# Some Simple Economics of the Blockchain

**Christian Catalini**
catalini@mit.edu
blockchain.mit.edu

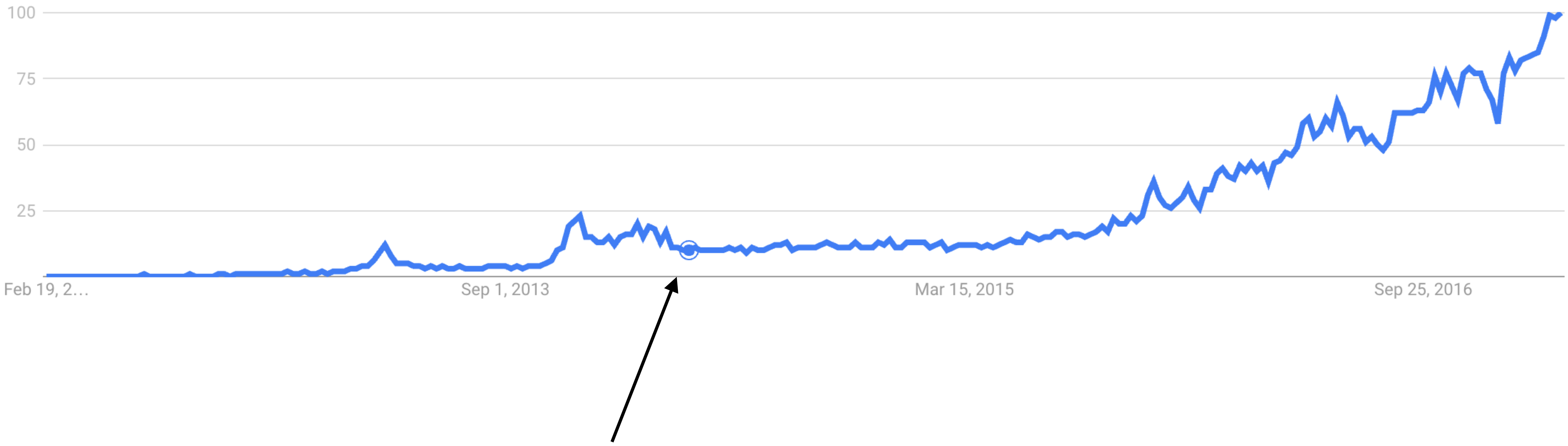
MIT MANAGEMENT SLOAN SCHOOL

# MIT Digital Currency Experiment (2014)

Main Street
Main Stre
Albany Street
Vassar Street
Lansdo
Massachusetts Avenue
Ames Street
Pacific Street
Albany Street
Land Boulevard
Lan
Memorial Drive
Erie Street
Vassar S
Memorial Drive
Memorial Drive
Memorial Drive
Harvard Bridge
Storrow Drive
Storrow Drive
Storrow Drive
Storrow Drive
Beacon Street
Massachusetts Avenue
Commonwealth Av
Bay State Road
Commonwealth Avenue
Beacon Street
Charlesgate Ea
Bowk
Here

blockchain.mit.edu

# Blockchain



MIT Digital Currency Experiment (2014)

blockchain.mit.edu

MIT MANAGEMENT SLOAN SCHOOL

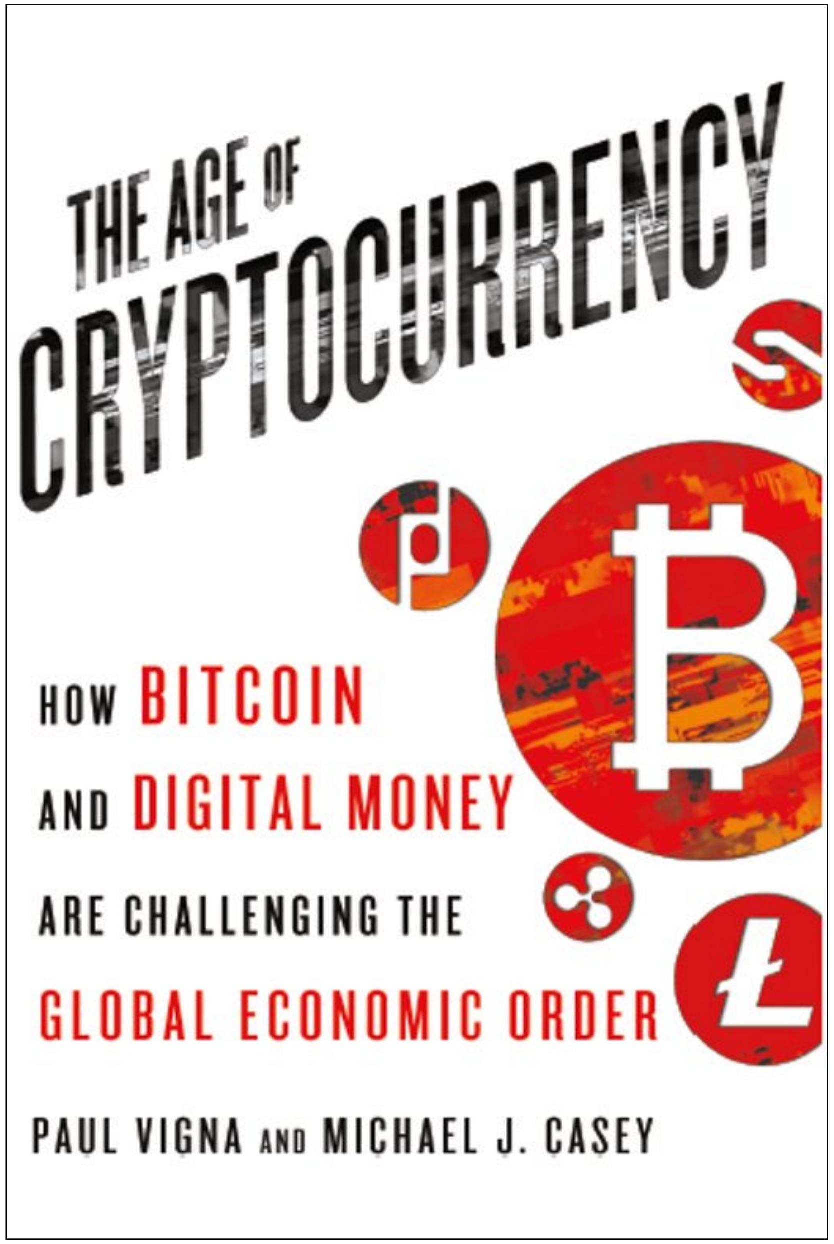
# From Fringe to Mainstream

Newsweek
03.14.2014
BITCOIN'S FACE
THE MYSTERY MAN BEHIND THE CRYPTO-CURRENCY

The Economist
OCTOBER 31ST–NOVEMBER 6TH 2015
Economist.com
Our guide to America's best colleges
Myanmar's free-ish election
Those ever-creative accountants
America takes the fight to IS
Coywolves: the new superpredator
The trust machine
How the technology behind bitcoin could change the world
IN BLOCKCHAIN WE TRUST

OCTOBER 2015
Bloomberg Markets
IT'S ALL ABOUT THE
BLOCKCHAIN
BLYTHE MASTERS IS BETTING THE DIGITAL LEDGER BEHIND BITCOIN WILL REVOLUTIONIZE THE WAY WE TRADE BONDS, LOANS, DERIVATIVES, AND MUCH ELSE.
+ THE INNOVATORS
BRAD KATSUYAMA'S NEXT CHAPTER
A BANK FOR PEOPLE WHO HATE BANKS
WHO WANTS TO START AN ETF?
A HUNDRED APPS BLOOM IN CHINA

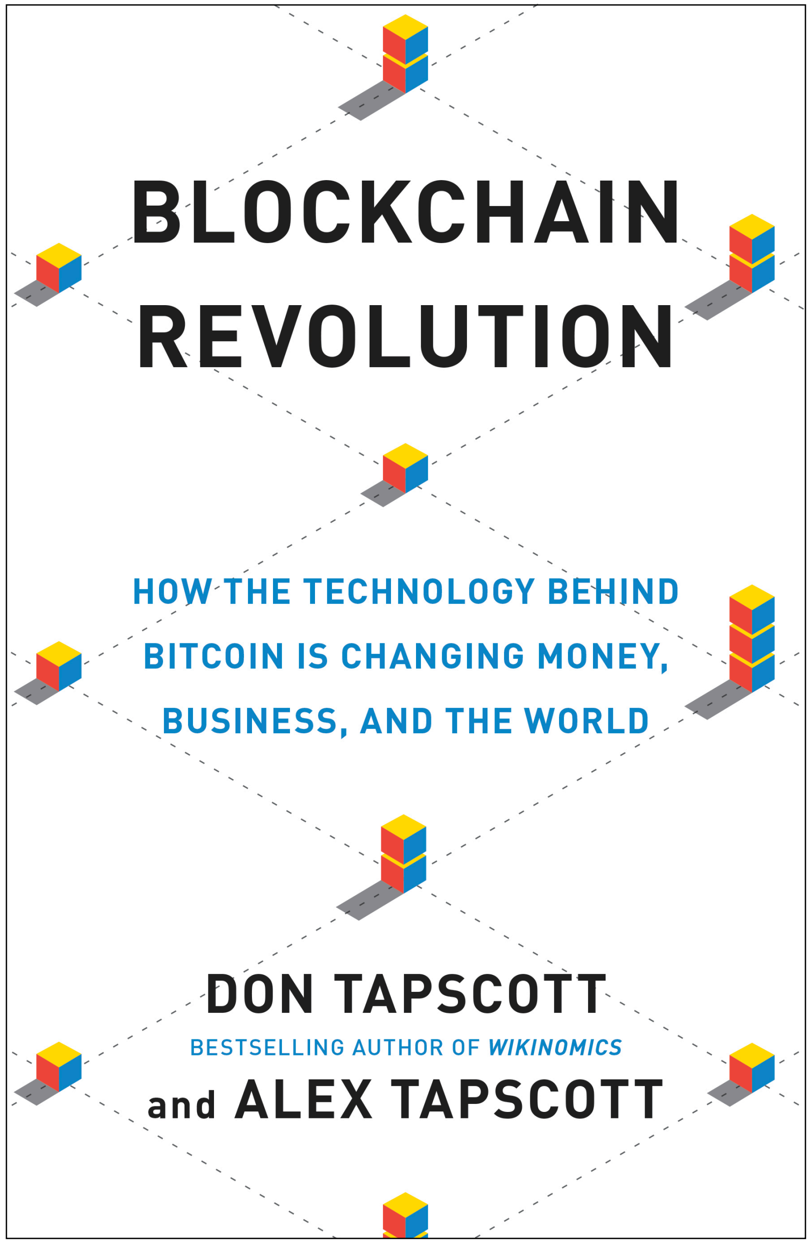
# Most Revolutions Take Time!



THE AGE OF CRYPTOCURRENCY

HOW BITCOIN AND DIGITAL MONEY ARE CHALLENGING THE GLOBAL ECONOMIC ORDER

PAUL VIGNA AND MICHAEL J. CASEY



BLOCKCHAIN REVOLUTION

HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD

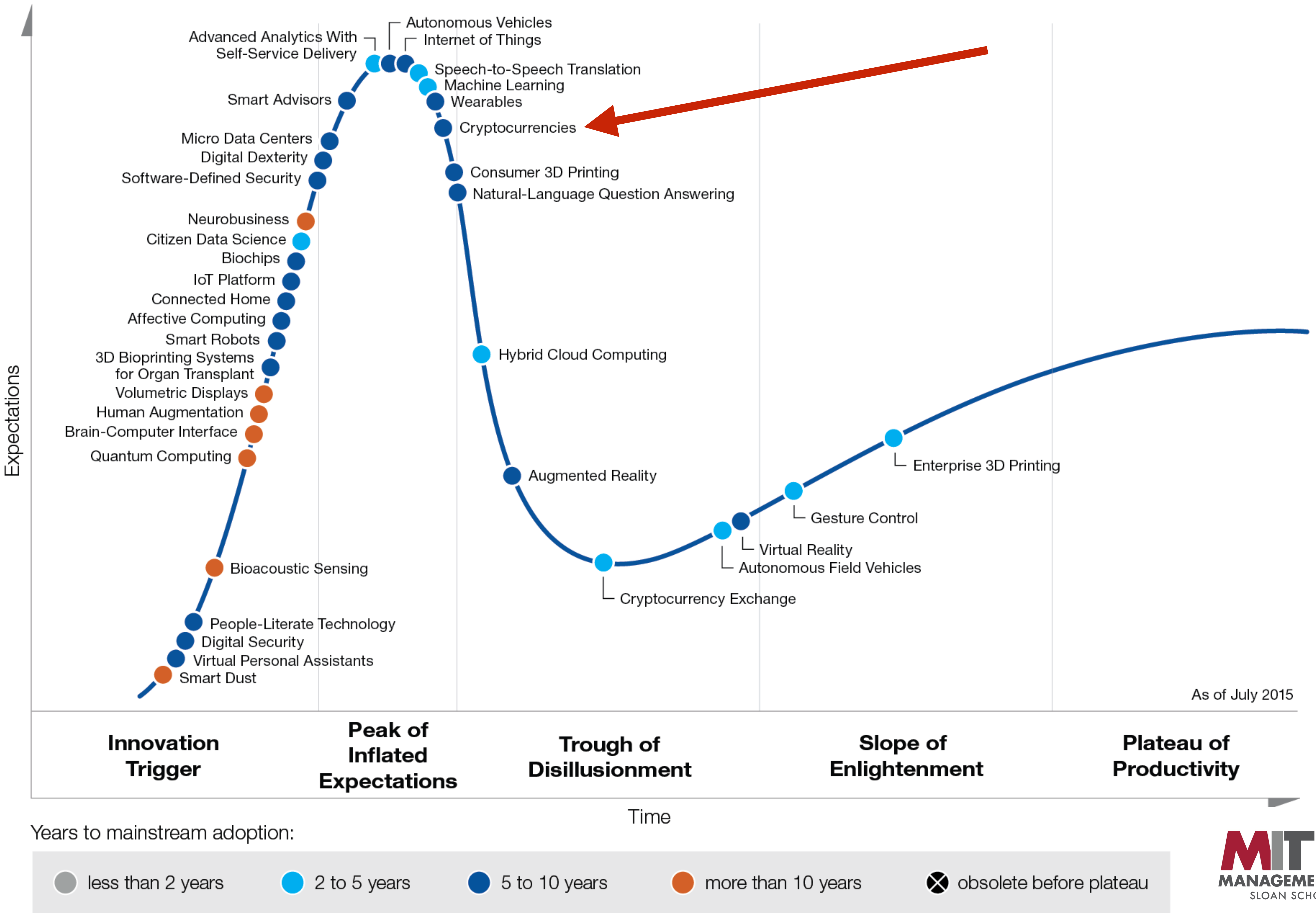
DON TAPSCOTT

BESTSELLING AUTHOR OF *WIKINOMICS*

and ALEX TAPSCOTT

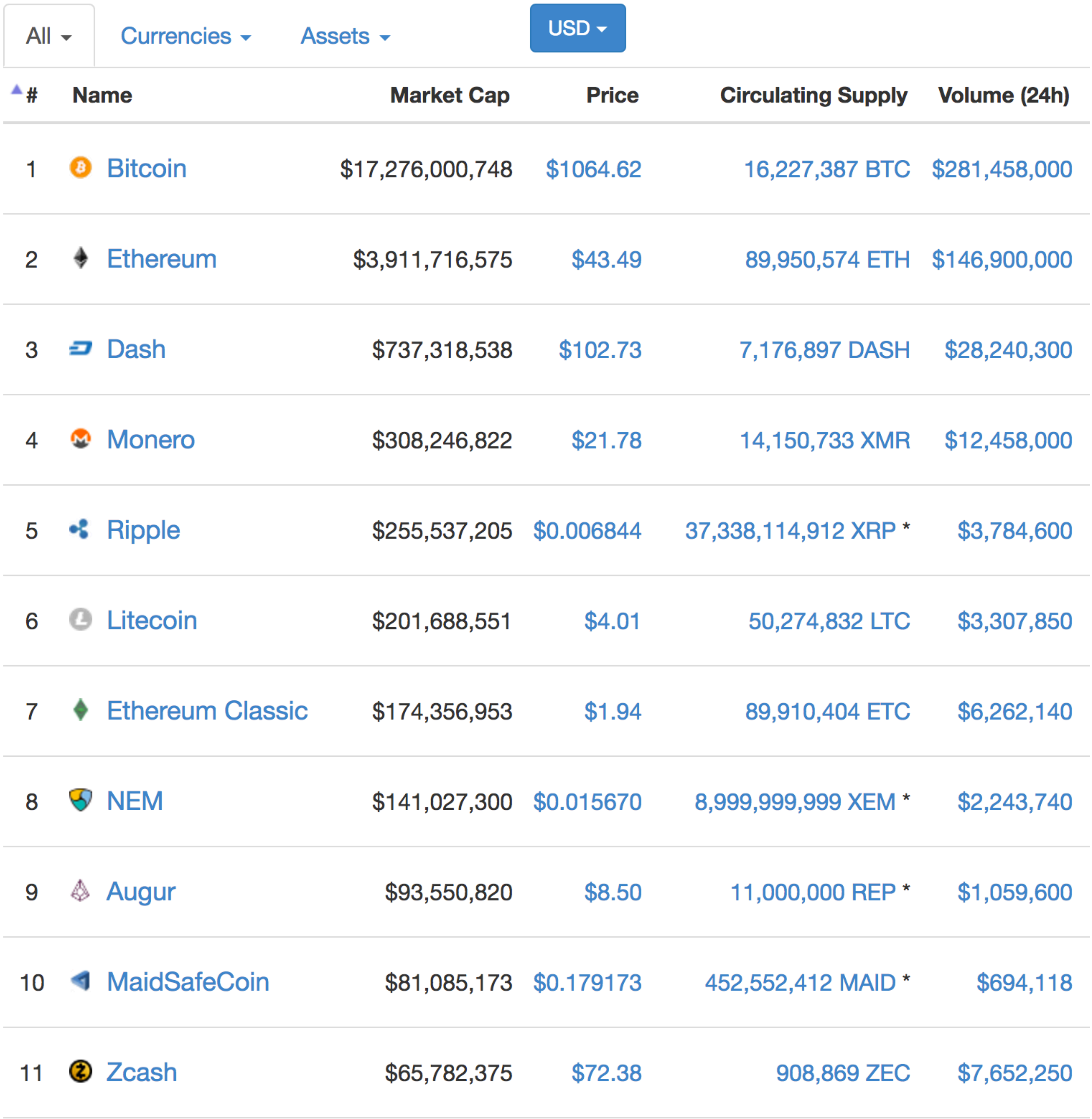
MIT MANAGEMENT SLOAN SCHOOL

# Emerging Technology Hype Cycle

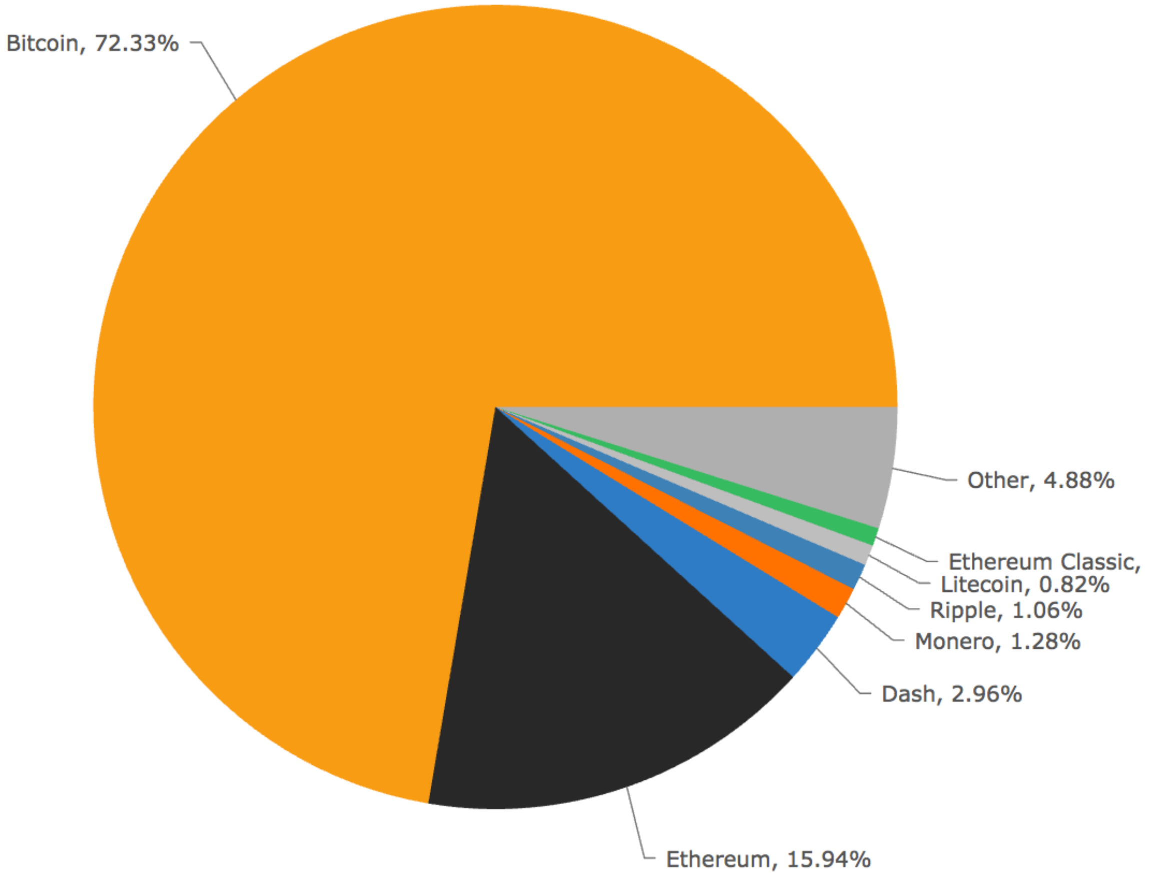


MIT MANAGEMENT SLOAN SCHOOL

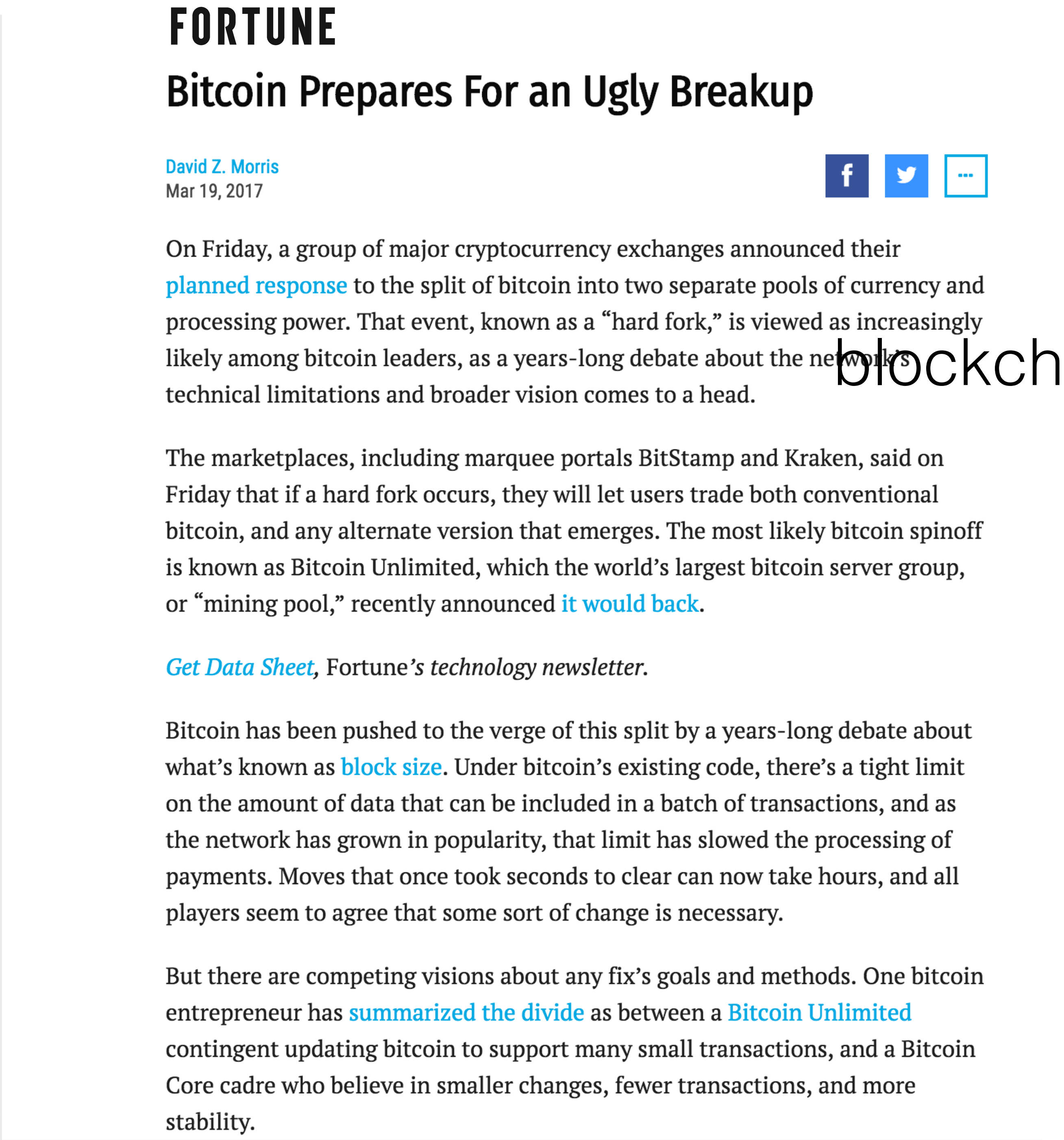
# Competing Standards



| # | Name | Market Cap | Price | Circulating Supply | Volume (24h) |
|---|---|---|---|---|---|
| 1 | Bitcoin | $17,276,000,748 | $1064.62 | 16,227,387 BTC | $281,458,000 |
| 2 | Ethereum | $3,911,716,575 | $43.49 | 89,950,574 ETH | $146,900,000 |
| 3 | Dash | $737,318,538 | $102.73 | 7,176,897 DASH | $28,240,300 |
| 4 | Monero | $308,246,822 | $21.78 | 14,150,733 XMR | $12,458,000 |
| 5 | Ripple | $255,537,205 | $0.006844 | 37,338,114,912 XRP * | $3,784,600 |
| 6 | Litecoin | $201,688,551 | $4.01 | 50,274,832 LTC | $3,307,850 |
| 7 | Ethereum Classic | $174,356,953 | $1.94 | 89,910,404 ETC | $6,262,140 |
| 8 | NEM | $141,027,300 | $0.015670 | 8,999,999,999 XEM * | $2,243,740 |
| 9 | Augur | $93,550,820 | $8.50 | 11,000,000 REP * | $1,059,600 |
| 10 | MaidSafeCoin | $81,085,173 | $0.179173 | 452,552,412 MAID * | $694,118 |
| 11 | Zcash | $65,782,375 | $72.38 | 908,869 ZEC | $7,652,250 |



# Even Within the Same Cryptocurrency, Competing Standards



FORTUNE

## Bitcoin Prepares For an Ugly Breakup

David Z. Morris
Mar 19, 2017

On Friday, a group of major cryptocurrency exchanges announced their planned response to the split of bitcoin into two separate pools of currency and processing power. That event, known as a "hard fork," is viewed as increasingly likely among bitcoin leaders, as a years-long debate about the network's technical limitations and broader vision comes to a head.

The marketplaces, including marquee portals BitStamp and Kraken, said on Friday that if a hard fork occurs, they will let users trade both conventional bitcoin, and any alternate version that emerges. The most likely bitcoin spinoff is known as Bitcoin Unlimited, which the world's largest bitcoin server group, or "mining pool," recently announced it would back.

*Get Data Sheet,* Fortune*'s technology newsletter.*

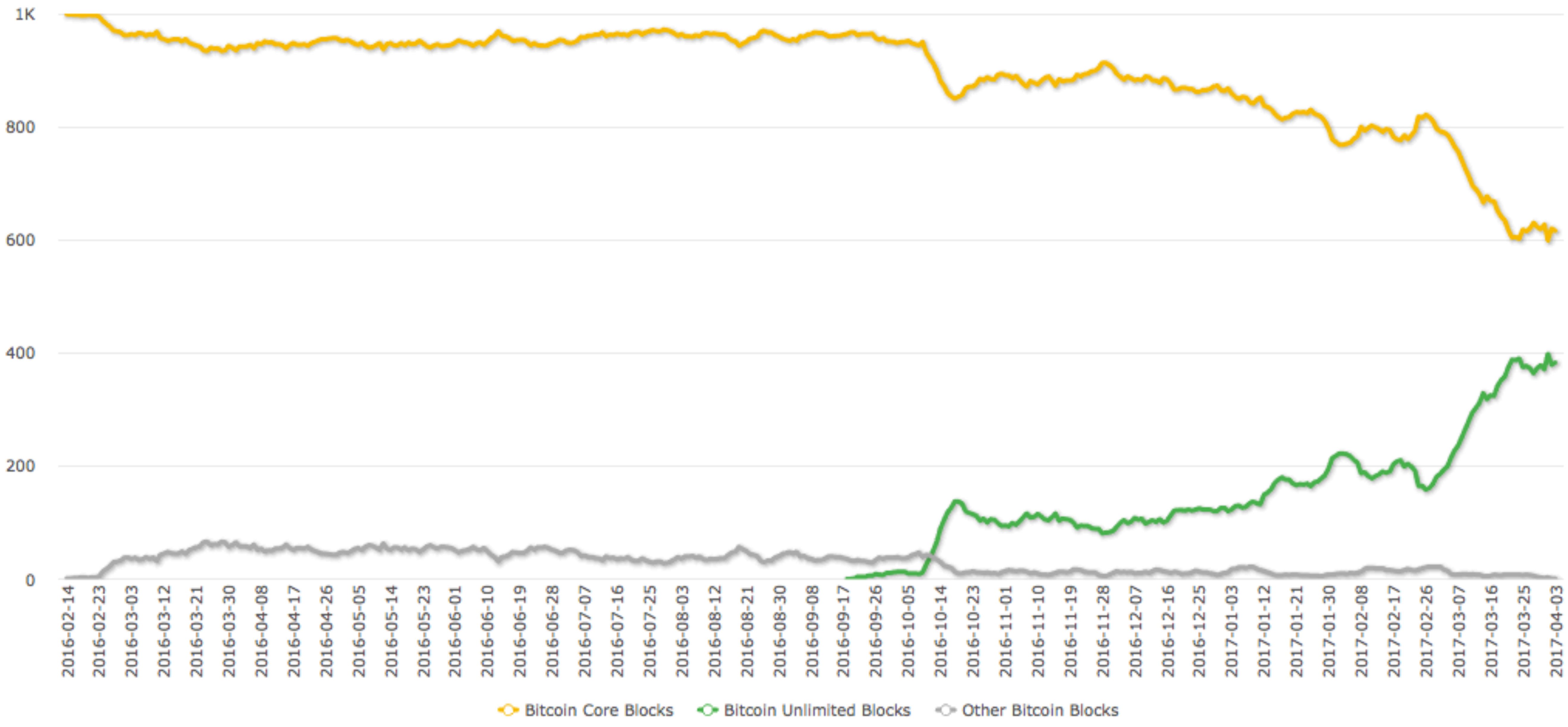
Bitcoin has been pushed to the verge of this split by a years-long debate about what's known as block size. Under bitcoin's existing code, there's a tight limit on the amount of data that can be included in a batch of transactions, and as the network has grown in popularity, that limit has slowed the processing of payments. Moves that once took seconds to clear can now take hours, and all players seem to agree that some sort of change is necessary.

