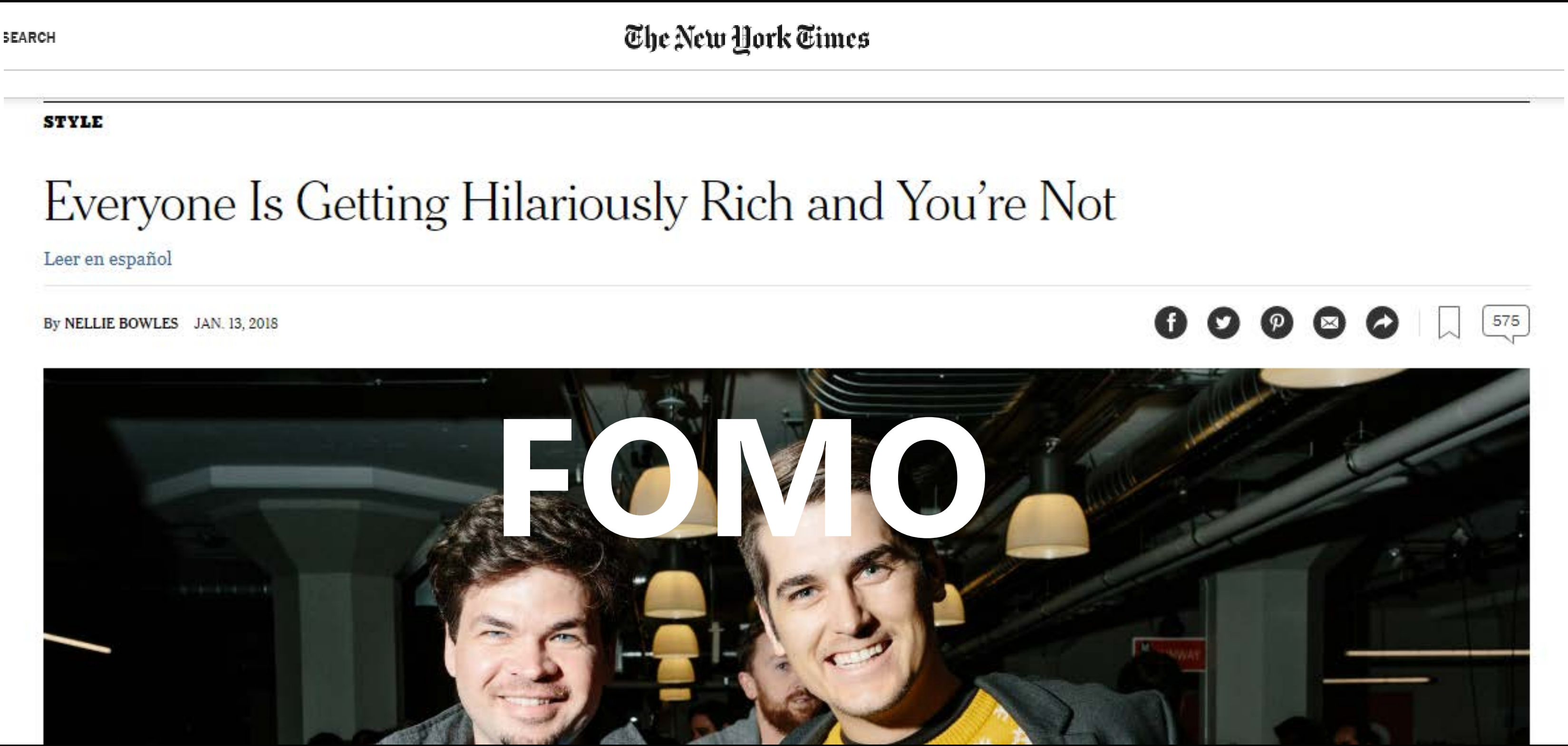
An Introduction to BlockChain

Roy Wilson – Solution Architect

Microsoft

IAPF Annual Benefits Conference 2018



SEARCH

The New York Times

STYLE

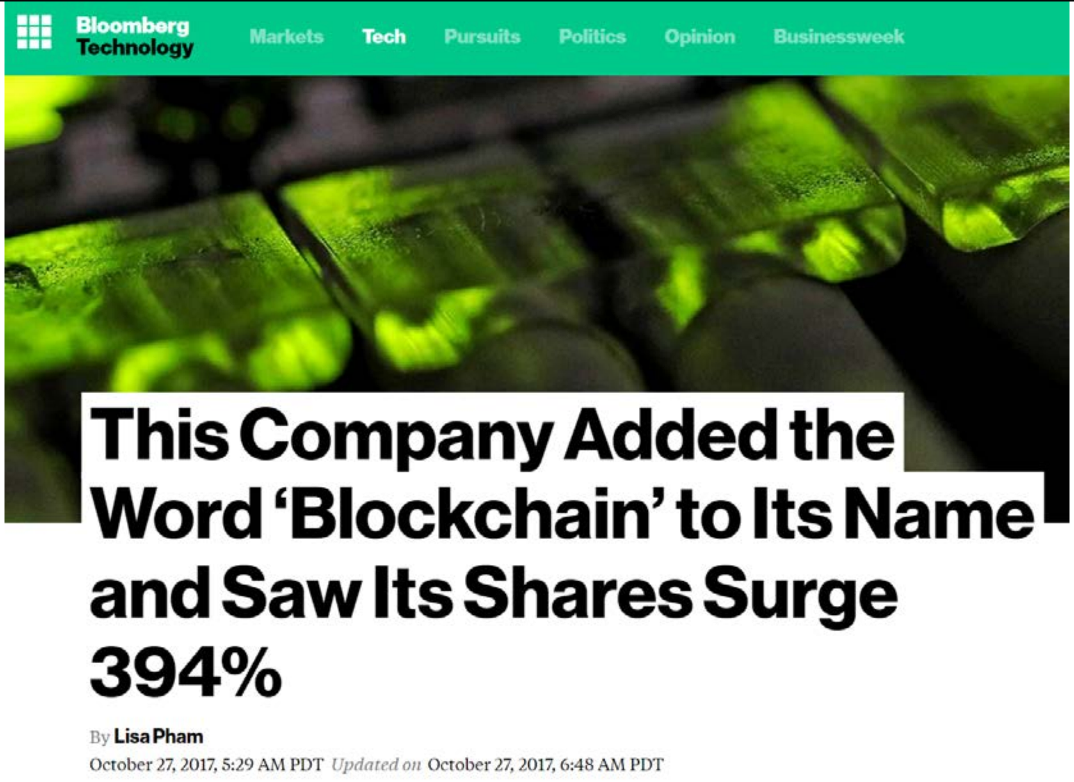
Everyone Is Getting Hilariously Rich and You're Not

Leer en español

By NELLIE BOWLES JAN. 13, 2018

575

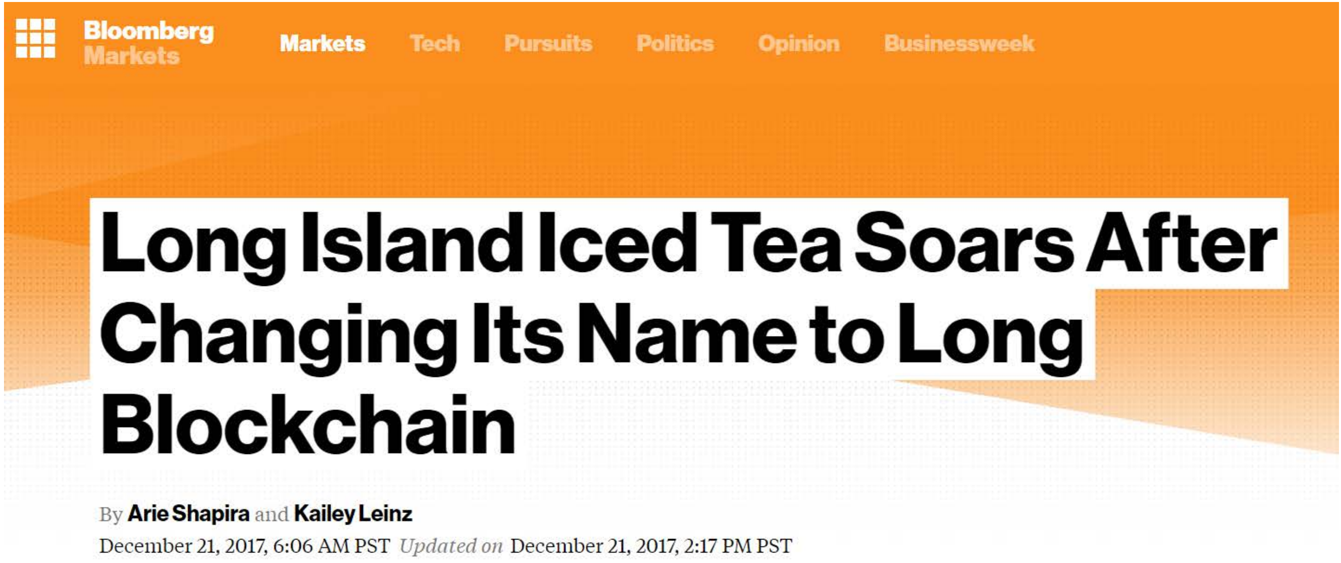
FOMO



This Company Added the Word 'Blockchain' to Its Name and Saw Its Shares Surge 394%

