

NTSA

IITSEC 2018

NOV 26TH - NOV 30TH | ORLANDO, FL

LAUNCHING INNOVATION IN LEARNING:
READY, SET, DISRUPT



The Truth About Blockchains and How They Apply to Training

Dr. Robby Robson, Eduworks

Mike Hernandez, Advanced Distributed Learning Initiative (SETA Contractor)



@IITSEC



NTSAToday



Introduction

PART I

A bit about us
and how we
came to look
at blockchains

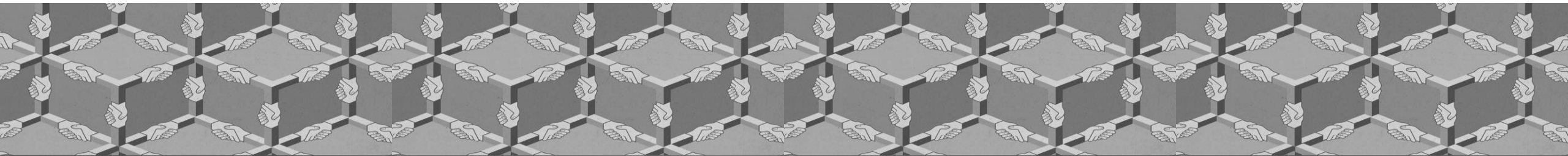
...

TOPICS (PART 2 - OVERVIEW)

- Why we care
- High level understanding of blockchains
- Deciding whether or not to use blockchains – and if so, what kind.
- Discussions of relevant use cases.

TOPICS (PART 3 - TECHNICAL)

- **How blockchains work**
- Real world implementations
- Blockchains and training
- Resources & Q&A



PART 1

HOW WE CAME TO LOOK AT BLOCKCHAINS



Why We are Doing This

Our focus is on training, credentialing, and careers – the human capital supply chain.

Changes in technology and operations have made it hard to gather and trust the records and data used in this supply chain.

- Trust is important
 - In the credentials a person has earned
 - In the capabilities of a team member
 - In the future for which a military career prepares you
 - In the data produced by training systems
- Trust requires records to be
 - Traceable (who did what **when** - the time is important!)
 - Verifiable (can't be faked)
 - Immutable (can't be changed)
 - Indestructible (can't be lost or erased)

This is *exactly* the type of problem that blockchains are being used to solve!



Why this matters

- Lumina Foundation has identified a challenge
 - Goal: 60% of Americans hold degrees, certificates or other high-quality postsecondary credentials by 2025
 - Essential to meeting our nation's growing need for talent.

TWO PARTS:

1. *Skill/Knowledge Acquisition*
2. *Skill/Knowledge Recognition*



Lumina™
FOUNDATION



@IITSEC



NTSAToday



Credentialing, Certification, and Licensing

- Records are in walled gardens
 - High school diplomas
 - College degrees
 - Technical certifications
 - Work performance records
- “Soft-skills” are seldom made explicit
- Records are not granular enough to capture skills and knowledge
- Systems do not communicate well with each other
- There is no shared index for data

WHY IS THERE A PROBLEM?



Lumina™
FOUNDATION



@IITSEC



NTSAToday



WHY ARE BLOCKCHAINS A SOLUTION?

- Blockchains enable granular record keeping
- Blockchains act as shared ledgers
- Blockchains engender trust

(We will talk about this a few times today)



Lumina™
FOUNDATION



@IITSEC



NTSAToday



So Just to Summarize ...

- Today
 - Electronic training records are tracked across a range of formats, in many databases, at varying levels of detail
 - Most records are not linked beyond their own community of interest
- Blockchains can provide
 - Distributed, immutable, secure, and trusted data
 - A common link across a learner's lifetime
 - The ability for individuals them to control their records
- But first we need to tell you the truth about blockchains ... and it may not be exactly what you have read or heard.

PART 1

OVERVIEW OF BLOCKCHAINS



The Blockchain Hype Cycle



The Buzz About Blockchains



Blockchain 101

Technology

Markets

Business

Data & Research

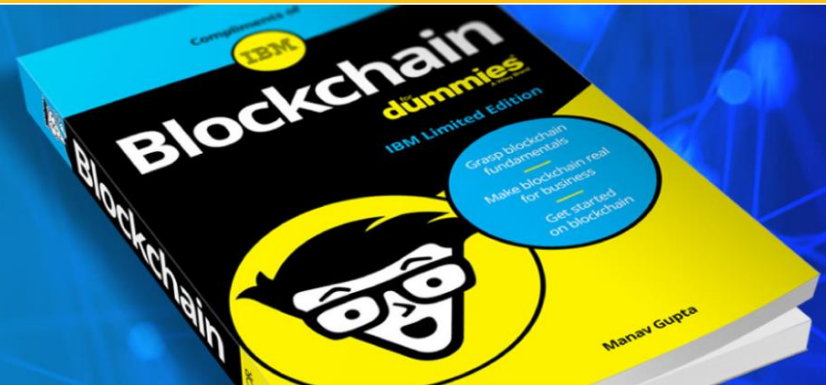
Consensus

Find your career in blockchain. Click here to the career center...

Understand the fundamentals of IBM Blockchain

Blockchain technology presents opportunities for disruptive innovation. It enables global business transactions with less friction and more trust.

[Download Blockchain for Dummies](#)



There's even an I/ITSEC tutorial on Blockchains!

➤ Bitcoin accounts for roughly 62% of the crypto-currency market and is using roughly 0.2% of the world's electricity – Morgan Stanley report, January 2018

- Equivalent of the energy consumption of Ireland or Argentina



Introduction to **Ethics**
of Blockchain Technology
An IEEE eLearning Module

[Learn More >>](#)

IMPORTANT: All That Glitters is Not Bitcoin



There are many other blockchains

- Some are public, some are private
- Some are open, some require permissions
- Some have nothing to do with currency
- Some just store transactions, some do more



