



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

# HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY



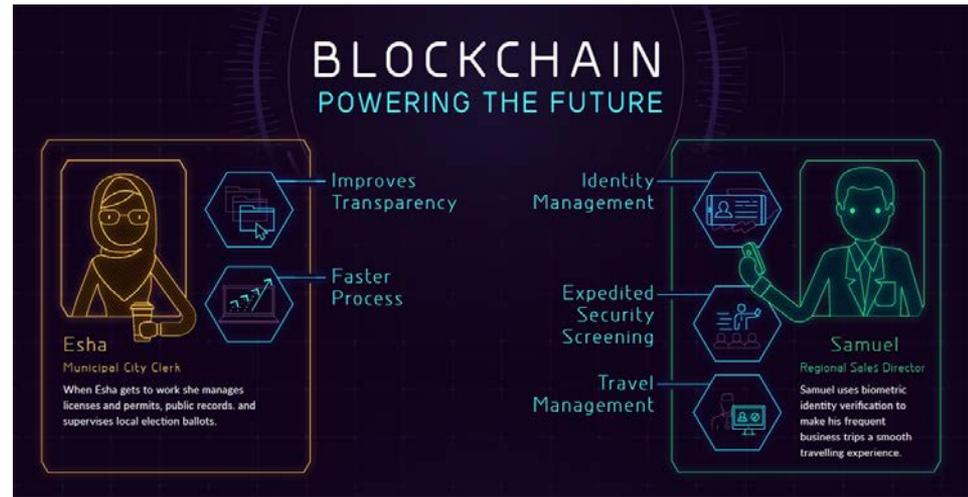
## HC3 Intelligence Briefing Blockchain Application in the Healthcare Industry

09/12/2019

# Agenda



- Overview
- What is Blockchain
- How Blockchain Works
- Types of Blockchain
- Layered View of Blockchain
- Blockchain Application to Supply Chain Management
- Blockchain Application to Employee Credentialing
- Blockchain Application to Electronic Health Records
- Challenges with Blockchain
- Conclusions



[Visual Capitalist](#)

## Slides Key:



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



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



- Satoshi Nakamoto released the whitepaper Bitcoin: A Peer to Peer Electronic Cash System in 2008 that described a “purely peer-to-peer version of electronic cash” known as Bitcoin, blockchain technology made its public debut.
- Several problems in Healthcare stem from the complex network of intermediaries and the lack of traceability of transactions.
  - Patient data is scattered across different entities in the value chain of the healthcare industry referred to as data silos and sharing of data is prone to a multi-level process of permission control.
- Blockchain has the potential to solve these problems as it provides trust without any intermediaries, has traceability as a default feature, and promises new business models by enabling novel incentive structures.



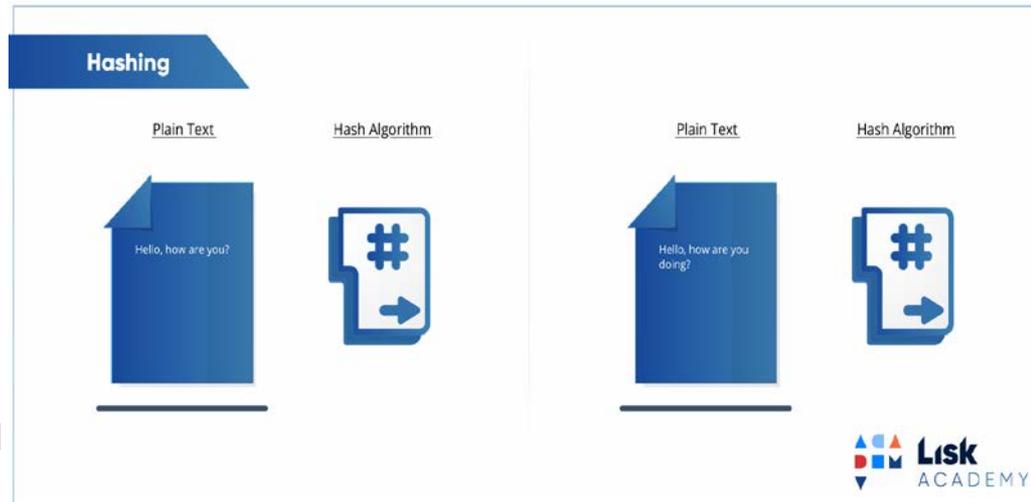
[Entrepreneur.com](https://www.entrepreneur.com)



