

Some Simple Economics of the Blockchain

Christian Catalini

catalini@mit.edu

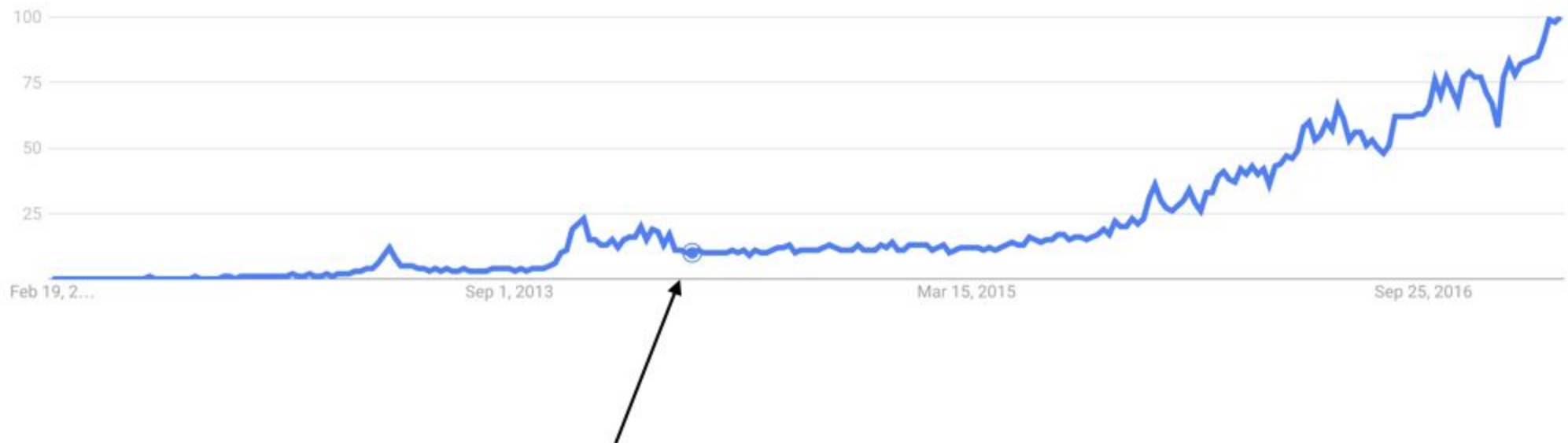
blockchain.mit.edu



MIT Digital Currency Experiment (2014)



Blockchain



MIT Digital Currency Experiment (2014)

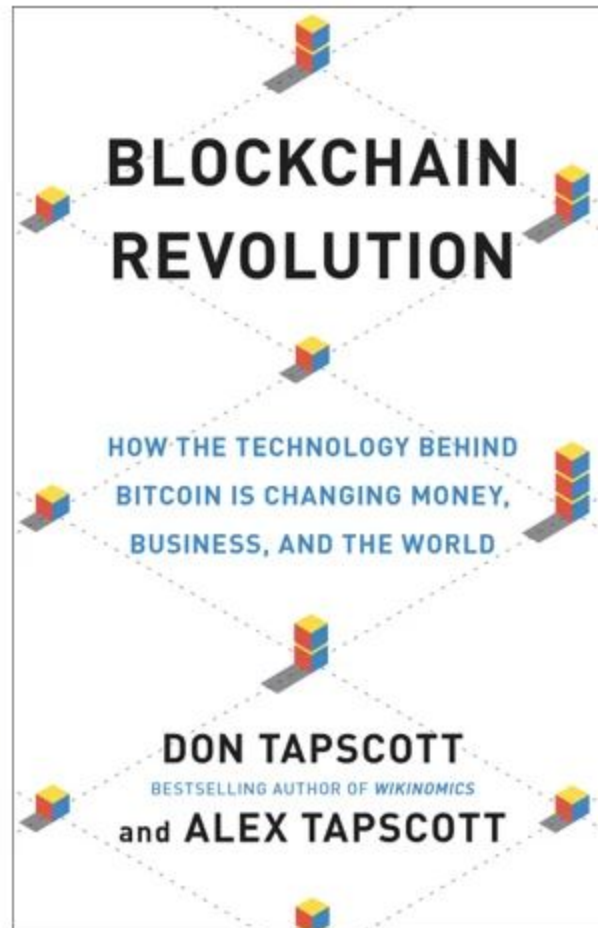
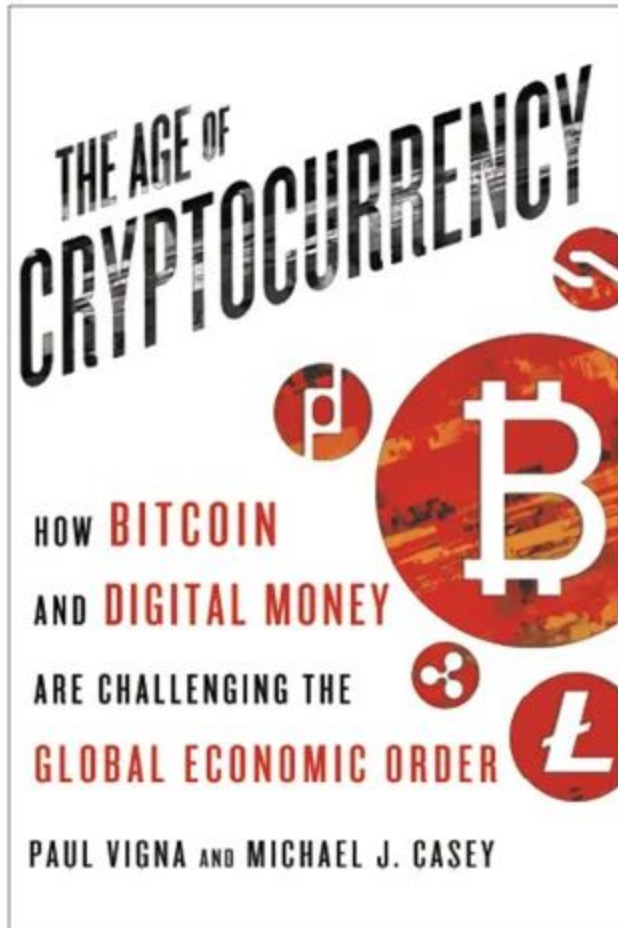


blockchain.mit.edu

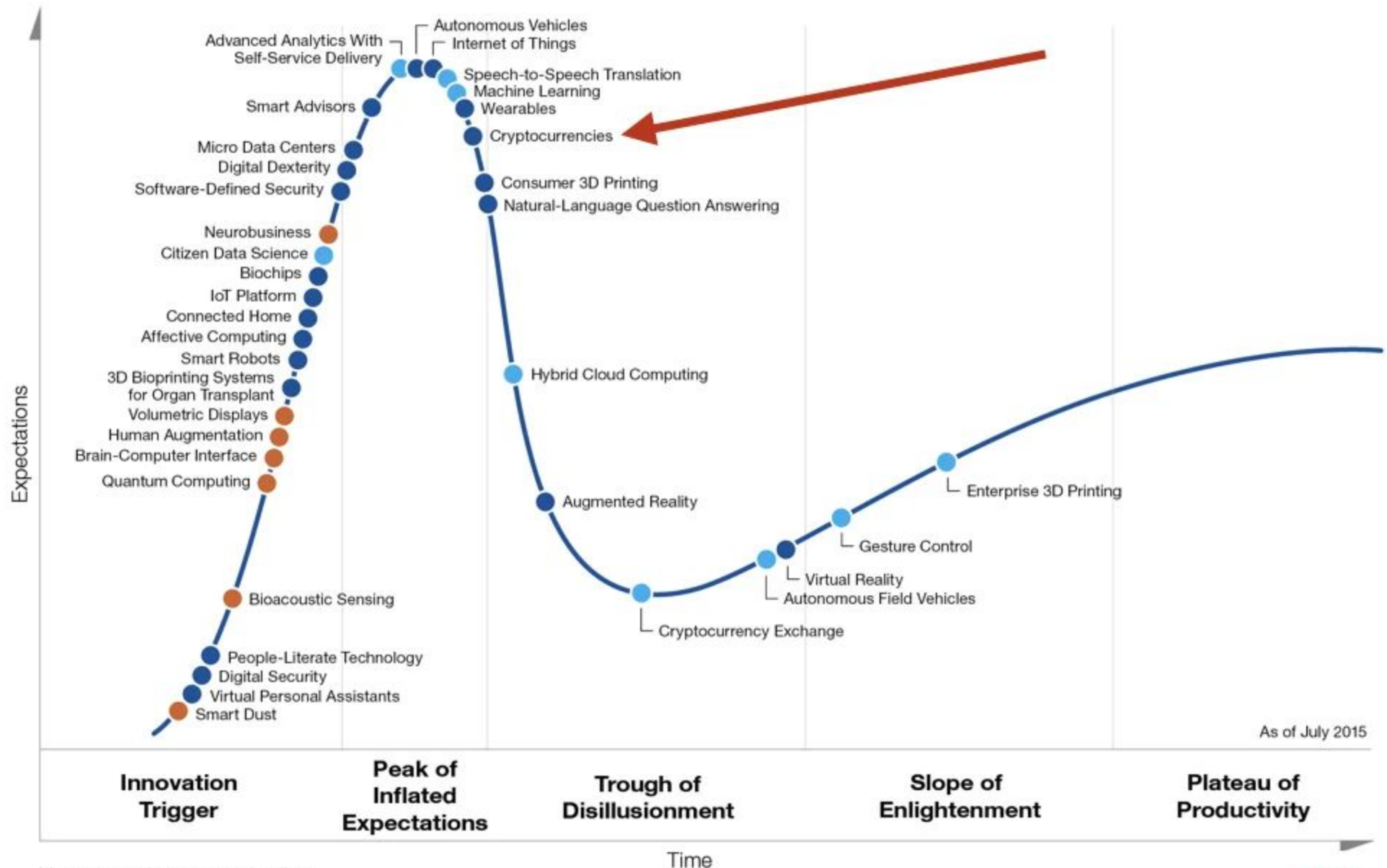
From Fringe to Mainstream



Most Revolutions Take Time!



Emerging Technology Hype Cycle

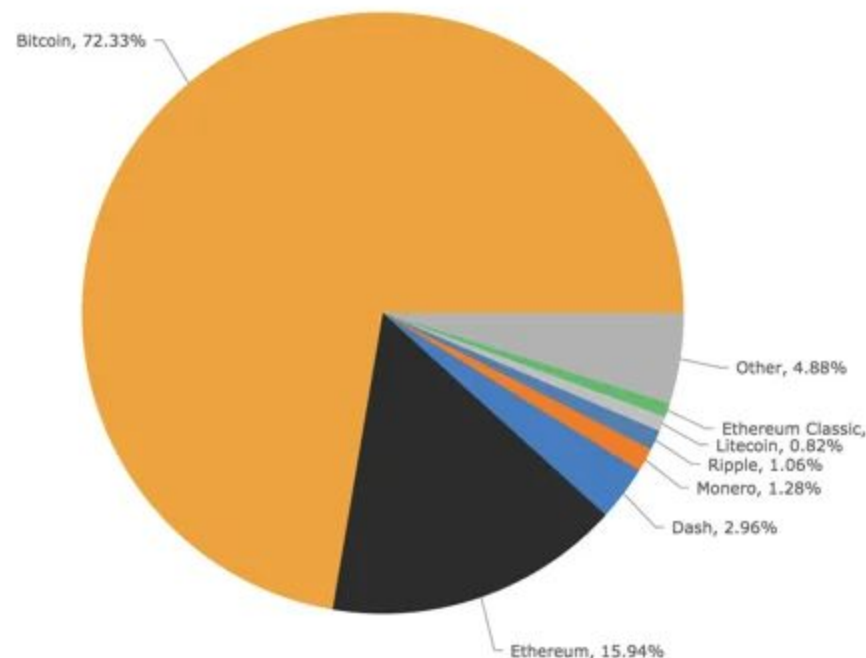


Years to mainstream adoption:

- less than 2 years
- 2 to 5 years
- 5 to 10 years
- more than 10 years
- obsolete before plateau

Competing Standards

All ▾ Currencies ▾ Assets ▾ USD ▾					
#	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



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.