Examples of Blockchain applications from a Recent Wired Article

Bots with nefarious intent	Cancer	Complying with Know Your Customer laws	Managing real estate workflow	A digital-only investment bank	Global supply chain's \$9 trillion cash flow issue	Settling payments faster	Currency for eSports betting	Simplifying the logo copyrighting process	Human suffering	Free mobile data for watching ads	Checking ID for purchases like alcohol	Large corporations' carbon footprints	Online gambling sites take commission	Improving the technology of the Russian gas industry	Borders	Improving privacy of blockchain	Improving institutional-grade crypto asset management	Improving traditional banking services for crypto world
Skynet	Earning money on personal data	Complying with Anti-Money-Laundering laws	International real estate purchases	Containers to transport sensitive pharmaceuticals and food	Trust in the global supply chain	Speeding transactions	Currency for sports betting	Resolving industry's "prevalent issues"	Security for luxury watches	Crypto rewards for watching entertainment content	"Uber for alcohol" on blockchain	"Decarbonizing" electricity grids	Helping retailers hurt by Amazon	A blockchain equivalent of Amazon, Groupon and Craigslist	Man-in-the-middle hacks	Decentralized database for decentralized technologies	"Painstakingly slow" manual crypto wallet process	Cryptocurrency based on Game Theory, IBM's Watson, and other theories
People not taking their medicine	Pensions	Complying with securities laws in token sales	Physical branches for crypto banking	Protecting consumer information on mobile	Economic crisis	The unbanked	Storing scholarly articles	Crowdsourcing for legal dispute resolution	Authenticity in cannabis sales	Gold-backed cryptocurrency	Inefficiencies in cargo delivery	Climate change	Online retail fraud	Too many non-valuable ad networks	Security sacrifices that come with innovation	Improving trust and confidence in blockchain system	More open global markets	Better social network + blockchain + AI + human touch
Device storage that could be used for bitcoin mining	The burden of car ownership	Censorship	Physical branches for crypto exchanges	Helping mobile phone users monetize their data	Cash flow problems at small and medium-sized businesses	The underbanked	Health insurance providers billing processes	Securing financial contracts	Crypto rewards for cannabis-focused social media site	Crypto-backed gold	Branded tokens for merchants to reward customers	Trust in governments	Paying for things with your face	Unregulated prison economies	Scams, fraud and counterfeits	More cohesive user experiences across blockchain and the cloud	Easier way to invest in real estate	Improving content streaming on the blockchain
Insurance bureaucracy	Inability to buy anything with cryptocurrency	A use for QR codes	Private equity	Not enough interconnection in the world	Improving the use of data in the transportation and logistics industries	The bidding process in art and collectibles markets	Healthcare providers	Paper	Crypto payments for rating cryptoassets	Metals-backed cryptocurrency	Fraud and corruption among non-profits	Trust in corporations	Streamlining interactions among shoppers, retailers and brands	Standardizing the value of advertisements	Tools to build decentralized apps	Democratizing gold trading	Easier way to invest in Swiss real estate	Supply chain transparency
Electronic health record accessibility	Better marketplaces for nautical shipping services	Rewards for buying alcohol by subscription	Venture capital	Complexity and risk in the crypto market	Poverty among African farmers	Assessing the value of collectibles	Shortage of workers with advanced tech skills	Automation	Crypto payments for taking surveys, watching videos and clicking links	Precious metals-based cryptocurrency	Better transparency at non-profits	Trust in social networks	Linking content across computers, tablets and phones	Advertising not transparent enough	Blockchain infrastructure	Giving investors more control of their assets	Easier way to combine smart contracts with crowd-funded home loans	
Health record storage security	Better ways to advertise to your friends	Tracing water supplies	AIDS, also online sales of classic Japanese domestic cars	Expensive AI research	Transparency in the food supply chain	Diamond industry's high banking and forex fees	Lack of diversity in tech	Control of personal data	Crypto rewards for video game skills	"Tokenizing" real world items	Better transparency around impact investing	Trust in medicine	Ranking apps by their value	Old real estate practices	Removing barriers separating blockchains	Simplifying the cryptocurrency market's roles	Easier way to borrow against crypto holdings	
Health record portability	Better ways to trade forex with your friends	Dearth of emergency responders	Efficiency and transparency at nonprofits	Counterfeit goods	Ad fraud	The illicit diamond trade	Elder care	Control of personal credit data	Crypto rewards for time spent playing video games	Nashville apartment buildings	Bitcoin mining uses too much energy	Universal billing system for travel industry	Aligning creativity and recognition for content creators	Free public information from silos	Safety in buying and selling blockchain tokens	Trading indexes as tokens	Education around blockchain technology	
Marine insurance risk	Ownership shares in ancient sunken treasures	High cost of medical information	Incorporating local preferences in decentralized banking options	Connecting "innovation players" and "knowledge holders"	Fake news	Availability of digital games	Rights management for photographers	No way to spend crypto	Buying, selling and trading your social media friends	Monaco real estate	Home appliances mining for bitcoin while not in use	Decentralized Uber and Lyft	Improving payments for artists on Spotify and Pandora	Speeding the rendering of animated movies	Improving privacy in online file storage	Improving crypto safekeeping solutions	Blockchain not mainstream enough	
Increasing public sector trust of cryptocurrencies	Poverty	Improved digital identity authentication	Boosting sales for local businesses	Movie industry's slow and opaque accounting practices	False news	Currency for eSports	Content rights management	Advertising for extended reality environments	Crypto rewards for social media sharing	Financial infrastructure for trading within video games	Bitcoin mining using hydropower	Online gambling not fair	Online piracy	Selling items for crypto instead of regular money	ICO projects could benefit from the "wisdom of the crowd"	Simplifying ICO investment, trading and cryptocurrency	Identifying and verifying users in online dating	

Medical

Copyright

Privacy

Real Estate

Ads

Health Care

Ecology

Food

Real Estate

Billing

Crypto-Currency

So ... What ARE Blockchains?

Double-entry bookkeeping system

From Wikipedia, the free encyclopedia



A place to record *transactions*

That is *permanent* and *auditable*

Any one of which can validate entries

Stored in *multiple* places

➤ Distributed Ledgers

Double-entry bookkeeping was pioneered in the Jewish community of the early-medieval period, for example, used a double-entry bookkeeping system which was used by the Messari, and whose records remained in the Republic of Genoa. It has been argued that the method was learned from the Republic of Genoa. The earliest extant accounting records that follow the modern double-entry system in Europe come from Amintore Manucci, a Florentine merchant at the end of the 13th century. Manucci was employed by the Farolfi firm and the firm's ledger of 1299-1300 evidences full double-entry bookkeeping. Giovannino Farolfi & Company, a firm of Florentine merchants headquartered in Nîmes, acted as moneylenders to the Archbishop of Arles, their most prominent client.