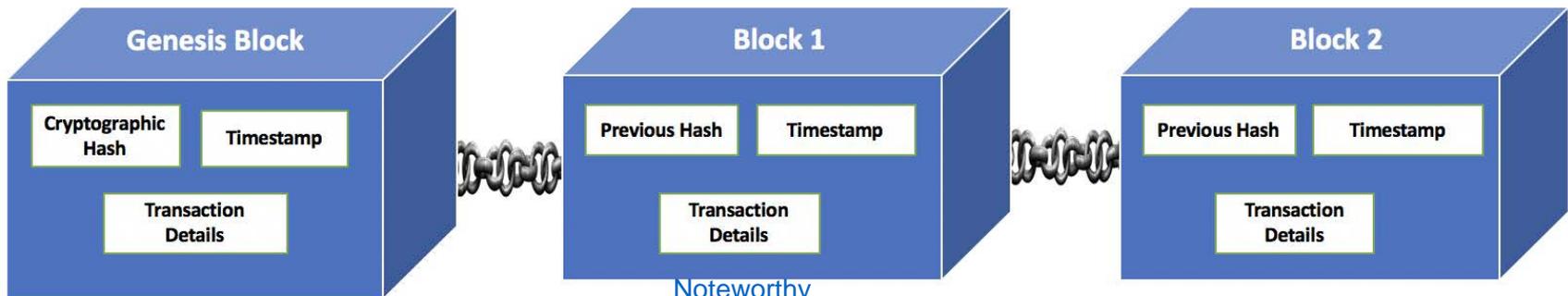
# What is Blockchain?



- Blockchain technology originated in 1991, and was conceived as a secure way to timestamp digital documents akin to how a notary timestamps physical documents. ([Medical Economics](#))
- Blockchain is an open distributed ledger, meaning that anyone provided with the requisite credentials can access and add to the ledger.
  - Each block contains the relevant encrypted data, which is referred to as a hash, and the hash of a previous block. The kind of data contained within a block depends on the type of blockchain being utilized. ([Medical Economics](#))



[Lisk Academy](#)

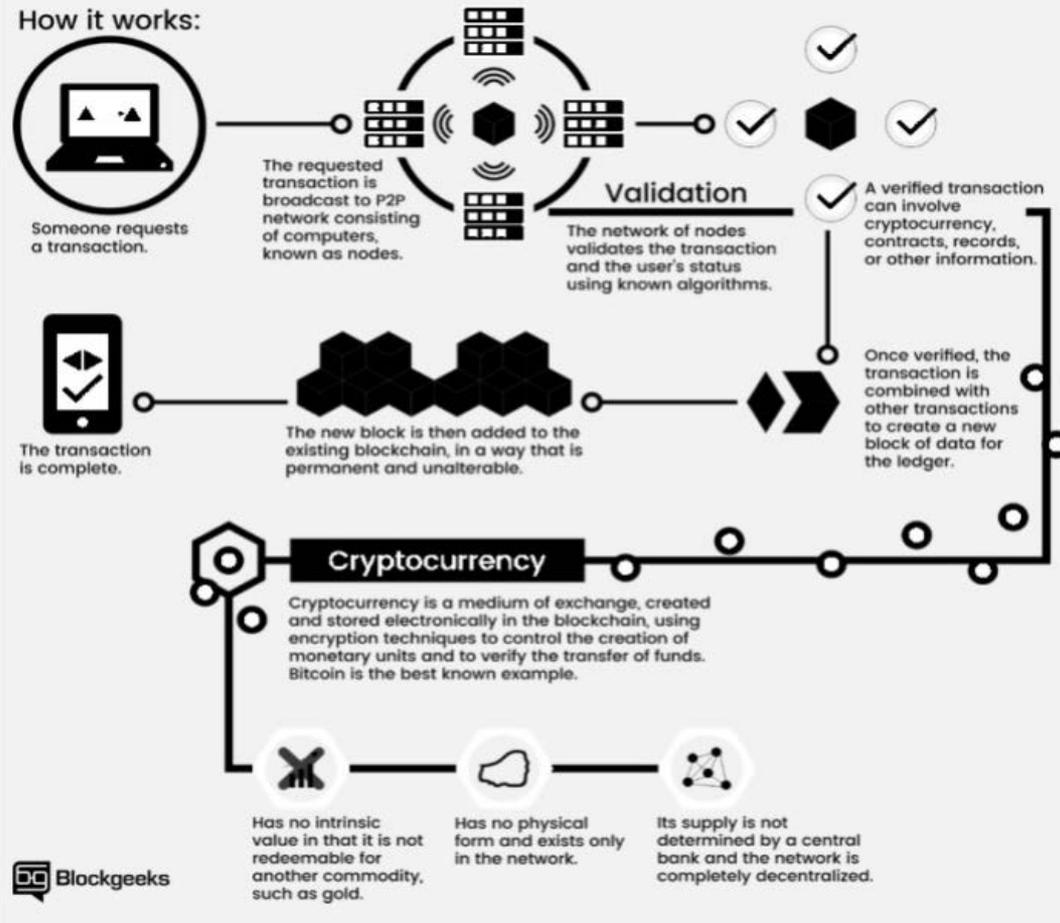


[Noteworthy](#)