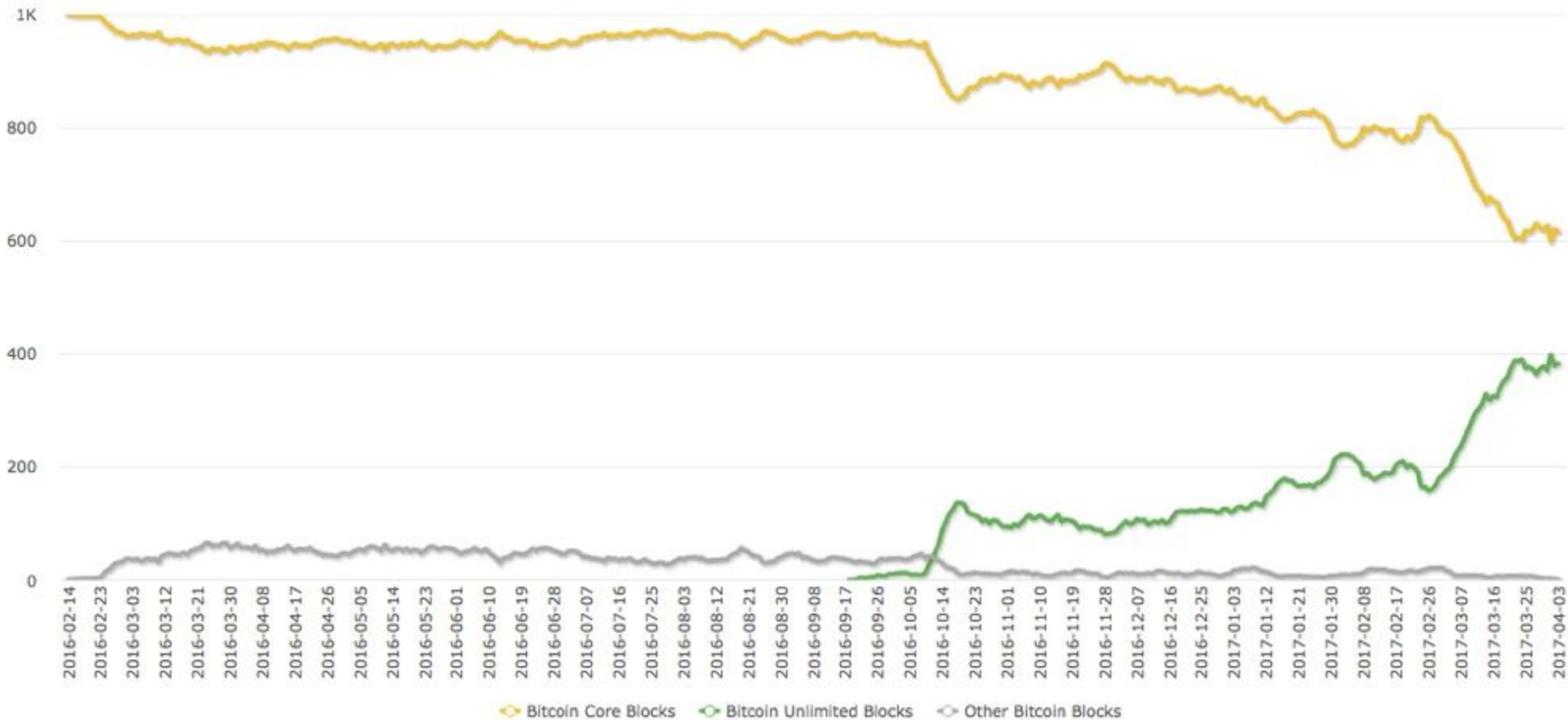
But there are competing visions about any fix’s goals and methods. One bitcoin entrepreneur has [summarized the divide](#) as between a [Bitcoin Unlimited](#) contingent updating bitcoin to support many small transactions, and a Bitcoin Core cadre who believe in smaller changes, fewer transactions, and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