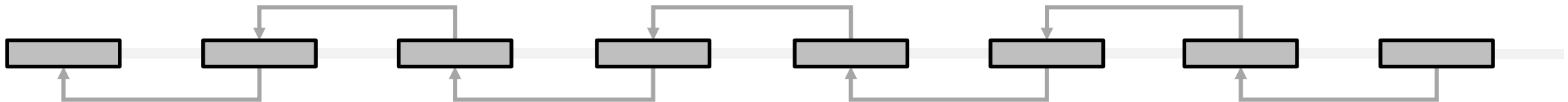
So ... What ARE Blockchains?

- Distributed Ledgers
- Consisting of linked blocks of data
- Whose content
 - requires *consensus* among a set of peers
 - and is cryptographically assured

A place to record *transactions*



That is *permanent* and *auditable*



<http://ethviewer.live/>

So ... What ARE Blockchains?

- Distributed Ledgers
- Consisting of linked blocks of data
- Whose content
 - requires *consensus* among a set of peers
 - and is cryptographically assured
- And that support
 - Smart contracts
 - Crypto-identities

A place to record *transactions*

Replace legalese with code!

Untraceable yet provable



That is *permanent* and *auditable*

What does this mean to the end user?

TRUST REQUIRES
RECORDS TO BE

- **Traceable** (who did what when)
 - Blockchains are ledgers that record the entire history of transaction, with timestamps
- **Verifiable** (can't be faked)
 - Blockchains use consensus and digital signatures to ensure the validity of records
- **Immutable** (can't be changed)
 - The “block & chain” mechanism ensures that changes can be detected
- **Indestructible** (can't be lost or erased)
 - The data on a blockchain is distributed and replicated in multiple places.



Applications of Blockchains

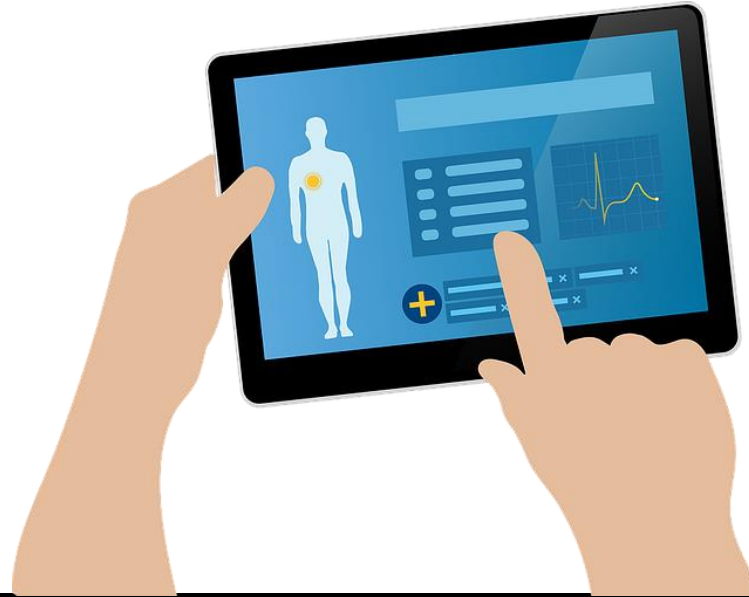
Finance



- Secure records with no single point of failure or authority
- Smart contracts that execute transactions automatically and accurately
- Equal access for everyone – from individuals to multi-national corporations
- Electronic wallets

Applications of Blockchains

Health Care



- Electronic Health Records that
 - Are permanent and protect your identity and your privacy
 - Record all medical “events” (exams, prescriptions, quantitative self, etc.)
- Record origin, expiration date, etc. of medications
- Provider as well as patient records



Applications of Blockchains

Supply Chain Management



- Record events from farm to table and from factory to consumer
- Helps identify problems, analyze processes, manage recalls
- Provides infrastructure for micro-payments and monitoring value-additions
- Open to all – can be joined by anyone in the supply chain
- Include smart contracts to initiative shipping or for time-based discounts

Applications of Blockchains

Product Certification



- Consumers can verify that a product has been certified or is standards-conformant
- Smart contracts can enforce warranties
- End users can examine entire chain of custody

