Blockchain Revolution

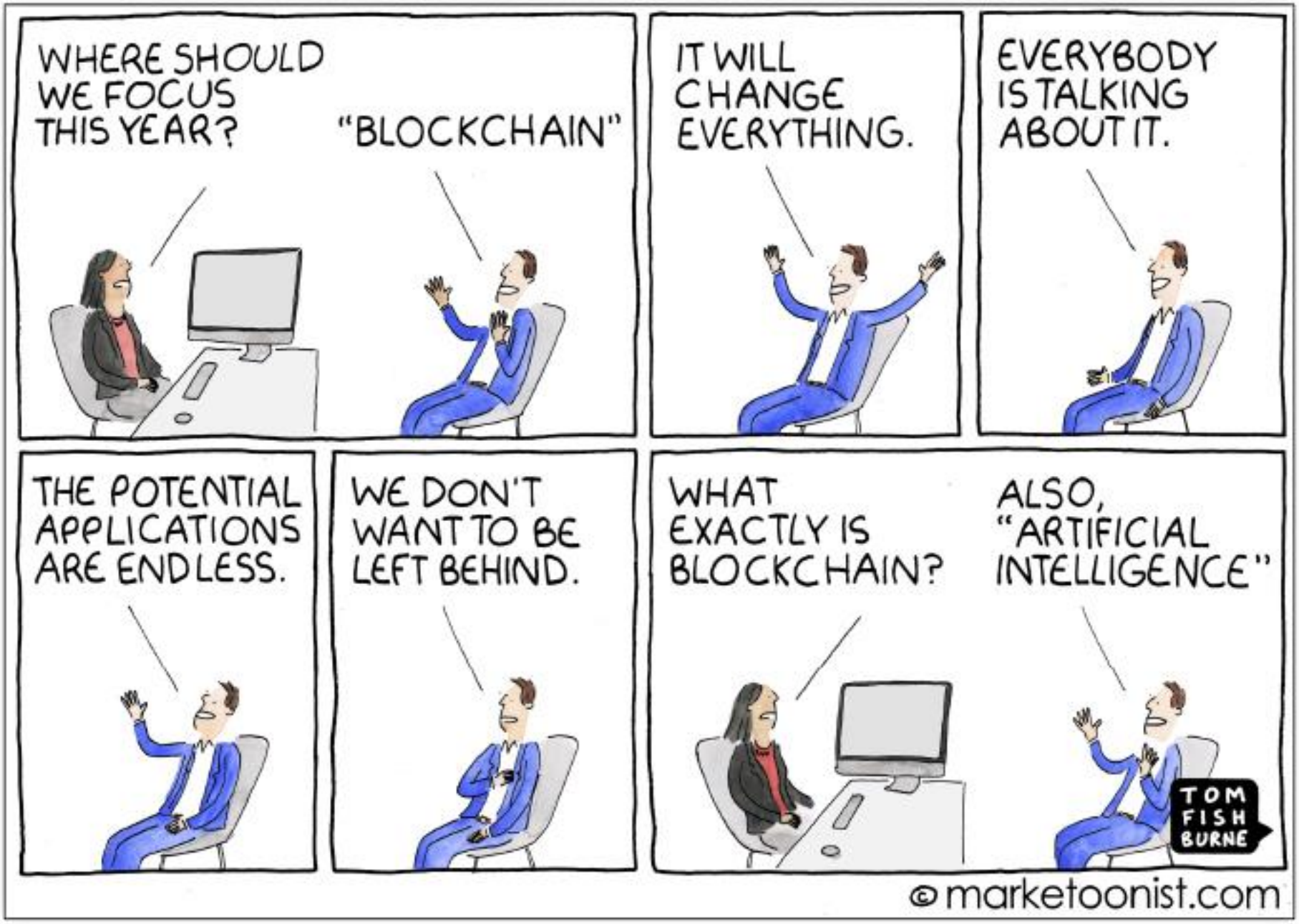
WHAT DO RECORDS MANAGERS & INFORMATION GOVERNANCE PROFESSIONALS NEED TO KNOW?

Today's Agenda

- Blockchain: Basics
- Blockchain: Industry Use Cases
- Blockchain: Impact on Data, Records & Information Governance

How the technology works!

BLOCKCHAIN BASICS


WHERE SHOULD WE FOCUS THIS YEAR?
"BLOCKCHAIN"
IT WILL CHANGE EVERYTHING.
EVERYBODY IS TALKING ABOUT IT.
THE POTENTIAL APPLICATIONS ARE ENDLESS.
WE DON'T WANT TO BE LEFT BEHIND.
WHAT EXACTLY IS BLOCKCHAIN?
ALSO, "ARTIFICIAL INTELLIGENCE"
TOM FISH BURNE
©marketoonist.com


There is no universal definition of blockchain

From the authors of Blockchain Revolution (2016)

The blockchain is an *incorruptible digital ledger* of *economic transactions* that can be programmed to record not just financial transactions but virtually *everything of value*.

~Don & Alex Tapscott

From the NIST Glossary (2018)

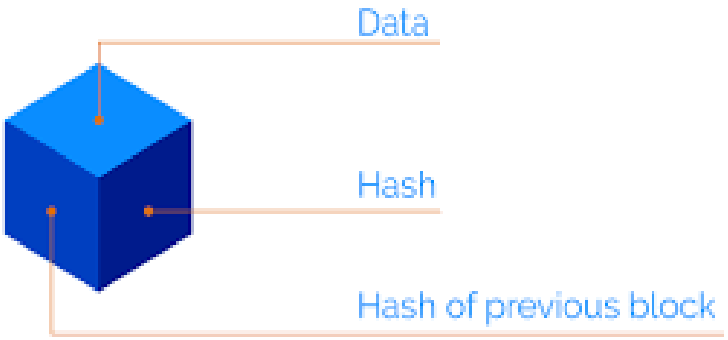
A distributed digital ledger of *cryptographically signed transactions* that are grouped into blocks. Each block is cryptographically linked to the previous one after *validation* and undergoing a *consensus decision*. As new blocks are added, older blocks become more difficult to modify. New blocks are *replicated across all copies of the ledger* within the network, and any *conflicts are resolved automatically* using established rules.

Blockchain is a DLT
Not all DLTs are Blockchain

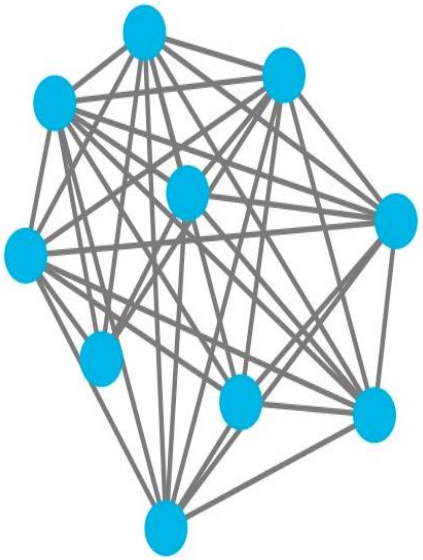
Disintermediation

Blockchain removes — or disintermediates — the middleman from business transactions and by doing so improves the value of existing products, services and interactions.

