LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Blockchain for Healthcare

10/07/2021

TLP: WHITE, ID# ***202110071300***

Agenda

- Introduction
- Concepts and Definitions
- History
- Functionality
- General Applications
- HPH Applications
- Conclusions
- References

Slides Key:

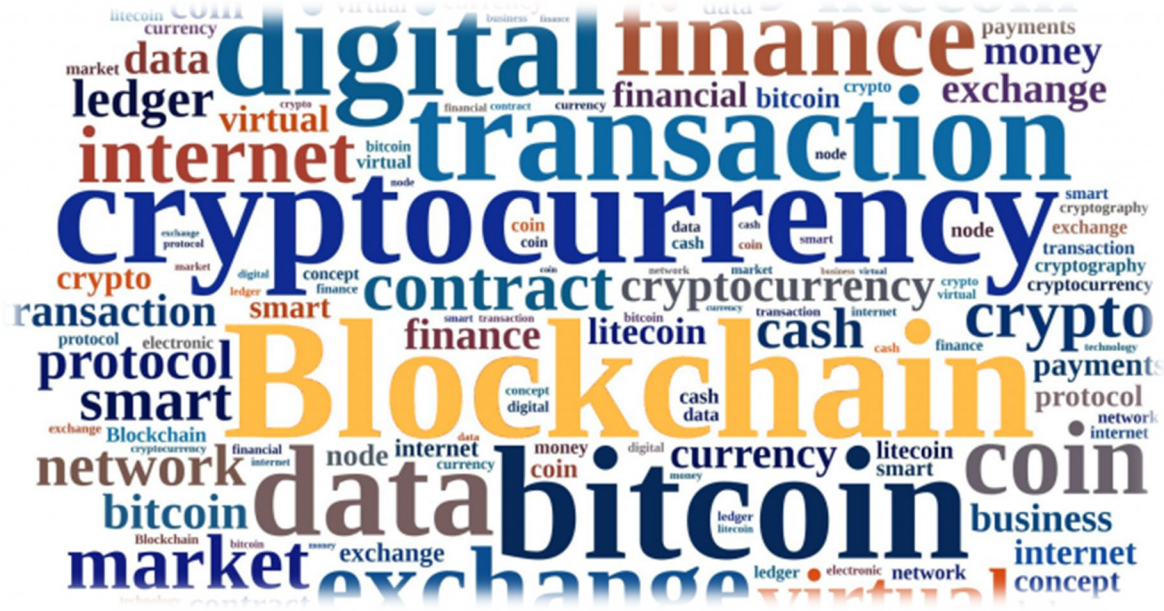
Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Blockchain as a Buzzword

What is blockchain at its most fundamental level?

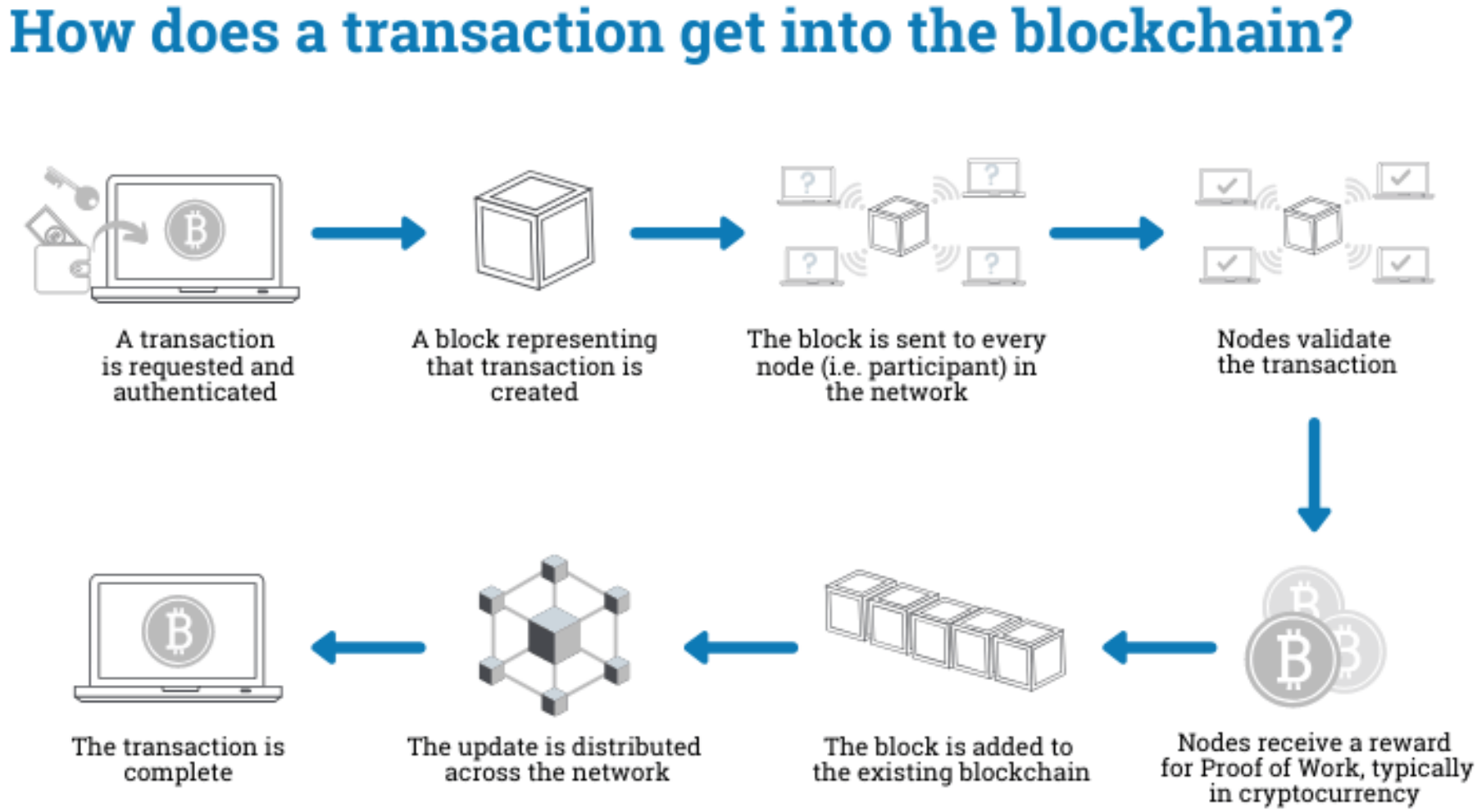
- A reconceptualization of trust relationships
  - No need for third party intermediaries
  - Highly secure
- Distributed trust – many witnesses are better than one
- Blockchain features:
  - Peer-to-peer (decentralized) network
    - Distributed ledger
  - Hashing
  - Consensus mechanism
- The hype is real!