Market Design

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

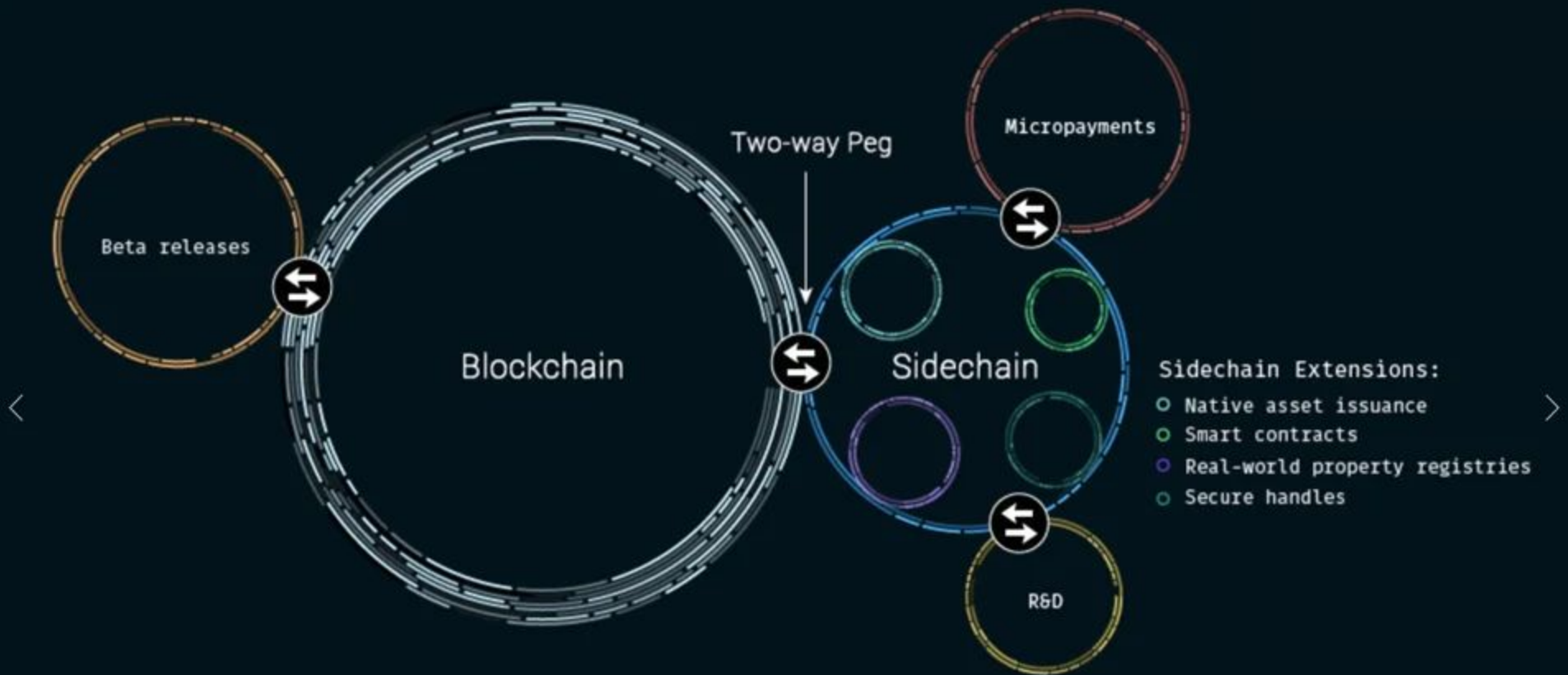
Battle for the Standard



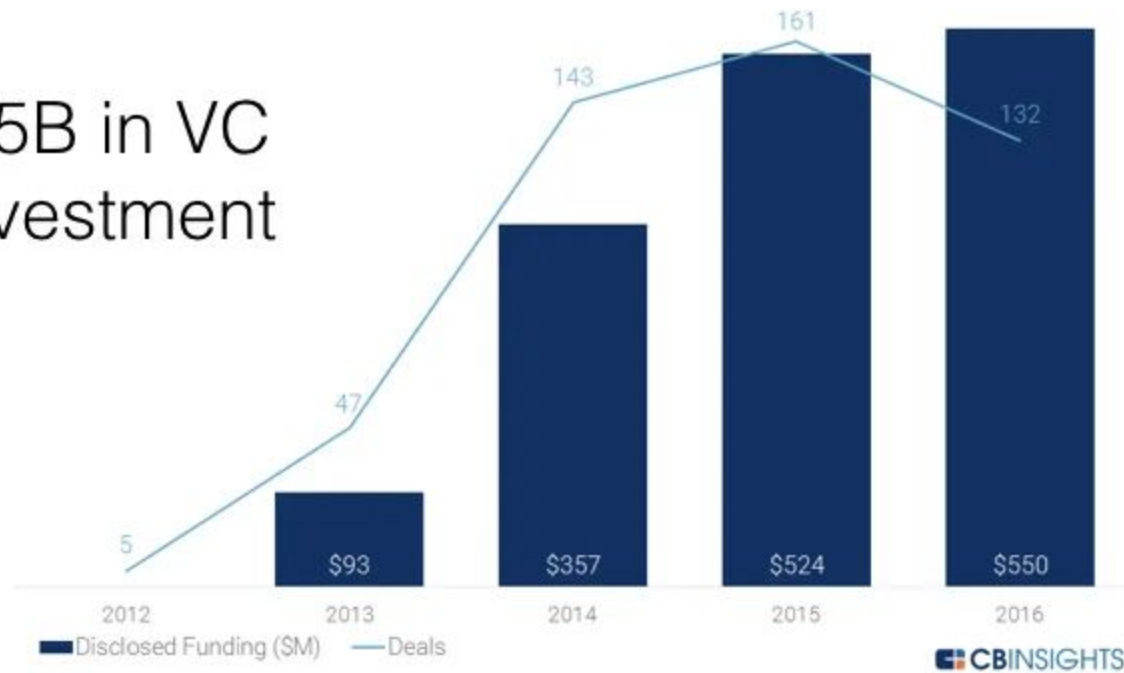
New Bitcoin Blocks

4/3/2017

Entrepreneurial Experimentation



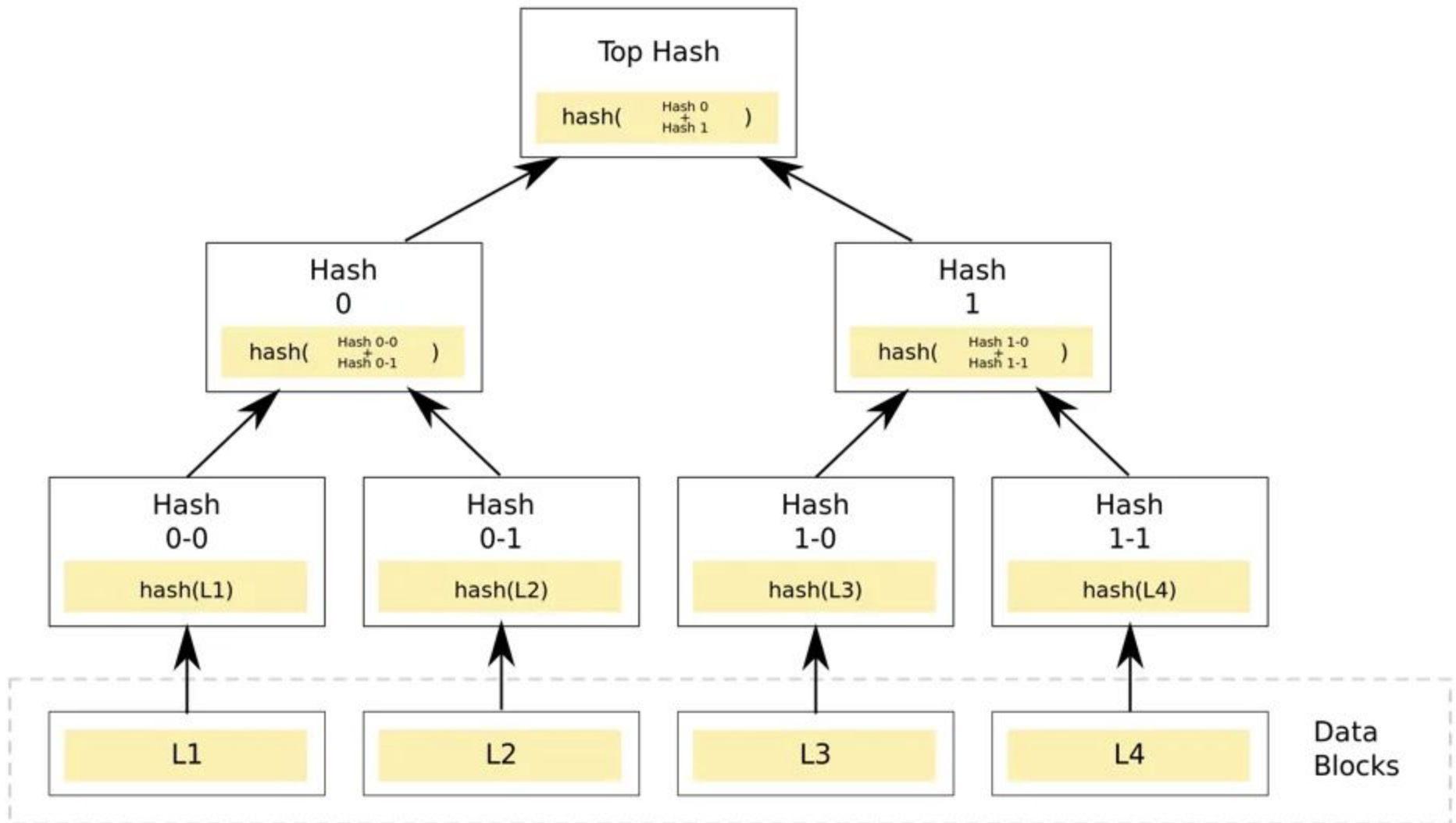
1.5B in VC Investment



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  
            $details['access'] = !$access  
            $this->_sql->delete( 'acl_ru  
        } else {  
            // Update the rule with the  
            $this->_sql->update( 'acl_ru
```

Computer
Science

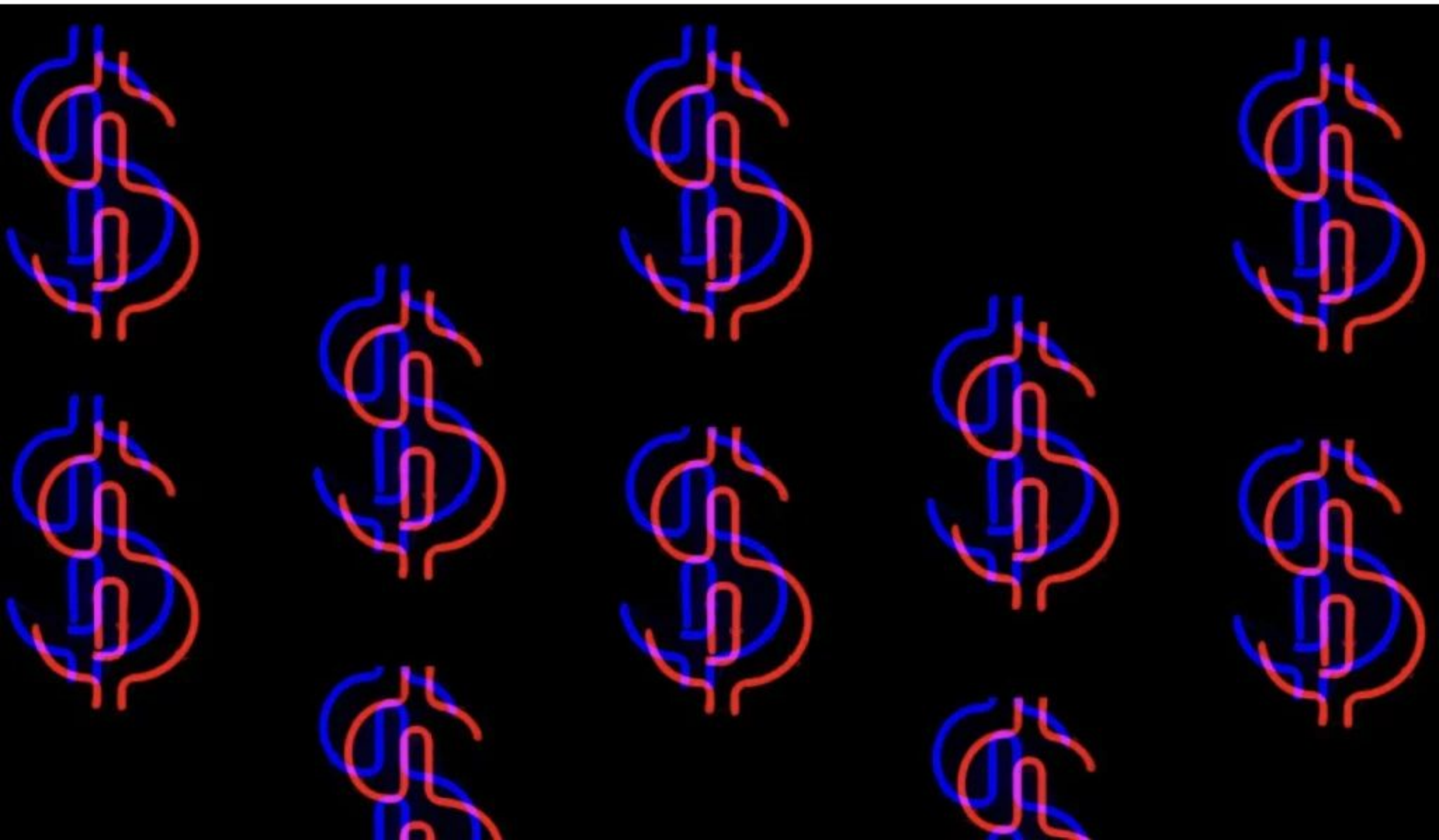


Economics and
Market Design



Law

Economists Like to Think of
Technology Changes in Terms of Costs...



A Reduction in Two Key Costs

1. Cost of Verification

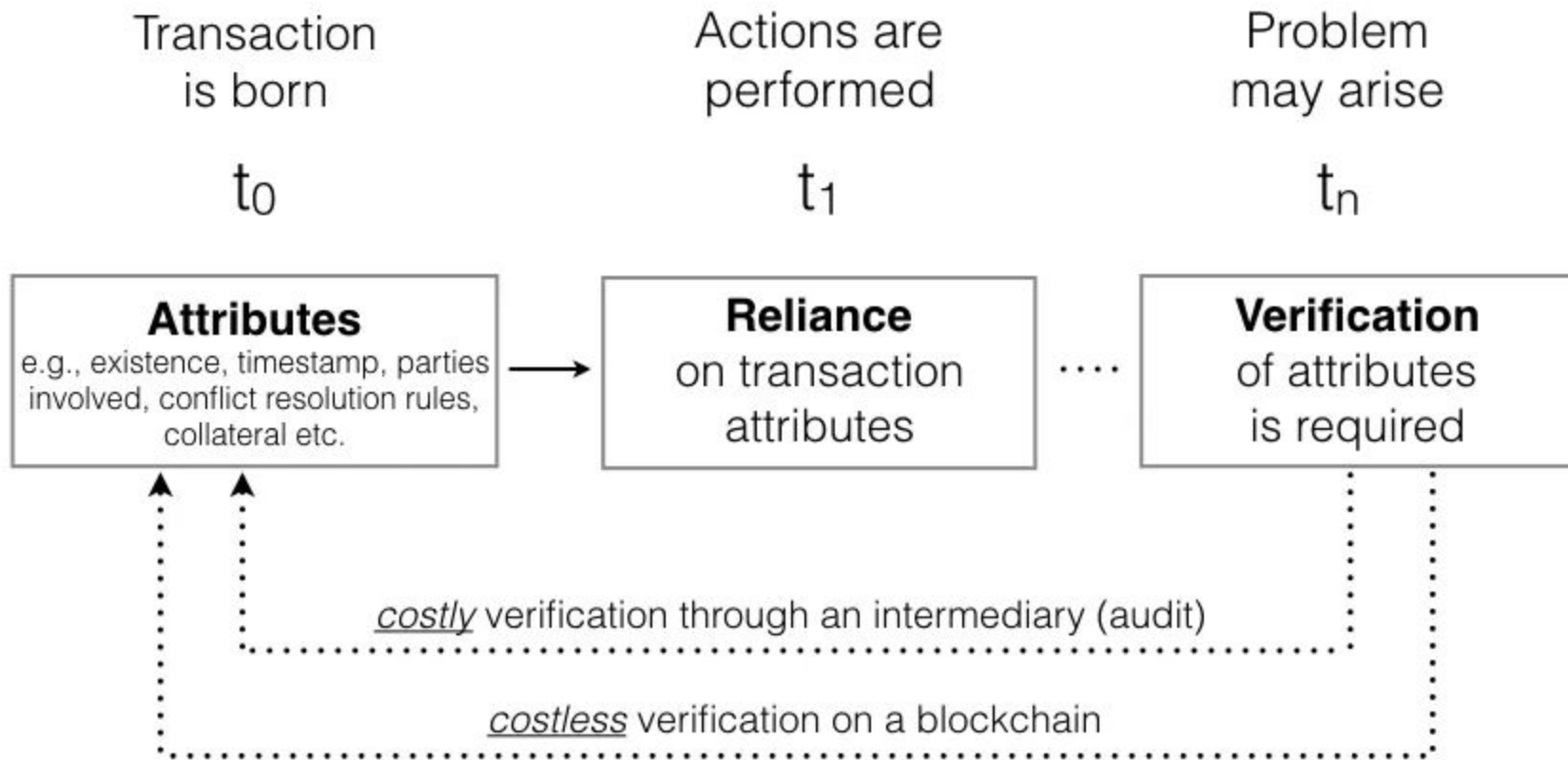
```
00: 09 05 79 AE-14 00 00 00-06 55 8E 71-4C 07 00 00 0x+y«ll «UAqL·
10: 4D 04 00 00-02 00 00 00-01 00 00 00-02 00 00 00 M+ 0 0 0
20: 08 00 00 00-01 00 00 00-01 00 00 00-01 00 00 00 0 0 0
30: E0 93 04 00-E0 70 72 00-80 84 1E 00-FE 04 00 00 αô+ apr Çä- l+
40: 01 00 00 00-01 00 00 00-01 00 00 00-80 EE 36 00 0 0 0 ÇE6
50: 64 00 00 00-2C 01 00 00-58 02 00 00-84 03 00 00 d 0 XO äv
60: 50 46 00 00-08 52 00 00-01 00 00 00-00 00 00 00 PF R 0
70: 00 00 00 00-5A 00 00 00-00 80 65 74-9F 48 CB 01 Z CøtfHfö
80: 03 00 00 00-40 48 4C 00-03 00 00 00 00 00 00 00 ♥ OKL ♥ LEL
90: 9C 51 CD 01-38 31 00 00-00 00 00 00-00 00 00 00 £Q=081
A0: 00 00 00 00-EE 07 38 11-06 6C CA 01-01 00 00 00 E-84+1400
B0: 00 00 00 00-EE 07 38 11-06 6C CA 01-00 00 00 00 E-84+140
C0: 5A 00 00 00-87 00 00 00-01 00 00 00-77 00 77 00 Z ç 0 ww
D0: 77 00 2E 00-77 00 69 00-6E 00 64 00-6F 00 77 00 w . window
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 ww
50: 77 00 2E 00-6D 00 73 00-6E 00 2E 00-63 00 6F 00 w . m e n . c o
60: 00 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