Blocks = record of transactions



The New Networks = Distributed



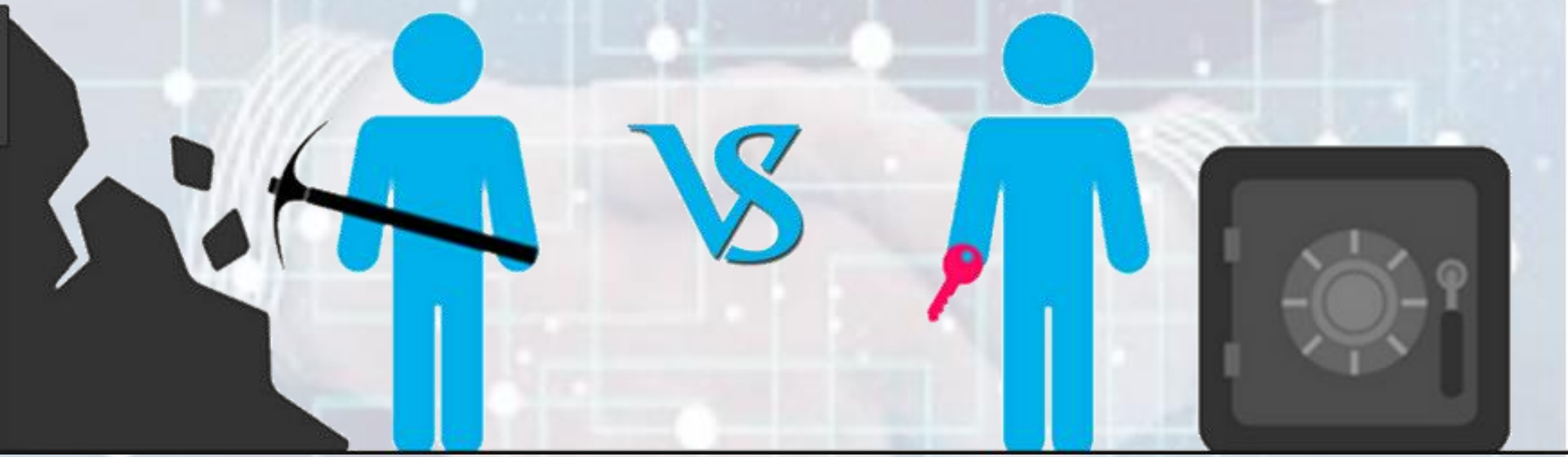
Chains = series of transactions (blocks)

There is more than one type of Blockchain!

	Bitcoin	Ethereum
Launched	2009	2015
Purpose	An alternative to regular money and therefore a medium of payment transaction and a store of value	A platform which facilitates peer-to-peer contracts and distributed applications (Dapps) via its own currency vehicle.
Currency	Bitcoin (BTC)	Ether (ETH)
Currency/USD Close 1/30/19	$3,663.003	$109.05

This is what a Cryptocurrency Mine really looks like.

Consensus Mechanisms



Proof of Work **Proof of Stake**

Agreement on a "single source of truth."

3 Generations of Blockchain

Blockchain 1.0: Transactions and payments via cryptocurrency.

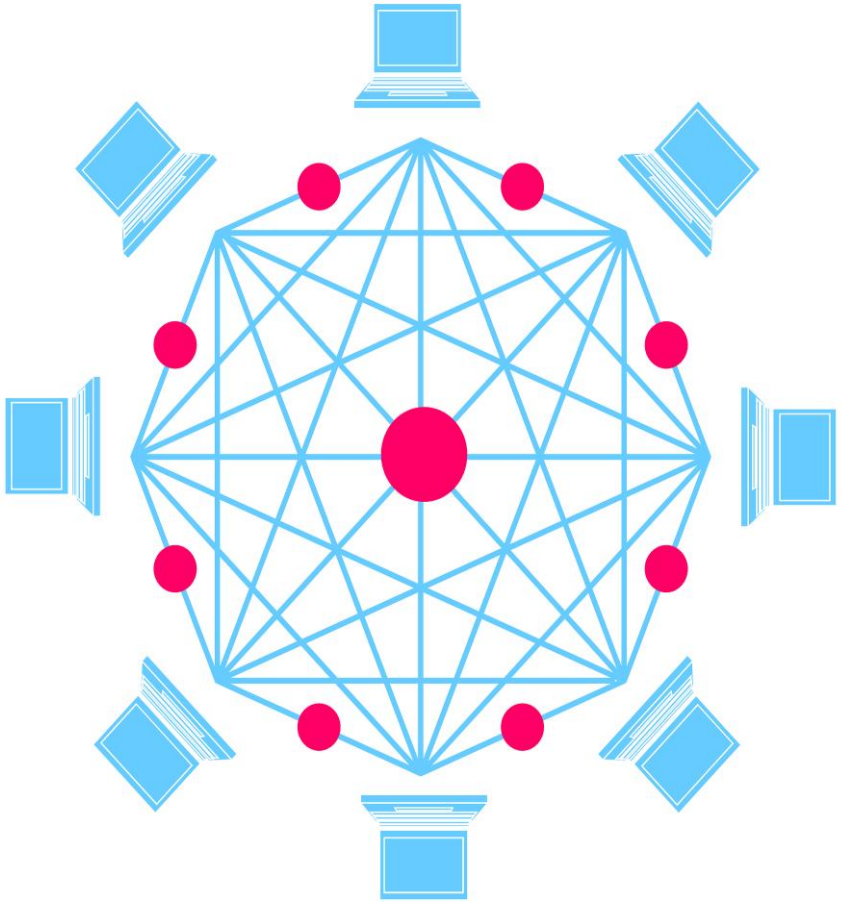
Blockchain 2.0: Decentralized applications and smart contracts that reside atop the blockchain.

Blockchain 3.0: Extensibility beyond the blockchain protocol—a connection with other systems, services, analytics, and more broadly, the outside world.

1st Generation = Bitcoin

Nodes can be **full** (storing a complete list of every single transaction that has occurred on a blockchain) or **light** or lightweight (storing a partial list).

Miners (mining nodes) typically also run full nodes—but not all nodes are miners.



1st Generation = Bitcoin

Private Key Storage

A wallet is an app, website, or device that manages private keys for you.

