

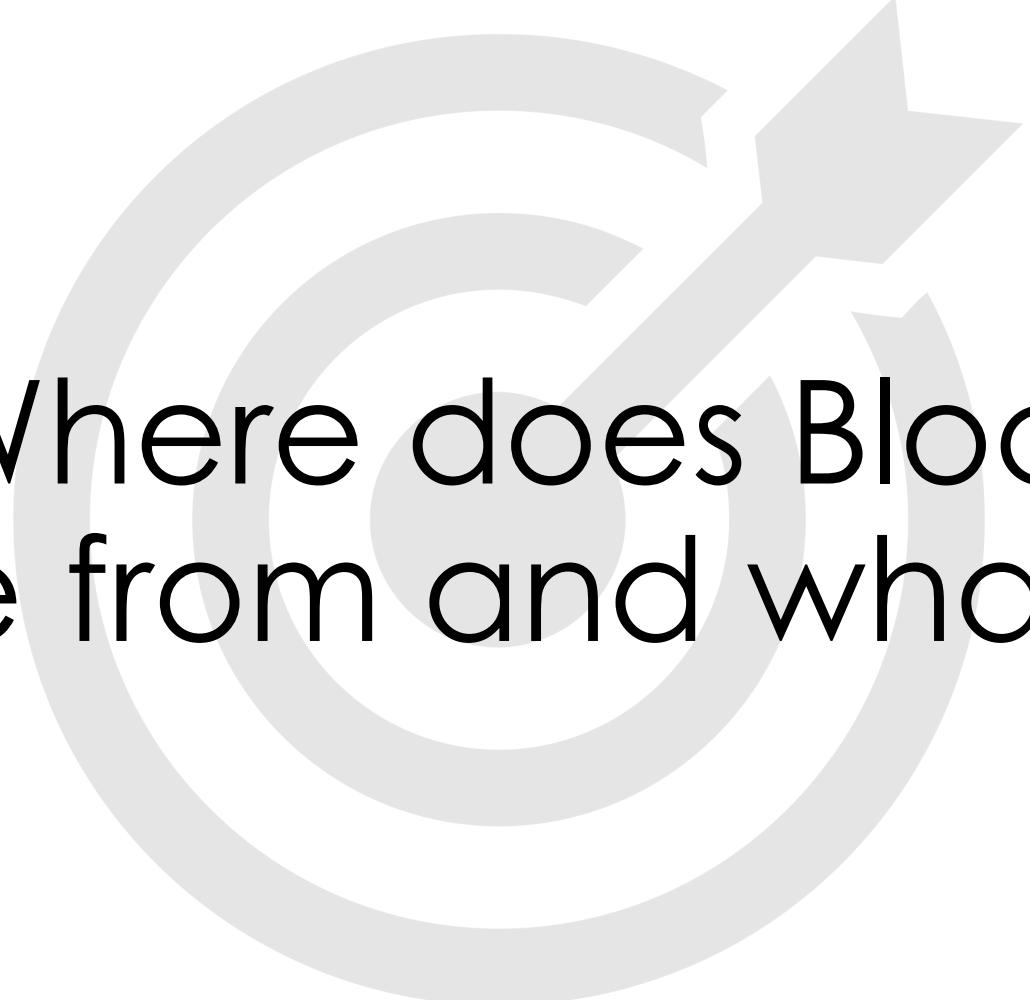


Lecture 0

Introduction to Blockchain

By Samuel Tang, TIBA

Fall 2020 @ Tsinghua University



Goal: Where does Blockchain come from and what is it?

Content

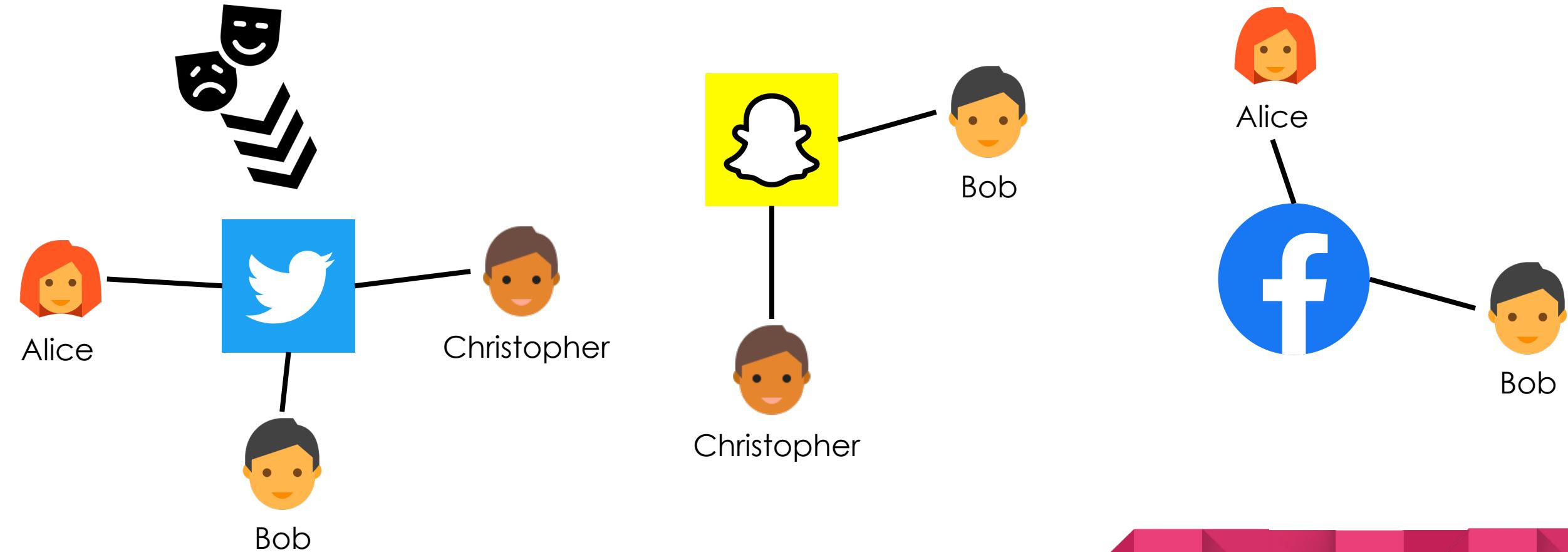
- ◊ The Problem
 - ◊ Is there really a problem?
- ◊ The Solution
 - ◊ History
- ◊ What is Blockchain?



Problem & Solution

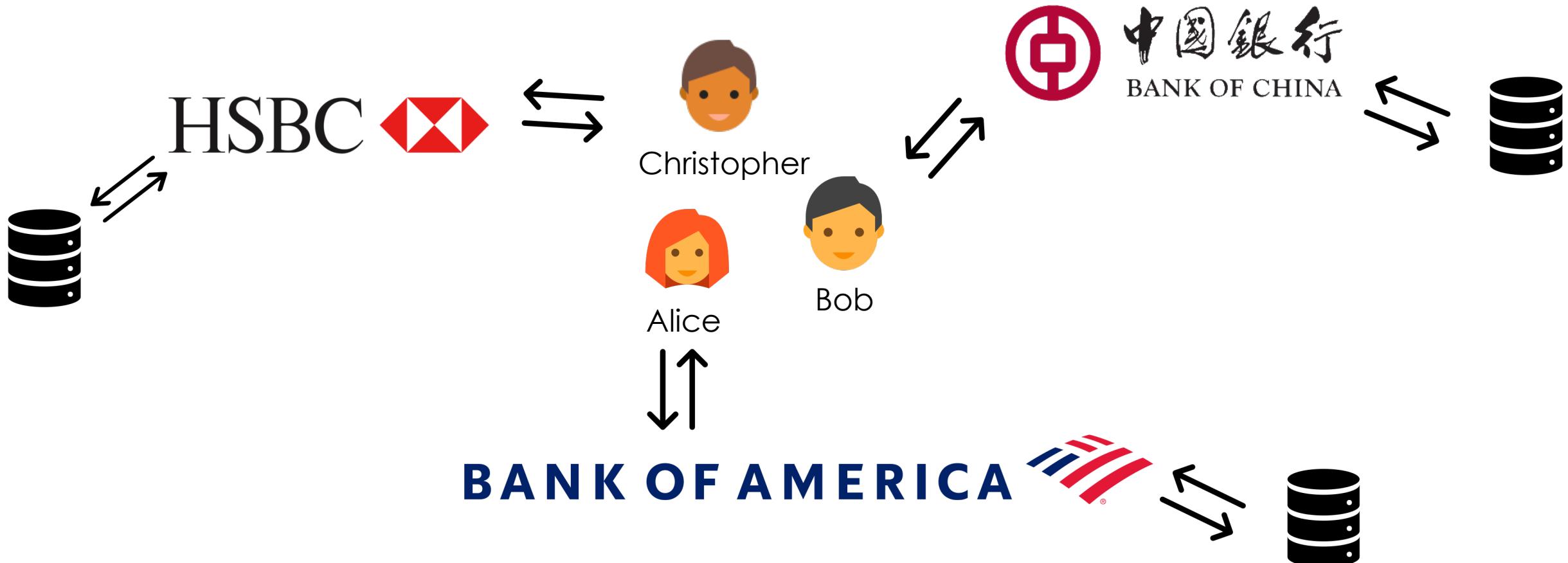
What's the problem?

Control of Data, Single Point of Failure



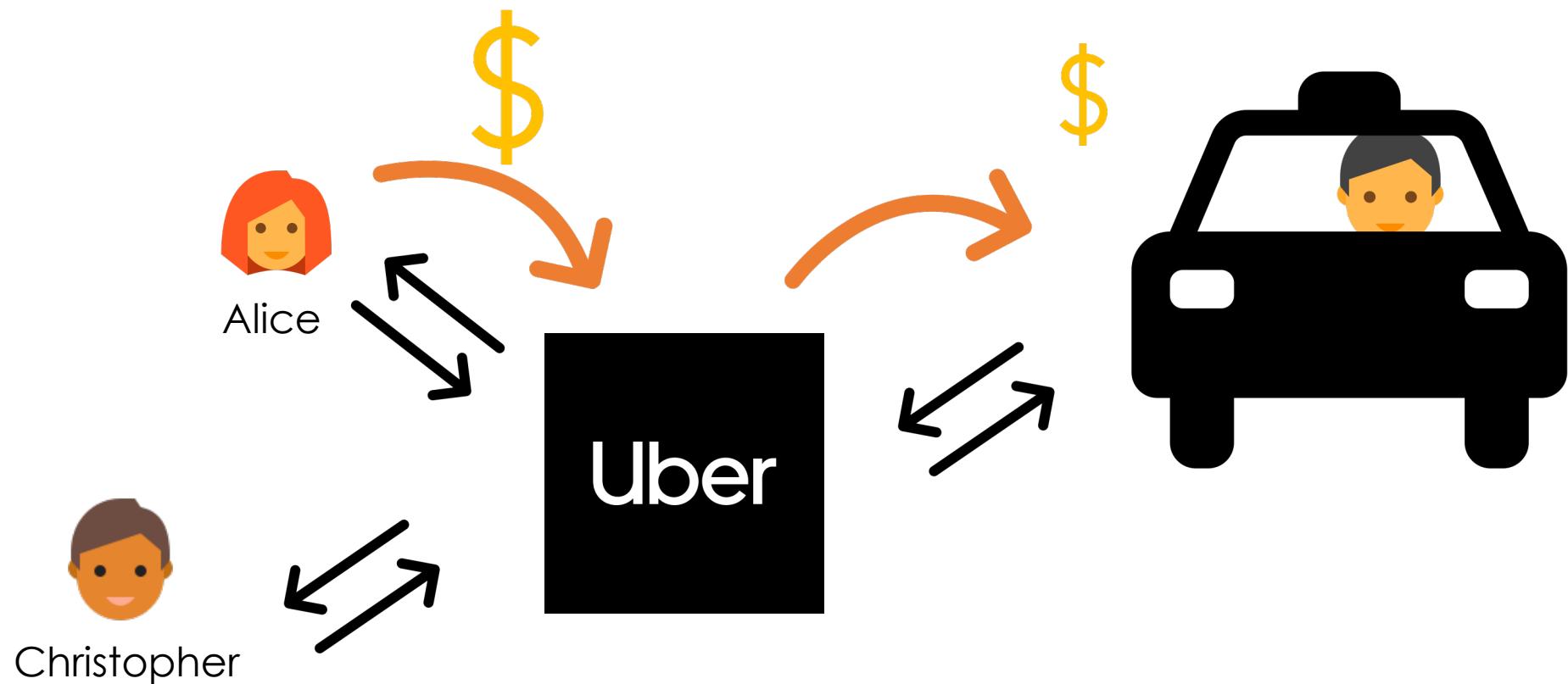
What's the problem?

Different systems different standards



What's the problem?

Reduced Value Transferred

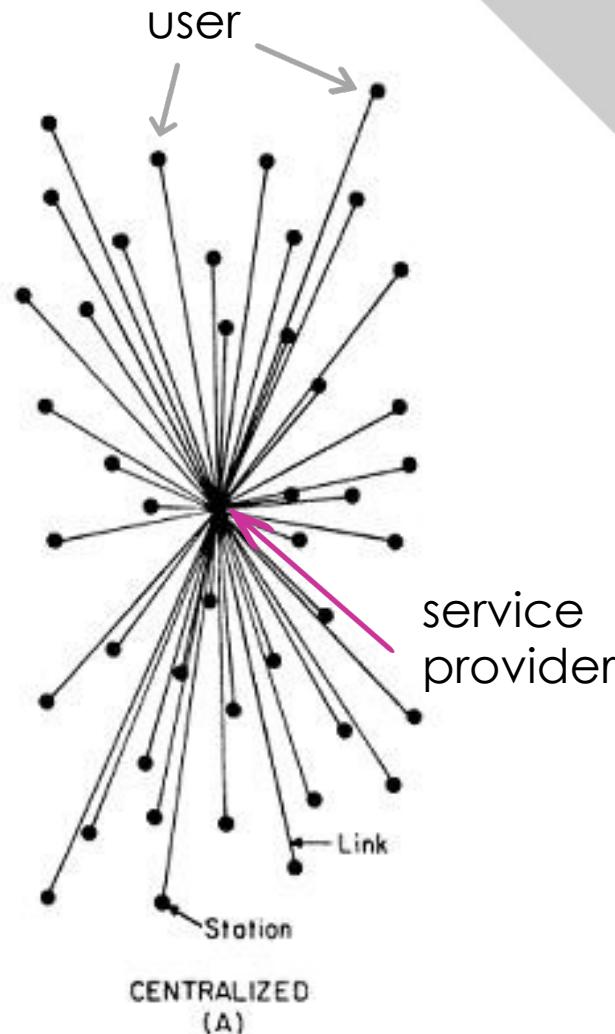




What's the problem?

Centralization is the enemy ... ?