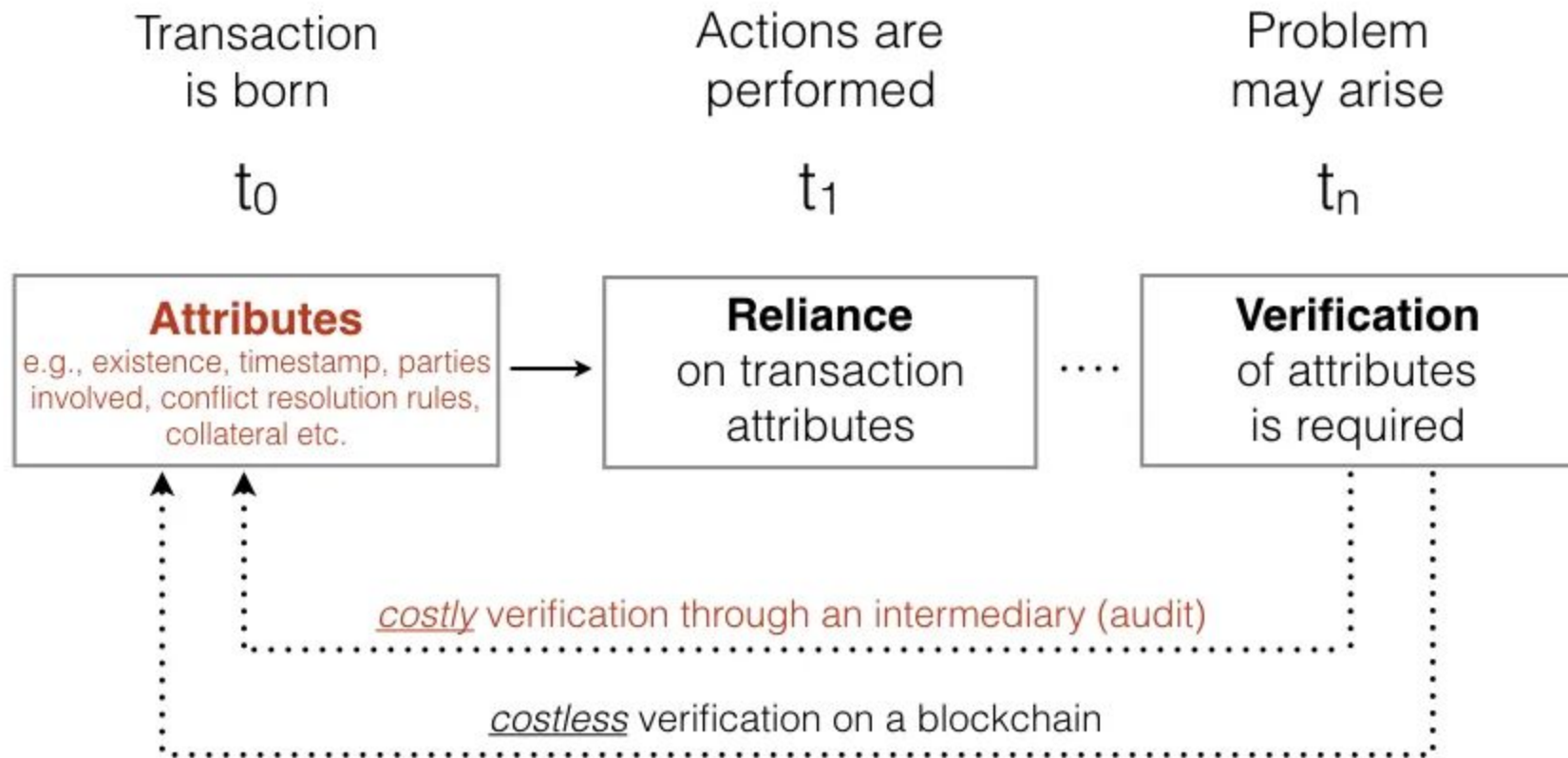
2. Cost of Networking



1. Costless Verification



Information Leakage

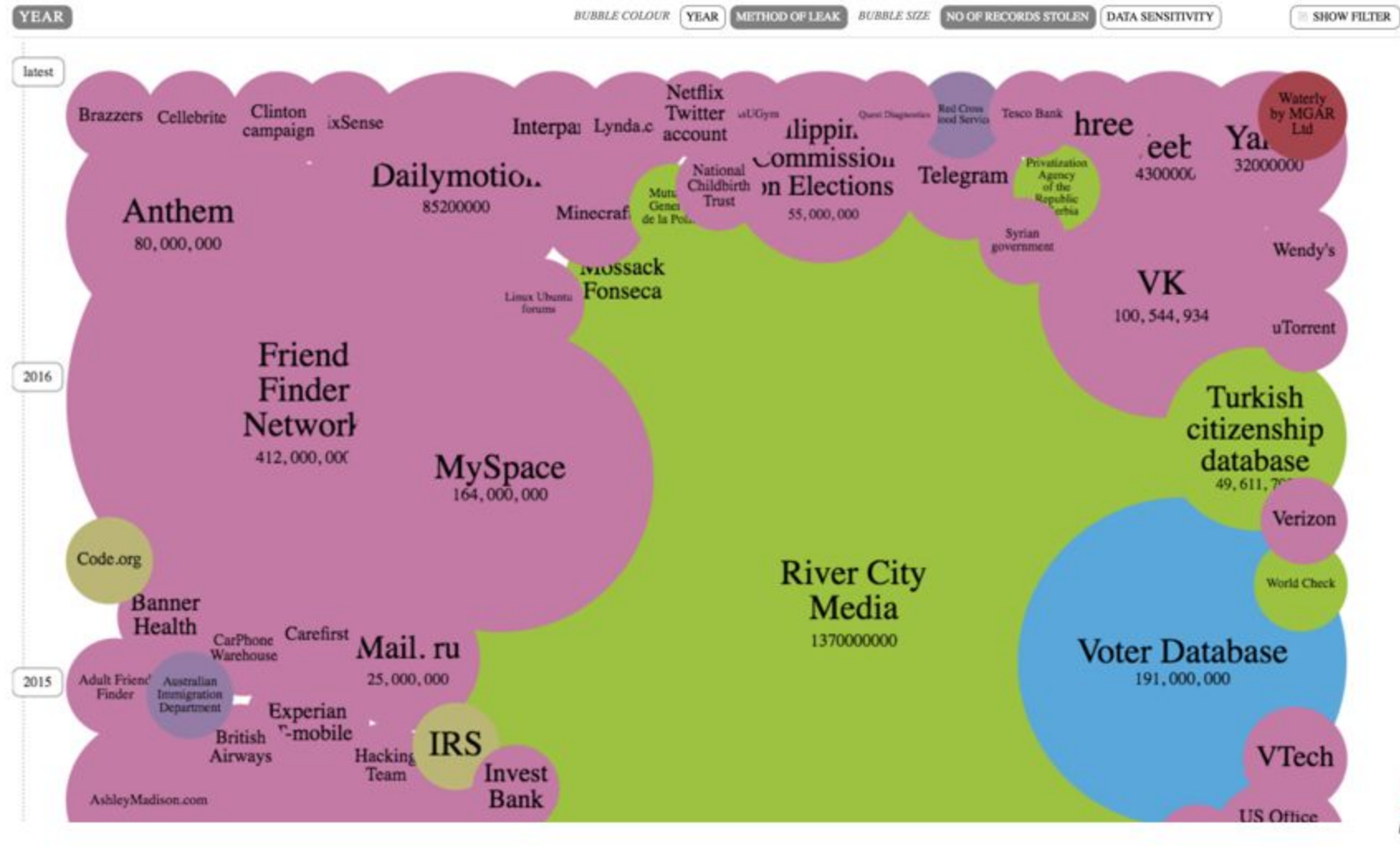


Information Leakage

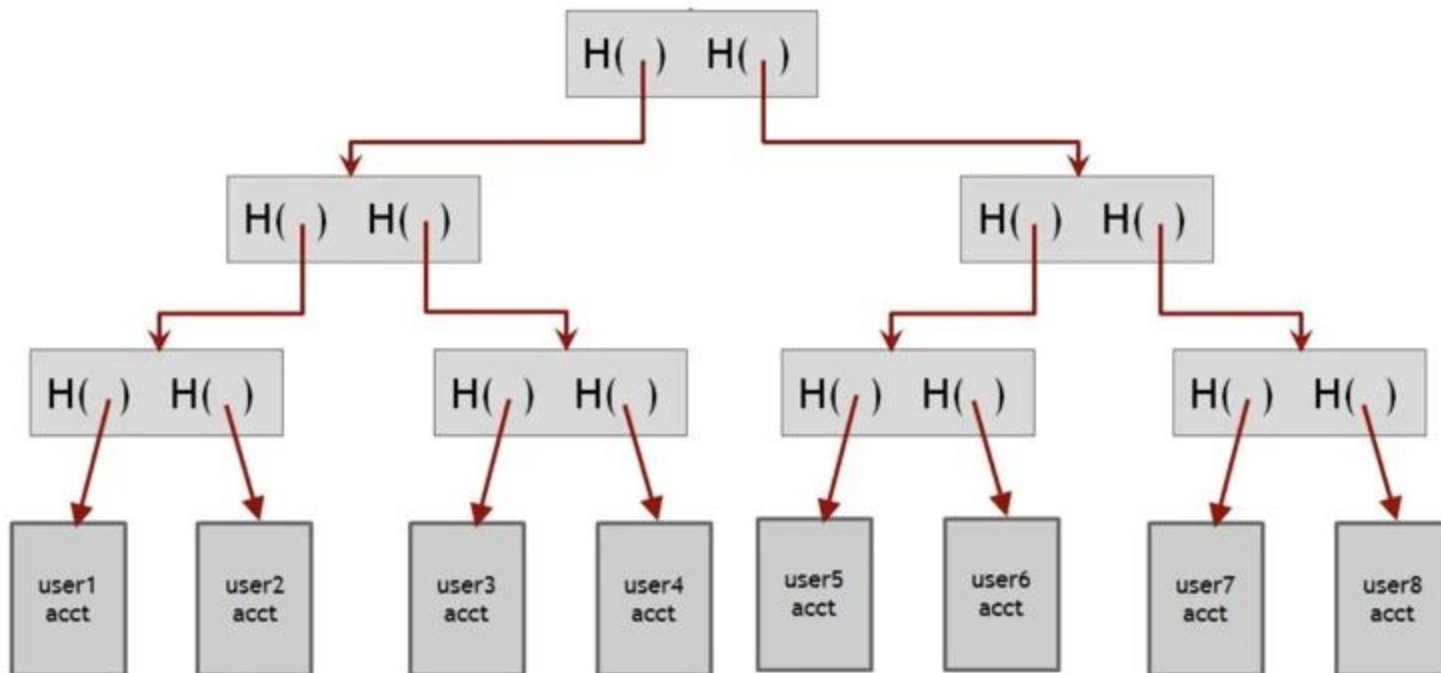
World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 5th Jan 2017)



Data Integrity Through Costless Verification



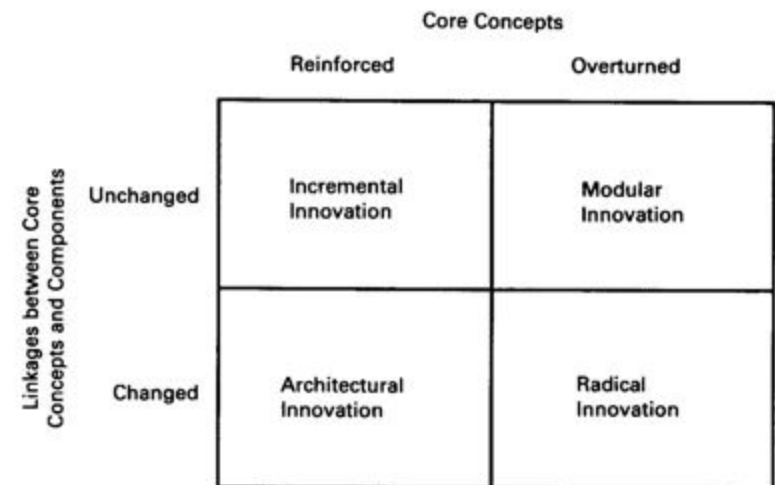
2. Cost of Networking

- 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



2. Cost of Networking

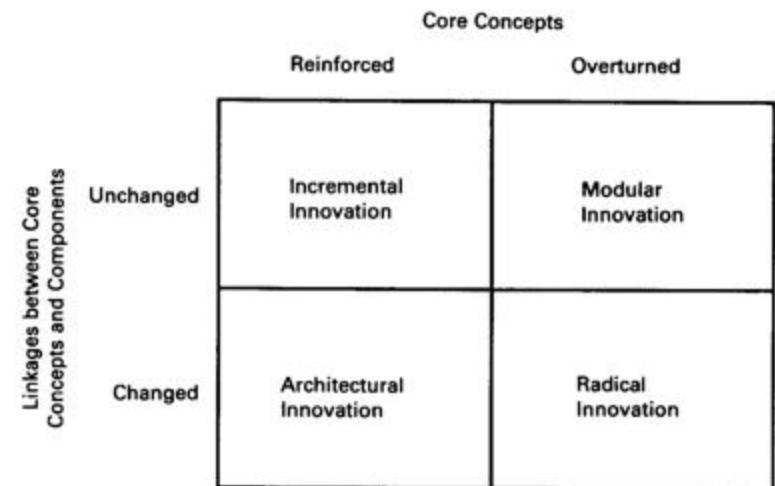
- The **architectural change** brought by cryptocurrencies is tied to their use of a native token to incentivize the growth, operations, and securing of a network
- “We show that architectural innovations **destroy the usefulness of the architectural knowledge of established firms**, and that since architectural 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