**Figure 1: How Blockchain Works**



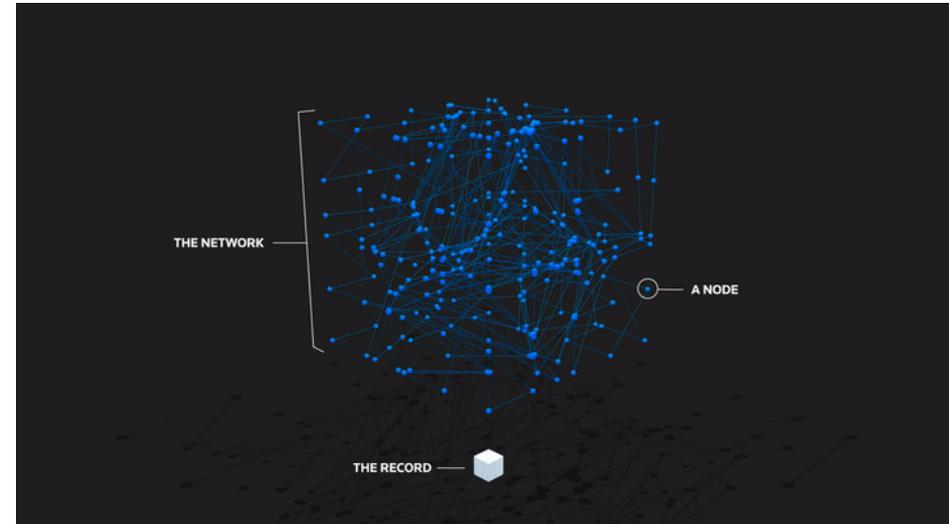


## STEP 1



A trade is recorded. For example, let's say Mr Pink is selling two of his coins to Mr Green for \$100. The record lists the details, including a digital signature from each party.

## STEP 2



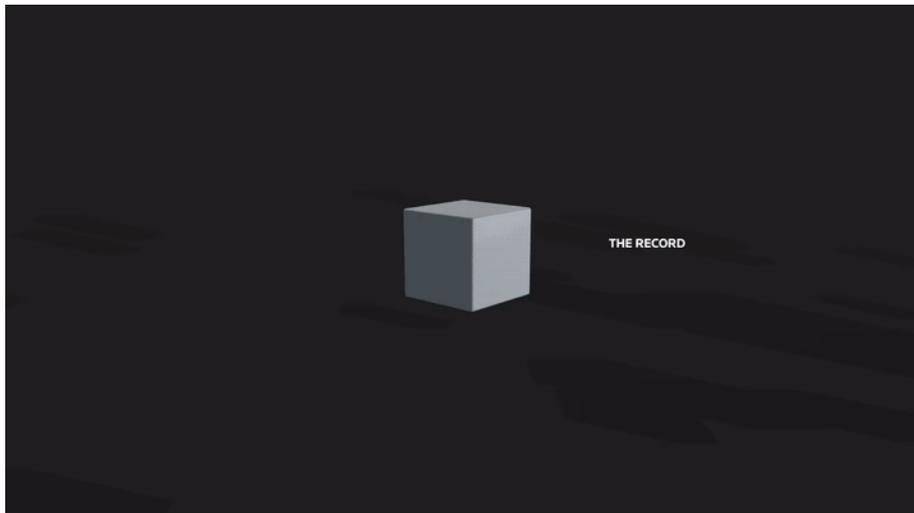
The record is checked by the network. The computers in the network, called 'nodes', check the details of the trade to make sure it is valid.

