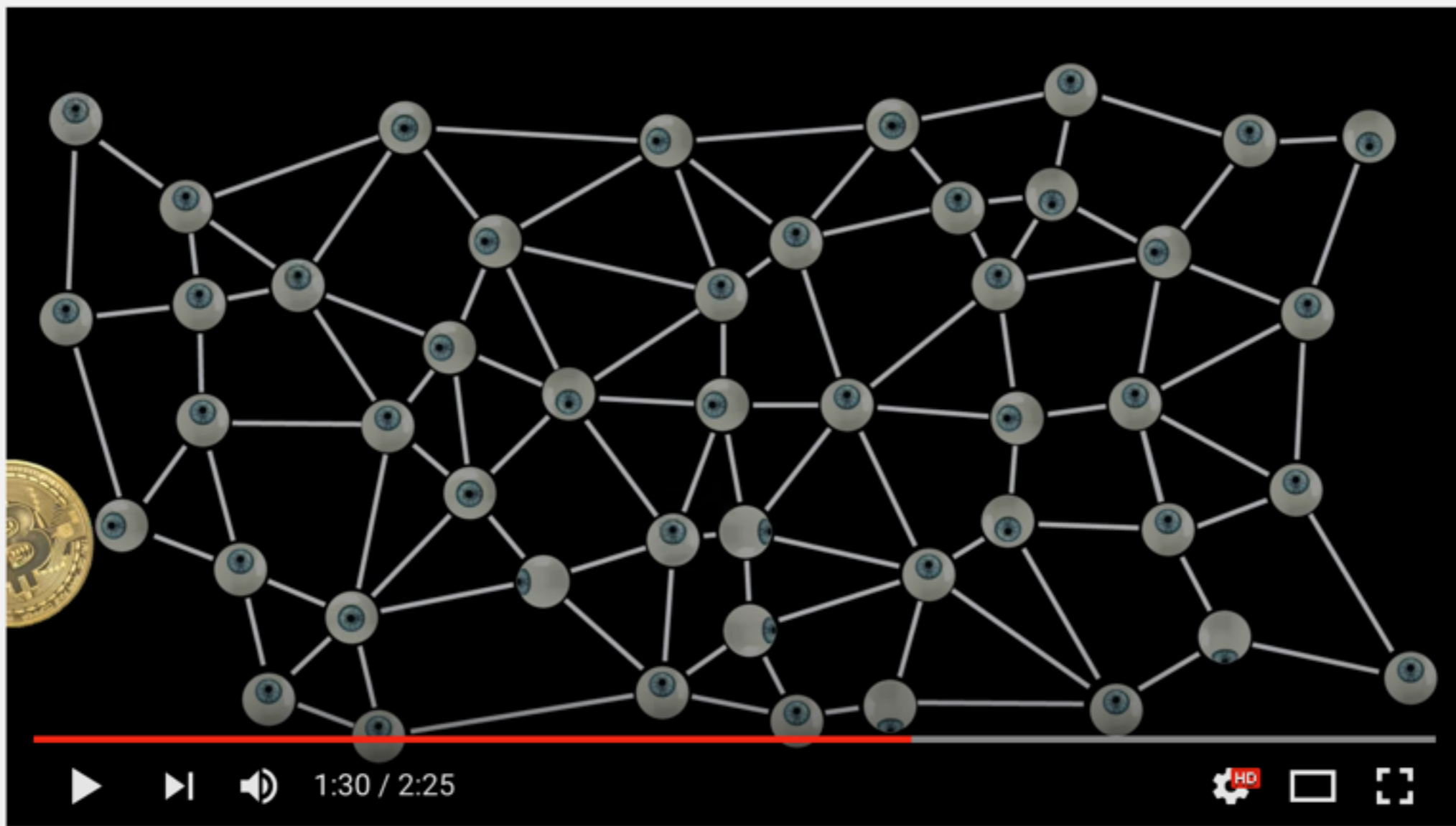


Bitcoin and Blockchains



Updated 8-7-2017



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" and the active tab is "Blockchain". The interface displays three blocks in a sequence, each with a "Mine" button.

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	0000b3b98b7208dfef33e...

Link Blockchain 10

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.

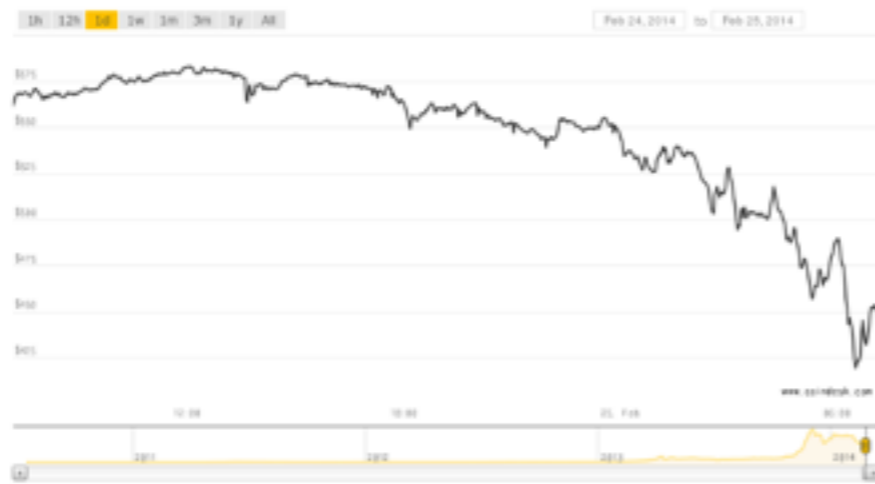


Sam Bowne @sambowne · May 24

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



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



**Bitcoin Exchange Gatecoin
Hacked; 250 BTC & 185,000 ETH
Lost**

© 16/05/2016  Elliot Maras  0

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

By [Adrienne 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

f

🐦

in

g+


✉


💬

⋮

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 <small>Unresolved as of December 2012</small>	18547.66867623 ฿ <small>39000 ฿ total impact</small>
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	<i>Bitomat.pl Loss</i>	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



China Controls Bitcoin

for the international acceptance of the cryptocurrency. In a recent interview with Finance Magnates, the CTO of the largest bank in Israel told us that banks shy away from bitcoin in part because of its mining centralization in China.