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

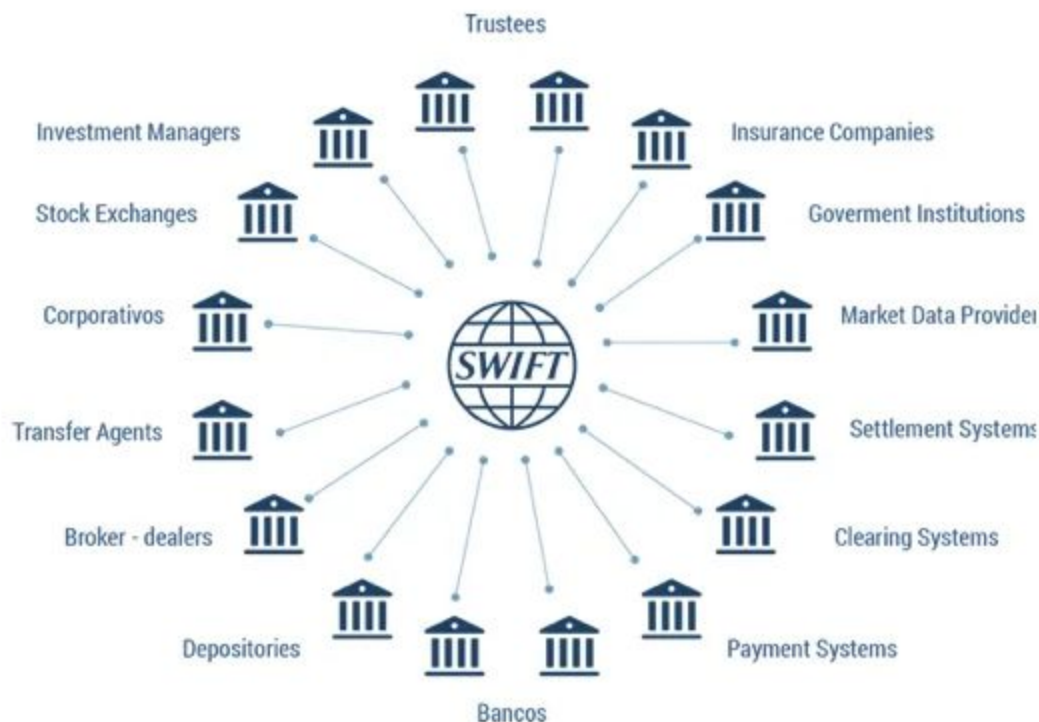
2. Cost of Networking

- 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**

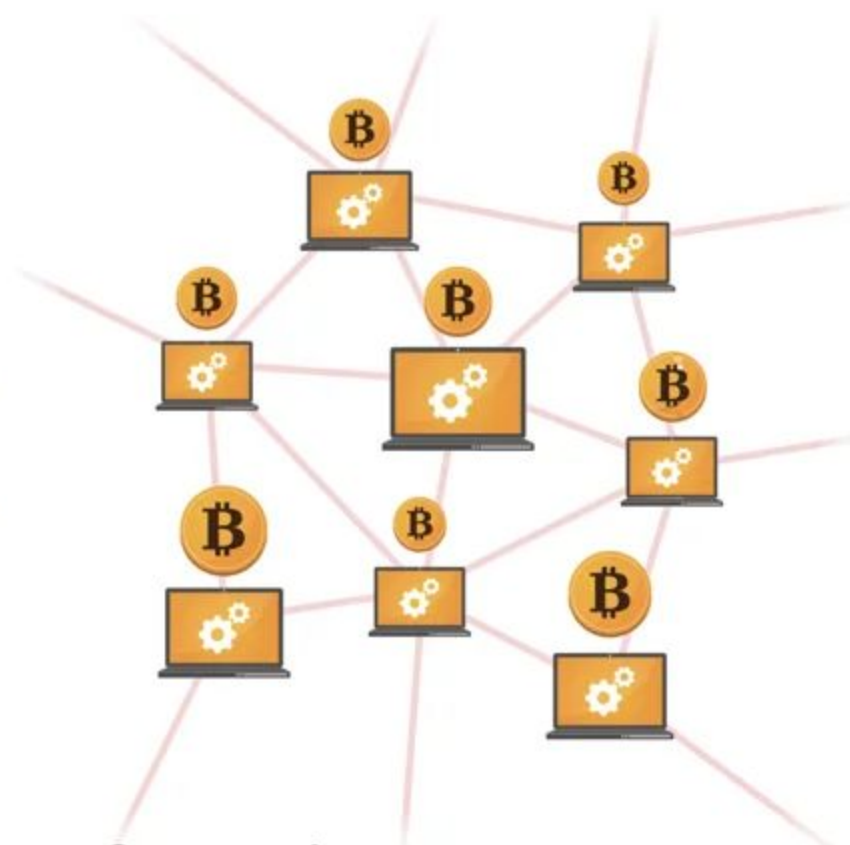


Henderson, R. M.; Clark, K. B., ASQ (1990) Architectural Innovation: The Reconfiguration Of Existing Product Technologies and the Failure of Established Firms

2. Cost of Networking

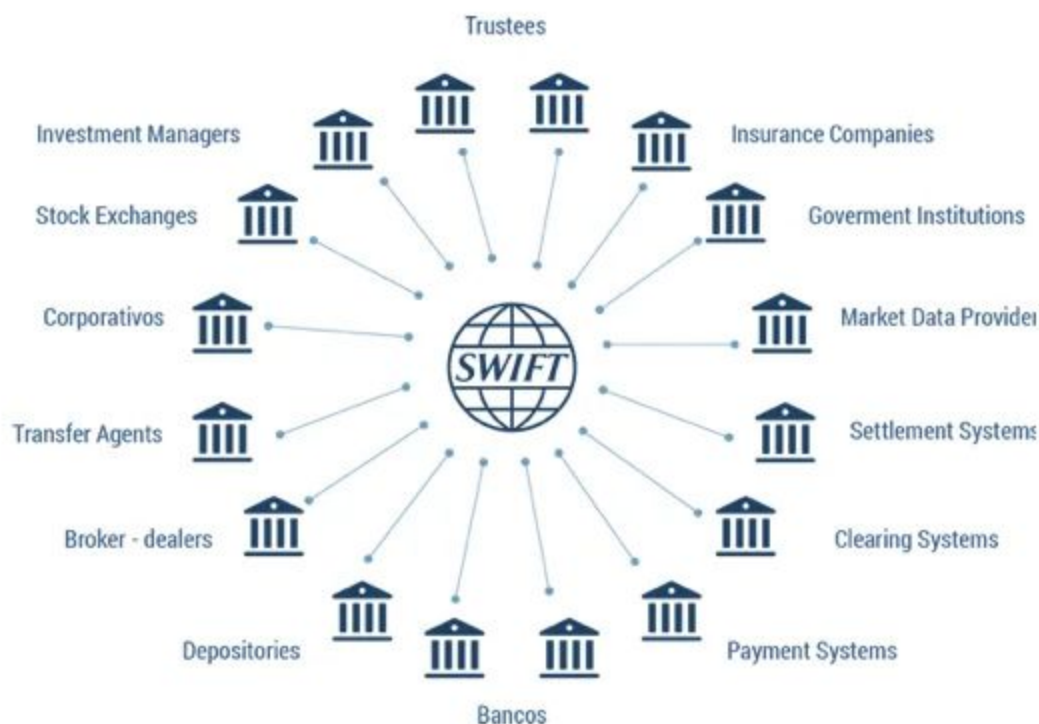


Cost of vetting and
maintaining the integrity
of the nodes

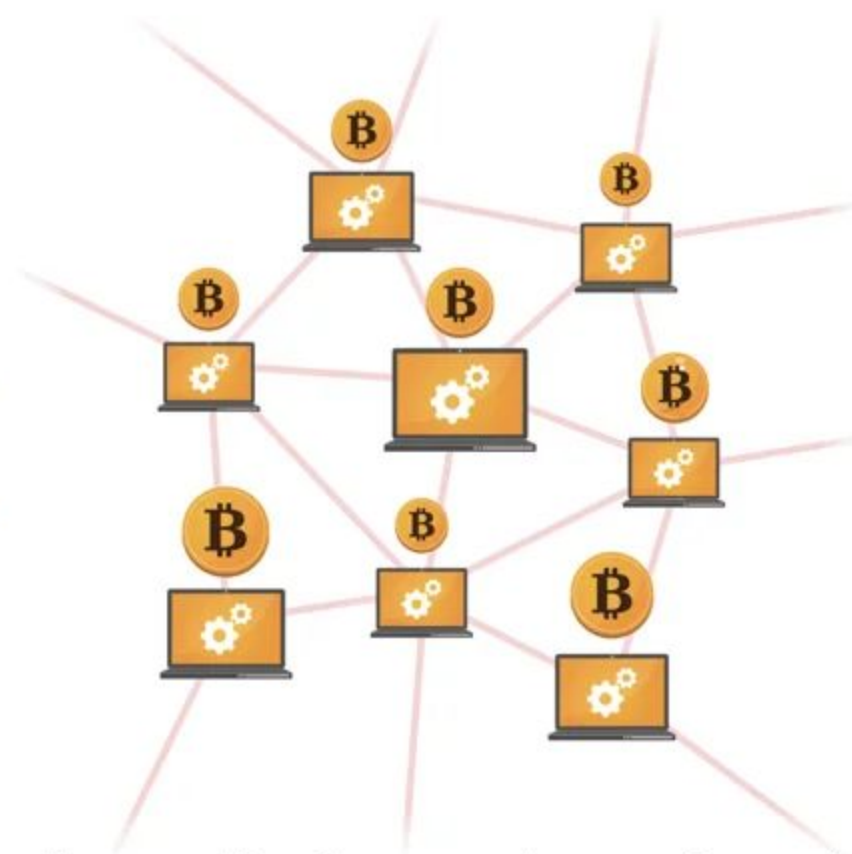


Cost of computation
(sunk commitment to the
shared ledger)

2. Cost of Networking

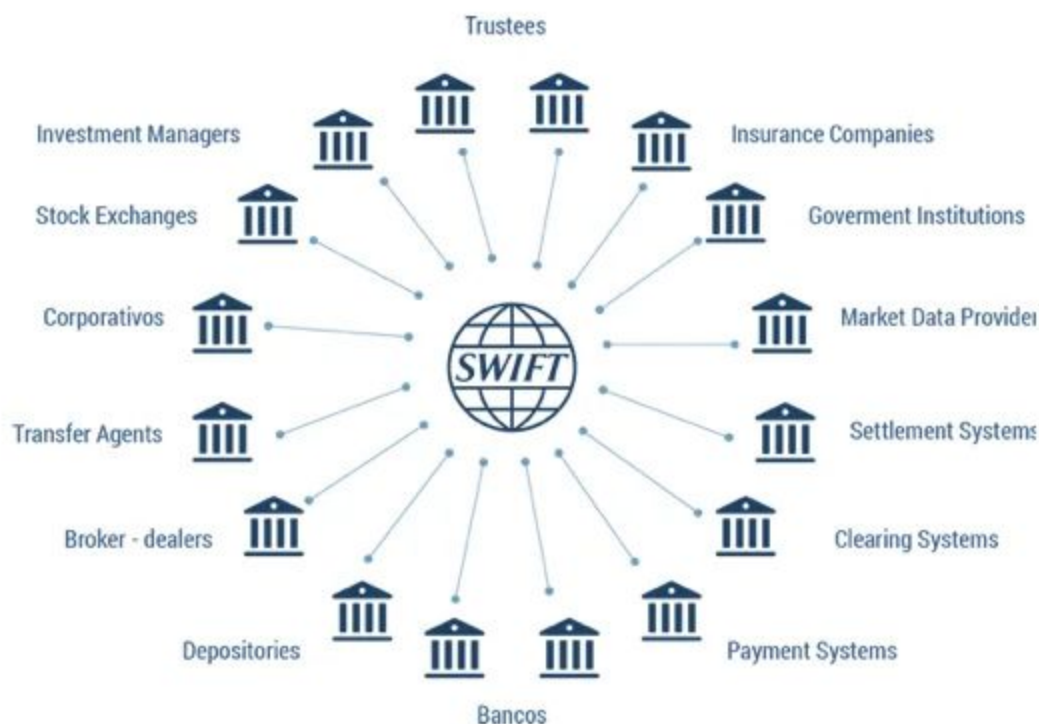


Security through trusted intermediaries / fiat.
Typically fast (e.g. VISA)

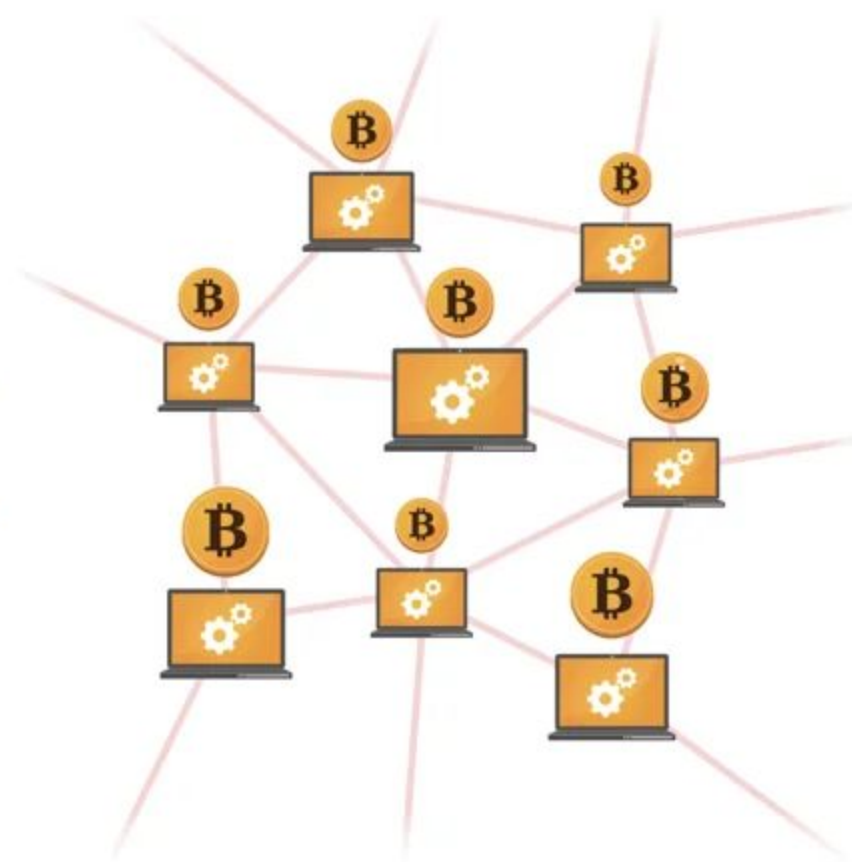


Security through protocol design, game theory.
Currently slow (e.g. BTC)