Important blockchain concepts and definitions:

- **Ledger** – A record of transactions over time while still allowing for tracking and analysis. It documents the transfer of ownership and is ultimately a means for proving ownership.
- **Block** – A block is a unit of data (or record) that holds a collection of transactions which, together with many other blocks arranged in a specific order, form a blockchain.
- **Hash** – Digital equivalent of a fingerprint; unique and useful for detecting change in a file. This is one component that makes the blockchain secure.
- **Consensus mechanism** – A fault-tolerant process to achieve agreement about a set of data among many users or nodes. Proof of work is one of the most common consensus mechanisms.
- **Miner** – A blockchain user/nodes who participates in a competition with others to solve complex cryptographic problems, in order to validate a particular block, have that block added to the blockchain, and receive a reward for doing so.
- **Blockchain** can refer to:
  - A data structure which represents a series of immutable transaction records
  - An algorithm
  - A collection of technologies
  - A distributed, peer-to-peer network of systems
  - A system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.

Overview of blockchain functionality:



Important milestones in the history of blockchain:

- 1982 – Cryptographer David Chaum proposes an early form of blockchain in his dissertation, "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups."
- 1991 – Stuart Haberand and Scott Stornetta improved on the idea in their Journal of Cryptology article, "How to time-stamp a digital document."
- 1995 – David Chaum created the first digital currency, DigiCash, which used blind signatures for anonymous transactions. Digicash would go bankrupt in 1998.
- 1996 – E-Gold was started by Douglas Jackson and Barry Downey, which was a digital currency backed by gold; the company was eventually brought down due to facilitation of fraud.
- 1997 – Cryptographer Adam Back develops Hashcash, an email filter based on a proof-of-work system to prevent spam and denial of service (DoS) attacks. It appended a textual encoding of a hashcash stamp to the email header to prove that the sender utilized some CPU power in calculating the hashcash stamp.
- 1998 – Computer engineer Wei Dai published a paper called "B-money, an Anonymous, Distributed Electronic Cash System" which contained many of the concepts used by modern cryptocurrencies, such as anonymity and the lack of traceability, and the ability to enforce contracts within the network.
- 2007 to 2008 – Global financial crisis
- 2008 – Satoshi releases white paper
  - Implements Blockchain and Bitcoin

Global Impact

How has (and is) blockchain changing the world?

- Estimated 300M global cryptocurrency users
  - Bitcoin
    - ~17% of the U.S. adult population owns Bitcoin
    - Global market cap: $775B
    - Accepted by more than 15K businesses for payment globally
  - Thousands of altcoins in existence
  - 81 countries considering implementing central bank digital currencies; 9 have implemented pilot programs
- Defi (decentralized finance) as a branch of finance is growing aggressively ($20B as of January 2021)
- Cryptoeconomics (economics based on blockchain technologies) is now a recognized academic field
- Non-fungible tokens (NFTs) are selling for millions of dollars
- Decentralized Autonomous Organizations (DAOs) are becoming more common

Blockchain is a distributed ledger…

What is a ledger?

- A record of accounts and transactions, usually including a beginning and ending balance.
  - Financial transactions related to a company
  - Three types: Creditors, debtors and general
  - General ledger: Assets, liabilities, income, expenses and capital

GENERAL LEDGER

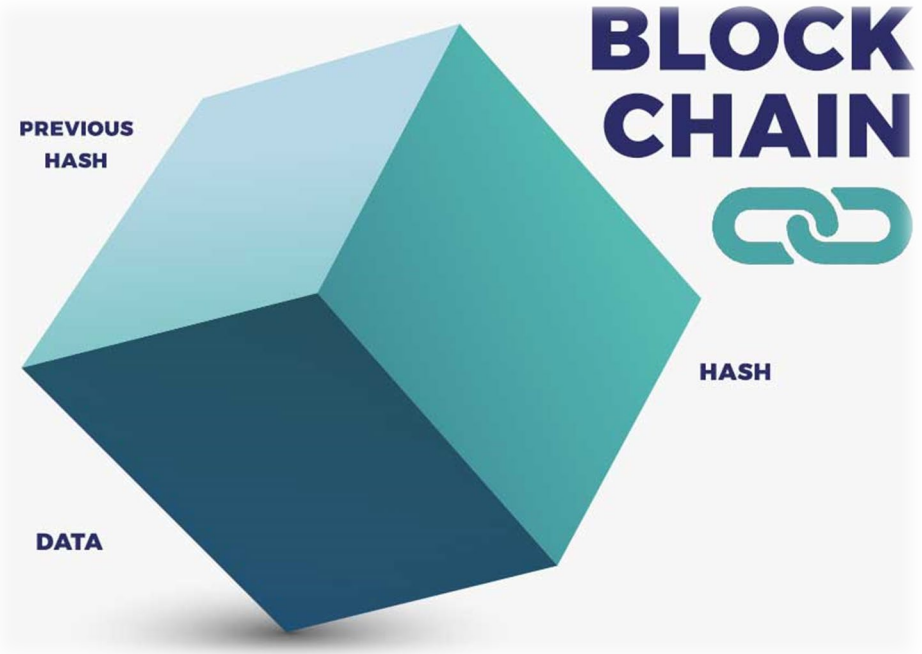
Cash					Account No. 101
Date	**Item**	**Ref.**	**Debit**	**Credit**	**Balance**
2019					
Jan. 3	Cash for common stock		20,000		20,000
Jan. 9	Payment from client		4,000		24,000
Jan. 12	Utility bill			300	23,700
Jan. 14	Dividends payment			100	23,600
Jan. 17	Cash for services		2,800		26,400
Jan. 18	Paid cash for equipment			3,500	22,900
Jan. 20	Paid employee salaries			3,600	19,300
Jan. 23	Customer payment		5,500		24,800

Block Composition

Blockchain maintains a distributed digital ledger via the use of blocks…a chain of blocks (hence the name).