- Links Bitcoin 27, 28

Bitcoin Mining in China

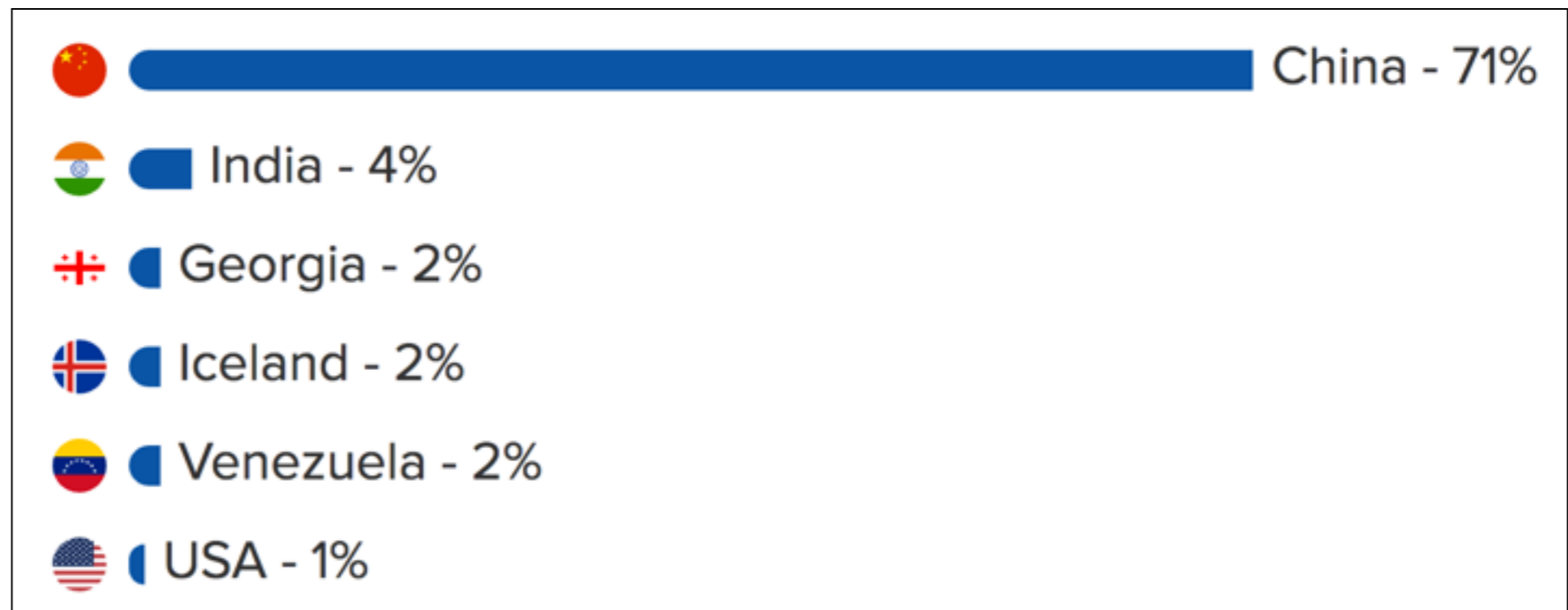


 Jordan Tuwiner



Last updated June 13, 2017

China is the undisputed world leader in Bitcoin mining.



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)

Digital currency Ethereum is cratering because of a \$50 million hack



Rob Price  

 Jun. 17, 2016, 5:34 AM  **50,181**  11

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.

Cross-Chain Replay Attacks

[Emin Gün Sirer](#)

dao ethereum

July 17, 2016 at 12:07 PM

[← Older](#)

[Newer →](#)

Following an Ethereum hard fork, there will be two chains. In cross-chain replay attacks, one can attack a smart contract by moving transactions from one chain to the other.



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.

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, ...

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.