2. Cost of Networking

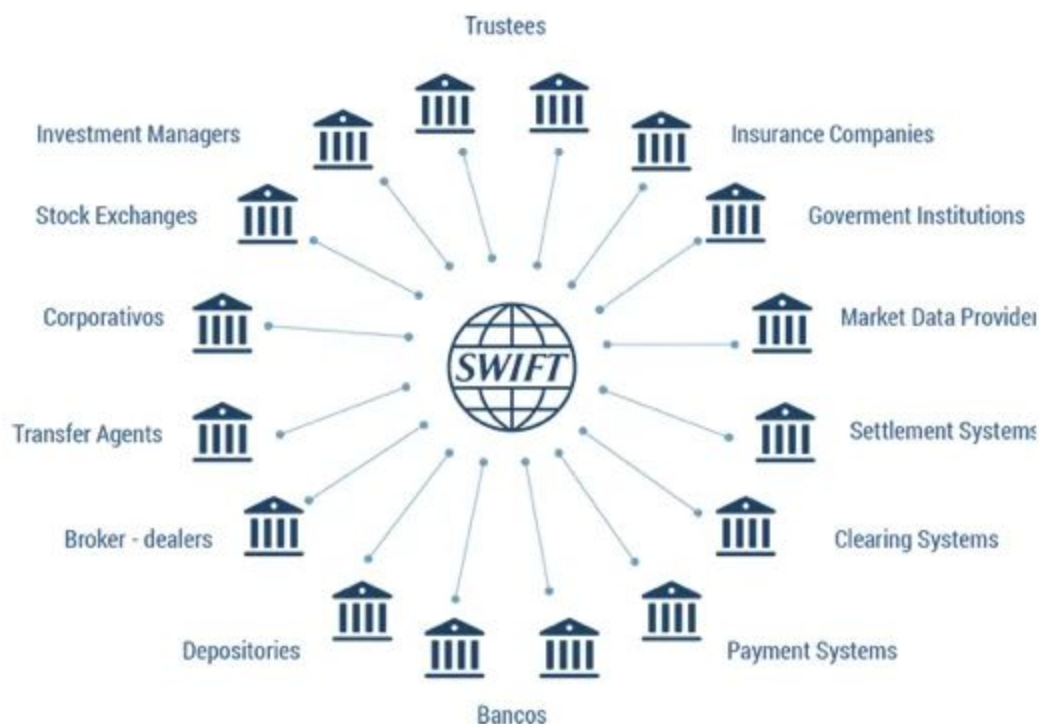


Ownership of the assets
resides with the nodes,
nodes certify txs

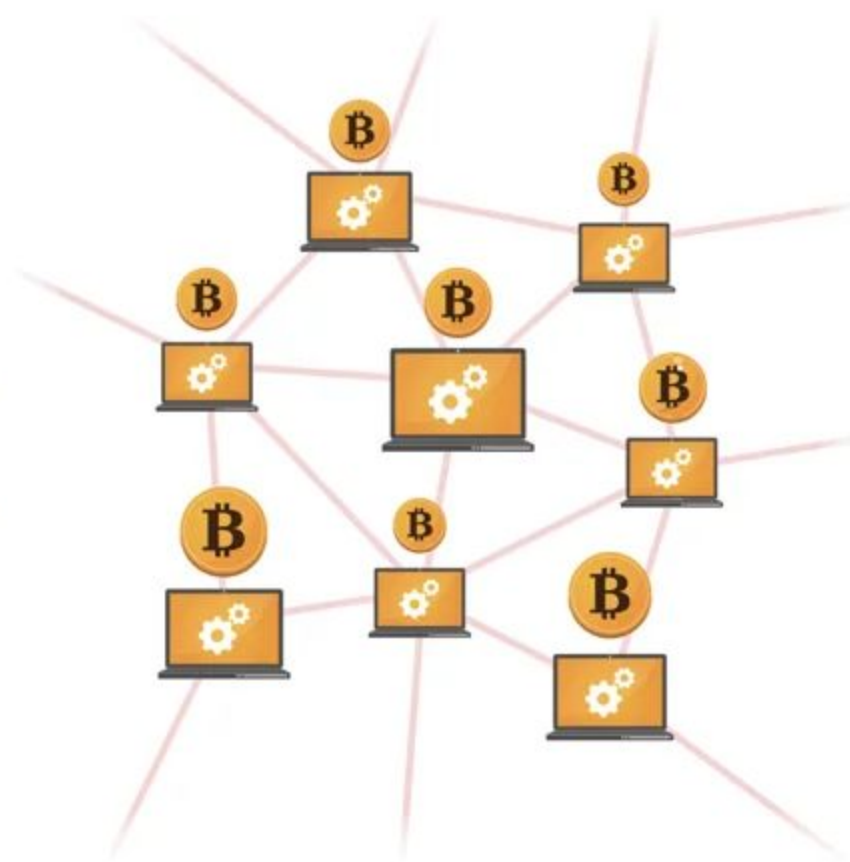


Ownership of the assets
resides with the users,
no censorship

2. Cost of Networking

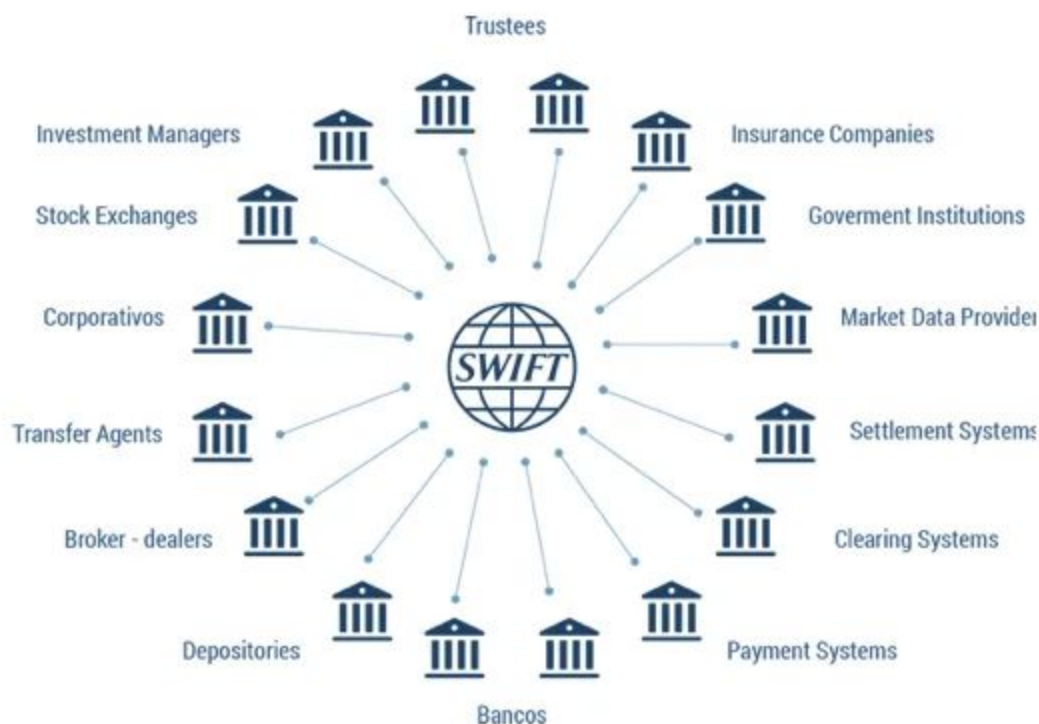


Innovation requires
approval (compliance)

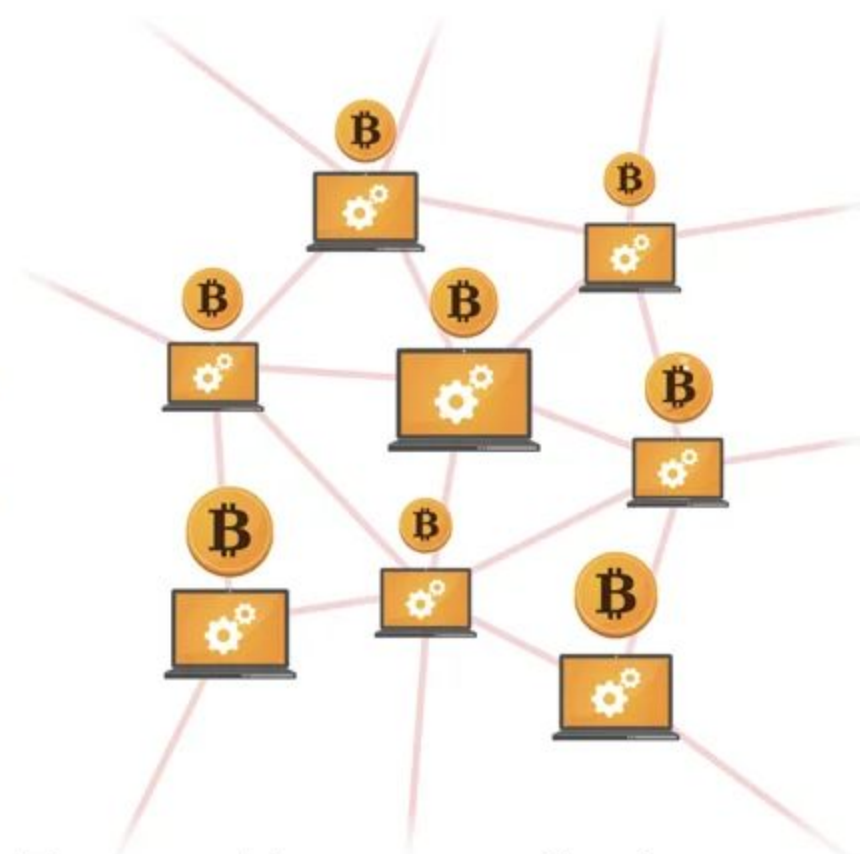


Permissionless
innovation (no compliance)

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



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

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?



Fintech



Identity & Privacy

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.

[Sign Up](#)

Already a member? [Log In](#)

New Business Models

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 appropriate. Please pay to the following address:

Please send **5 mBTC** or more to:
 1J7H-t58xY228G7gv1fwL2V09k37myo4c

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

IP & Smart Contracts

Filecoin

Filecoin is a data storage network and electronic currency based on Bitcoin.

[Earn Filecoin by renting disk space](#) [Use Filecoin to store files in the network or to transact](#) [Exchange Filecoin currencies, like](#)

New Types of Platforms



IoT, AI Robotics

Central Banks


MENU

FINANCIAL TIMES

myFT

Blockchain [+ Add to myFT](#)

Nov 4th

Central banks explore blockchain to create digital currencies

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



Finance

ripple Solutions Technology Network

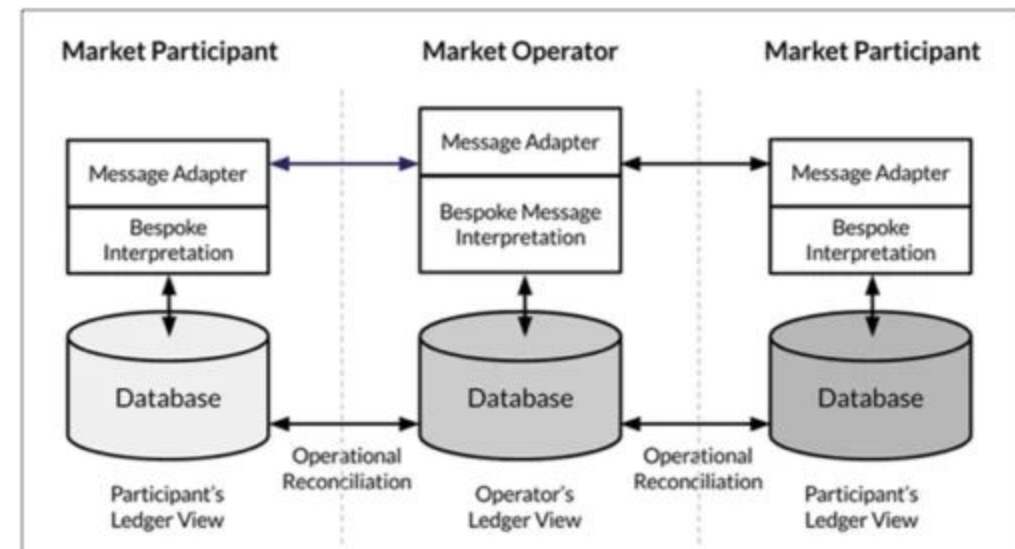
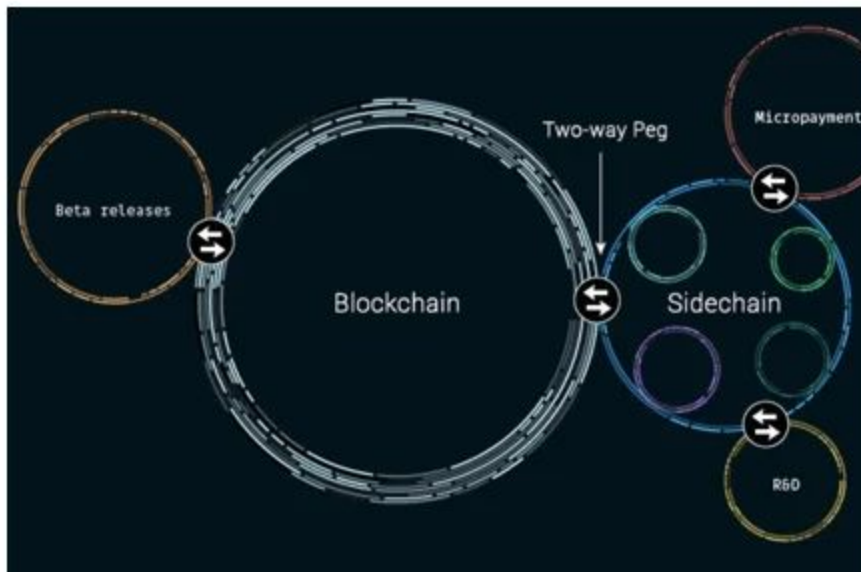
Join the Global Settlement Network

Instant, certain, low-cost international payments

Digital Asset

BUSINESS APPLICATIONS

ASSET SPECIFIC, BEHAVIOR AND BUSINESS LOGIC PLUGINS

The diagram shows several dark, rectangular blocks representing digital assets, each with a unique label like 'DA-BLE-FX' and 'DA-BLE-LOANS'. These blocks are arranged in a cluster, with blue lines extending downwards from them, suggesting a connection to a network or database.