[REUTERS](#)



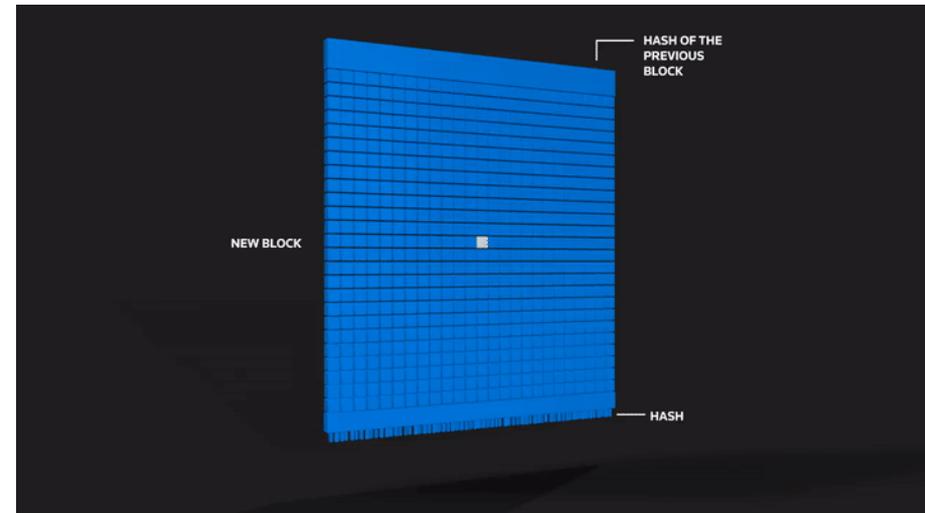


## STEP 3



The records that the network accepted are added to a block. Each block contains a unique code called a hash. It also contains the hash of the previous block in the chain.

## STEP 4



The block is added to the blockchain. The hash codes connect the blocks together in a specific order.

[REUTERS](#)

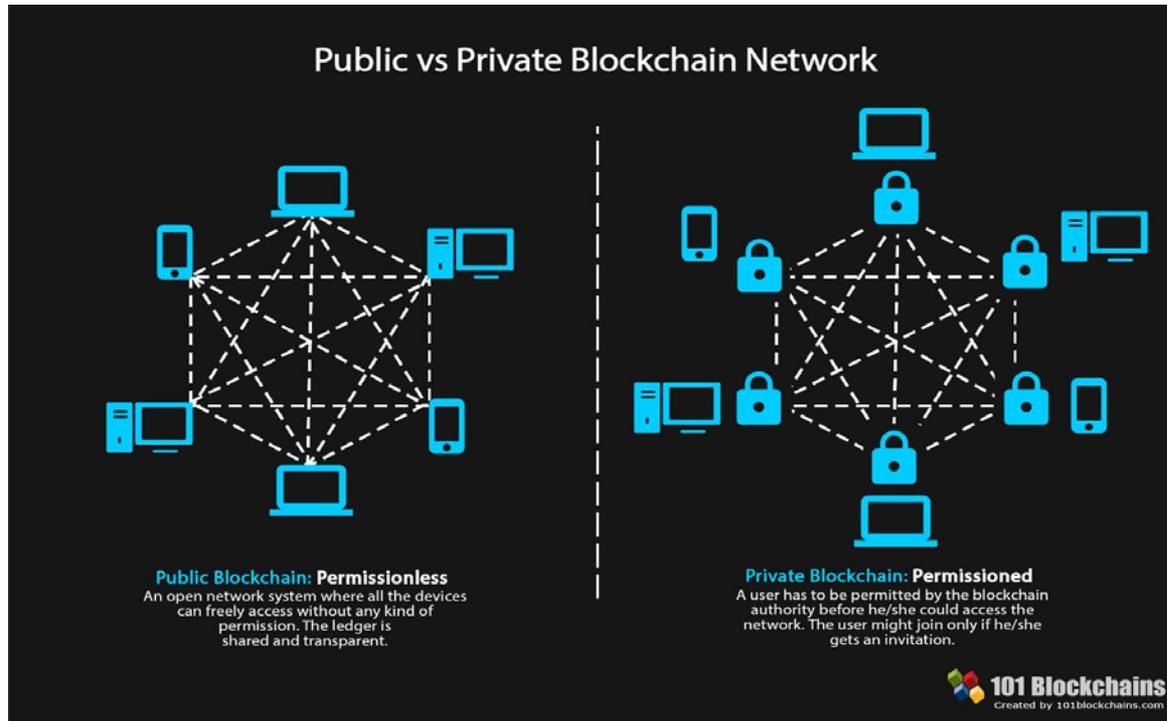


# Types of Blockchain



- **Public blockchain** A public blockchain is permissionless, and anyone can easily participate and validate the transactions. ([HIMSS](#))
  - Bitcoin is the pioneer public blockchain. Bitcoin, Ethereum, Waves, Dash, and Bitshares are few examples of public blockchains.