But there are competing visions about any fix's goals and methods. One bitcoin entrepreneur has summarized the divide as between a Bitcoin Unlimited contingent updating bitcoin to support many small transactions, and a Bitcoin Core cadre who believe in smaller changes, fewer transactions, and more stability.

## Market Design

- **Transactions per second versus security (happening now!)**
- Decentralization versus compliance
- Degree of privacy

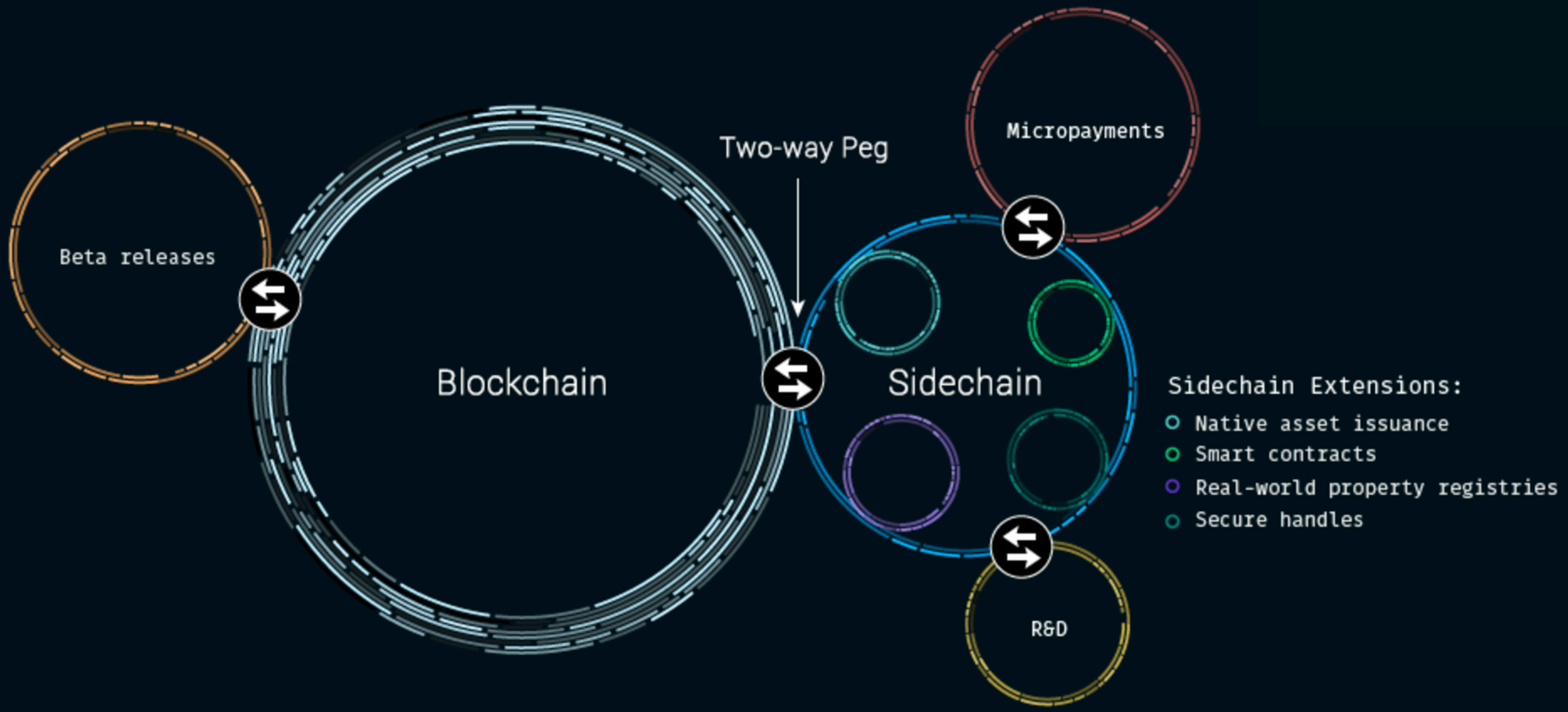
# Battle for the Standard



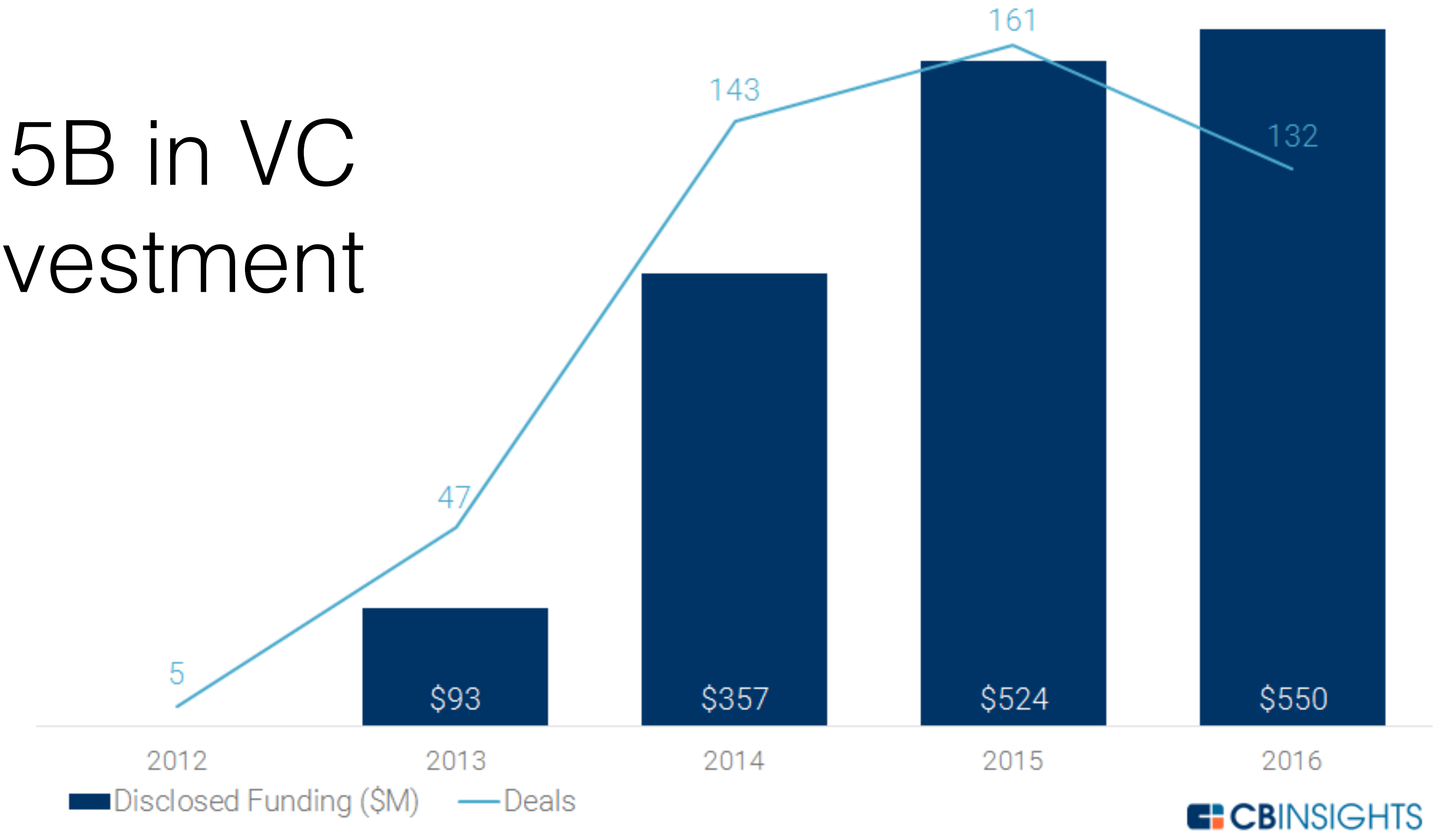
New Bitcoin Blocks

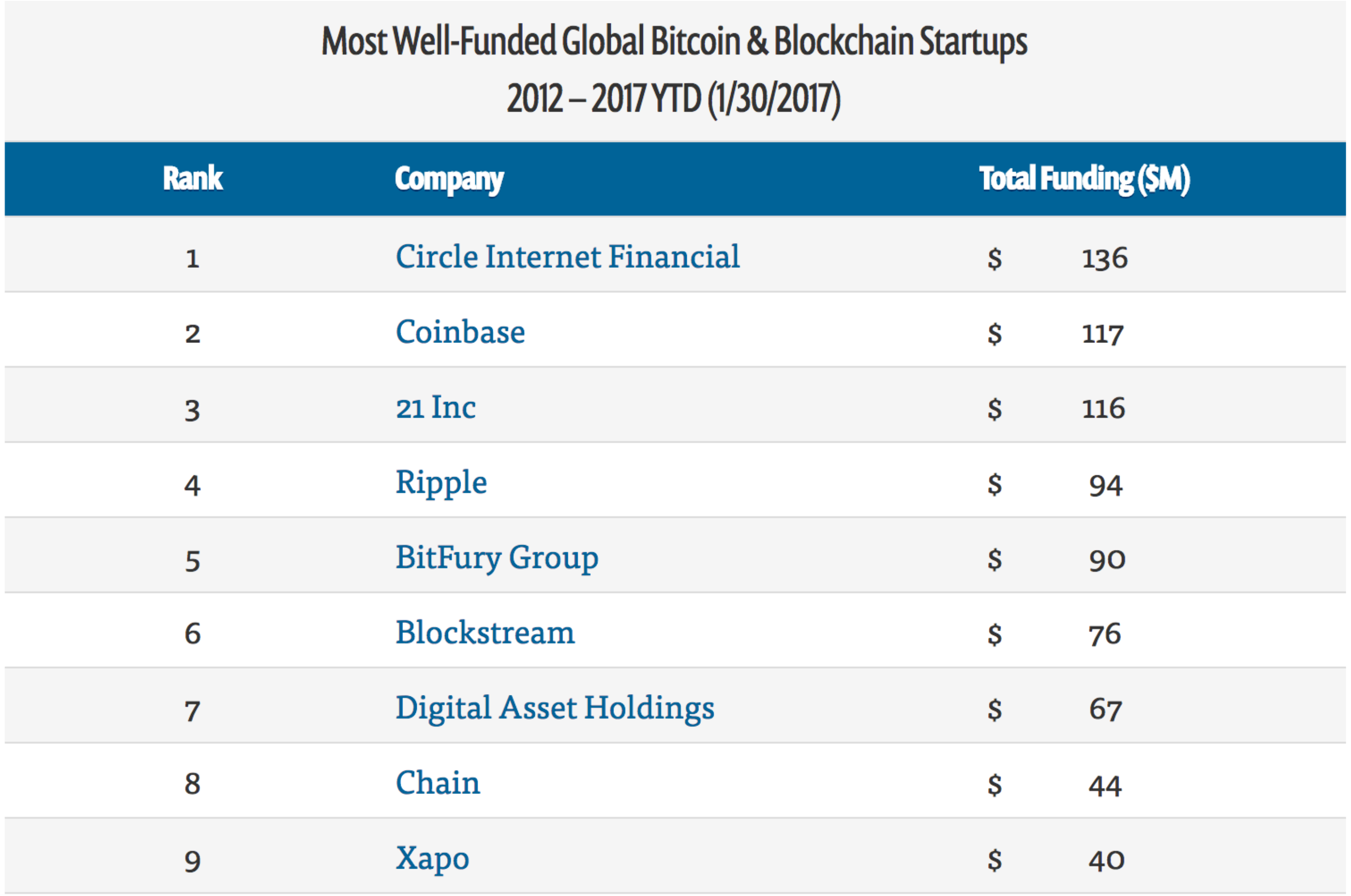
4/3/2017

# Entrepreneurial Experimentation



# 1.5B in VC Investment

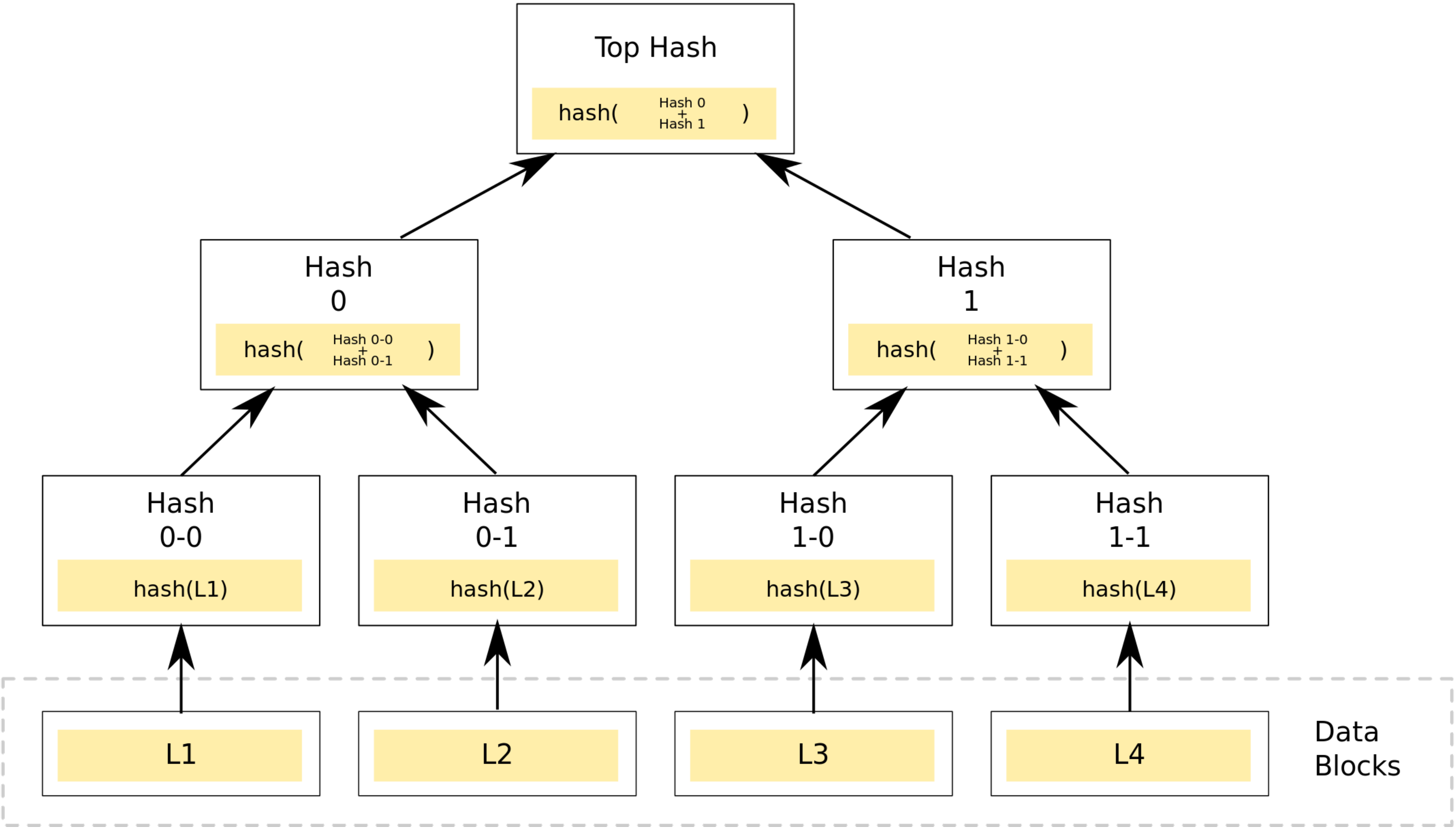




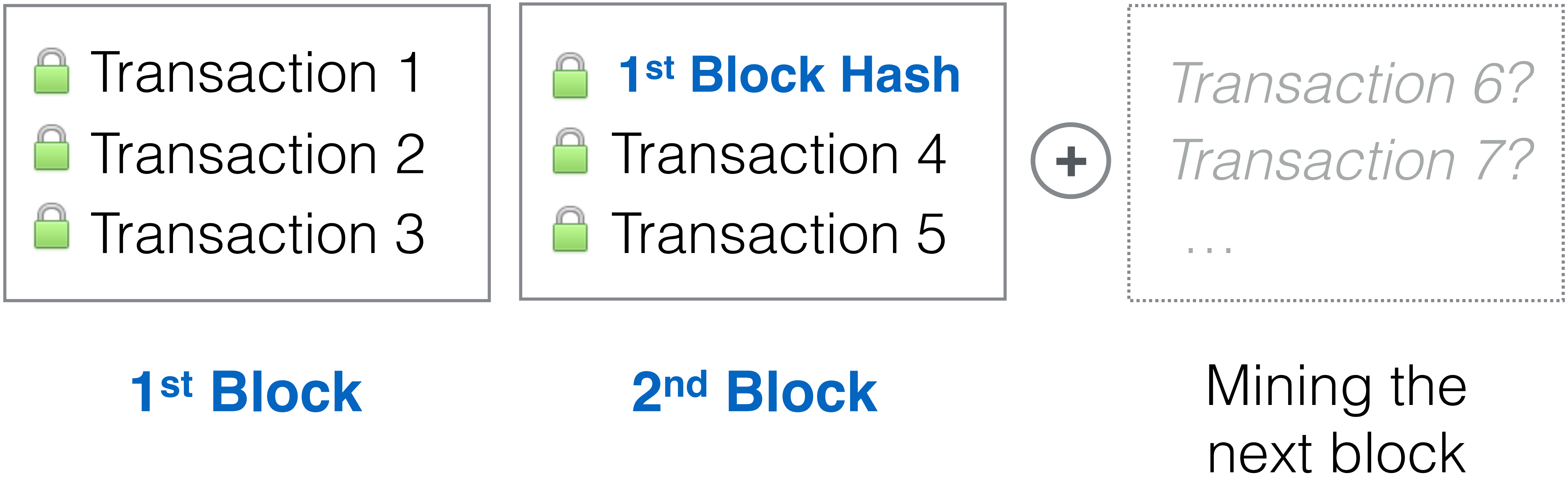
Most Well-Funded Global Bitcoin & Blockchain Startups
2012 – 2017 YTD (1/30/2017)

| Rank | Company | Total Funding ($M) |
|---|---|---|
| 1 | Circle Internet Financial | $ 136 |
| 2 | Coinbase | $ 117 |
| 3 | 21 Inc | $ 116 |
| 4 | Ripple | $ 94 |
| 5 | BitFury Group | $ 90 |
| 6 | Blockstream | $ 76 |
| 7 | Digital Asset Holdings | $ 67 |
| 8 | Chain | $ 44 |
| 9 | Xapo | $ 40 |

# Where is the Breakthrough?



# The Blockchain



🔒 Transaction 1
🔒 Transaction 2
🔒 Transaction 3

**1st Block**

🔒 **1st Block Hash**
🔒 Transaction 4
🔒 Transaction 5

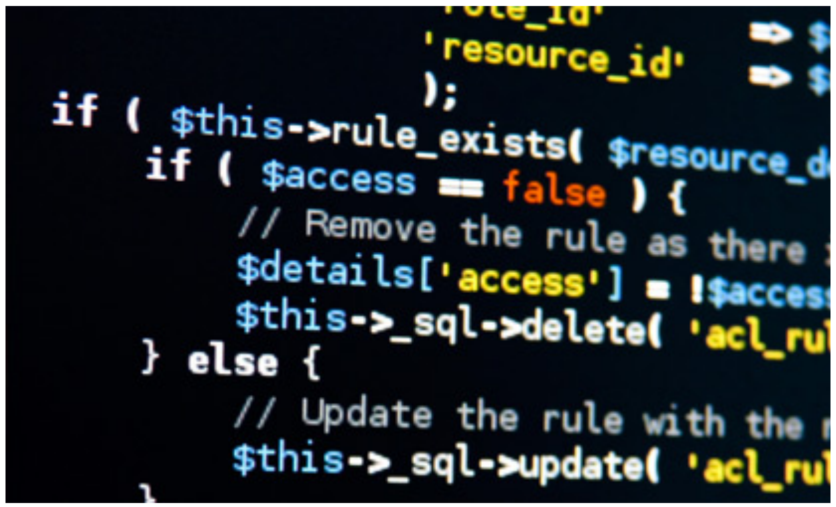
**2nd Block**

+

*Transaction 6?*
*Transaction 7?*
…

Mining the
next block

# The Blockchain



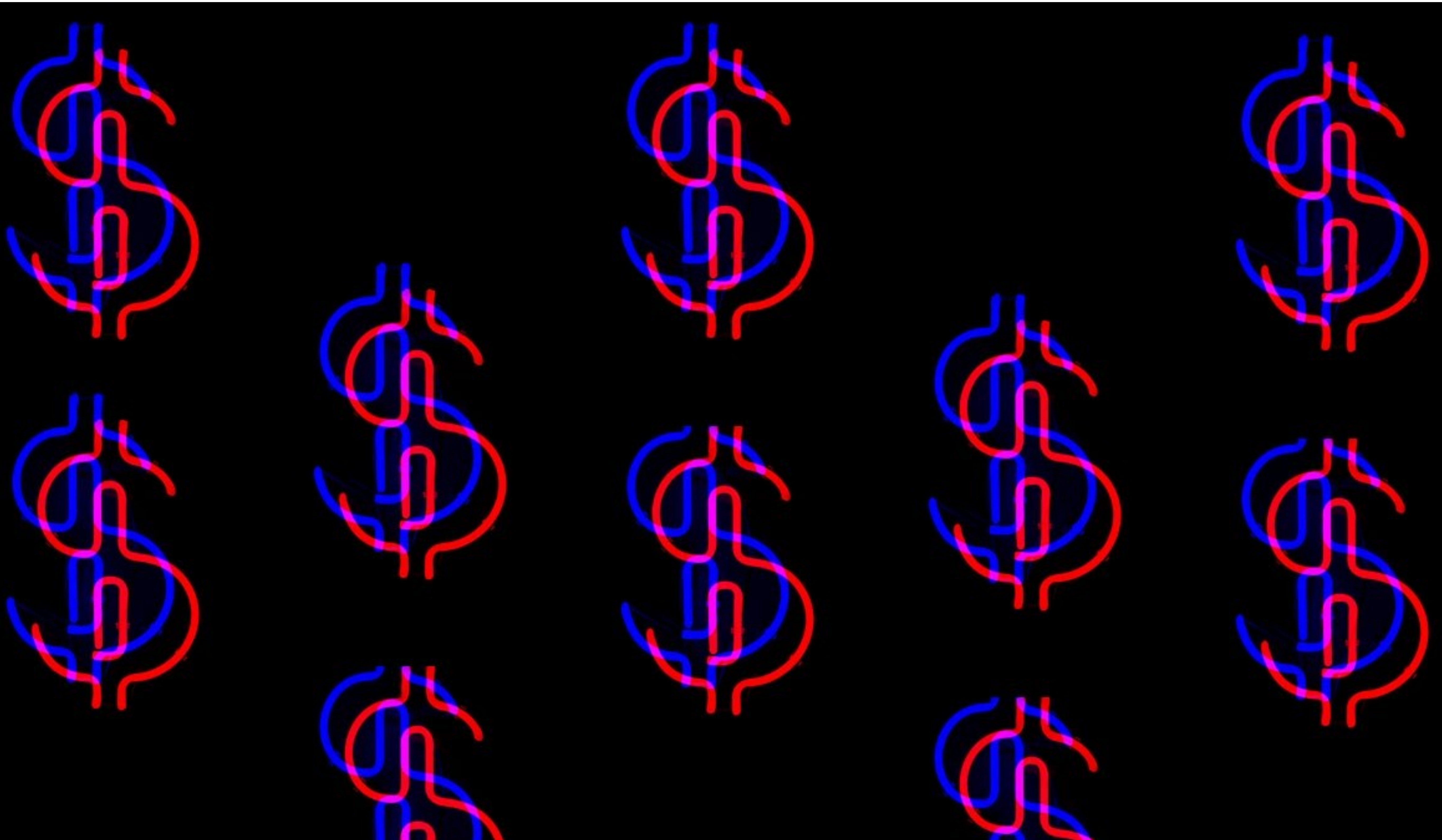
```
                         'role_id'          => $
                         'resource_id'      => $
                         );
  if ( $this->rule_exists( $resource_d
       if ( $access == false ) {
            // Remove the rule as there
            $details['access'] = !$acces
            $this->_sql->delete( 'acl_rul
       } else {
            // Update the rule with the
            $this->_sql->update( 'acl_rul
       }
```

Computer Science

Economics and Market Design

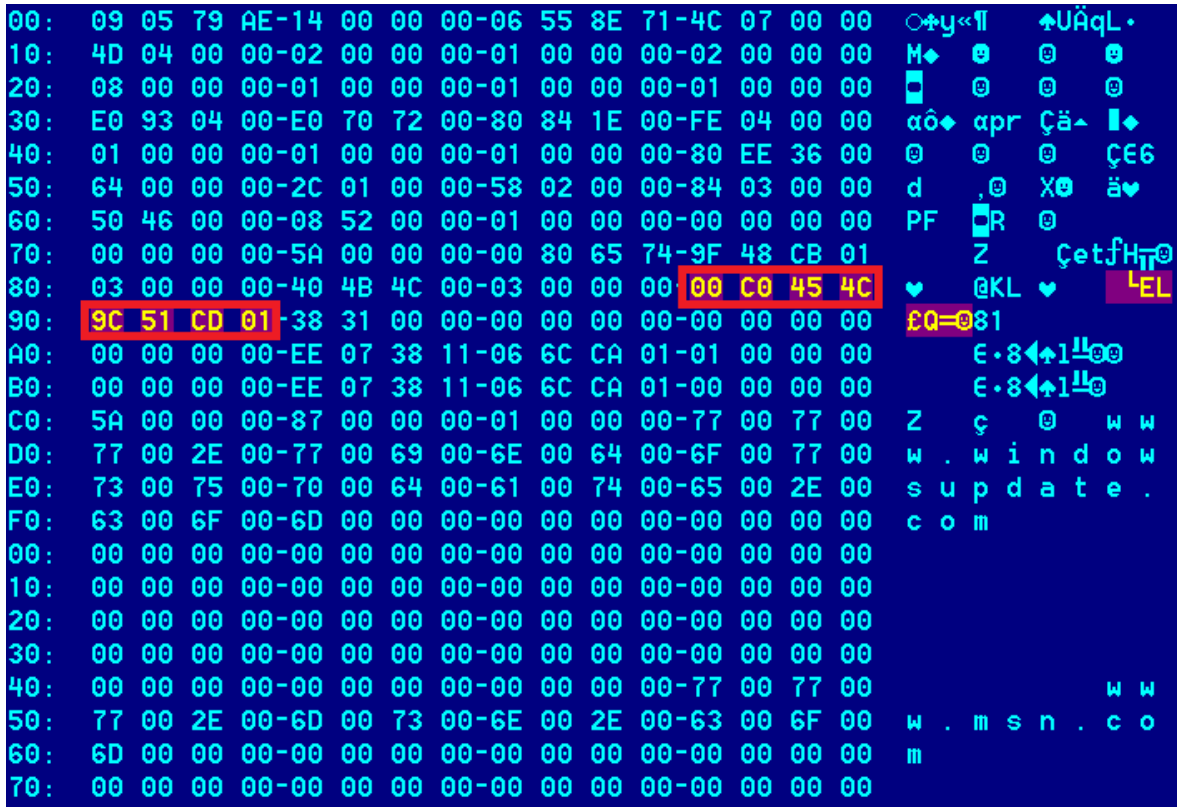
Law

# Economists Like to Think of Technology Changes in Terms of Costs…



# A Reduction in Two Key Costs

## 1. **Cost of Verification**

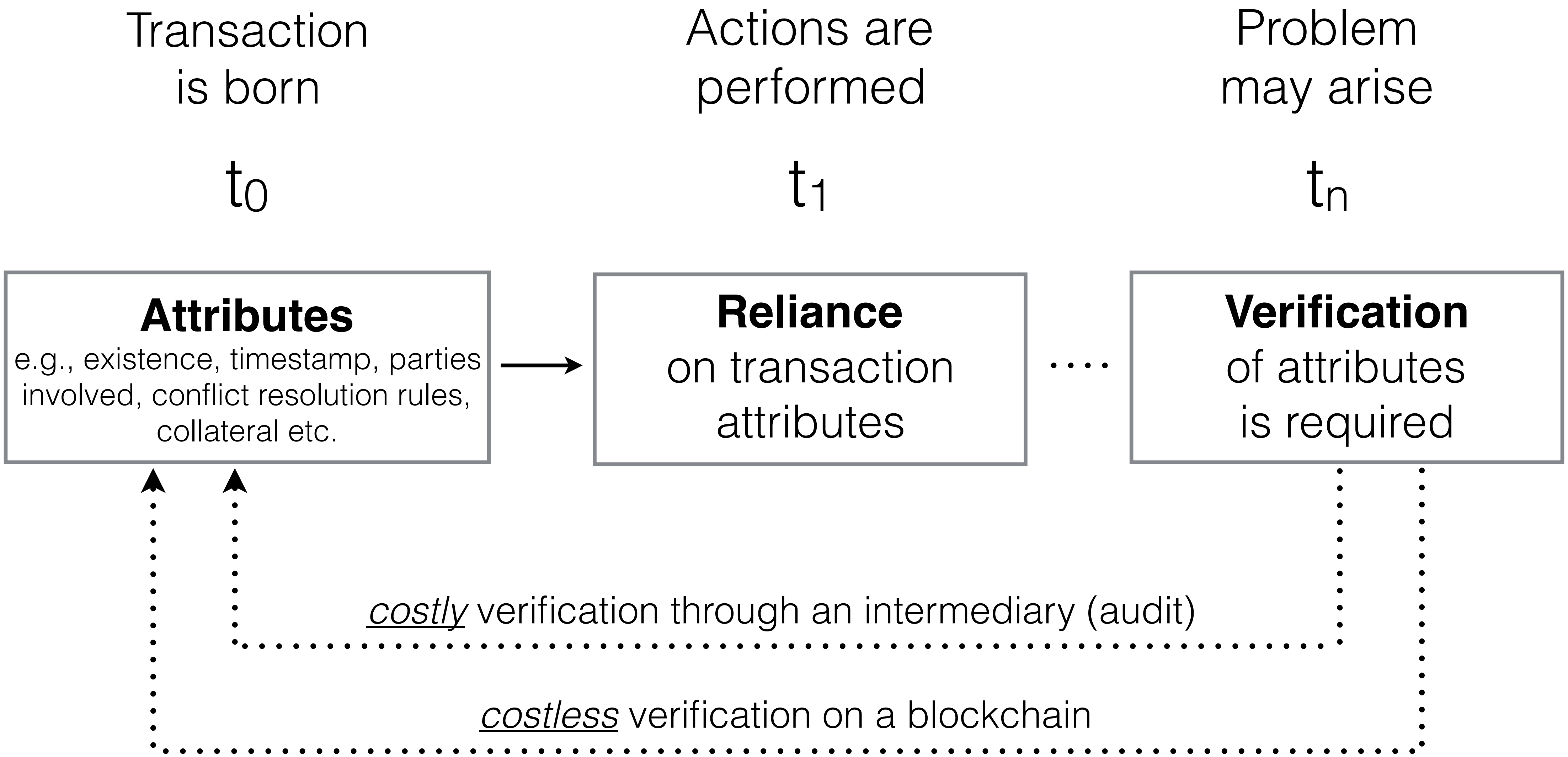


```
00:   09 05 79 AE-14 00 00 00-06 55 8E 71-4C 07 00 00  ○♣y«¶   ♠UÄqL•
10:   4D 04 00 00-02 00 00 00-01 00 00 00-02 00 00 00  M♦  ☻   ☺   ☻
20:   08 00 00 00-01 00 00 00-01 00 00 00-01 00 00 00  ◘   ☺   ☺   ☺
30:   E0 93 04 00-E0 70 72 00-80 84 1E 00-FE 04 00 00  αô♦ αpr Çä▲ ■♦
40:   01 00 00 00-01 00 00 00-01 00 00 00-80 EE 36 00  ☺   ☺   ☺   Çε6
50:   64 00 00 00-2C 01 00 00-58 02 00 00-84 03 00 00  d   ,☺  X☻  ä♥
60:   50 46 00 00-08 52 00 00-01 00 00 00-00 00 00 00  PF  ◘R  ☺
70:   00 00 00 00-5A 00 00 00-00 80 65 74-9F 48 CB 01      Z    Çetƒ H╦☺
80:   03 00 00 00-40 4B 4C 00-03 00 00 00-00 C0 45 4C  ♥   @KL ♥    └EL
90:   9C 51 CD 01-38 31 00 00-00 00 00 00-00 00 00 00  £Q═☺81
A0:   00 00 00 00-EE 07 38 11-06 6C CA 01-01 00 00 00      ε•8◄♠l╩☺☺
B0:   00 00 00 00-EE 07 38 11-06 6C CA 01-00 00 00 00      ε•8◄♠l╩☺
C0:   5A 00 00 00-87 00 00 00-01 00 00 00-77 00 77 00  Z   ç   ☺   w w
D0:   77 00 2E 00-77 00 69 00-6E 00 64 00-6F 00 77 00  w . w i n d o w
E0:   73 00 75 00-70 00 64 00-61 00 74 00-65 00 2E 00  s u p d a t e .
F0:   63 00 6F 00-6D 00 00 00-00 00 00 00-00 00 00 00  c o m
00:   00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
10:   00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
20:   00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
30:   00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
40:   00 00 00 00-00 00 00 00-00 00 00 00-77 00 77 00              w w
50:   77 00 2E 00-6D 00 73 00-6E 00 2E 00-63 00 6F 00  w . m s n . c o
60:   6D 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00  m
70:   00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
```