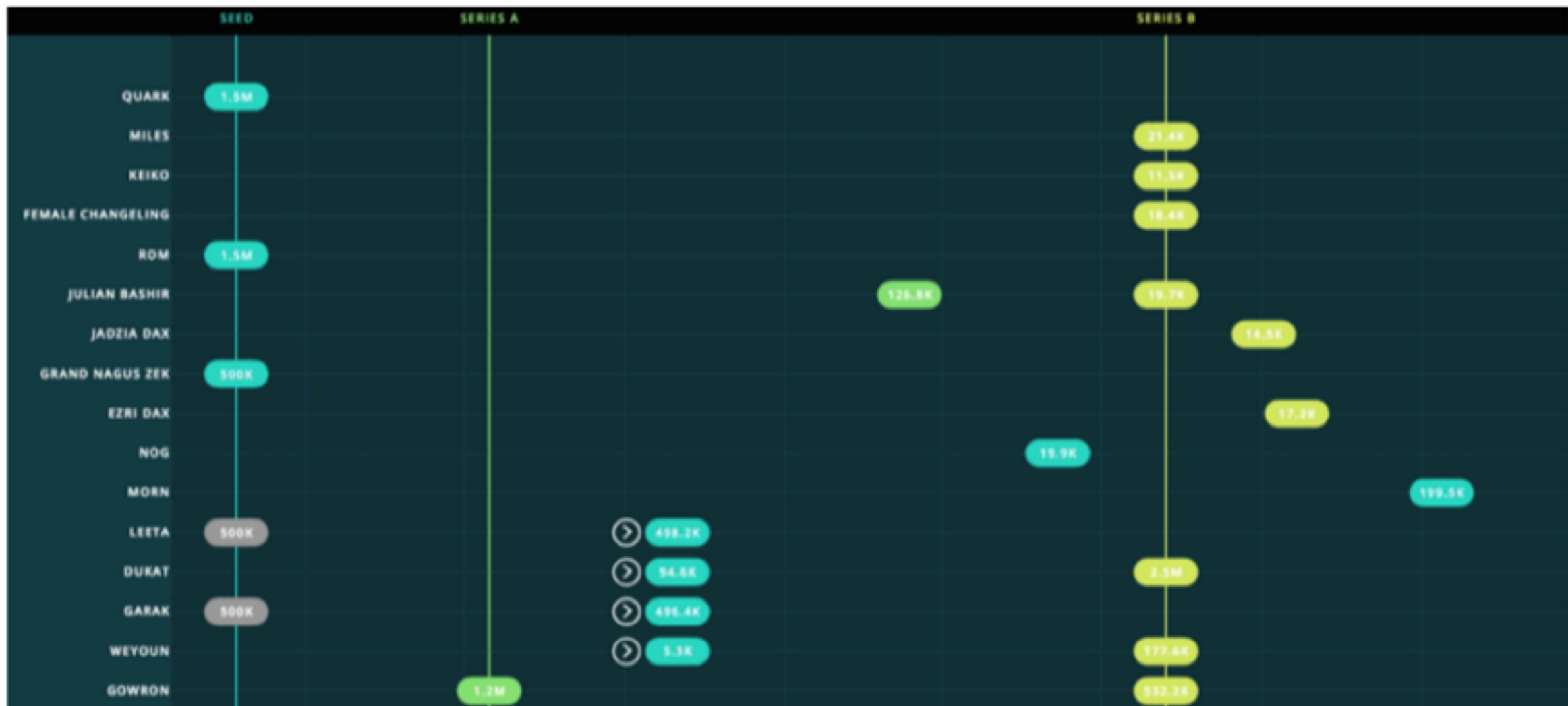


Hands On With Linq, Nasdaq's Private Markets Blockchain Project

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

FEATURE

675 229 21 446 41



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

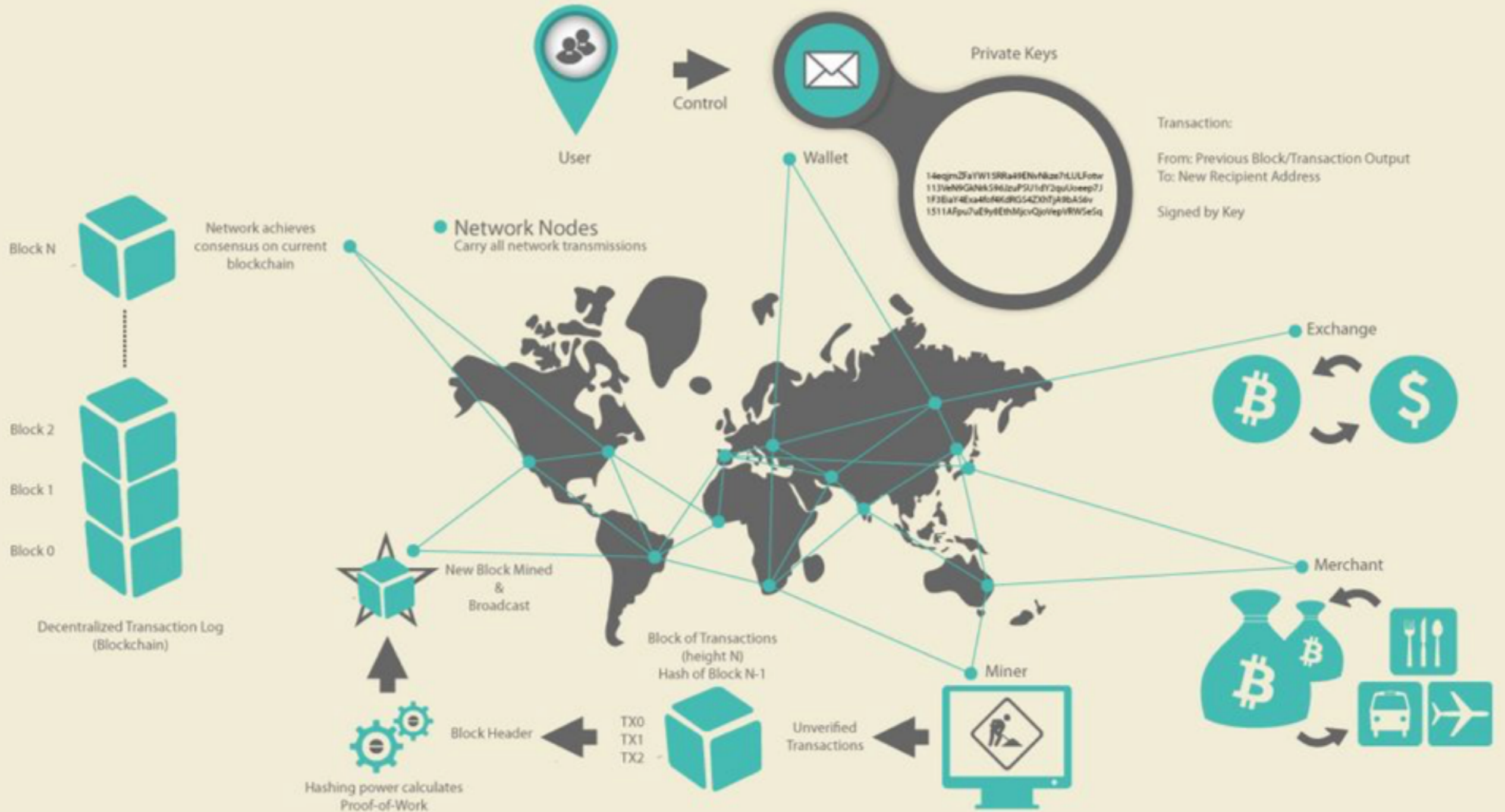


Sydney Stock Exchange Developing Blockchain Trading System

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



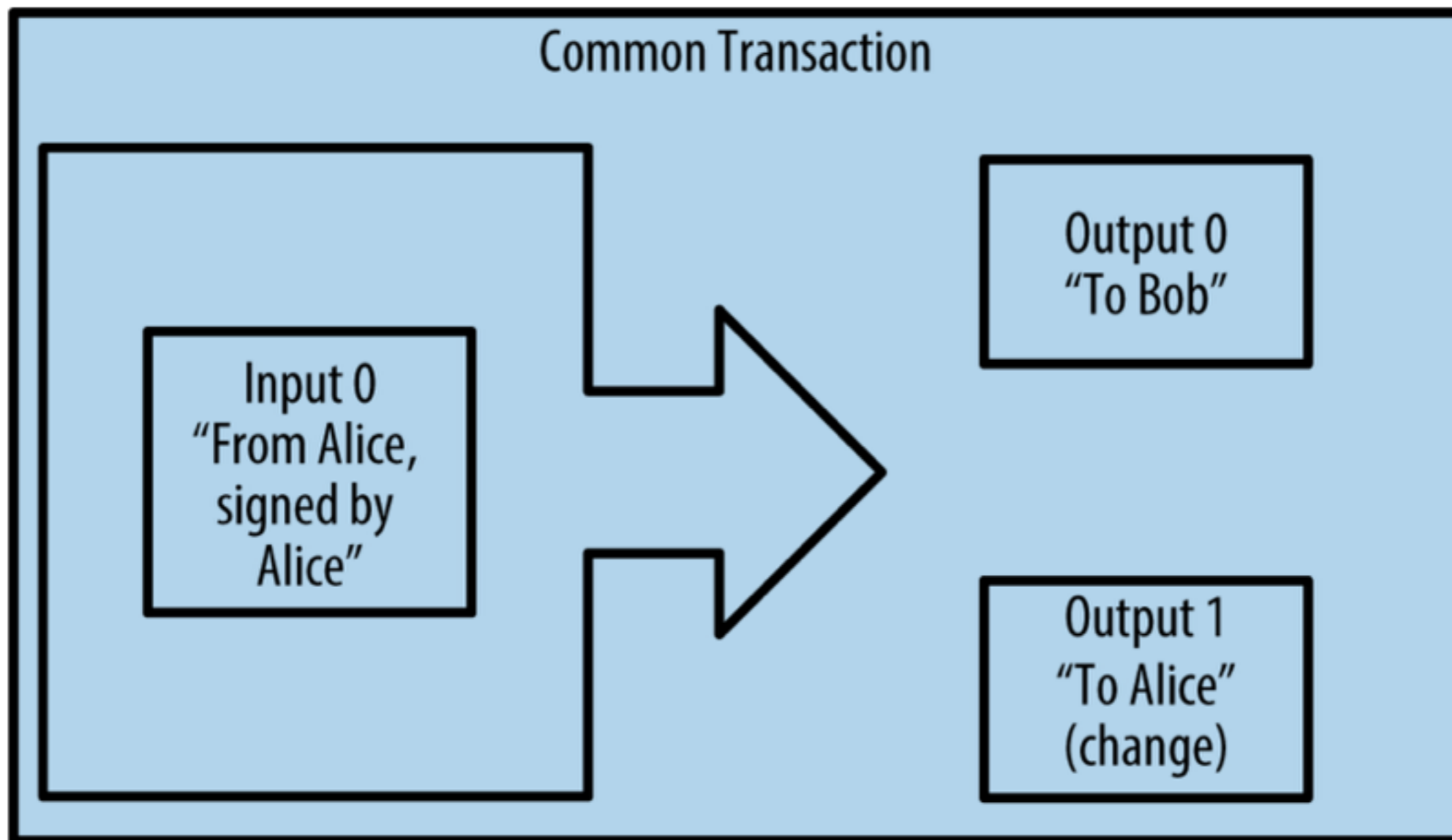


Figure 2-5. Most common transaction

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

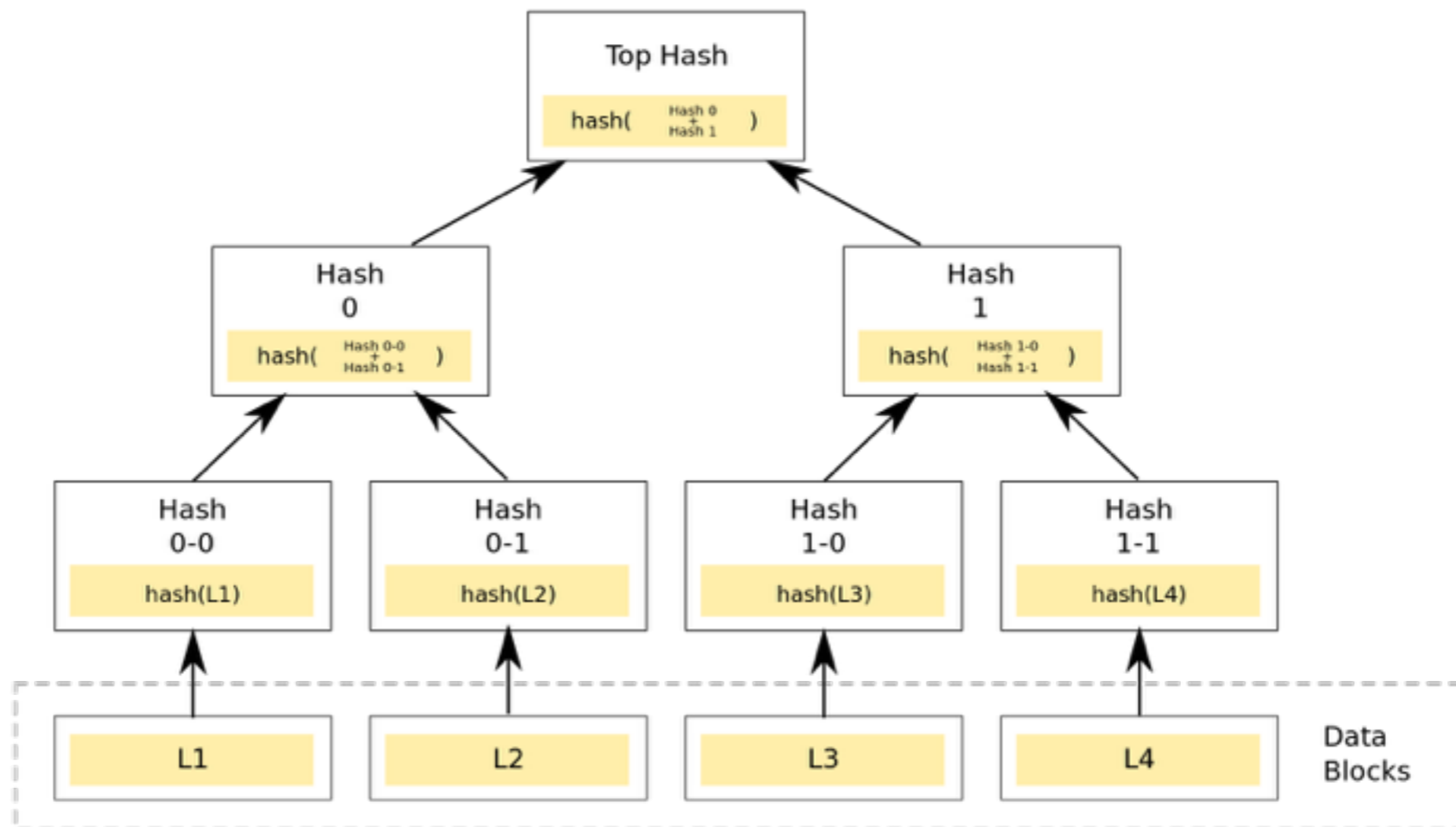
- Bitcoin is a real-world test of blockchain technology
- A bunch of rebels, criminals, scammers, and suckers
- Demonstrated how well blockchains work
- AND THEY WORK

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

The screenshot shows the Blockchain.info website interface. At the top, there is a navigation bar with the Blockchain logo and menu items: Home, Charts, Stats, Markets, API, and Wallet. A search bar and language selector (English) are also present. The main content area is titled "Transaction" and provides information about a specific Bitcoin transaction. The transaction ID is `4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b`. It shows "No Inputs (Newly Generated Coins)" and a single output of 50 BTC to the address `1A1zP1eP5QGefi2...`, which is identified as the "Genesis of Bitcoin" and is marked as "Unspent". Below this, a "Summary" table lists transaction details: Size (204 bytes), Received Time (2009-01-03 18:15:05), Reward From Block (0), Scripts (Hide scripts & coinbase), Relayed by IP (0.0.0.0), and a link to visualize the transaction tree. At the bottom, the "CoinBase" section shows the decoded transaction data: `04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e636556c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73`, which decodes to "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks".