Money Transfer



DEPOSIT

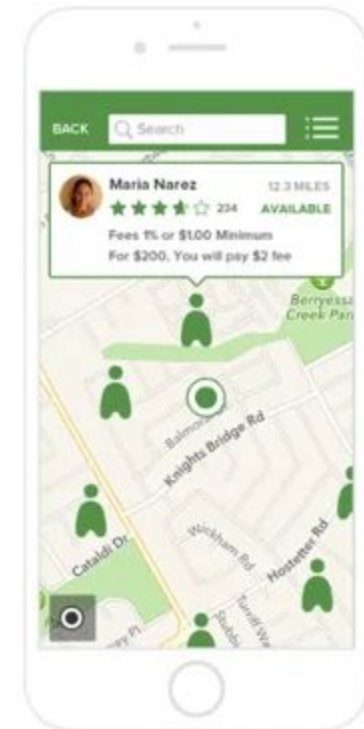
Fund your wallet with your bank account or use cash by visiting an Abra Teller in your area.

SEND

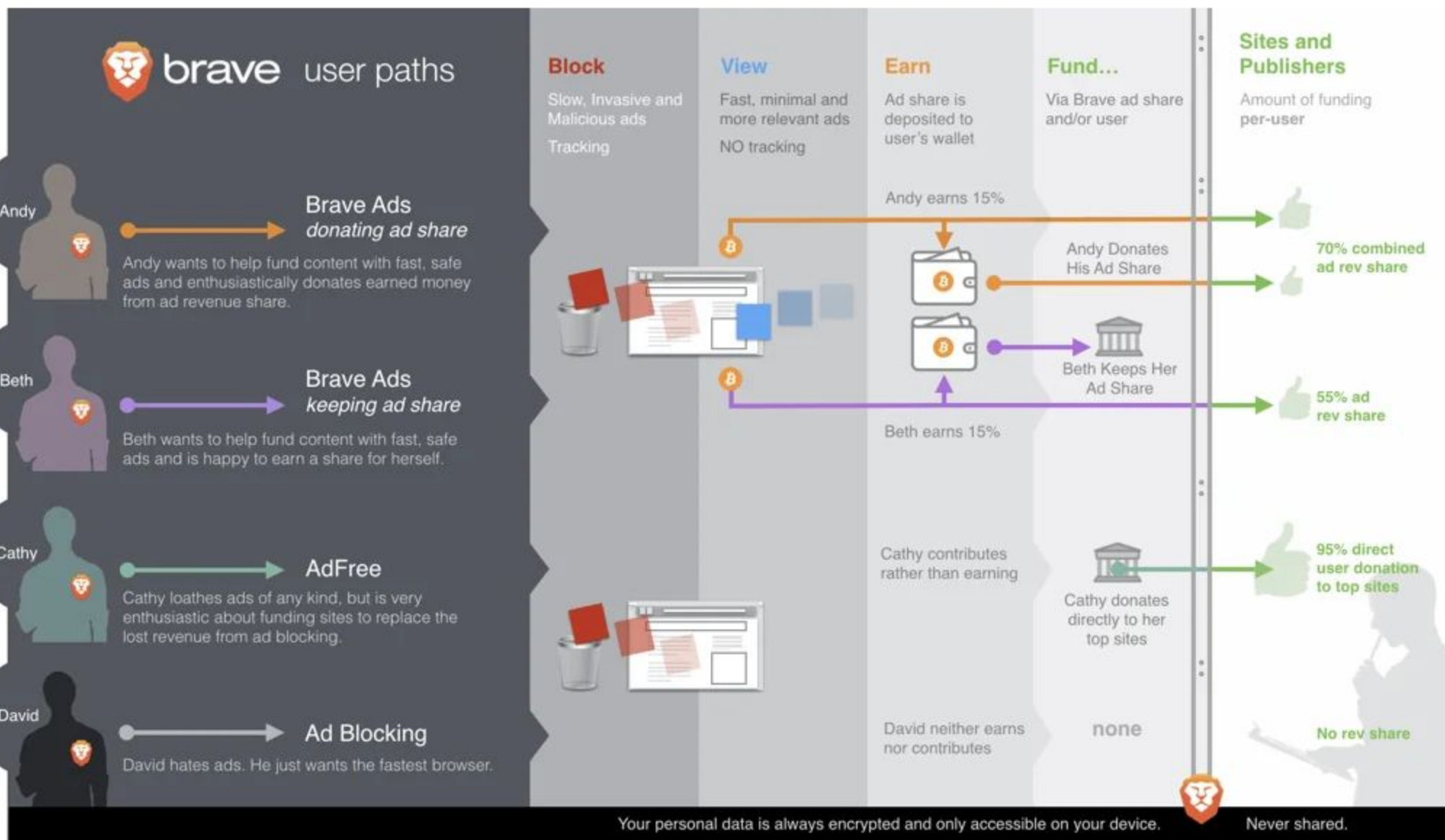
Use the Abra app to send or receive money worldwide with no fees. Buy things online wherever Abra is accepted.

WITHDRAW

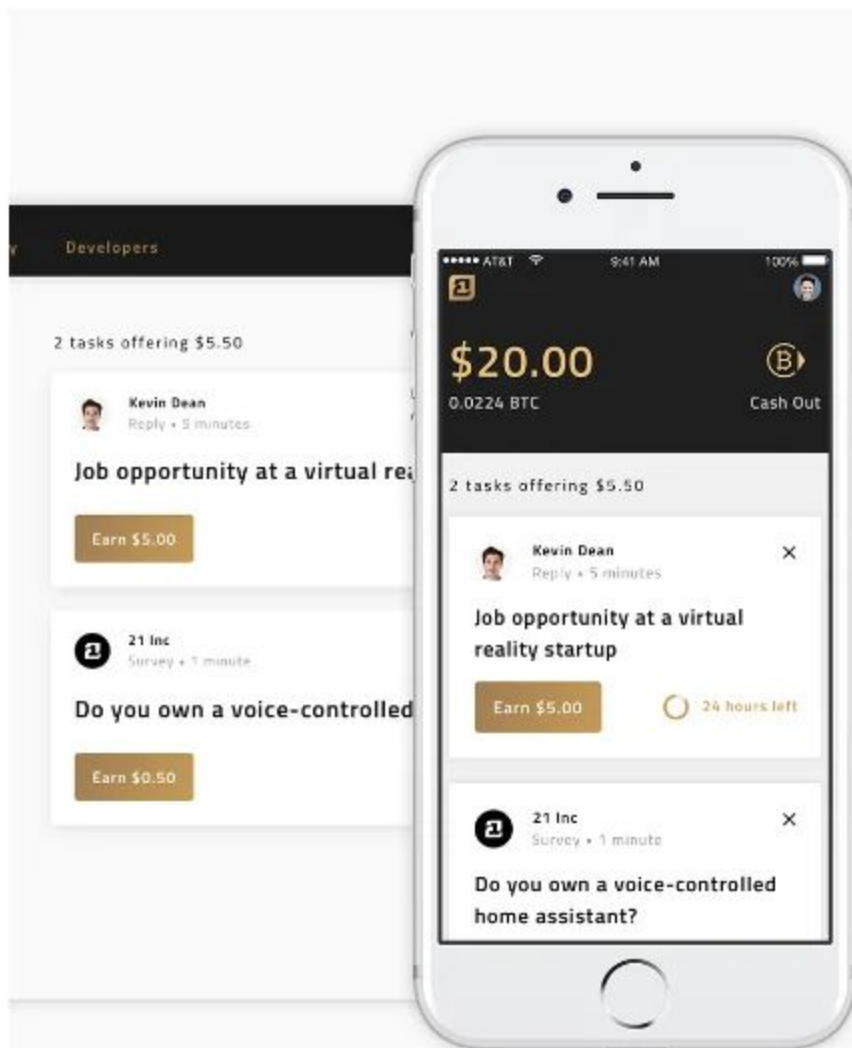
Use the app to transfer funds to your bank account, or find a nearby Teller to get cash.



Micropayments



Crowdsourcing



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.

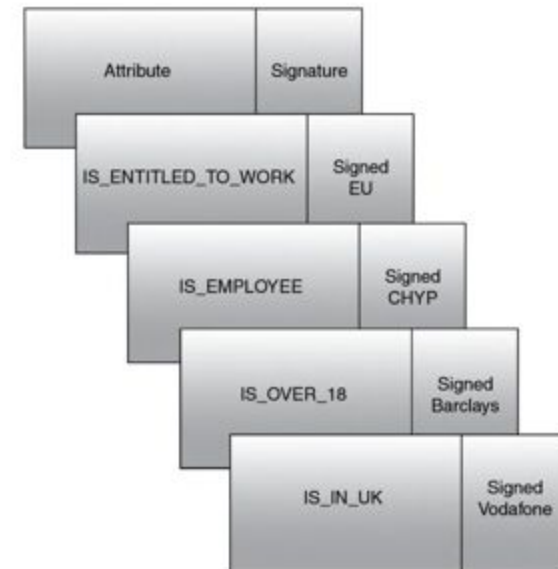
According to documents filed with the United States District Court in Minnesota this month, shoppers affected by the breach could be awarded up to \$10,000 each in damages. The settlement includes a draft of the form victims must complete to make claims, processed through a dedicated website.

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.

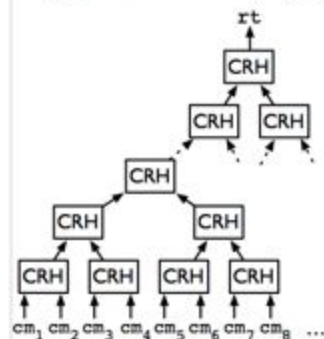
Molly Snyder, a Target spokeswoman, said, "We are pleased to see the process moving forward and look forward to its resolution." The pending settlement was first reported by CNBC.



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



(a) Merkle tree over $(cm_1, cm_2, \dots)$

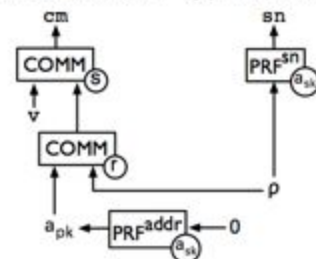


(b) coin

$$c = ((a_{pk}, pk_{enc}), v, p, r, s, cm)$$

(c) coin commitment

(d) serial number



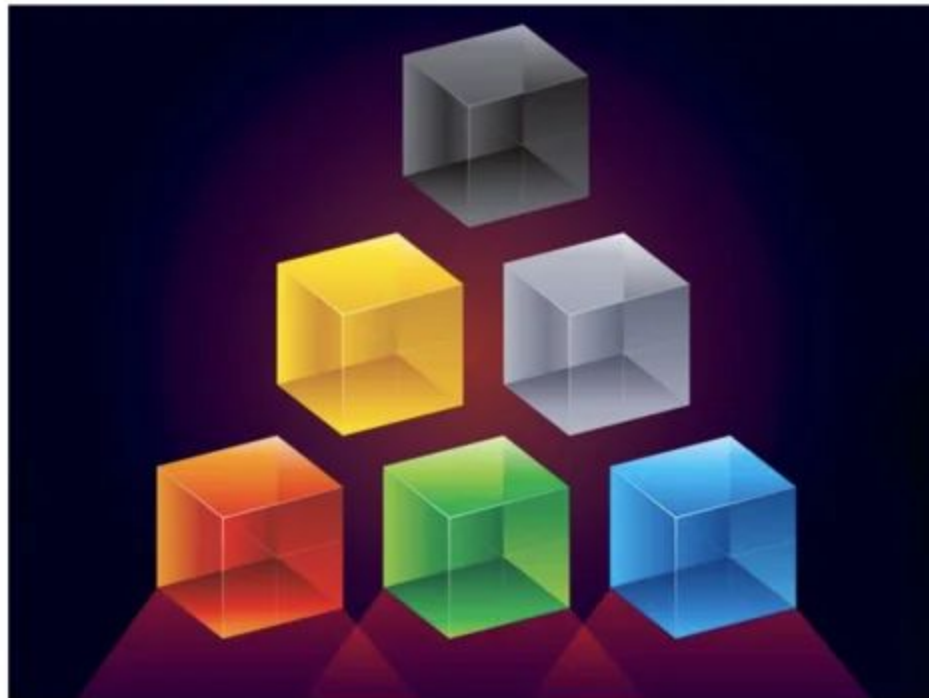
rt = Merkle-tree root
 cm = coin commitment
 sn = serial number
 v = coin value
 r, s = commitment rand.
 p = serial number rand.
 (a_{pk}, pk_{enc}) = address public key
 (a_{sk}, sk_{enc}) = address secret key

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

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...

X

Provenance

The image shows the top section of the Everledger website. It features a dark background with a close-up of a diamond being examined under a magnifying glass. The Everledger logo is in the top left, and navigation links are in the top right. The main headline is 'Welcome to the digital vault of the future.' followed by a paragraph about the company's technology and a 'FIND OUT MORE' button.

everledger

What We Do Our Journey Our Technology Press Coverage Contact

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.