“00 c0 45 4c 9c 51 cd 01” translates to June 24th, 2012

## 2. **Cost of Networking**

# 1. Costless Verification



Transaction is born

$t_0$

Actions are performed

$t_1$

Problem may arise

$t_n$

**Attributes**
e.g., existence, timestamp, parties involved, conflict resolution rules, collateral etc.

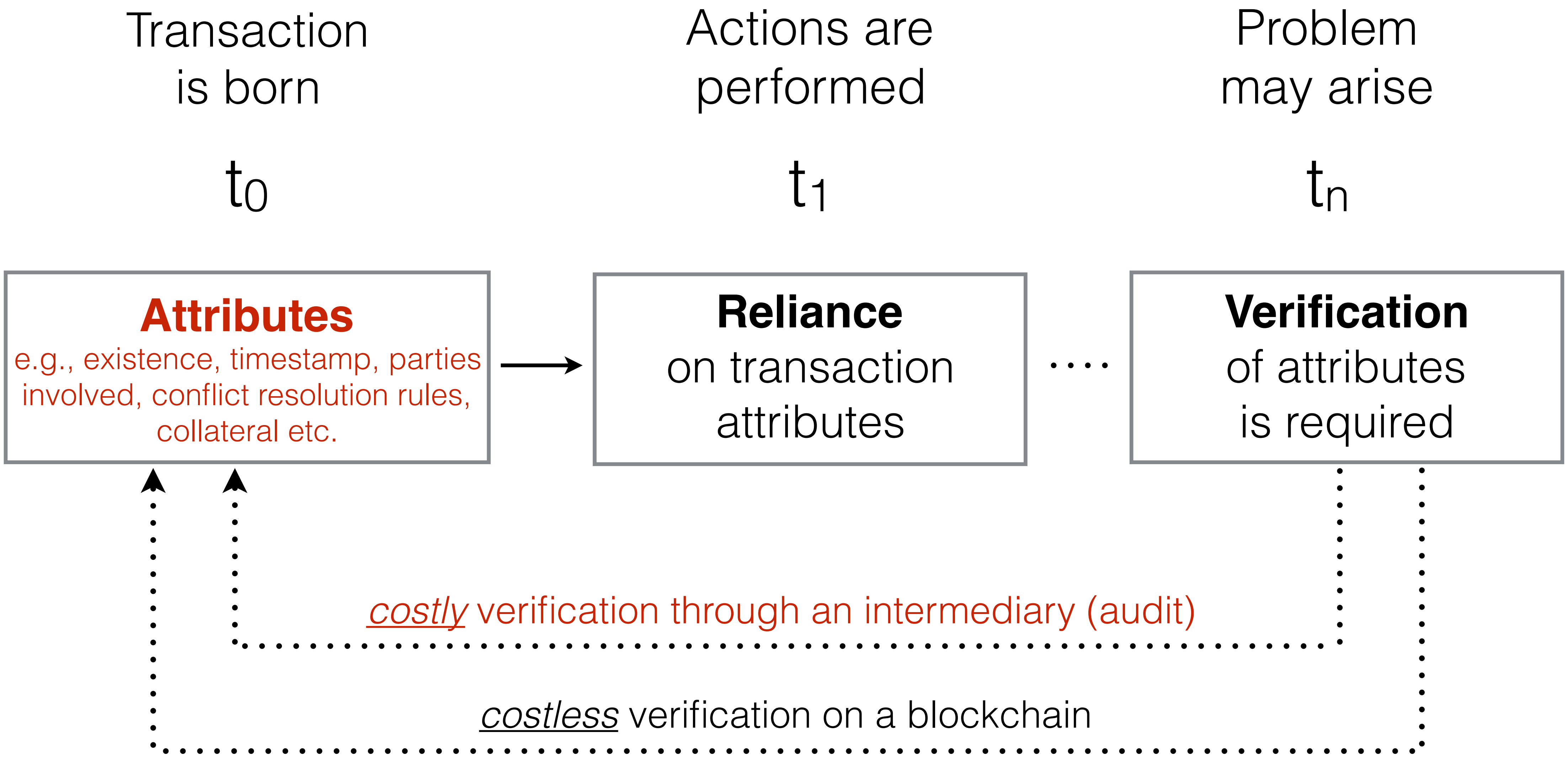
**Reliance**
on transaction attributes

**Verification**
of attributes is required

*costly* verification through an intermediary (audit)

*costless* verification on a blockchain

# Information Leakage



Transaction is born

$t_0$

**Attributes**

e.g., existence, timestamp, parties involved, conflict resolution rules, collateral etc.

Actions are performed

$t_1$

**Reliance**

on transaction attributes

Problem may arise

$t_n$

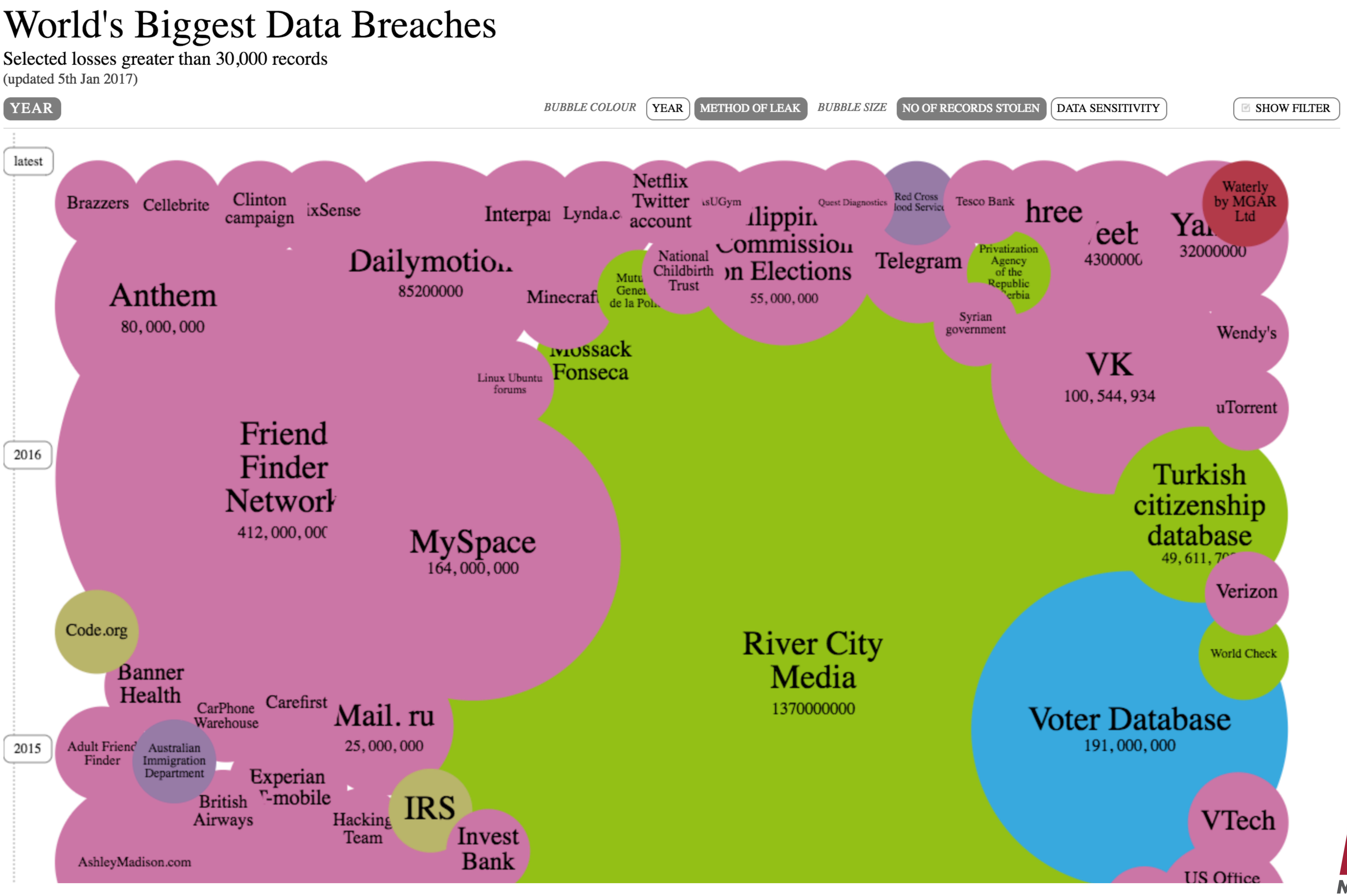
**Verification**

of attributes is required

*costly* verification through an intermediary (audit)

*costless* verification on a blockchain

# Information Leakage

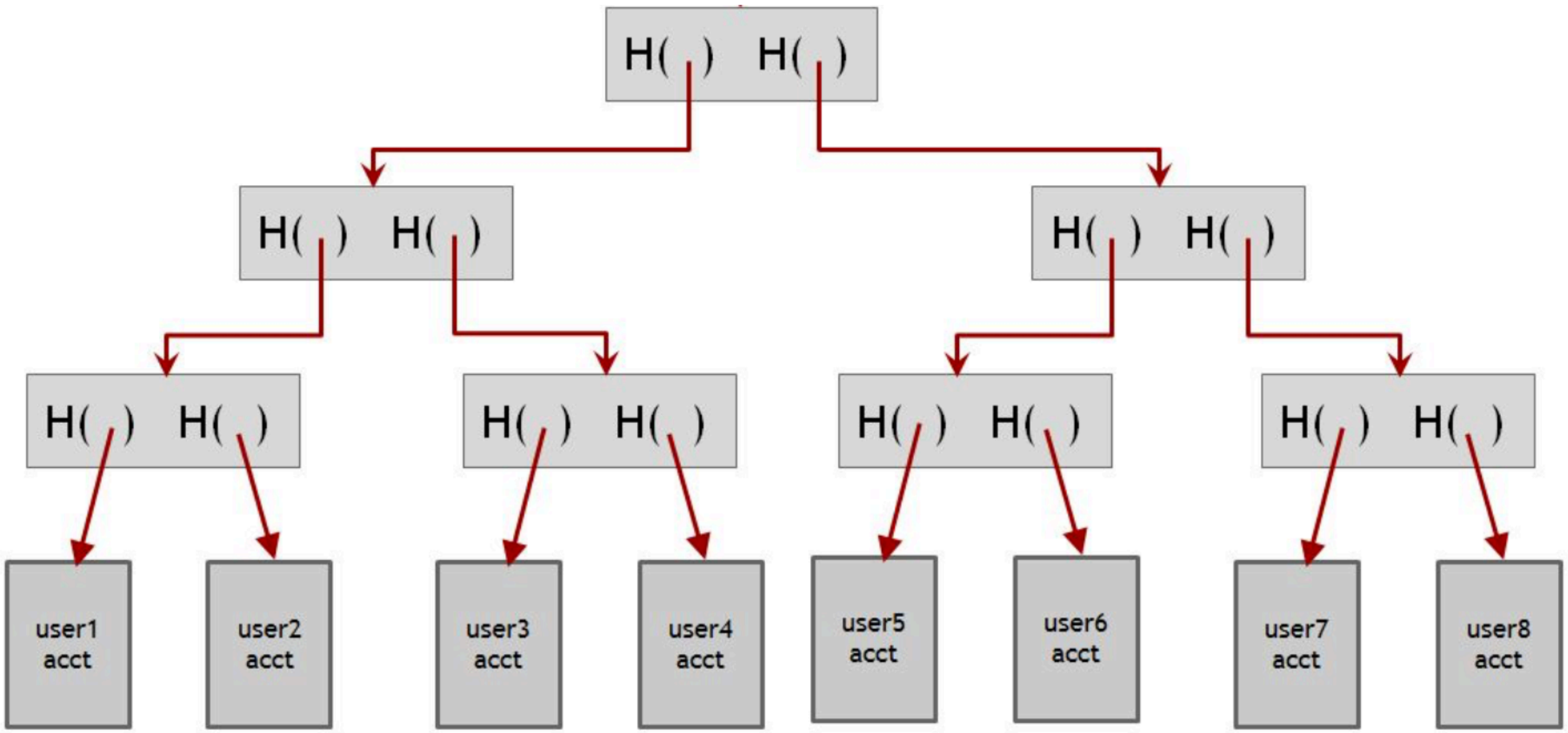


World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 5th Jan 2017)

# Data Integrity Through Costless Verification



# 2. Cost of Networking

- One could argue that we had the ability to crowdsource **ideas**, **labor**, **capital**, and other **resources** for some time…

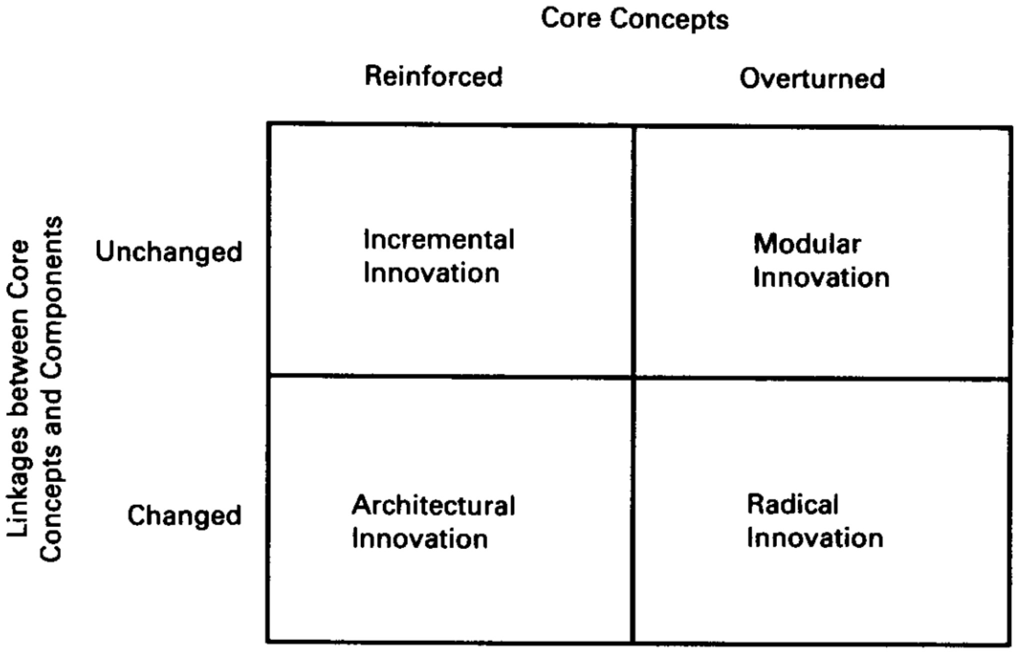
- However current solutions rely on traditional intermediaries (typically **platforms**) to aggregate the intentions of the crowd, source expertise, redistribute returns

MIT MANAGEMENT SLOAN SCHOOL

# 2. Cost of Networking

- The **architectural change** brought by cryptocurrencies is tied to their use of a native token to incentivize the growth, operations, and securing of a network

- “We show that architectural innovations **destroy the usefulness of the architectural knowledge of established firms**, and that since architectural knowledge tends to become embedded in the structure and information-processing procedures of established organizations, **this destruction is difficult for firms to recognize and hard to correct**”
  - Rebecca Henderson and Kim Clark

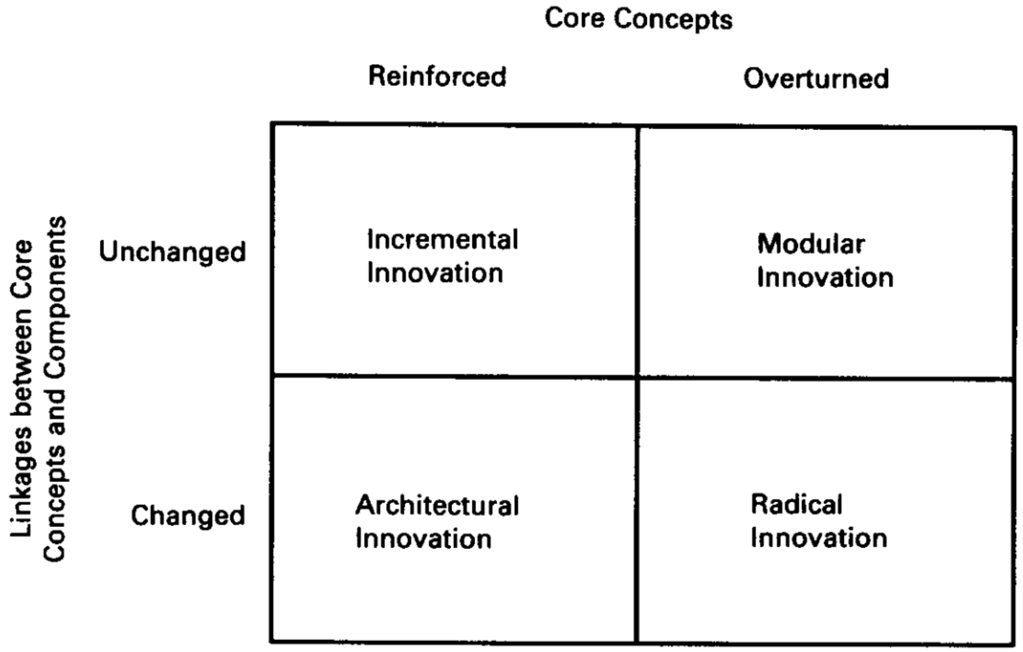


| Linkages between Core Concepts and Components | Core Concepts: Reinforced | Core Concepts: Overturned |
|---|---|---|
| Unchanged | Incremental Innovation | Modular Innovation |
| Changed | Architectural Innovation | Radical Innovation |

Henderson, R. M.; Clark, K. B., ASQ (1990) Architectural Innovation: The Reconfiguration Of Existing Product Technologies and the Failure of Established Firms

# 2. Cost of Networking

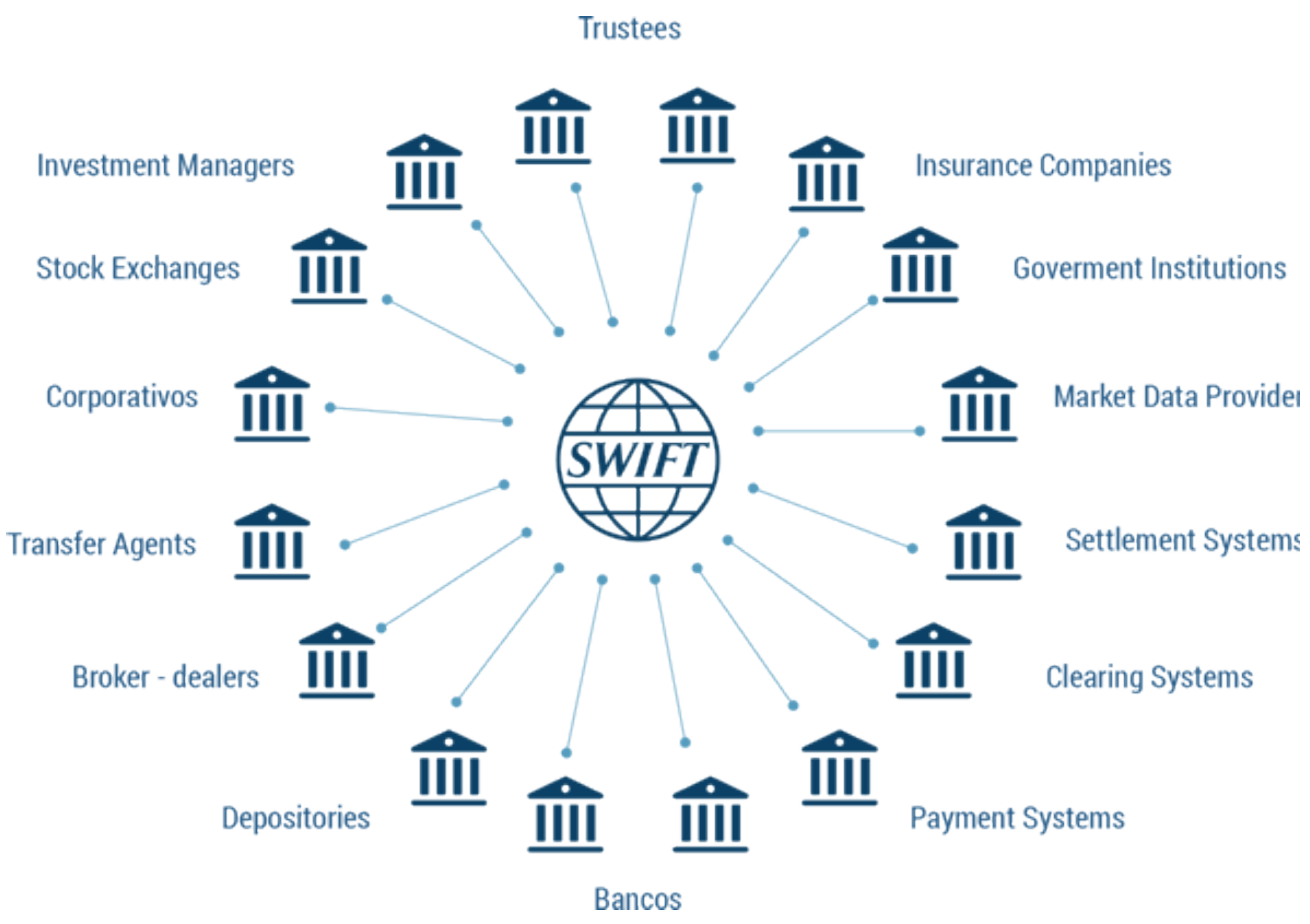
- Traditional networks (and platforms) rely on trusted nodes, reputation systems
  - e.g. SWIFT, ACH, Uber, Airbnb
- These **nodes are costly to maintain**, often labor intensive
- A cryptocurrency allows you to **bootstrap an ecosystem** without trusted nodes
  - e.g. in Bitcoin use PoW to provide incentives for maintaining and updating a shared ledger
- The role of **internet-level consensus**



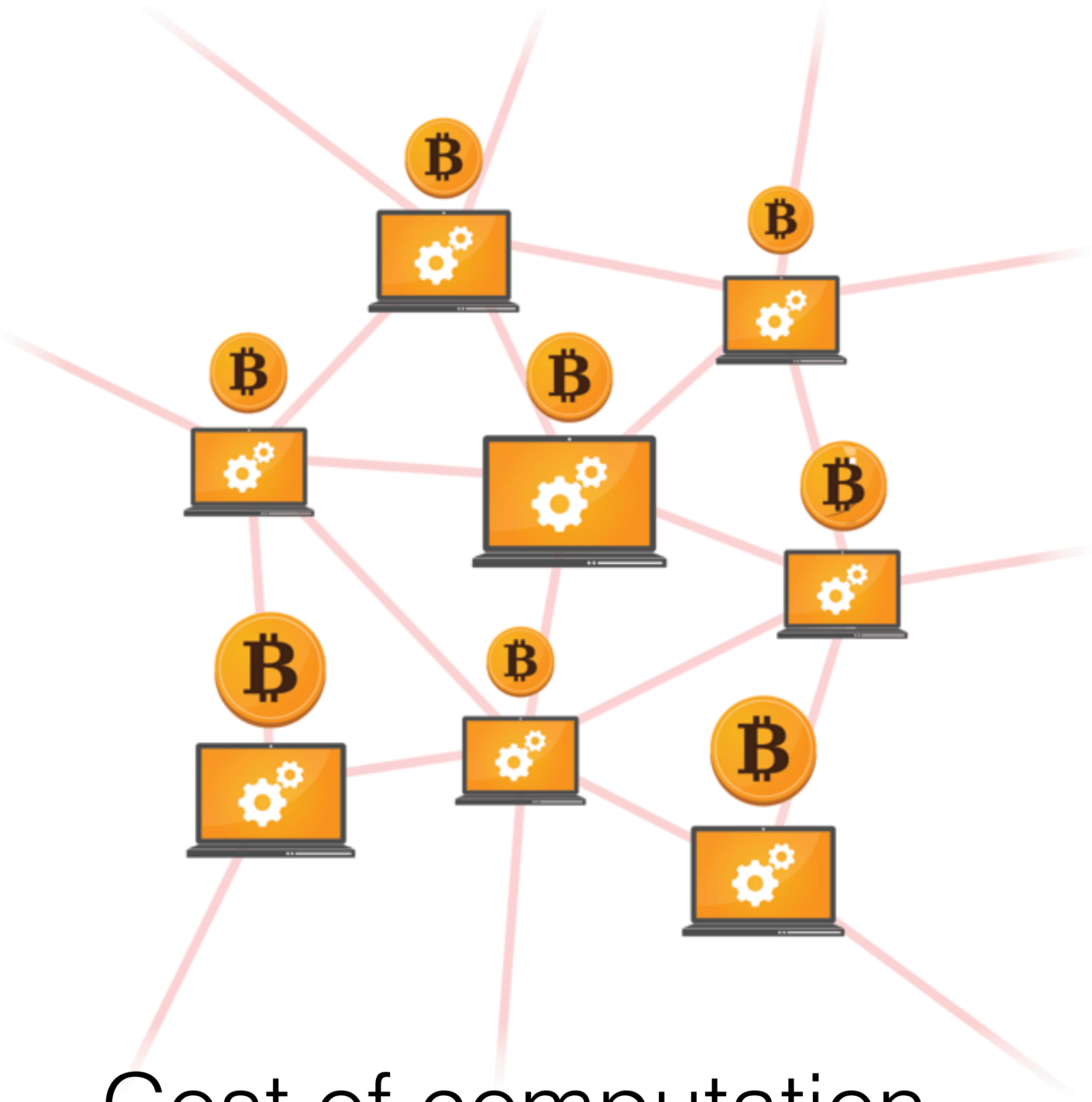
| Linkages between Core Concepts and Components | Core Concepts: Reinforced | Core Concepts: Overturned |
|---|---|---|
| Unchanged | Incremental Innovation | Modular Innovation |
| Changed | Architectural Innovation | Radical Innovation |

Henderson, R. M.; Clark, K. B., ASQ (1990) Architectural Innovation: The Reconfiguration Of Existing Product Technologies and the Failure of Established Firms

# 2. Cost of Networking

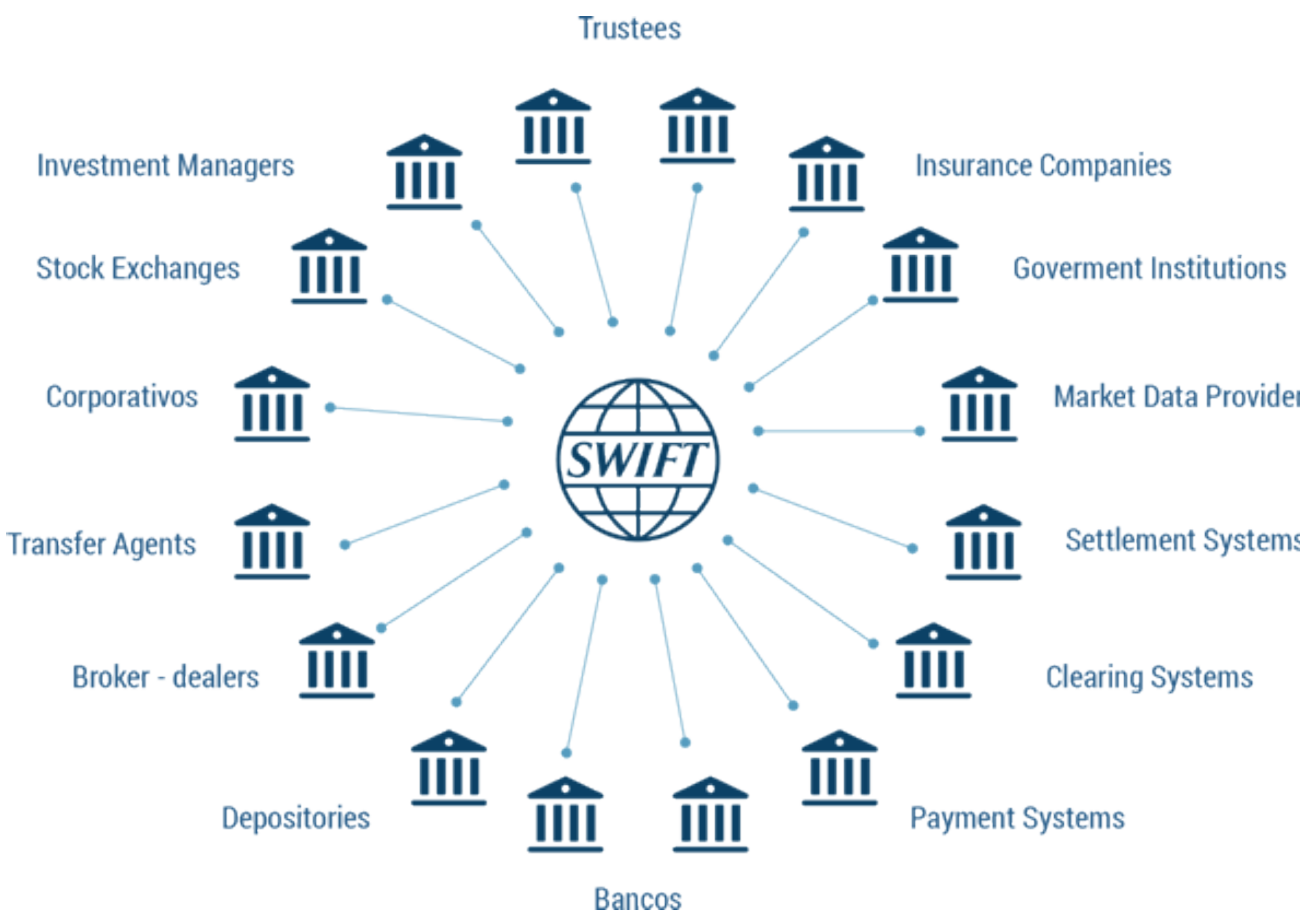


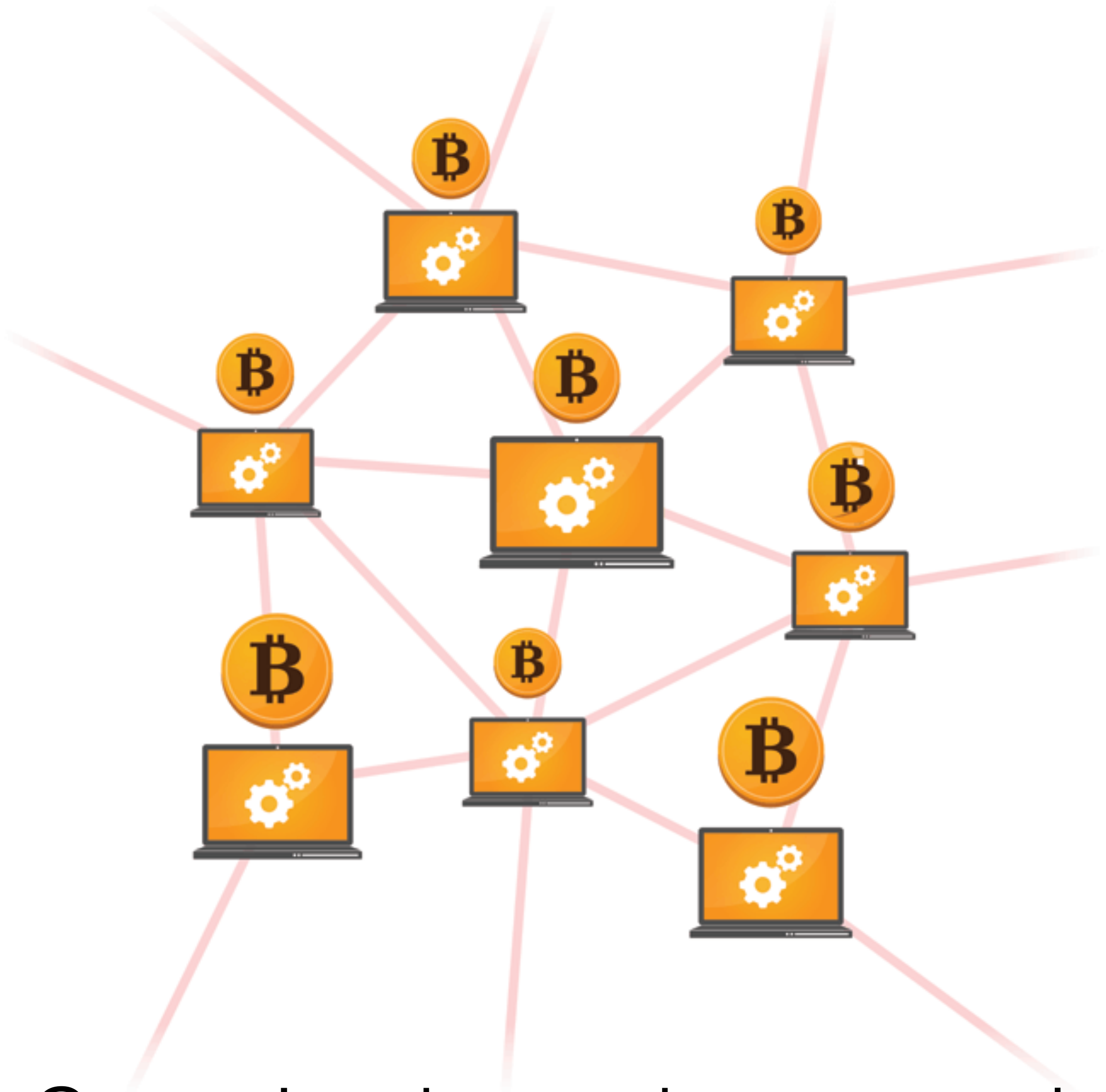
Cost of vetting and maintaining the integrity of the nodes