By **Lisa Pham**

October 27, 2017, 5:29 AM PDT *Updated on* October 27, 2017, 6:48 AM PDT

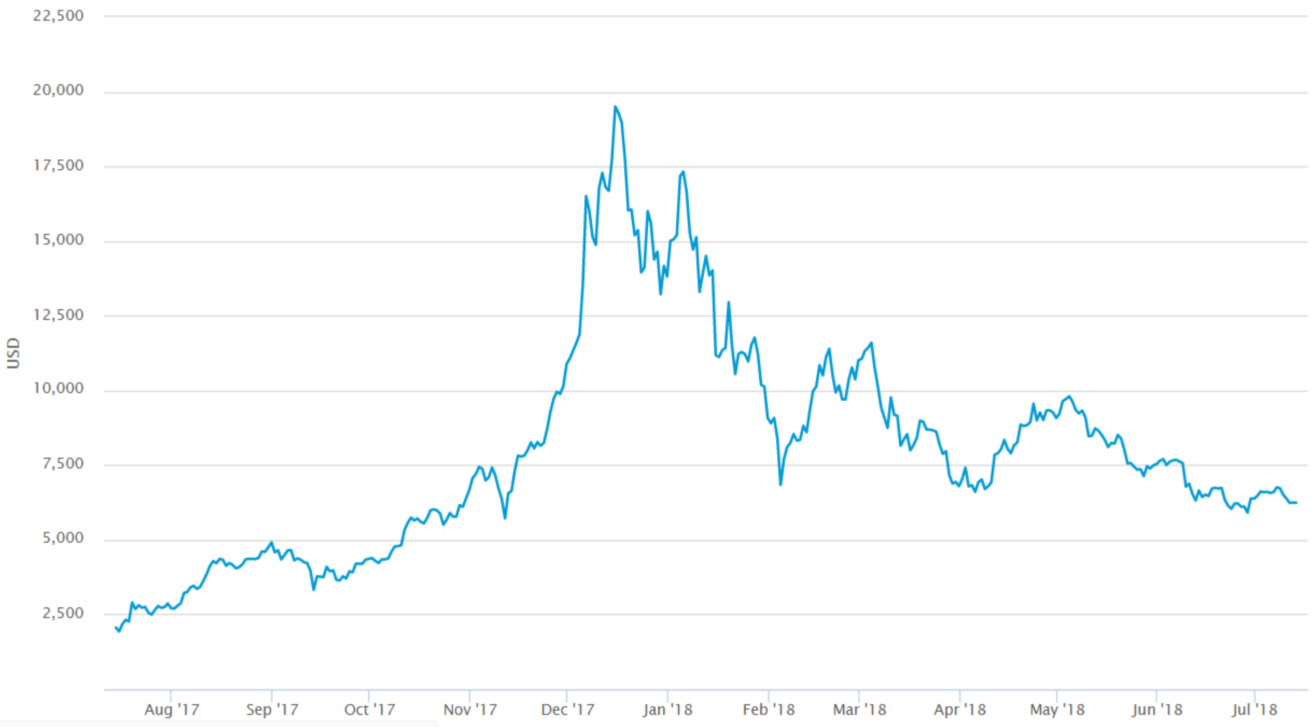


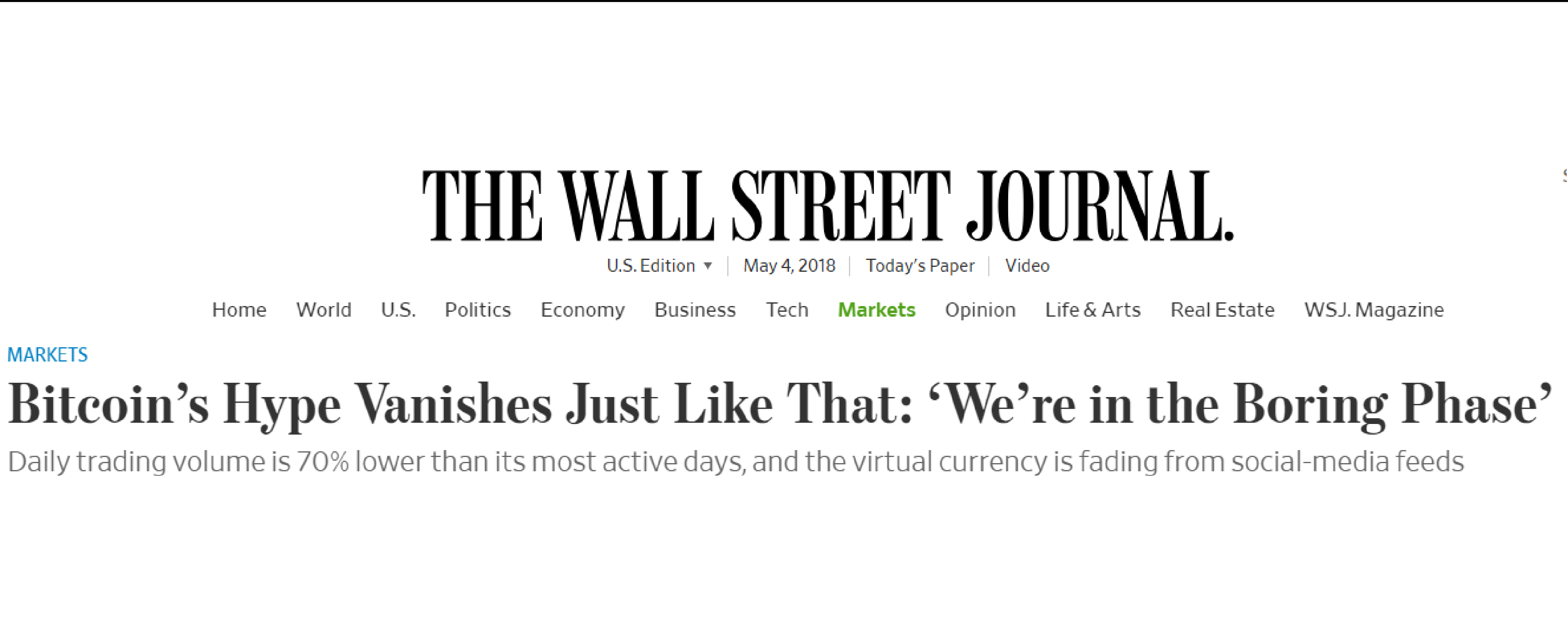
Long Island Iced Tea Soars After Changing Its Name to Long Blockchain

By **Arie Shapira** and **Kailey Leinz**

December 21, 2017, 6:06 AM PST *Updated on* December 21, 2017, 2:17 PM PST

BTC


22,500
20,000
17,500
15,000
12,500
10,000
7,500
5,000
2,500
USD
Aug '17
Sep '17
Oct '17
Nov '17
Dec '17
Jan '18
Feb '18
Mar '18
Apr '18
May '18
Jun '18
Jul '18



THE WALL STREET JOURNAL.

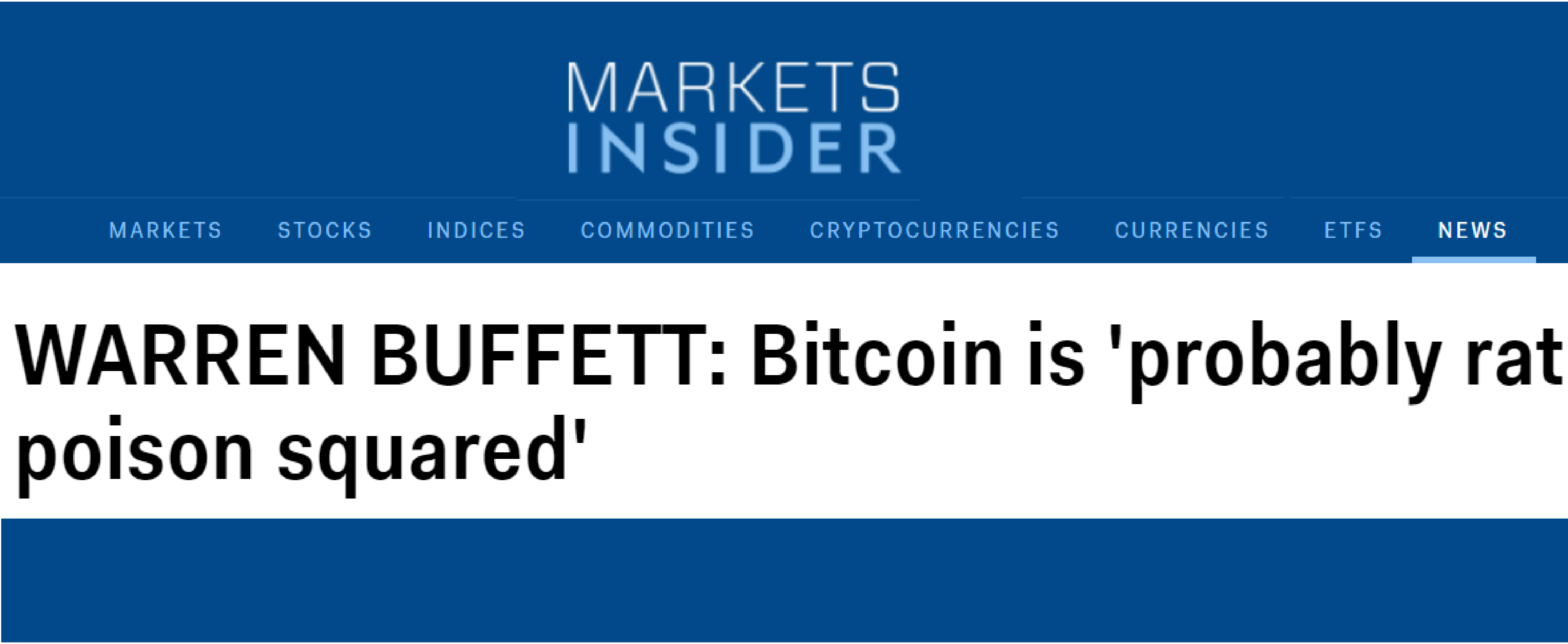
U.S. Edition ▾ | May 4, 2018 | Today's Paper | Video