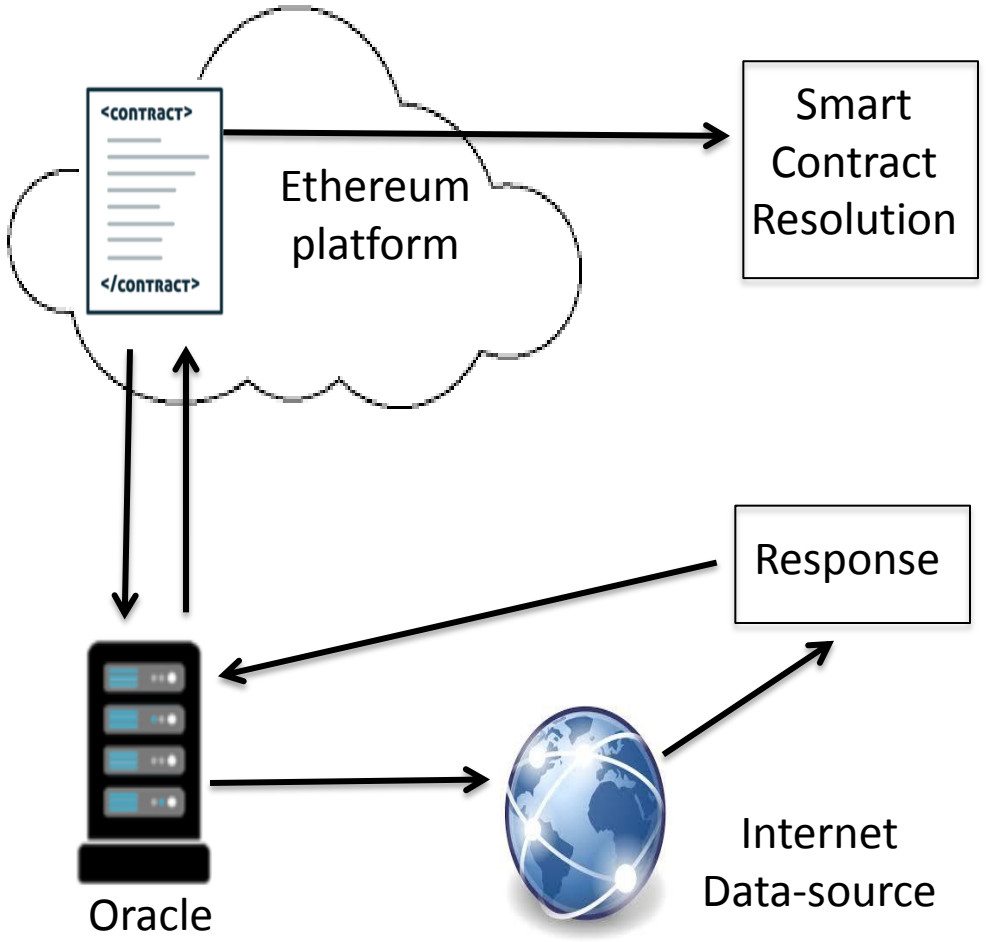
2nd Generation = Ethereum


```
pragma solidity ^0.4.22;

/// @title Voting with delegation.
contract Ballot {
    // This declares a new complex type which will
    // be used for variables later.
    // It will represent a single voter.
    struct Voter {
        uint weight; // weight is accumulated by delegation
        bool voted;  // if true, that person already voted
        address delegate; // person delegated to
        uint vote;   // index of the voted proposal
    }

    // This is a type for a single proposal.
    struct Proposal {
        bytes32 name;   // short name (up to 32 bytes)
        uint voteCount; // number of accumulated votes
    }

    address public chairperson;

    // This declares a state variable that
    // stores a `Voter` struct for each possible address.
    mapping(address => Voter) public voters;

    // A dynamically-sized array of `Proposal` structs.
    Proposal[] public proposals;

    /// Create a new ballot to choose one of `proposalNames`.
    constructor(bytes32[] proposalNames) public {
        chairperson = msg.sender;
        voters[chairperson].weight = 1;
```

ethereum

2nd Generation = Ethereum

The **oracle/oracle network** is the party in charge of connecting you to the data-source.



Blockchain-as-a-Service (BaaS)

3rd Generation = SaaS Providers

BaaS is an offering that allows customers to leverage cloud-based solutions to build, host and use their own blockchain apps, smart contracts and functions on the blockchain while the cloud-based service provider manages all the necessary tasks and activities to keep the infrastructure agile and operational.

Source: Investopedia

ORACLE

AWS

IBM

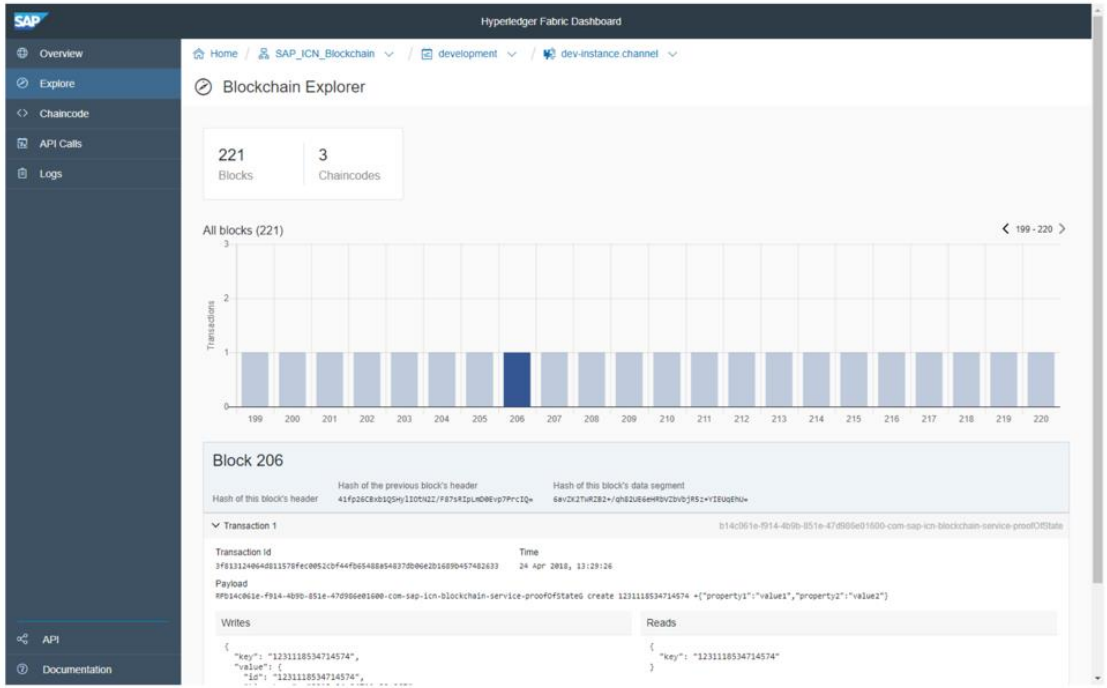
SAP

hp

Microsoft

Hyperledger Fabric on SAP Cloud Platform

3rd Generation = SaaS Providers



Benefits:

- Ease of use
- Efficient processes
- Transparency & visibility
- Security
- Access Control
- Connect your network to a blockchain