- **Centralized** means:
 - Easy to maintain and update
 - Fast & Efficient in its closed system
 - Single source of reference & truth in its own system
 - Less work on most people
 - Different systems different standards
 - Control of data
 - No guarantee of personal privacy
 - Take a cut of the value transferred
 - Single point of failure

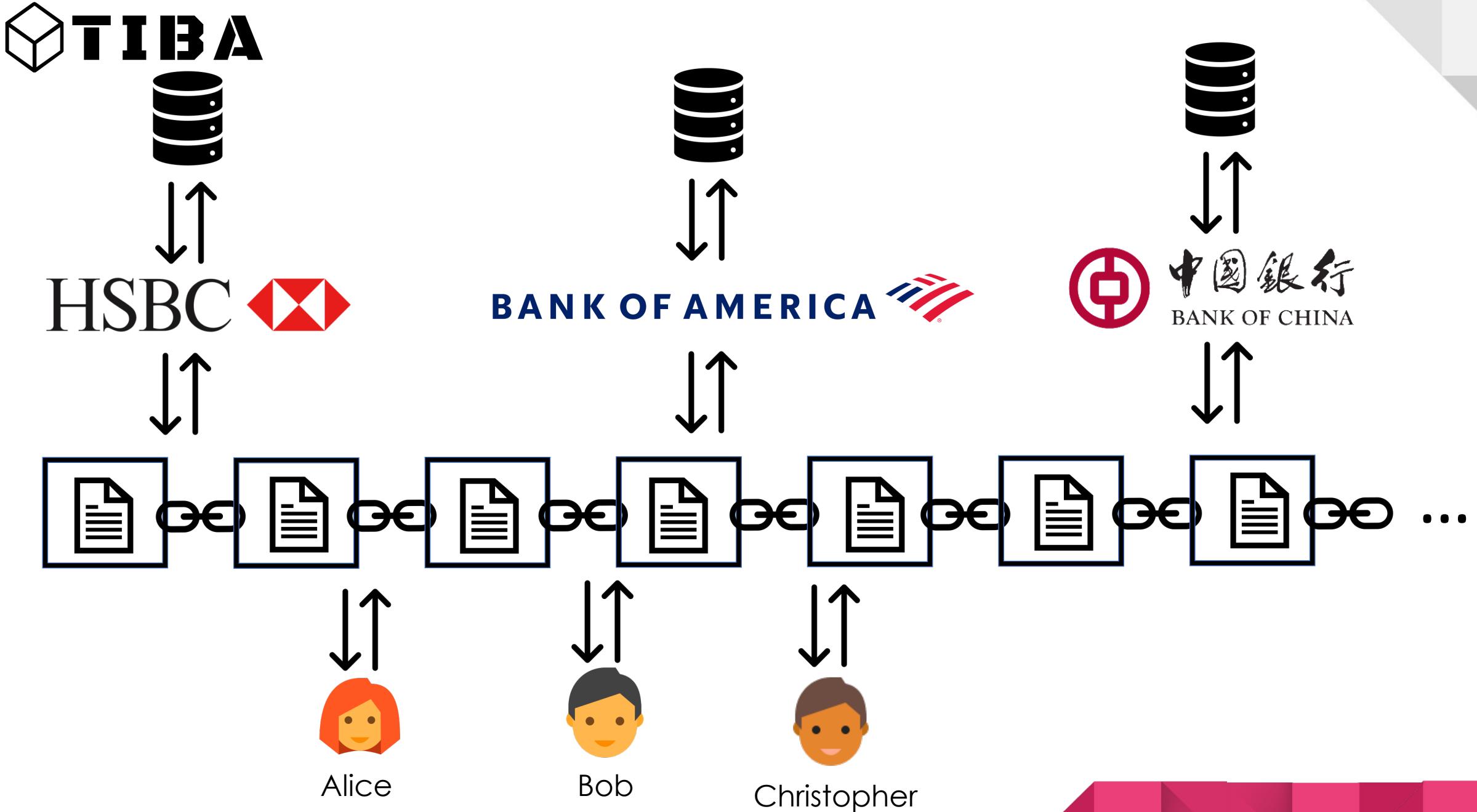




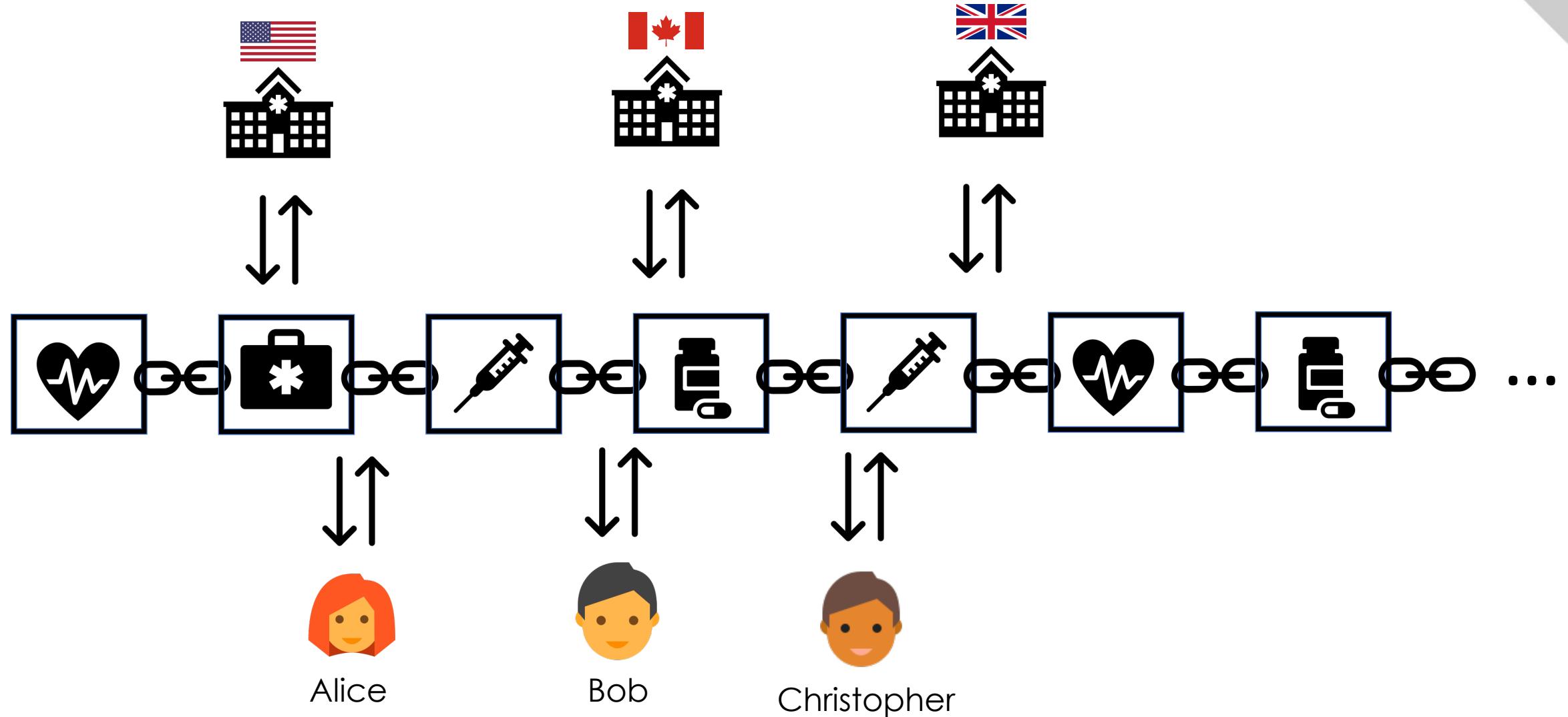
Is there a problem?

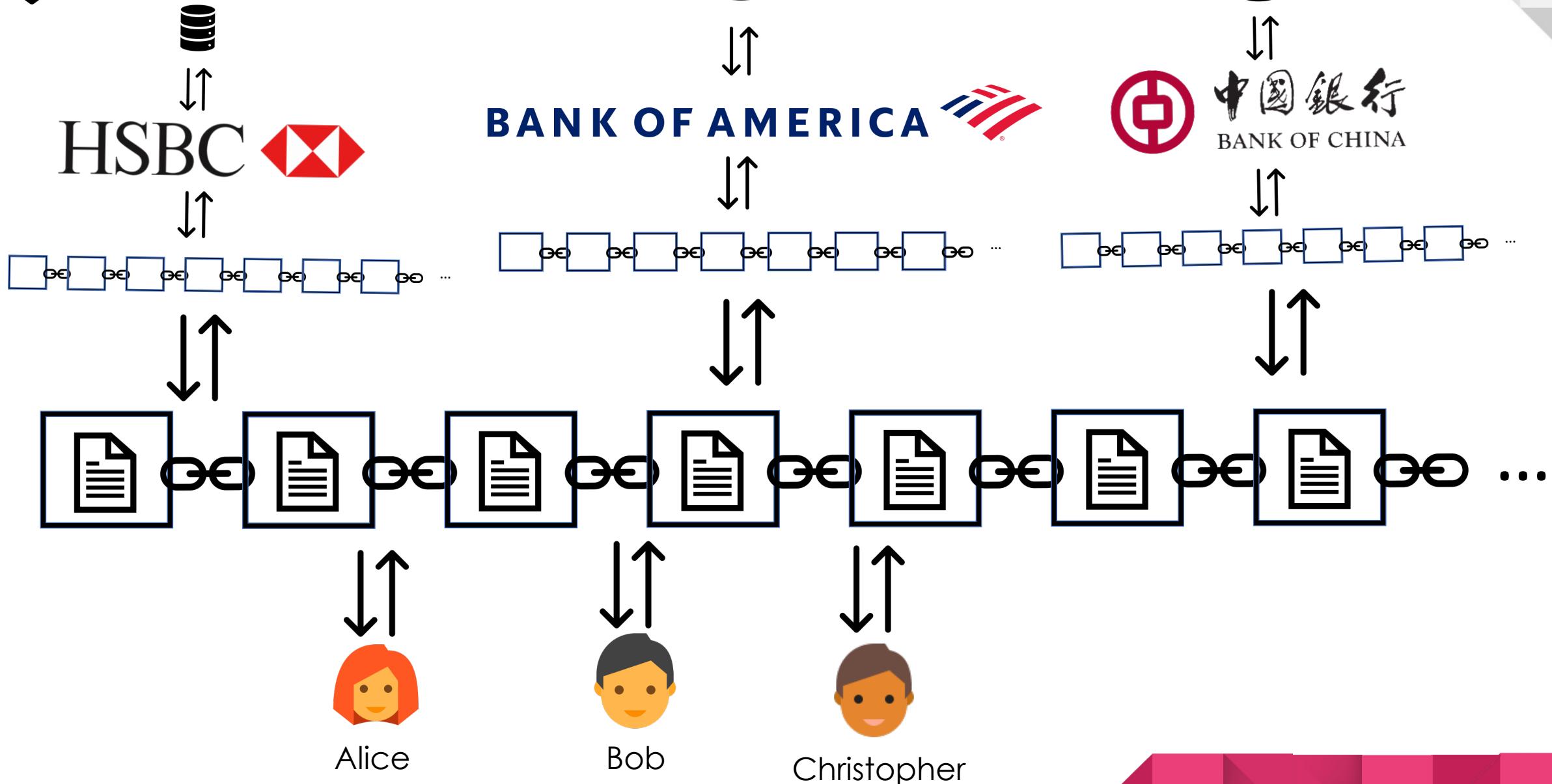
"Data is the oil of the 21st century. "





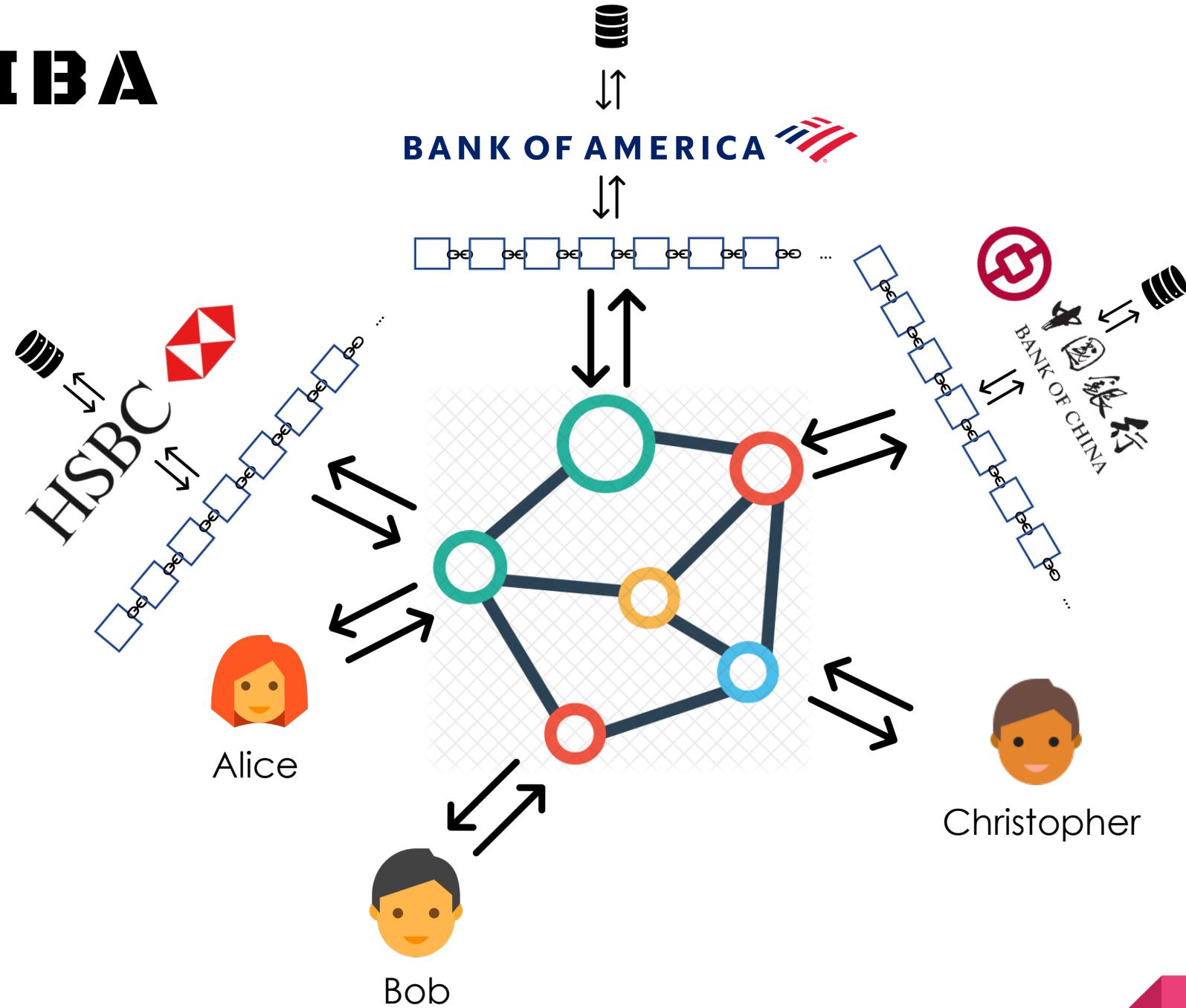
TIBA

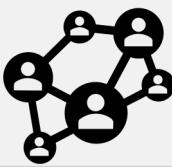




Q: Who decides the state of the blockchain?
(Who defines the single source of truth?)