Home World U.S. Politics Economy Business Tech **Markets** Opinion Life & Arts Real Estate WSJ. Magazine

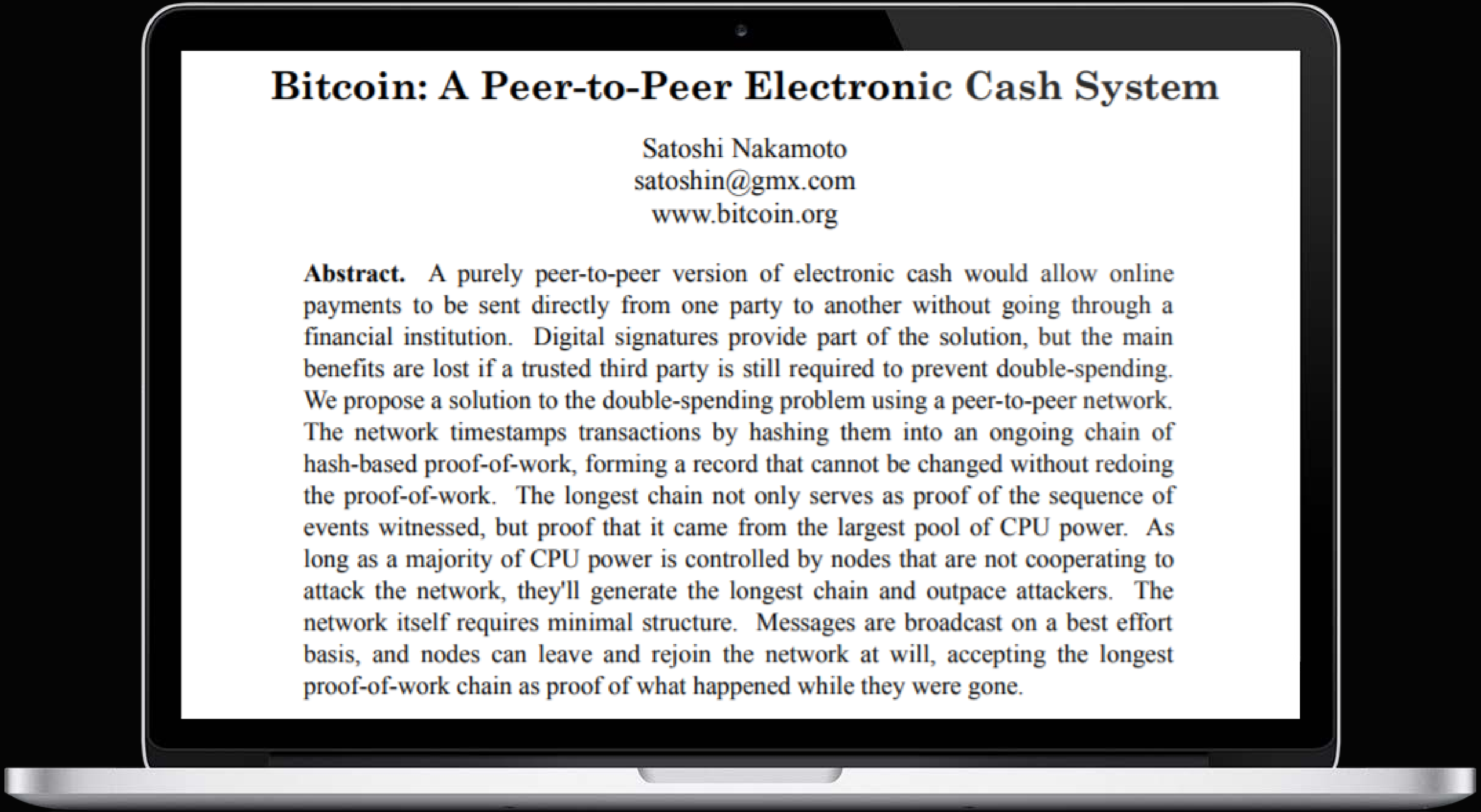
MARKETS

Bitcoin's Hype Vanishes Just Like That: 'We're in the Boring Phase'

Daily trading volume is 70% lower than its most active days, and the virtual currency is fading from social-media feeds



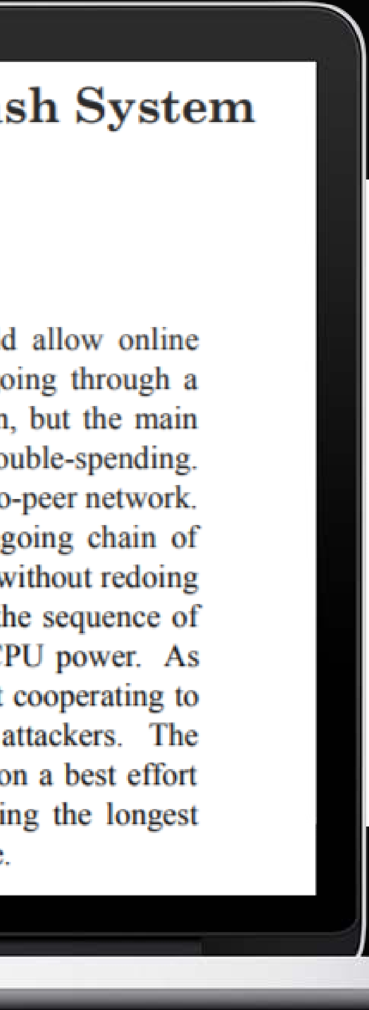
WARREN BUFFETT: Bitcoin is 'probably rat poison squared'



Bitcoin: A Peer-to-Peer Electronic Cash System

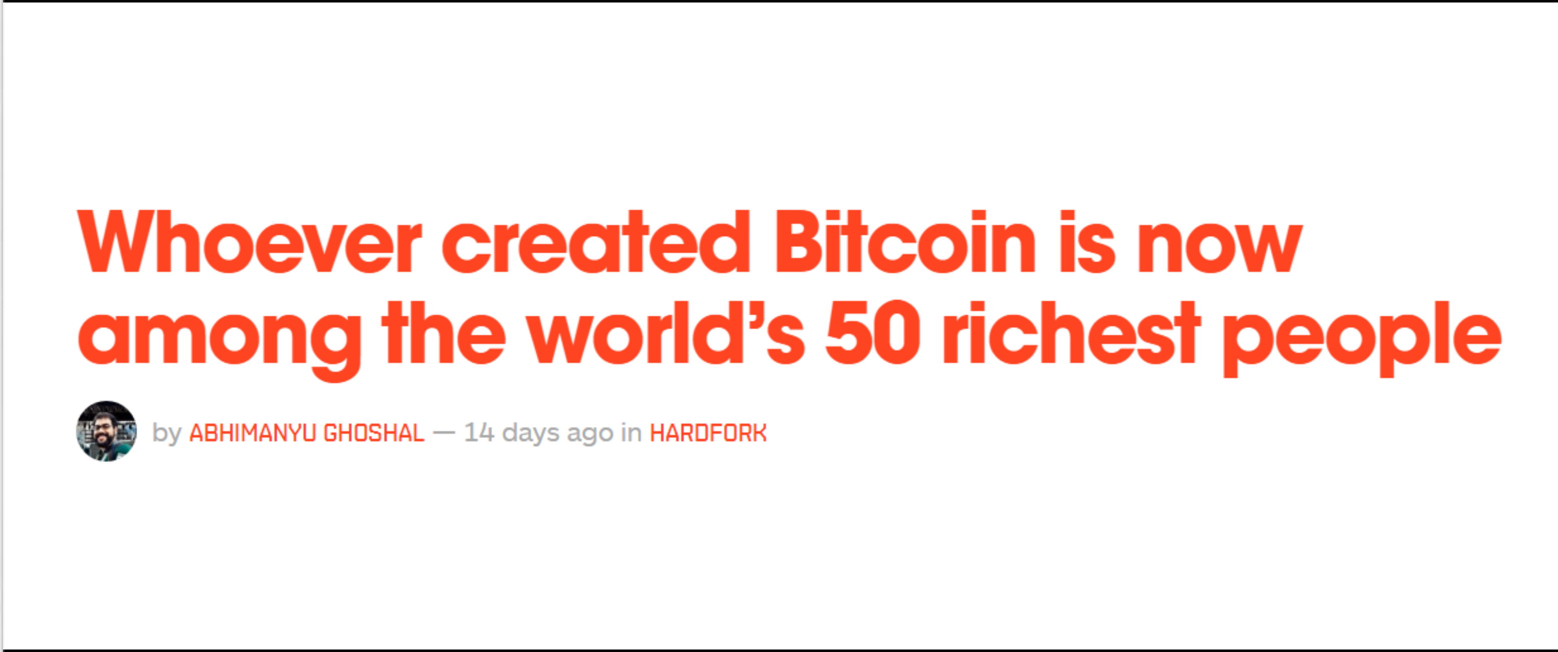
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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.