Cost of computation (sunk commitment to the shared ledger)

# 2. Cost of Networking

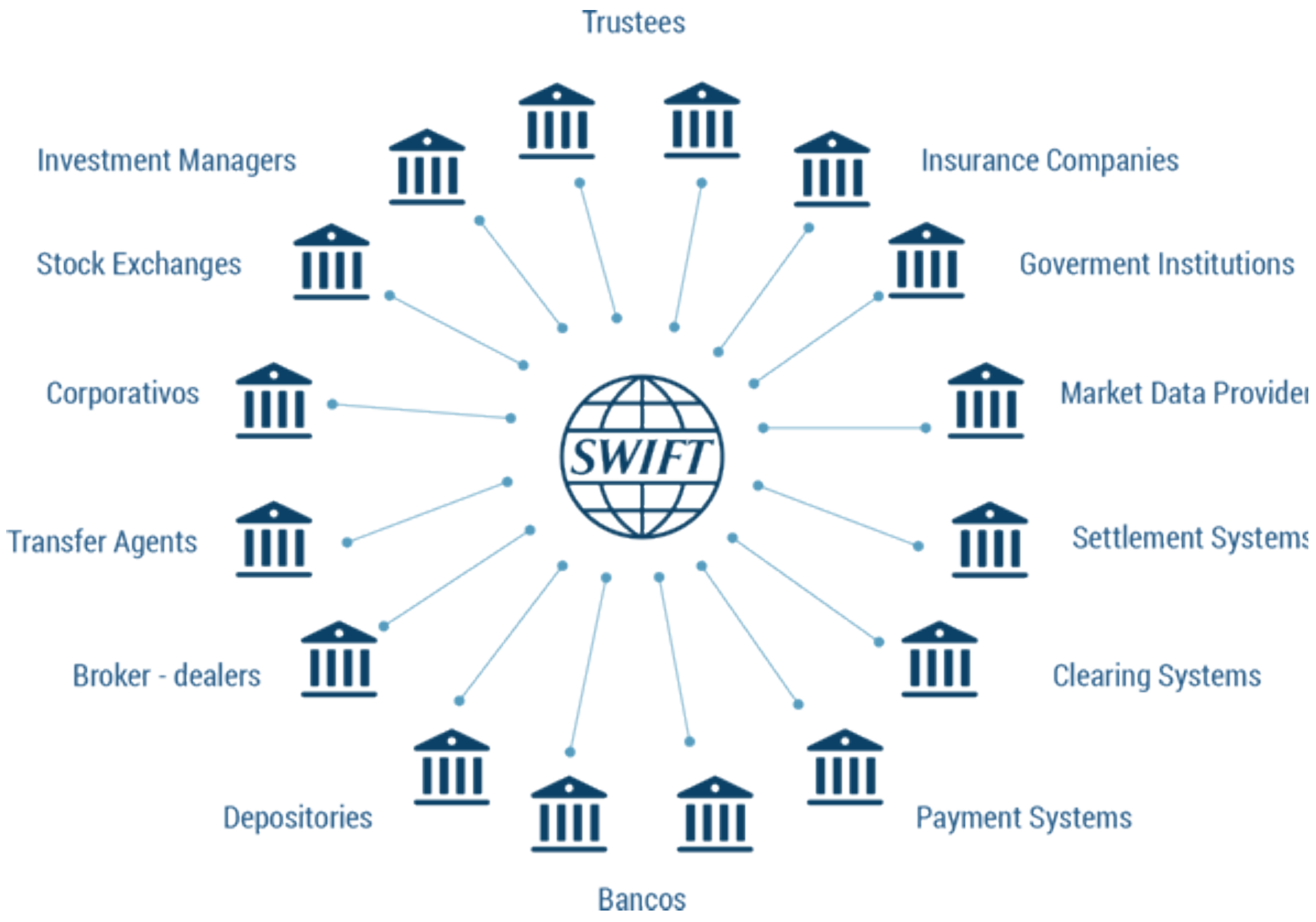


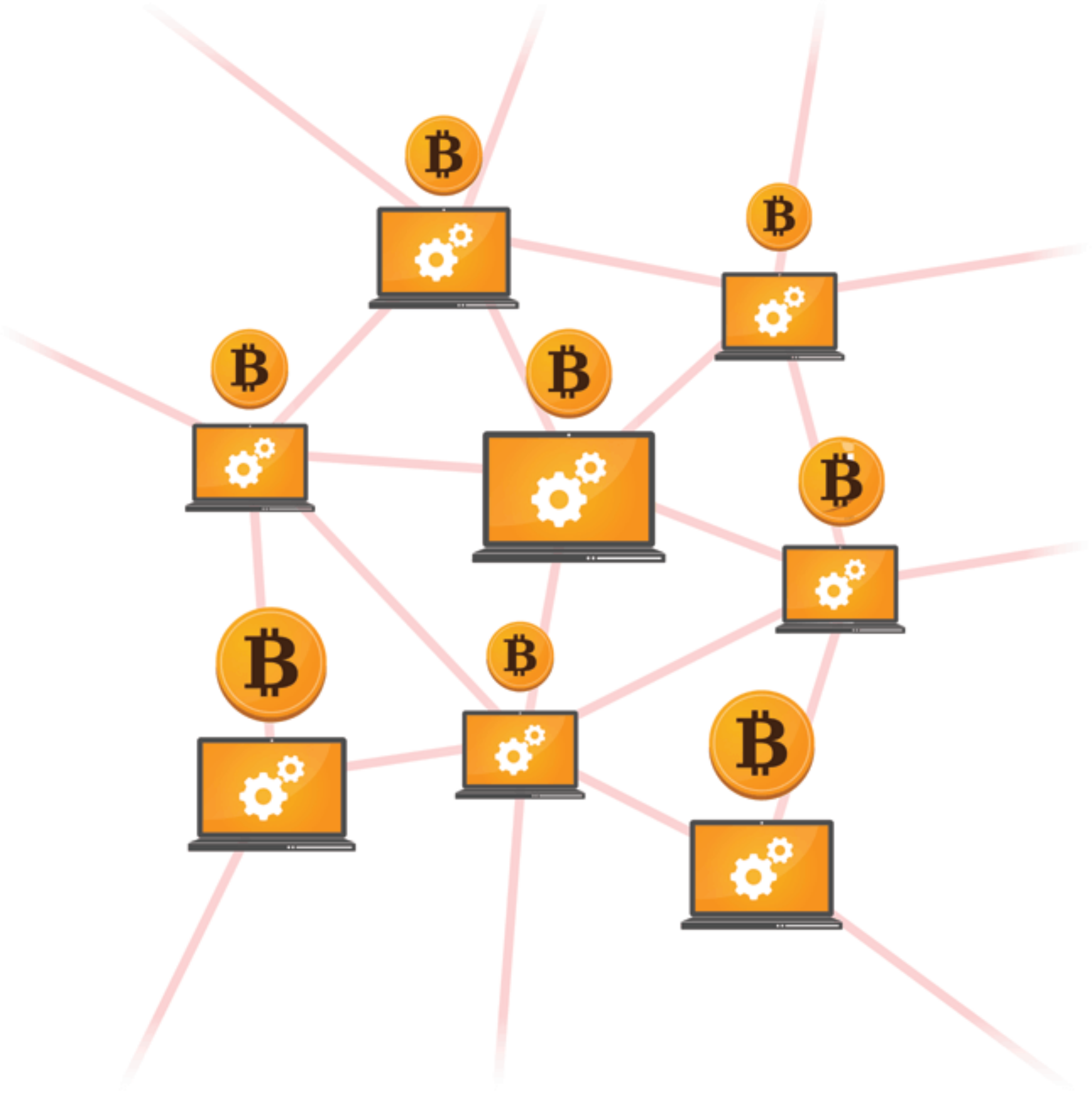


Security through trusted intermediaries / fiat. Typically fast (e.g. VISA)

Security through protocol design, game theory. Currently slow (e.g. BTC)

# 2. Cost of Networking

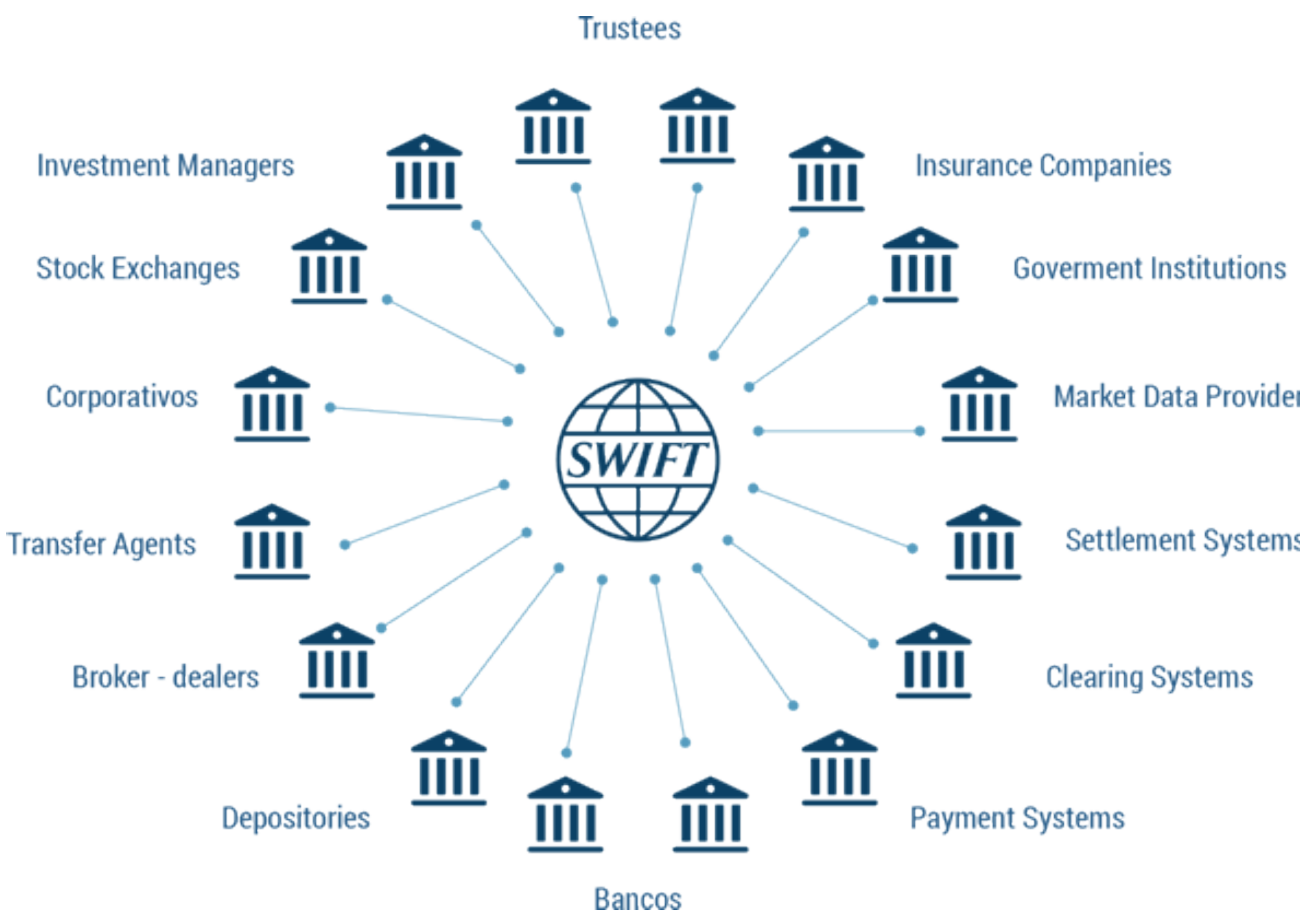


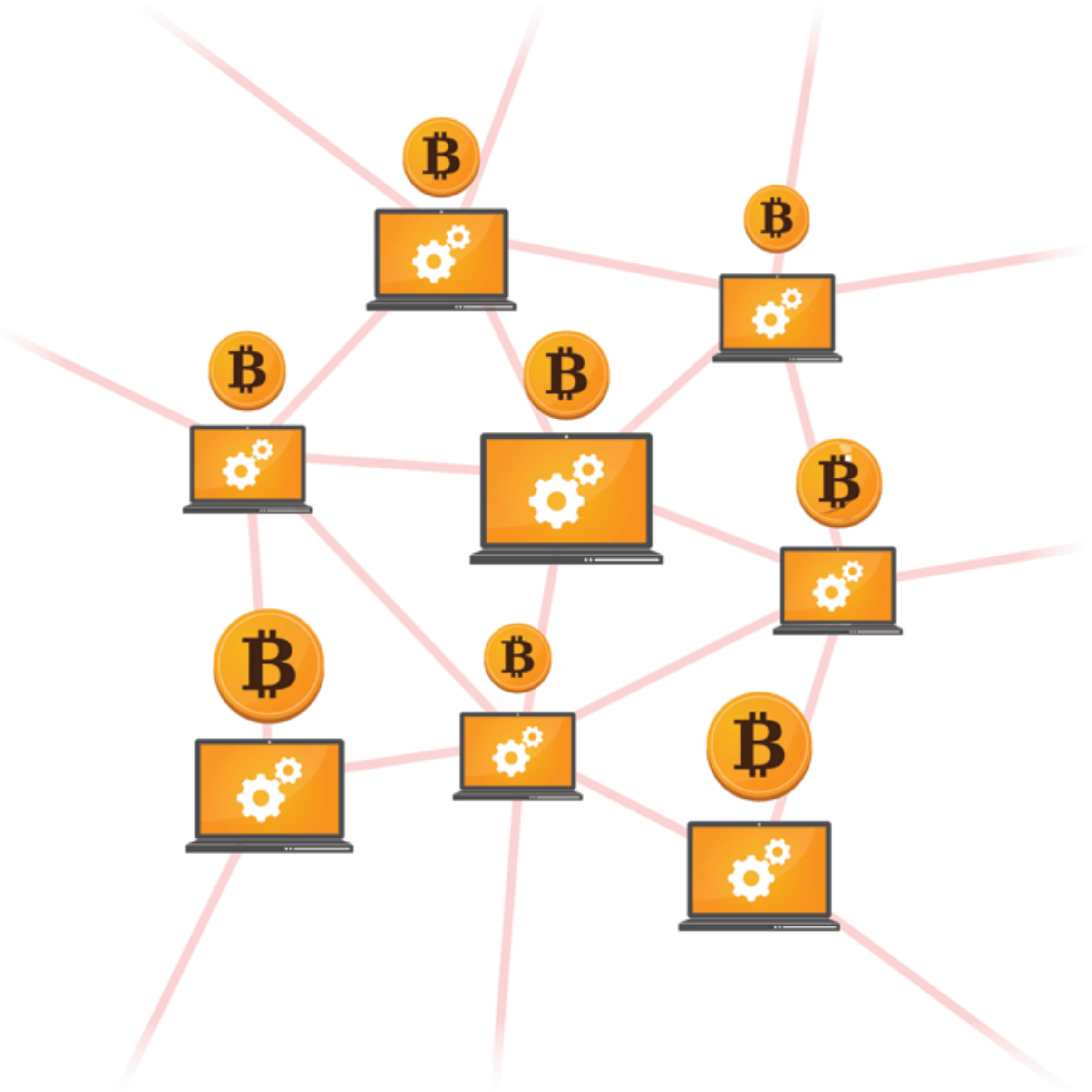


Ownership of the assets resides with the nodes, nodes certify txs

Ownership of the assets resides with the users, no censorship

# 2. Cost of Networking

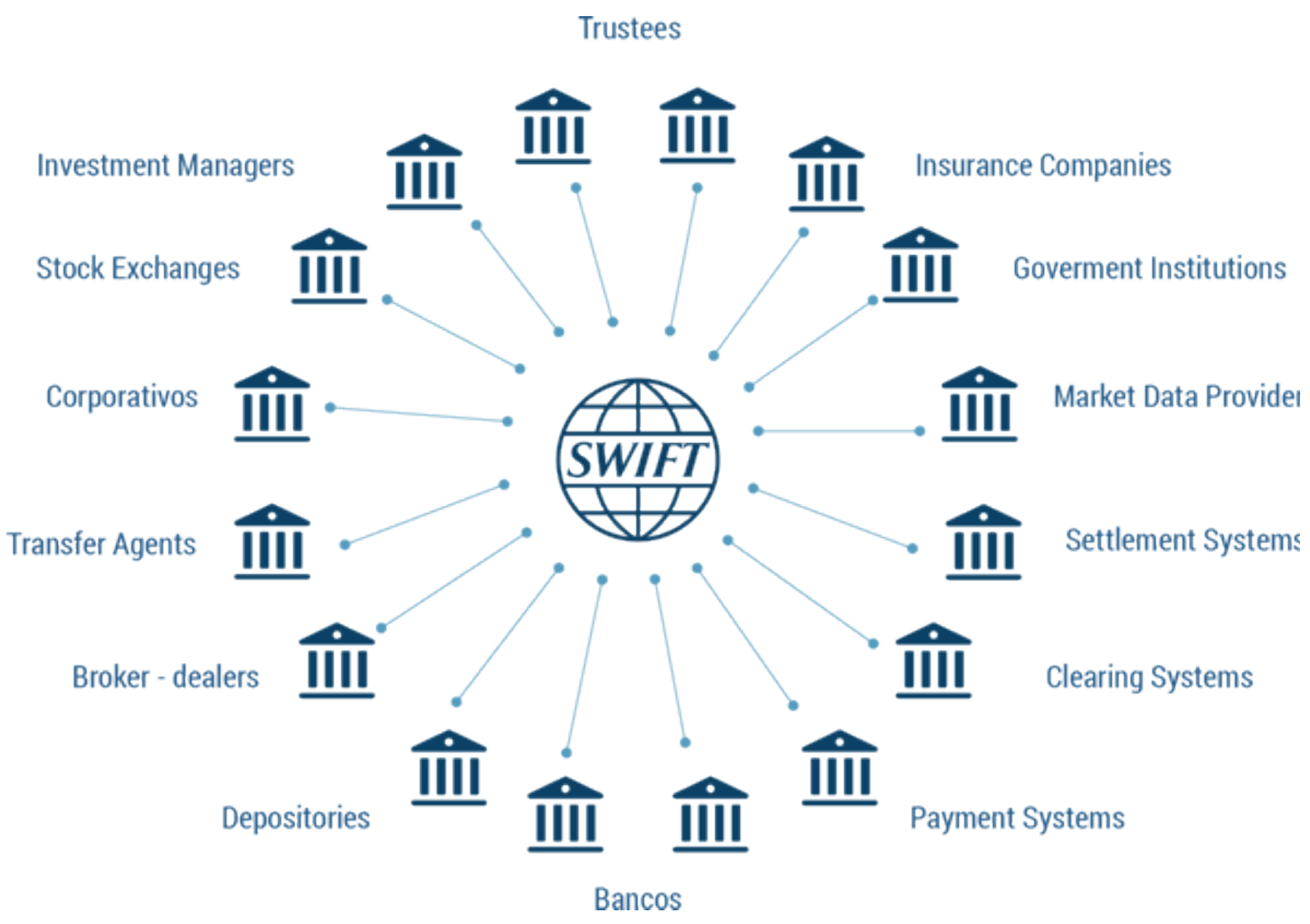


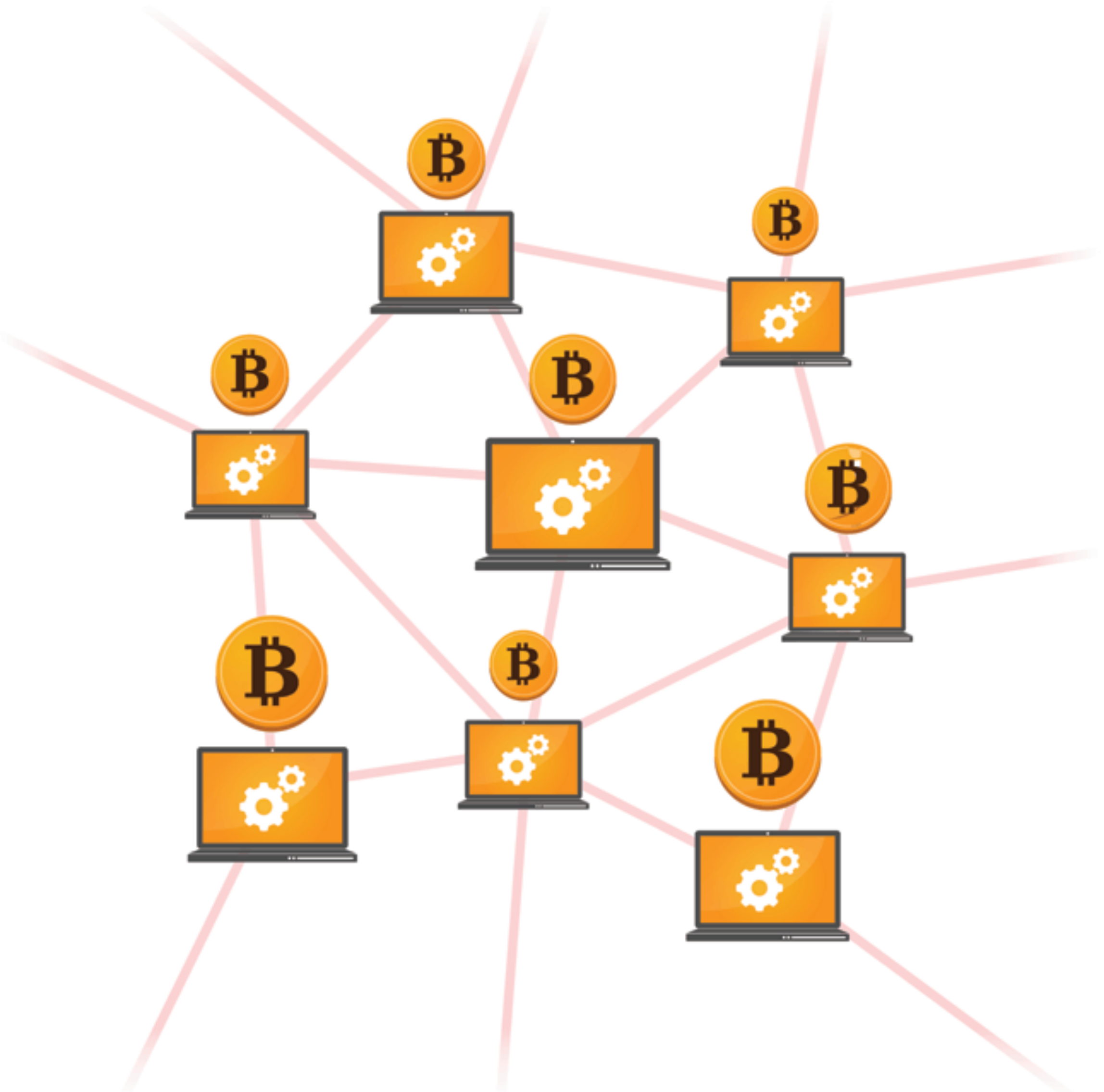


Innovation requires approval (compliance)

Permissionless innovation (no compliance)

# 2. Cost of Networking



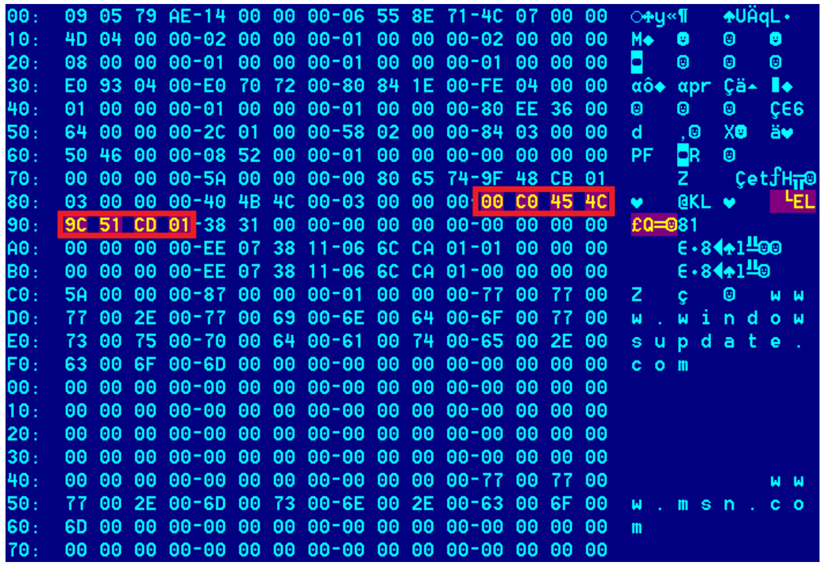


Trusted intermediaries **retain market power** (e.g. payment rails, reputation scores etc)

Trusted intermediaries need to **add value through market design layer** (e.g. curation)

# Economic Impact

## 1. **Cost of Verification**



```
00:  09 05 79 AE-14 00 00 00-06 55 8E 71-4C 07 00 00  ○♠y«¶   ♠UÄqL·
10:  4D 04 00 00-02 00 00 00-01 00 00 00-02 00 00 00  M♦  ☻   ☺   ☻
20:  08 00 00 00-01 00 00 00-01 00 00 00-01 00 00 00  ◘   ☺   ☺   ☺
30:  E0 93 04 00-E0 70 72 00-80 84 1E 00-FE 04 00 00  αô♦ αpr Çä▲ ■♦
40:  01 00 00 00-01 00 00 00-01 00 00 00-80 EE 36 00  ☺   ☺   ☺   Çε6
50:  64 00 00 00-2C 01 00 00-58 02 00 00-84 03 00 00  d   ,☺  X☻  ä♥
60:  50 46 00 00-08 52 00 00-01 00 00 00-00 00 00 00  PF  ◘R  ☺
70:  00 00 00 00-5A 00 00 00-00 80 65 74-9F 48 CB 01      Z    Çetƒ H╦☺
80:  03 00 00 00-40 4B 4C 00-03 00 00 00-00 C0 45 4C  ♥   @KL ♥    └EL
90:  9C 51 CD 01-38 31 00 00-00 00 00 00-00 00 00 00  £Q═☺81
A0:  00 00 00 00-EE 07 38 11-06 6C CA 01-01 00 00 00      ε•8◄♠l╩☺☺
B0:  00 00 00 00-EE 07 38 11-06 6C CA 01-00 00 00 00      ε•8◄♠l╩☺
C0:  5A 00 00 00-87 00 00 00-01 00 00 00-77 00 77 00  Z   ç   ☺   w w
D0:  77 00 2E 00-77 00 69 00-6E 00 64 00-6F 00 77 00  w . w i n d o w
E0:  73 00 75 00-70 00 64 00-61 00 74 00-65 00 2E 00  s u p d a t e .
F0:  63 00 6F 00-6D 00 00 00-00 00 00 00-00 00 00 00  c o m
00:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
10:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
20:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
30:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
40:  00 00 00 00-00 00 00 00-00 00 00 00-77 00 77 00              w w
50:  77 00 2E 00-6D 00 73 00-6E 00 2E 00-63 00 6F 00  w . m s n . c o
60:  6D 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00  m
70:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
```

**Incremental innovation**

- More verification!
- Data integrity from the ground up
- Privacy vs customization
- Economies of scale

## 2. **Cost of Networking**

**Architectural innovation**

- Increased competition (e.g. payment and settlement rails, reputation systems)
- Intermediaries can still add value through market design layer
- New ecosystems (e.g. permissionless ones)

# A New Organizational Form?

*“These operations are often **extremely costly**, sufficiently costly at any rate to **prevent many transactions** that would be carried out in a world in which the **pricing system worked without cost**”*
- Nobel laureate Ronald Coase (1960)

- Decentralized and incentives-driven like a **spot market**
- Can replicate the **complex forms of governance** that take place within a traditional corporation

MIT MANAGEMENT SLOAN SCHOOL

# A New Organizational Form?

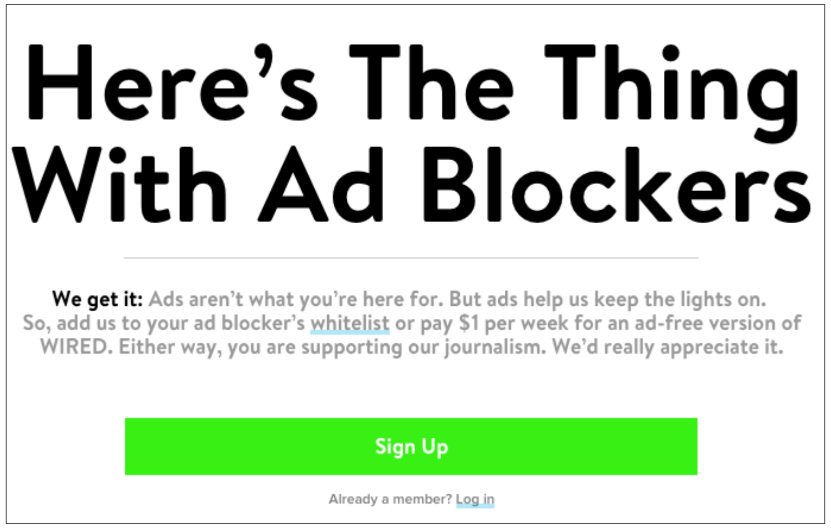
*"If we possess* ***all the relevant information****, if we can start out from a given system of* ***preferences****, and if we command complete* ***knowledge of available means****, the problem which remains is purely one of* ***logic****."*
*- Hayek* (1945)

- A novel approach to **value creation** and **value capture**
- Intermediaries will still add substantial value to markets, but the **nature of intermediation will change**
- Economies of scale in matching demand and supply of labor, capital and ideas
- Lower infrastructure costs than incumbents?