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	Hide scripts & coinbase
Relayed by IP 	0.0.0.0 (whois)
Visualize	View Tree Chart

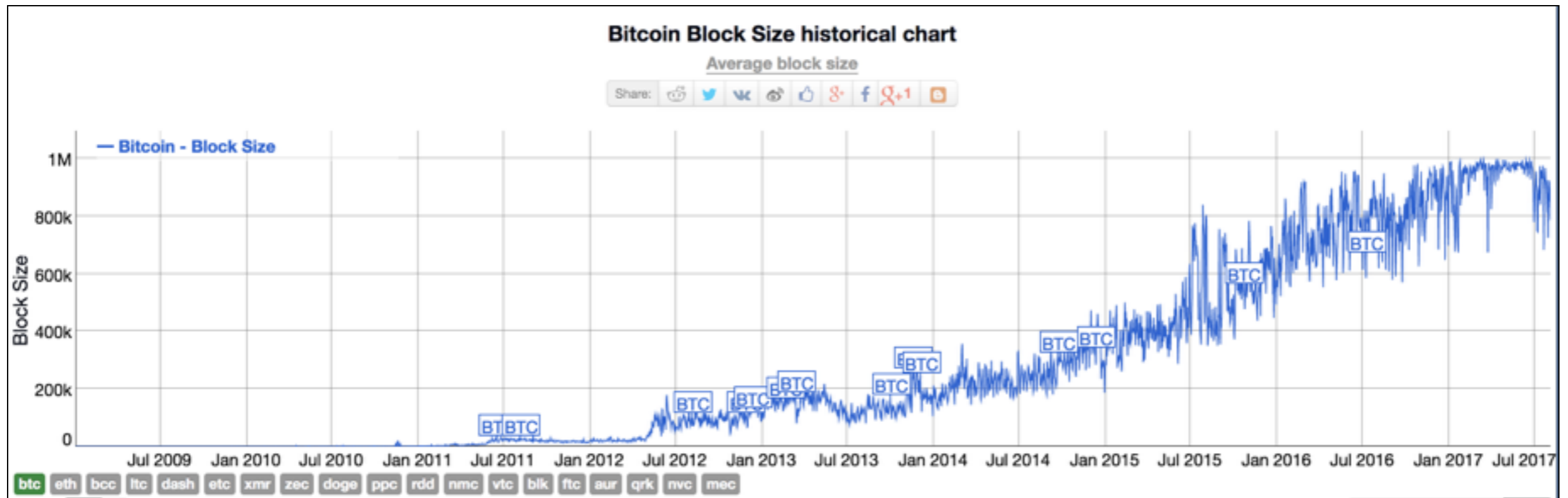
CoinBase

`04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e636556c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73`
(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
```

Bitcoin's Block Size Limit



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

Bitcoin Forked in Aug, 2017



The image is a screenshot of a web browser displaying the Bitcoin Cash website. The browser's address bar shows the URL <https://www.bitcoincash.org> and indicates a secure connection. The website features a large orange square logo with a white Bitcoin symbol on the left. To the right, the text "Bitcoin Cash" is written in a large, bold, italicized font, with "Peer-to-Peer Electronic Cash" in a smaller green font below it. A paragraph of text below the logo announces the launch of Bitcoin Cash (BCC) on August 1st, 2017, and provides details about the first block produced by the ViaBTC pool.

We are pleased to announce that on August 1st 2017, Bitcoin Cash (BCC) successfully launched.