A: a network of computers collectively reach a consensus

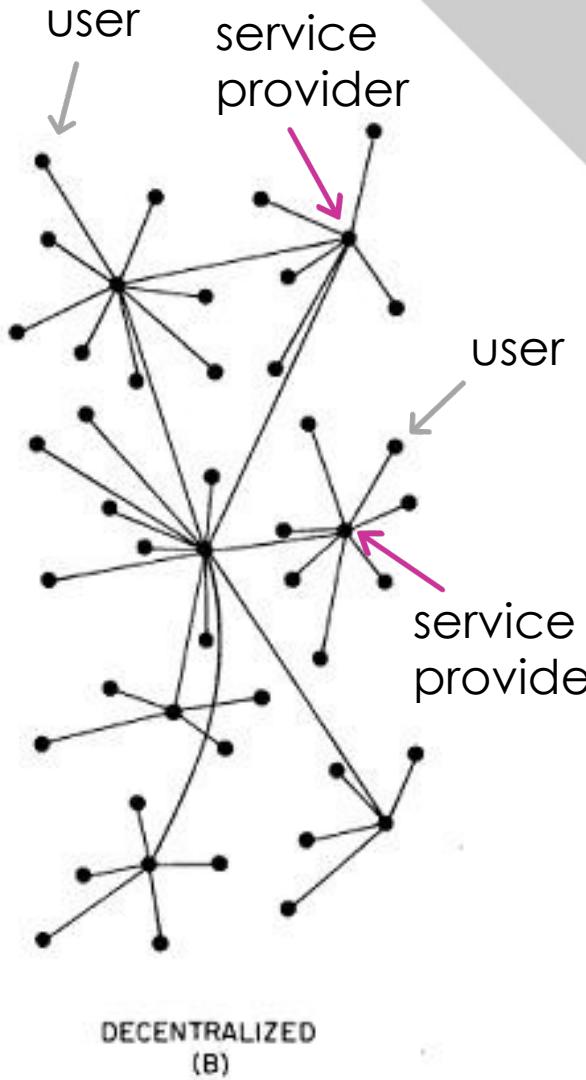


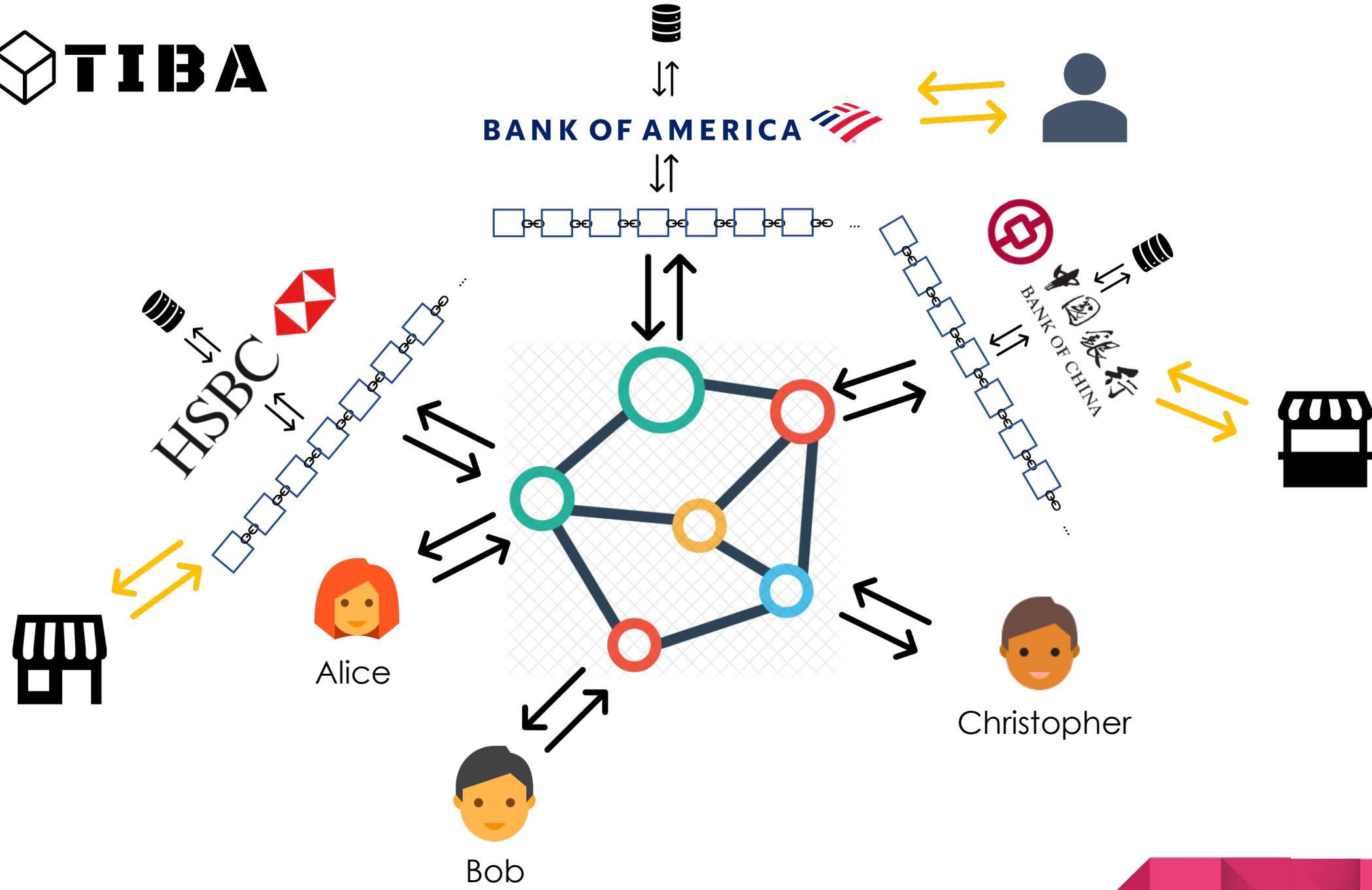


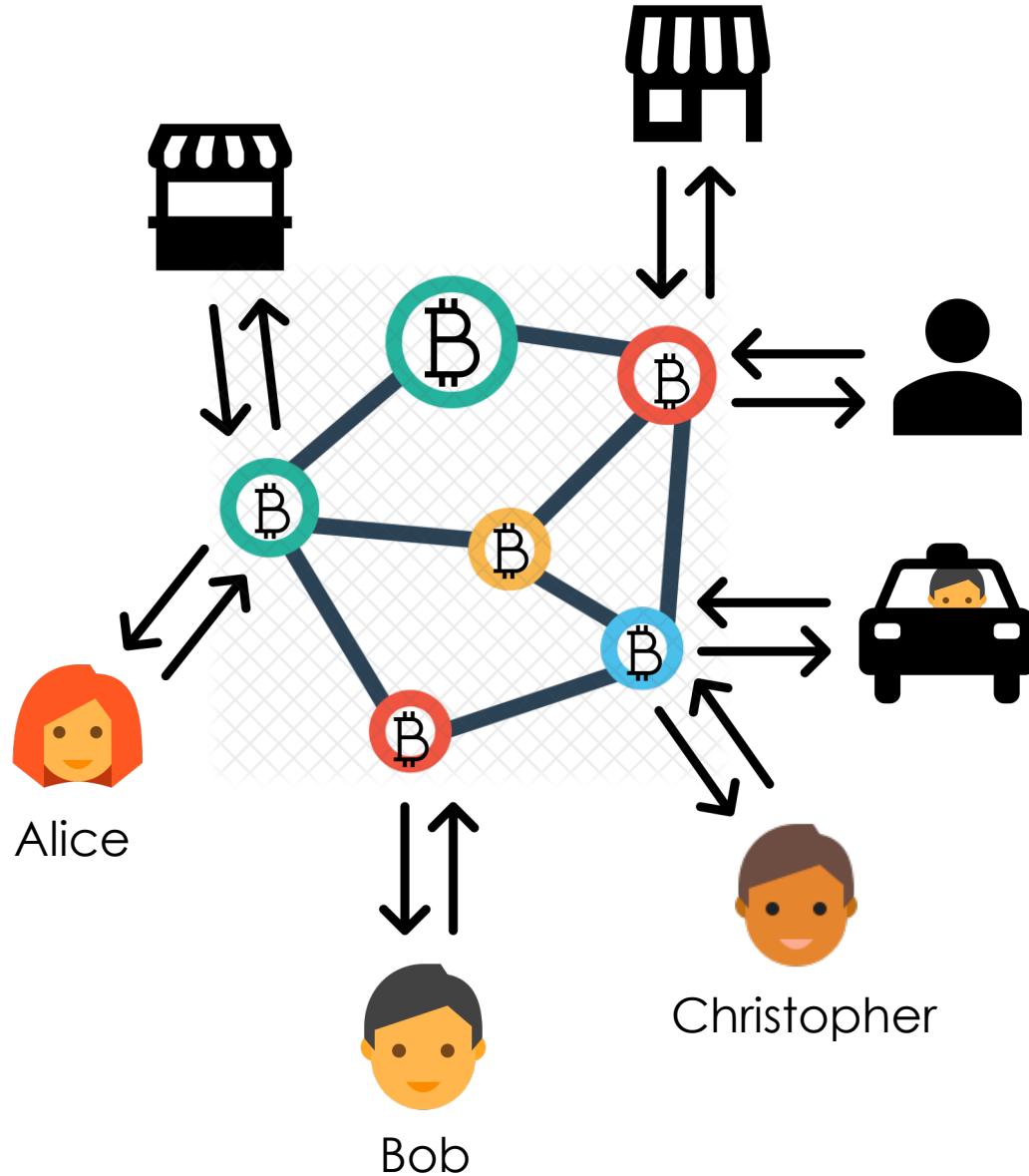
What's the solution?

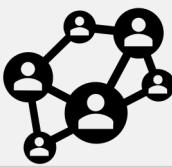
An alternative future...?

- **Decentralized** means:
 - Standardized basic-level Protocol
 - Single source of reference & truth for all
 - Democratize control of data
 - Harder to maintain and update
 - Slower and less efficient
 - More work on some people
 - Multiple points of smaller failure
 - If one got cut, connect to another!
 - Bitcoin Payment System





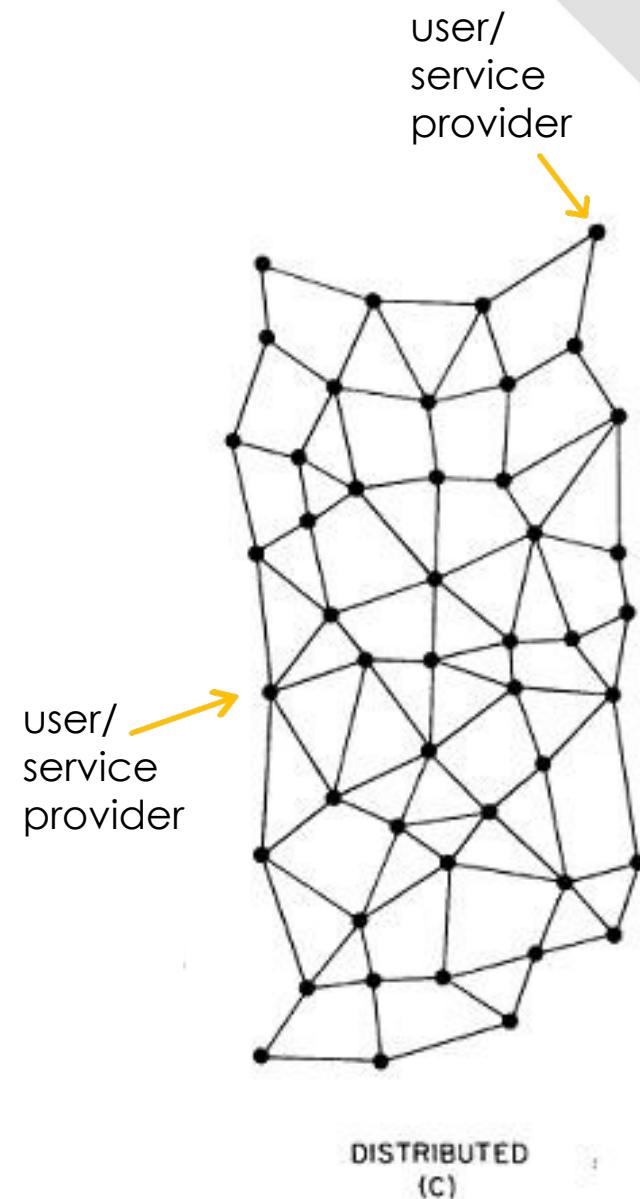
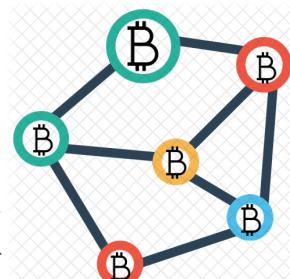




Taking to the extreme

A utopian future...?

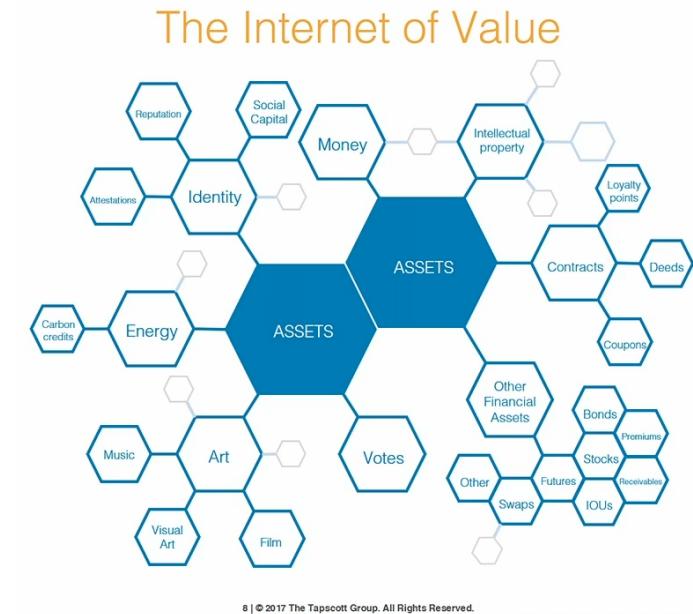
- **Distributed** means:
 - Standardized all-level Protocol
 - Single source of reference & truth for all
 - Complete control of own data
 - Even harder to maintain and update
 - Slow and less efficient
 - More work on all people
 - Near impossible to hack
- Bitcoin Peer-to-Peer Network



Internet of Value

Blockchain Enabled Internet 2.0

- Internet 1.0 = Internet of Information
 - virtually free transfer of information
 - Email
 - Video
 - ...
- Internet 2.0 = Internet of Value
 - Lower cost and secure transfer of value
 - Money
 - Asset
 - Identity
 - ...
 - Blockchain enables the peer-to-peer transfer of value



8 | © 2017 The Tapscott Group. All Rights Reserved.

Figure 2. Moving toward the Internet of value

Web 1.0/ Web 2.0

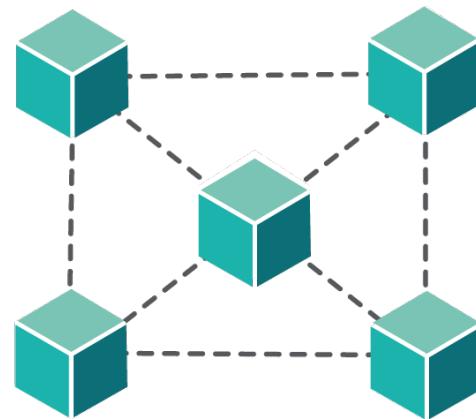
Data is copied



User 1 User 2

Blockchain

Ownership is transferred



VS.

Types of data

- Texts
- Images
- Videos
- Music

Types of transactions**Intangible assets**

- Currency
- Shares
- Copyrights
- Patents

Tangible assets

- Real estate
- Goods

Obligations

- Contracts
- Pledges

Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

Is Blockchain the Future?