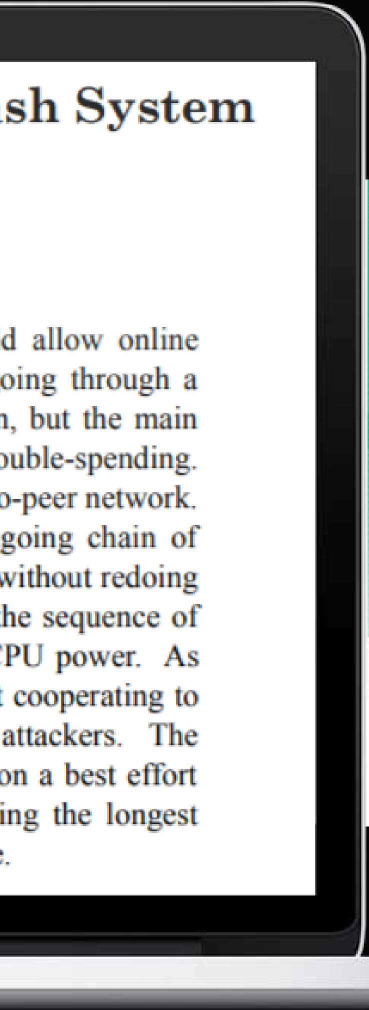
sh System

d allow online
oing through a
n, but the main
ouble-spending.
o-peer network.
going chain of
without redoing
he sequence of
PU power. As
t cooperating to
attackers. The
on a best effort
ing the longest
e.



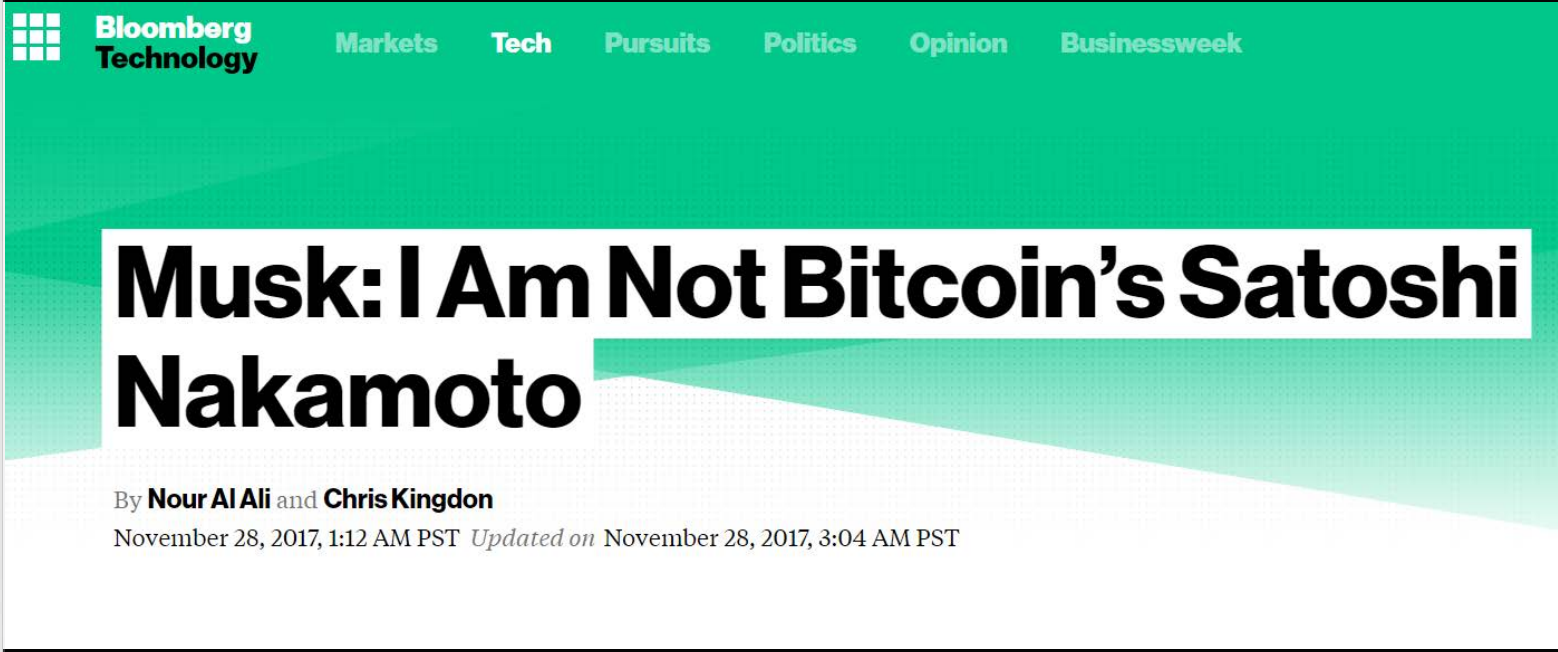
Whoever created Bitcoin is now among the world's 50 richest people

by ABHIMANYU GHOSHAL — 14 days ago in HARDFORK



sh System

d allow online
oing through a
n, but the main
ouble-spending.
o-peer network.
going chain of
without redoing
he sequence of
PU power. As
t cooperating to
attackers. The
on a best effort
ing the longest
e.



Musk: I Am Not Bitcoin’s Satoshi Nakamoto

By **Nour Al Ali** and **Chris Kingdon**

November 28, 2017, 1:12 AM PST *Updated on* November 28, 2017, 3:04 AM PST

Fiat Currency

Issued by governments

Delays between transaction and settlement

Need for intermediaries to prevent fraud and loss

High transaction fees

Cryptocurrency

No central authority

No clearing

No intermediaries

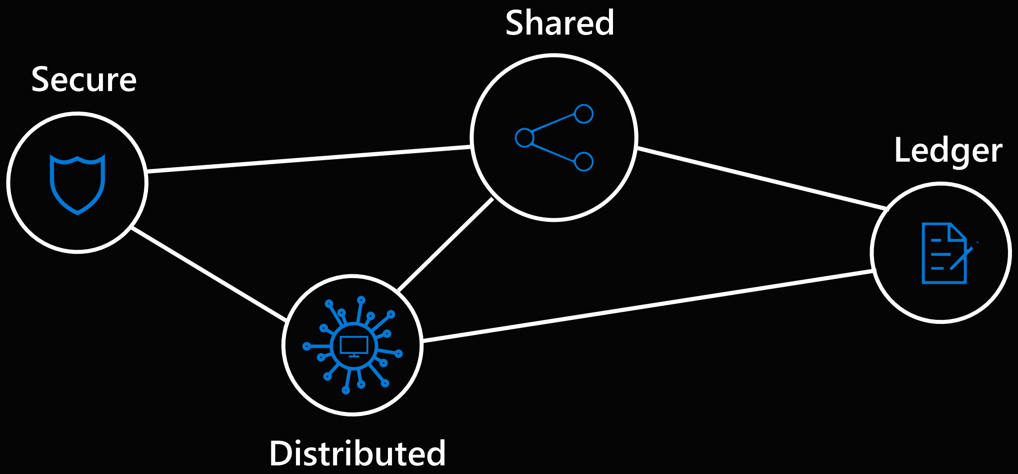
Immutable transaction history

Blockchains

Cryptocurrency is built on BLOCKCHAIN

Blockchains are also called Distributed Ledger Technology (DLT)