# Applications?

MIT MANAGEMENT SLOAN SCHOOL

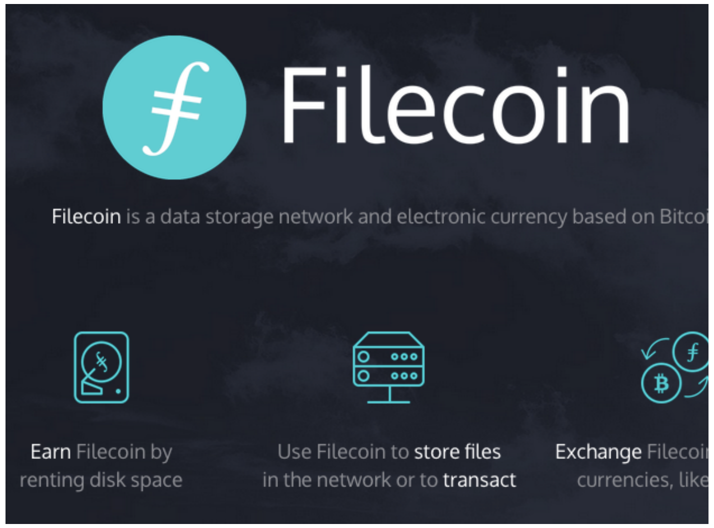
Fintech



# Here's The Thing With Ad Blockers

**We get it:** Ads aren't what you're here for. But ads help us keep the lights on. So, add us to your ad blocker's whitelist or pay $1 per week for an ad-free version of WIRED. Either way, you are supporting our journalism. We'd really appreciate it.

New Business Models



Filecoin

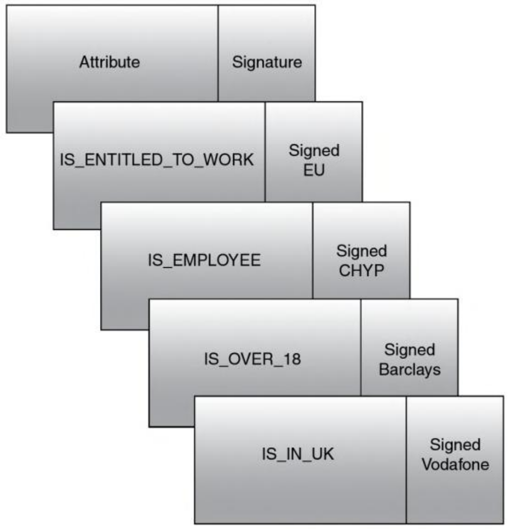
Filecoin is a data storage network and electronic currency based on Bitcoi

Earn Filecoin by renting disk space

Use Filecoin to store files in the network or to transact

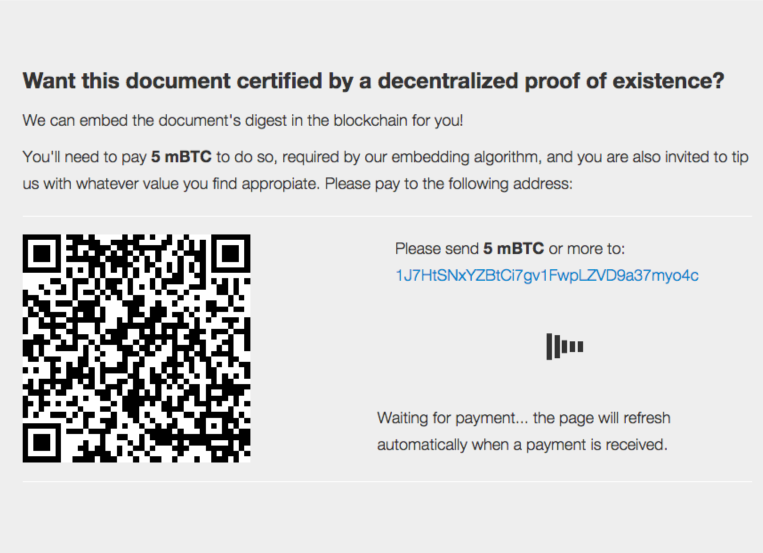
Exchange Filecoi currencies, like

New Types of Platforms



| Attribute | Signature |
|---|---|
| IS_ENTITLED_TO_WORK | Signed EU |
| IS_EMPLOYEE | Signed CHYP |
| IS_OVER_18 | Signed Barclays |
| IS_IN_UK | Signed Vodafone |

Identity & Privacy



**Want this document certified by a decentralized proof of existence?**

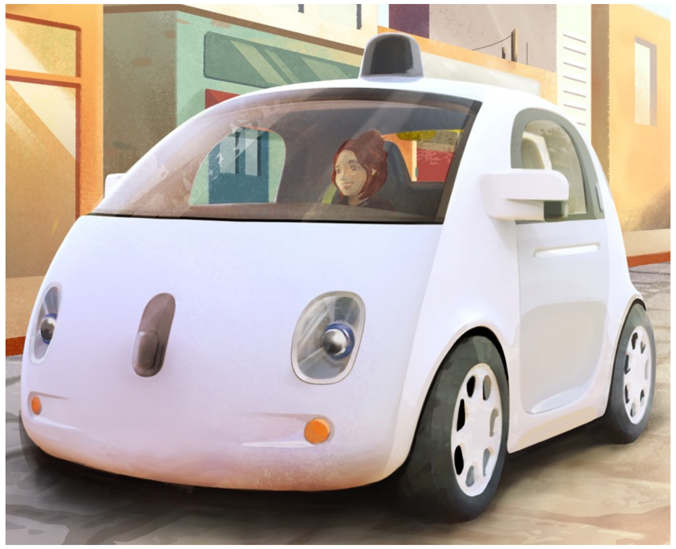
We can embed the document's digest in the blockchain for you!

You'll need to pay **5 mBTC** to do so, required by our embedding algorithm, and you are also invited to tip us with whatever value you find appropiate. Please pay to the following address:

Please send **5 mBTC** or more to:
1J7HtSNxYZBtCi7gv1FwpLZVD9a37myo4c

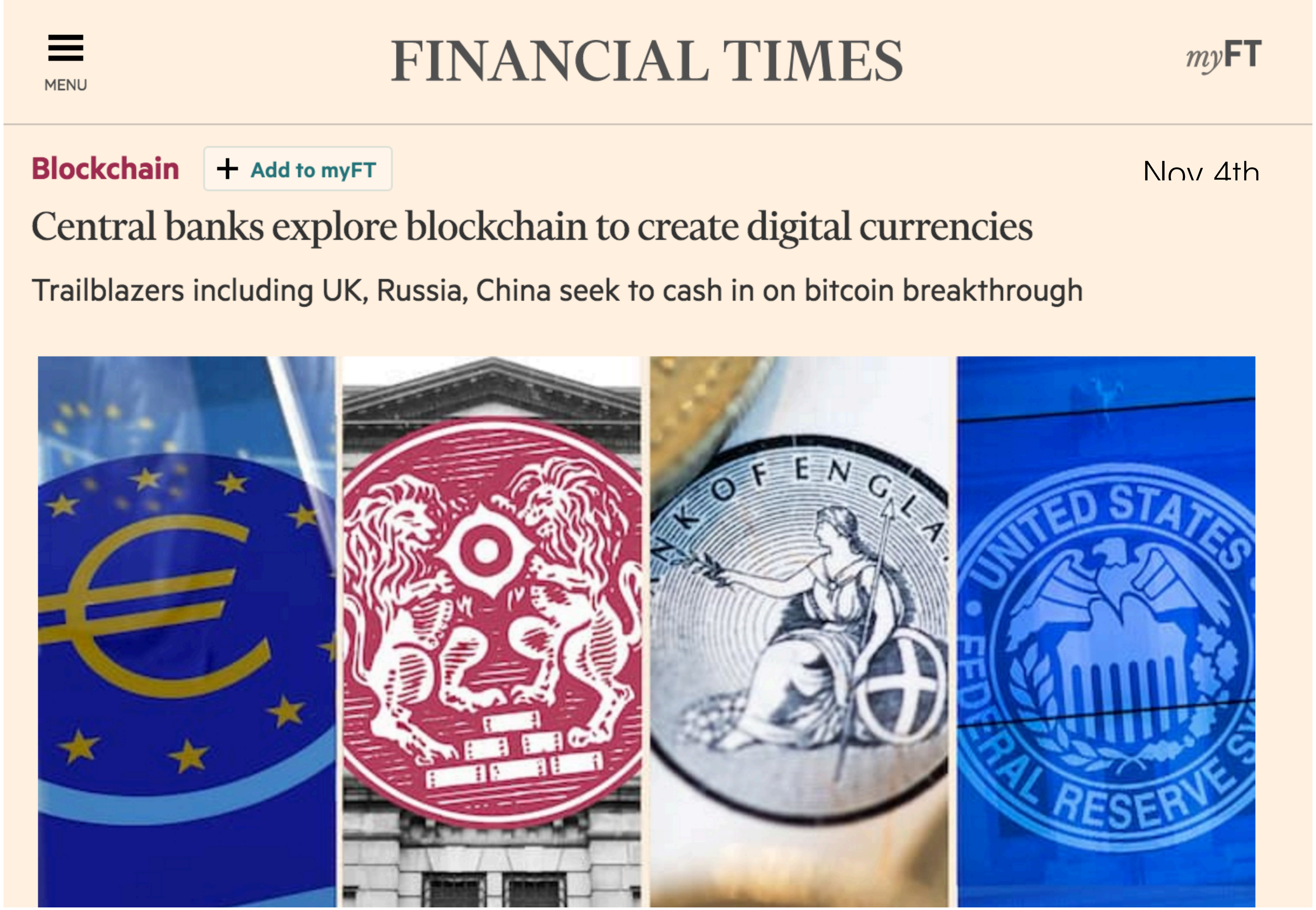
Waiting for payment... the page will refresh automatically when a payment is received.

IP & Smart Contracts



IoT, AI Robotics

# Central Banks



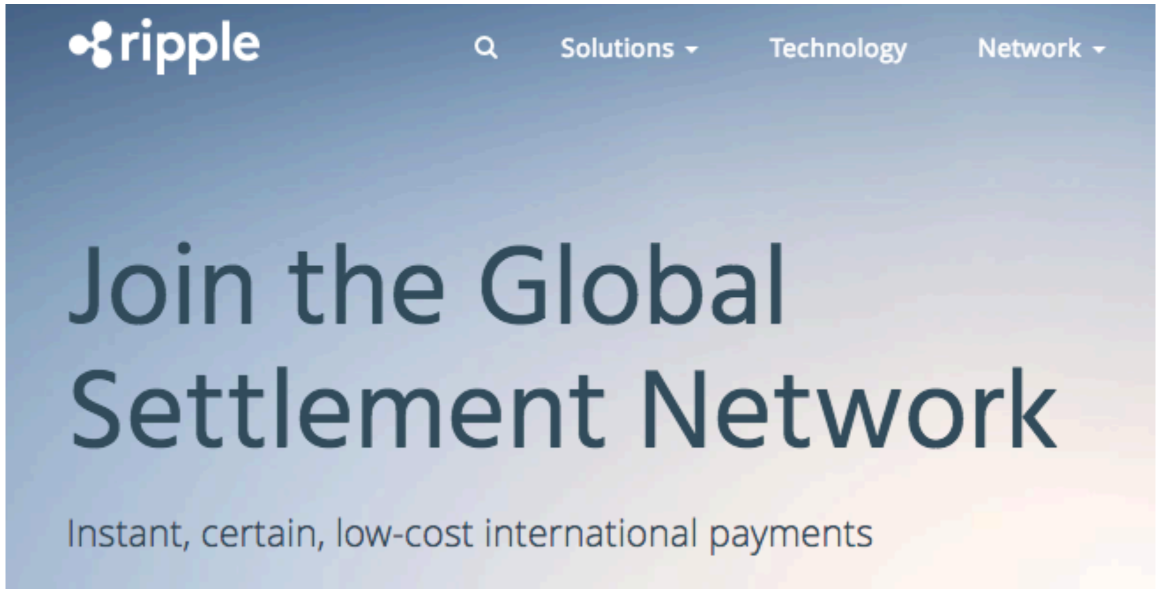
FINANCIAL TIMES

Nov 4th

## Central banks explore blockchain to create digital currencies

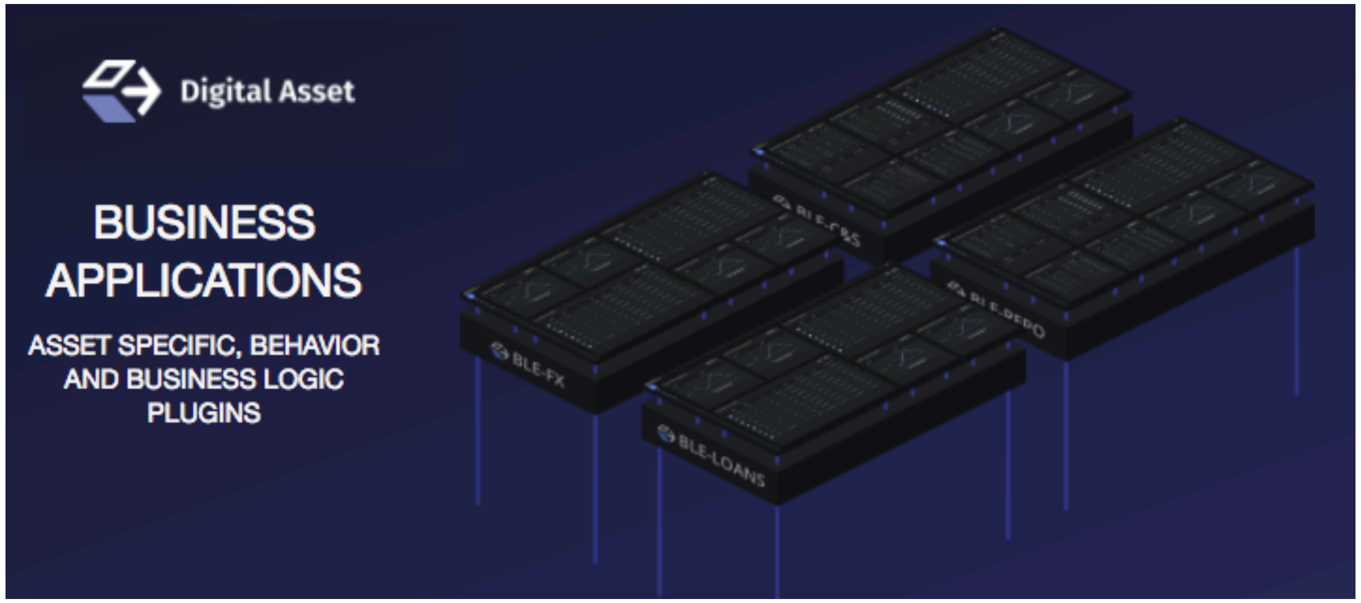
Trailblazers including UK, Russia, China seek to cash in on bitcoin breakthrough

# Finance



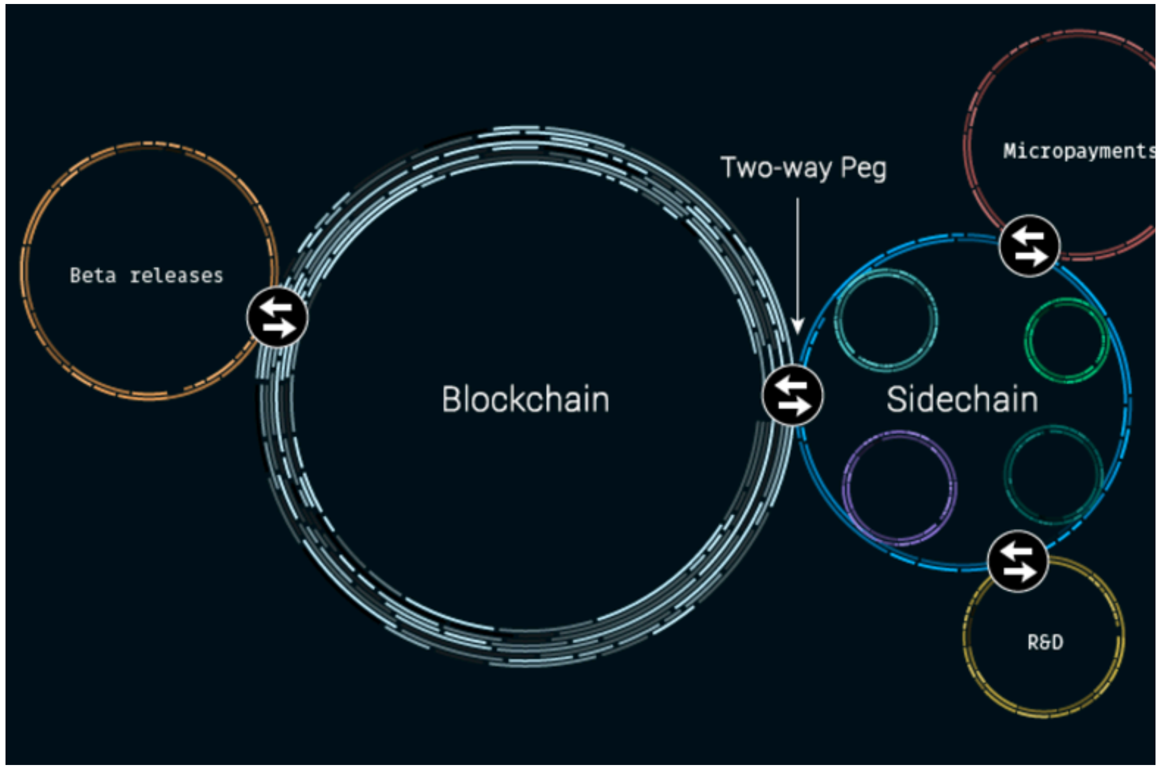
Join the Global Settlement Network

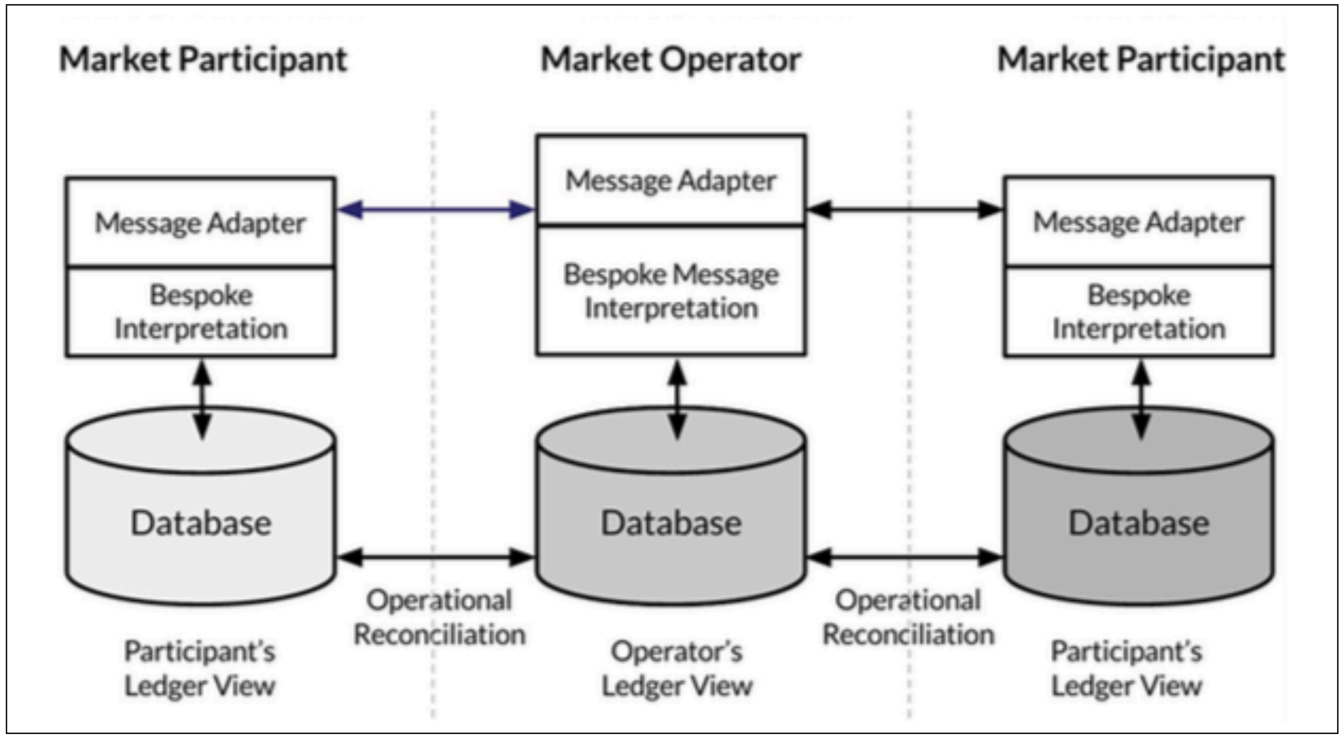
Instant, certain, low-cost international payments



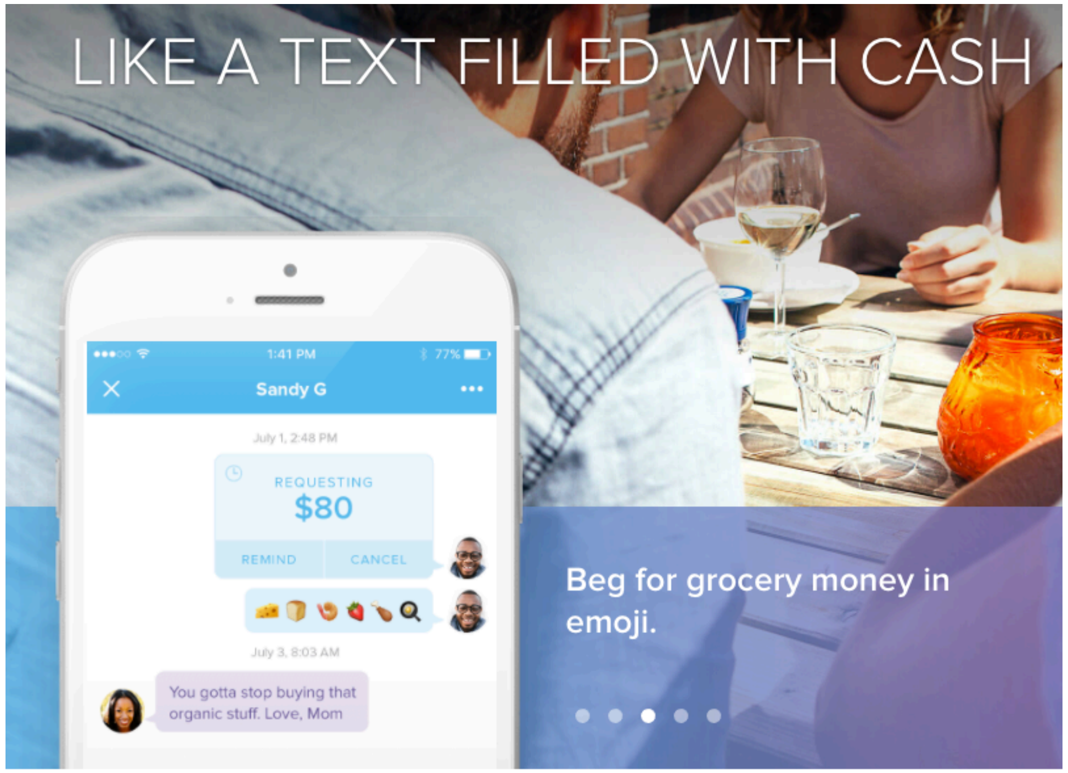
BUSINESS APPLICATIONS

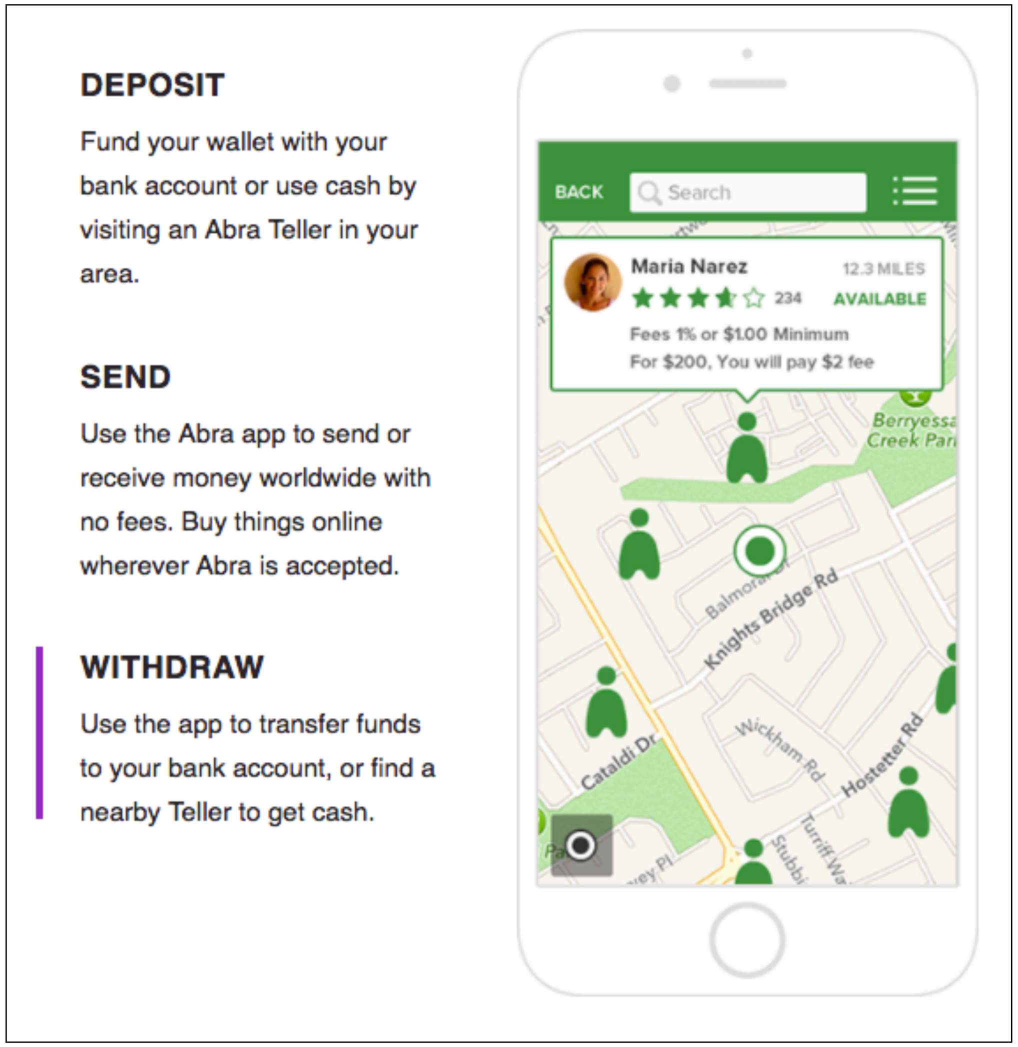
ASSET SPECIFIC, BEHAVIOR AND BUSINESS LOGIC PLUGINS





# Money Transfer


LIKE A TEXT FILLED WITH CASH
1:41 PM
Sandy G
July 1, 2:48 PM
REQUESTING
$80
REMIND
CANCEL
July 3, 8:03 AM
You gotta stop buying that organic stuff. Love, Mom
Beg for grocery money in emoji.



**DEPOSIT**

Fund your wallet with your bank account or use cash by visiting an Abra Teller in your area.

**SEND**

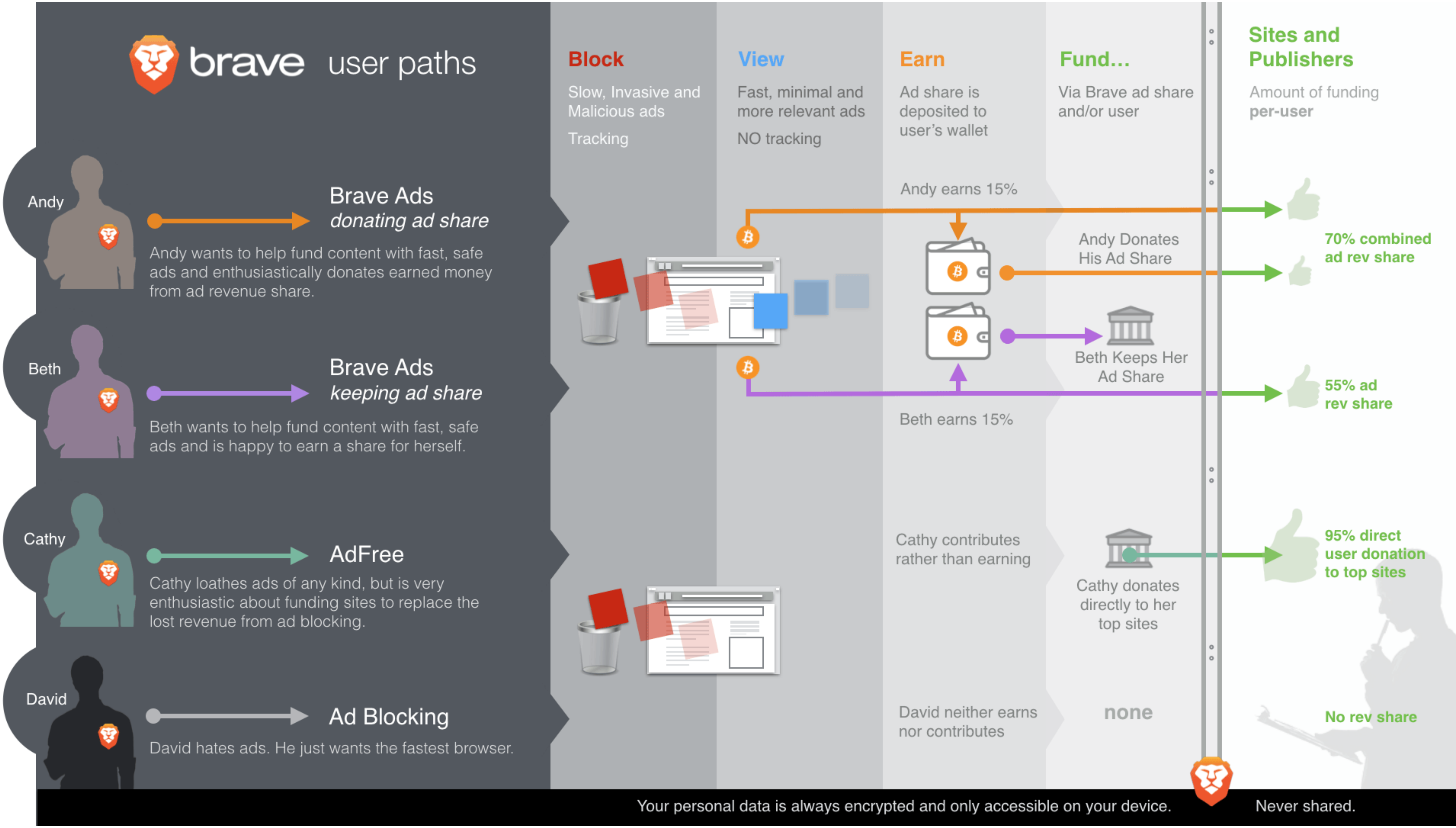
Use the Abra app to send or receive money worldwide with no fees. Buy things online wherever Abra is accepted.

