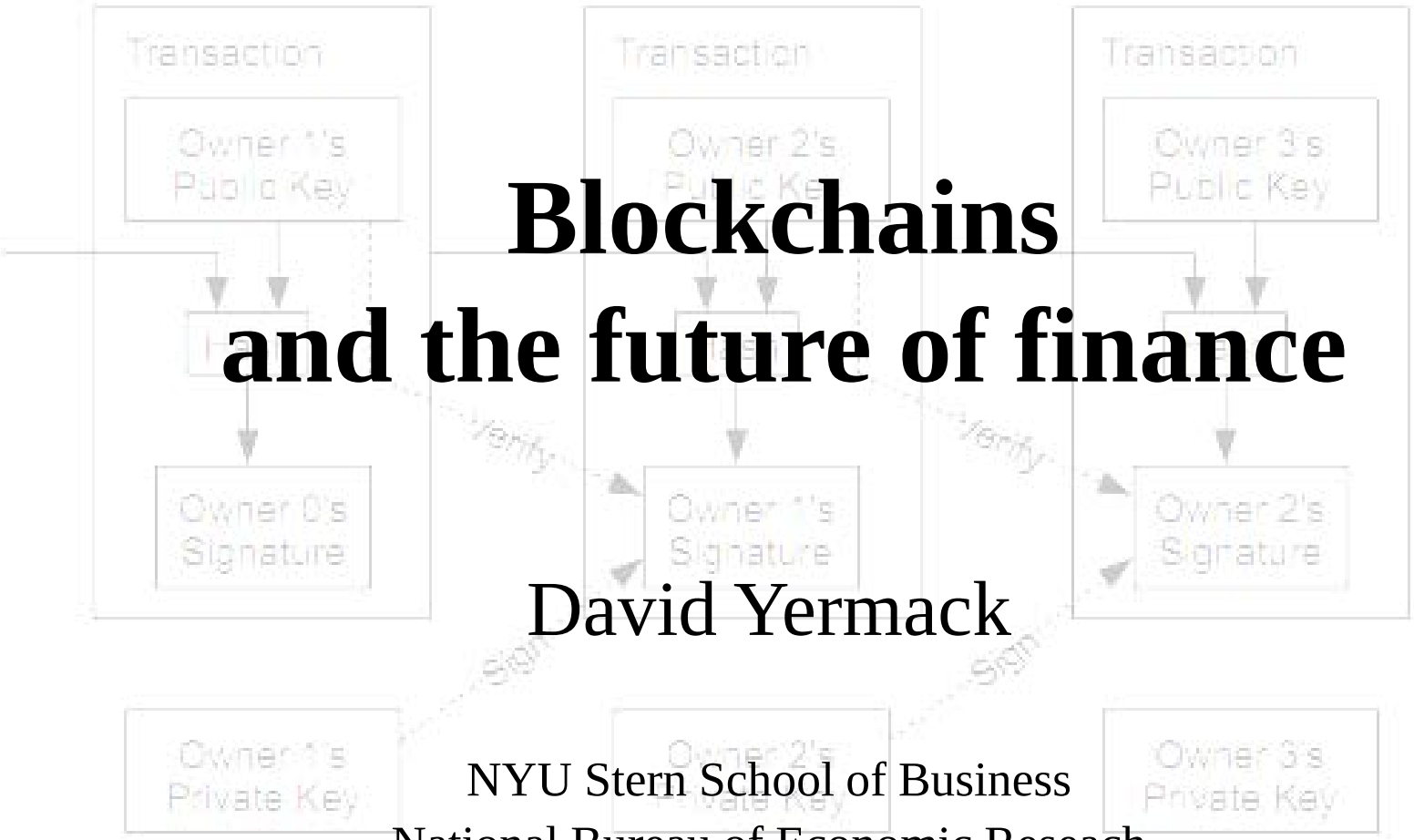


Blockchains and the future of finance

David Yermack

NYU Stern School of Business
National Bureau of Economic Reseach

FinTech

UBS's trading floor, Stamford, Ct., USA

2005

2016

The blockchain

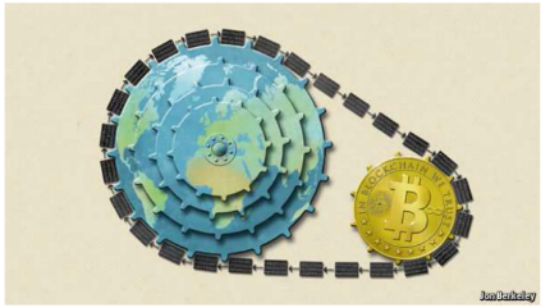
The Economist

The promise of the blockchain

The trust machine

The technology behind bitcoin could transform how the economy works

Oct 31st 2015 | From the print edition



BITCOIN has a bad reputation. The decentralised digital cryptocurrency, powered by a vast computer network, is notorious for the wild fluctuations in its value, the zeal of its supporters and its degenerate uses, such as extortion, buying drugs and hiring hitmen in the online bazaars of the "dark net".

This is unfair. The value of a bitcoin has been pretty stable, at around $250, for most of this year. Among regulators and financial institutions, scepticism has given way to enthusiasm (the European Union recently recognised it as a currency). But most unfair of all is that bitcoin's shady image causes people to overlook the extraordinary potential of the "blockchain", the technology that underpins it. This innovation carries a significance stretching far beyond cryptocurrency. The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority. Simply put, it is a machine for creating trust.

When will the blockchain get here?

Daimler Benz's blockchain bond issue

June 2017

German automaker Daimler AG has issued a corporate bond worth €100m as part of a blockchain pilot project.

The carmaker announced the completed test today, working alongside Landesbank Baden-Württemberg (LBBW), Germany's largest state-backed wholesale banks group, to create a testbed for issuing the one-year corporate bond known as a Schuldschein.

According to Daimler, the entire transaction cycle – from origination, distribution, allocation and execution of the loan agreement, to the confirmation of repayment and of interest payments – was automated digitally through the blockchain network. Lending technical support were the IT subsidiaries of Daimler and LBBW, which also adopted the blockchain's cryptographic signature to prevent manipulation of transactions.

Daimler and LBBW are now looking at other applications, including the issuance of syndicated loans by way of a distributed ledger.

Maersk's blockchain marine insurance

September 2017

Shipping Giant Maersk to Deploy Blockchain Maritime Insurance Solution

Sep 6, 2017 at 12:06 UTC by Rachel Rose O'Leary

A joint venture between shipping giant Maersk, Microsoft, accounting firm EY and blockchain firm Guardtime aims to apply blockchain technology in the field of marine insurance.

Built using Azure – Microsoft's cloud-based platform that recently revealed a new blockchain framework – the new effort will see the creation of a shared database that logs information about shipments, as well as potential risks, in order to help ships comply with insurance regulations. The database would also insure that this information is transparent across what is a complex network of variables.

Notably, the project has already been trialled, and Maersk plans to use it in real-world applications, along with insurers MS Amlin and XL Catlin, according to Reuters.