Blockchains gets their properties from cryptography



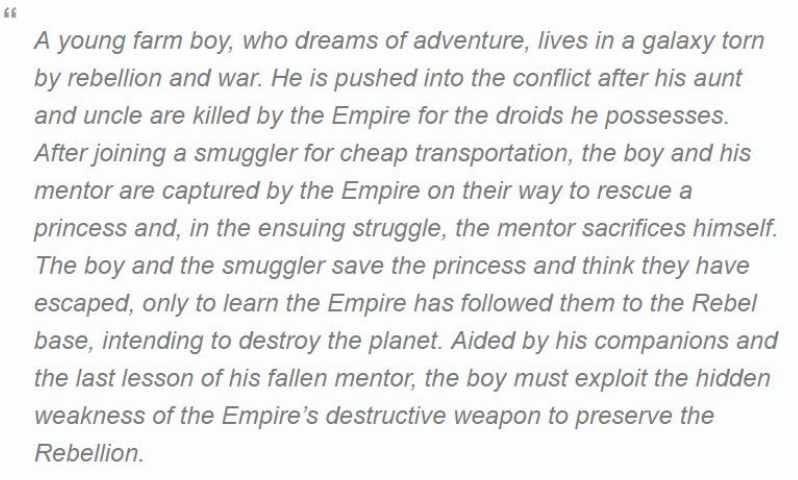
Blockchain cryptography basics

- Hash function
- Public-key cryptography
- Digital signature

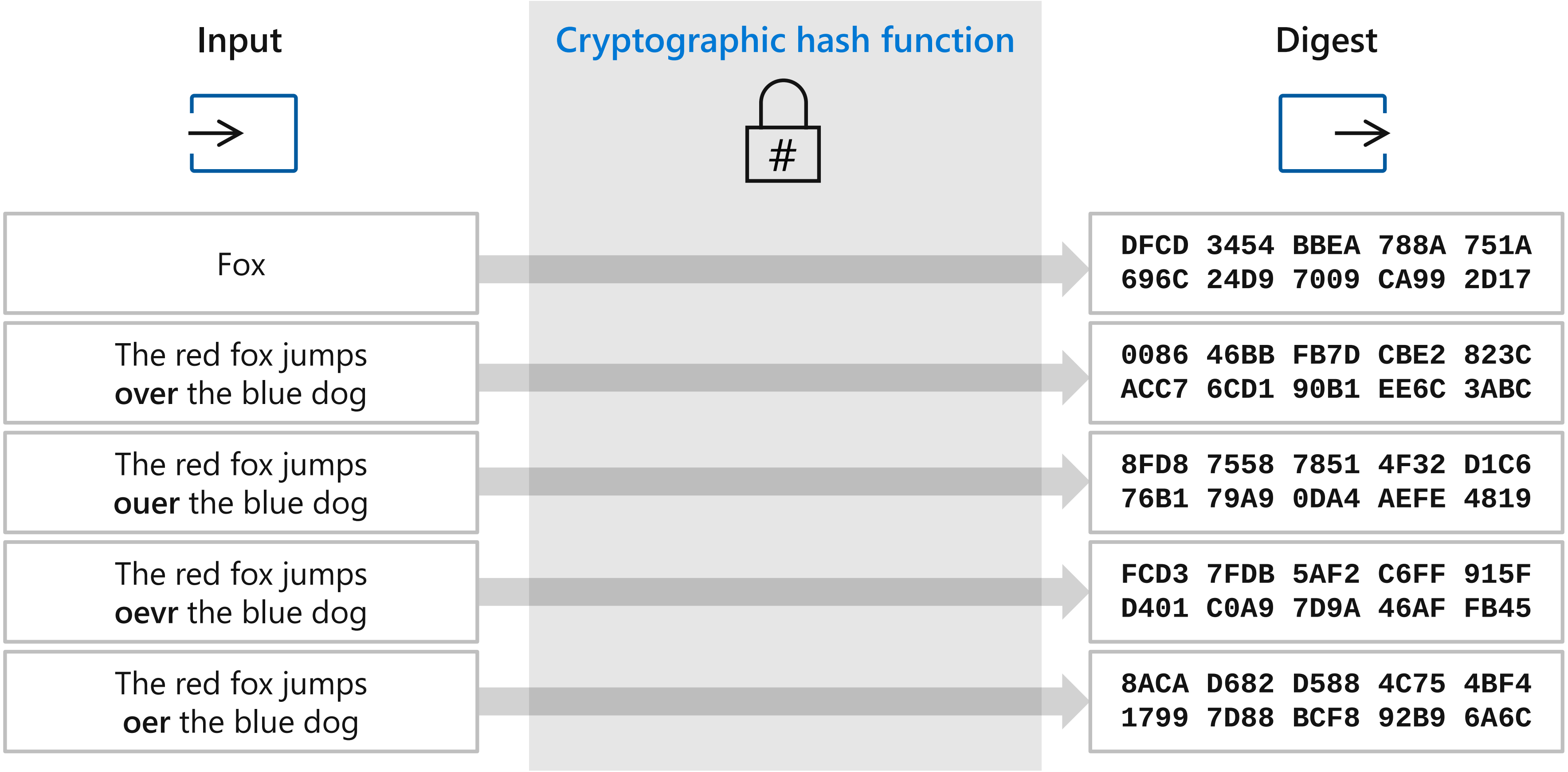
Cryptographic hash

Algorithm that creates a succinct representation ("digest") of data

Summary


"

A young farm boy, who dreams of adventure, lives in a galaxy torn by rebellion and war. He is pushed into the conflict after his aunt and uncle are killed by the Empire for the droids he possesses. After joining a smuggler for cheap transportation, the boy and his mentor are captured by the Empire on their way to rescue a princess and, in the ensuing struggle, the mentor sacrifices himself. The boy and the smuggler save the princess and think they have escaped, only to learn the Empire has followed them to the Rebel base, intending to destroy the planet. Aided by his companions and the last lesson of his fallen mentor, the boy must exploit the hidden weakness of the Empire's destructive weapon to preserve the Rebellion.

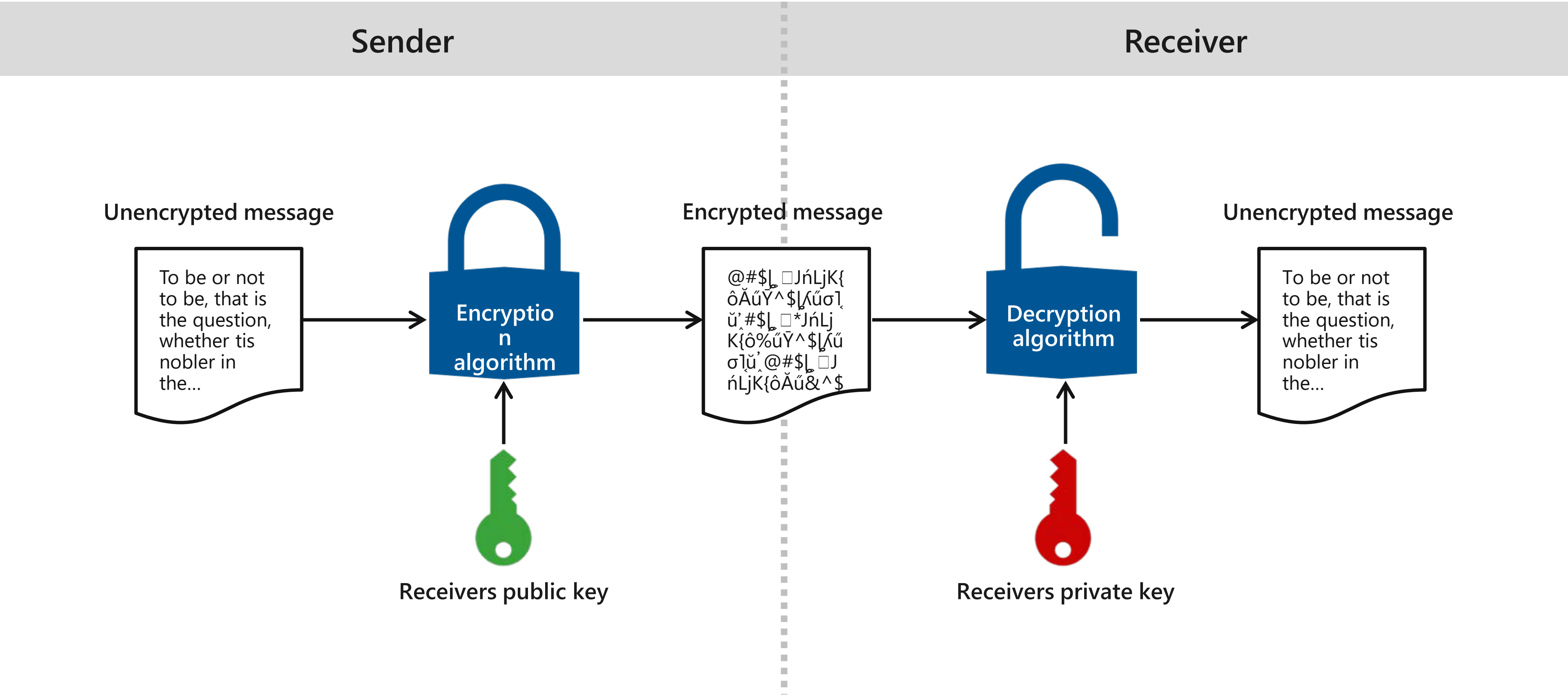


Cryptographic hash function

#

Input	Digest
Fox	DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps **over** the blue dog	0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6C 3ABC
The red fox jumps **ouer** the blue dog	8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps **oevr** the blue dog	FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps **oer** the blue dog	8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Public Key Encryption