At 18:24:41 UTC, ViaBTC pool produced a 1.9 MB BCC block, which was not valid on the legacy Bitcoin network. This marked a clean break and the birth of Bitcoin Cash.

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?

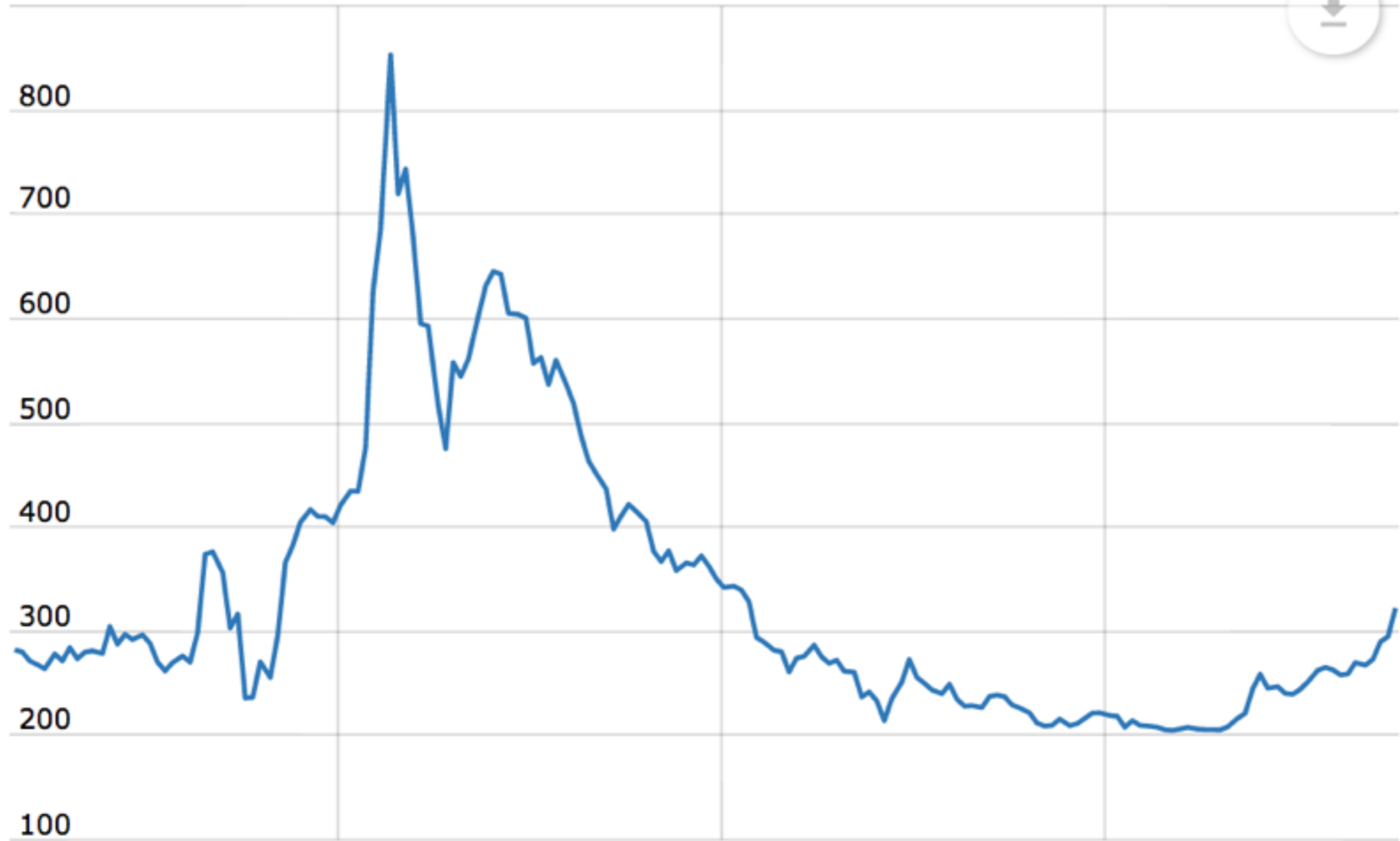
Yes. Bitcoin Cash immediately raises the blocksize limit to 8MB as part of a massive on-chain scaling approach. There will be ample capacity for everyone's transactions.

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.

Bitcoin Cash Charts

1d 7d 1m 3m 6m 1y All

Value

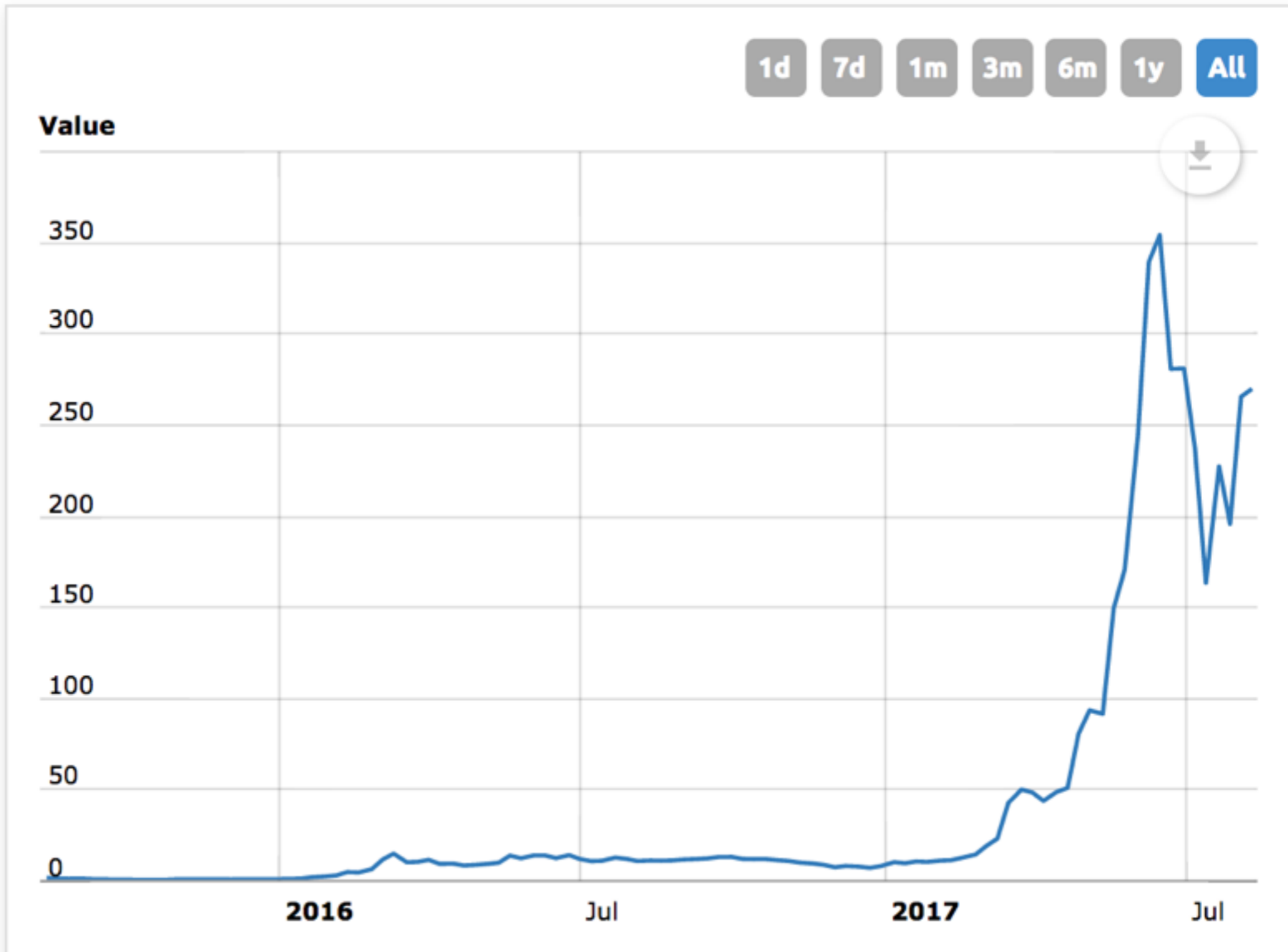


Aug

Aug 04

Aug 06

Ethereum Charts



Iota Charts



Three Bitcoins?



Could there be three bitcoins? With Segwit only, Segwit + 2MB, and an 8MB version.

Let's Not Forget About Segwit2x

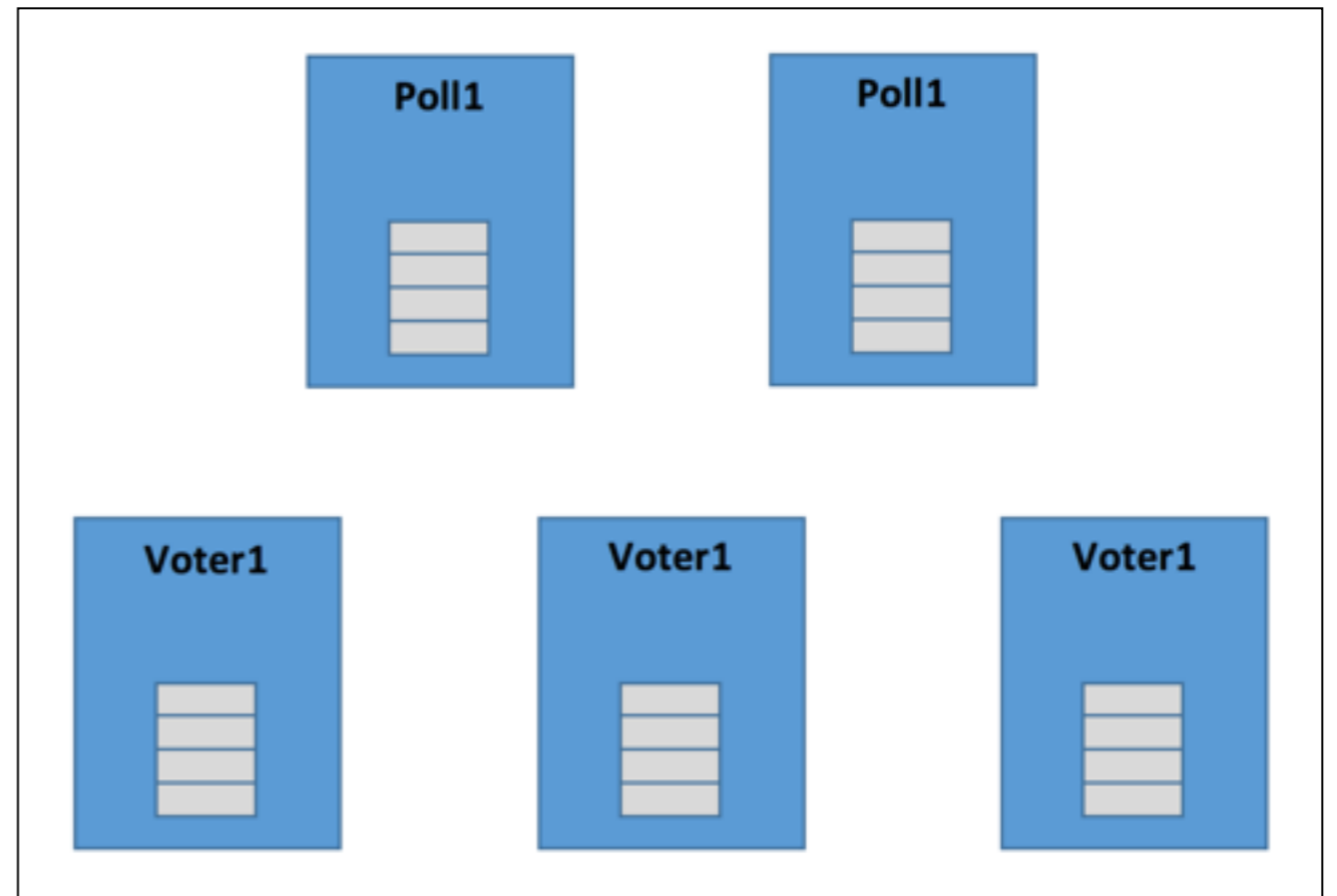
A few more changes are coming to the Bitcoin network in the near future. The **Segwit2x** plan often referred to as NYA is still following its course towards protocol activation of Segwit. At the time of writing, there are 621 blocks remaining for BIP 141 (Segwit) lock-in, and the plan 'seems' to be running smoothly. The vast majority of miners who agreed to the Segwit2x proposal are still following through with at least half of the plan. The second half of Segwit2x intention involves the 2MB hard fork which is scheduled to occur in November.

- [Link Bitcoin 25](#)

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

Cloud Blockchain Voting Prototype

14



15



28



[What's a Blockchain?](#) · [Vote \(easy\)](#) · [Join the Blockchain \(harder\)](#)

Verify that Your Vote was Counted

attack.samsclass.info:2750

MultiChain Explorer

Search by address, block number or hash, transaction or chain name:

Address or hash search requires at least the first 6 characters.

Status	Chain	Blocks	Transactions	Assets
Connected	MultiChain survey-sam	69255	69375	2

Asset Balances

Asset Name	Asset Reference	Transactions
receipts	23-529-15118	1

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

Introducing a secure and transparent online voting solution for the modern age:

FOLLOW MY VOTE

Join Our List Of Supporters!



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



100% Secure

Blockchain technology ensures
that the ballot box cannot be
hacked.