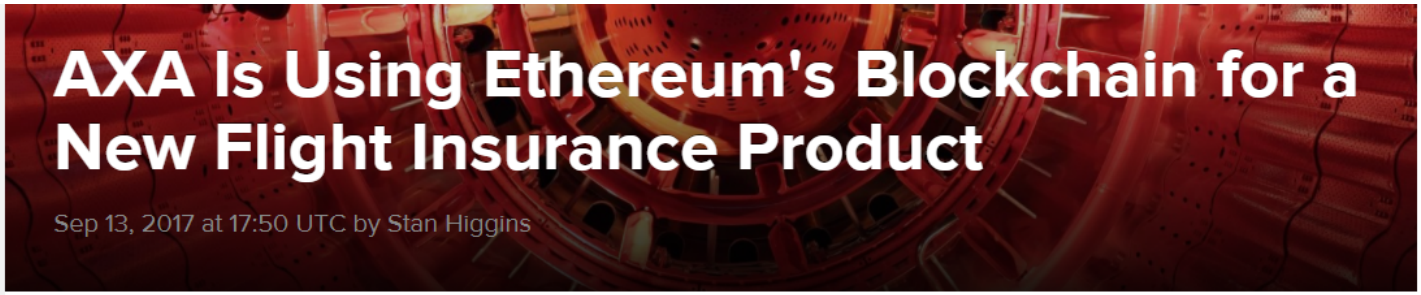
EY told CNBC that securing marine insurance data with blockchain was necessary due to the "complete inefficiency" of the industry.

Mark Russinovish, chief technology officer at Microsoft Azure, explained further:

> *"Marine insurance is a prime example of a complex business process that can be optimized with blockchain."*

AXA's smart contract flight insurance

September 2017



AXA Is Using Ethereum's Blockchain for a New Flight Insurance Product

Sep 13, 2017 at 17:50 UTC by Stan Higgins

French insurance giant AXA has launched a new flight delay insurance product that uses the public ethereum blockchain to store and process payouts.

The product, called Fizzy, is being pitched as a "smart insurance" tool that flyers can use to insure their trips if their flight is delayed by two hours or more. As such, the product makes notable use of smart contracts, self-executing piece of code that triggers once certain conditions are met on a blockchain.

According to AXA, ethereum's public blockchain plays two key roles here. It maintains an accessible record of the insurance contract itself within a smart contract, and serves as a mechanism for triggering the payment to the client once the two-hour mark is passed.

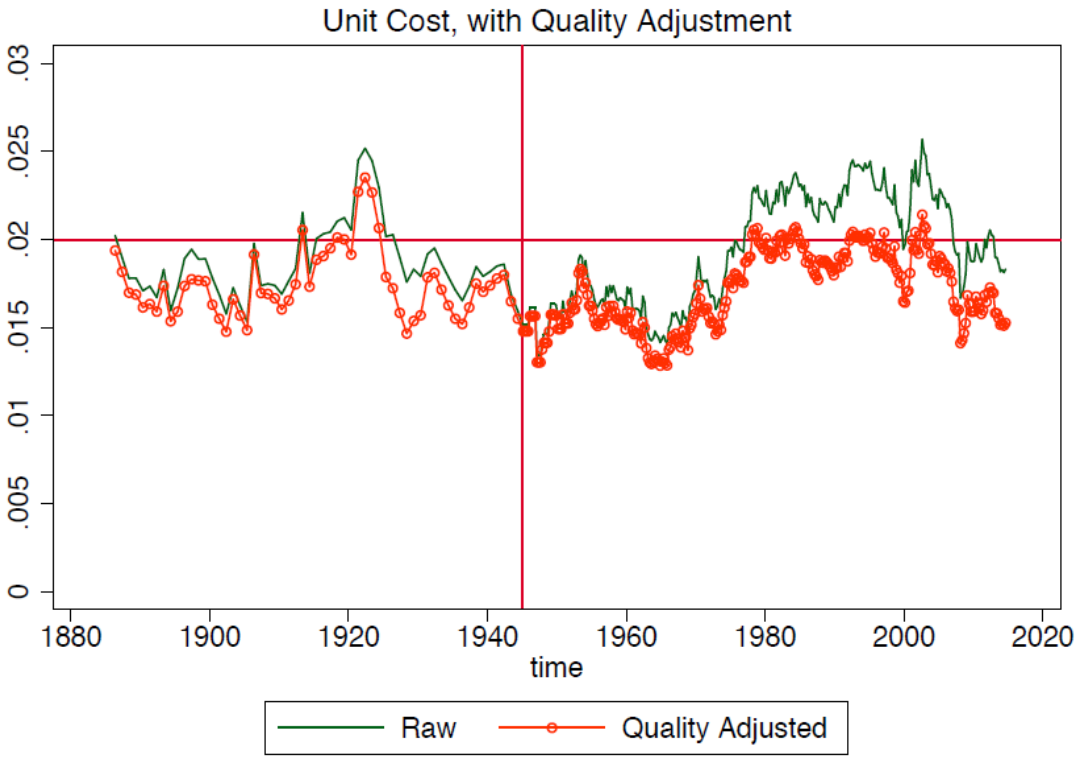
AXA representative Jean-Baptiste Mounier told CoinDesk in an email:

> *"The smart contract is the party that decides whether or not we should indemnify the policy holder and triggers a payment request to our system. The use of a smart contract to trigger claims will add trust in the insurer / policy holder relationship."*

The cost of financial transactions

A long view: 1886-2015

- 2% per transaction, unchanged for 130 years



Source: Philippon (2016)

Stability of the financial system

1873

1932

2007

Intelligent redesign of the financial system

Bitcoin network is launched, January 3, 2009

Bitcoin: A Peer-to-Peer Electronic Cash System

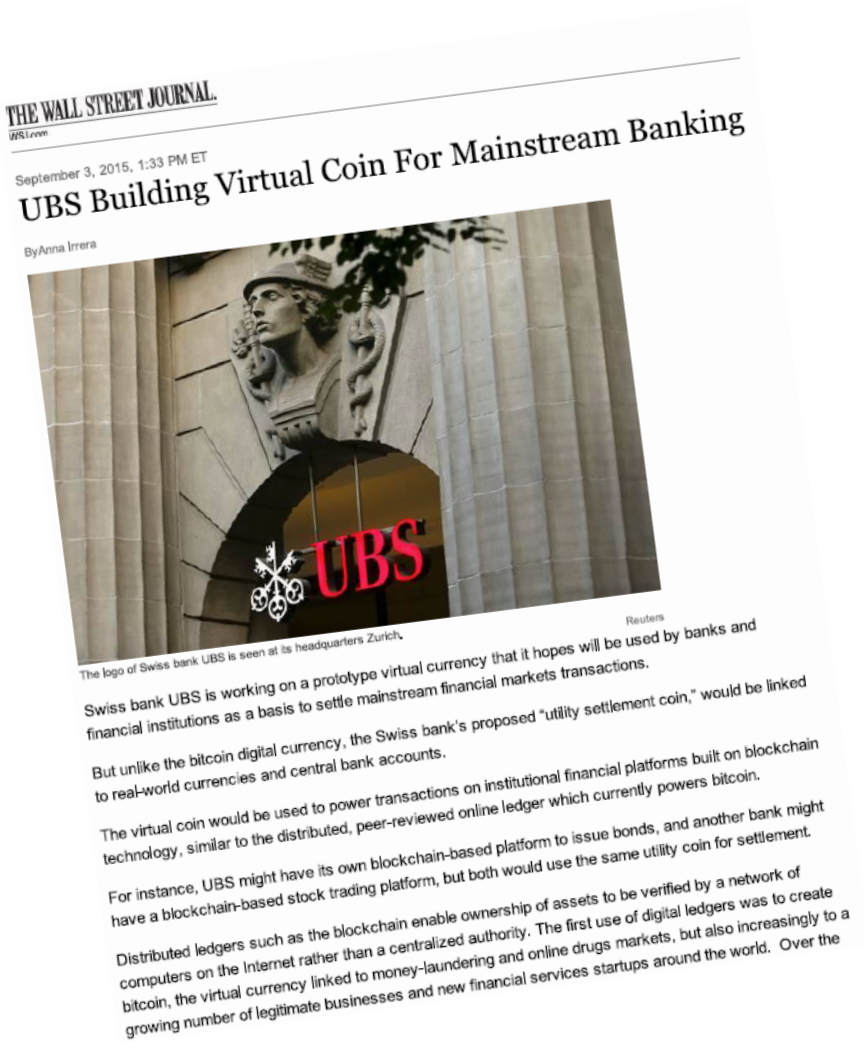
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