- ▶ **Private blockchain** A private blockchain is a permissioned blockchain centralized to one governing organization. Transactions are validated internally and may or may not be public readable.
  - [Monax](#), [HyperLedger](#) with Sawtooth, private Ethereum are a few examples of private blockchains.



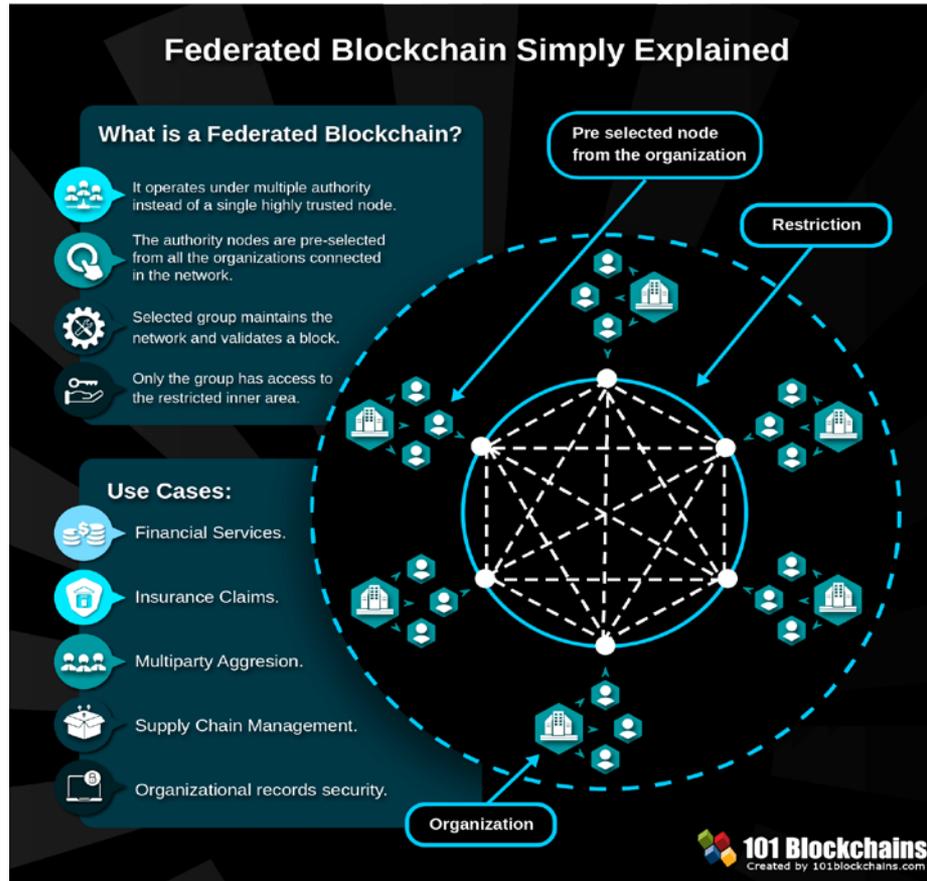
101 Blockchain



# Types of Blockchain



- **Federated blockchain** A federated blockchain is a permissioned blockchain operating under the leadership of a group often called the consortium. ([HIMSS](#))
  - Some examples includes [R3 Corda](#), [EWF](#) (Energy Web Foundation), and [B3i](#) (Insurance).



101 Blockchains





## *A Layered View of Blockchain, Smart Contracts, Cryptocurrencies, Artificial Intelligence, and Machine Learning in Healthcare*