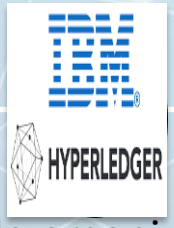
Permissionless/trustless

Public

- Decentralized
- Everyone participates in consensus process (proof of work or proof of stake)
- Open for all to read/write and audit
- Cryptographic verification
- Incentives for miners
- Likely applications: B2B & B2C use cases
- Ex. Bitcoin, Ethereum

Permissioned/trusted

Private



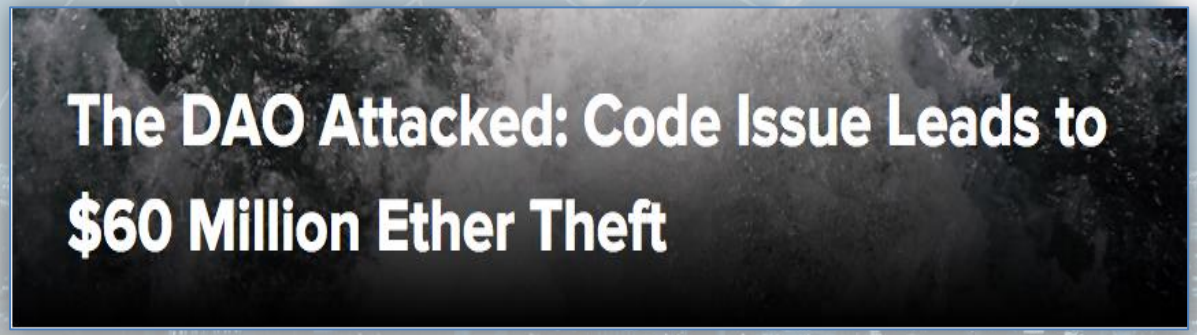
- Single organization
- Voting or multi-party consensus algorithm
- Read permissions may be public or restricted
- Encrypted database commonly shared
- Likely applications: internal database management and auditing
- Ex. Atos, IBM Hyperledger

Permissioned/trusted

Consortium

- Multiple organizations (partially decentralized)
- Voting or multi-party consensus algorithm (voting by pre-selected set of nodes)
- Cyrptographic auditability
- Likely applications: organizational collaboration
- Ex. R3's Corda

Blockchain solutions may be immutable but not infallible



Errors can be made—calling for Smart Contract Audits!

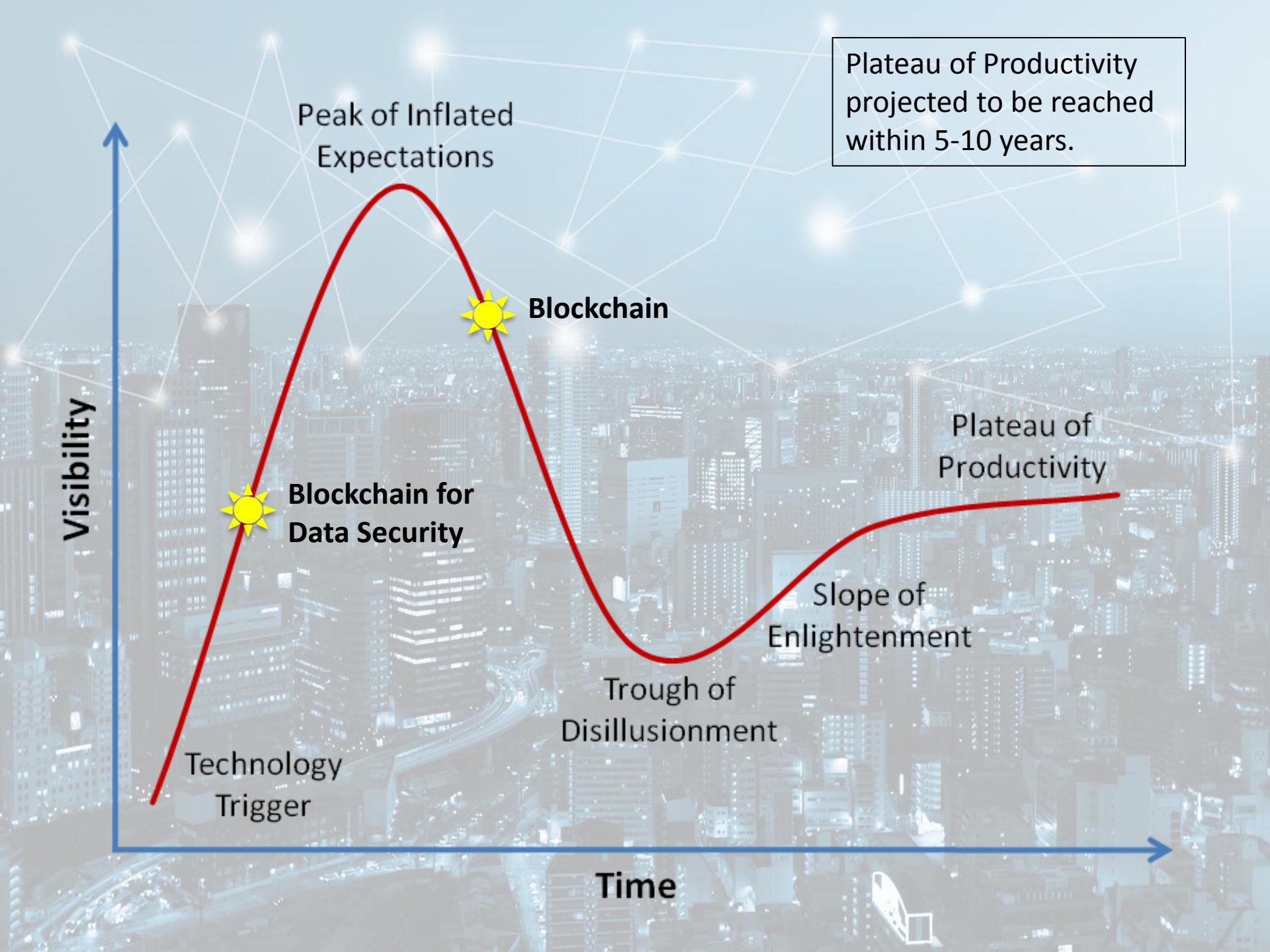
DAO Statement: https://www.sec.gov/news/public-statement/corpfin-enforcement-statement-report-investigation-dao

DAO Report: https://www.sec.gov/litigation/investreport/34-81207.pdf

Blockchain Risks

1. Endpoint Vulnerabilities
2. Vendor Risks
3. Untested at Full Scale
4. Lack of Standards & Regulations
5. Untested Code

~Rick Martin, 2018


Plateau of Productivity projected to be reached within 5-10 years.
Peak of Inflated Expectations
Blockchain
Visibility
Blockchain for Data Security
Plateau of Productivity
Slope of Enlightenment
Trough of Disillusionment
Technology Trigger
Time

It’s all about trust!