What is Bitcoin?

- A stateless, decentralized, “algorithmic” currency
- That exists only in cyberspace
- Major demand is in U.S., China, and certain European countries
- Bitcoin / USD exchange rate:
  - July 17, 2010 1 Bitcoin = $0.05
  - September 6, 2017 1 Bitcoin = $3,918.09

A disruptive technology



THE WALL STREET JOURNAL.

September 3, 2015, 1:33 PM ET

UBS Building Virtual Coin For Mainstream Banking

By Anna Irrera

The logo of Swiss bank UBS is seen at its headquarters Zurich. Reuters

Swiss bank UBS is working on a prototype virtual currency that it hopes will be used by banks and financial institutions as a basis to settle mainstream financial markets transactions.

But unlike the bitcoin digital currency, the Swiss bank's proposed "utility settlement coin," would be linked to real-world currencies and central bank accounts.

The virtual coin would be used to power transactions on institutional financial platforms built on blockchain technology, similar to the distributed, peer-reviewed online ledger which currently powers bitcoin.

For instance, UBS might have its own blockchain-based platform to issue bonds, and another bank might have a blockchain-based stock trading platform, but both would use the same utility coin for settlement.

Distributed ledgers such as the blockchain enable ownership of assets to be verified by a network of computers on the Internet rather than a centralized authority. The first use of digital ledgers was to create bitcoin, the virtual currency linked to money-laundering and online drugs markets, but also increasingly to a growing number of legitimate businesses and new financial services startups around the world. Over the

"... The blockchain has been increasingly eyed by mainstream financial institutions as a breakthrough.

... it could enable financial institutions to settle trades in seconds rather than two or three days

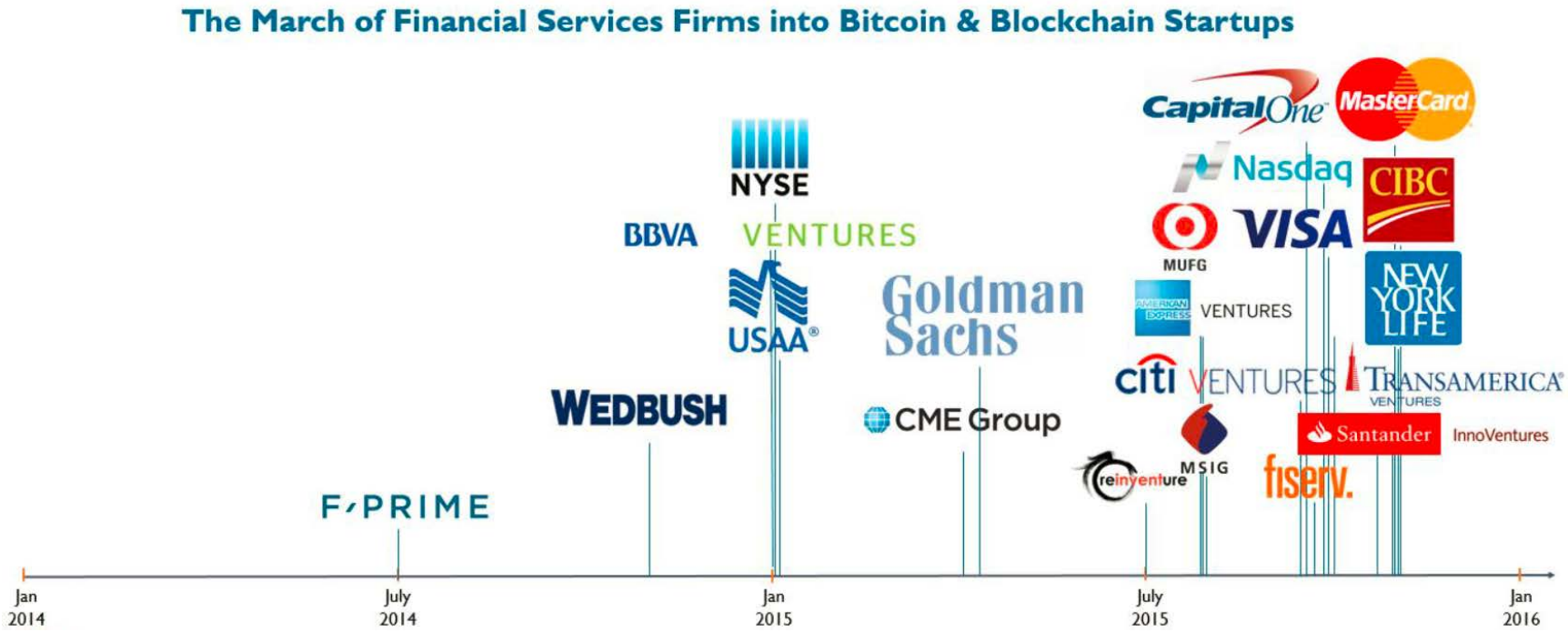
... blockchain technology could reduce the bank's infrastructure costs ... **by as much as $20 billion a year** by 2022."

What could become unnecessary in a world with blockchains?

- No more banks
- No more stock exchanges
- No more government property registers
- No more accountants and auditors
- Far fewer lawyers
- Etc…

Wall Street discovers the blockchain

The gold rush begins, late 2015



High profile examples:
ASX stock exchange, Sydney

Morgan Stanley
GLOBAL INSIGHT

June 2, 2016

Global Exchanges

Global Insight: Blockchain - Is ASX set to shape a brave new world?

ASX is pioneering a blockchain proof of concept, with a "go or no go" decision by mid-2017. If successful, innovation in the global US$77bn post-trade market would increase, impacting exchanges. Vertically integrated exchanges are best placed to shape the market.

ASX

Media Release

22 January 2016

ASX SELECTS DIGITAL ASSET TO DEVELOP DISTRIBUTED LEDGER TECHNOLOGY FOR THE AUSTRALIAN EQUITY MARKET

ASX Limited (ASX) today announced that it has selected US-based firm Digital Asset Holdings, LLC (Digital Asset) to develop solutions for the Australian market utilising Distributed Ledger Technology.

ASX has joined 12 other global financial services leaders and made a minority investment in Digital Asset. ASX has paid A$14.9 million to acquire a 5% equity interest in Digital Asset, fund an initial phase of development, and acquire a warrant that will give ASX the right to purchase further equity and appoint a director to the board. The warrant is exercisable if certain conditions are met.