**Layer 4**

Artificial Intelligence & Machine Learning Enable Major New Insights, Value

**Layer 3**

Cryptocurrencies & Tokens Enable New Commerce & Incentive Systems

**Layer 2**

Smart Contracts Increasingly Automate Transactions, Improving Efficiency

**Layer 1**

Blockchain Enables Secure Sharing of Healthcare Data Across B2B Networks

**Layer 0**

Healthcare Data Mostly in Silos, Little Sharing, Massive Untapped Potential

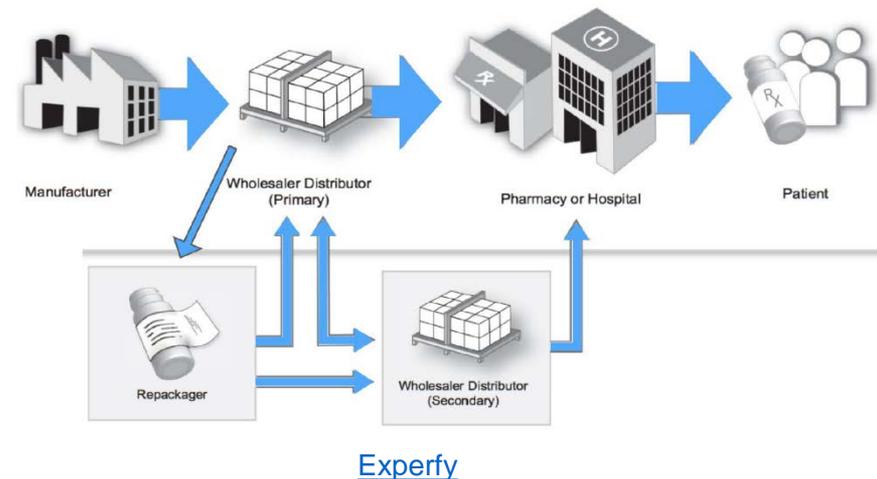
[Healthcare Information and Management Systems Society](#)



# Blockchain Solution to Drug Supply Chain



- The purpose of Drug Supply Chain Security Act (DSCSA) is to improve tracking, detection, and removal of counterfeit, misbranded, or potentially harmful drugs from the drug supply chain.
  - The DSCSA establishes a national standard for drug security, as opposed to the varying state requirements that had been regulating the space, by mandating the development of a prescription drug traceability system encompassing the full supply chain from manufacturer to dispenser for pharmaceuticals distributed in the United States.
- One of the core requirements of the DSCSA is that each package and homogenous case of product must contain a product identifier, which will be used to identify a product at any point in the drug supply chain.
  - The ability of blockchain to track and store data chronologically across a peer-to-peer network makes the technology particularly well suited to solve for the traceability requirements imposed by the DSCSA.



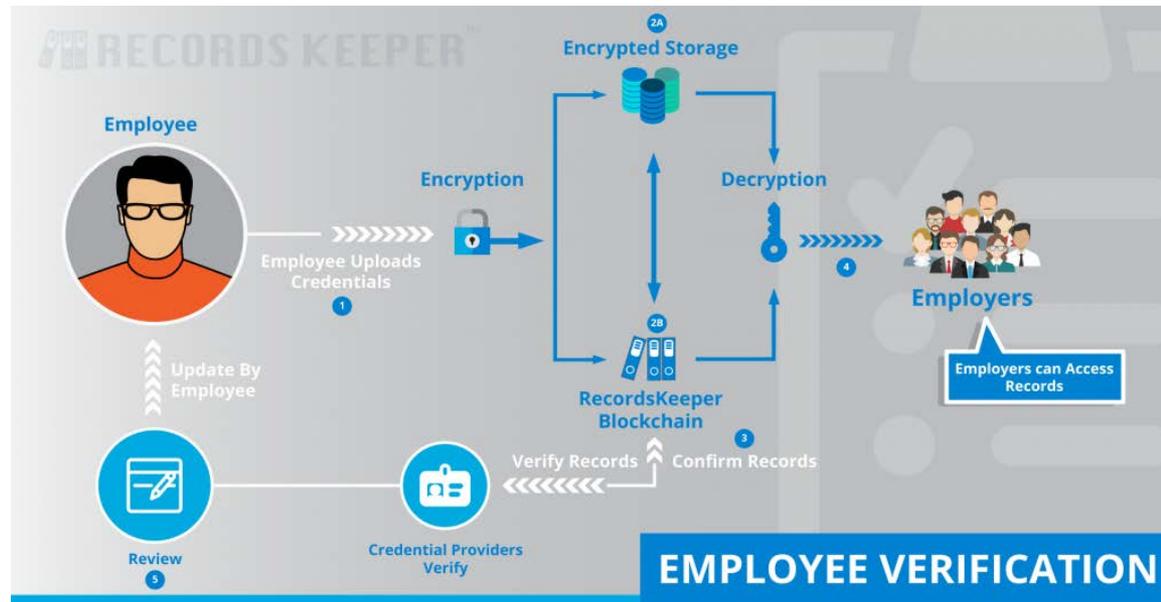
## Medical Economics



# Blockchain Solution to Credentialing



- Medical staff credentialing can be a costly and time-consuming effort that conducted via phone calls, faxes, and snail mail.
  - Because blockchains can be verified and updated incrementally, the technology may be well suited for the credentialing process.
- Another possible blockchain application is a credentialing “smart contract,” an agreement to participate in a “living” credentialing database specifically designed to use blockchain technology as its infrastructure.
  - The concept is that a practitioner’s credentialing information would be continually updated within a single database, with both inputs and access provided by those who have entered into a Blockchain Credentialing Process Agreement.