BLOCKCHAIN: INDUSTRY USE CASES

Authenticity

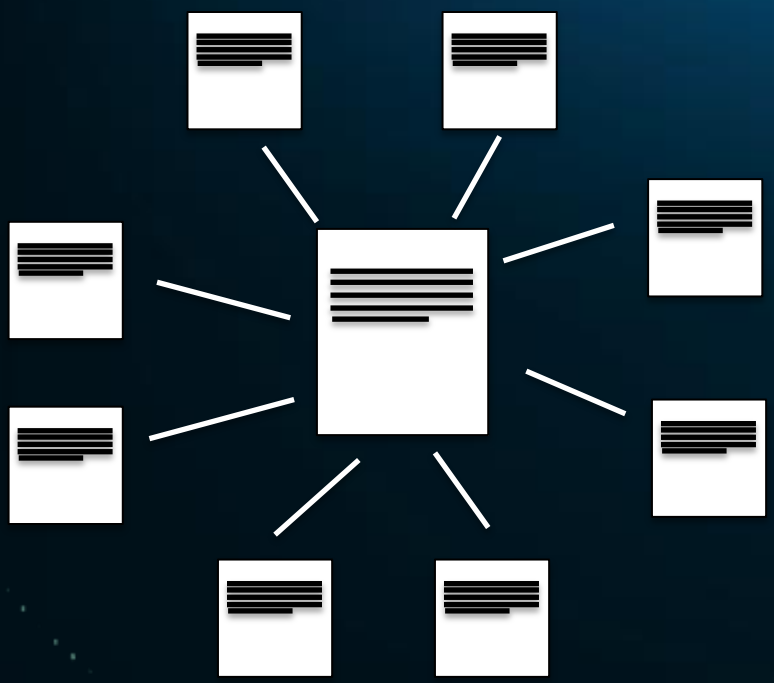
Reliability

Integrity

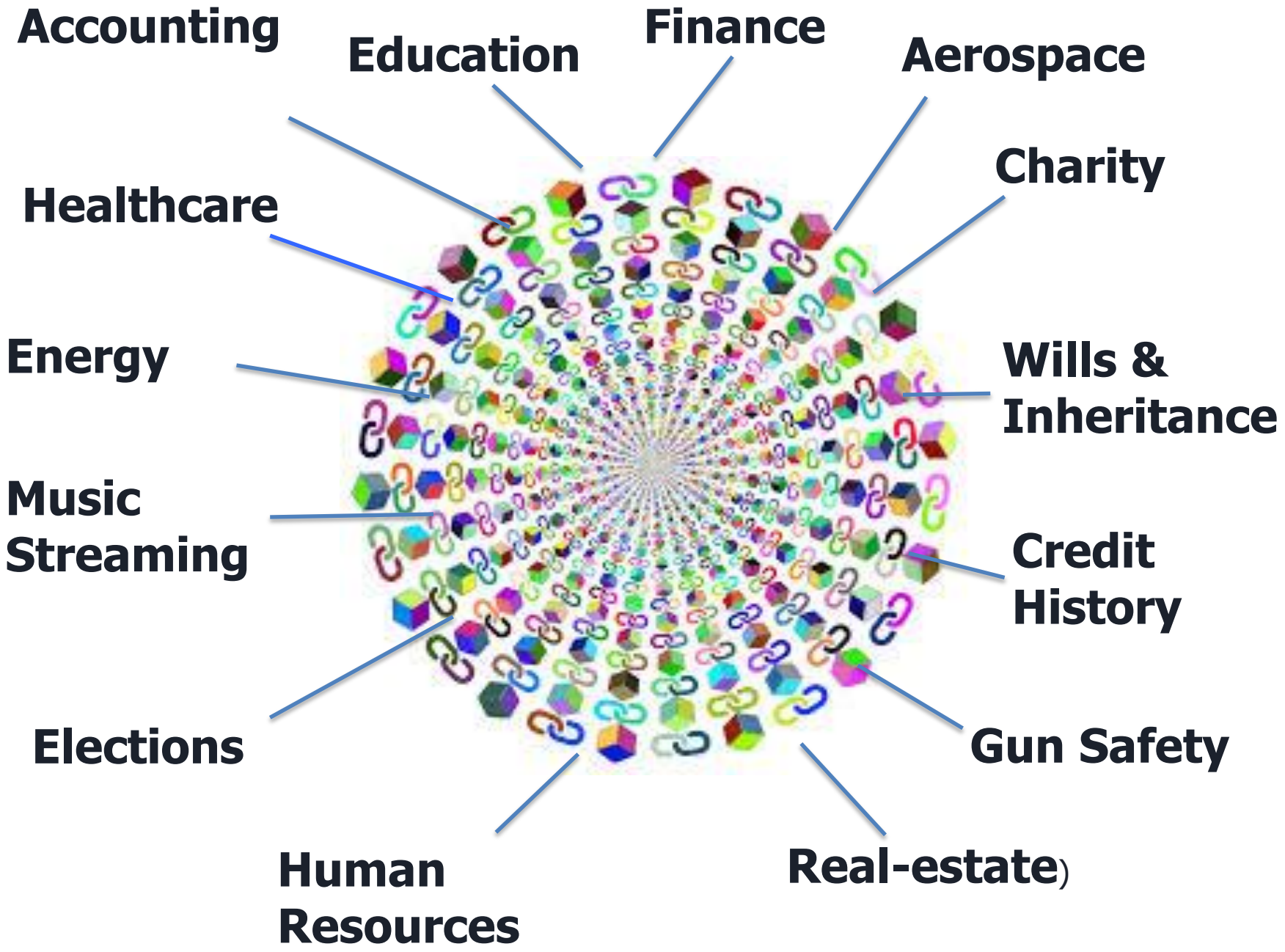
Usability

Records Management	Blockchain Technology
Integrity - ISO 15489-1:2016	Immutable ledger (record)
Reliability - ISO 15489-1:2016	Used as legal evidence
LOCKSS - Stanford University	Multiple copies avoid points of failure
Backup - ARMA Glossary	Multiple backups not necessary
Chain of Custody - SAA Glossary	Chain of custody established

Distributed Ledger = Distributed Trust



- Datasets (records) are shared among all parties (nodes).
- Every party can verify the datasets of other participants in the network.
- Tampered datasets are excluded.
- An immutable *single source of truth* is established


Accounting
Education
Finance
Aerospace
Charity
Healthcare
Energy
Wills &
Inheritance
Music
Streaming
Credit
History
Elections
Gun Safety
Human
Resources
Real-estate)

Blockchain Implementations Compliment RIM for Blockchain	
Document Management	PKO BP, a major Polish Bank
Electronic Health Records	Groves Medical Group, London

Document Management

PKO BP, a major Polish Bank

Basic RIM Blockchain Process

Document, Record, File

Encrypted to a unique hash

Added to a blockchain

Result: non-repudiable, irreversible, cryptographically-secure block
Public access or role-based access can be provided

2018 Blockchain-based document management system for Polish Bank

Every document recorded in the blockchain as irreversible hash signed with bank's private key.

A client can verify remotely if files received are true, or if a modification of the document was attempted."