In February 2015, ASX announced that it would replace or upgrade all of its main trading and post-trade platforms. Phase 1 of the program runs to the end of 2016 and will replace ASX's existing trading and risk management systems.

Phase 2 focuses on ASX's post-trade services, including clearing and settlement of the cash equities market. The system that currently provides the clearing and settlement services to the Australian equity market is known as CHESS.

ASX will work with Digital Asset to design a new post-trade solution for the Australian equity market.

High profile examples:
BHP Billiton supply chain management

World's Largest Mining Company to Use Blockchain for Supply Chain

The world's largest mining firm by market value intends to begin using the ethereum blockchain to improve its supply chain processes.

BHP Billiton revealed at the second annual Global Blockchain Summit that it will use blockchain to record movements of wellbore rock and fluid samples and better secure the real-time data that is generated during delivery. According to BHP geophysicist R Tyler Smith, the new system will enable benefits for its internal efficiency while allowing it to work more effectively with partners.

Smith explained that BHP relies on vendors at nearly every stage in the mining process, contracting with geologists and shipping companies to collect samples and conduct analyses that drive business decisions that occur with parties distributed across continents.

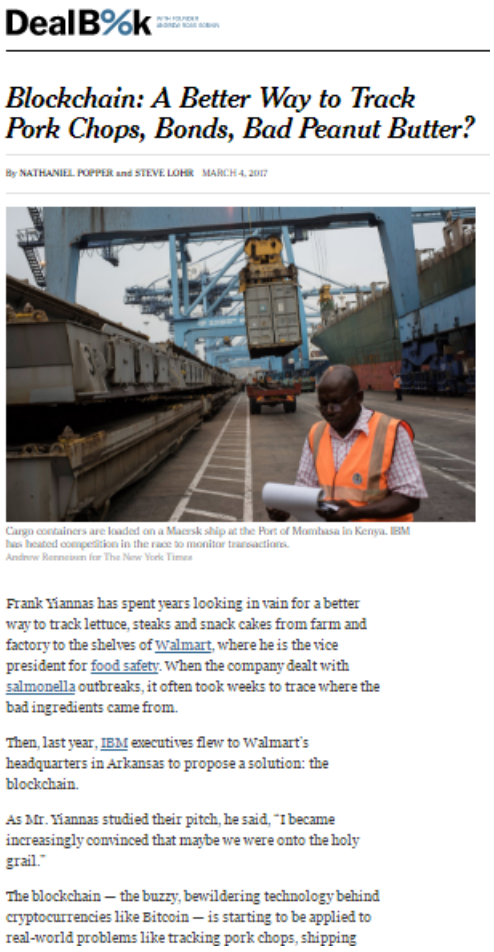
"With blockchain, we would share data between the vendor and ourselves, and have a constant understanding of where it is," Smith told CoinDesk, adding:

> *"Everything right now is being tracked through spreadsheets."*

High profile examples:
IBM's "blockchain garage," Manhattan

- 400 clients testing blockchain solutions to logistics and supply chain management

- 650 staff dedicated to this technology



DealB%k

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

Frank Yiannas has spent years looking in vain for a better way to track lettuce, steaks and snack cakes from farm and factory to the shelves of Walmart, where he is the vice president for food safety. When the company dealt with salmonella outbreaks, it often took weeks to trace where the bad ingredients came from.

Then, last year, IBM executives flew to Walmart's headquarters in Arkansas to propose a solution: the blockchain.

As Mr. Yiannas studied their pitch, he said, "I became increasingly convinced that maybe we were onto the holy grail."

The blockchain — the buzzy, bewildering technology behind cryptocurrencies like Bitcoin — is starting to be applied to real-world problems like tracking pork chops, shipping

High profile examples:
Authentication of gems, art, luxury goods

High profile examples:
Bank of Canada (and many other governments)

FINANCIAL TIMES

Canada experiments with digital dollar on blockchain

Country's central bank poised to embrace technology behind bitcoin

High profile examples:
Peer-to-peer distribution of electric power

Power Ledger expands trials of blockchain electricity trading

By Jonathan Gifford on 28 October 2016

West Australian software developer Power Ledger is currently applying its blockchain-based software in an attempt to open up peer-to-peer (P2P) energy trading behind the meter and across the network.

Peer to peer

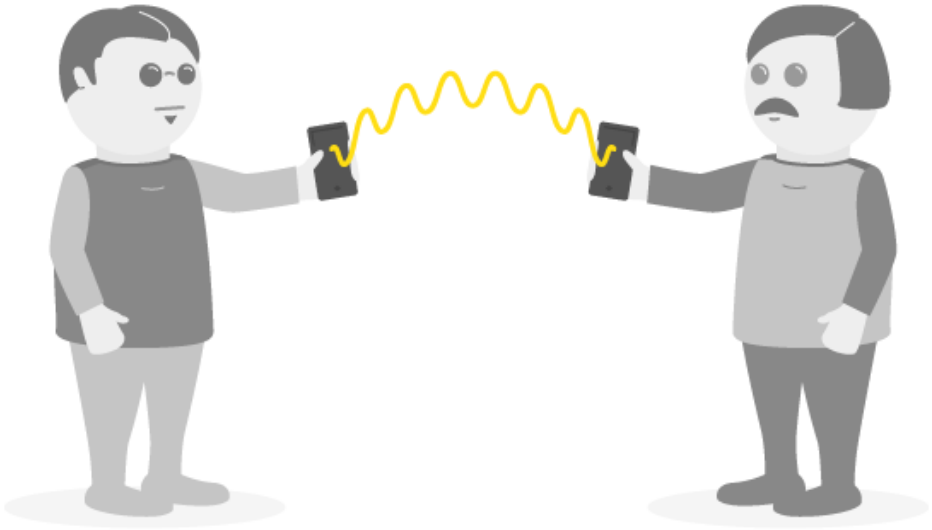
- The early breakthroughs

- Now

Peer to peer payments

PayPal

M-PESA



Peer to peer payments: who guarantees and regulates them?