Each block contains:

- Data – Purpose of the blockchain will dictate type of data
- Hash – Digital fingerprint, identifies block and all its contents uniquely
- Previous hash – Links current block to previous block; key to security

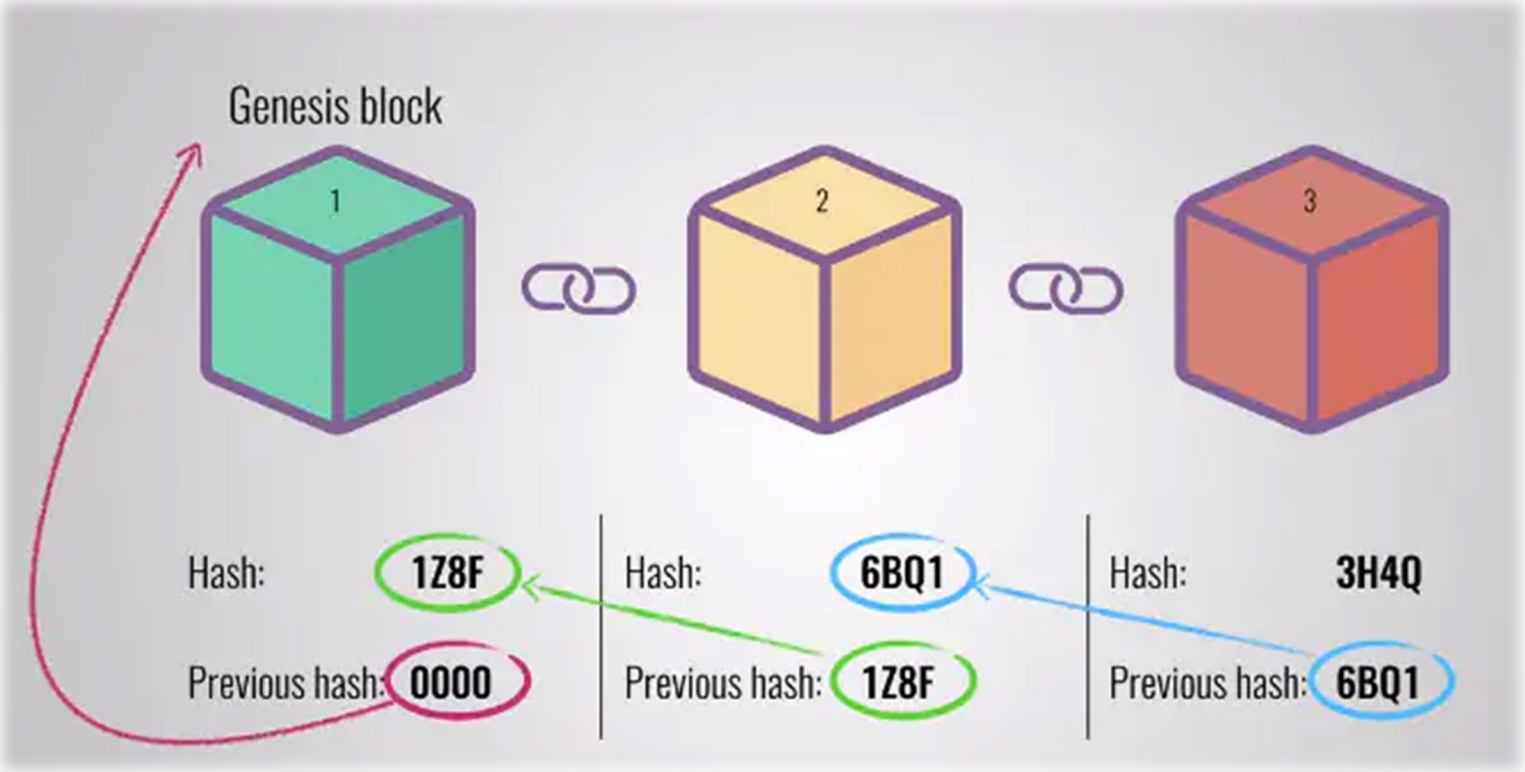


- Hash function
  - Maps data of arbitrary value to a fixed-size value
  - Output known as digest, hash value, or hash
  - One way; irreversible
  - Collision resistant
  - Equivalent to human fingerprint

Again, each of these blocks refers to the previous block due to the fact that it contains a hash of it. If a block is tampered with, the hash of it will change for it and all previous blocks, making detection trivial.

This is one of the key concepts of blockchain integrity, and is one of several mechanisms that ensures that records can't be deleted or modified.

Also worth noting: The first block in any blockchain is called the genesis block.



Hashes are necessary but not sufficient to prevent tampering. Why?

- Hashing means tampering with a block makes all following blocks invalid. However, due to modern processing capabilities, it is possible to calculate a large number of hashes – those in all the following blocks – all over again, making that modified blockchain valid again. Therefore, we need something else…

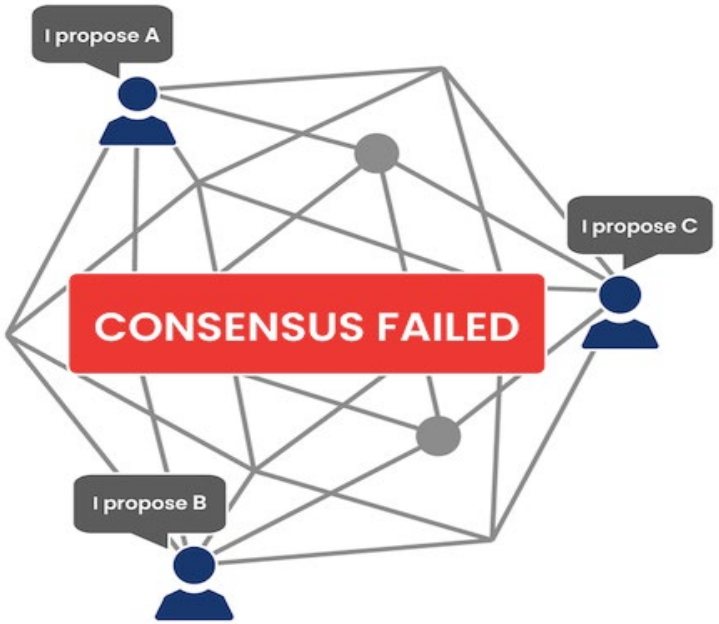
Blockchain has a consensus mechanism called proof of work. What is a consensus mechanism?