FIND OUT MORE

DealB%k WITH FOUNDER ANDREW ROSS SCHWEN

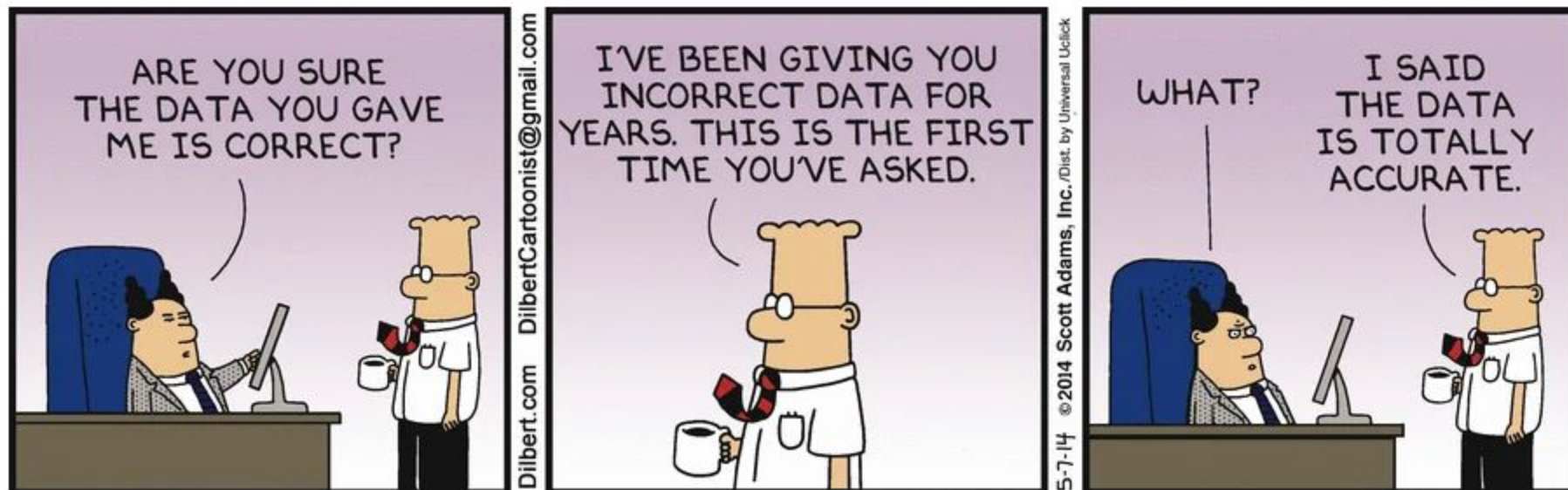
Blockchain: A Better Way to Track Pork Chops, Bonds, Bad Peanut Butter?

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 Ross Schwab for The New York Times

Provenance



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 appropriate. 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

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**

May 10, 2015

16 COMMENTS

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.



Dec 30, 2015

◀ Previous Release | Next Release ▶



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...



```
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]
```

A screenshot of the Namecoin website. The header includes the Namecoin logo and navigation links: Home, Video, Exchanges, Download, and a partially visible "For" link. The main banner features the text "Decentralize all the things!" in large white letters on a dark background. Below this, a paragraph states: "Namecoin is a decentralized open source internet registration and transfer system based on the cryptocurrency." Two columns of bullet points follow. The left column, titled "What does it do?", lists: "Securely record and transfer arbitrary names (keys)." and "Attach a value (data) to the names (up to 520 bytes, more in the future)." The right column, titled "What can it be used for?", lists: "Protect free-speech rights, make the web more resistant to censorship." and "Access websites using the Namecoin protocol (via TLS/SSL)."

namecoin Home Video Exchanges Download For

Decentralize all the things!

Namecoin is a decentralized open source internet registration and transfer system based on the cryptocurrency.

What does it do?

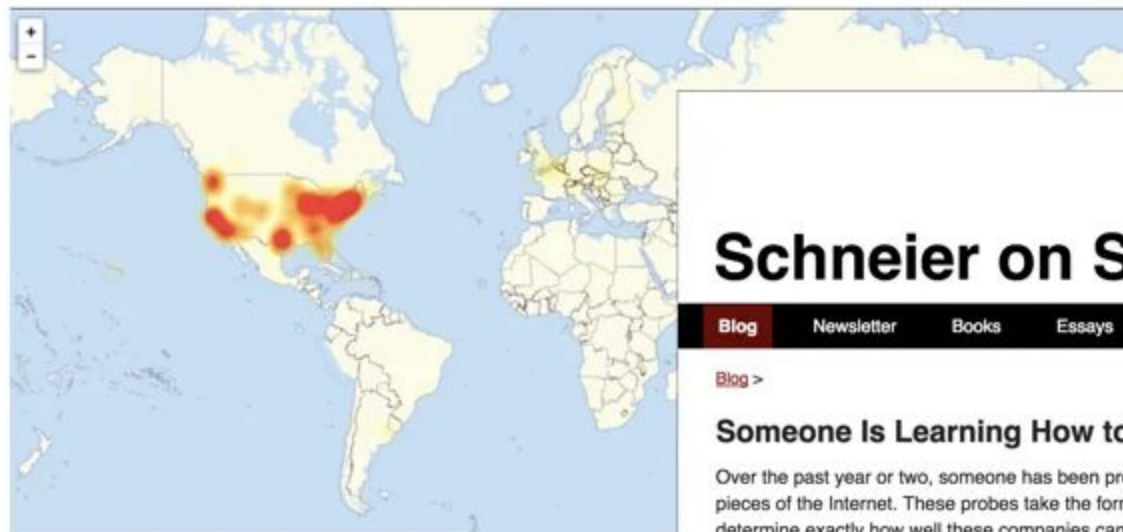
- Securely record and transfer arbitrary names (keys).
- Attach a value (data) to the names (up to 520 bytes, more in the future).

What can it be used for?

- Protect free-speech rights, make the web more resistant to censorship.
- Access websites using the Namecoin protocol (via TLS/SSL).

Internet Attack Disrupts Major Websites

By NICOLE PERLROTH OCT. 21, 2016



A map of the areas experiencing problems, as of Friday afternoon, according to...

Schneier on Security

[Blog](#) [Newsletter](#) [Books](#) [Essays](#) [News](#) [Talks](#) [Academic](#) [About Me](#)

[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.

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



BLOCKSTACK

[Intro](#)
[Docs](#)
[Blog](#)
[Papers](#)
[Videos](#)

Build on the New Internet

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

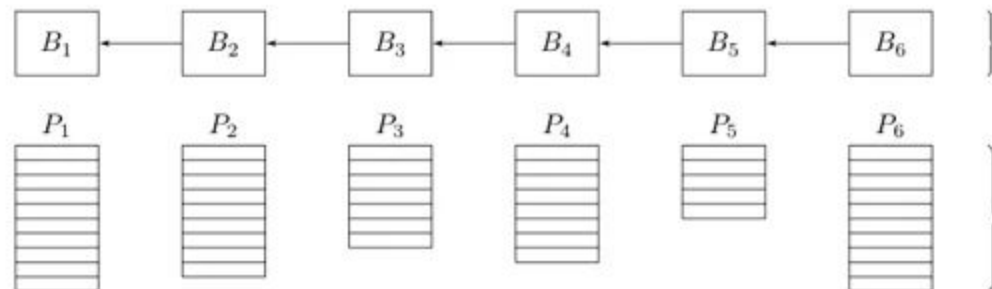
[Join the Community](#)
[Install the Software](#)

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

The Filecoin logo features a teal circle with a white 'f' symbol. Below it, the text 'Filecoin' is written in white. A description states: 'Filecoin is a data storage network and electronic currency based on Bitcoin'. Three icons are shown: a hard drive, a server rack, and a circular arrow with a Bitcoin symbol. Below each icon is a description: 'Earn Filecoin by renting disk space', 'Use Filecoin to store files in the network or to transact', and 'Exchange Filecoin currencies, like Bitcoin'.

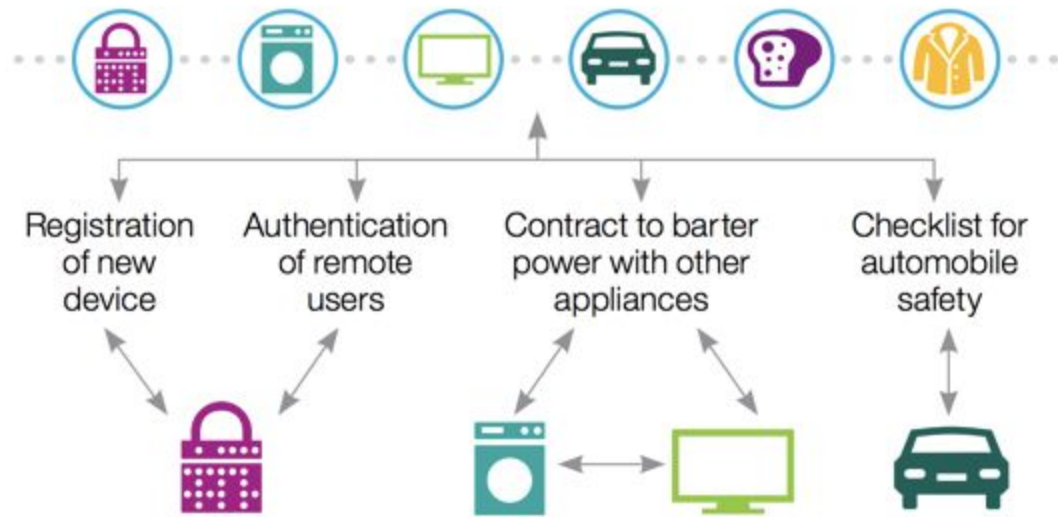
...or Sensors

Sensor21: Earn bitcoin by collecting environmental data

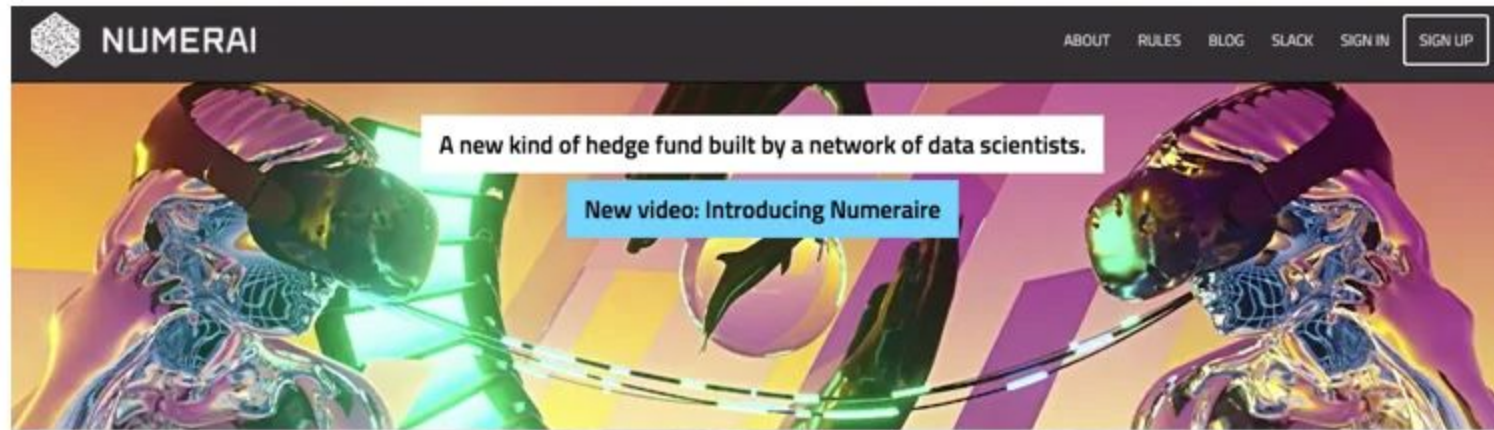
By Tyler Pate, Jeremy Kun, and Balaji S. Srinivasan



Internet of Things, Robotics, AI



The Firm as a Nexus of Contracts



NUMERAIR

ABOUT RULES BLOG SLACK SIGN IN SIGN UP

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

New video: Introducing Numeraire

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

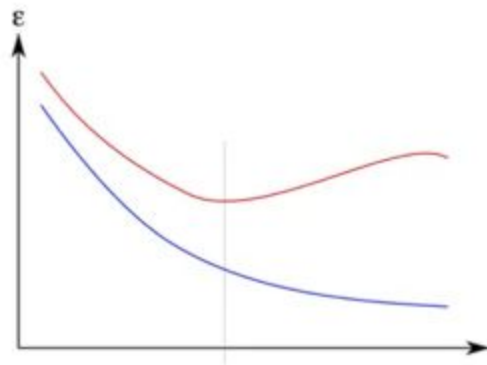


Figure 1: An overfitting curve where the blue test error continues to decrease with more submissions from data scientists, but the error on new data increases. [2]



Thank You!

catalini@mit.edu
blockchain.mit.edu