Medical Economics

Records Keeper



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS  
**HHS CYBERSECURITY PROGRAM**  
OFFICE OF INFORMATION SECURITY

TLP: WHITE, ID# 201909121000

12

# Blockchain solution to Electronic Health Records

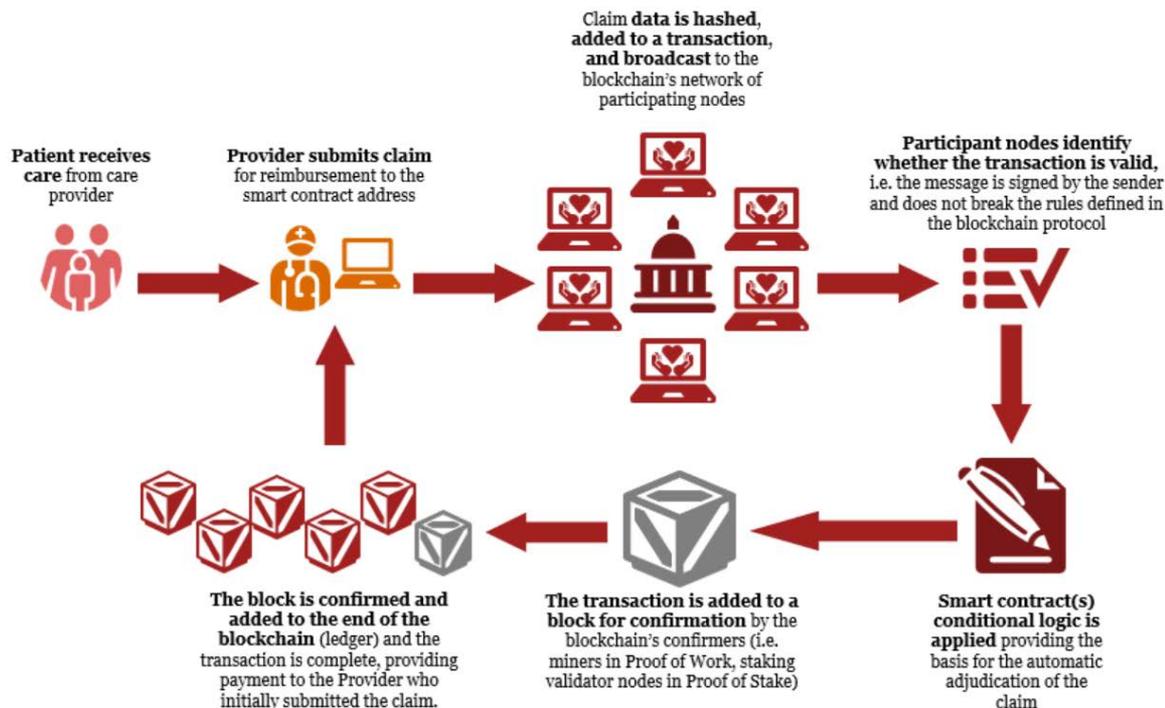


- Patient data is scattered across different entities in the value chain of the healthcare industry referred to as data silos and sharing of data is prone to a multi-level process of permission control.

- Blockchain can solve this issue with health information exchange (HIE) by serving as a basis for a trusted decentralized database. ([ARXIV](#))

- Blockchain updates every piece of EHR information on an open-source, community-wide trusted ledger, so audits can be transparent and understood by all participants.

- With blockchain, the EHR reconciles community information, with integrity from the point of data generation to the point of usage (diagnosis, prescription or research), without any human intervention.



[Academy Health](#)