- A consensus mechanism refers to any number of methodologies used to achieve agreement, trust, and security across a decentralized computer network. It slows down the creation of new blocks.

Possible consensus mechanisms:

- Proof of work
- Proof of stake
- Delegated Proof of Stake
- Delegated Byzantine Fault Tolerance
- Proof of Burn
- Proof of Activity
- Proof of Elapsed Time
- Proof of Capacity
- Others…

MOST COMMON



Proof of work is used to validate transactions and broadcast new blocks to the blockchain.

Proof of work is a way for someone to prove that they have engaged in a significant amount of computational effort. That effort can be validated in a way that is easier and quicker than the original calculations.

How does it work?

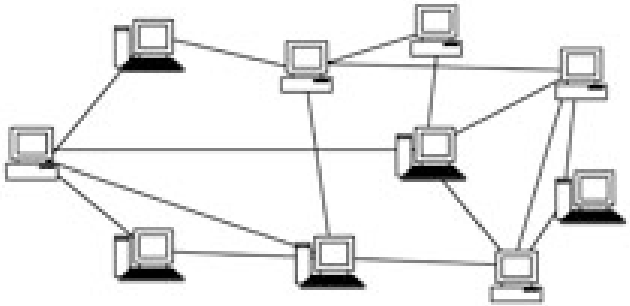
- Miners on a network will compete against each other in solving complex computational puzzles.
  - "Miners" are actually working to guess a pseudorandom number (nonce).
  - When the solution is found by a miner, other miners will validate it.
  - Upon validation, the miner is rewarded with a block reward.

Proof of work slows own the creation of new blocks. If you want to tamper with one block, you will have to recalculate the proof of work for that block, and all the following blocks as well.

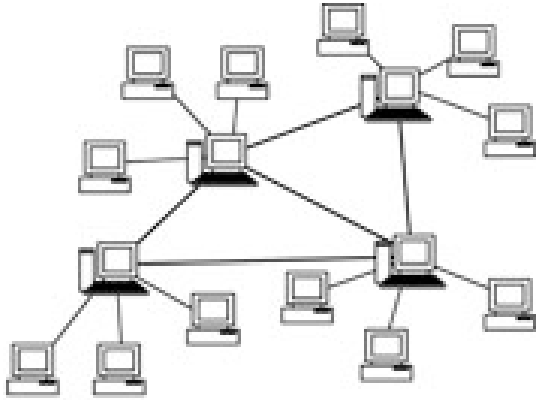
- Example: For Bitcoin's blockchain, it takes ~10 minutes to calculate a new block – multiply that by many blocks, and a tampering attack becomes infeasible due to the time and computing power required.
- Proof of work means costs of an attack is greater than the reward.
- Proof of work also means any node can compete.

Blockchain is a distributed/decentralized, peer-to-peer system. What does this mean?

a Centralized overlay. Central peer facilitates the interactions among the leaf-peers.



b Decentralized overlay. No central authority, all peers treated equally.



c Hybrid overlay. Hierarchical topology, interconnected super-peers locally serve the subsets of leaf-peers.

Blockchain Implementation: Cryptocurrencies

Cryptocurrencies have demonstrated traditional properties of fiat money:

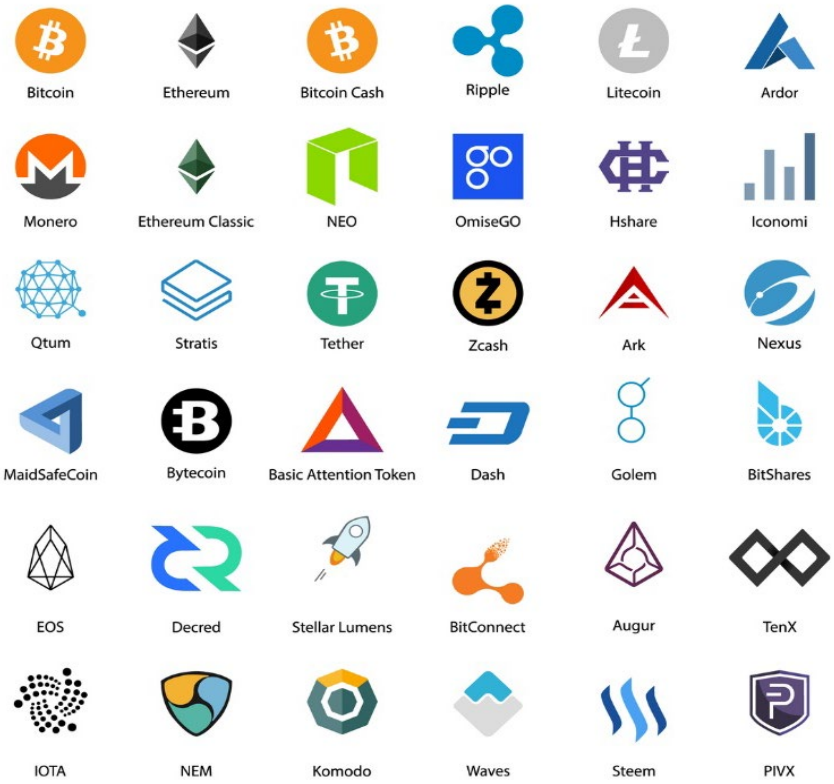
1. Medium of exchange
2. Measure of value
3. Standard of deferred payment
4. Store of value

Cryptocurrencies have demonstrated function as an investment vehicle:

- Individuals and companies

Cryptocurrencies have demonstrated political value:

- Considered to be a “censorship-free” form of payment
- They are also used by criminals



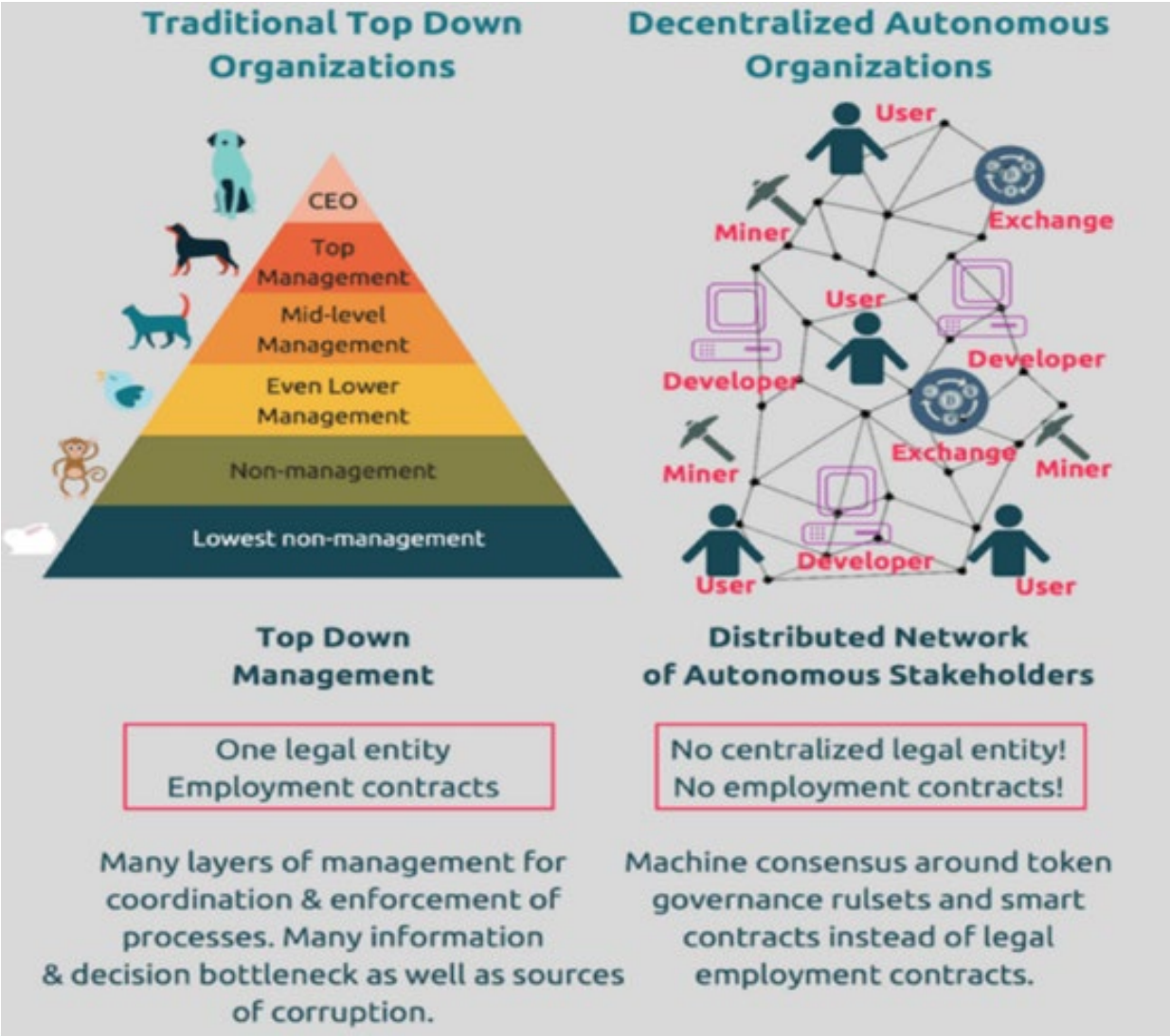
Cryptocurrencies are also controversial: there are people who would disagree with each of the above uses, questioning the value of cryptocurrencies for these purposes.

What is a smart contract?

- A self-executing contract has certain terms of the agreement, which are automatically initiated when specified conditions are met
- Run on blockchain and use algorithms to create and measure execution conditions
- Properties:
  - Self-executable
  - Self-verifiable
  - Highly resistant to tampering
- Benefits
  - High level of trust
  - Minimization of errors
  - Resistant to fraud
  - Cost-efficient

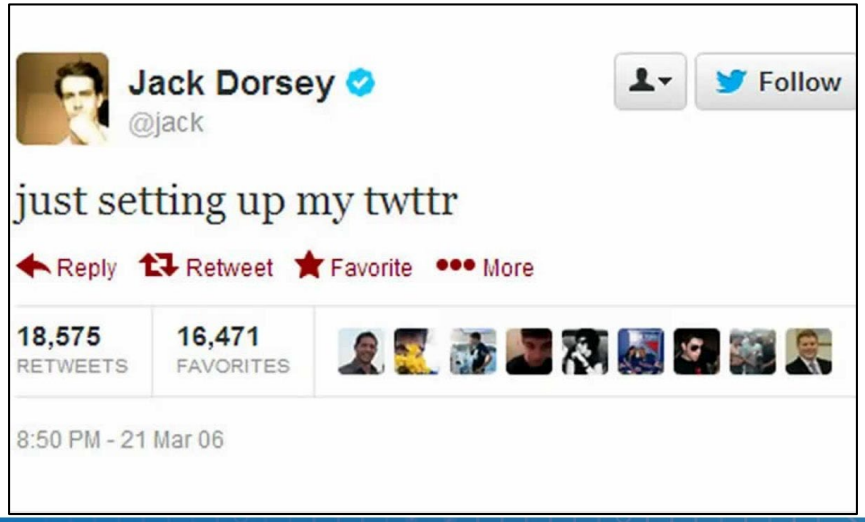
Decentralized autonomous organizations:

- An organization that has much less legal structure and is operated with rules that are predicated on blockchain
- An alternative to traditional, “top-down” hierarchies
- Unsettled legal status – not recognized by entities and unlikely to be anytime soon
- No traditional “employees”
- Peer-to-peer internal relationships



What is a non-fungible token?