Sender

Receiver

Unencrypted message

To be or not
to be, that is
the question,
whether tis
nobler in
the…

Encryptio
n
algorithm

Receivers public key

Encrypted message

@#$ḻ □JńLjK{
ôĂűŸ^$ḻ⁄űσ]
ŭ'#$ḻ □*JńLj
K{ô%űŸ^$ḻ⁄ű
σ]ŭ'@#$ḻ □J
ńLjK{ôĂű&^$

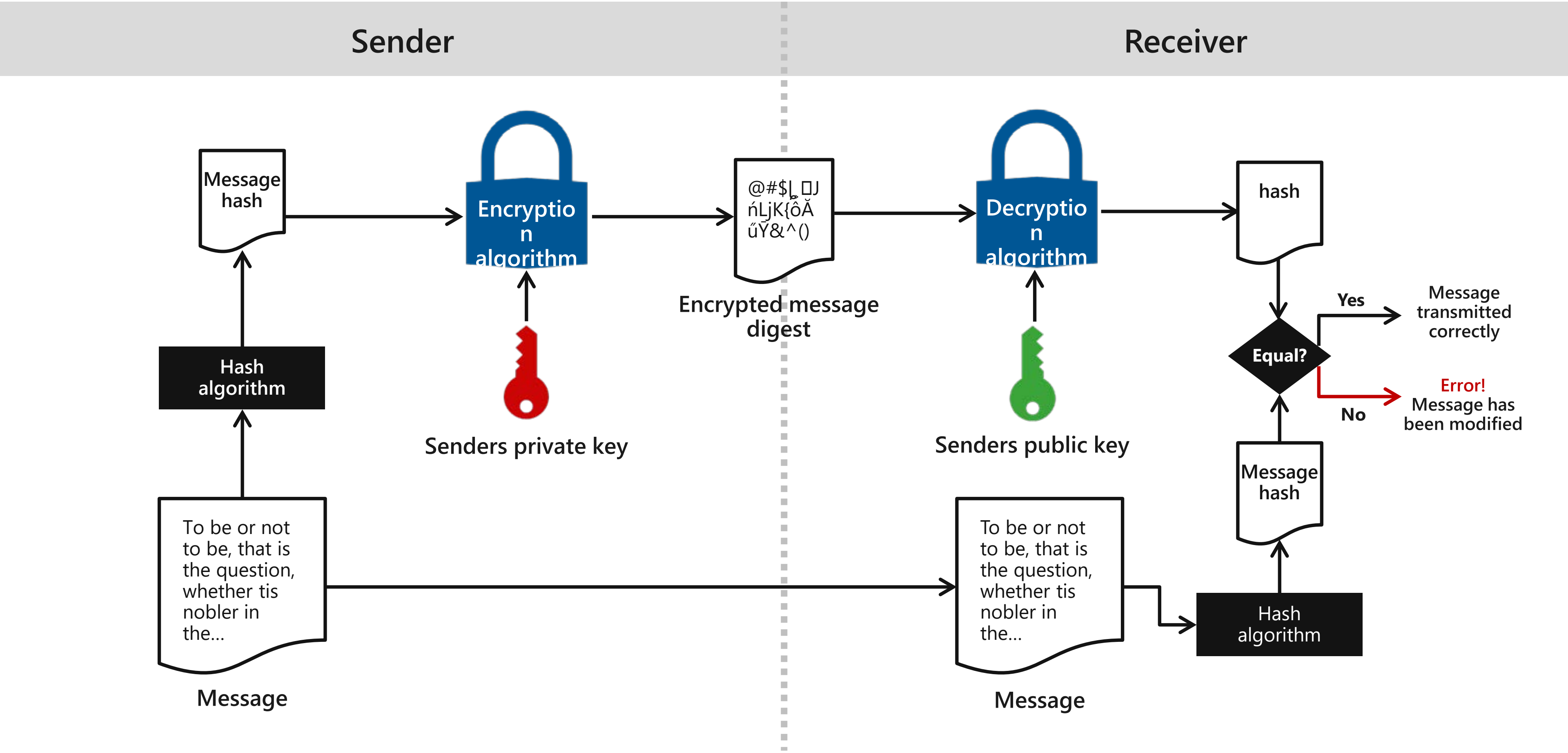
Decryption
algorithm

Receivers private key

Unencrypted message

To be or not
to be, that is
the question,
whether tis
nobler in
the…

Digital Signatures



Sender

Receiver

Message hash

Encryptio n algorithm

@#$ڸ □J
ńLjK{ôĂ
űȲ&^()

Encrypted message digest

Decryptio n algorithm

hash

Hash algorithm

Senders private key

Senders public key

Equal?

Yes

Message transmitted correctly

No

Error!
Message has been modified

Message hash

To be or not to be, that is the question, whether tis nobler in the…

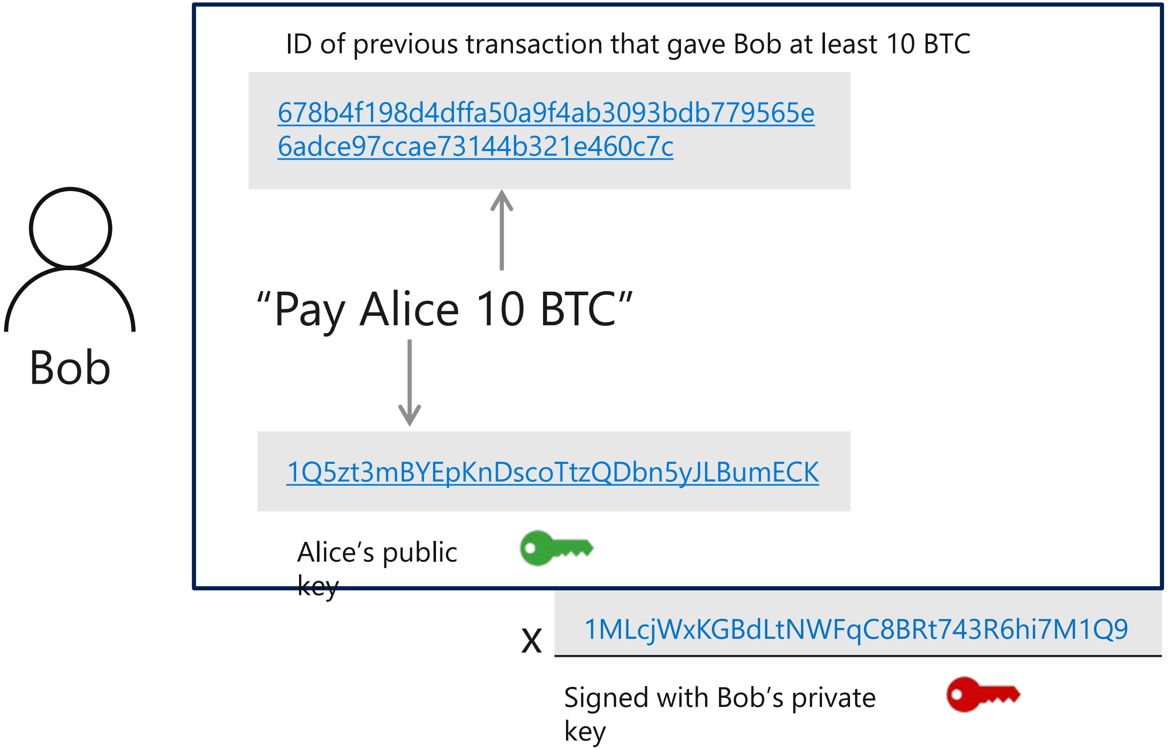
Message

To be or not to be, that is the question, whether tis nobler in the…

Message

Hash algorithm

Transactions



Bob

ID of previous transaction that gave Bob at least 10 BTC

678b4f198d4dffa50a9f4ab3093bdb779565e
6adce97ccae73144b321e460c7c

“Pay Alice 10 BTC”