Tool: Trudatum Firm: Coinfirm AML/KYC Platform

~Biggs, 3/29/2018 Source: https://techcrunch.com/2018/03/29/polish-bank-begins-using-a-blockchain-based-document-management-system/

Data Ownership Provenance

Document, Record, File is created and sent to Trudatum

RegTech provider digitally signs document and …

Registers to the Dash public blockchain—a confirmation hash is generated

Owner

Recipient checks contents against record on the Dash blockchain

Content match?

No – Recipient is notified.

Yes – Recipient can use to make business decisions.

https://www.coinfirm.com/products/trudatum

Electronic Healthcare Records

Groves Medical Group, London

Katrina Shows Need for Electronic Health Records

Doctors on front lines of Hurricane Katrina disaster relief call for universal medical records.

Sept. 21, 2005 Sept. 21, 2005
Problem – Paper-based healthcare records destroyed.
Solution – electronic healthcare records.

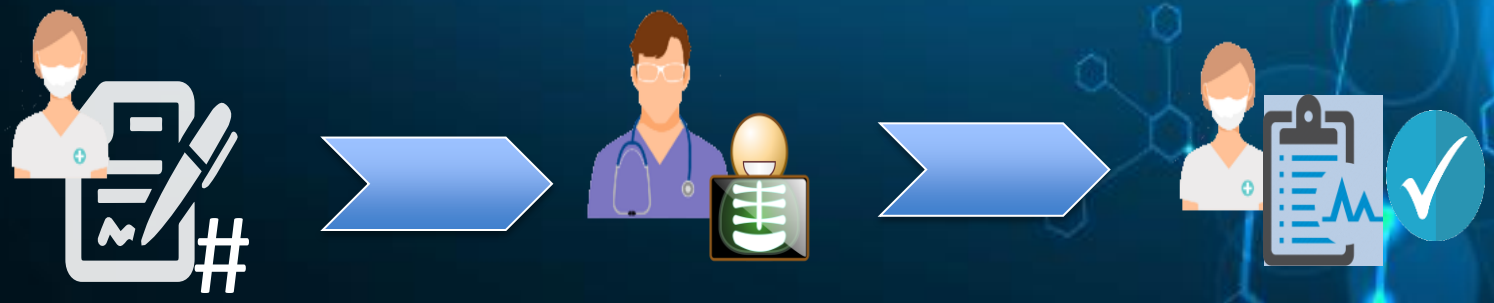
Sept. 17, 2017
Problem – Siloed medical information
Potential Solution – Blockchain Technologies

HARVEY EVACUEES LEAVE THEIR BELONGINGS—AND HEALTH RECORDS—BEHIND

Broken Records – UK Entrepreneurs See Blockchain As The Solution To The Patient Data Problem

August 31, 2018
EHRs on a Blockchain—in this case using Tokens to pay for Medical Services

Medical Order for Treatment on a Blockchain



Doctor creates order which gets unique ID

Radiologist accesses order and does study—then adds images and report to record history.

Doctor views updated record, adds final report.

MedicalChain – Pilot with Groves Medical Group, London, UK

MedTokens
MTN/USD: $0.005236
MTN/BTC: $0.005180
MTN/ETH: $0.004563

Read / Write Permissions	
Practitioner	• Read/Write on permissioned EHRs
Patient	• Read own EHR • Permission Practitioner/Institution to Read/Write • Revoke permission • Permission next of kin/emergency contact to Read/Grant permission • Write certain attributes to EHR (e.g. alcohol consumption, weekly exercise) • Integrate IoT data into HER
Research Institution	• Read permissioned EHRs

Access to EHRs on Blockchain

#

vs.

#

Response

Doctor or patient requests data using a private key

Hash on ledger compare with hash of document in secure storage

- No match: Request flagged
- Match: Verified data sent

Revolutionizing Healthcare

- Electronic Health Records
- Insurance Records & Reporting
- Preventing Fraudulent Billing
- Reducing Counterfeit Pharmaceuticals
- Clinical Trials
- Protecting Patient Data

https://www.disruptordaily.com/blockchain-use-cases-healthcare/

Additional Examples

Walmart patent to maintain medical records on a blockchain

A method for obtaining a medical record of a patient that is unable to communicate, wherein the medical record of the patient is stored on a blockchain, is provided, including receiving an encrypted private key and a public key associated with the patient stored on a wearable device of the patient, in response to a scanning of the wearable device of the patient at a scene of an emergency

https://cointelegraph.com/news/walmart-awarded-patent-for-blockchain-based-medical-records-system

IBM Food Trust Technology

- Seamless collaboration
- Fast response to food safety issues
- Publish & query standards compliant data for food trace and recall
- Share and view single-sourced inspection and quality certifications and registrations

Each member owns its data and maintains full control over who can access it. All data is stored on blockchain ledgers, encrypted, and made accessible only when permission to view relevant records is granted.

https://www.ibm.com/blockchain/solutions/food-trust

Step 1 of 5
Computing local hash [DONE]

Step 2 of 5
Fetching remote hash [DONE]

Step 3 of 5
Comparing local and remote hashes [DONE]

Step 4 of 5
Checking Merkle root [DONE]

Step 5 of 5
Checking receipt [DONE]

VERIFIED

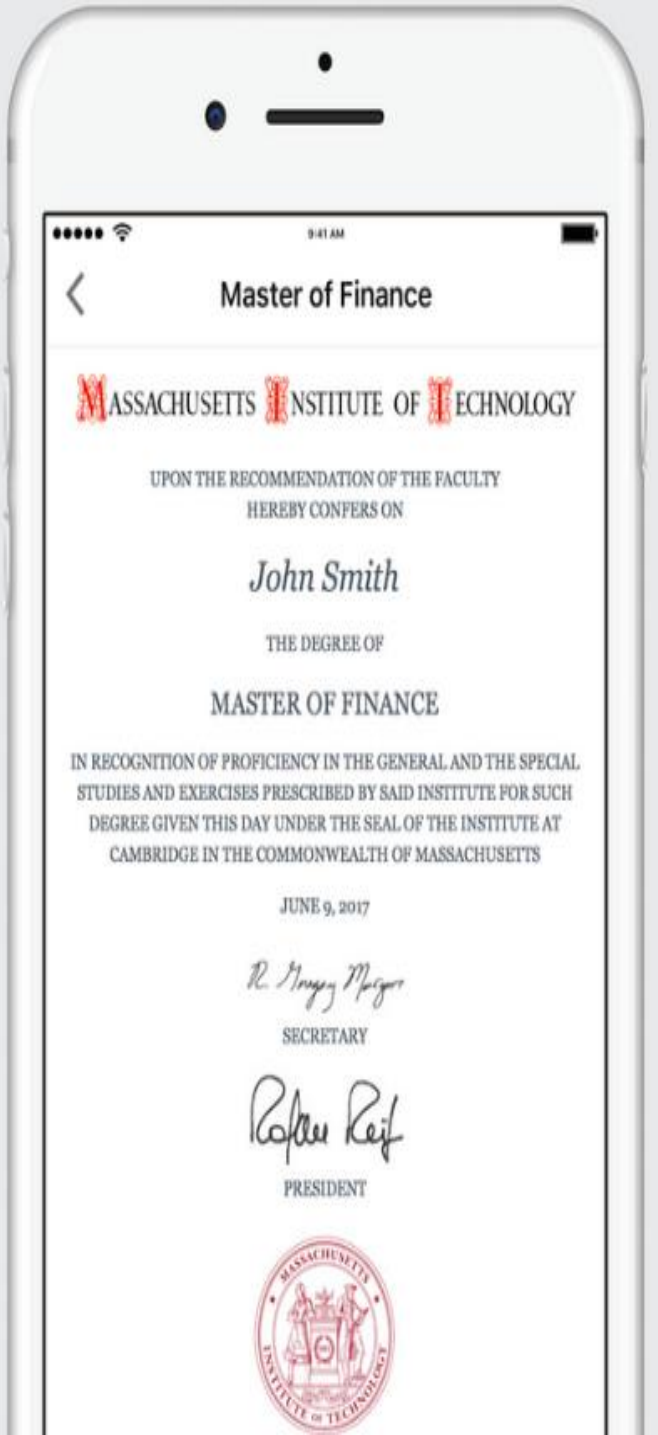
Public Key
1HYPitzbwR83M3Smw6GWs5XeQzBWoJAEes