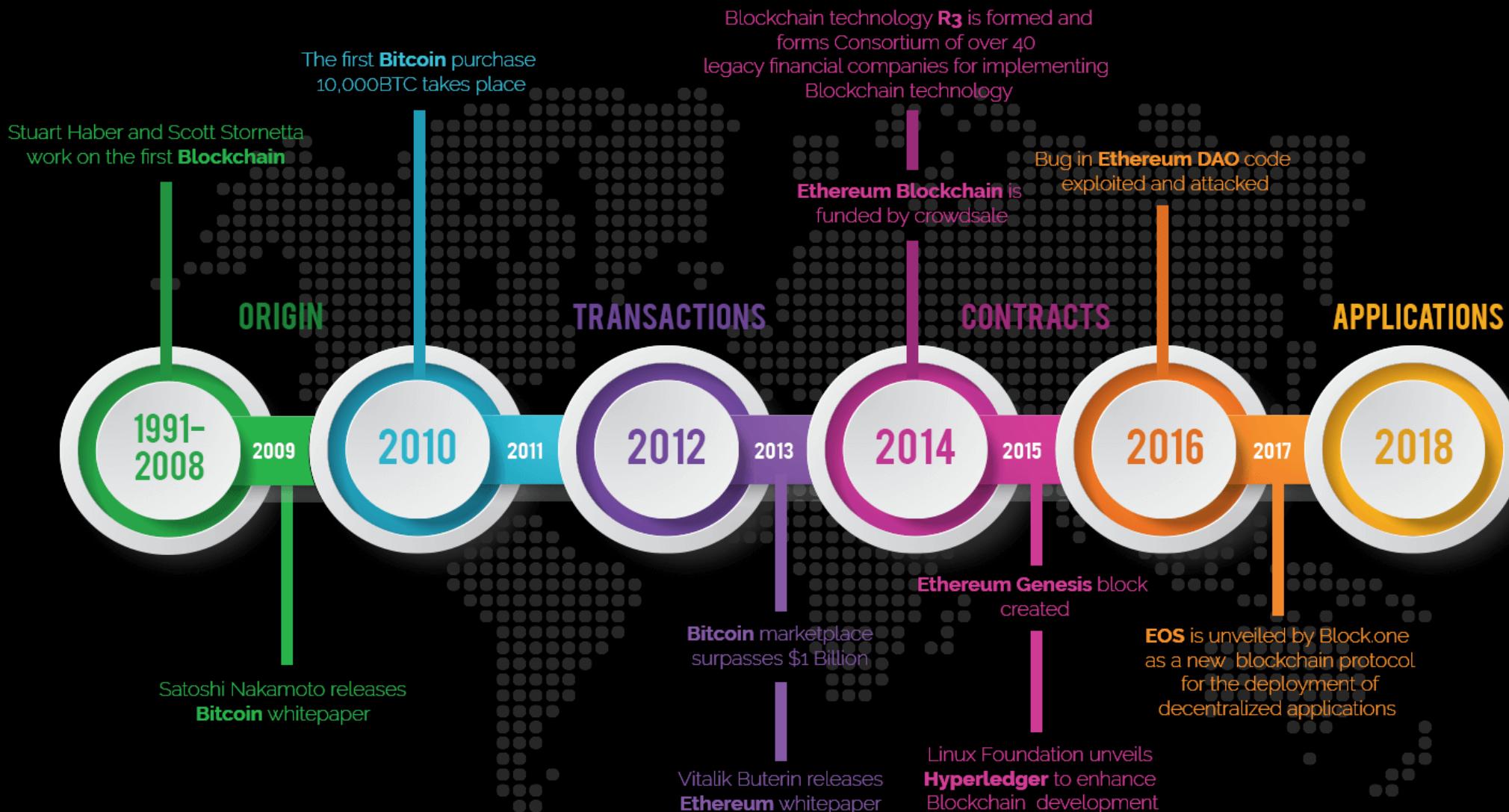
- Bubble or Revolution?
 - Buzzword/over-hyped
 - Limited applications
 - Inefficient use of resources (energy consumption, duplicate data,...)
 - Scalability problem
 - Regulation
 - Trustless system
 - Decentralization
 - Immutability
 - Transparency
 - Anonymity
- Learn & know for yourself!





Blockchain History

THE HISTORY OF BLOCKCHAIN TECHNOLOGY

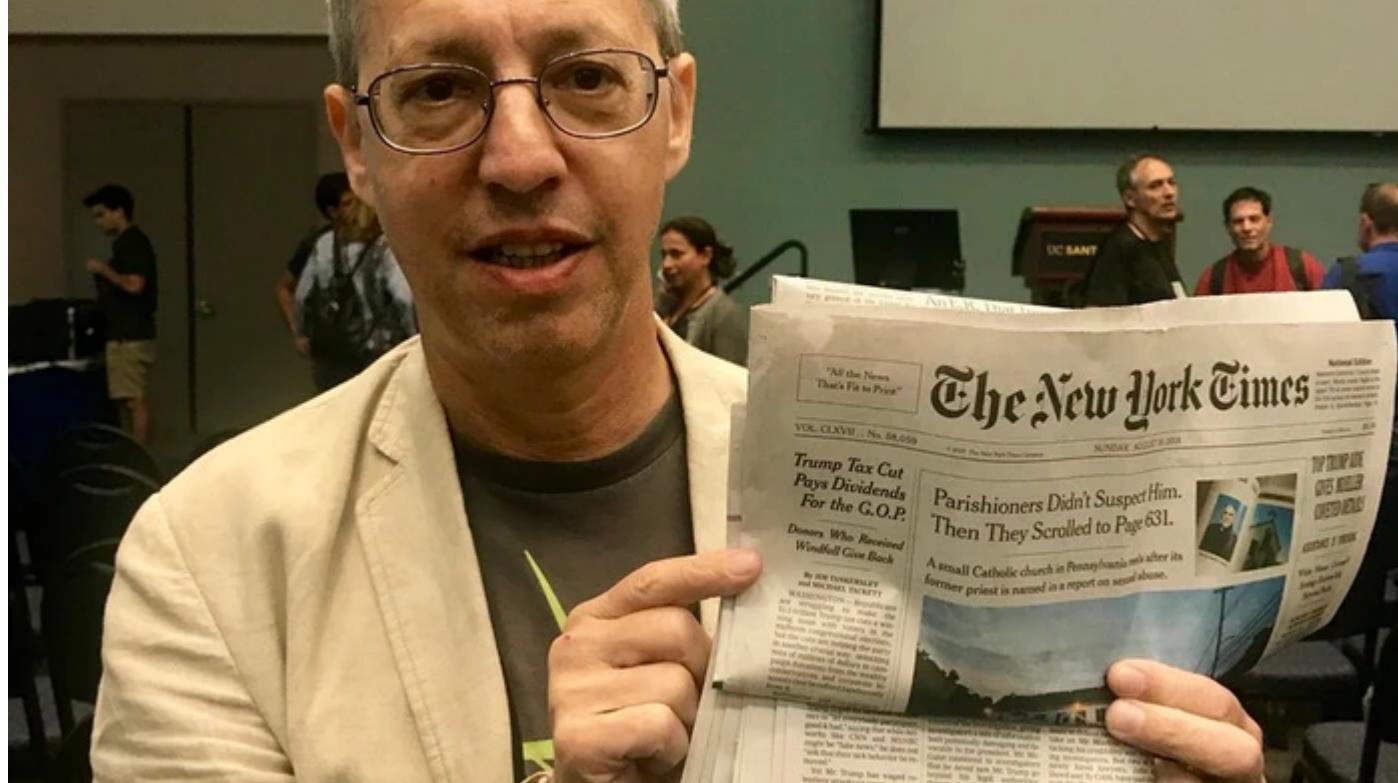




Blockchain History – Early Stage

- **1991**, cryptographer **Stuart Haber and W. Scott Stornetta** co-wrote a paper called “How to Time-Stamp a Digital Document”, where they try to use a cryptographically secured chain of blocks to secure documents.
- **1992**, incorporate Merkle trees data structure
- **1995**, founded a company called Surety, **the world's oldest running blockchain**, uses the New York Times as timestamp!

Blockchain History – Early Stage



**NOTICES &
LOST AND
FOUND
(5100-5102)**

Universal Registry Entries:
Zone 2 -

d58492cgVOFAoP9kvE1XzMOrQ
HgEwzkVbVafNyIkUz99qvq8/ME
p5y9EFSG8Xxz/MBalGQQ==

Zone 3 -

JnFCg+HCmvhj8GmmIUP7VZna71
NgZup/RfuKUQNzCHWXMuqLK
durxHQV5pSHLqBGPRIy+mg==

These base64-encoded values represent the combined fingerprints of all digital records notarized by Surety between 2009-06-03Z 2009-06-09Z.
www.surety.com 571-748-5800

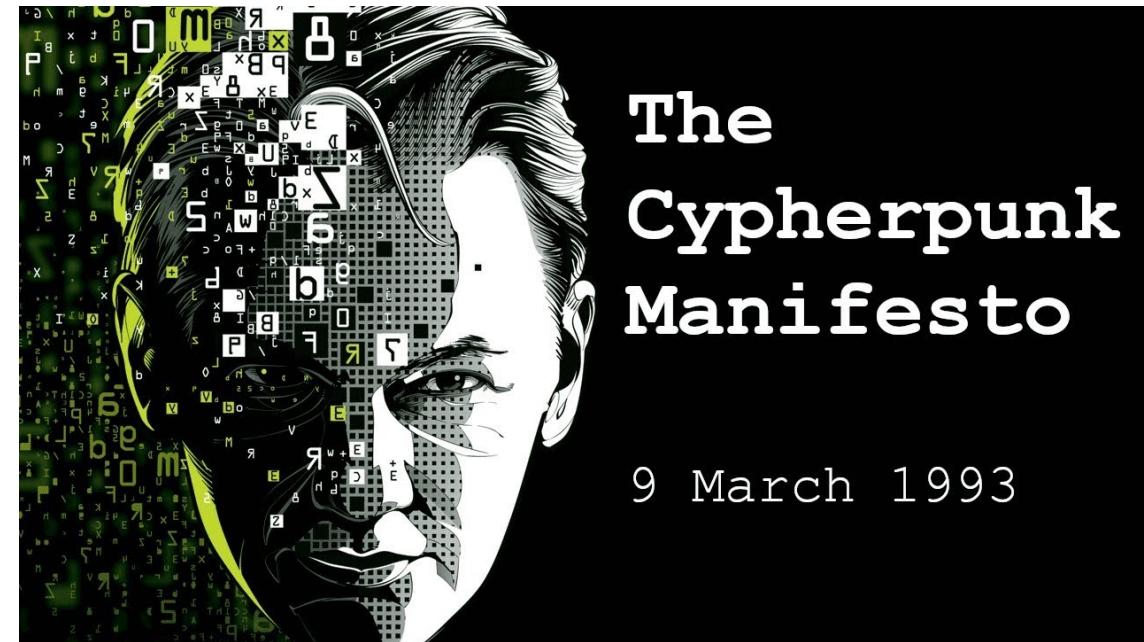
Blockchain History – Cypherpunk

- **A Cypherpunk's Manifesto
by Eric Hughes**

“Privacy is necessary for an open society in the electronic age.

Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know.

Privacy is the power to selectively reveal oneself to the world. ... ”





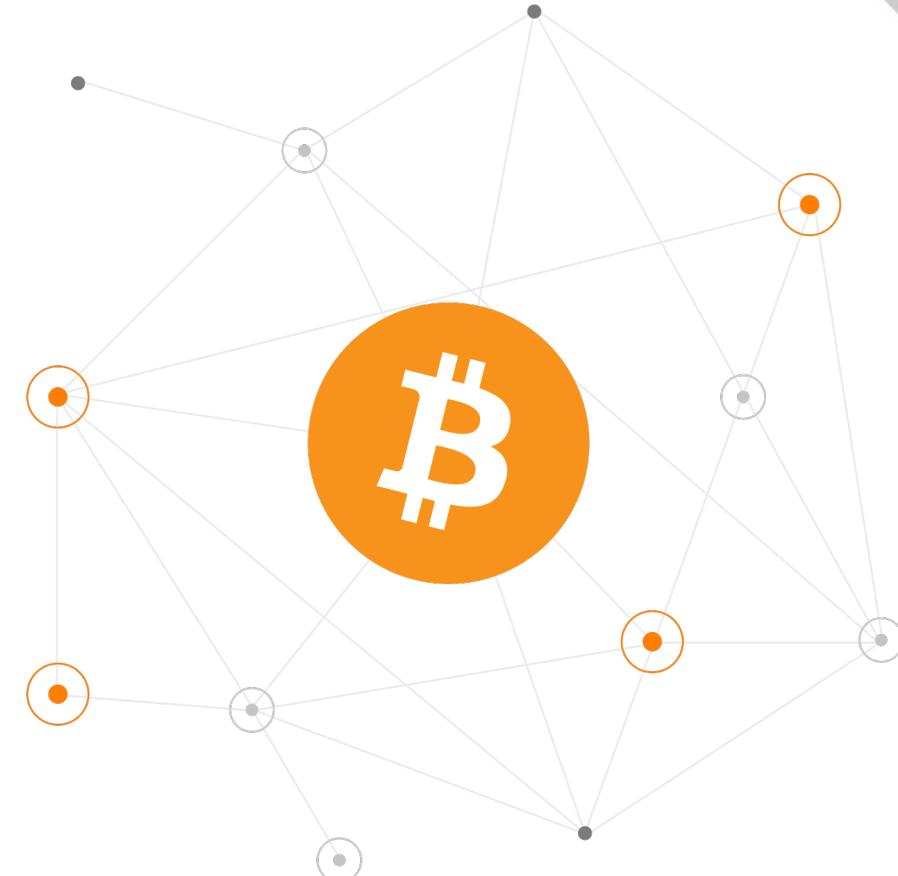
**Do you even
Bitcoin?**



What is Bitcoin?

The First Peer-to-Peer Cryptocurrency

- Bitcoin = bit + coin
= data + monetary value
- “Bitcoin (฿) is a **cryptocurrency**. It is a **decentralized** digital currency without a central bank or single administrator that can be sent from user to user on the **peer-to-peer** bitcoin network without the need for intermediaries. “ - Wikipedia





Blockchain History – Bitcoin

Just Another Email

Cryptography Mailing List

Bitcoin P2P e-cash paper

2008-10-31 18:10:00 UTC - [Original Email](#) - [View in Thread](#)

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:

<http://www.bitcoin.org/bitcoin.pdf>

Blockchain History – Bitcoin

- **August 2008**, domain name bitcoin.org was registered
- **October 2008**, a paper titled “*Bitcoin: A Peer-to-Peer Electronic Cash System*” was published by the name **Satoshi Nakamoto**
- **January 2009**, Satoshi mined the genesis block of the bitcoin blockchain (block number 0), with a reward of 50 bitcoins

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.



Source: The Face Behind Bitcoin, Newsweek, <https://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html>



Bitcoin Creator

- **Satoshi Nakamoto**, a pseudonym!
- Several potential suspects:
 - Hal Finny (Bitcoin network's first transaction recipient)
 - NSA (US National Security Agency)
 - Dorian Nakamoto (a Japanese American computer engineer, whose birth name is Satoshi Nakamoto)
 - Craig Wright (self-claim to be Satoshi)
 - Nick Szabo (proposed the idea of smart contract)
 - ...
- no one knows for sure and it'll likely remain this way

Blockchain History – Bitcoin

- **January 2009**, first bitcoin transaction (Satoshi to **Hal Finney**)
- **May 2010**, \$25 worth of pizza for 10,000 BTC, purchased by **Laszlo Hanyecz** (Bitcoin has real value!)