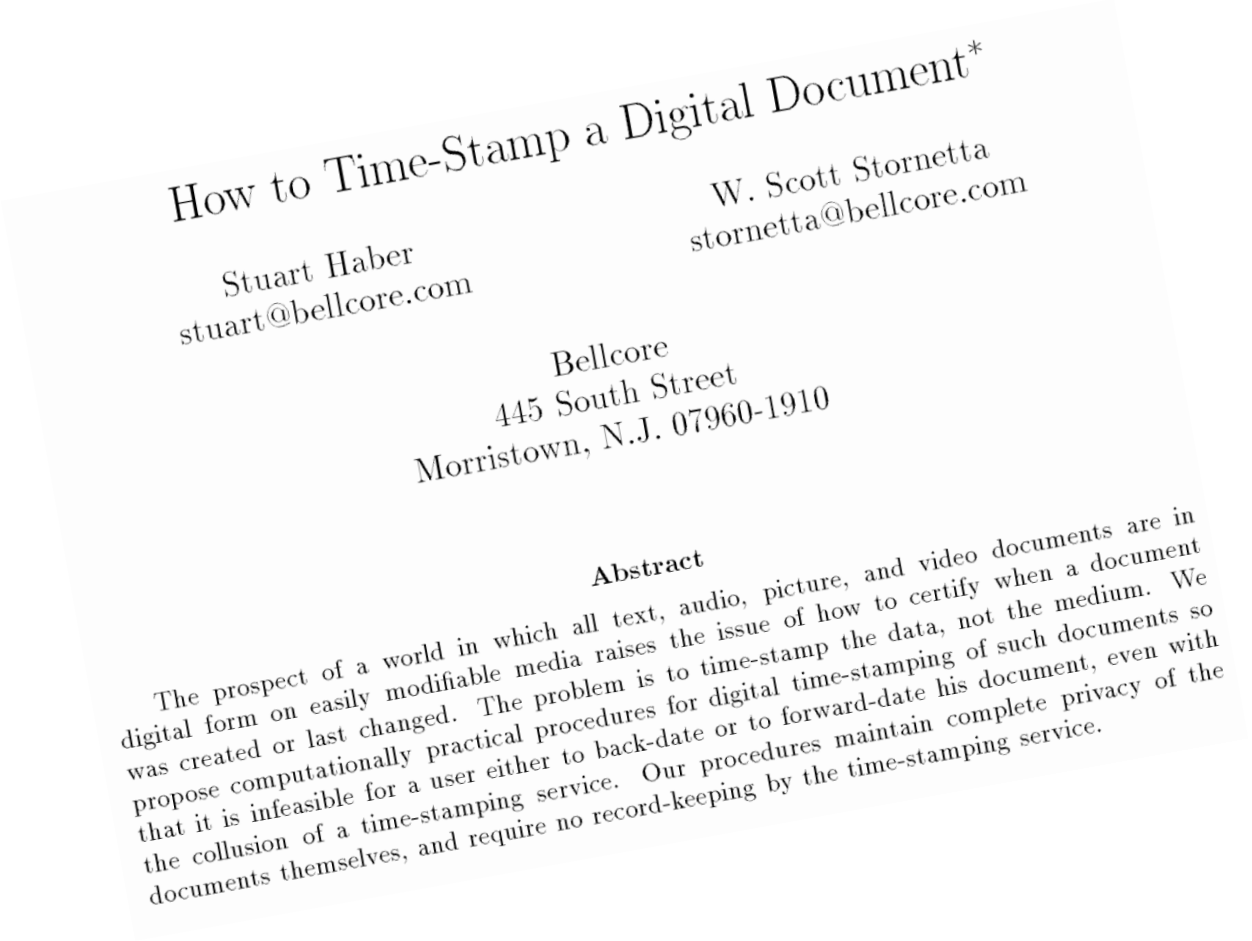
Credit card companies

Mobile phone companies

Consensus of the network

The original blockchain

Authenticating digital documents – Haber & Stornetta (1991)



How to Time-Stamp a Digital Document*

Stuart Haber
stuart@bellcore.com

W. Scott Stornetta
stornetta@bellcore.com

Bellcore
445 South Street
Morristown, N.J. 07960-1910

Abstract

The prospect of a world in which all text, audio, picture, and video documents are in digital form on easily modifiable media raises the issue of how to certify when a document was created or last changed. The problem is to time-stamp the data, not the medium. We propose computationally practical procedures for digital time-stamping of such documents so that it is infeasible for a user either to back-date or to forward-date his document, even with the collusion of a time-stamping service. Our procedures maintain complete privacy of the documents themselves, and require no record-keeping by the time-stamping service.

Using a blockchain for payments

Nakamoto (2008)

"Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments . . . What is needed is an electronic payment system based on cryptographic proof instead of trust."

Time	Digital Signature(s) used in current transaction:	Source Address (controlled by current signatory)	Reference to prior tranaction	Recipient Address	Data	Bitcoins at source address prior to transaction	Bitcoins Sent to Recipient	Fee to Verif Agent	Signature(s) required for next transaction:
2:59:38 PM	*Tammy Tone*	1Zefew		1estgE	[a secret]	0.050	0.020	0.015	Person A or B
2:53:31 PM	*John Smith*	1wEfet		1ewYUe	null	25.000	6.000	0.010	Frank Xao
2:52:37 PM	*Joe Bookie*	1Nuyts		1wEfet	[bet winner]	87.500	25.000	0.020	John Smith
2:52:25 PM	*John Smith*	1EWseg		1Nuyts	[sports bet]	12.515	12.500	0.015	Joe Bookie
2:51:04 PM	*Frank Heinz*	1Wefvs		1EWseg	null	18.000	12.515	0.015	John Smith

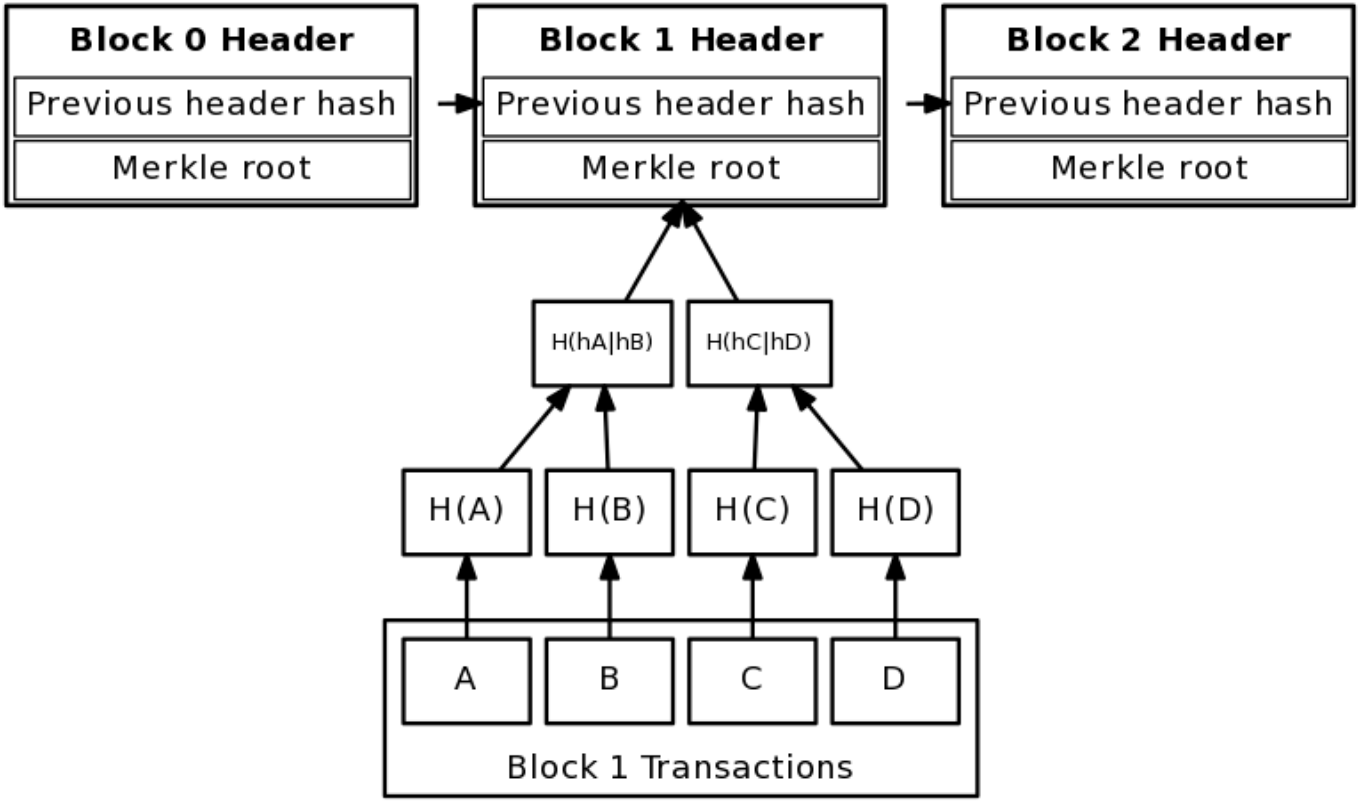
Links to addresses further down in the blockchain

Not all entries are required at all times but some must always be included (examples: signatures, references to prior updates)

Source: SolidX Partners Inc.