Blockchain Address
4bf64ff1517554dac3496e9da0a28ca9ae492682b0898e384ea17e7f90ee1295

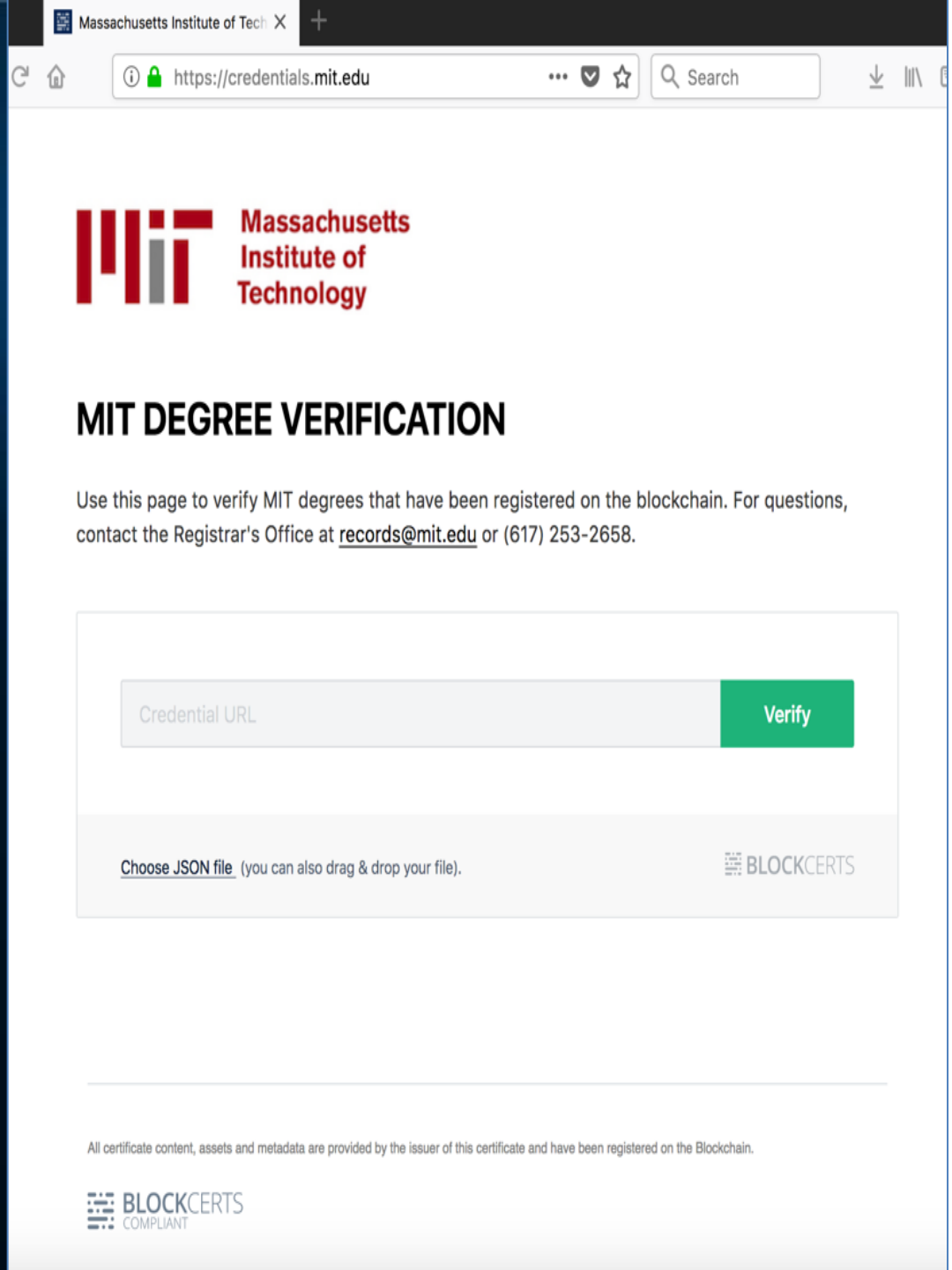
Student Experience

1. Receive email invitation to download the open source mobile app (Blockcerts) and add MIT as an issuer.
2. The mobile app is used to generate keys, which demonstrate ownership, and send the public key to MIT.
3. Students must login to the MIT identity system as part of this process.
4. Once issued, students receive diplomas by email as an attachment they can store anywhere. Importing the file into the mobile app allows viewing and sharing with others. MIT also hosts the files, which makes them easy to share with a link.

Source: https://www.learningmachine.com/case-studies-mit



MIT provides a verification site using an open source blockchain lookup service (Blockcerts) to compare the uploaded diploma to the hash stored on the blockchain. See: https://credentials.mit.edu



Austin is piloting blockchain to improve homeless services

- Replace paper records with electronic encrypted records that would be more reliable and secure.
- Create a decentralized authentication mechanism to verify a particular person's identity.
- Build vital records on the blockchain over time, so different providers would know what services (example—healthcare) a person had used previously.

https://techcrunch.com/2018/04/14/austin-is-piloting-blockchain-to-improve-homeless-services/

Trusted Concert Tickets

BLOCKPARTY

Real Tickets at Fair Prices

Say goodbye to fake tickets and unfair pricing. Blockparty has developed "Two Factor Ticketing" that links a user's ticket to their digital identity. Our protocol tracks a ticket from issue through to the secondary market to the gate. Enter the event by unlocking your ticket using our app that fully encrypts your digital identity from your phone's in-built facial recognition or fingerprint scanning technology.

https://www.goblockparty.com/?gclid=Cj0KCQiA1sriBRD-ARIsABYdwwFevKURaJKoXk984oY8D6mtjwprhaGGHbzqP3EDm-i1ho4R9Gku5UcaAiLCEALw_wcB

Delaware Corporate Records

May 2016

The *Delaware Blockchain Initiative* announced.