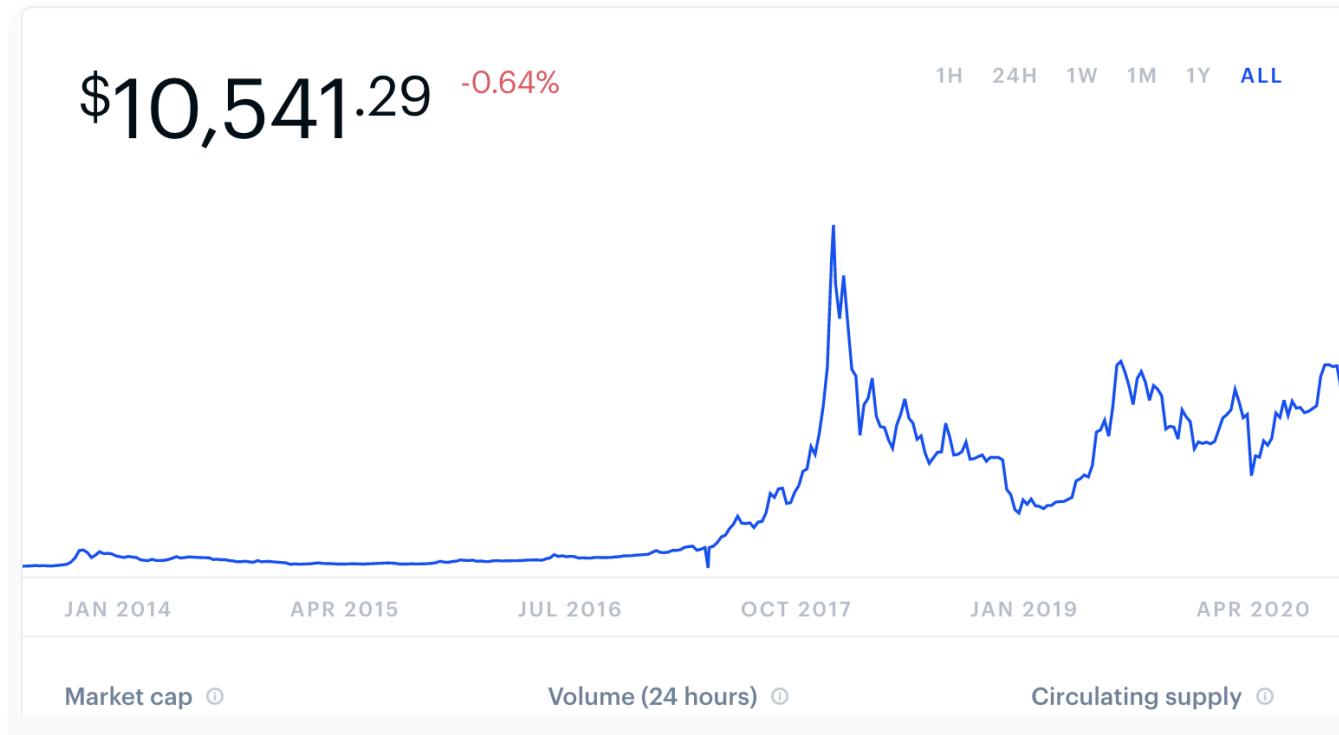
Blockchain History – Bitcoin



- **Oct 2, 2020,**
10,000 BTC
=
105,431,000 USD

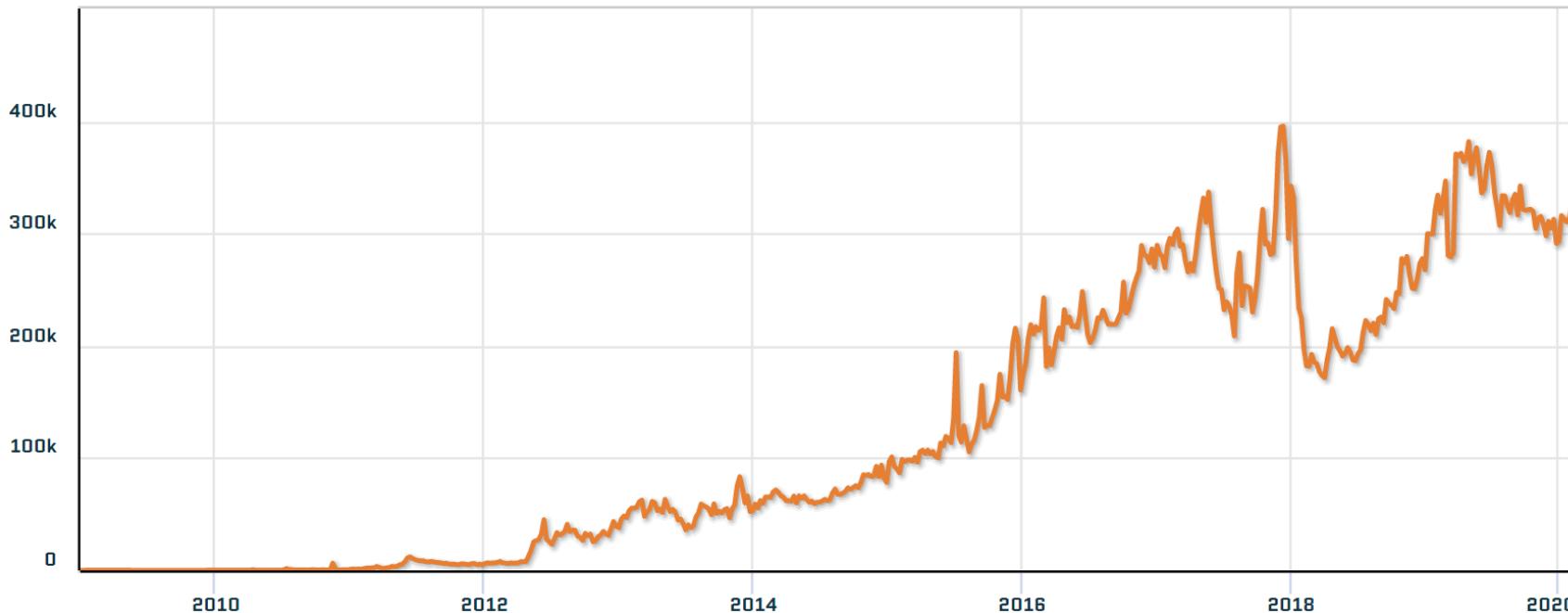
Blockchain History – Bitcoin

 Bitcoin price (BTC)



- Oct 2, 2020, 17:04 US ET
1 BTC = 10,541.29 USD

Blockchain History – Bitcoin



- Number of Bitcoin transactions over the years



Blockchain History – Bitcoin

Mt.Gox – the Centralized Exchange for Decentralized Bitcoin

- **July 2010, Mt. Gox** was launched by **Jed McCaleb**, the biggest online Bitcoin exchange platform
- **June 2011**, suffered a significant security breach which allow the hacker to change the Bitcoin pricing to a single cent
- **End of 2013**, handled over **70%** of all Bitcoin (BTC) transactions worldwide



Source: https://en.wikipedia.org/wiki/Mt._Gox

Reading: <https://www.coindesk.com/2-billion-lost-in-mt-gox-bitcoin-hack-can-be-recovered-lawyer-claims>



Blockchain History – Bitcoin

Mt.Gox

- **February 2014, Mt. Gox** was hacked and filed for bankruptcy
- **Mt. Gox** lost about 850,000 bitcoins, (750,000 belonged to its customers) valued more than \$450 million, at the time and \$8.5 billion today



Source: https://en.wikipedia.org/wiki/Mt._Gox; <https://www.theverge.com/2014/2/19/5425220/protest-at-mt-gox-bitcoin-exchange-in-tokyo>

Reading: <https://www.coindesk.com/2-billion-lost-in-mt-gox-bitcoin-hack-can-be-recovered-lawyer-claims>

<https://www.ledger.com/hack-flasback-the-mt-gox-hack-the-most-iconic-exchange-hack/>



Blockchain History – Bitcoin

Mt.Gox

- 200,000 bitcoins were eventually recovered, the remaining 650,000 (3.7% of Bitcoin's circulating supply) have never been recovered
- The victims of the **Mt.Gox** hack have not seen a Satoshi of their Bitcoins returned to this day
- The Bitcoin price **drop to nearly 50%** of its value prior to the hack. It took till the end of 2016 to return to the same value





Blockchain History – Bitcoin

Silk Road – Bitcoin's Anonymity is Perfect for Illegal Activities

- **February 2011**, **Ross Ulbricht** used **Tor**(anonymous communication) and **Bitcoin**(anonymous transaction) to create an online black market for drugs
- <http://tdgccccykixpbu6uz.onion>
- February 2012, **Ross Ulbricht** called himself Dread Pirate Roberts



SNAPSHOT OF THE SILK ROAD

THE SITE HAS HAD LISTINGS FOR:

ILLEGAL DRUGS

COUNTERFEIT
CASH

FORGED
DOCUMENTS

HACKERS

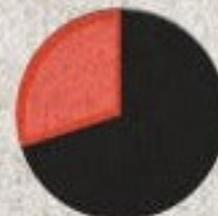
FIREARMS &
AMMUNITION



It lasted

2 ½ YEARS

before being shut down
upon Ulbricht's arrest.



The indictment
stated it had nearly

1 MILLION
registered users.

30% were based in the U.S.

One analysis showed Silk
Road received about

**60,000
VISITS DAILY.³**

ACCORDING TO THE COMPLAINT, SILK
ROAD PROCESSED TRANSACTIONS
WORTH MORE THAN



9.5 MILLION BITCOINS
ABOUT \$1.2 BILLION IN SALES.²

Blockchain History – Bitcoin

Silk Road – the Downfall

- **October 2013**, FBI arrested Ross Ulbricht and shut down the website
- **May 2015**, Ross sentenced To double life imprisonment without the possibility of parole
- **October 2015**, two agents involved with the case charged with corruption
- **Silk Road 2.0** shut down by FBI and Europol on 6 November 2014
- **Silk Road 3.0** went offline in 2017 due to loss of funds



THE RISE & FALL O F S I L K R O A D

Part I

How a 29-year-old idealist built a global drug bazaar and became a murderous kingpin.

BY JOSHUA BEARMAN
● TOMER HANUKA
with additional reporting
by Joshua Davis and Steven Leckart





More on Silk Road

- Forbes, 2019, ["Best Stories Of The Decade: 'Meet The Dread Pirate Roberts, The Man Behind Booming Black Market Drug Website Silk Road'"](#),
- Newsweek, 2015, ["The Rise and Fall of Silk Road, the Dark Web's Amazon"](#),



DIGITAL GOLD

BITCOIN AND THE
INSIDE STORY OF
THE MISFITS AND
MILLIONAIRES TRYING
TO REINVENT MONEY

NATHANIEL POPPER

Blockchain History – Ethereum

What is Ethereum?

- **Ethereum** is a public blockchain-based distributed computing platform featuring **smart contract**
 - Ethereum VM, decentralized Turing-complete virtual machine for executing scripts
 - “ether”, cryptocurrency token
 - “gas”, a priced resource for computation

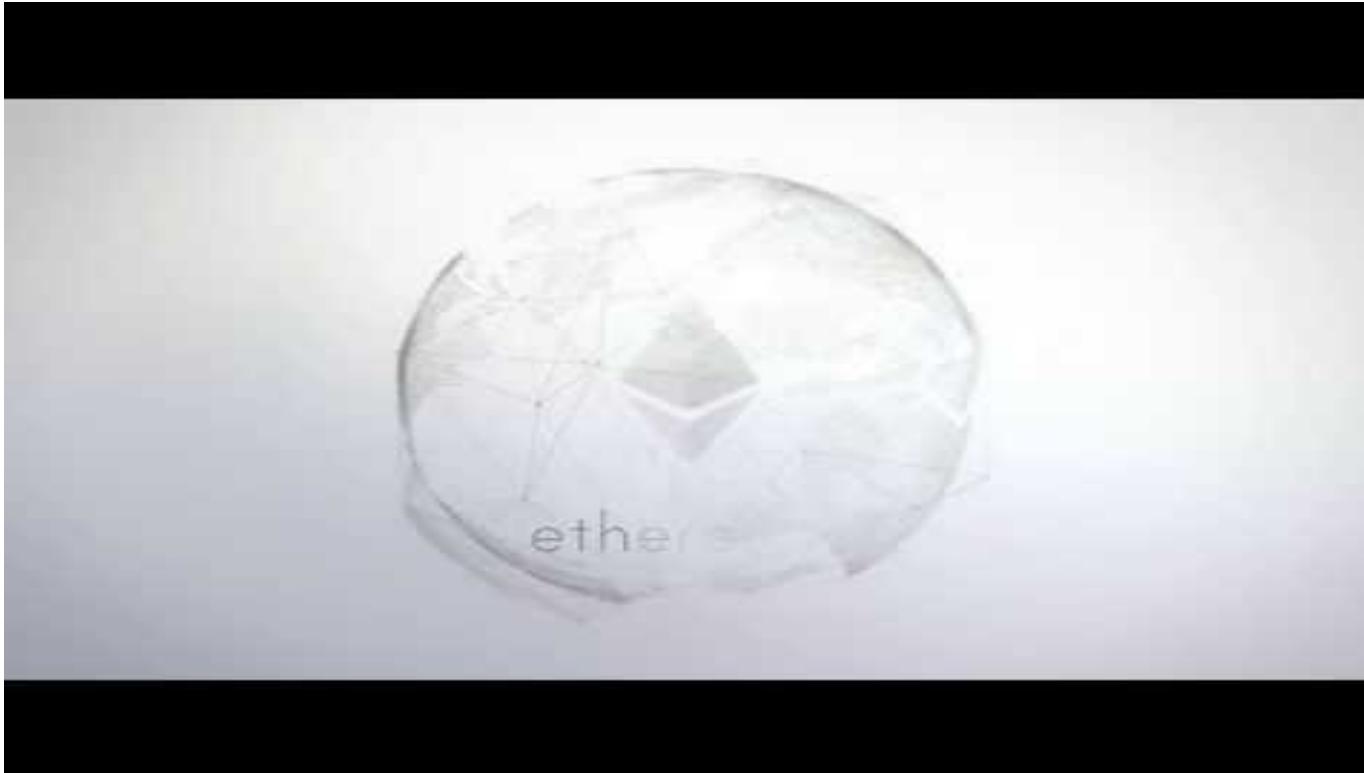


ethereum



Blockchain History – Ethereum

Ethereum: the World Computer

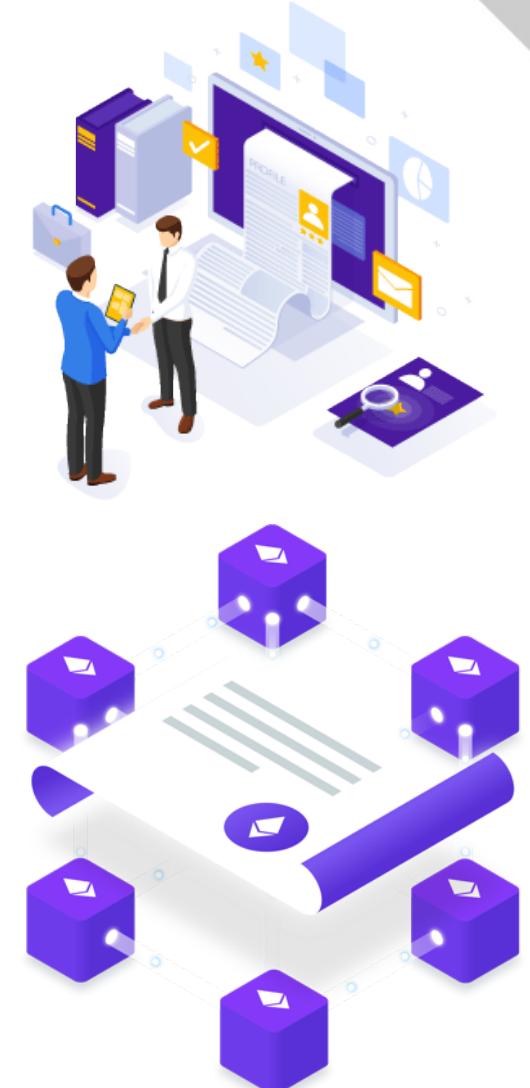


ethereum

Blockchain History – Ethereum

Smart Contract

- A **smart contract** is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code
- The code is stored on and exist across a distributed, decentralized **blockchain** network
- first proposed in 1994 by **Nick Szabo** (invented "Bit Gold" in 1998)



Blockchain History – Ethereum

Ethereum History – The Beginning

- **November 2013**, **Vitalik Buterin** published the Ethereum whitepaper
- **June 2014**, Ethereum foundation founded
- **July & August 2014**, Ethereum crowdsale, future users and investors allowed to purchase Ether in exchange for Bitcoin, 11.9 million Ethereum tokens were sold (about 13% of the circulating supply), raising about 18.4 million USD



Source:

<https://www.coinmama.com/guide/history-of-ethereum> ;

<https://www.cnbc.com/2018/02/19/ethereum-creator-vitalik-buterin-warns-about-cryptocurrency-investment.html>