1Q5zt3mBYEpKnDscoTtzQDbn5yJLBumECK

Alice’s public key

X 1MLcjWxKGBdLtNWFqC8BRt743R6hi7M1Q9

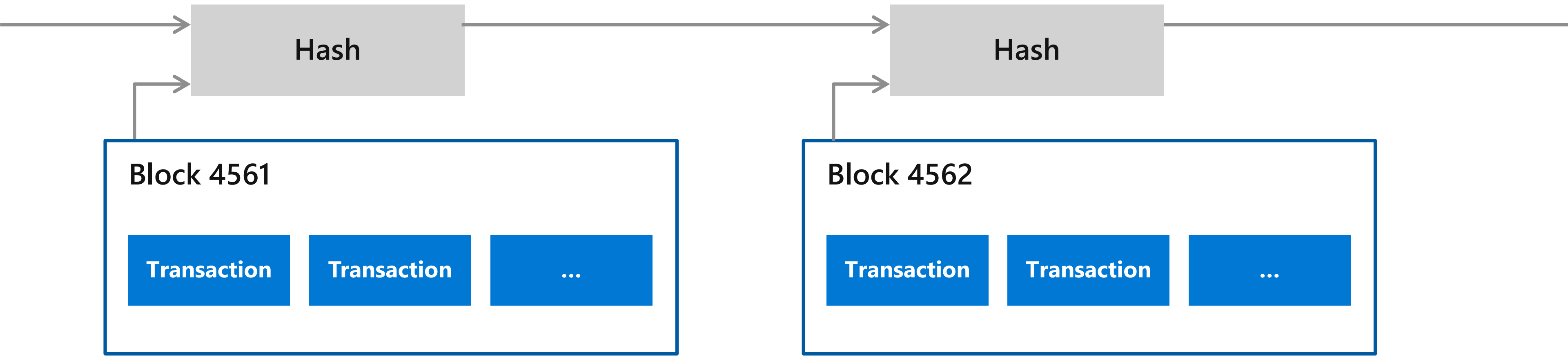
Signed with Bob’s private key

Mining

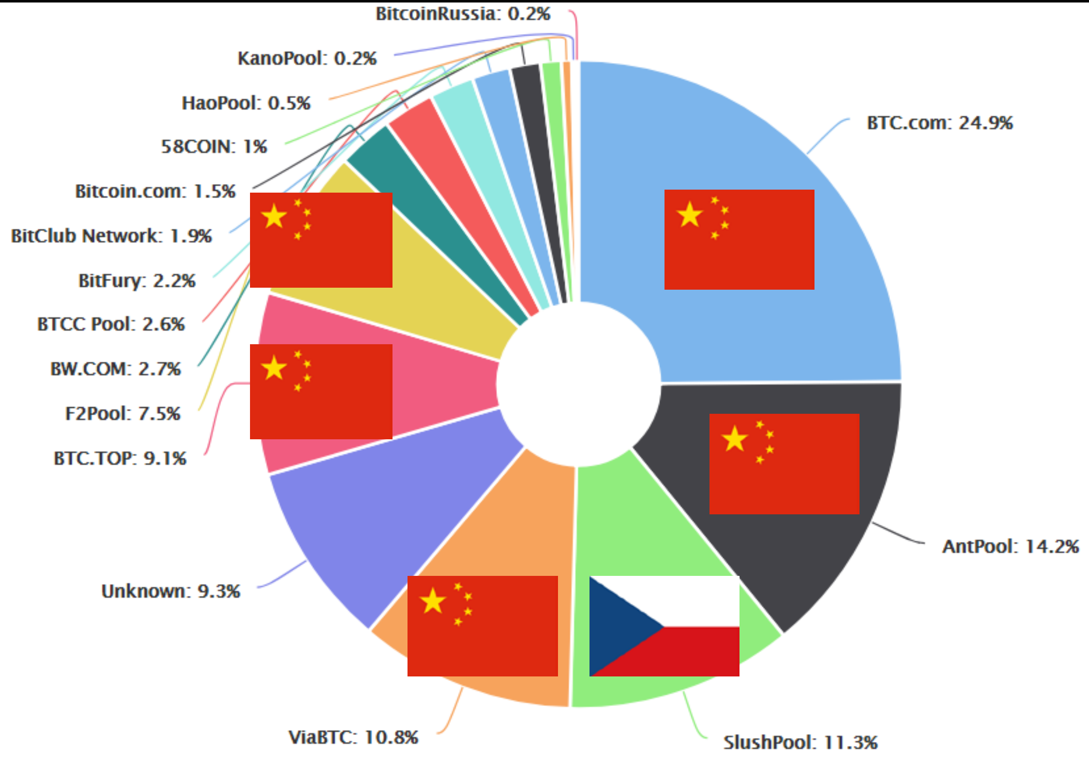
Miners collect transactions into *blocks*

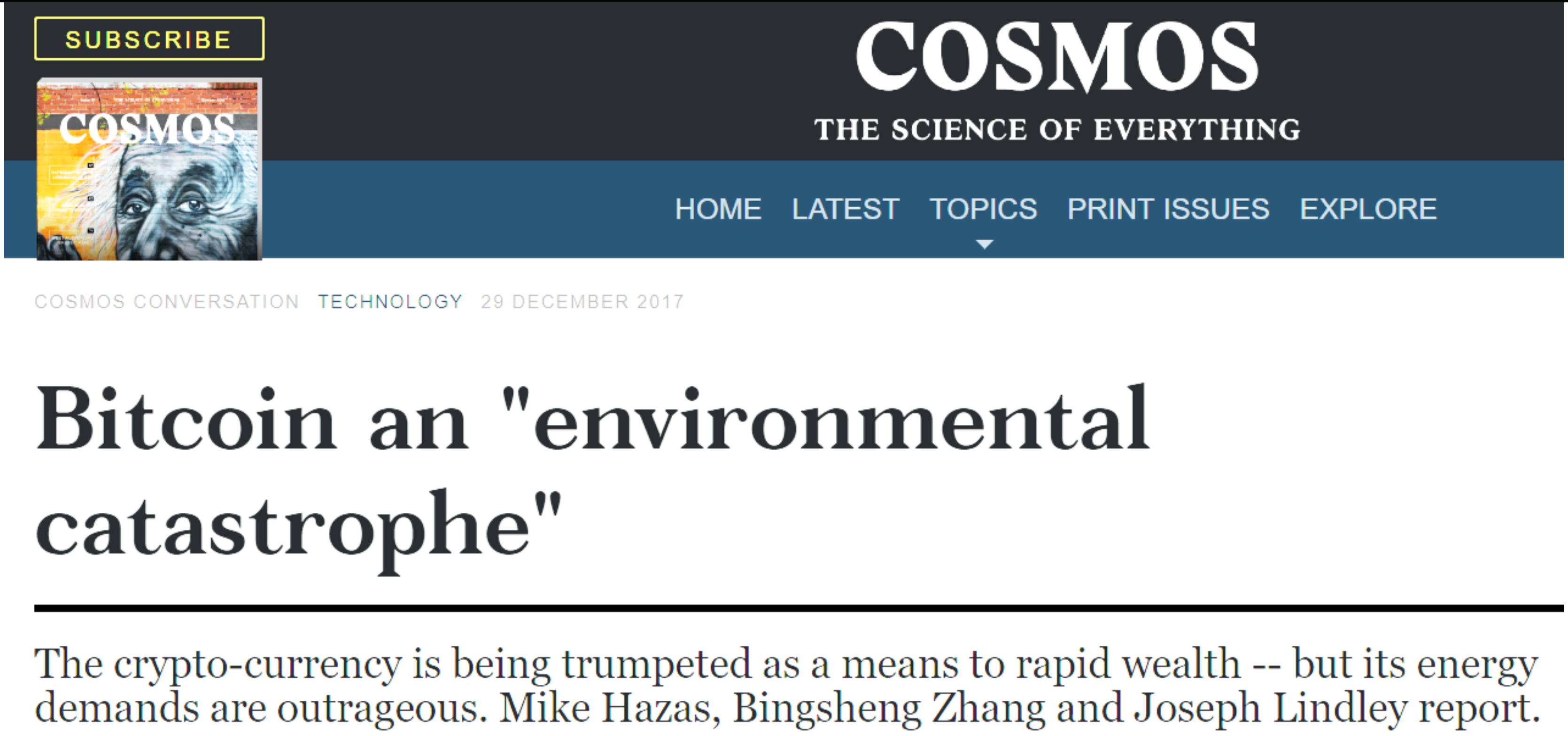
Then submit a proposal for a block after solving a cryptographic puzzle (Hard to compute)

The winner receives an incentive (BTC)



Kncmine


BitcoinRussia: 0.2%
KanoPool: 0.2%
HaoPool: 0.5%
58COIN: 1%
Bitcoin.com: 1.5%
BitClub Network: 1.9%
BitFury: 2.2%
BTCC Pool: 2.6%
BW.COM: 2.7%
F2Pool: 7.5%
BTC.TOP: 9.1%
Unknown: 9.3%
ViaBTC: 10.8%
SlushPool: 11.3%
AntPool: 14.2%
BTC.com: 24.9%



COSMOS CONVERSATION TECHNOLOGY 29 DECEMBER 2017

Bitcoin an "environmental catastrophe"

The crypto-currency is being trumpeted as a means to rapid wealth -- but its energy demands are outrageous. Mike Hazas, Bingsheng Zhang and Joseph Lindley report.

Smart Contracts

Extending blockchains from just data to code

corda

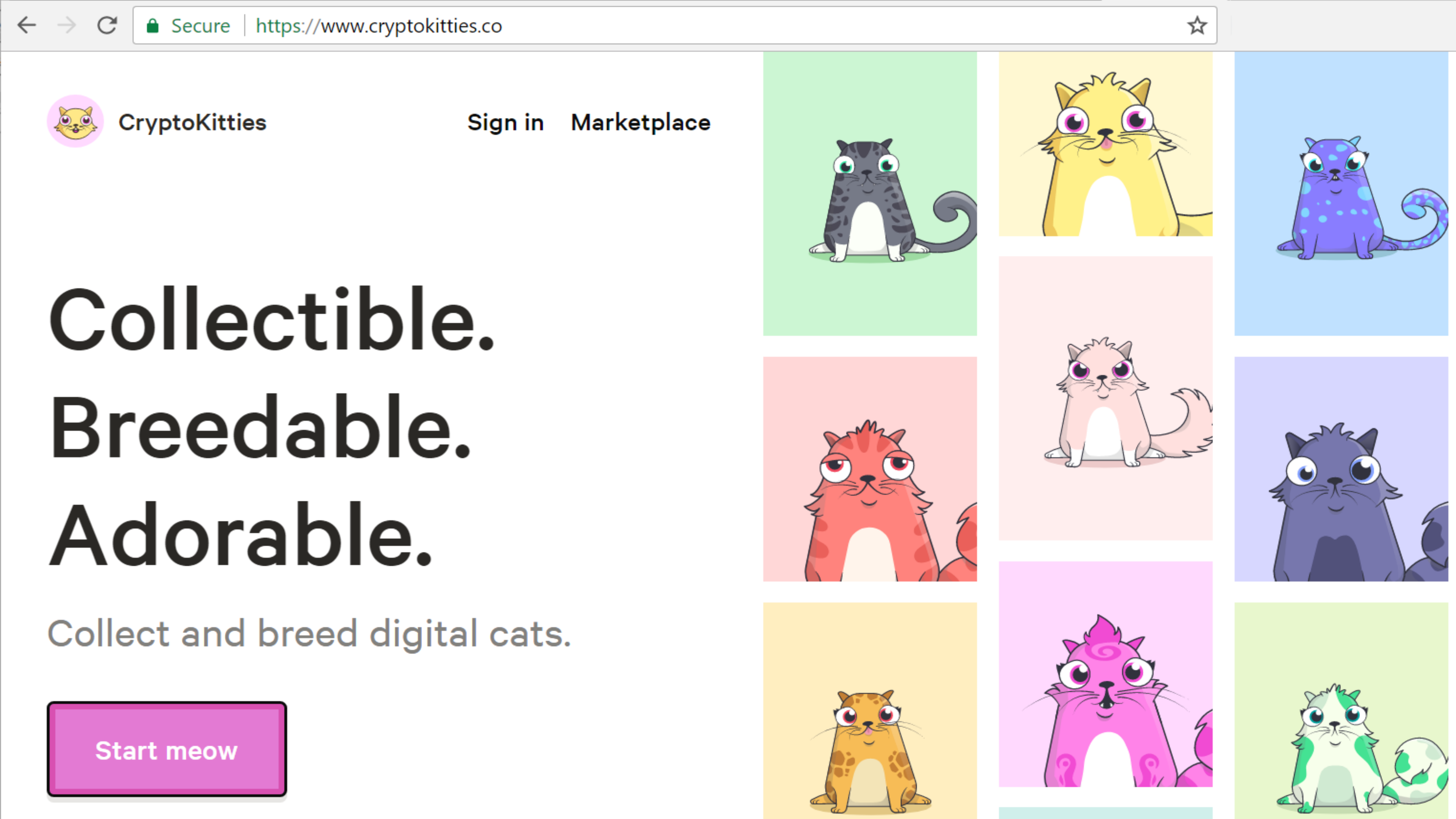
HYPERLEDGER FABRIC

Quorum

Business processes do not complete instantaneously

Problem
How to ensure and establish trust that the right action will happen in the future?