Grouped into *blocks* every 10 minutes

About 1,500 transactions currently in each Bitcoin block

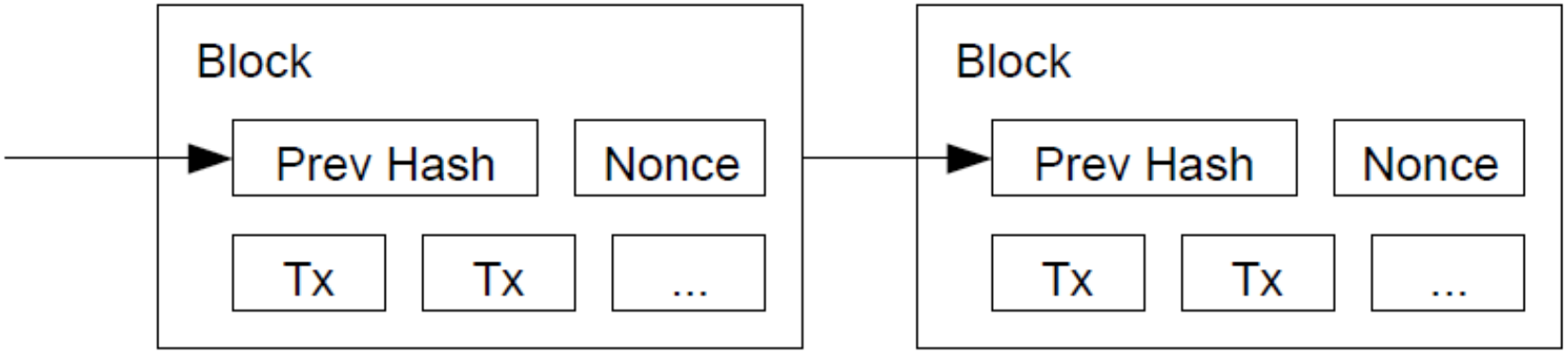


Merkle tree connecting block transactions to block header merkle root

Source: bitcoin.stackexchange.com

How the blocks are *chained*

The hash code of each previous block is included in the next; changes to data in any block ripple through the entire chain



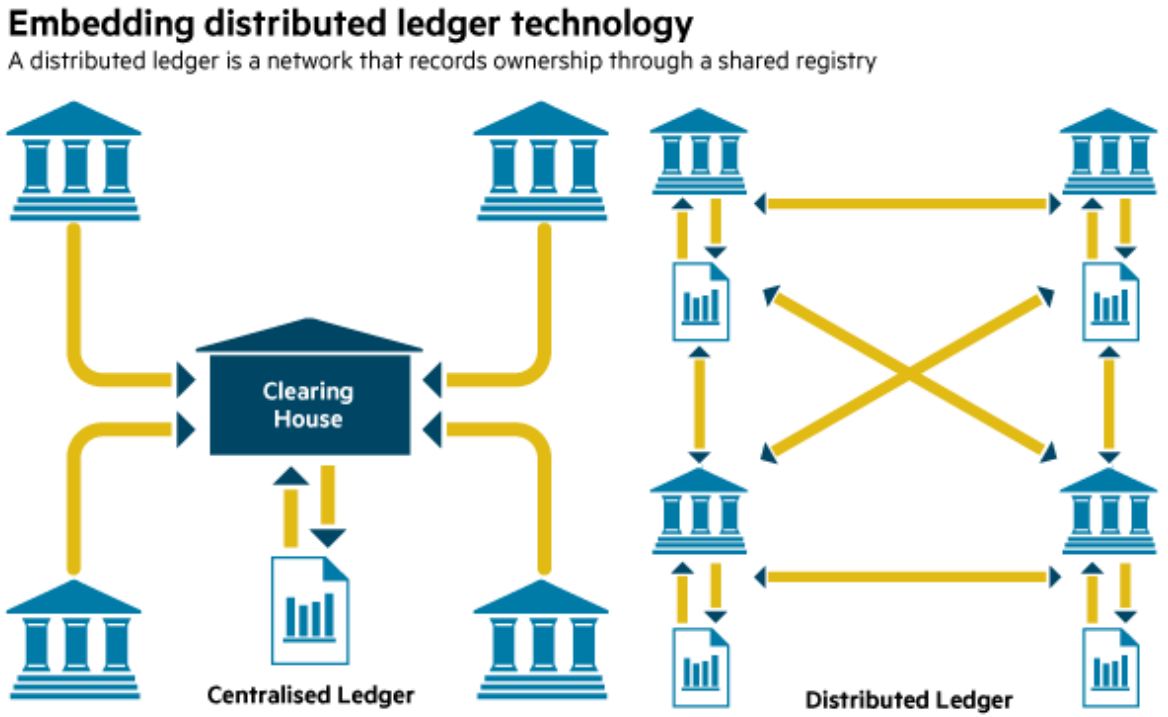
Source: bitcoin.stackexchange.com

Who updates the blockchain?

- Haber and Stornetta (1991)
  - A ***trusted third party*** takes responsibility for coding blocks
  - The chain is posted publicly, becoming a ***distributed ledger*** that can be verified by anyone

- Nakamoto's (2008) crowd-sourcing solution
  - ***Network members compete*** to create new blocks
  - Anyone can join the network and take part
  - A reward goes to the fastest
    (seigniorage of new coins)

A distributed ledger with shared responsibility for updating



In contrast to today's networks, distributed ledgers eliminate the need for central authorities to certify ownership and clear transactions. They can be open, verifying anonymous actors in the network, or they can be closed and require actors in the network to be already identified. The best known existing use for the distributed ledger is the cryptocurrency Bitcoin

FT graphic. Source: Santander InnoVentures, Oliver Wyman & Anthemis Partners

Why eliminate the "trusted third party"?