Blockchain History – Ethereum

Ethereum History

- **July 2015**, Ethereum blockchain launched
- **May 2016**, Value of Ethereum tokens worth more than \$1 billion
- **July 2016**, the Dao hack



Blockchain History – Ethereum

The Dao Hack

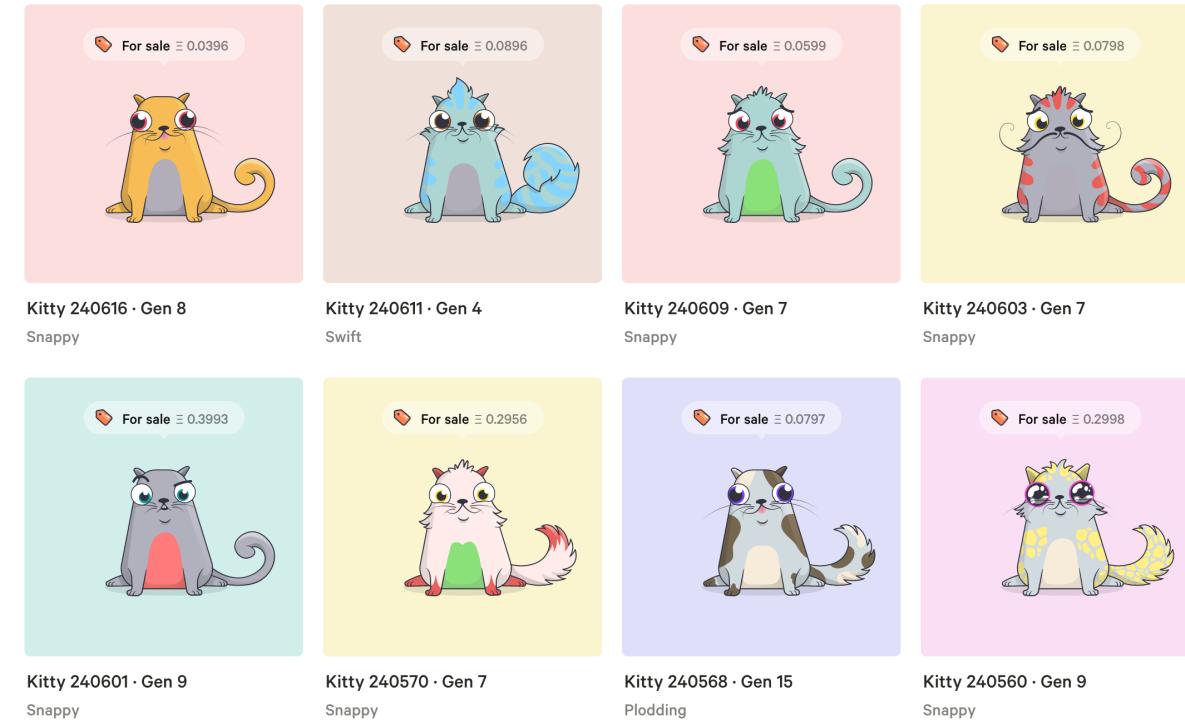
- **Dao**(Decentralized autonomous organization)
 - a complicated smart contract that allows any app idea to be voted on by token holders
 - “**The DAO**” was a specific DAO created on the Ethereum blockchain, raised over 150 million USD with crowdsale
 - **June 2016**, an unknown attacker exploited the vulnerability and withdrew 50 million USD in Ether from the smart contract (roughly 15% of all Ether at the time)

Blockchain History – Ethereum

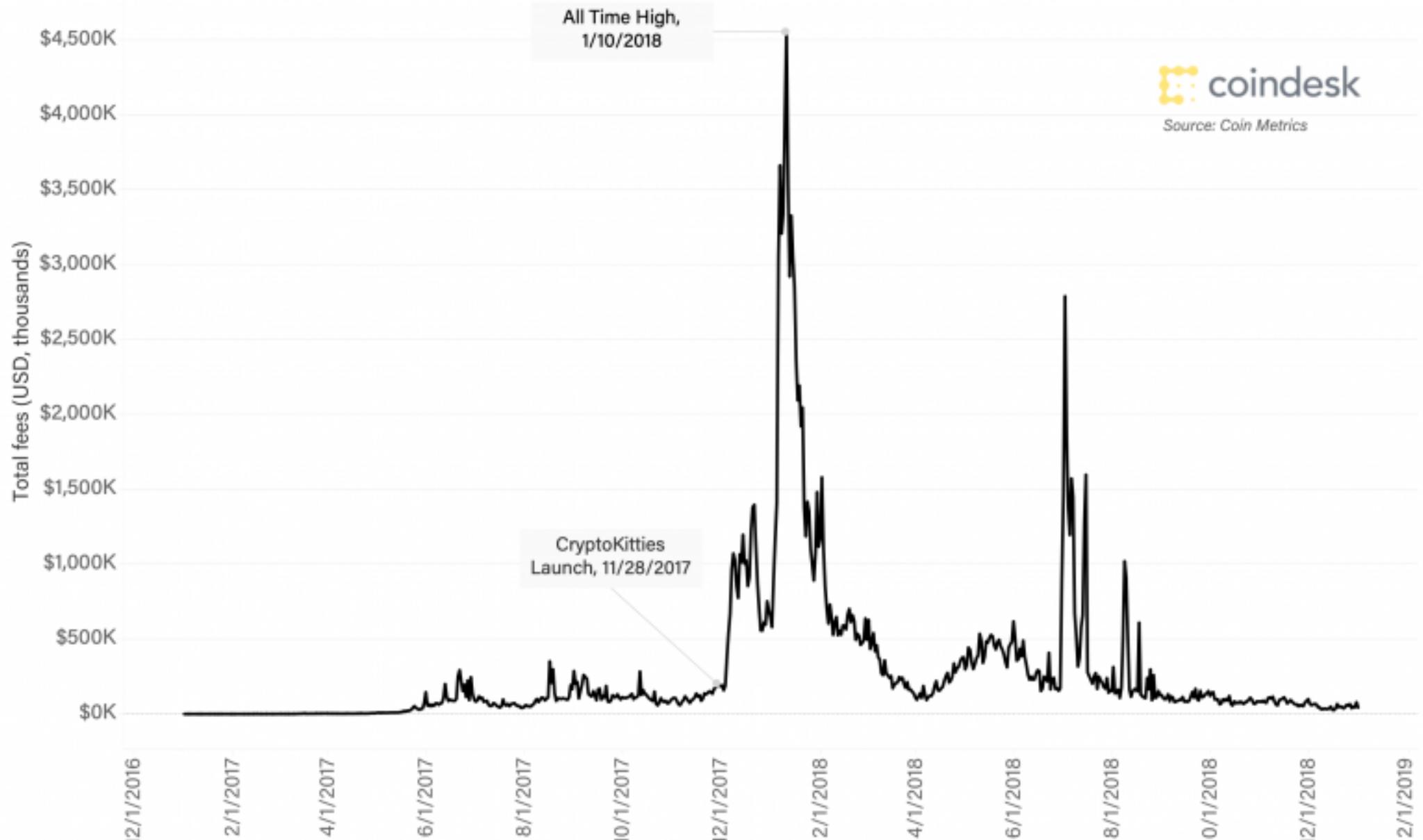
CryptoKitties

- **CryptoKitties**

- <https://www.cryptokitties.co/>
- A blockchain application built on Ethereum
- Launched November 28, 2017
- “CryptoKitties is a game centered around breedable, collectible, and oh-so-adorable creatures we call CryptoKitties! Each cat is one-of-a-kind and 100% owned by you; it cannot be replicated, taken away, or destroyed.”



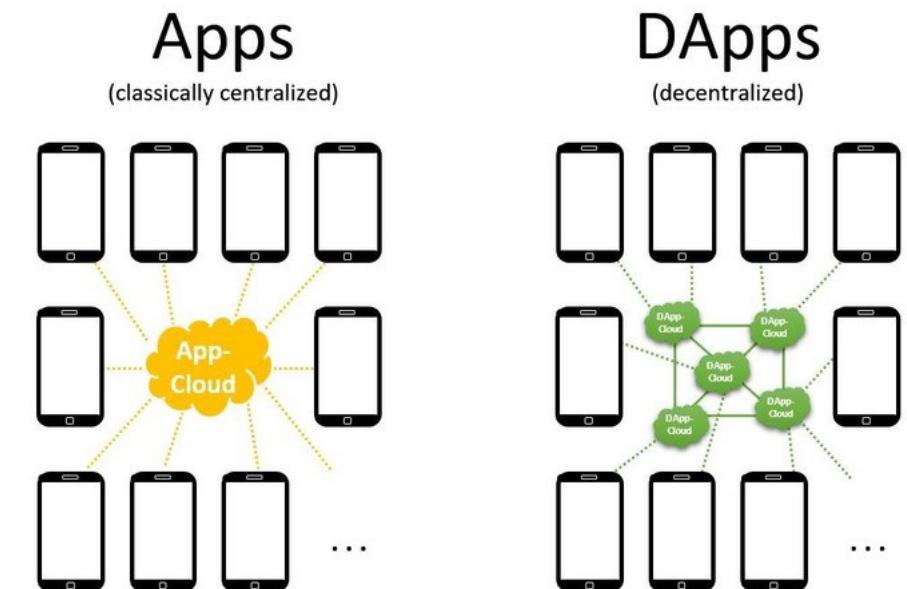
Daily transaction fees on ethereum from 2017-2018



Blockchain History – Ethereum

DApps

- **Dapps (Decentralized Applications)**
 - Ethereum becomes the go-to platform for creating dapps



Blockchain History – Ethereum



- Oct 2, 2020,
17:06 US ET
1 ETH = 346.30 USD

Blockchain History

Bitcoin vs. Ethereum



	bitcoin	ethereum
concept	digital money	smart contracts
transaction	send from alice to bob	send from alice to bob if.. <ul style="list-style-type: none">• date = jan 1, 2018• bob's balance < 10 eth
market cap (as of feb 2017)	~\$18 billion	~\$1 billion
founder	satoshi nakamoto (unknown)	vitalik buterin and team
release date	jan 2009	july 2015



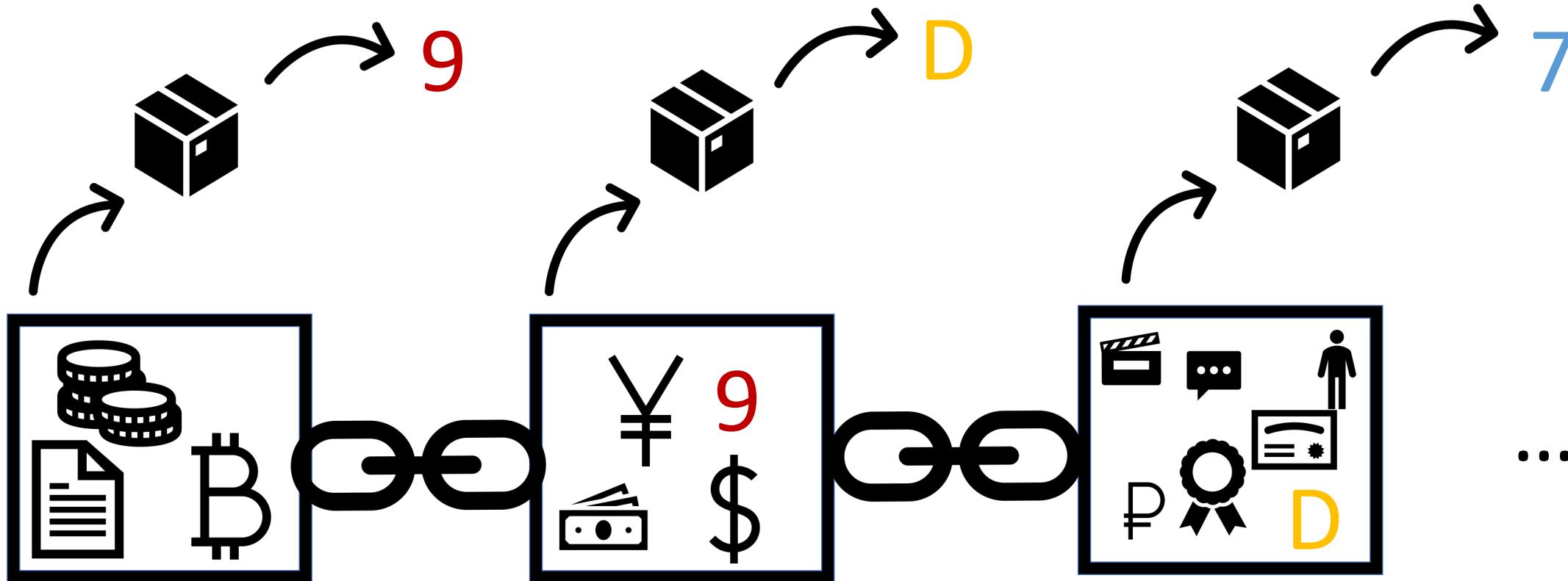
What is Blockchain?

Blockchain Definition

Blockchain = Block + Chain

“Blockchain is a data structure that's **secure** (tamper-resistant) by the nature of cryptography and a **decentralized** database by giving a network of users each a copy of the data and the possible ability to modify those data and a **trustless system/distributed network** by allowing users to constantly check on one another to reach a single consensus.”

- Samuel Tang



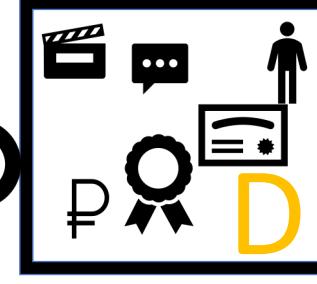
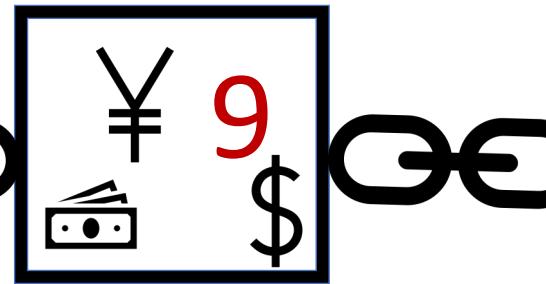
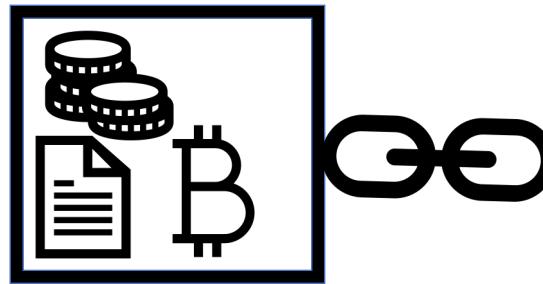
9

D

7



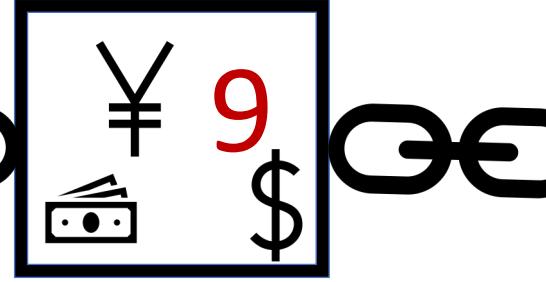
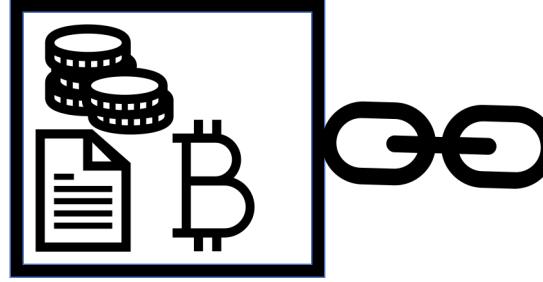
Alice



...