**WITHDRAW**

Use the app to transfer funds to your bank account, or find a nearby Teller to get cash.

# Micropayments

MIT MANAGEMENT SLOAN SCHOOL



brave user paths

**Block**
Slow, Invasive and Malicious ads
Tracking

**View**
Fast, minimal and more relevant ads
NO tracking

**Earn**
Ad share is deposited to user's wallet

**Fund…**
Via Brave ad share and/or user

**Sites and Publishers**
Amount of funding **per-user**

Andy
**Brave Ads**
*donating ad share*
Andy wants to help fund content with fast, safe ads and enthusiastically donates earned money from ad revenue share.

Andy earns 15%

Andy Donates His Ad Share

**70% combined ad rev share**

Beth
**Brave Ads**
*keeping ad share*
Beth wants to help fund content with fast, safe ads and is happy to earn a share for herself.

Beth Keeps Her Ad Share

Beth earns 15%

**55% ad rev share**

Cathy
**AdFree**
Cathy loathes ads of any kind, but is very enthusiastic about funding sites to replace the lost revenue from ad blocking.

Cathy contributes rather than earning

Cathy donates directly to her top sites

**95% direct user donation to top sites**

David
**Ad Blocking**
David hates ads. He just wants the fastest browser.

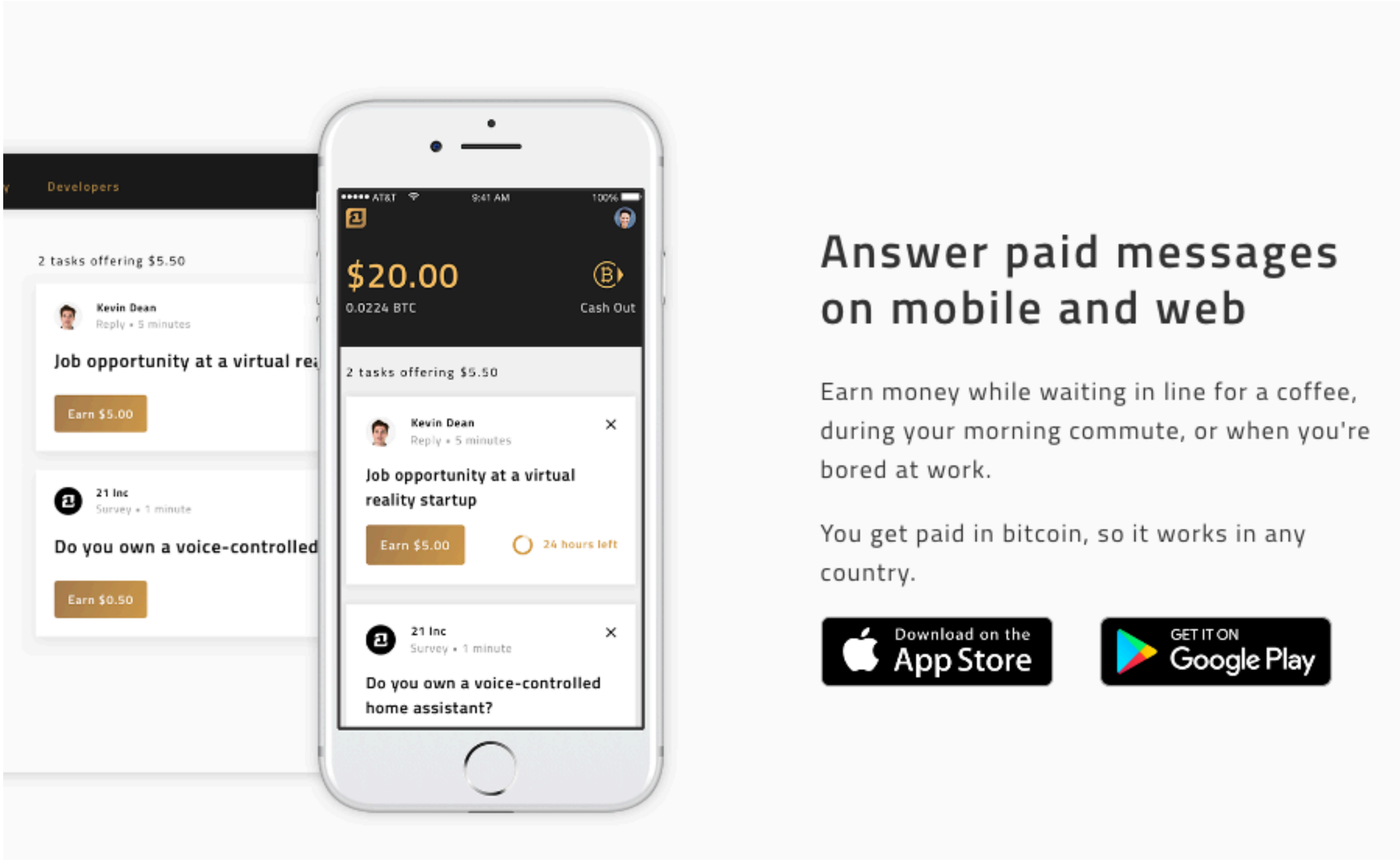
David neither earns nor contributes

none

**No rev share**

Your personal data is always encrypted and only accessible on your device. Never shared.

# Crowdsourcing



2 tasks offering $5.50

Kevin Dean
Reply • 5 minutes

Job opportunity at a virtual reality startup

21 Inc
Survey • 1 minute

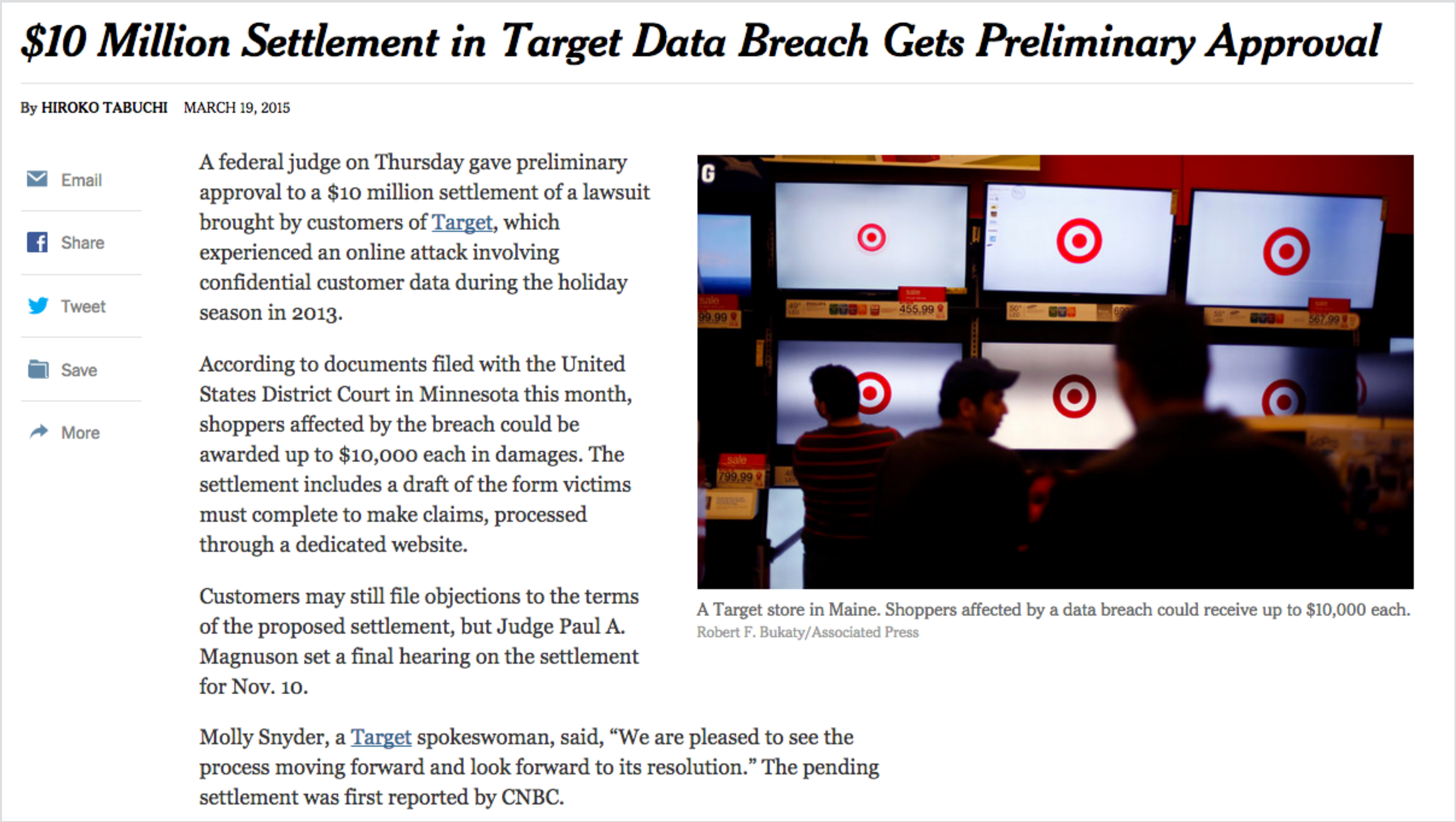
Do you own a voice-controlled home assistant?

## Answer paid messages on mobile and web

Earn money while waiting in line for a coffee, during your morning commute, or when you're bored at work.

You get paid in bitcoin, so it works in any country.

# Identity and Privacy



## $10 Million Settlement in Target Data Breach Gets Preliminary Approval

By HIROKO TABUCHI MARCH 19, 2015

Email
Share
Tweet
Save
More

A federal judge on Thursday gave preliminary approval to a $10 million settlement of a lawsuit brought by customers of Target, which experienced an online attack involving confidential customer data during the holiday season in 2013.

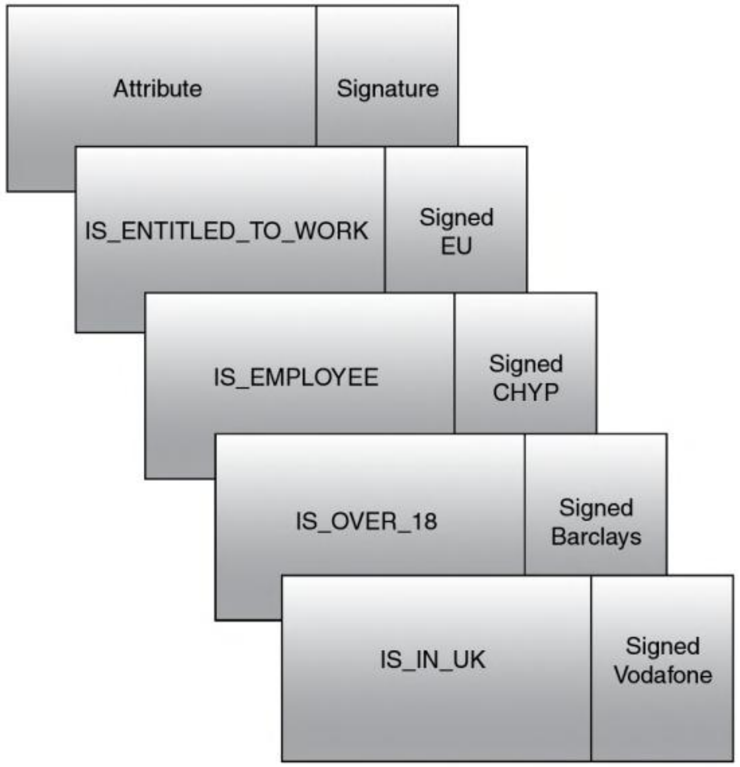
According to documents filed with the United States District Court in Minnesota this month, shoppers affected by the breach could be awarded up to $10,000 each in damages. The settlement includes a draft of the form victims must complete to make claims, processed through a dedicated website.

Customers may still file objections to the terms of the proposed settlement, but Judge Paul A. Magnuson set a final hearing on the settlement for Nov. 10.

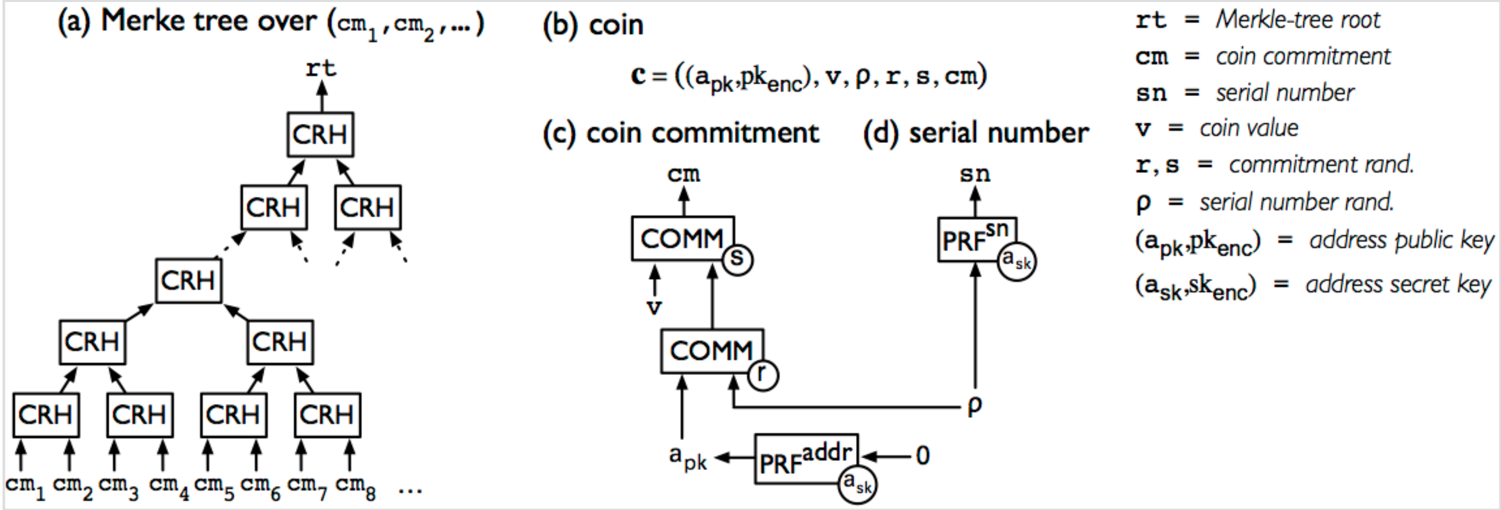
A Target store in Maine. Shoppers affected by a data breach could receive up to $10,000 each.
Robert F. Bukaty/Associated Press

Molly Snyder, a Target spokeswoman, said, “We are pleased to see the process moving forward and look forward to its resolution.” The pending settlement was first reported by CNBC.

ZCASH



| Attribute | Signature |
|---|---|
| IS_ENTITLED_TO_WORK | Signed EU |
| IS_EMPLOYEE | Signed CHYP |
| IS_OVER_18 | Signed Barclays |
| IS_IN_UK | Signed Vodafone |

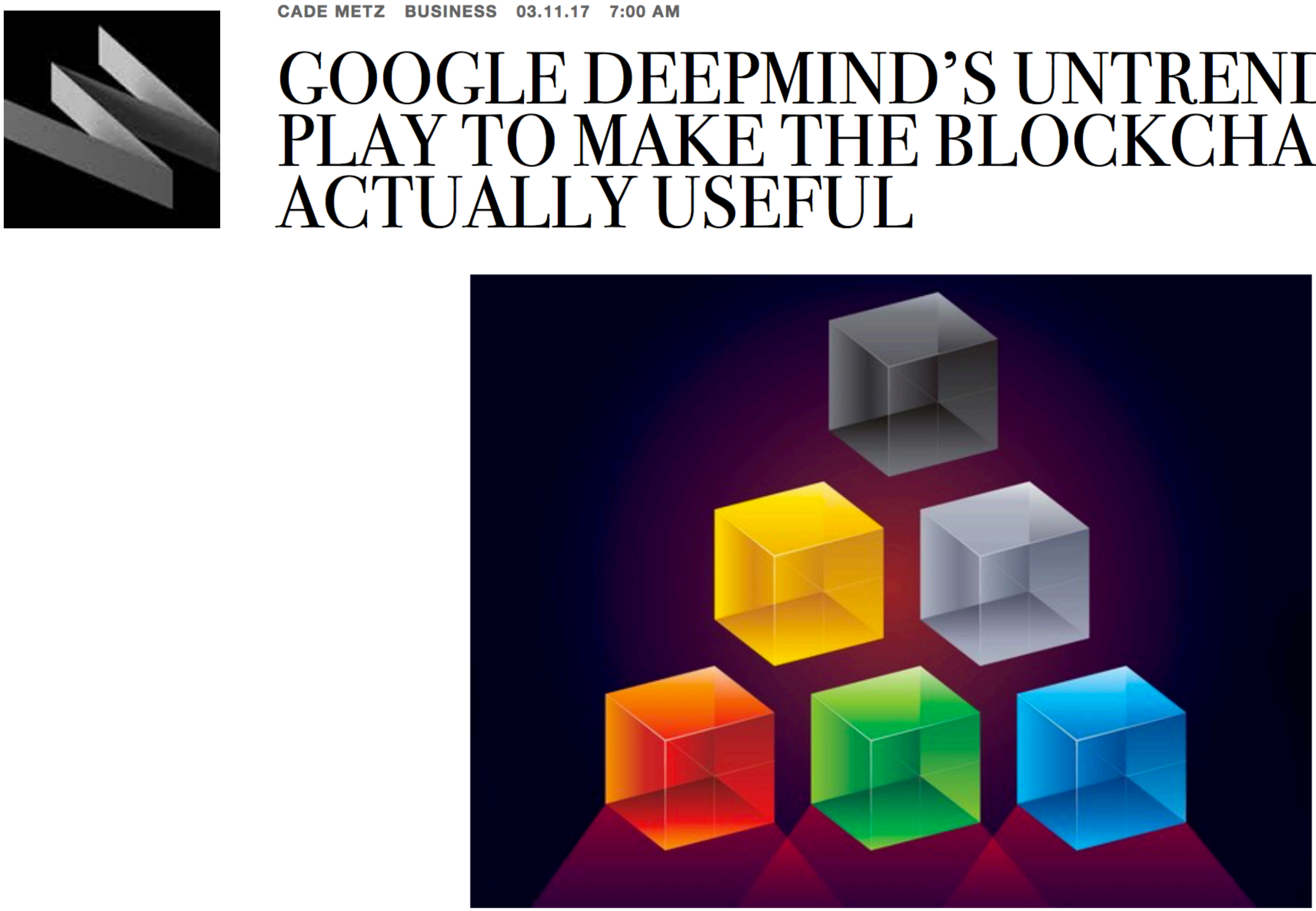


(a) Merke tree over ($\mathtt{cm}_1, \mathtt{cm}_2, \ldots$)
rt
CRH
$\mathtt{cm}_1$ $\mathtt{cm}_2$ $\mathtt{cm}_3$ $\mathtt{cm}_4$ $\mathtt{cm}_5$ $\mathtt{cm}_6$ $\mathtt{cm}_7$ $\mathtt{cm}_8$ …
(b) coin
$\mathbf{c} = ((a_{pk}, pk_{enc}), \mathtt{v}, \rho, \mathtt{r}, \mathtt{s}, \mathtt{cm})$
(c) coin commitment
(d) serial number
cm
COMM
s
v
COMM
r
$a_{pk}$
$\mathrm{PRF}^{addr}$
$a_{sk}$
0
sn
$\mathrm{PRF}^{sn}$
$a_{sk}$
$\rho$

$\mathtt{rt}$ = *Merkle-tree root*
$\mathtt{cm}$ = *coin commitment*
$\mathtt{sn}$ = *serial number*
$\mathtt{v}$ = *coin value*
$\mathtt{r}, \mathtt{s}$ = *commitment rand.*
$\rho$ = *serial number rand.*
$(a_{pk}, pk_{enc})$ = *address public key*
$(a_{sk}, sk_{enc})$ = *address secret key*

MIT MANAGEMENT SLOAN SCHOOL

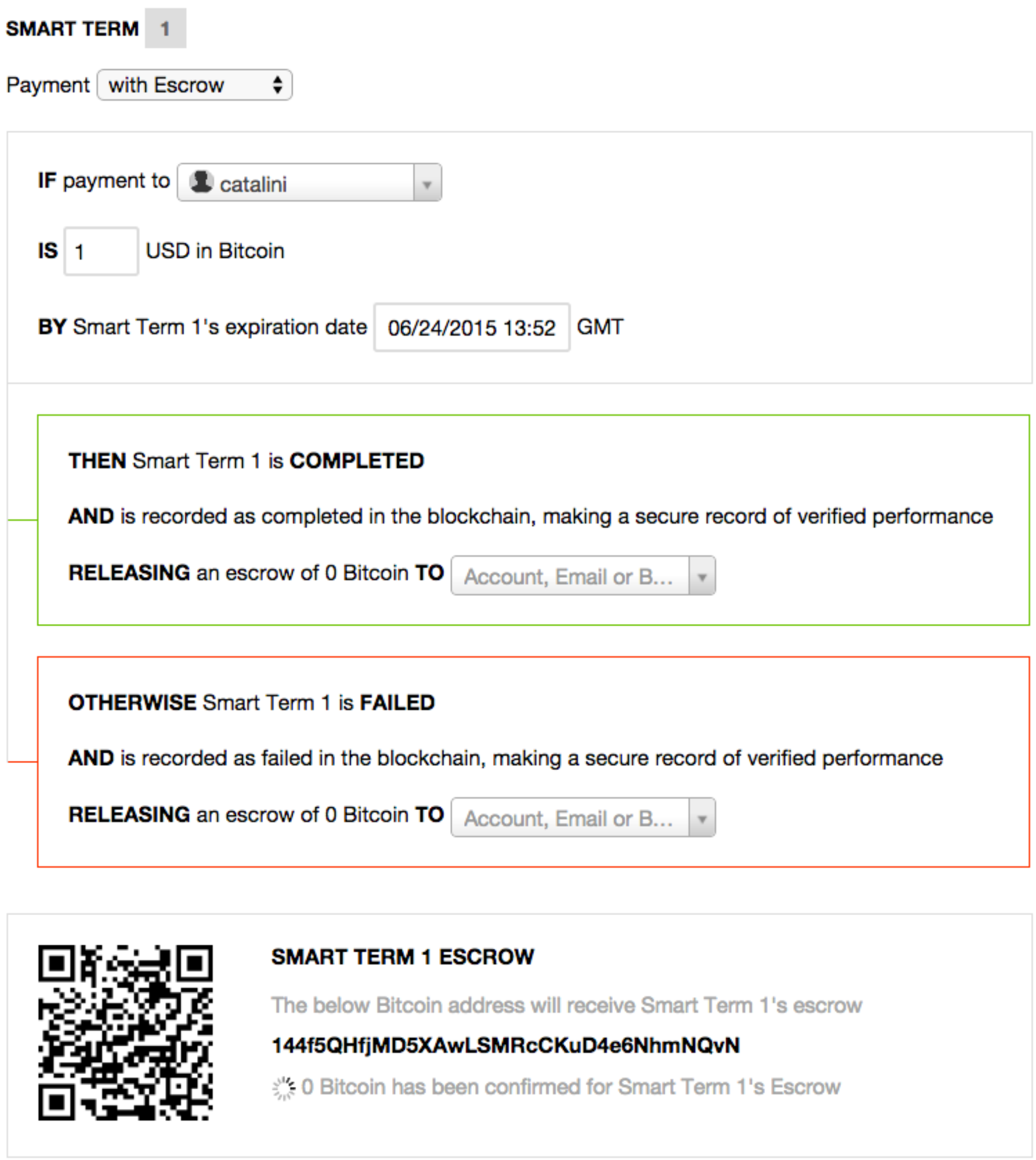
# How Costless Verification Allows for Data Integrity and Privacy



CADE METZ BUSINESS 03.11.17 7:00 AM

GOOGLE DEEPMIND'S UNTRENDY PLAY TO MAKE THE BLOCKCHAIN ACTUALLY USEFUL

# Smart Contracts



**SMART TERM** 1

Payment with Escrow

**IF** payment to catalini

**IS** 1 USD in Bitcoin

**BY** Smart Term 1's expiration date 06/24/2015 13:52 GMT

**THEN** Smart Term 1 is **COMPLETED**

**AND** is recorded as completed in the blockchain, making a secure record of verified performance

**RELEASING** an escrow of 0 Bitcoin **TO** Account, Email or B...

**OTHERWISE** Smart Term 1 is **FAILED**

**AND** is recorded as failed in the blockchain, making a secure record of verified performance

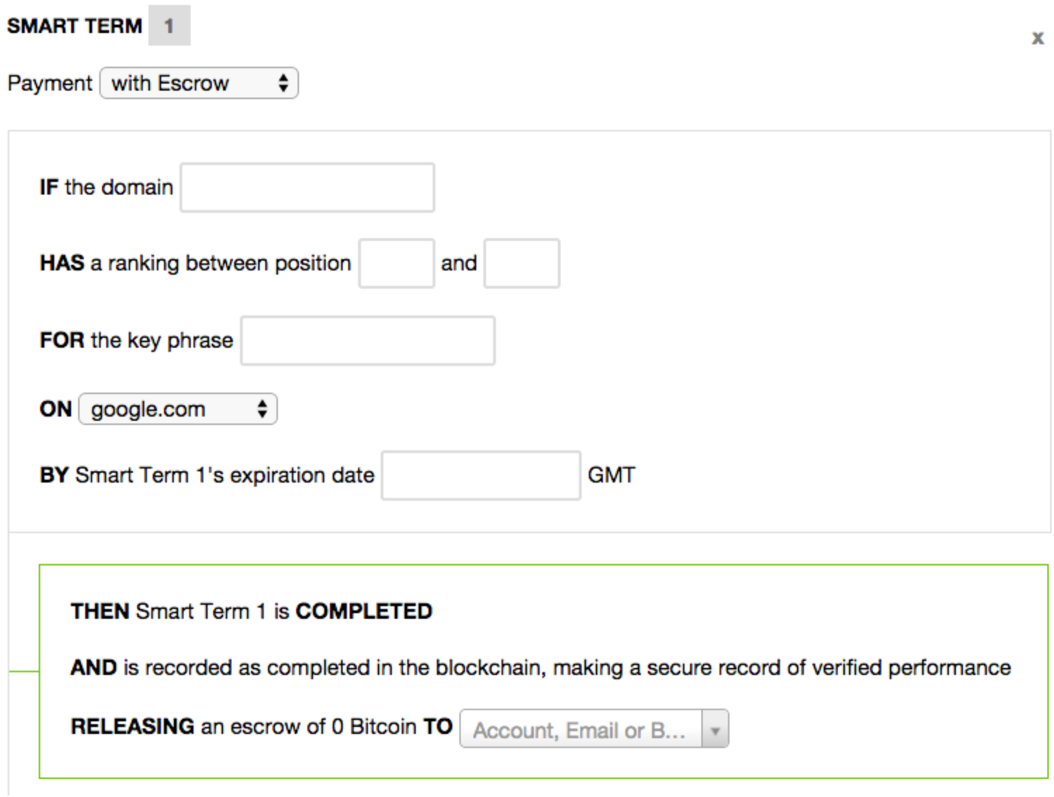
**RELEASING** an escrow of 0 Bitcoin **TO** Account, Email or B...