Solution
Hold instructions (Contracts) on the BlockChain and execute them automatically when all programmed pre-conditions met



Collectible.
Breedable.
Adorable.

Collect and breed digital cats.

Smart Contract Use Cases

Trade finance

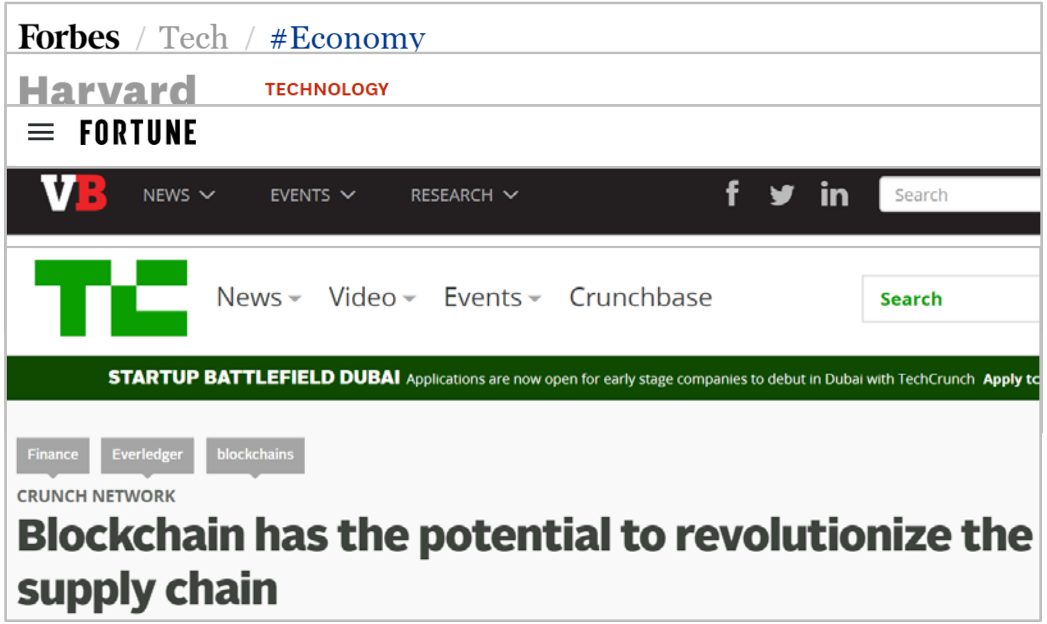
Digital music rights

Diamond tracking

Real estate sales

Supply chain management

...



STARTUP BATTLEFIELD DUBAI Applications are now open for early stage companies to debut in Dubai with TechCrunch Apply tc

CRUNCH NETWORK

Blockchain has the potential to revolutionize the supply chain

Validate your product’s authenticity

Challenge

3M sought a solution to reduce tampering and prevent the introduction of counterfeit drugs into the pharmaceutical supply chain – which is a $200 billion criminal industry

Counterfeit drugs negatively impact brand reputation and overall revenue but, ultimately, they hurt unsuspecting customers

Strategy

3M and Microsoft leveraged Azure Blockchain to build an innovative service to track specially labeled packages through any supply chain

Multilayer QR code labels were used to expose tampering and facilitate easy tracking

Results

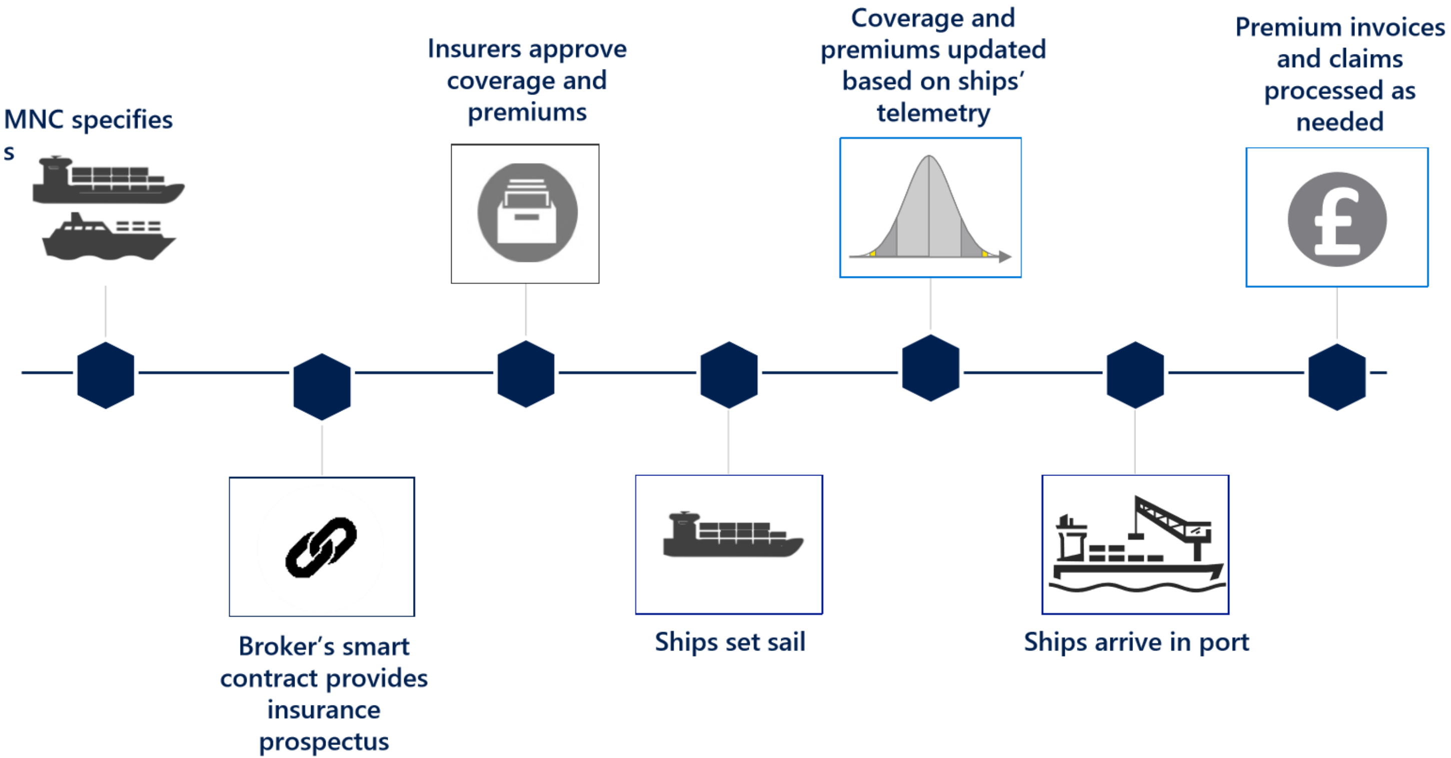
Blockchain technology improved visibility and security at each transfer to ensure products are authentic and free of tampering

Real-time registry, validation, and custodial recordings combated counterfeits and eliminated the risk of fraudulent double selling through secure, attestable data

“We combined 3M DoubleTrust tamper-evident labels with Azure Blockchain to create a label-as-a-service supply chain solution that can help identify counterfeits, protect business performance, and save lives.”

— Oscar Naim, PhD, Lead Software Architecture Specialist, 3M

Insurwave



MNC specifies
s

Broker’s smart contract provides insurance prospectus

Insurers approve coverage and premiums

Ships set sail

Coverage and premiums updated based on ships’ telemetry

Ships arrive in port

Premium invoices and claims processed as needed

EY

MAERSK

Blockchain will provide unprecedented visibility to accurate ship and coverage data across the entire maritime market landscape

Some potential applications

- Streamline transfer of funds
- Syndicated Loans
- P2P Insurance
- Clearing and Settlement
- Automation of claims and reduced fraud
- Parametric insurance
- Smart contract based fund Infrastructure

Summary

- Blockchain (aka Distributed Ledger Technology) has the potential to enable a new programmable economy
- Decentralisation, Security, Transparency and Immutability are the key attributes
- Organisations are embracing it today
- However…Still in it's infancy - adoption is gradual and steady (2022, 10% of Enterprises – Gartner)
- Reducing transaction cost, improving transparency and automating Business to Business processes are just some of the potential benefits