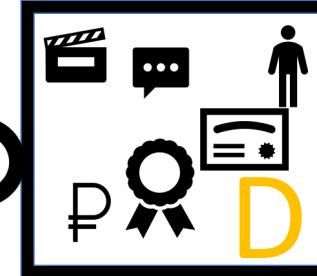
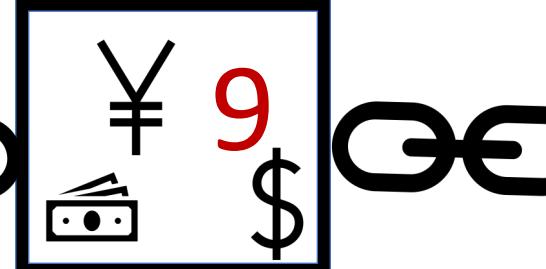
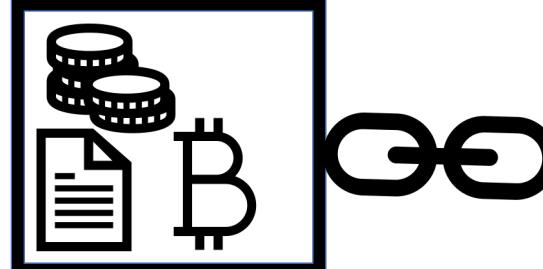
Bob



...



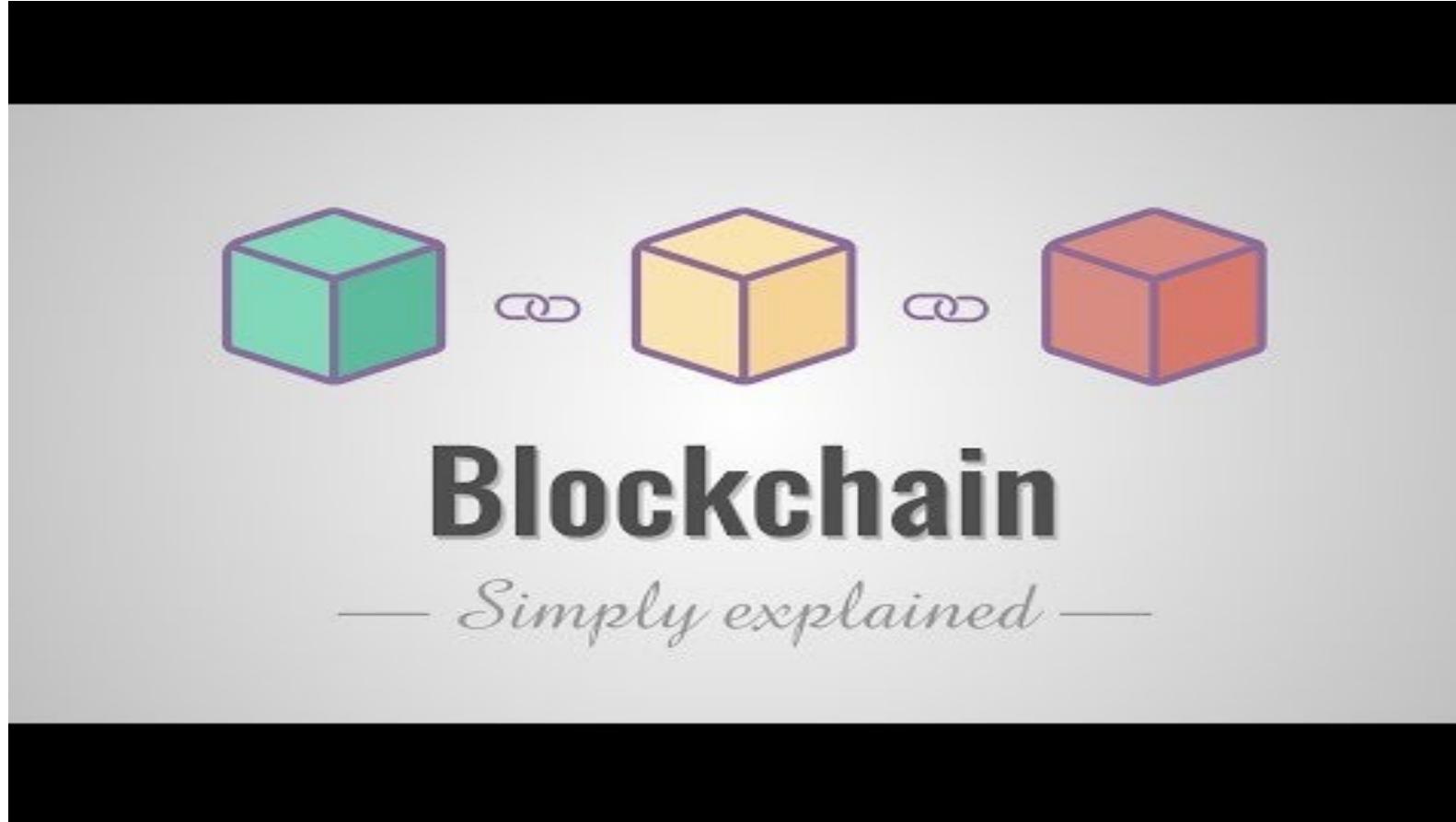
Christopher



...



Blockchain Definition



Source: Simply Explained – Savjee, Youtube
https://www.youtube.com/watch?v=SSo_ElwHSd4

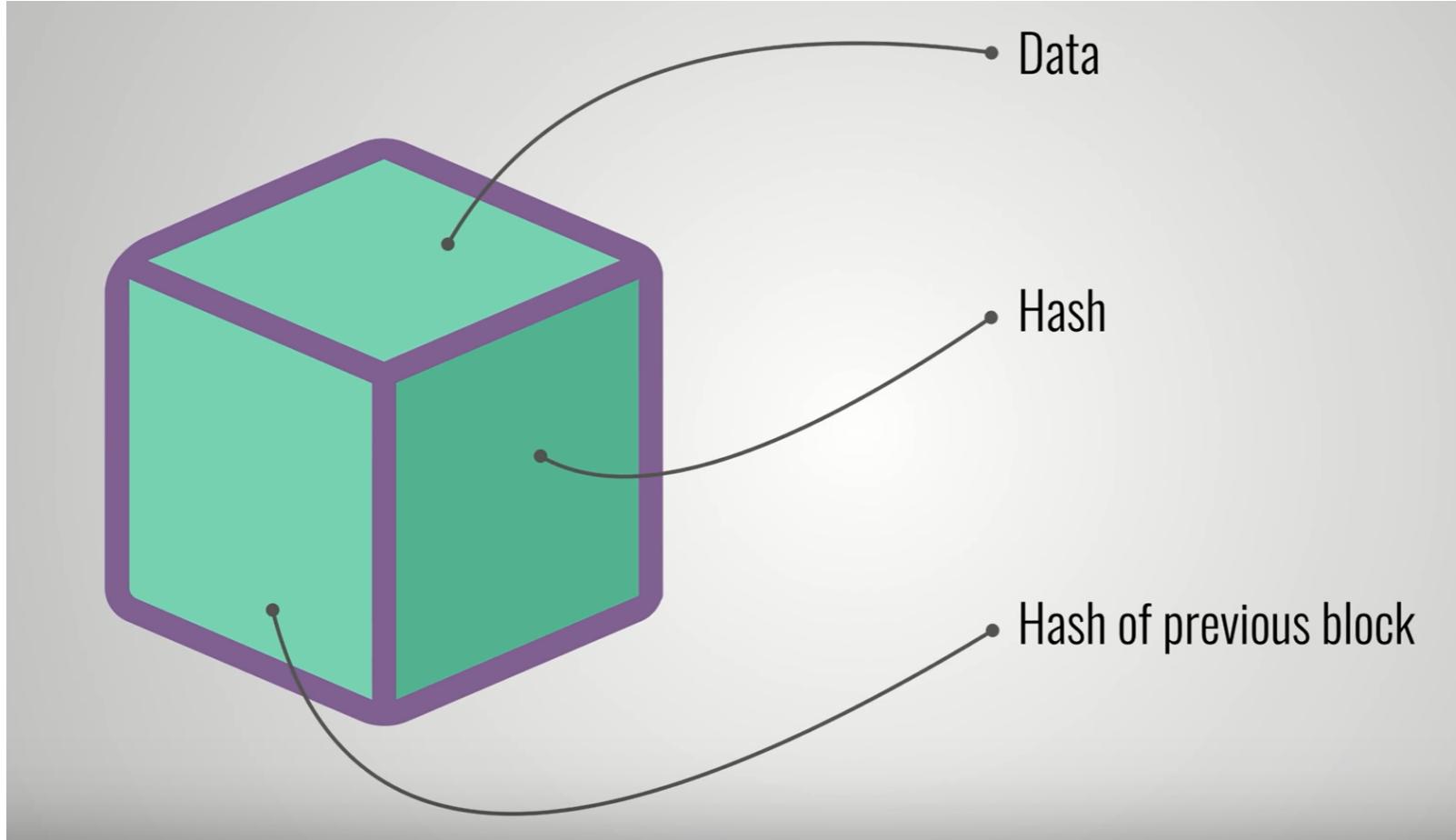
By:



Simply Explained - Savjee
158K subscribers

Blockchain Definition

Data Storage



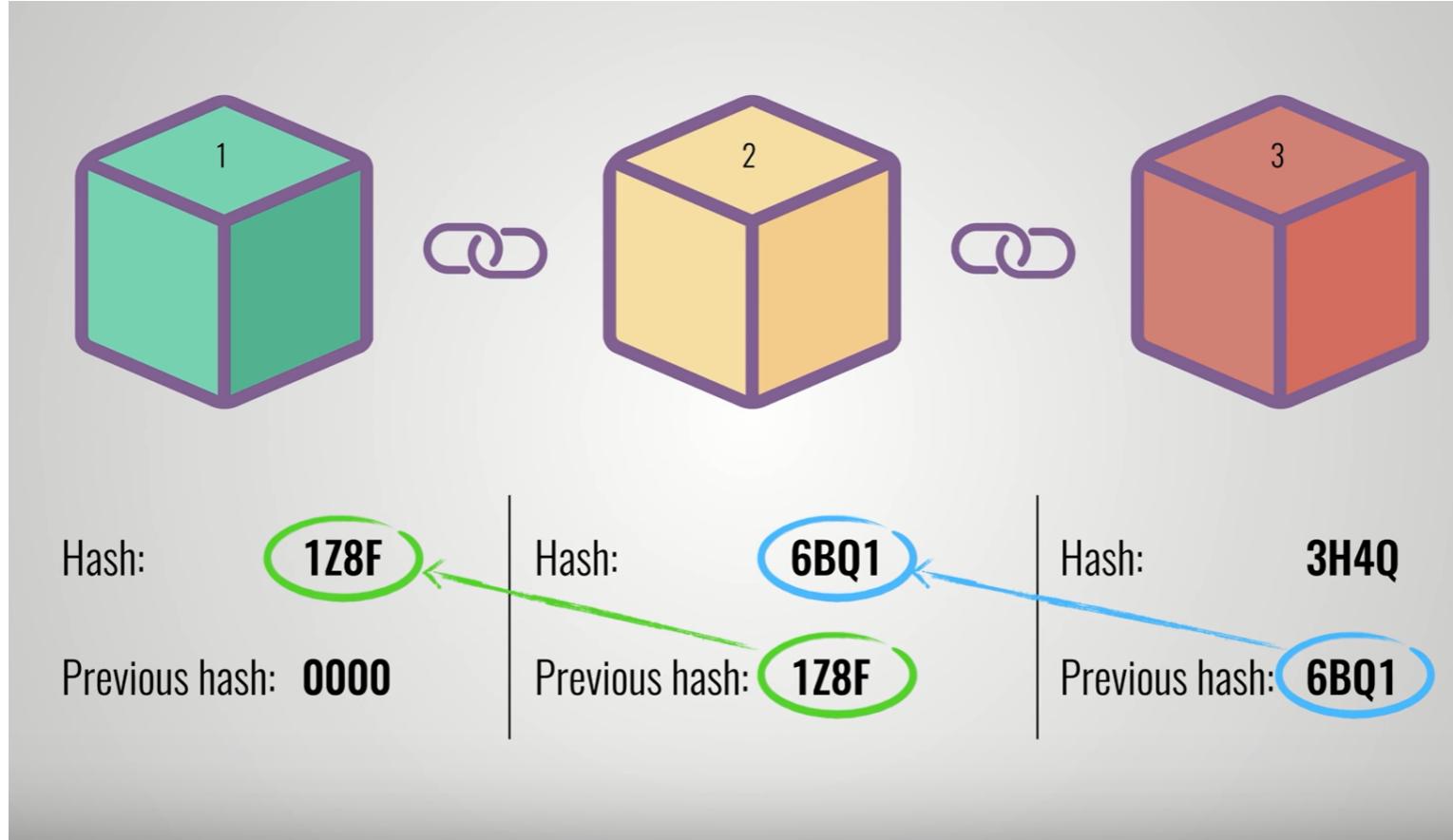
By:



Simply Explained - Savjee
158K subscribers

Blockchain Definition

Chain of Blocks

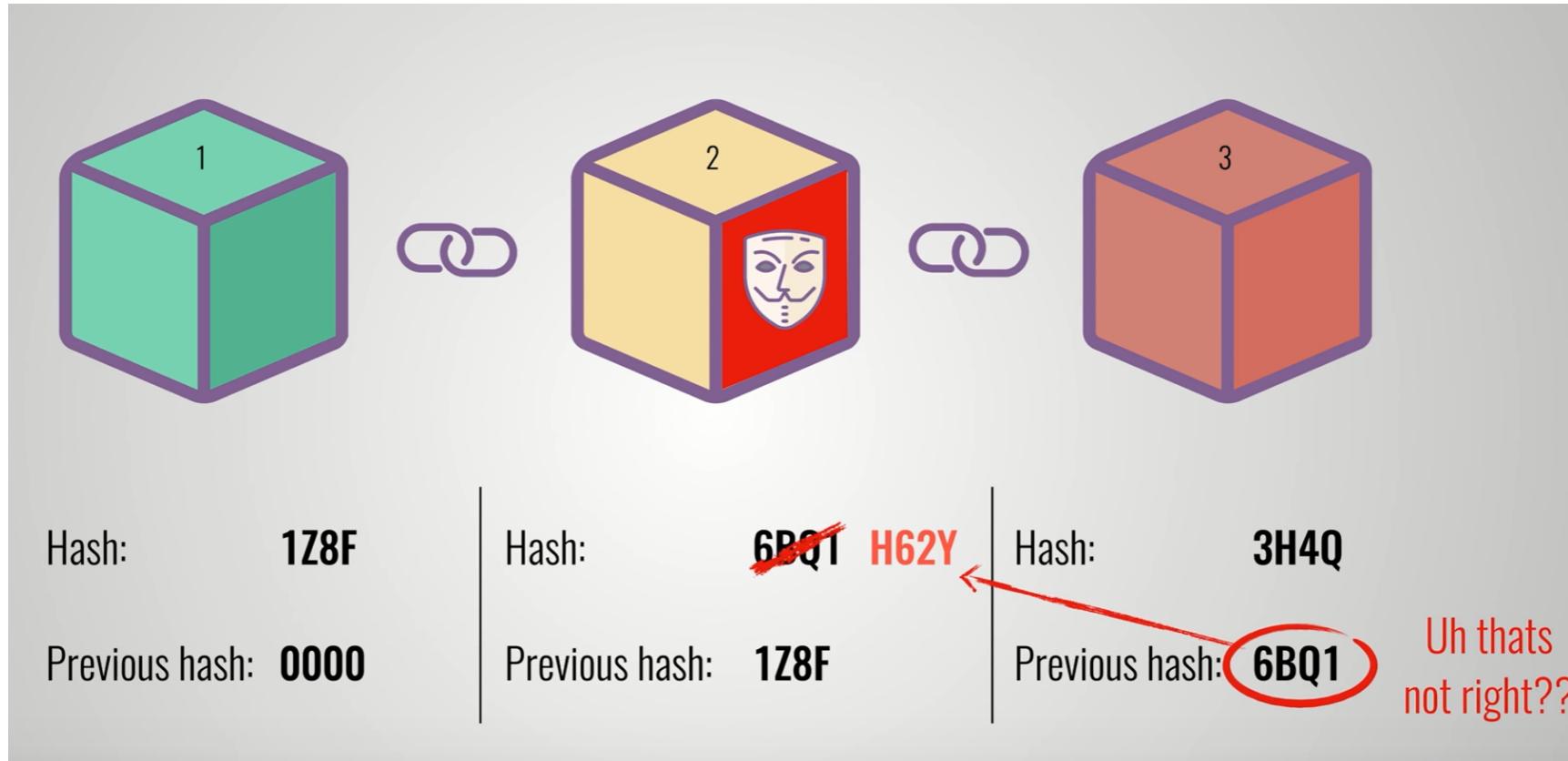


By:



Simply Explained - Savjee
158K subscribers

Blockchain Definition Tamper-Resistant



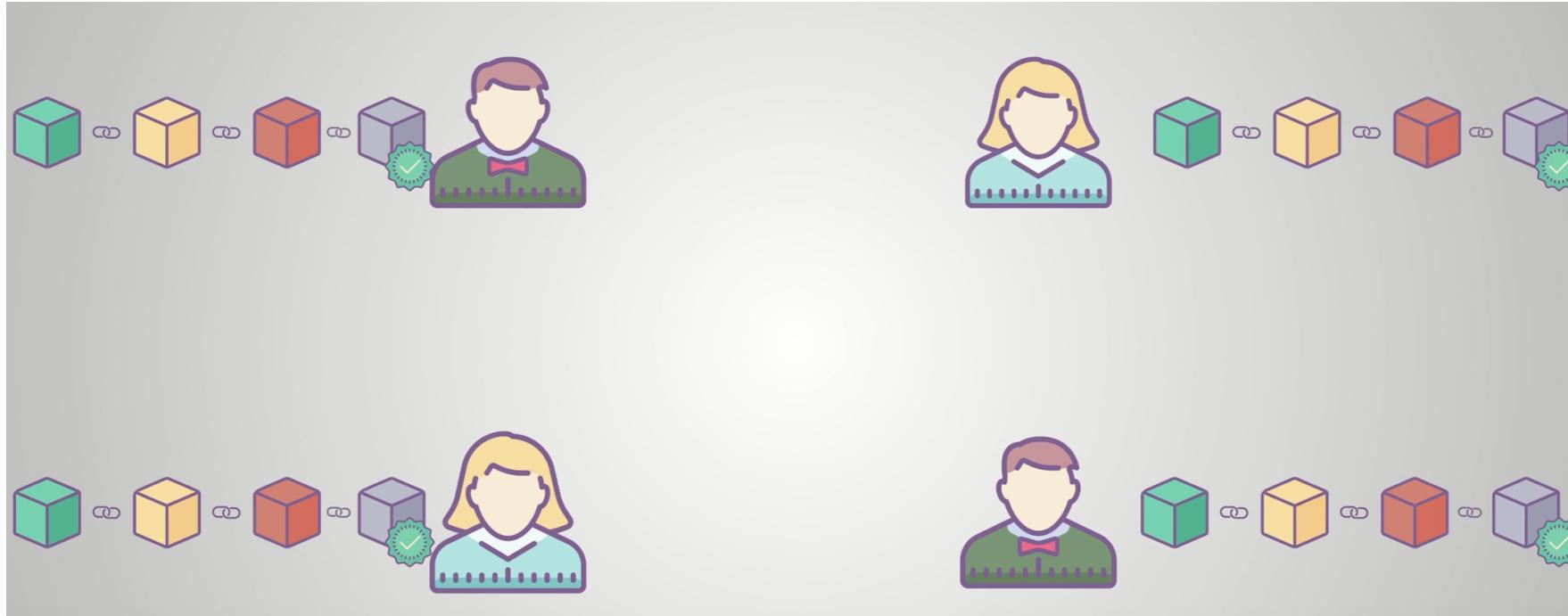
By:



Simply Explained - Savjee
158K subscribers

Blockchain Definition

Distributed/Decentralized



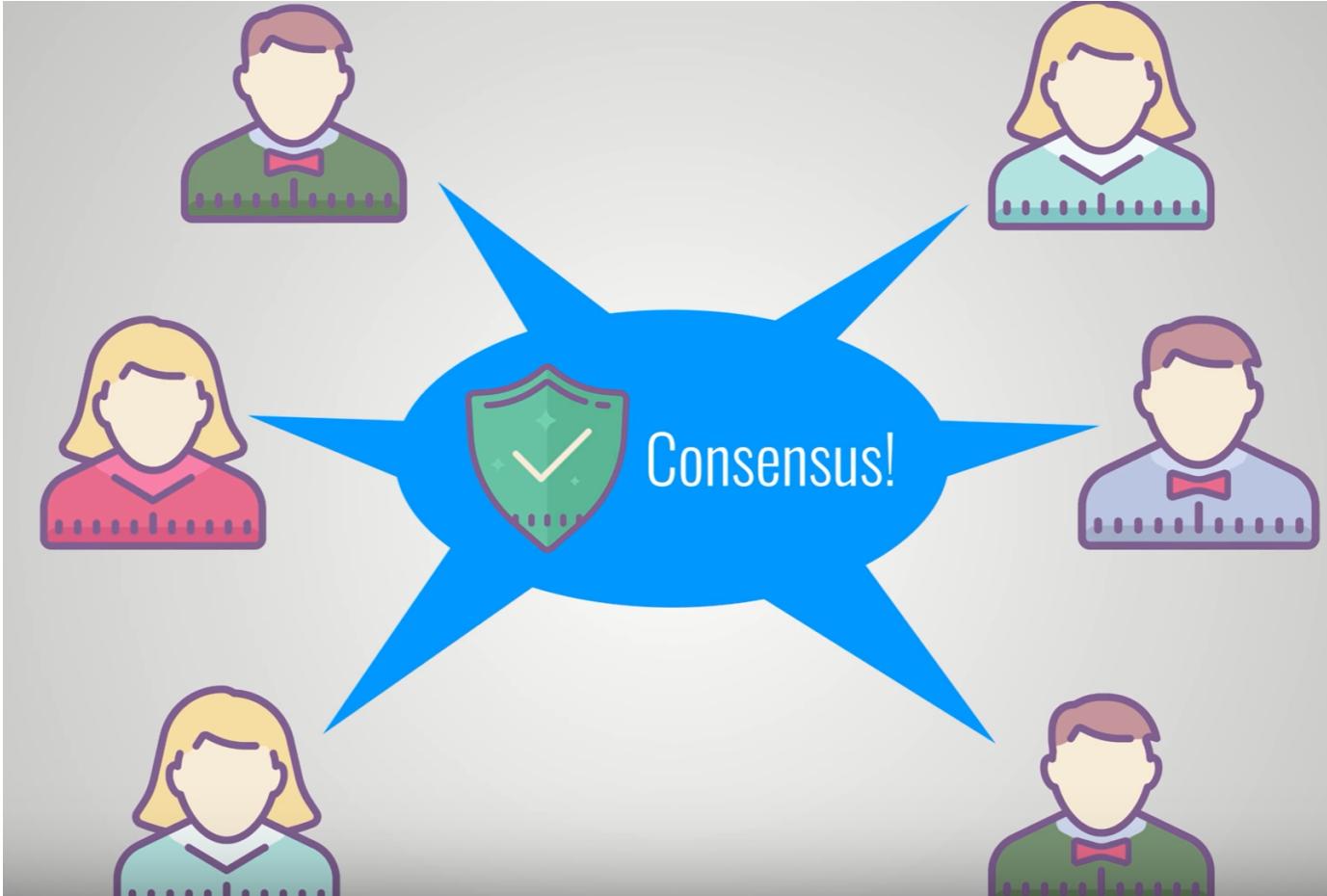
By:



Simply Explained - Savjee
158K subscribers

Blockchain Definition

Consensus



By:



Simply Explained - Savjee
158K subscribers



Blockchain Definition

Core Idea:

Blockchain == an immutable ledger of data without relying on a central authority

Still, many questions remain:

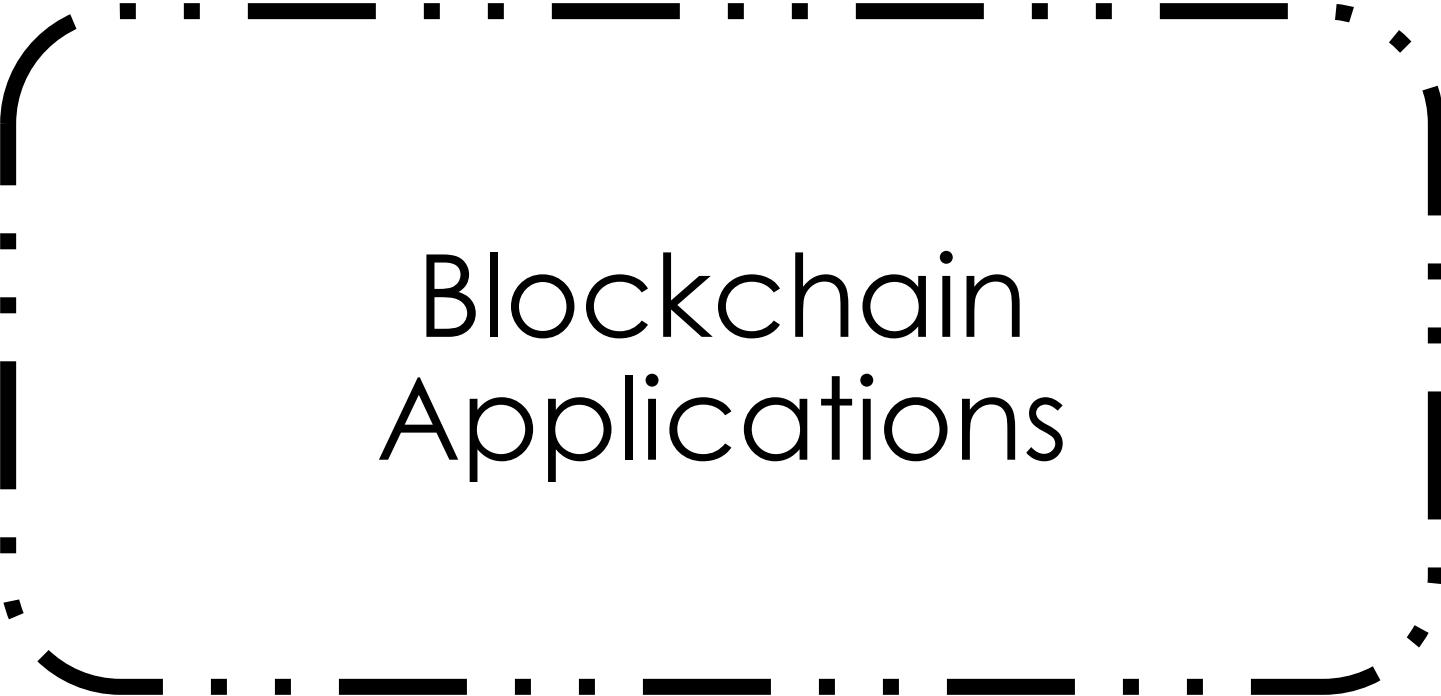
- What are those magical boxes? 
- How do we reach consensus on the state of the blockchain?
 - which block to keep, which to discard?
- Who would want to store the entire blockchain?
 - Who gets to make new blocks?
 - Who verifies the correctness of the data?
- What data to put inside a block?
 - Transparent while private?
- What applications?



Blockchain Definition

Additional Material:

- [Blockchain Explained, Investopedia](#),
- [Understand the Blockchain in Two Minutes](#), YouTube,
- ['Blockchain' is Meaningless](#), The Verge,
- [A simple explanation of how blockchain works](#), Medium,
- [What is blockchain technology?](#), IBM

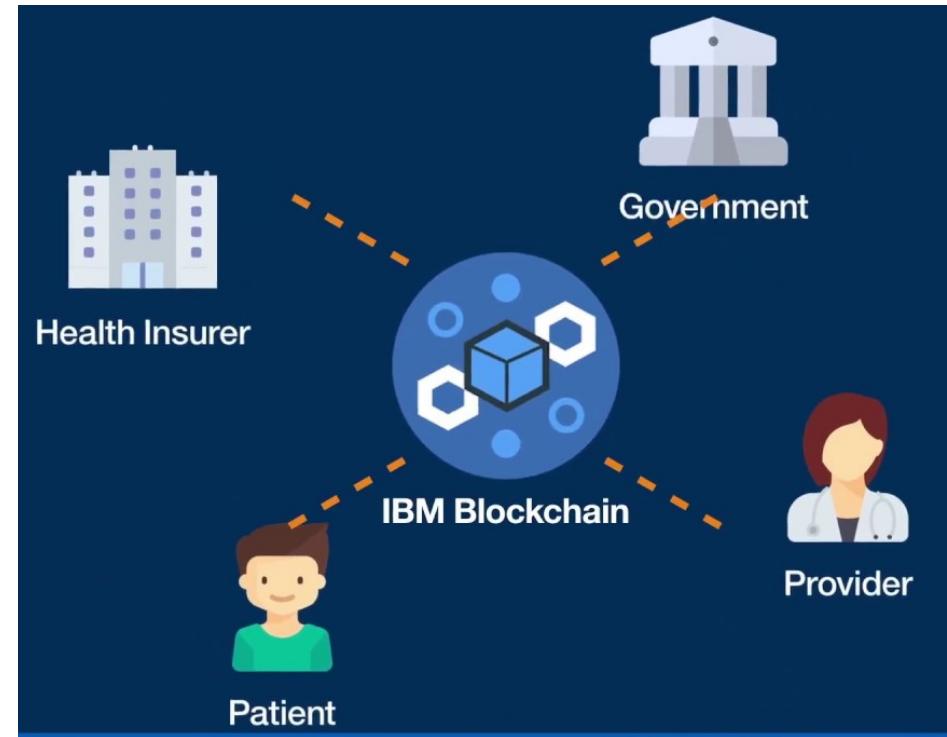


Blockchain Applications

Blockchain Applications

Potential Applications

- **Cryptocurrency**
 - Bitcoin
 - Ethereum
 - ...
- **Healthcare**
 - patients assign access rules for their medical data
 - same record for all parties
- **Government**
 - secure online voting system



Blockchain Applications

Potential Applications

- **Music**
 - musicians to receive equitable royalty payments
- **Insurance**
 - improved transparency
- **Digital identification**
 - more secure management & storage of digital identities with tamper-proof infrastructure
- **Supply chain**
 - IBM Food Trust – used by Walmart to trace lettuce
 - and many more...

BLOCKCHAIN REVOLUTION

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

DON TAPSCOTT

BESTSELLING AUTHOR OF WIKINOMICS

and ALEX TAPSCOTT





Homework Assignments

- Vinay Gupta - the Promise of the Blockchain
- How does a blockchain work - Simply Explained
- Blockchain Expert Explains One Concept in 5 Levels of Difficulty | WIRED
- [optional] You Might Have Missed it, but Blockchain is Now Mainstream
- [optional] How the blockchain is changing money and business | Don Tapscott
- [optional] What the heck is Blockchain?



Questions?



Introduction
to
Blockchain
by
Samuel Tang



Thank you for listening!
See you next week!



Discussion

1. Introduce yourself
2. Why do you want to learn blockchain?
3. What are some applications of blockchain that you're excited about?