**SMART TERM 1 ESCROW**

The below Bitcoin address will receive Smart Term 1's escrow

**144f5QHfjMD5XAwLSMRcCKuD4e6NhmNQvN**

0 Bitcoin has been confirmed for Smart Term 1's Escrow



**SMART TERM** 1

x

Payment with Escrow

**IF** the domain

**HAS** a ranking between position and

**FOR** the key phrase

**ON** google.com

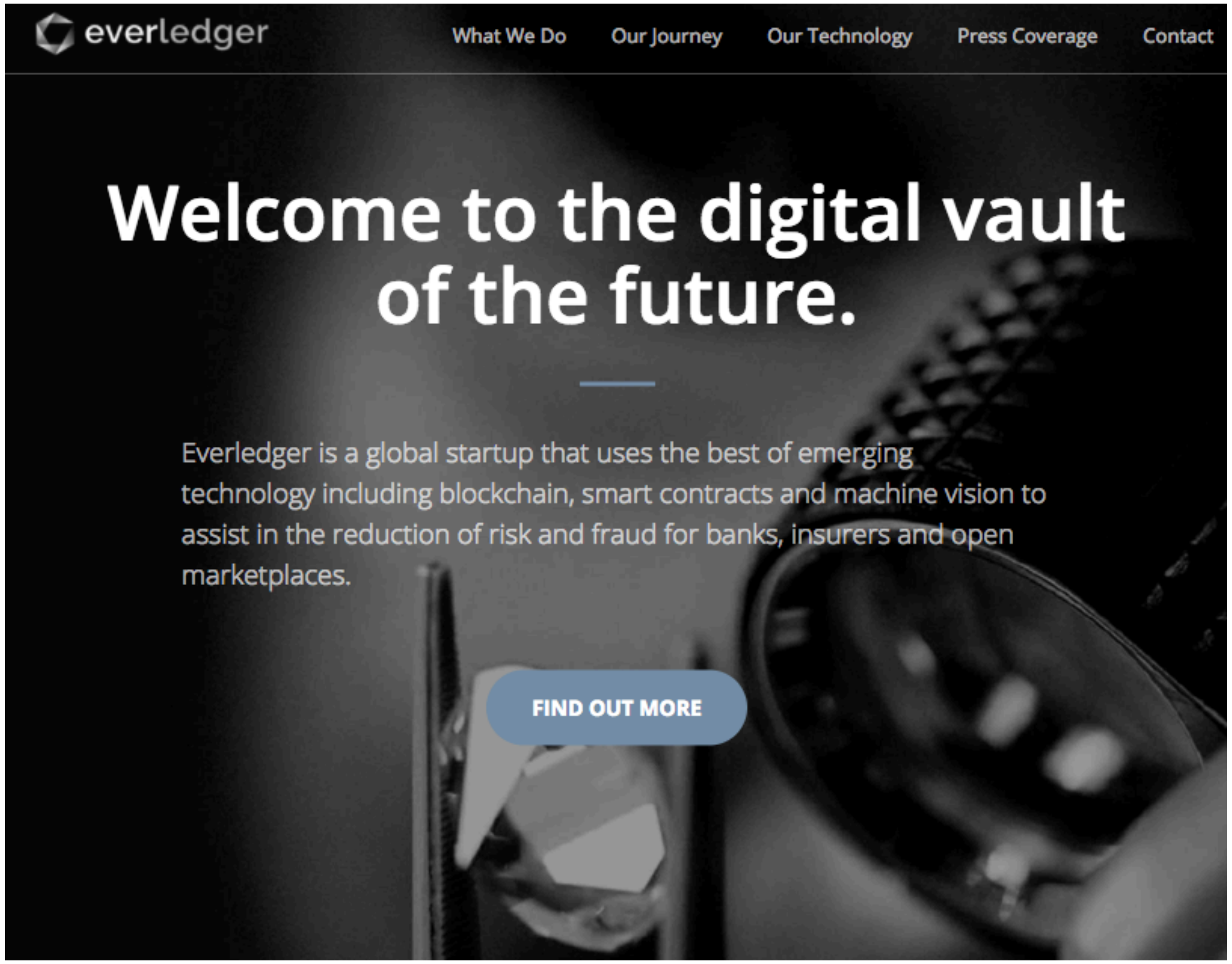
**BY** Smart Term 1's expiration date GMT

**THEN** Smart Term 1 is **COMPLETED**

**AND** is recorded as completed in the blockchain, making a secure record of verified performance

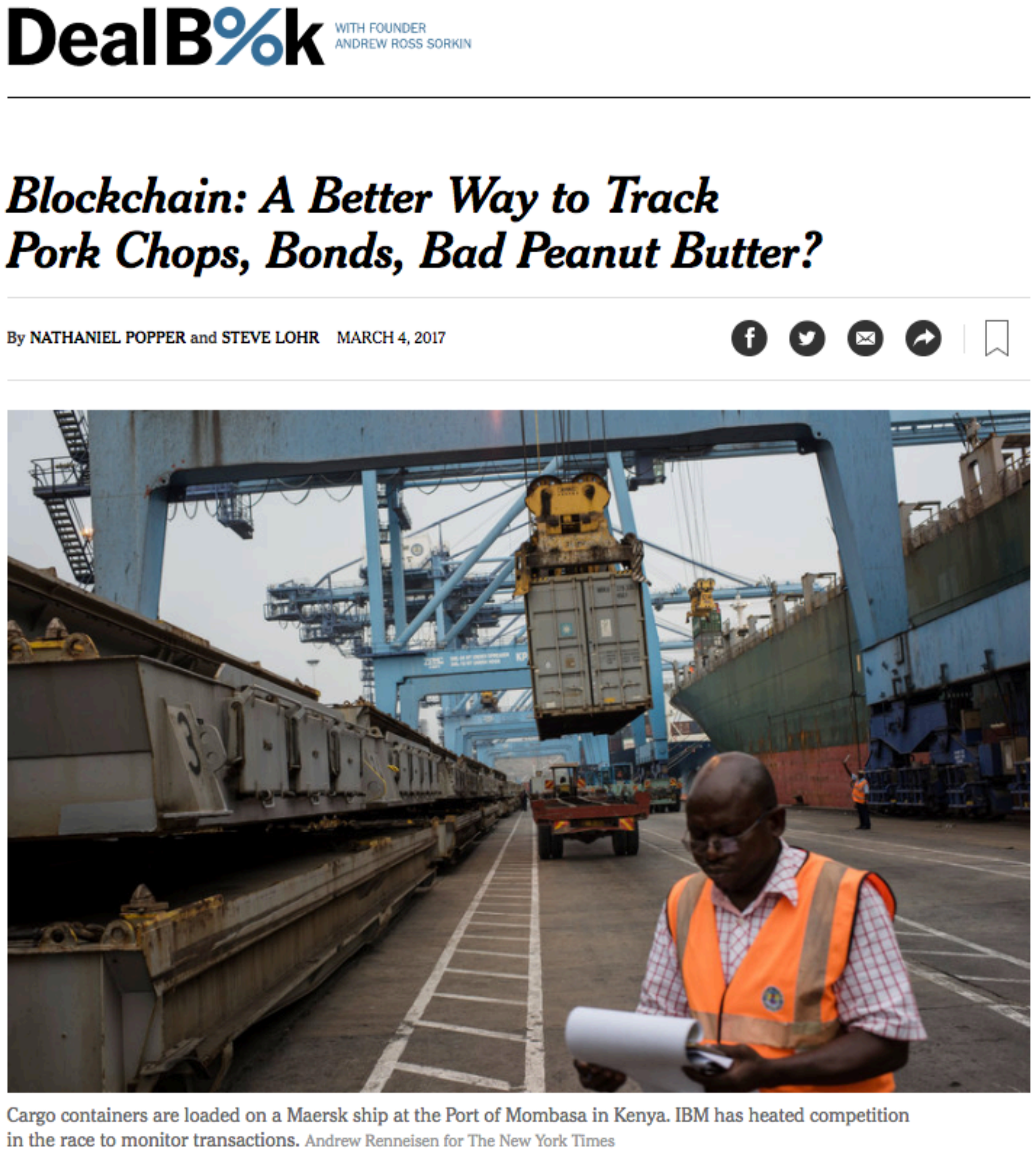
**RELEASING** an escrow of 0 Bitcoin **TO** Account, Email or B...

# Provenance



Welcome to the digital vault of the future.

Everledger is a global startup that uses the best of emerging technology including blockchain, smart contracts and machine vision to assist in the reduction of risk and fraud for banks, insurers and open marketplaces.



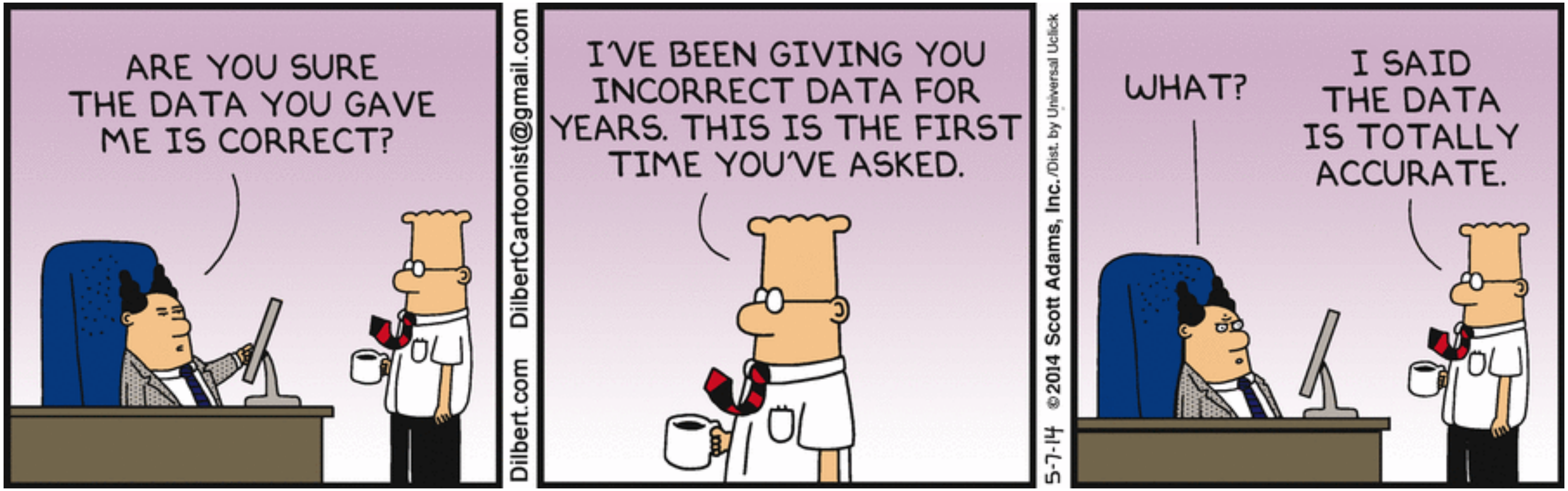
DealB%k WITH FOUNDER ANDREW ROSS SORKIN

*Blockchain: A Better Way to Track Pork Chops, Bonds, Bad Peanut Butter?*

By NATHANIEL POPPER and STEVE LOHR MARCH 4, 2017

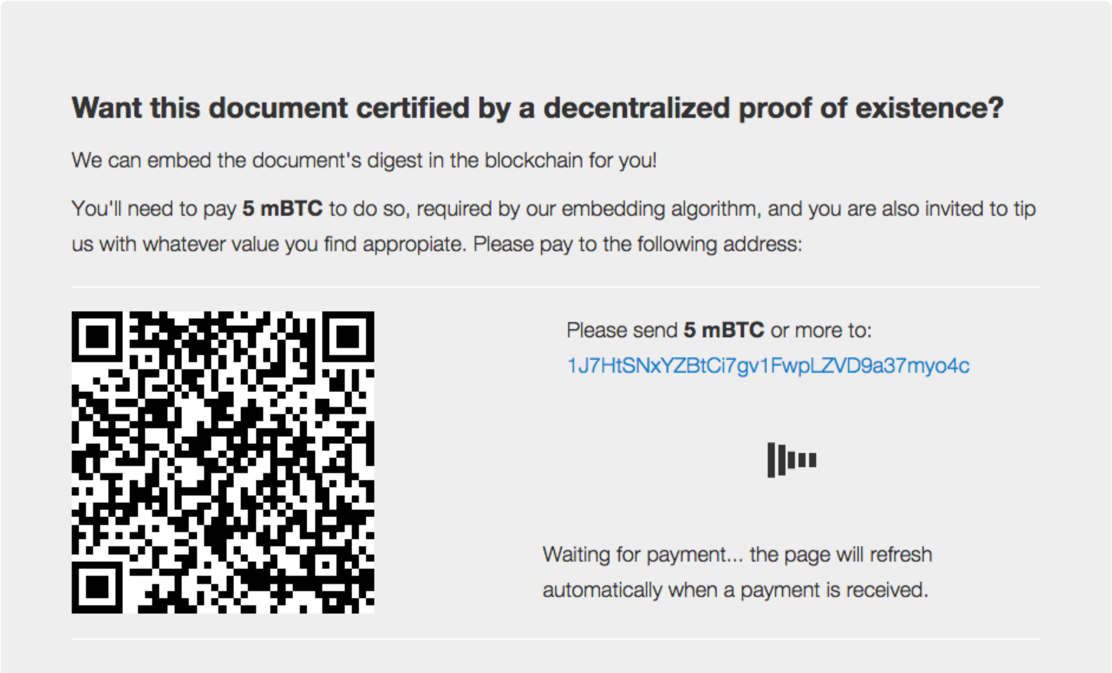
Cargo containers are loaded on a Maersk ship at the Port of Mombasa in Kenya. IBM has heated competition in the race to monitor transactions. Andrew Renneisen for The New York Times

# Provenance


ARE YOU SURE THE DATA YOU GAVE ME IS CORRECT?
Dilbert.com DilbertCartoonist@gmail.com
I'VE BEEN GIVING YOU INCORRECT DATA FOR YEARS. THIS IS THE FIRST TIME YOU'VE ASKED.
5-7-14 ©2014 Scott Adams, Inc./Dist. by Universal Uclick
WHAT?
I SAID THE DATA IS TOTALLY ACCURATE.

The immutability offered by a blockchain is only useful if the original information entered on it is accurate!

# Intellectual Property and Digital Rights Management



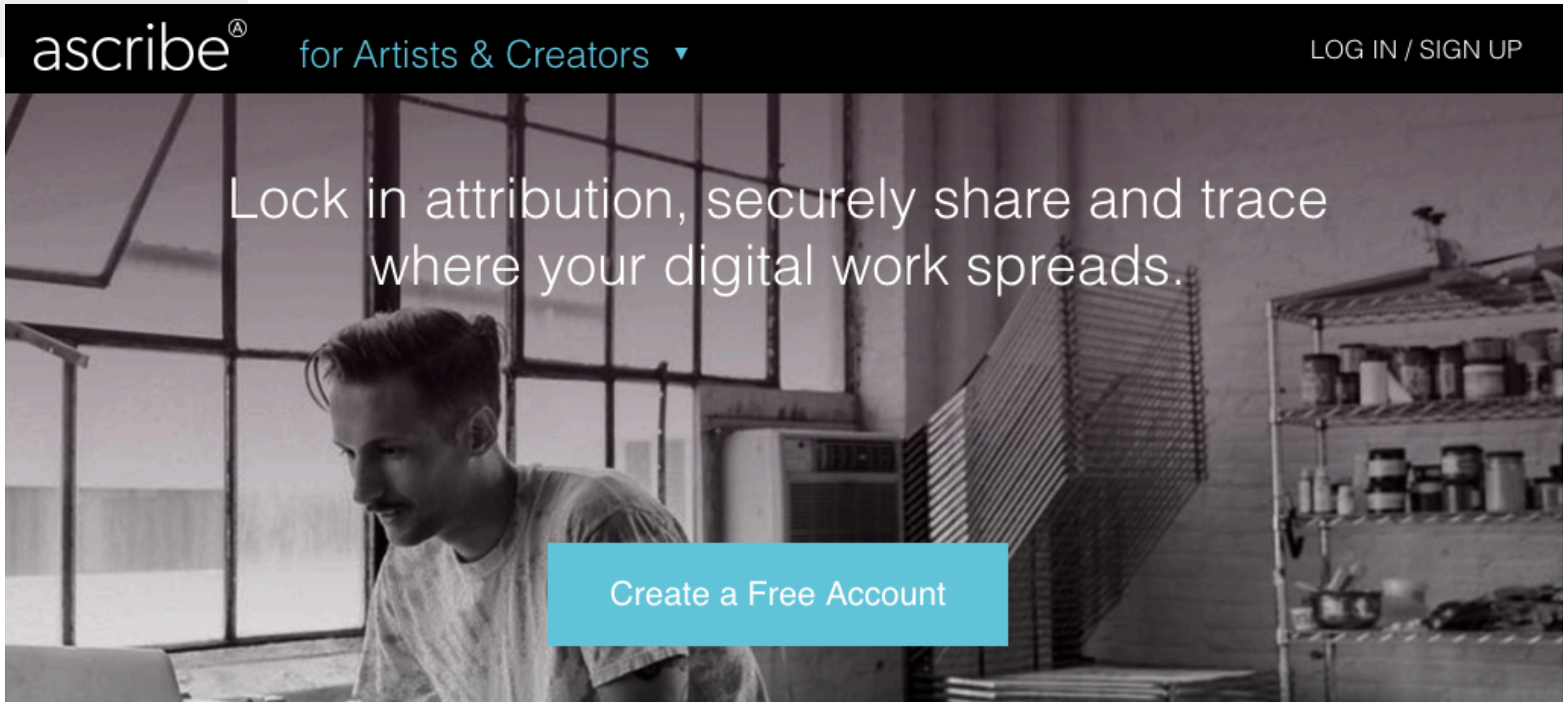
**Want this document certified by a decentralized proof of existence?**

We can embed the document's digest in the blockchain for you!

You'll need to pay **5 mBTC** to do so, required by our embedding algorithm, and you are also invited to tip us with whatever value you find appropiate. Please pay to the following address:

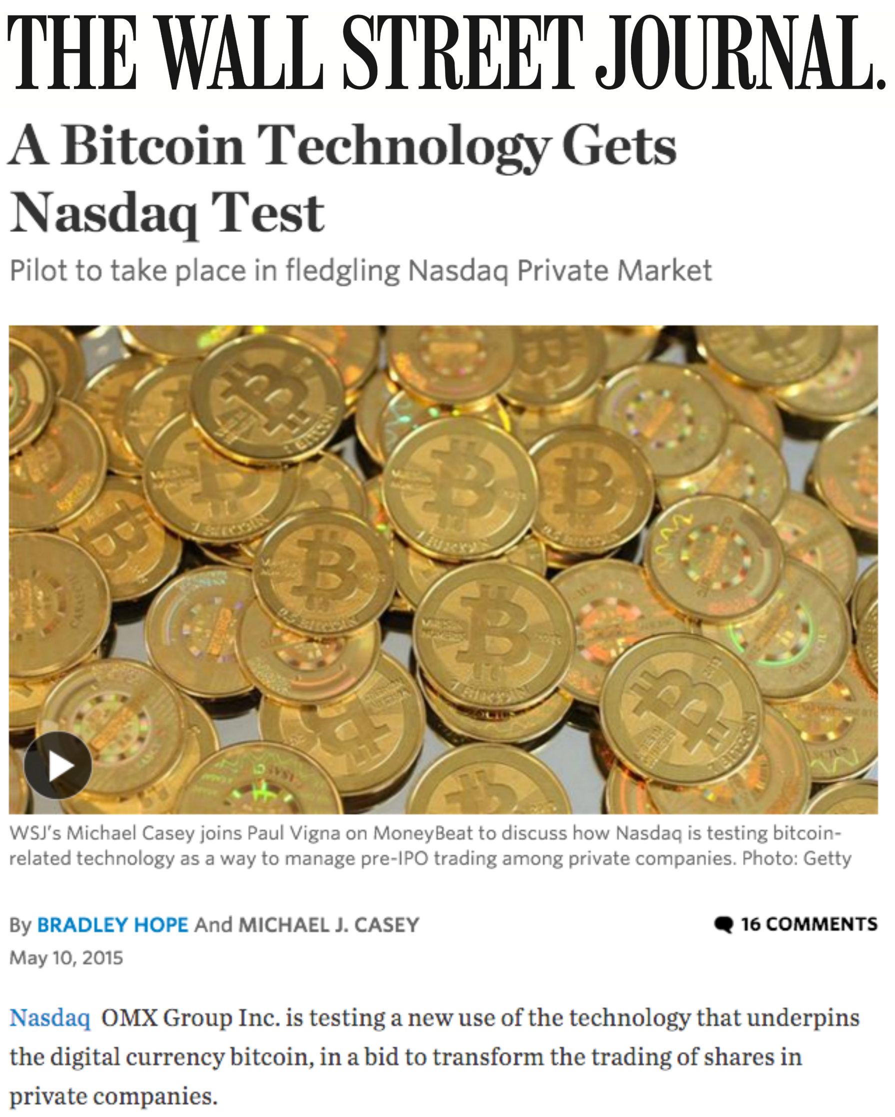
Please send **5 mBTC** or more to:
1J7HtSNxYZBtCi7gv1FwpLZVD9a37myo4c

Waiting for payment... the page will refresh automatically when a payment is received.



ascribe®
for Artists & Creators ▾
LOG IN / SIGN UP
Lock in attribution, securely share and trace where your digital work spreads.
Create a Free Account

MIT MANAGEMENT SLOAN SCHOOL



THE WALL STREET JOURNAL.

## A Bitcoin Technology Gets Nasdaq Test

Pilot to take place in fledgling Nasdaq Private Market

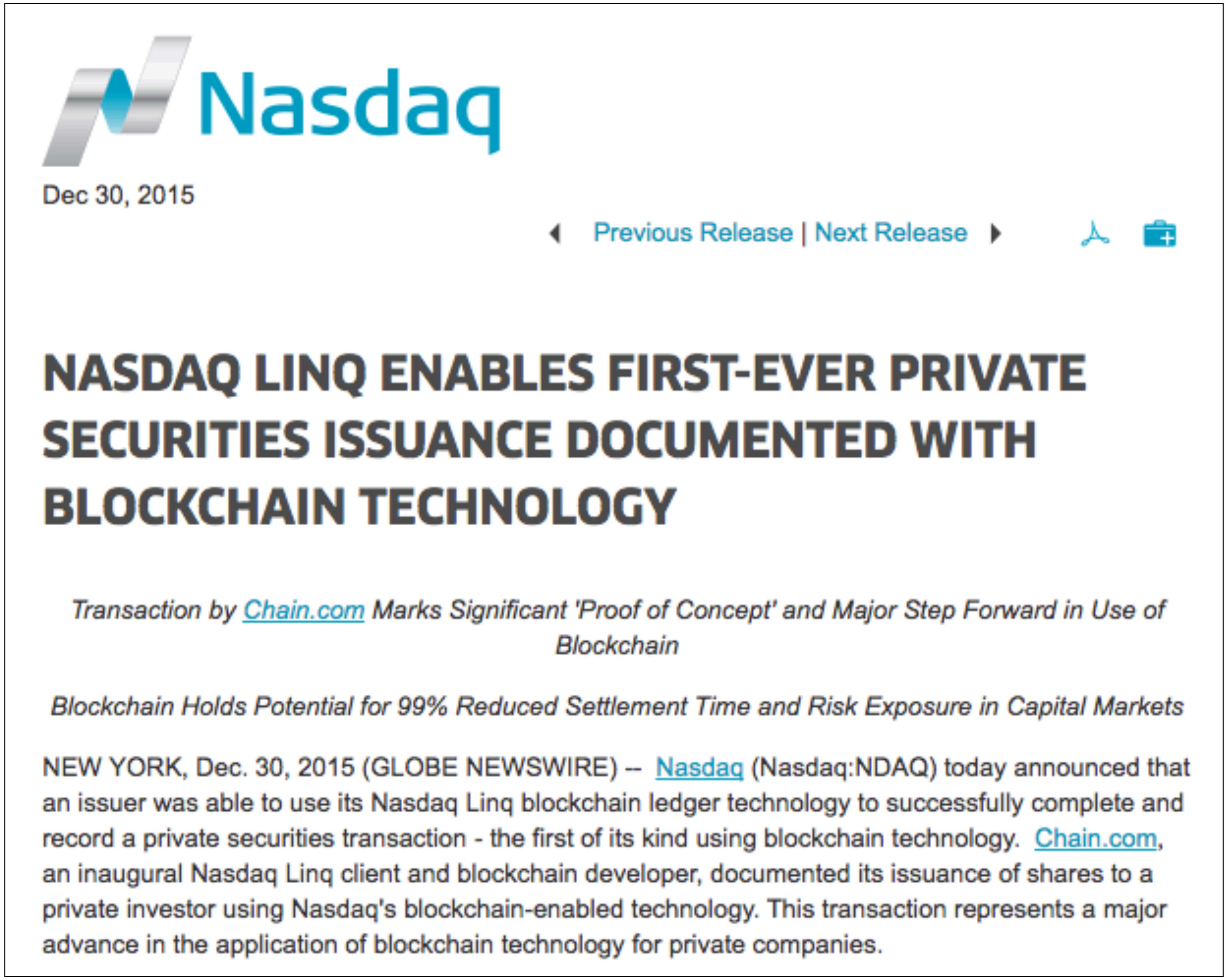
WSJ's Michael Casey joins Paul Vigna on MoneyBeat to discuss how Nasdaq is testing bitcoin-related technology as a way to manage pre-IPO trading among private companies. Photo: Getty

By BRADLEY HOPE And MICHAEL J. CASEY

16 COMMENTS

May 10, 2015

Nasdaq OMX Group Inc. is testing a new use of the technology that underpins the digital currency bitcoin, in a bid to transform the trading of shares in private companies.



Nasdaq

Dec 30, 2015

## NASDAQ LINQ ENABLES FIRST-EVER PRIVATE SECURITIES ISSUANCE DOCUMENTED WITH BLOCKCHAIN TECHNOLOGY

*Transaction by Chain.com Marks Significant 'Proof of Concept' and Major Step Forward in Use of Blockchain*

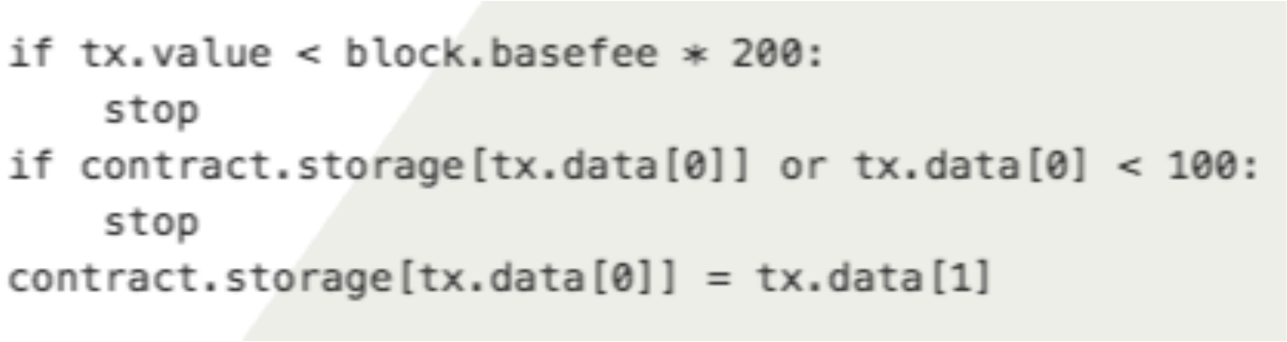
*Blockchain Holds Potential for 99% Reduced Settlement Time and Risk Exposure in Capital Markets*

NEW YORK, Dec. 30, 2015 (GLOBE NEWSWIRE) -- Nasdaq (Nasdaq:NDAQ) today announced that an issuer was able to use its Nasdaq Linq blockchain ledger technology to successfully complete and record a private securities transaction - the first of its kind using blockchain technology. Chain.com, an inaugural Nasdaq Linq client and blockchain developer, documented its issuance of shares to a private investor using Nasdaq's blockchain-enabled technology. This transaction represents a major advance in the application of blockchain technology for private companies.

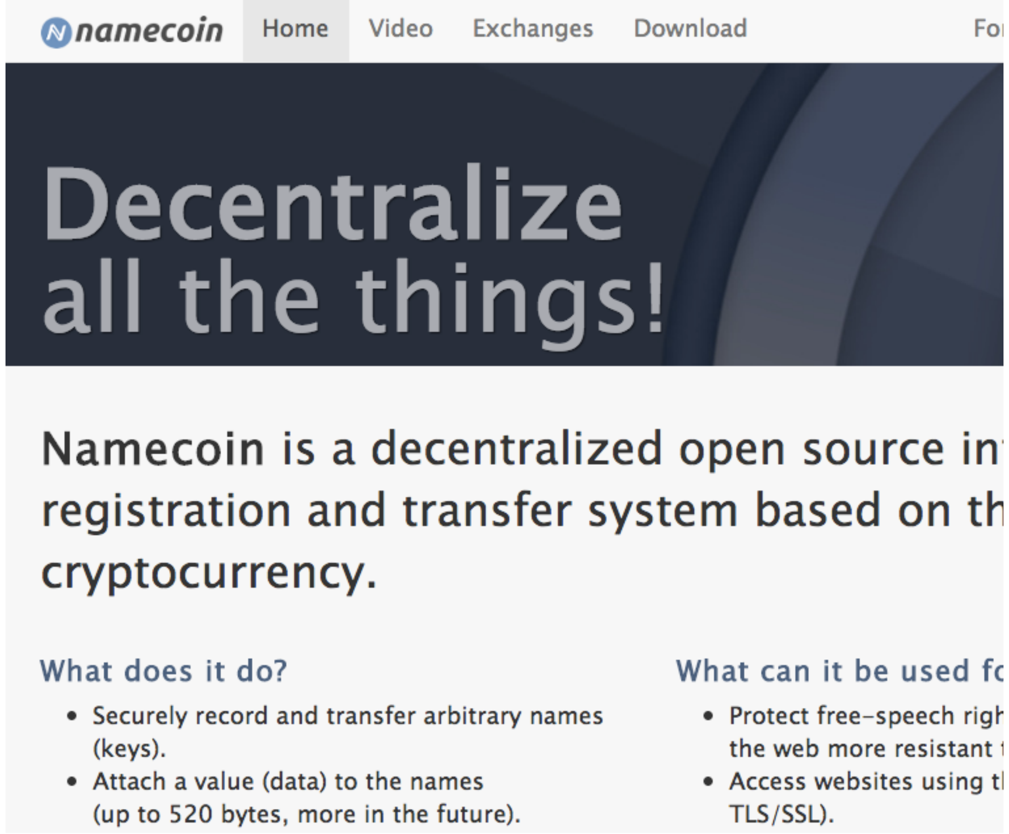
# From Digital Assets…

ICANN

network solutions



```
if tx.value < block.basefee * 200:
    stop
if contract.storage[tx.data[0]] or tx.data[0] < 100:
    stop
contract.storage[tx.data[0]] = tx.data[1]
```



Decentralize all the things!

Namecoin is a decentralized open source in registration and transfer system based on th cryptocurrency.

What does it do?

- Securely record and transfer arbitrary names (keys).
- Attach a value (data) to the names (up to 520 bytes, more in the future).

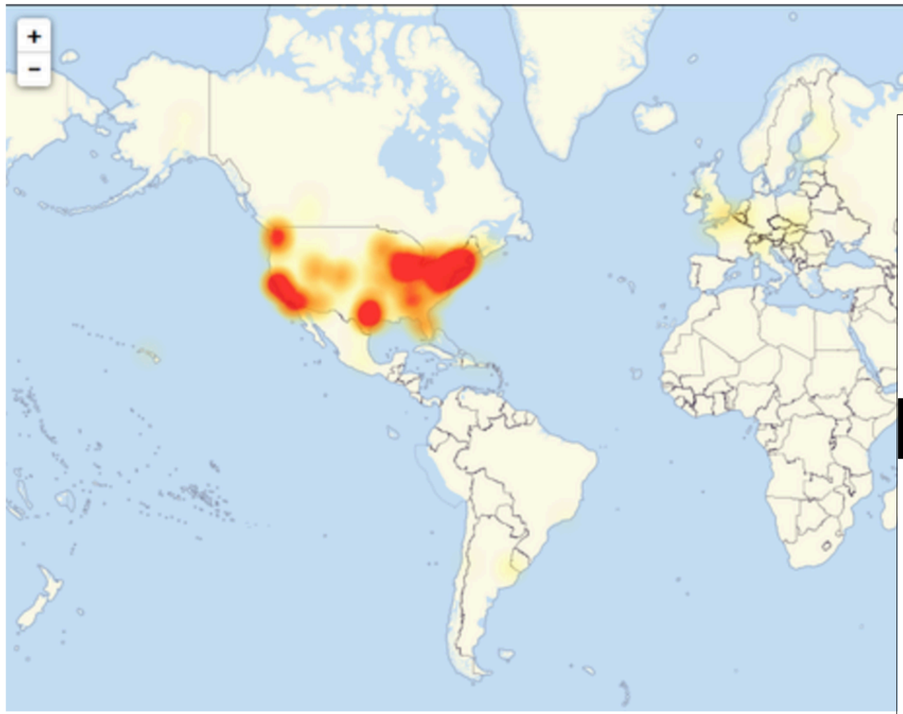
What can it be used fo

- Protect free-speech righ the web more resistant
- Access websites using t TLS/SSL).

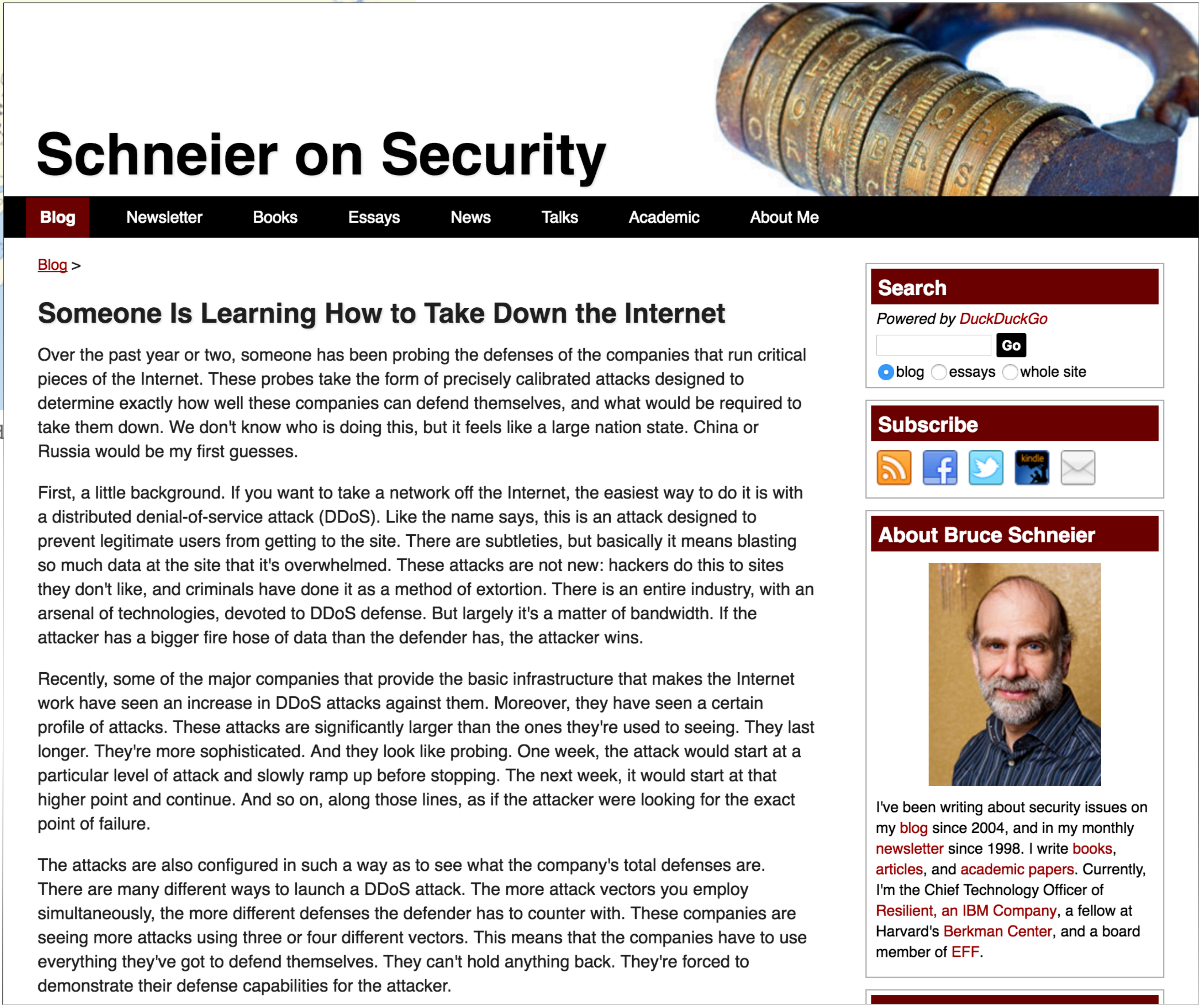
TECHNOLOGY

# *Internet Attack Disrupts Major Websites*

By NICOLE PERLROTH OCT. 21, 2016



A map of the areas experiencing problems, as of Friday afternoon, accord



Blog >

## Someone Is Learning How to Take Down the Internet

Over the past year or two, someone has been probing the defenses of the companies that run critical pieces of the Internet. These probes take the form of precisely calibrated attacks designed to determine exactly how well these companies can defend themselves, and what would be required to take them down. We don't know who is doing this, but it feels like a large nation state. China or Russia would be my first guesses.