Applications of Blockchains

And of course ... training & education

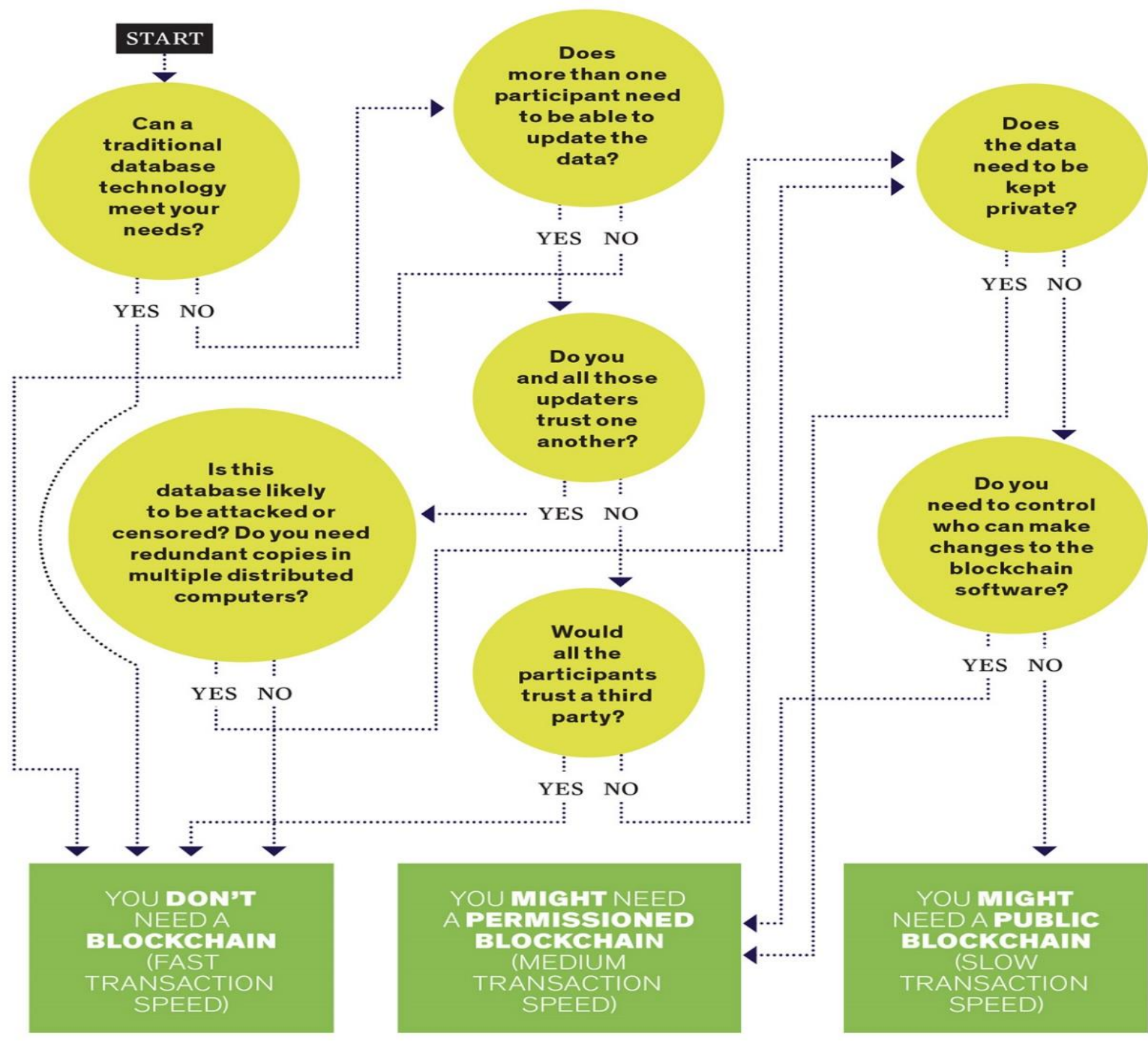


- Secure verifiable credentials (degrees, licenses, ratings, etc.) with privacy controls
- Records of the data exhaust from LMSs, serious games, simulations, etc.
- Records of informal and non-formal learning (e.g. this tutorial)
- Consensus-based qualifications

Types of Blockchains

- **Public** —  —  — Anyone can use from anywhere
- **Permissioned** —  — **HYPERLEDGER** — Access is controlled and may involve an authority rather than consensus
- **Paid by users** —  — Users pay to have their transactions recorded and smart contracts executed
- **Paid via mining** —  — Peers are paid in cryptocurrency when they win the right to write a block

When do I Need a Blockchain?



<https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain>



@IITSEC



NTSAToday

Let's Check These Against Some Use Cases!



- Supply Chain Management & EHR*
- Credentialing (Licensing / Certification)
 - Issued by multiple organizations
 - Need permanence and validation. Also privacy controls.
 - Transactional in nature (issue / revoke / transfer)
- Ashore & Afloat Records
 - Eliminate replication across multiple systems
 - Would like automated updating based on achievements
- Workforce Development (Civilian Transition)
 - Joint Military Transcripts
 - Mapping to Civilian Credentials (COOL)
- M&S (and adaptive instructional systems)
 - Persistent federation management
 - Persistent learner models

*Electronic Health Records

Supply Chain Management & EHR

Transactional data that must be verifiable, trusted, and protected

Data comes from many sources operating independently

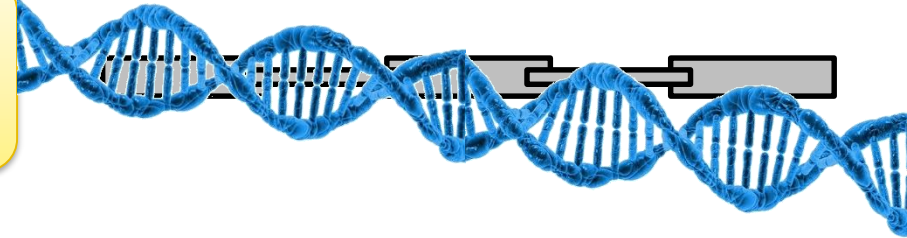
Redundancy is desired and chains of custody are required to instill trust

A third party authority is impractical and infeasible – if something goes wrong the public won't buy it

Privacy (PII) and end-user control are (legally) required

Blockchains are an ideal solution (and are being used)

Discussion topic: Will blockchains become the standard for acquisition and product certification?



Credentialing, Certification, and Licensing

- Lumina Foundation has identified a challenge
 - Goal: 60% of Americans hold degrees, certificates or other high-quality postsecondary credentials by 2025
 - Essential to meeting our nation's growing need for talent.
 - <https://www.luminafoundation.org/lumina-goal>
- Spans all industries
- Relevant to veteran transition



Lumina™
FOUNDATION



@IITSEC



NTSAToday



Credentialing, Certification, and Licensing

Credentialing is massively distributed and must be secure & immutable. A single traditional DB is out!

Data comes from many sources. Must support write / read / revoke / transfer / contest / etc.



They don't know each other and there are issues with trust (e.g. low standards / faked credentials)

A third party authority is impractical and politically infeasible

Blockchains seem like an ideal solution (and are being explored for this)

Privacy (PII) and end-user control are (legally) required

Discussion topic: Public chains? Permissioned? Locally Permissioned?

Credentialing, Certification, and Licensing

AN EXAMPLE FROM THE AVIATION INDUSTRY

Ashore and Afloat Records

- Data Challenges
 - Data must move between ships and shore
 - Bandwidth is at a premium
 - Security is paramount
- Information Challenges
 - Knowing capabilities with certitude
 - Updating them as they evolve
 - Synchronizing between ship and shore




Ashore and Afloat Records

The current DB does not seem to stay current – often hard to know if a sailor’s records are up-to-date

Many systems across the fleet are generating and updating data – some ashore and some afloat

Need verifiability and immutability
Want redundancy and security

Blockchains could solve many problems and offer advantages – *worth exploring* –



Smart contracts will allow sailors to acquire new credentials based on afloat actions and training*

Privacy (PII) and control over who sees the data when shared externally are important issues

* A few more details to follow ...



Ashore and Afloat Records – A Use Case for Smart Contracts

Smart contracts can potentially ...