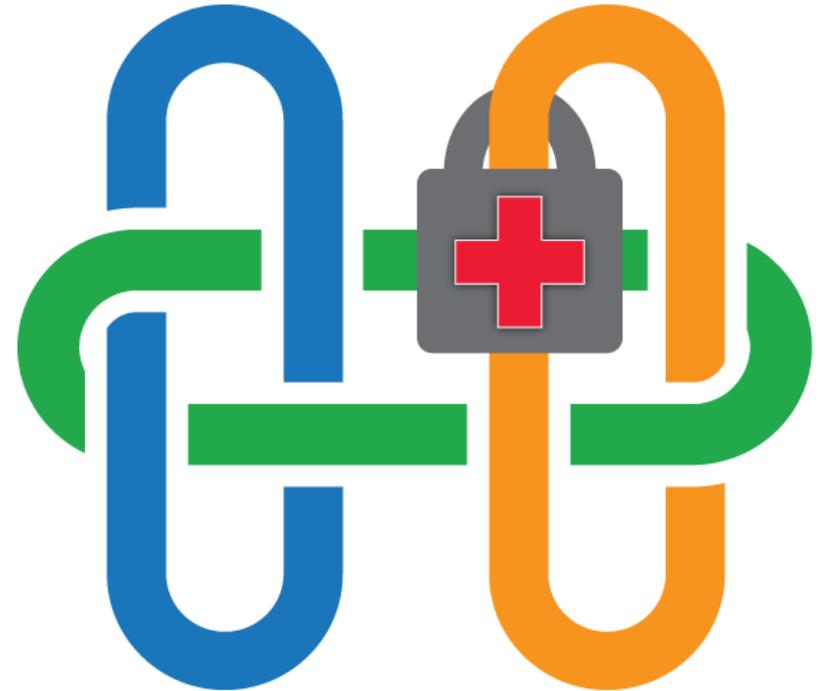
## Medical Economics





- **Interoperability & integration with the legacy systems** Healthcare space has a vast number of technologies, devices, and components, not forgetting the personnel, which all come together to solve the current needs in the space. There are large rooms for improvements, with blockchain technology providing a promise to cover up some of this room.
  - The blockchain technology has to integrate well with existing systems, and the integration is going to be a challenging ordeal because of several reasons such as interoperability.
- **Uncertain cost of operation** While blockchain has promising features such as no need of central authority (and hence no central point of failure), transparency and relatively fast settlement of transactions, the cost of operating blockchain systems are not yet known.

## Blockchain Challenge



[CCC Innovation Center](#)

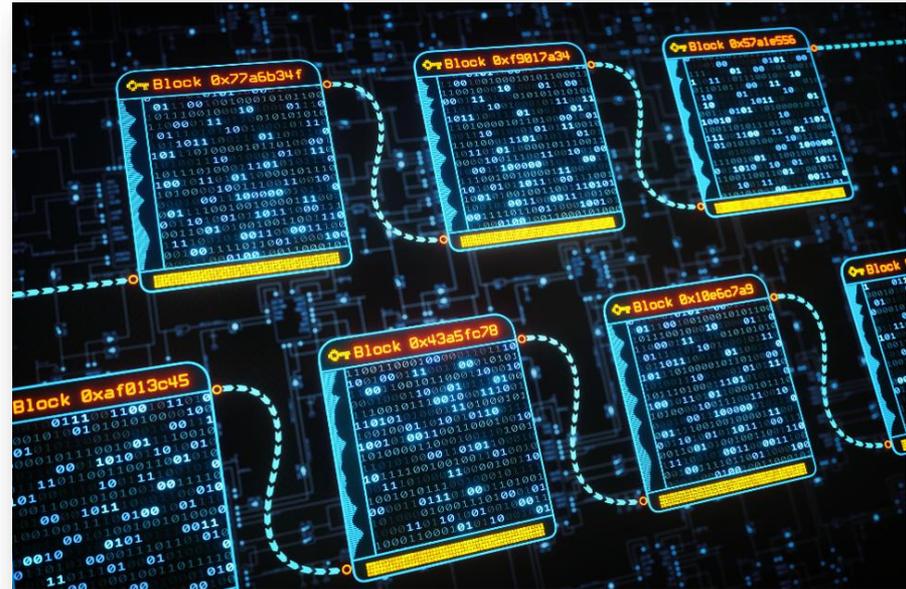
[ARXIV](#)



# Challenges with Blockchain



- **Governance** In certain operational models of blockchain based solutions, it might be imperative to have a certain stakeholder assuming the role of a regulator to govern the overall operation of the blockchain.
- **Scaling** Not only in healthcare but any industry, the underlying blockchain network has to be scalable for successful application of any blockchain-based solutions.
  - Likely in the early phases, several solutions in healthcare will use semi-permissioned blockchains which are scalable and have high transaction throughput at the cost of decentralization.



Forbes



# Reference Materials

# References



- Abcd
  - Abcdefg.com





**Questions**



## Upcoming Briefs

- Misconfiguration Errors
- Sodinokibi/Revil
- Data Breachs 2019



## Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to [HC3@HHS.GOV](mailto:HC3@HHS.GOV).

## Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to [HC3@HHS.GOV](mailto:HC3@HHS.GOV) or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110**.





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

## Products



### Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently 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 document and presentation that provides 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](mailto:HC3@HHS.GOV) or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.



# Contact



**Health Sector Cybersecurity  
Coordination Center (HC3)**



**(202) 691-2110**



**HC3@HHS.GOV**