August 2017

The *Delaware General Corporation law (Senate Bill 69, 149th Congress,* went into effect.

February 2018

Delaware eased off its blockchain zeal after concerns to disruption of business.

July 2018

State contracts for $738,000 with IBM to develop and test a Blockchain prototype.

What are the implications?

BLOCKCHAIN: IMPACT ON DATA, RECORDS & INFORMATION GOVERNANCE

A Digital Record

TRANSACTION 01

Address

LJFJ5721SFXX2312G2Q

Size

136 BYTES

Lock Time

BLOCK: 2982385

Received

2017-10-03 14:25:01

Blockchain Legislation

WY

NV

IL

HI

NY

AZ

MD

DE

VT

CT

NJ

MO

TN

ME

VA

MI

CA

CO

NE

OH

Authenticity of records

UTEA & electronic signatures

Cyber coding cryptology

Corporate records

Casino gaming

Firearm tracking

Smart contracts

Taxing & use restrictions

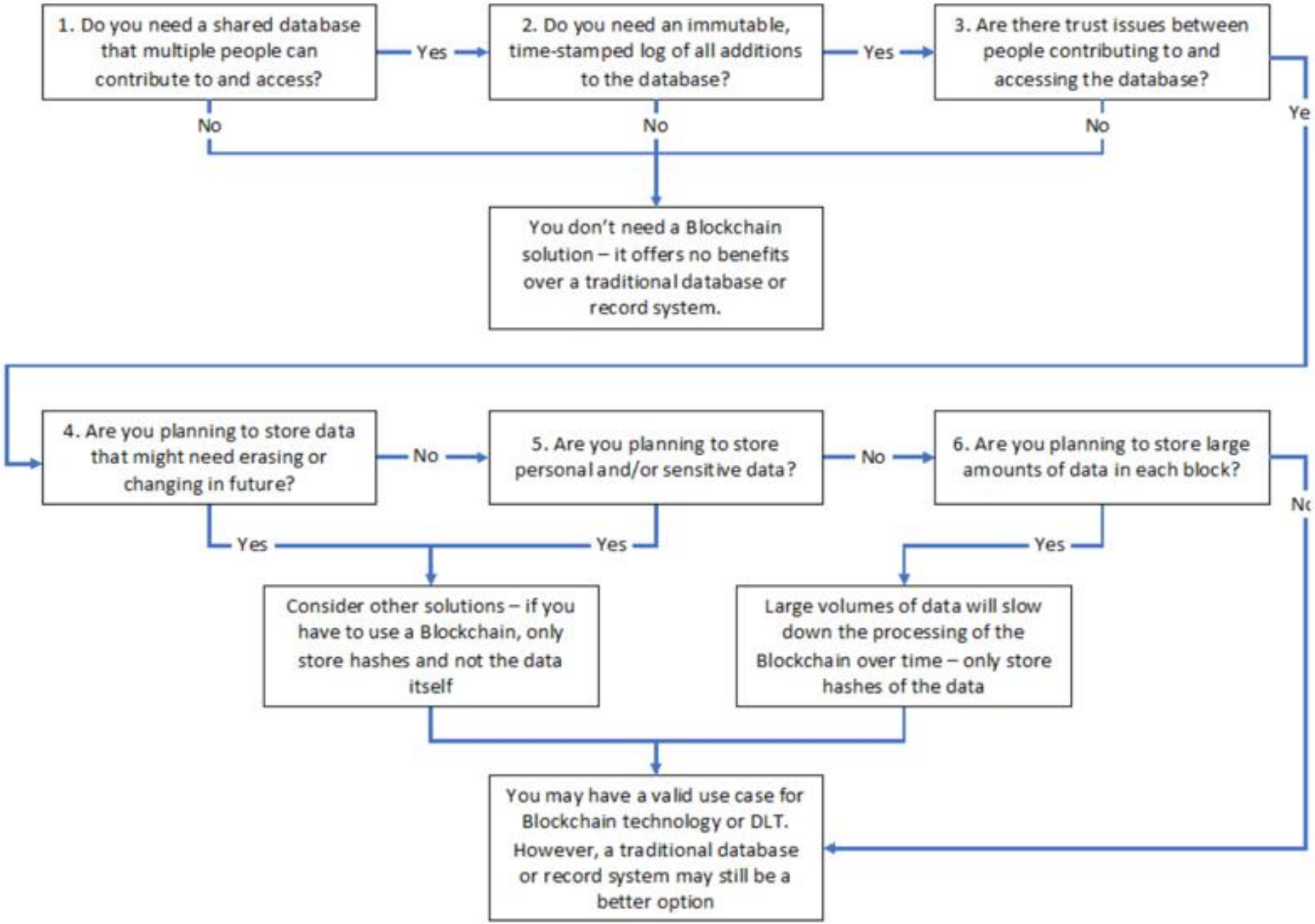
Marijuana tracking

Voting records & election results

Crimes (forgery, money laundering)

Information ownership rights

Immutability & Trust



~Pelz-Sharpe, Begley, Bushell, August 2018, Records Management & Blockchain "Proceed, but with caution"

Centralized Database	Distributed Ledger
Internal and external reconciliation required	Consensus on data
No restrictions	Append only (immutable)
Single point of failure	Distributed across nodes
Single point of control	Decentralized control
Gateways & Middlemen involved	Peer-to-Peer relationship
Cryptography as an after thought	Cryptographic verification
Actions taken on behalf of others	Cryptographic authentication & authorization
Backups must be provided for “manually”	Resiliency and availability increase with node count

Implementation Challenges (not exhaustive)

- Required third party input (information/conformation)
- Data residency restrictions
- Transparency of transaction information and digital content (Access permissions)
- Integration with digital content that is off the blockchain
- Compliance with regulations (e.g., GDPR, CCPA of 2018)

Information Governance Considerations

- There is still the question of governance over the blockchain.
- While it is intended to be run without a sole overseer, the technology itself is made up of machines and code developed by people.
- Resulting conflict resolution procedures are not solidified, and the entire system itself may not even technically be covered by existing laws.
- This could open up the possibility of fraudulent and unethical behavior if procedures and laws are not properly thought out prior to implementation.

What can you do now?

According to Don Tapscott, Blockchain Revolution

- Download a digital wallet
- Buy some cryptocurrency
- Purchase something

- Get pilots going in your organization—Experiment
- Find people into this—promote them, give them resources and help them transform the organization

- Understand the strategic impact on your organization & industry through deep research
- Become aware of technologies linking blockchains together and with other systems currently in use

https://www.youtube.com/watch?v=isuAPyuqS7Y

Comments? Questions?

Dr. Patricia C. Franks
MARA Program Coordinator
School of Information
San José State University
Email: patricia.franks@sjsu.edu