- No gatekeeper controls access
  - Could exclude certain agents
  - Could play favorites, in exchange for side payments
- No monopolist transaction fees
- No ability to change the ledger arbitrarily
- No single point of failure vulnerable to hacking, operator error or hardware failure
- No rationing of market hours; available 24-7-365
- Greater user control over data

Two kinds of blockchains

Open

- Anyone can opt in
- Decentralized governance
- Size is endogenous
- Blocks updated via competition
  - Organic rewards to miners
  - Bidding by users to advance in queue

Permissioned

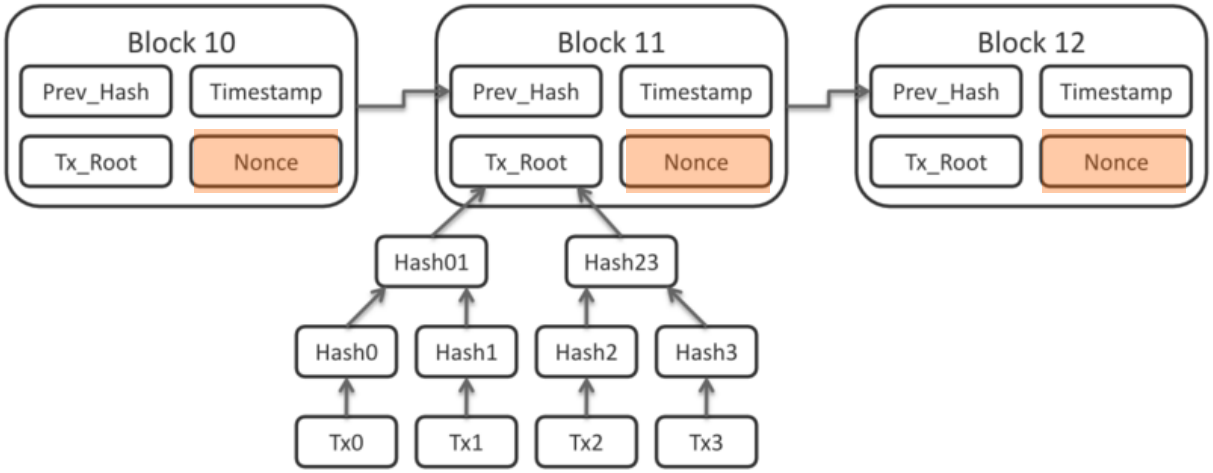
- Participation restricted
- Powerful gatekeeper
- Size is limited
- Blocks updated by central authority
  - User fees charged

Emerging industry consortia

The 'Big Four' to Establish Their Own Blockchain Consortium

A blockchain with “proof of work”

Nakamoto (2008)



- A valid “nonce” must be discovered by trial-and-error, so that the hash for the entire block is below a pre-specified target value. This *raises the cost for hackers*.

- Difficulty of the problem is recalibrated every two weeks, so that the time to solve each block remains at c. ten minutes

Miners: successors to accountants

"Competitive bookkeeping"

- Mining is computationally intensive, with supercomputers specially configured to look for nonces at very high "hash rates"

- Generally located in bunkers where electric power is cheap
  - Iceland
  - Inner Mongolia
  - Venezuela

Icelandic bitcoin mining farm

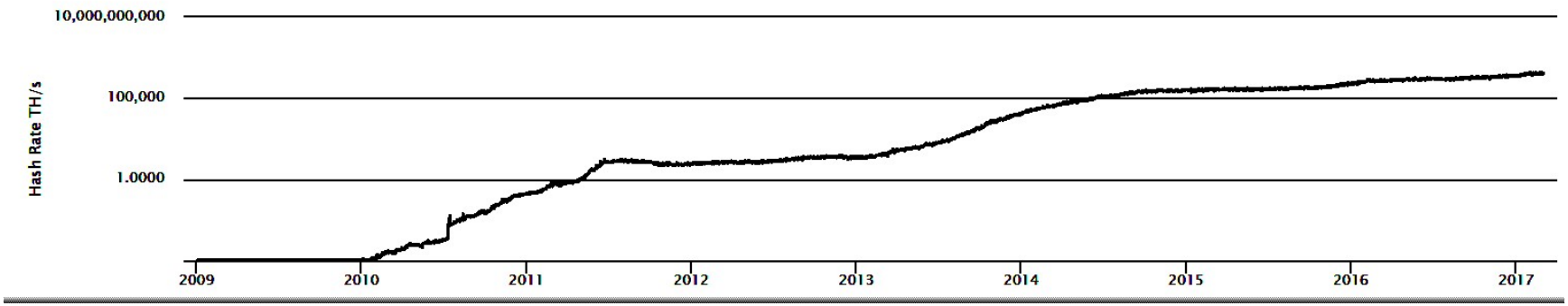
The New York Times

Bitcoin mining farms

Life Inside a Secret Chinese Bitcoin Mine:
https://www.youtube.com/watch?v=K8kua5B5K3I