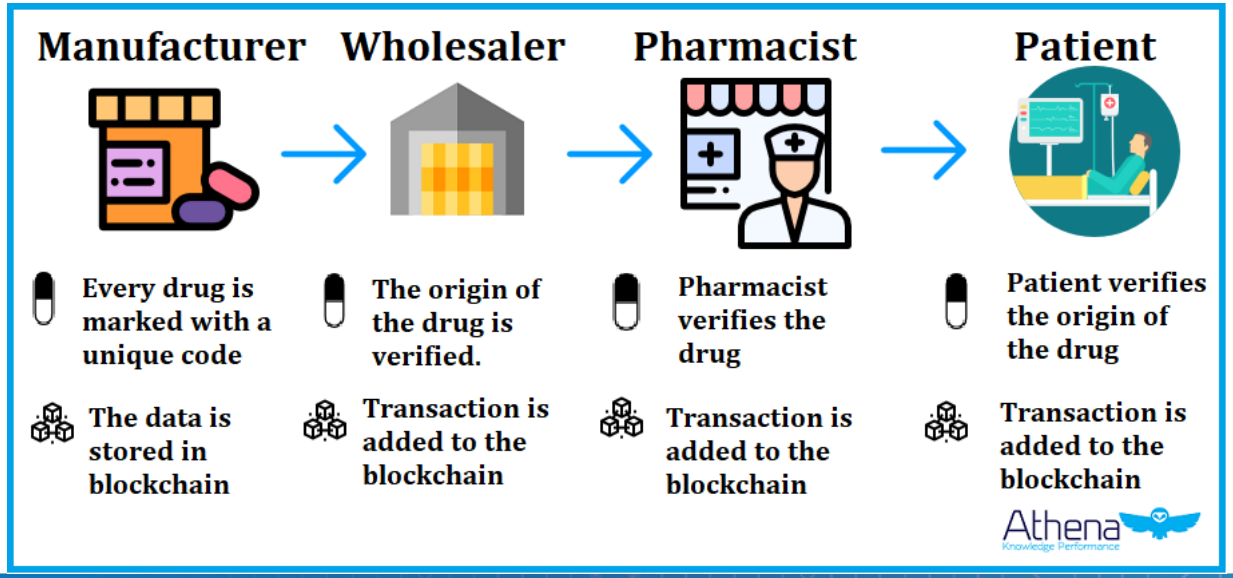
- It's "non-fungible" – it's unique and can't be exchanged for another identical NFT.
- It's digital in its form – it doesn't exist in the physical world.
- It's a unique digital/virtual asset with ownership certified by blockchain.
- One example: Digital collector of unique art
  - Jack Dorsey (CEO of Twitter) sold a certified copy of his first tweet for $2.9M, and donated the proceeds to charity.
  - An artist sold a collage of his art in JPG – a digital graphics format – for $69M.
- Markets for NFTs exist and are growing quickly.



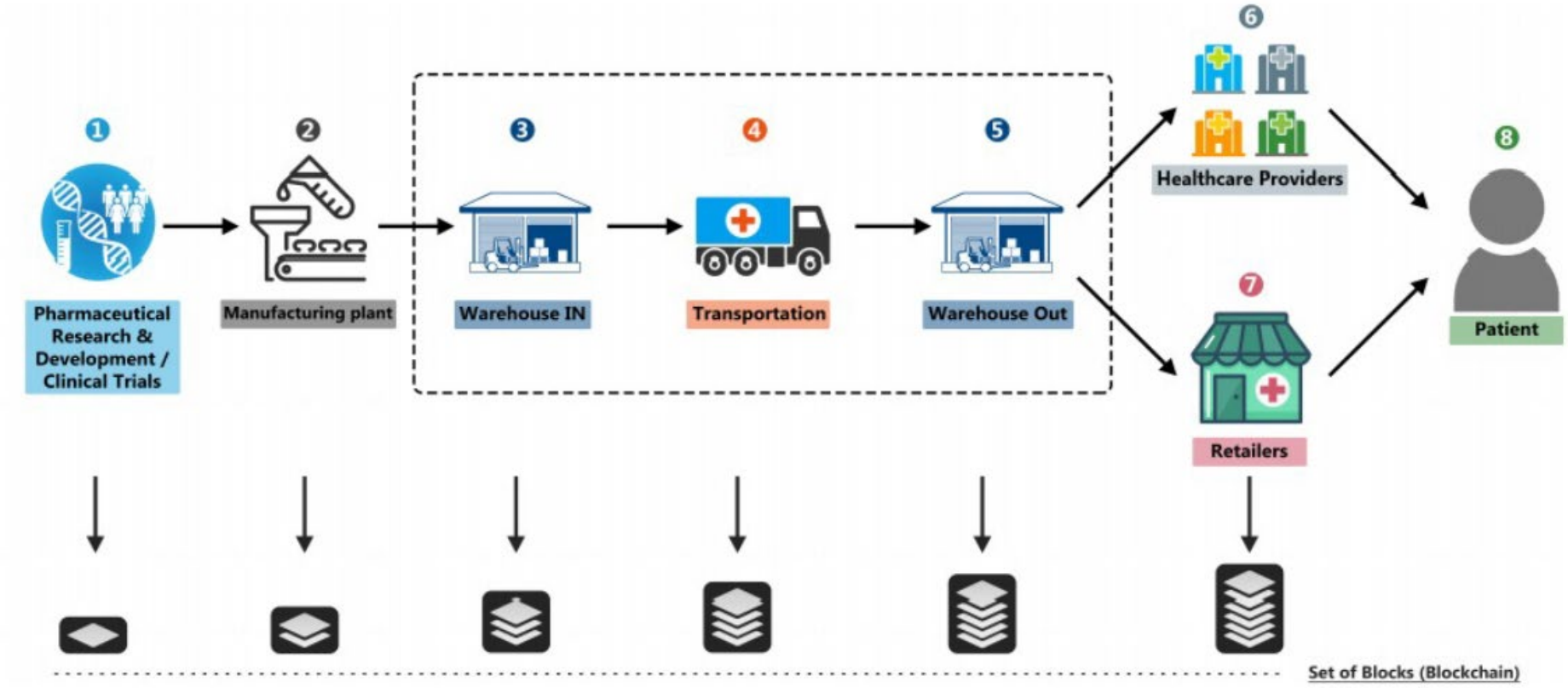
Healthcare Blockchain Use Case: Supply Chain Transparency