- Establish prerequisites before deploying
- Update records based on acquired qualifications
- Codify training plans (and check whether they are being followed)
- Include logic to adjust training plans
- Respond to changes in equipment and requirements

A **smart contract** is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a **contract**. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.^[1] Smart contracts were first proposed by **Nick Szabo**, who coined the term, in 1994.^[2]

Proponents of smart contracts claim that many kinds of contractual clauses may be made partially or fully self-executing, self-enforcing, or both. The aim of smart contracts is to provide security that is superior to traditional contract law and to reduce other **transaction costs** associated with contracting. Various **cryptocurrencies** have implemented types of smart contracts.

Source: Wikipedia

M&S and Adaptive Instructional Systems

- Require an understanding of
 - The learner's knowledge, skills, and abilities (competencies)
 - The learner's preferences
 - The learner's goals
 - The learner's traits and context
- "Learning portability" is a hard problem
 - Technically solvable ... but
 - Challenged by privacy laws and public perception
 - Even more challenged in DoD by security concerns
- Not solvable by a monolithic system
 - Trust, security, perception, and practicalities mitigate against this



Home » Centers » Center for Adaptive Instructional Sciences (CAIS)

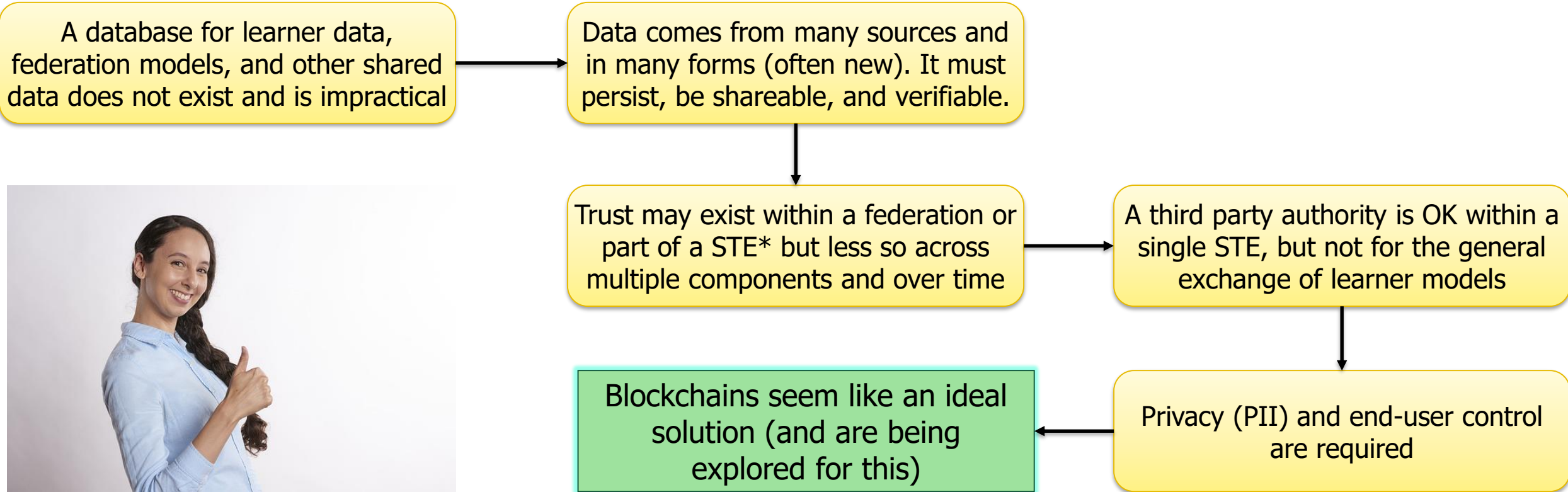
Center For Adaptive Instructional Sciences (CAIS)

Background

As part of the Army Research Laboratory's Open Campus Initiative, ARL has established a Center for Adaptive Instructional Sciences (CAIS). The purpose of CAIS is to bring together government, industry, and academia to advance adaptive instructional science and technology for application in training and educational systems through a collaborative, innovative research ecosystem. Adaptive or tailored instruction in the form of Intelligent Tutoring Systems (ITSs) has been shown to be significantly more effective than traditional classroom instruction for both individual learners and teams. While the promise of adaptive instructional tools and methods are high, there remain significant technical challenges to its practical application in large organizations (e.g., US Army, large corporations, and universities).



M&S and Adaptive Instructional Systems



Discussion topic: Can we use blockchains for the entire data exhaust? Are there scale and performance issues?

*Synthetic Training Environment

PART 2

Technical

(But returning to training in the end)



@IITSEC

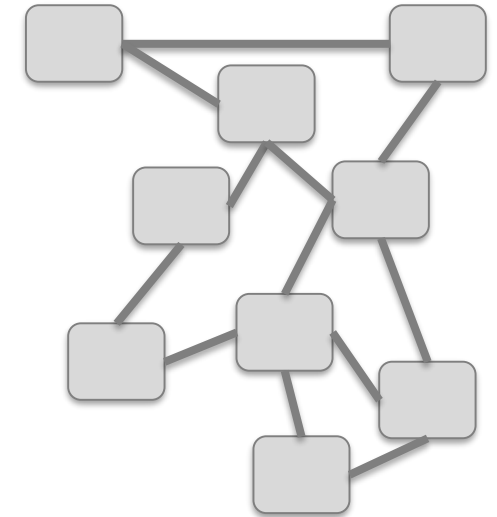
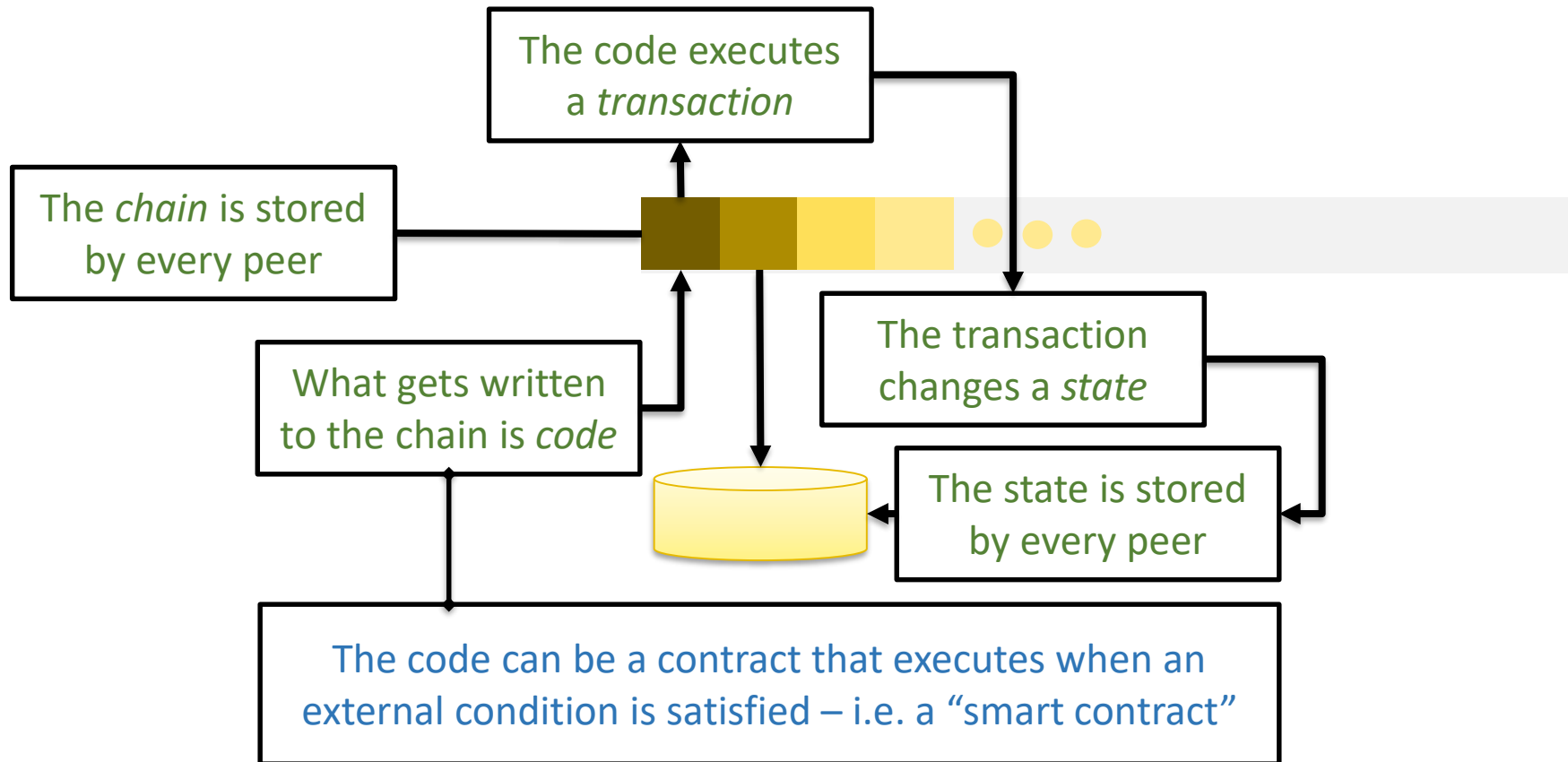


NTSAToday



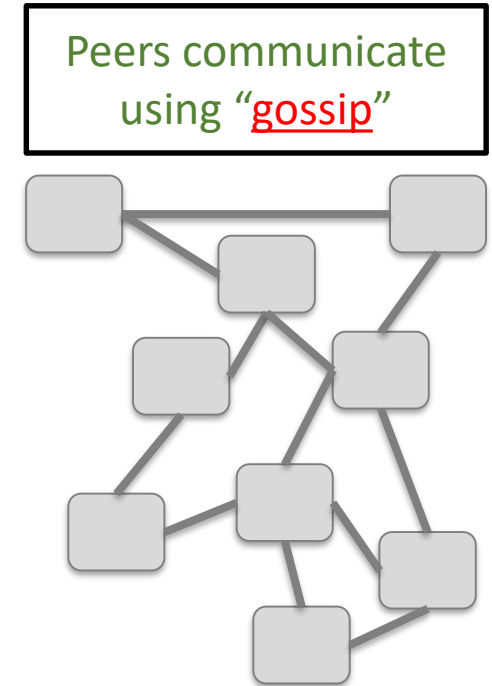
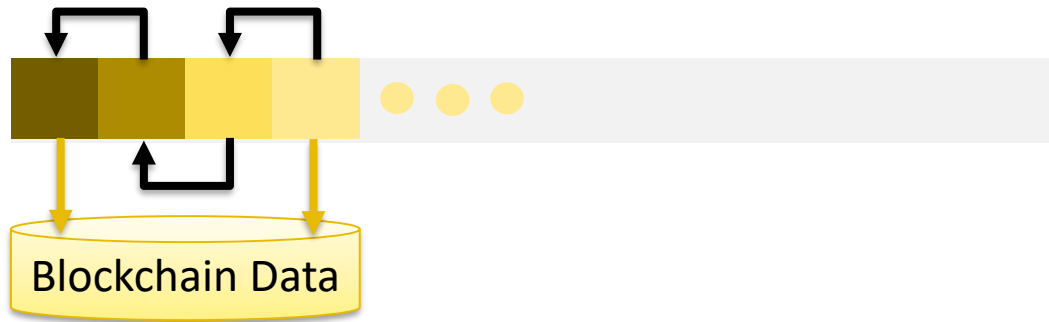
What is a Blockchain (really)

A blockchain is a network of peers (“nodes”) that provides a distributed database service