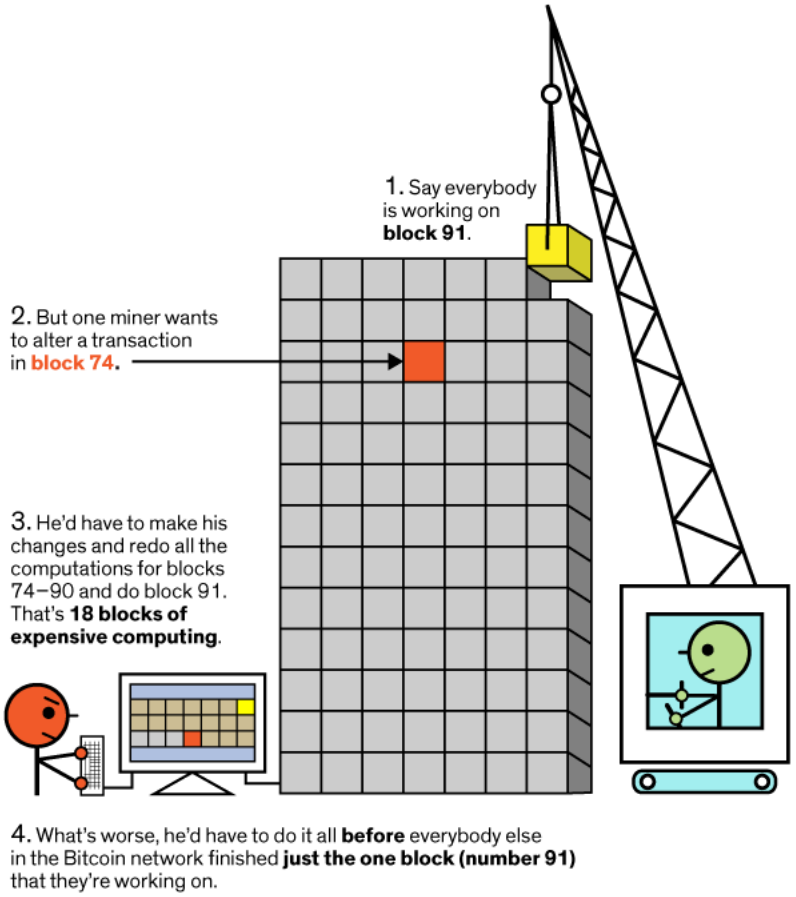
Hash rate of bitcoin network

Trillions of hashes per second



https://blockchain.info/charts/hash-rate

Indelibility of data on a blockchain

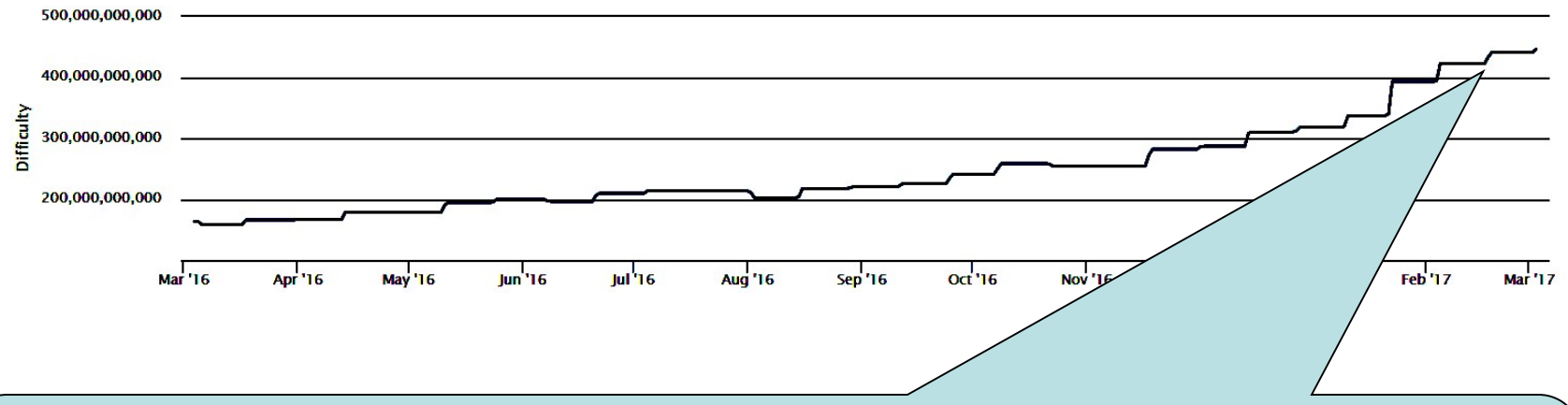


- Fraud = rewriting old transactions
- Implication: transactions are ***indelible***, but also ***irreversible***

Source: Mark Montgomery / IEEE Spectrum

Mining difficulty

Recalibrated automatically every 2,016 blocks, or two weeks

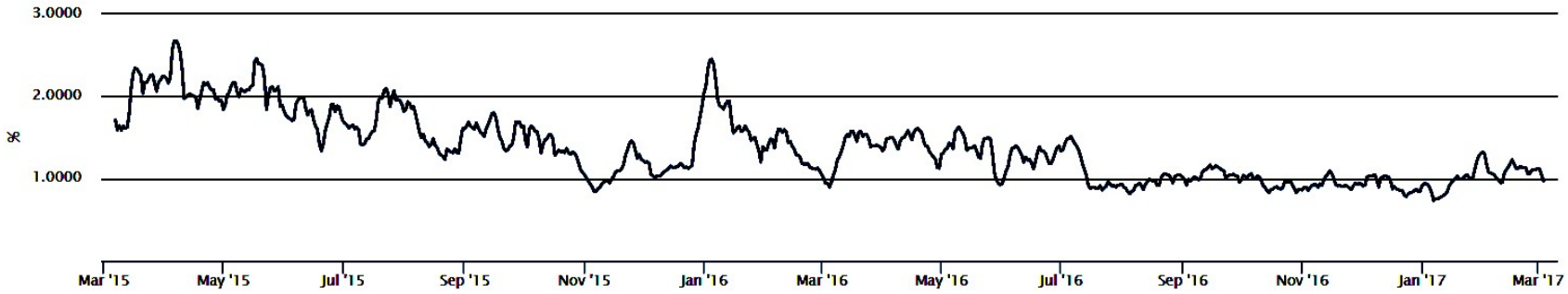


On February 18, 2017, hash target value was reduced from
00000000000000029ab9000000000000000000000000000000000000000000
to
00000000000000027e9300000000000000000000000000000000000000000

https://blockchain.info/charts/difficulty

Mining revenue / value processed

7 day moving average



https://blockchain.info/charts/cost-per-transaction-percent

What else can be tracked on a blockchain?

Source: SolidX Partners Inc.

Do companies need the stock exchange?

- Permissioned blockchain: operated by the company

- Open blockchain: operated competitively
  - Issuance of new shares to competitive miners
  - User fees to competitive miners

The reaction of industry

THE WALL STREET JOURNAL.

Bitcoin Technology Gets Nasdaq Test

By BRADLEY HOPE And MICHAEL J. CASEY
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.

The experiment j
technology. If th
technology in its
systems that hav

"Utilizing the blo
said Nasdaq Chie
to "benefit not or

Nasdaq will start
launched in Janu
platform has mor

Private companie
systems, includir
hand. Nasdaq wa
technology.

The blockchain l
aspect of bitcoin
services with a n

NASDAQ®

Nasdaq

December 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.

For this transaction, Nasdaq enabled the issuer to digitally represent a record of ownership using Nasdaq Linq, while significantly reducing settlement time and eliminating the need for paper stock certificates. In addition to its equity management function, Nasdaq Linq also provides issuers and investors an ability to complete and execute subscription documents online.

Nasdaq's use of blockchain technology also holds promise for expediting trade settlement for transactions in public markets. Blockchain technology has the potential to assist in expediting trade clearing and settlement from the current equity market standards of three days to as little as ten minutes. As a result,

What would be different on a blockchain stock exchange?

- Much lower cost
- Quicker speed of trading and settlement
- More accurate record-keeping
- Transparency of ownership
- Autonomous “smart contracts” for debt and contingent securities

What is Ethereum?

		Market Cap	Price	Circulating Supply	Volume (24h)
1	Bitcoin	$64,395,628,279	$3884.35	16,578,225 BTC	$1,198,140,000
2	Ethereum	$26,709,632,576	$281.92	94,743,567 ETH	$395,739,000
3	Bitcoin Cash	$7,823,739,462	$471.34	16,599,000 BCH	$429,397,000
4	Ripple	$6,937,052,842	$0.180917	38,343,841,883 XRP *	$30,817,600
5	Litecoin	$2,708,544,129	$51.08	53,027,607 LTC	$142,764,000
6	Dash	$2,617,419,291	$345.76	7,570,112 DASH	$82,209,500
7	NEM	$2,027,511,000	$0.225279	8,999,999,999 XEM *	$3,205,040
8	IOTA	$1,509,557,338	$0.543098	2,779,530,283 MIOTA *	$9,961,290
9	Monero	$1,423,889,602	$94.27	15,104,906 XMR	$28,047,900

Vitalik Buterin

Smart contracts: Szabo (1997)

http://ojphi.org/ojs/index.php/fm/article/view/548/469

- “The basic idea behind smart contracts is that many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive. . .”

Nick Szabo

Smart contracts

- Certainty of performance
- Reduced cost of dispute resolution
- Reduced transaction costs
- Eliminate need for trusted third party

Performance is automatic; costs of dispute resolution are non-existent.

A simple example of smart contracts: Secured corporate debt

- Collateral conveyed automatically upon default
- Restrictive covenants no longer necessary
- Financial distress resolved *ex ante* by contract
- Cost of debt should drop
  - Certainty of performance
    - Less moral hazard of “strategic default”
    - Less adverse selection by untrustworthy borrowers
  - Zero enforcement costs

The way forward: what industry wants

Incremental upgrading of the current system

The way forward
Three potential channels of disruption

- Challengers
  - wildcat firms bypassing the status quo
- Collaboration
  - consortia of existing market participants
- Mandates by regulators or legislatures

Learn more

White papers circulated by Goldman Sachs, UK Government, many others . . .