Healthcare supply chain transparency, especially with regard to pharmaceuticals:

- Challenge: Assuring the authenticity, origin and supply chain of medical products – easier said than done in a globalized world where international commerce can create complications
- Especially important in developing markets where counterfeit prescription medicines and medical devices can cause tens of thousands of deaths annually
- To solve this, companies and end consumers need to be able to track each package's end-to-end movement from the point of origin, including manufacturers, wholesale, transport, etc.
- Blockchain can enable companies throughout the prescription drug supply chain to verify the authenticity of medicines, expiry dates and other important information.



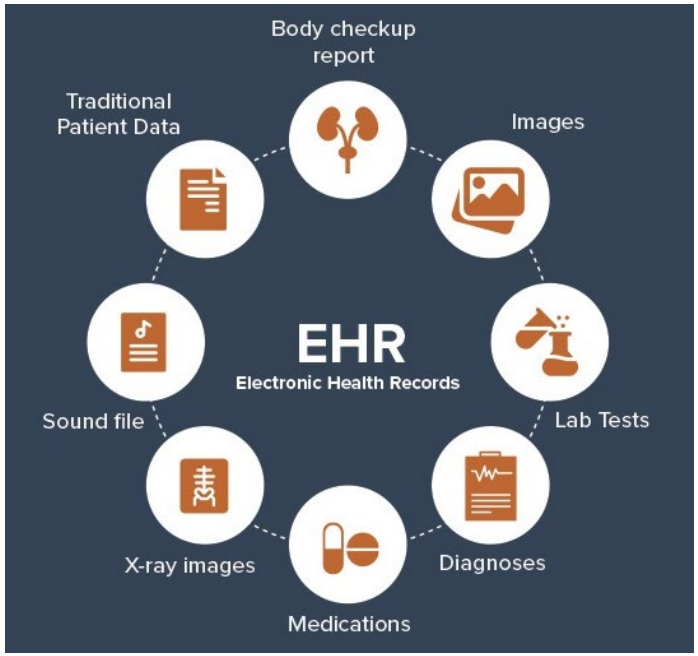
Blockchain facilitates transparency and security at many stages of the healthcare supply chain:



Healthcare Blockchain Use Case: Electronic Health Records

Immediate and secure access to health records by patients and their healthcare providers

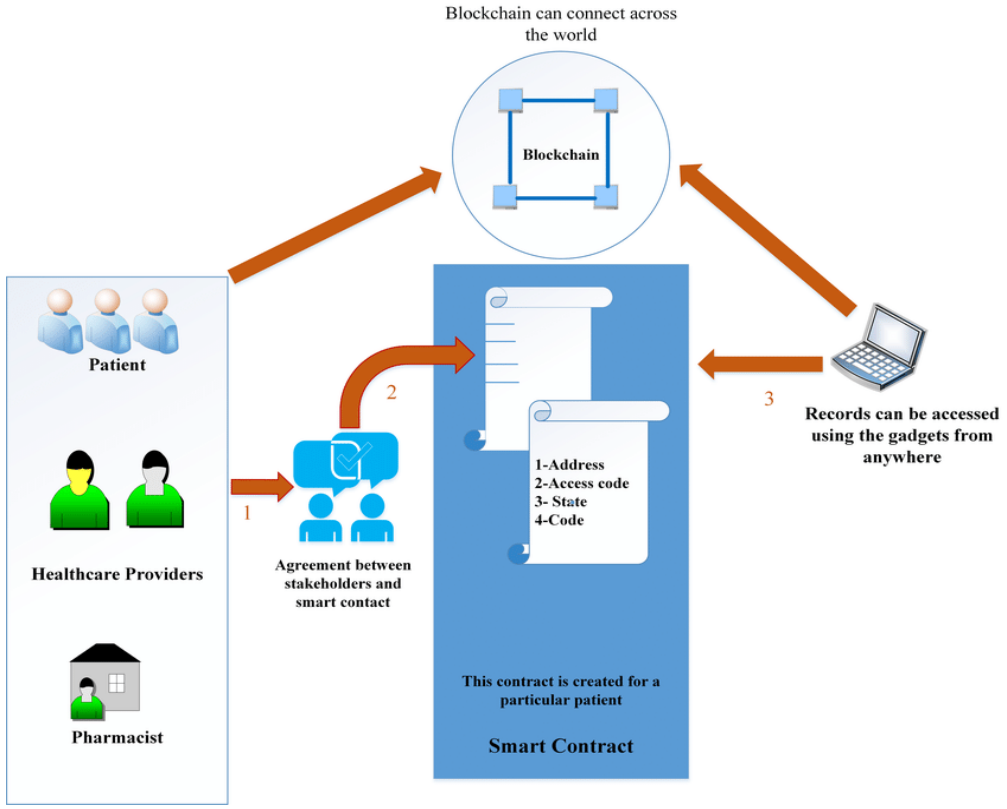
- Challenge: Ensuring patient access to all their heath/medical records across all service providers in order to have a complete view of medical histories, while ensuring their records are secure.
- Johns Hopkins University published research in 2016 revealing that the third leading cause of death in the US was medical errors that resulted from poorly coordinated care, such as planned actions not completed as intended, or errors of omission in patient records.
- Blockchain-based medical record systems can be linked into existing medical record software and act as an overarching, single view of a patient's record without placing patient data on the blockchain.
- Each new record can be appended to the blockchain in the form of a unique hash function, which can only be decoded if the person who owns the data – in this case, the patient – gives their consent.
- Benefits:
  - A comprehensive, single-source for accurate medical records
  - Direct access by medical insurers of validated, confirmed of healthcare services directly from patients, not requiring time and cost of an intermediary
  - The development of further advances in analytics