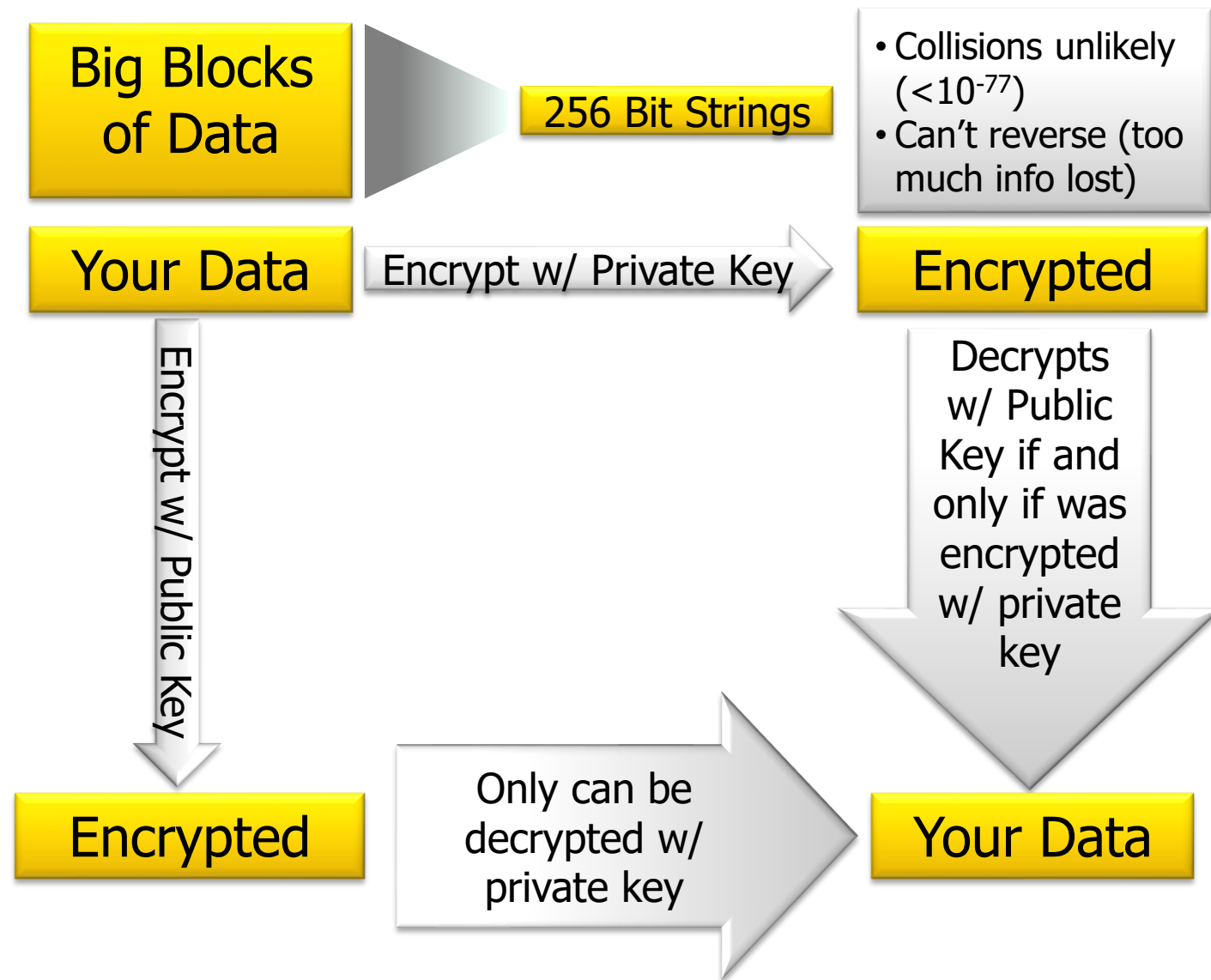
What Makes it a Blockchain?

- Each block contains a digital signature of the previous block
- Each peer accumulates proposed transactions
- The next block is determined by a consensus process
- Peers get paid for their work (by acquiring coins or directly by users)
- Private implementations include permissioned access to data



Some Technical Details

- Hash Functions
 - Ensure data has not been altered
- Public / Private Keys
 - Used to encrypt (protect) data
 - Used to furnish and verify identity
 - Encrypted + Hashed = Signed
- Bitcoin's proof-of-work concept
 - Add numbers to data before hashing
 - Different choices = different hashes
 - Find one that starts with lots of 0's
 - Takes computation – reward with coin



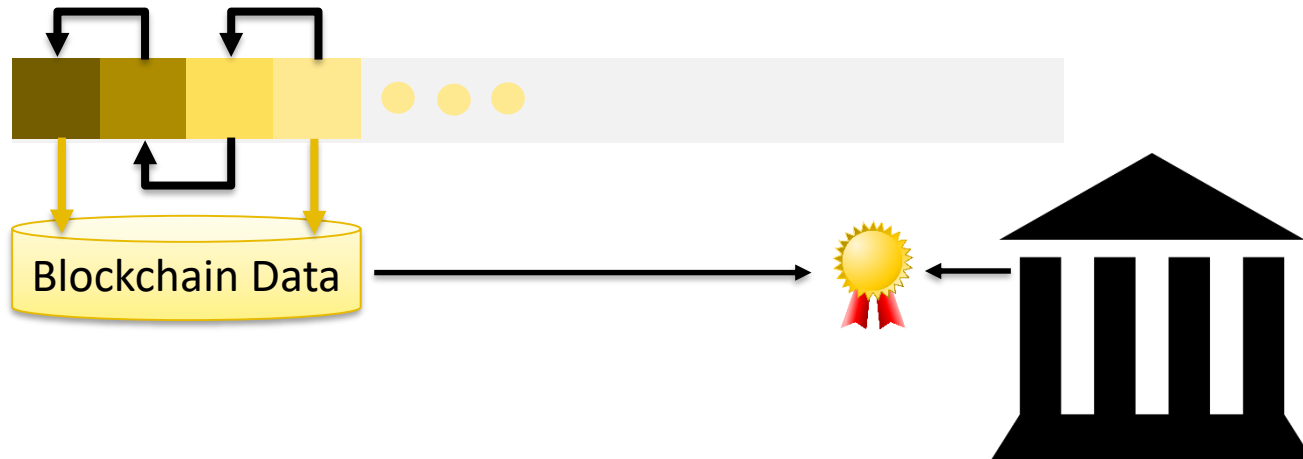
Off-chain Data

PROBLEM: Data on a blockchain can be encrypted but is visible to all

- Conflicts with privacy policies
- Makes it non-erasable (with some caveats)

SOLUTION: Sensitive data that may need to be erased or altered is kept *off the chain*

- Transactions awarding the data are on chain
- A hash of the data is on the chain



“Off chain” implementations (such as <https://www.blockcerts.org/> and CEDAR) store pointers to external, authoritative data plus *digital fingerprints* (hashes) that can be used to verify the data



A Range of Chains

- Bitcoin (and other dedicated financial Blockchains)
 - Only track transaction data on their chains by design
 - Use a coding language that has limitations
- Other Blockchains offer additional functionality, e.g.,
 - Storage capacity (Storj)
 - Distributed computing environments (Ethereum)
 - Specialized in the Internet of Things (IOTA)
 - Cater to enterprise uses, e.g. enable centralized authority and use standard computing languages (Hyperledger)
- Ethereum
 - Supports smart contracts and uses a robust programming language
 - Requires users to pay for processing and enables peers to set prices (payment in *ether*)

Ethereum

Market capitalization: \$73 bln

IOTA

Market capitalization: approx. \$15 bln

Coinbase

Market capitalization: \$2 bln (GDAX)

Ripple

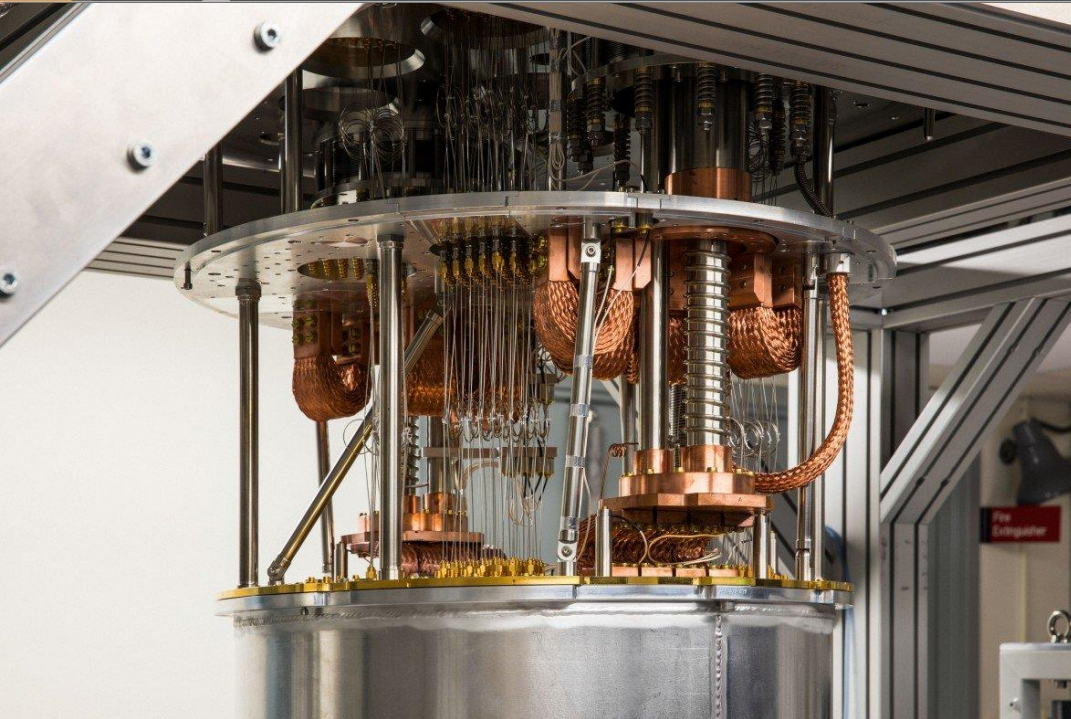
Market capitalization: \$30 bln

Qtum

Market capitalization: \$5 bln

<https://cointelegraph.com/news/top-10-companies-of-the-blockchain-industry-in-2017>

Quantum Computing and Blockchain



JEREMY LIEBMAN

Intelligent Machines

Serious quantum computers are finally here. What are we going to do with them?

Hello, quantum world.

by Will Knight February 21, 2018

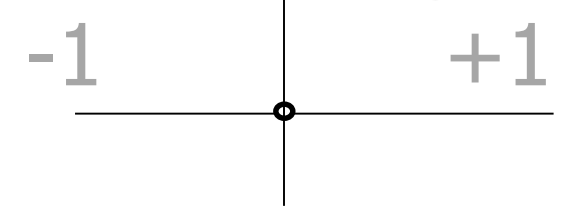
Source: MIT Technology Review

Quantum computing and Blockchain

Cryptography (and hash functions) are based on mathematical problems that are believed to be computationally hard.

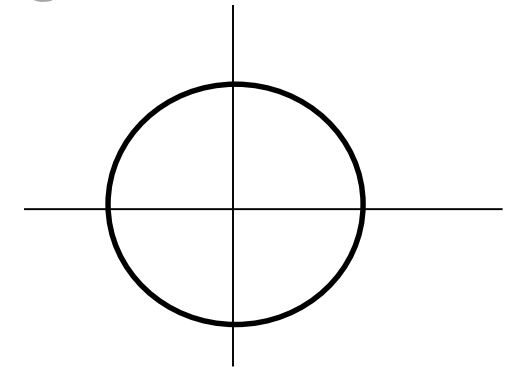
- There are two basic ways that “hard” can become “easy”
 - Better theory
 - More computing power
- Example: What is $1 + 2 + 3 + \dots + 1,000,000$?
 - You can't do the sum quickly by adding up all the numbers but ..
 - You can if you know that the answer is $(1,000,000) * (1,000,001) / 2$ – much easier! (Better theory)
 - You can if you have a computer that can add really fast (like the one in your phone)
- *Public Key Cryptography, as done today, is known to be susceptible to Quantum Computing.*

Binary Digits



Values in “0-dimensional Circle” instantiated as $\{-1, +1\}$

Quantum Bits



Values in 1-dimensional circle instantiated as complex unit circle



Getting Back to Training ... A Demo

We are researching blockchains for:

- Lifelong Learner Records
- Learning Record Stores
- DoD Training Jackets
- HLA-type Federations



DEMO OF CEDAR/CaSS (OPEN SOURCE ADL PROJECT)

(SCREENSHOTS TO BE ADDED AS BACKUP)



On the Road Ahead

- What's coming in the future for Blockchain technology
- Something regarding its use as a currency
 - Further international regulation
 - Potential to further disrupt worldwide economies
- DoD Policy will need to address the use of the technology
 - Research on its impact on cybersecurity capabilities
 - What distribution of data can mean to the Warfighter
 - Acquisition guidance, opportunity to partner with industry
- Standardization across a range of industries



Discussion & Resources for Further Study

Presenter emails:

robby.robson@eduworks.com

mike.hernandez.ctr@adlnet.gov

- <http://ethereum.registry.cassproject.org/>
- <https://www.blockcerts.org/>
- <https://www.ethereum.org/>
- <https://bitcoin.org/en/>
- <https://www.wired.com/story/187-things-the-blockchain-is-supposed-to-fix/>
- <http://blockchain.mit.edu/>
- <https://bitcoin.org/bitcoin.pdf>