First, a little background. If you want to take a network off the Internet, the easiest way to do it is with a distributed denial-of-service attack (DDoS). Like the name says, this is an attack designed to prevent legitimate users from getting to the site. There are subtleties, but basically it means blasting so much data at the site that it's overwhelmed. These attacks are not new: hackers do this to sites they don't like, and criminals have done it as a method of extortion. There is an entire industry, with an arsenal of technologies, devoted to DDoS defense. But largely it's a matter of bandwidth. If the attacker has a bigger fire hose of data than the defender has, the attacker wins.

Recently, some of the major companies that provide the basic infrastructure that makes the Internet work have seen an increase in DDoS attacks against them. Moreover, they have seen a certain profile of attacks. These attacks are significantly larger than the ones they're used to seeing. They last longer. They're more sophisticated. And they look like probing. One week, the attack would start at a particular level of attack and slowly ramp up before stopping. The next week, it would start at that higher point and continue. And so on, along those lines, as if the attacker were looking for the exact point of failure.

The attacks are also configured in such a way as to see what the company's total defenses are. There are many different ways to launch a DDoS attack. The more attack vectors you employ simultaneously, the more different defenses the defender has to counter with. These companies are seeing more attacks using three or four different vectors. This means that the companies have to use everything they've got to defend themselves. They can't hold anything back. They're forced to demonstrate their defense capabilities for the attacker.

### Search

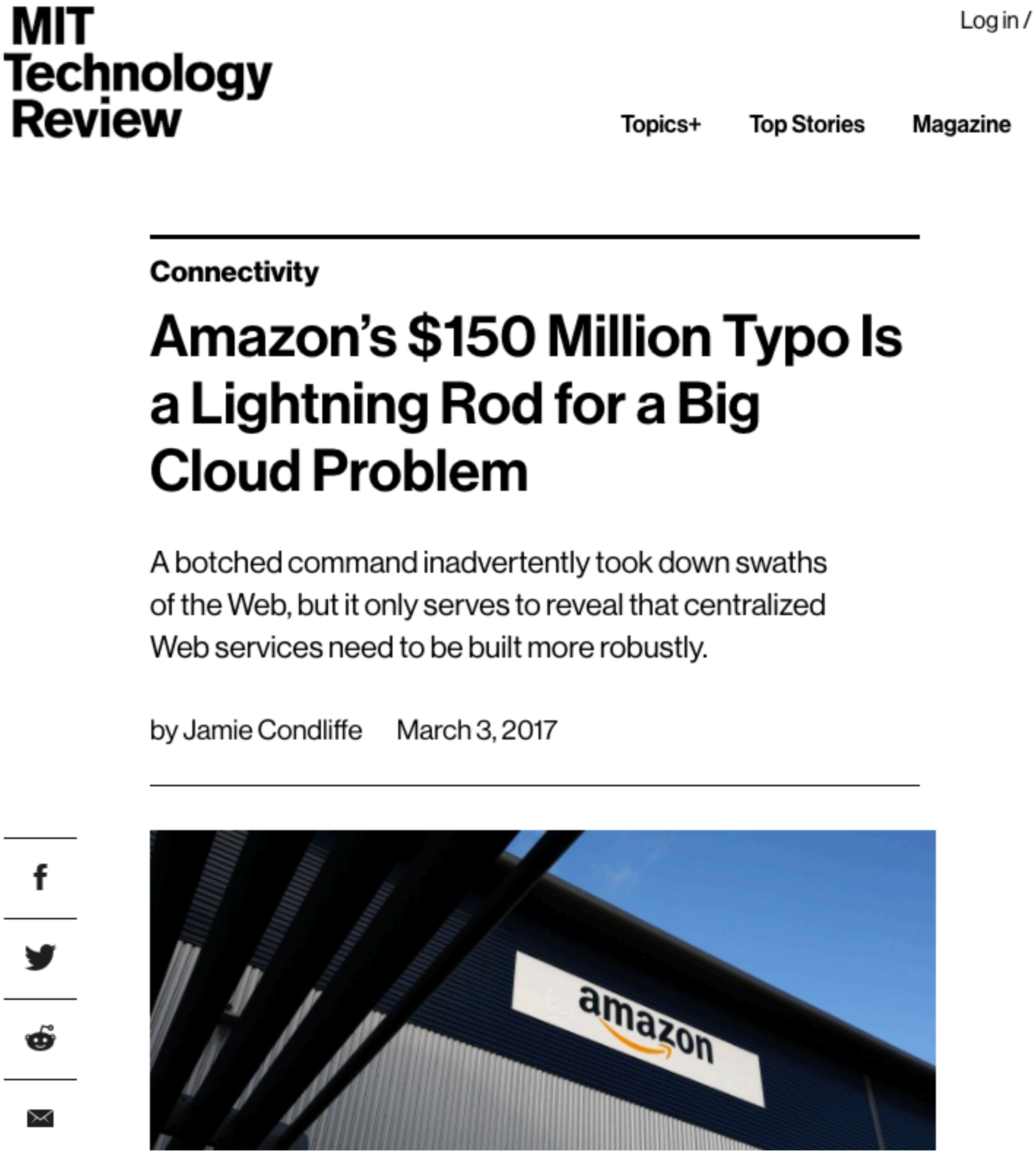
*Powered by DuckDuckGo*

● blog ○ essays ○ whole site

### Subscribe

### About Bruce Schneier

I've been writing about security issues on my blog since 2004, and in my monthly newsletter since 1998. I write books, articles, and academic papers. Currently, I'm the Chief Technology Officer of Resilient, an IBM Company, a fellow at Harvard's Berkman Center, and a board member of EFF.



MIT Technology Review

Log in /

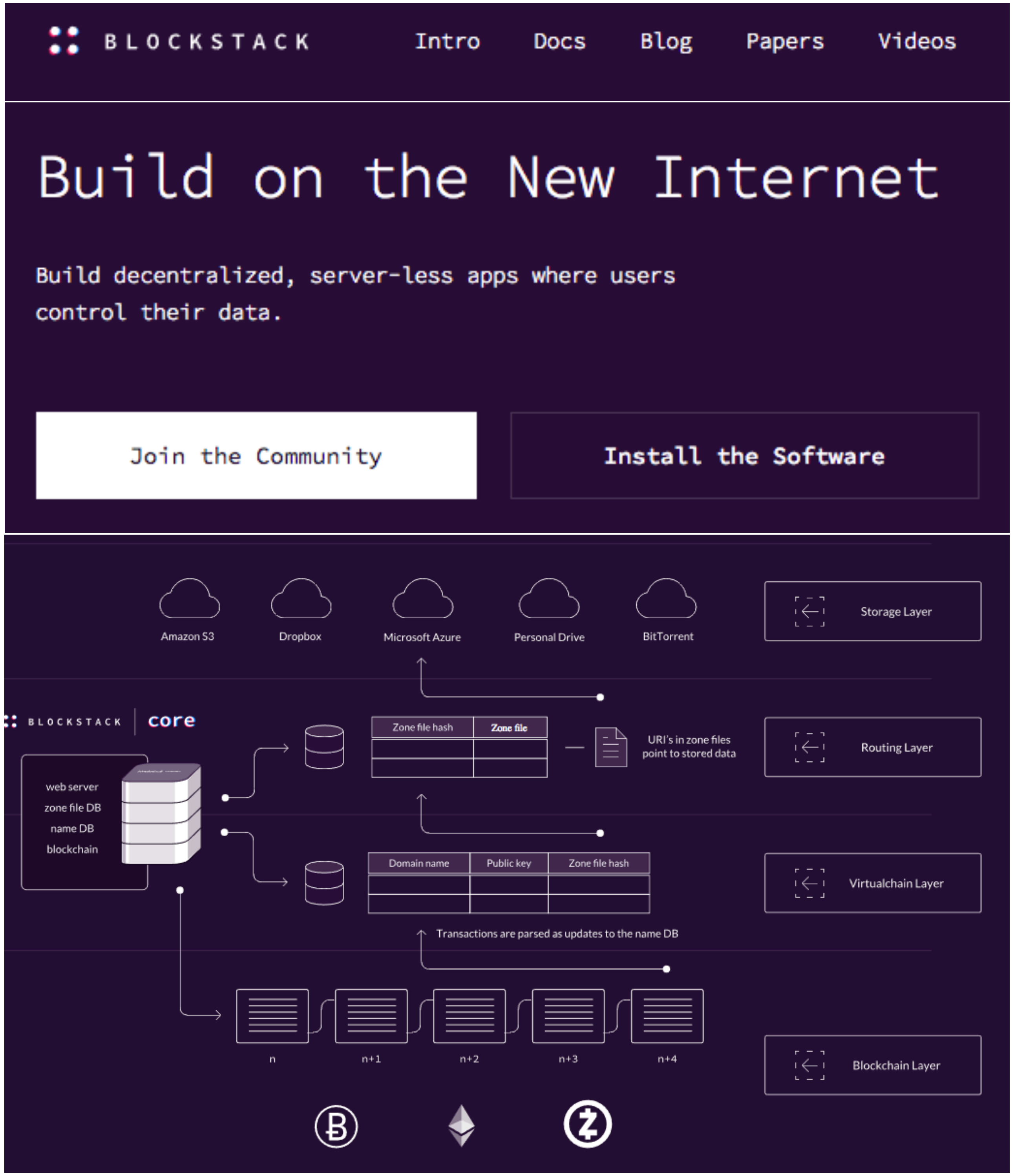
Topics+ Top Stories Magazine

Connectivity

# Amazon’s $150 Million Typo Is a Lightning Rod for a Big Cloud Problem

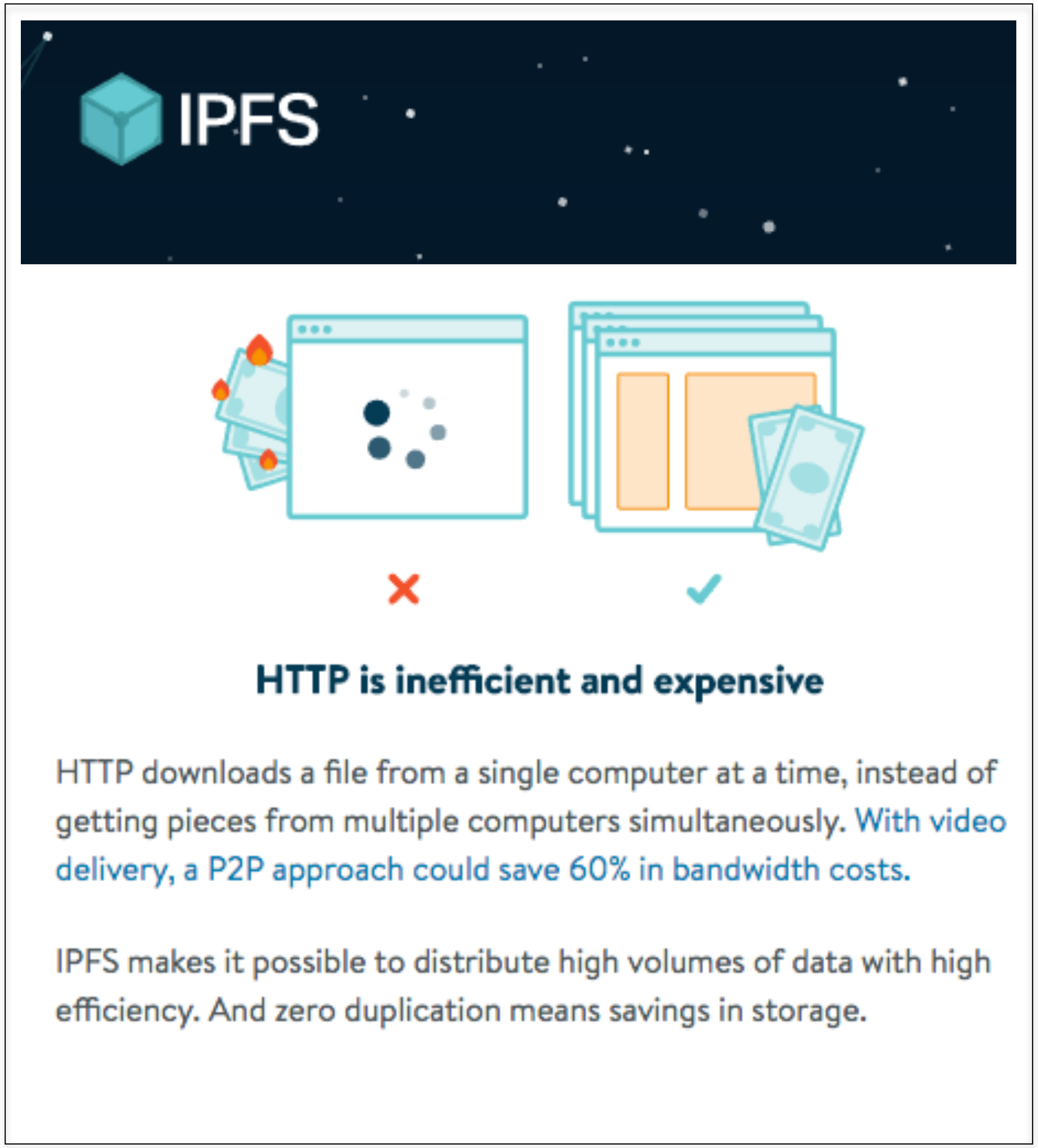
A botched command inadvertently took down swaths of the Web, but it only serves to reveal that centralized Web services need to be built more robustly.

by Jamie Condliffe March 3, 2017



# Build on the New Internet

Build decentralized, server-less apps where users control their data.

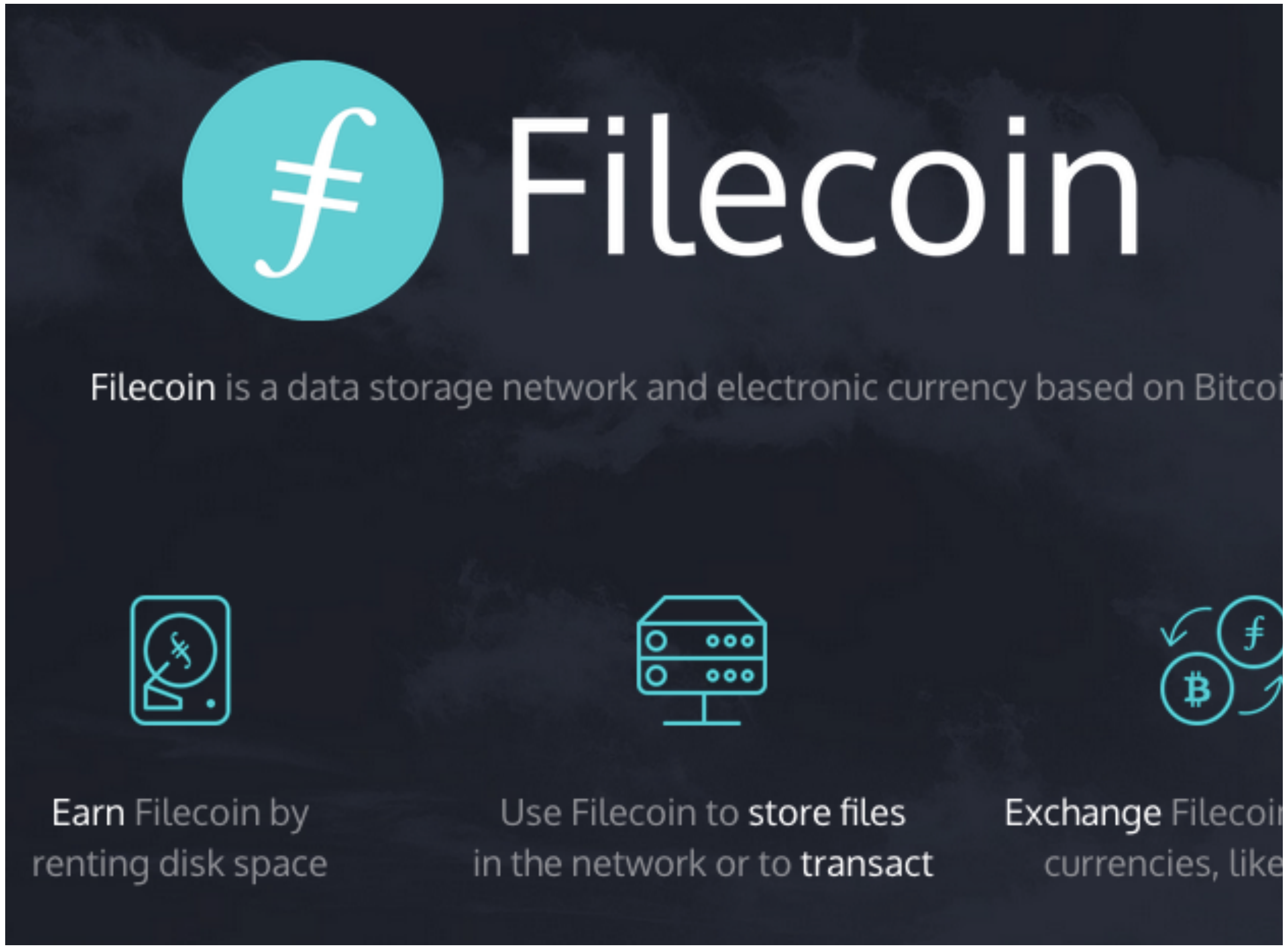


## HTTP is inefficient and expensive

HTTP downloads a file from a single computer at a time, instead of getting pieces from multiple computers simultaneously. With video delivery, a P2P approach could save 60% in bandwidth costs.

IPFS makes it possible to distribute high volumes of data with high efficiency. And zero duplication means savings in storage.

# …to Physical Assets



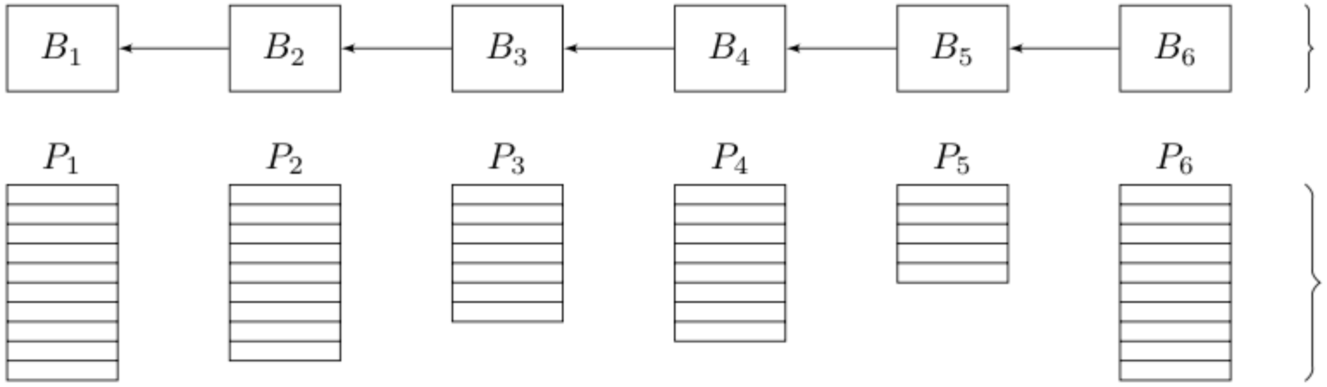
Filecoin

Filecoin is a data storage network and electronic currency based on Bitcoi

Earn Filecoin by renting disk space

Use Filecoin to store files in the network or to transact

Exchange Filecoi currencies, like

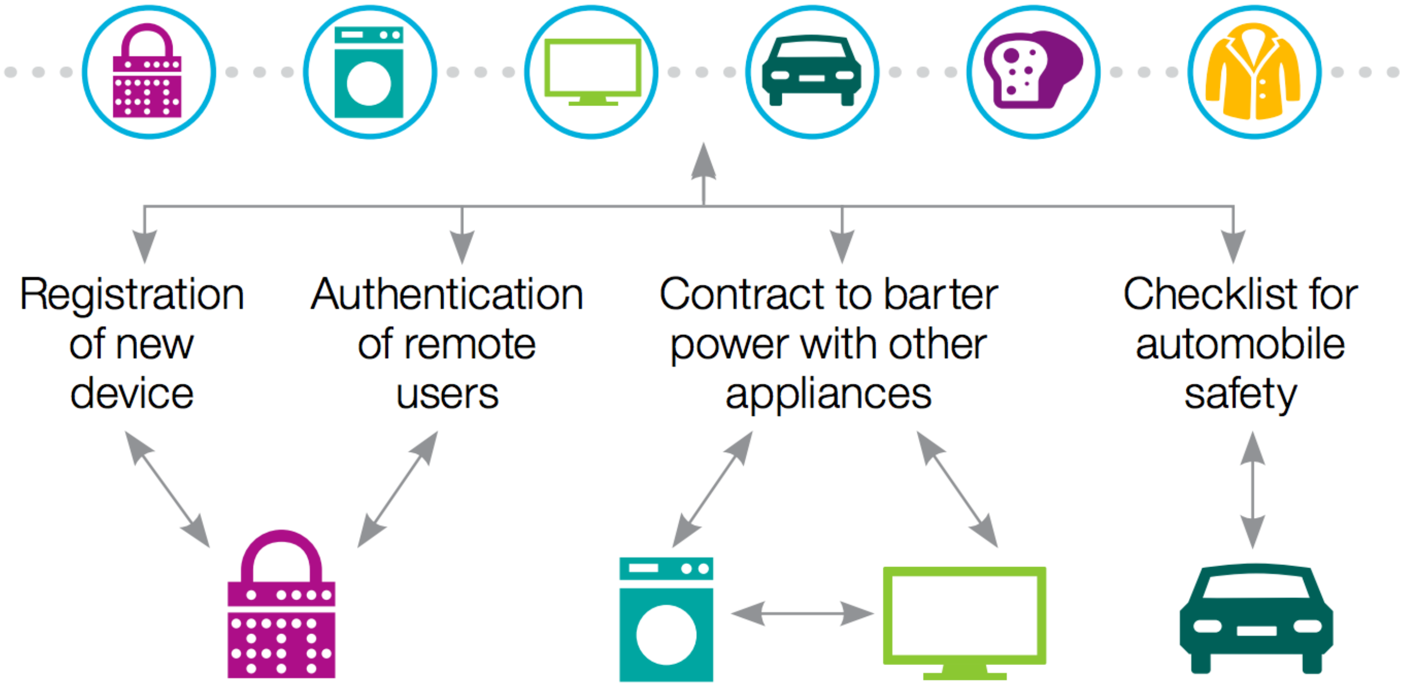


# …or Sensors

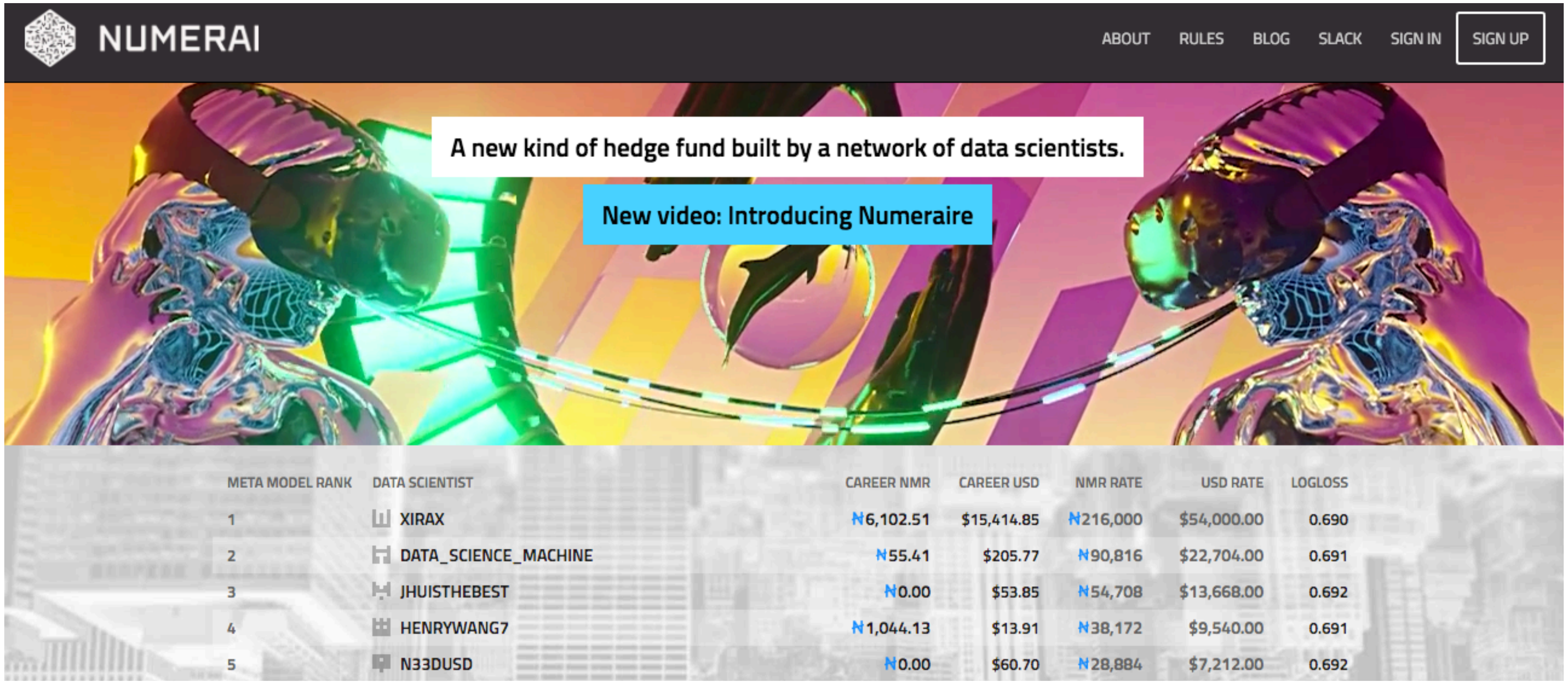
## Sensor21: Earn bitcoin by collecting environmental data

*By Tyler Pate, Jeremy Kun, and Balaji S. Srinivasan*

# Internet of Things, Robotics, AI


Registration of new device
Authentication of remote users
Contract to barter power with other appliances
Checklist for automobile safety

# The Firm as a Nexus of Contracts



A new kind of hedge fund built by a network of data scientists.

| META MODEL RANK | DATA SCIENTIST | CAREER NMR | CAREER USD | NMR RATE | USD RATE | LOGLOSS |
|---|---|---|---|---|---|---|
| 1 | XIRAX | ₦6,102.51 | $15,414.85 | ₦216,000 | $54,000.00 | 0.690 |
| 2 | DATA_SCIENCE_MACHINE | ₦55.41 | $205.77 | ₦90,816 | $22,704.00 | 0.691 |
| 3 | JHUISTHEBEST | ₦0.00 | $53.85 | ₦54,708 | $13,668.00 | 0.692 |
| 4 | HENRYWANG7 | ₦1,044.13 | $13.91 | ₦38,172 | $9,540.00 | 0.691 |
| 5 | N33DUSD | ₦0.00 | $60.70 | ₦28,884 | $7,212.00 | 0.692 |

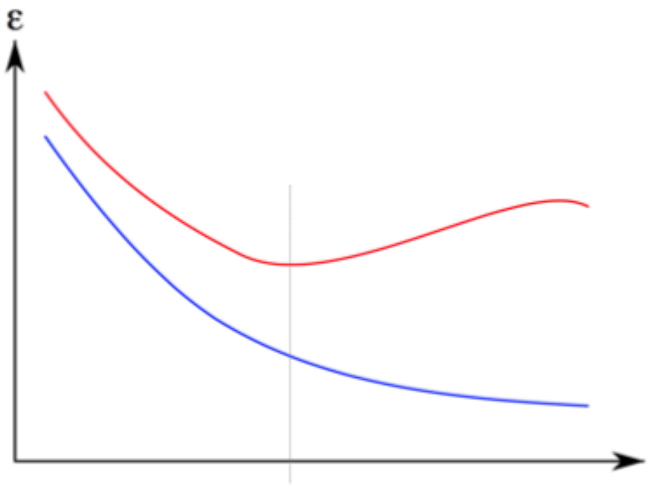
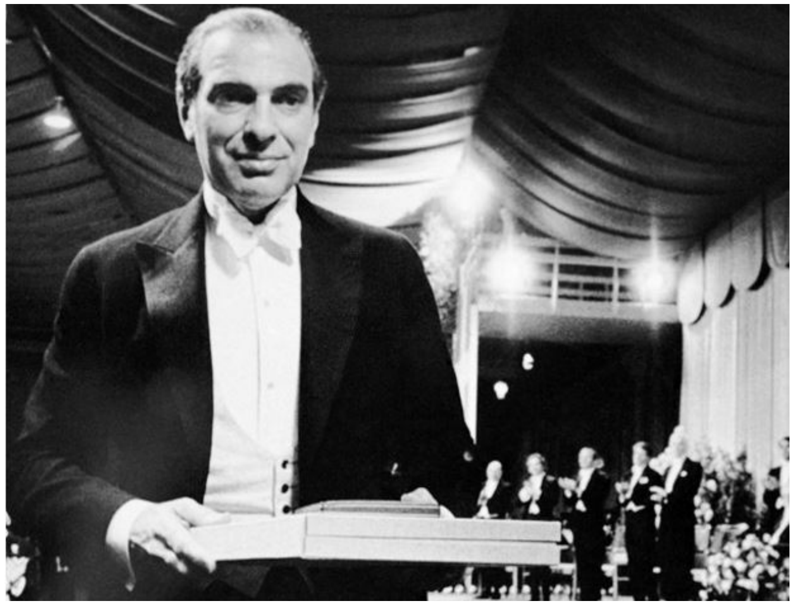


Figure 1: An overfitting curve where the blue test error continues to decrease with more submissions from data scientists, but the error on new data increases. [2]



# Thank You!

catalini@mit.edu
blockchain.mit.edu

MIT
MANAGEMENT
SLOAN SCHOOL