Healthcare Blockchain Use Case: Smart Contracts

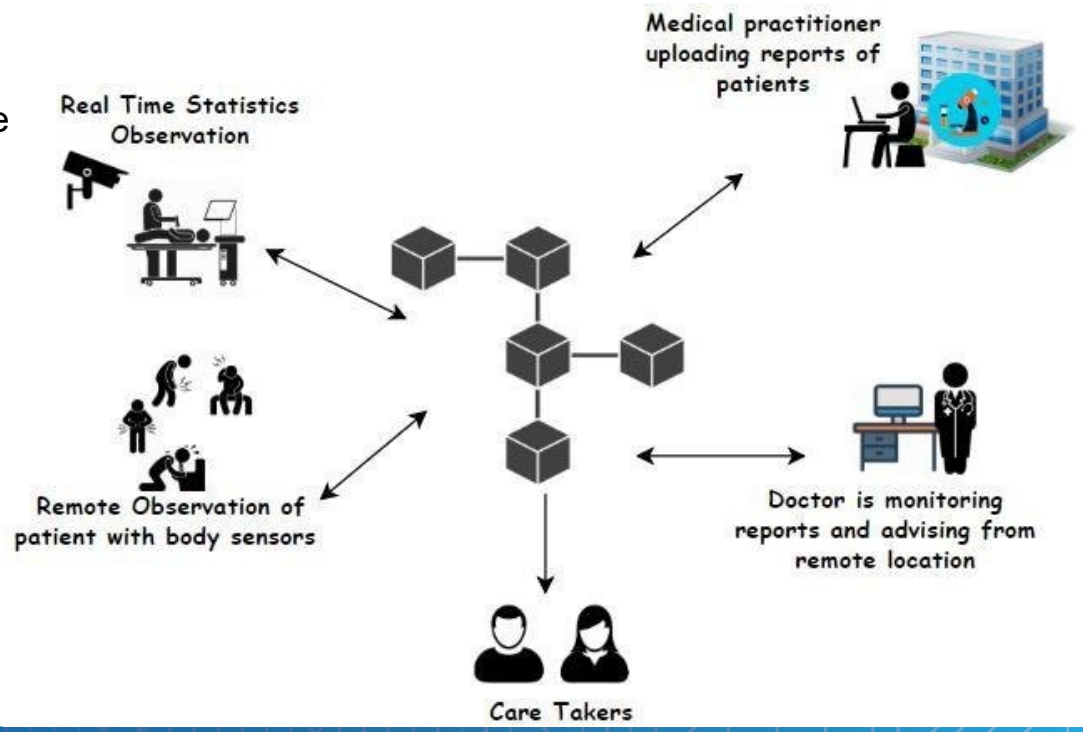
Immediate, secure and accurate communications with insurance companies and supply chains

- Challenge: Maintaining contracts of various types can cause unnecessary bureaucratic delays, additional costs, and inaccuracies which can consume time and legal resources to mitigate
- Blockchain can facilitate transactions between healthcare stakeholders, authenticating their organizational identities, logging contract details, and tracking transactions and payments for goods and services.
- This goes beyond traditional supply chain management to enable business partners and insurance providers in the health sector to operate based on fully digital and automated contract terms.
- Shared smart contracts between manufacturers, distributers and healthcare organizations included on a blockchain ledger, vice individual types of contracts, can significantly reduce payment disputes, which can be lengthy and consume resources.
- Shared smart contracts can be used to manage medical insurance contracts for patients, which, once this data is digitized and easily accessible, insurance providers can leverage more advanced analytics to optimize health outcomes and costs.



Reliable access to Internet of Things (IoT) technologies for remote patient monitoring

- Challenge: IoT and Internet of Medical Things (IoMT) technologies are susceptible to Distributed Denial of Service (DDoS) and other similar disruptive attacks. 5G is increasing the availability and deployment of these technologies, ultimately increasing the attack surface and making them more attractive targets.
- Many patients rely on remote monitoring solutions, where sensors measure patients' vital signs to provide healthcare practitioners visibility into patients' health, enabling more proactive and preventative care.
- Security can be an issue due to disruptive attacks
- Blockchain limits unauthorized data access
- IoT and IoMT devices – directly communicate
  - Less opportunities for disruption



Blockchain is turning traditional trust models on their head!

- A reconceptualization of trust relationships
  - No need for third party intermediaries
  - Highly secure
- Distributed trust – many witnesses are better than one
- Blockchain features:
  - Peer-to-peer (decentralized) network
    - Distributed ledger
  - Hashing
  - Consensus mechanism
- Blockchain is expected to provide the healthcare industry with
  - Improved confidentiality hand-in-hand with increased access to more comprehensive data
  - Better quality and more trustworthy goods and services (both procedures and medicine)
  - Less fraud, cheaper prices, more innovation
- The hype is real!

Reference Materials

References

How blockchain is set to revolutionize the healthcare sector
https://technative.io/how-blockchain-is-set-to-revolutionize-the-healthcare-sector/

HIMSS: Blockchain in Healthcare
https://www.himss.org/resources/blockchain-healthcare

Deloitte - Blockchain: opportunities for healthcare
https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html

National Institute of Standards and Technology – Blockchain
https://www.nist.gov/blockchain

Will blockchain save the healthcare system?
https://www.modernhealthcare.com/article/20190209/TRANSFORMATION02/190209953/will-blockchain-save-the-healthcare-system

Blockchain healthcare and life sciences solutions
https://www.ibm.com/blockchain/industries/healthcare

How Health Care Is Moving Toward Blockchain
https://www.investopedia.com/tech/how-health-care-moving-toward-blockchain/

Blockchain Technology and Healthcare
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6517629/

Blockchain in Health Care: Hope or Hype?
https://www.jmir.org/2020/7/e17199/

The Use of Blockchain in Healthcare
https://cloudsecurityalliance.org/artifacts/the-use-of-blockchain-in-healthcare/

Questions

Upcoming Briefs

- 10/21 – Hive Ransomware
- 11/4 – Cobalt Strike vs. the Health Sector

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV**.

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback, please complete the HC3 Customer Feedback Survey.

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or visit us at www.HHS.Gov/HC3.

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV