Blockchain 101

Trends – Applications - Challenges

Mauricio Angée, CISSP

Mount Sinai Medical Center, CISO

March 2019

Disclaimer:

The information provided in this presentation does not represent the opinions of Mount Sinai medical center. This material, views and opinions expressed in this presentation are solely those of the presenter(s) for general information purposes only.

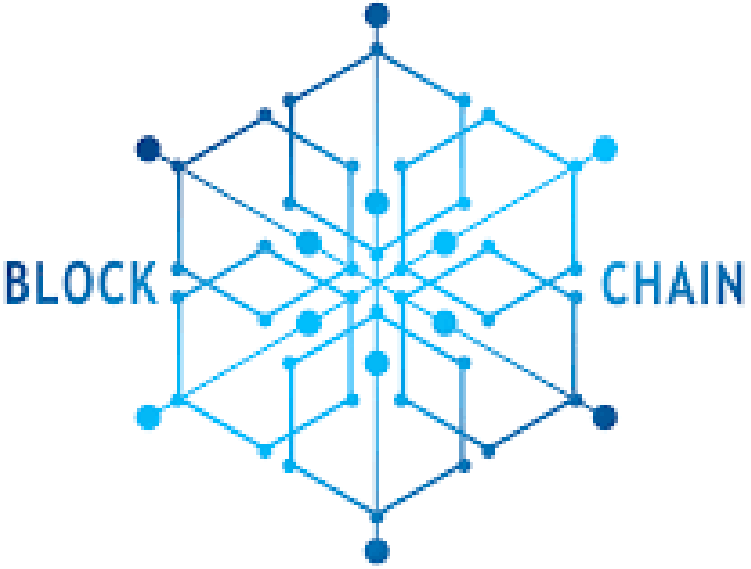
Introduction

- Thought leader, Certified Information Systems Security Professional (CISSP) with over 30 years of experience in healthcare, banking and financial services, hospitality, entertainment, and the government sector.
- Expertise in cybersecurity, information assurance, privacy, regulatory compliance, and risk management.
- Serves in the Board of Directors at Infragard (FBI public-private information sharing group) and the South Florida CISO Council.

- **Professional Experience**:
  - CISO at Mount Sinai Medical Center
  - VP Information Security at Mercantil Bank
  - Sr. Manager Security and Compliance / CISO at Universal Studios Florida
  - ISSO at Harris Corporation - supporting **FAA** and **Census Bureau**
  - CSO at **NASA's Kennedy Space Center**
- **Education**
  - Executive Doctorate of BA in Information Security – STU (Class of 2019)
  - MS Information Security - NSU
  - BS Information Studies - FSU
- Keynote speaker in local, national and international forums. Featured on CNN (Español).
- Adjunct faculty at Florida International University and St. Thomas University.

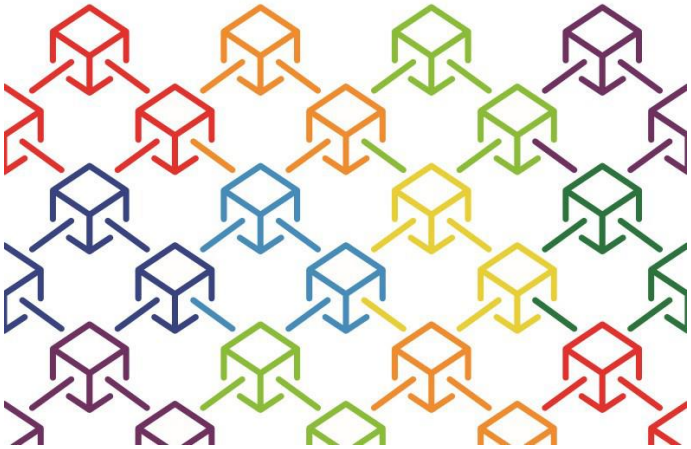
Agenda

- Overview
- What is Blockchain (Blockchain 101)
- Blockchain Applications
- Blockchain in Healthcare
- Challenges
- Summary



Overview

- The concept of “Block and Chains” was originally published by Heber and Stornetta in 1991. Its original purpose, a “Digital Documents Timestamp” impossible to modify or tamper with.
- Block and chain technology was first introduced in a whitepaper entitled: “Bitcoin: A Peer-to-Peer Electronic Cash System,” by ***Satoshi Nakamoto*** in 2008.
- The term *block and chain* was later changed to what we know today as “Blockchain.”
- By design and by purpose blockchains are inherently resistant to modification of the data (preservation of integrity.)

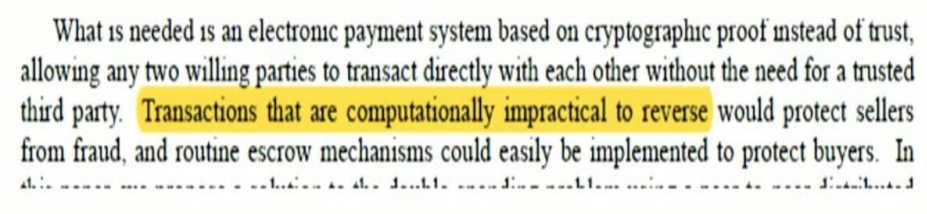


The Pillars of Blockchain

The Three Pillars of Blockchain Technology

The three main properties of the Blockchain Technology which has helped it gain widespread acclaim are as follows:

- Immutability — In the context of the blockchain, means that once something has been entered into the blockchain, it cannot be tampered with.
- Decentralization — Storing data across peer-to-peer networks. Once verified, the informatio is copied to every node.
- Transparency — Trusted third-party - there is absolute transparency as every node has a copy of the ledger.



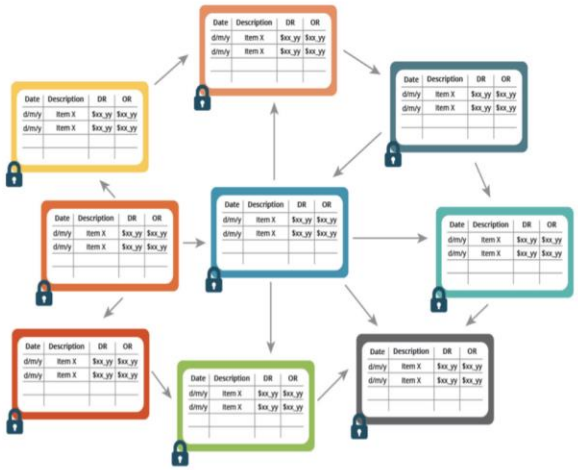
What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In

Satoshi Nakamoto

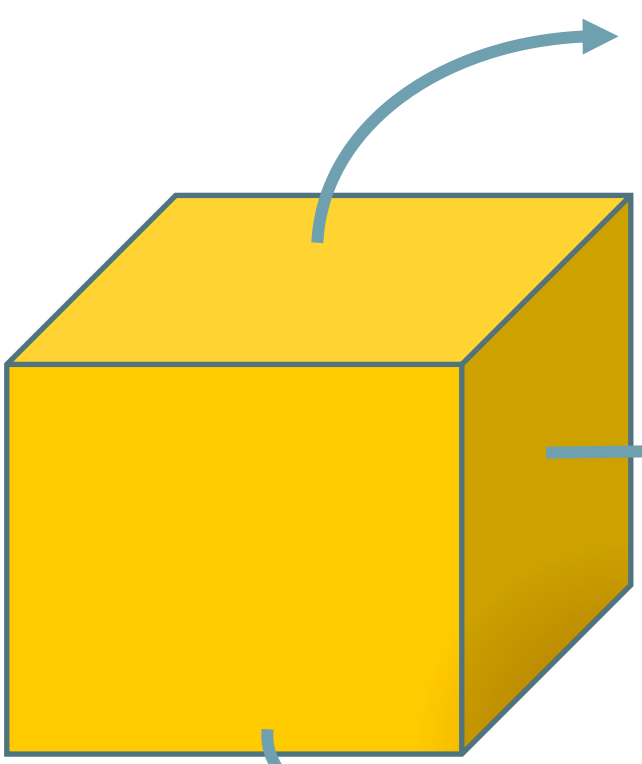
What is Blockchain?

What is Blockchain?

- A blockchain is a digital ledger, a growing list of records, in which all transactions are recorded chronologically and openly.
- A blockchain is a decentralized, distributed database that is used to maintain a continuously growing list of records, called blocks.
- Each block contains a timestamp and a link to a previous block.
- In its simplest form, a distributed ledger is a database held and updated independently by each participant (or node) in a large network.
- Once there is this consensus, the distributed ledger has been updated, and all nodes maintain their own identical copy of the ledger.
- This architecture allows for a new set of applications as a system of record that goes beyond being a simple database.



What's A Block?



Data

Cryptographic (HASH)

Digital Fingerprint

e2c521bc53bb5db4fc0aa497da2ba5d4c8444db3

HASH of previous Block

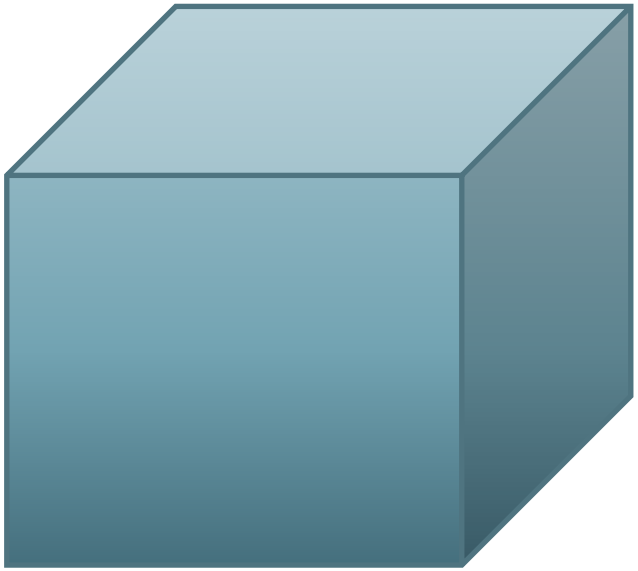
What's A Cryptographic HASH?

A "Cryptographic Hash" is a Long Random String of Numbers,

A Unique Signature

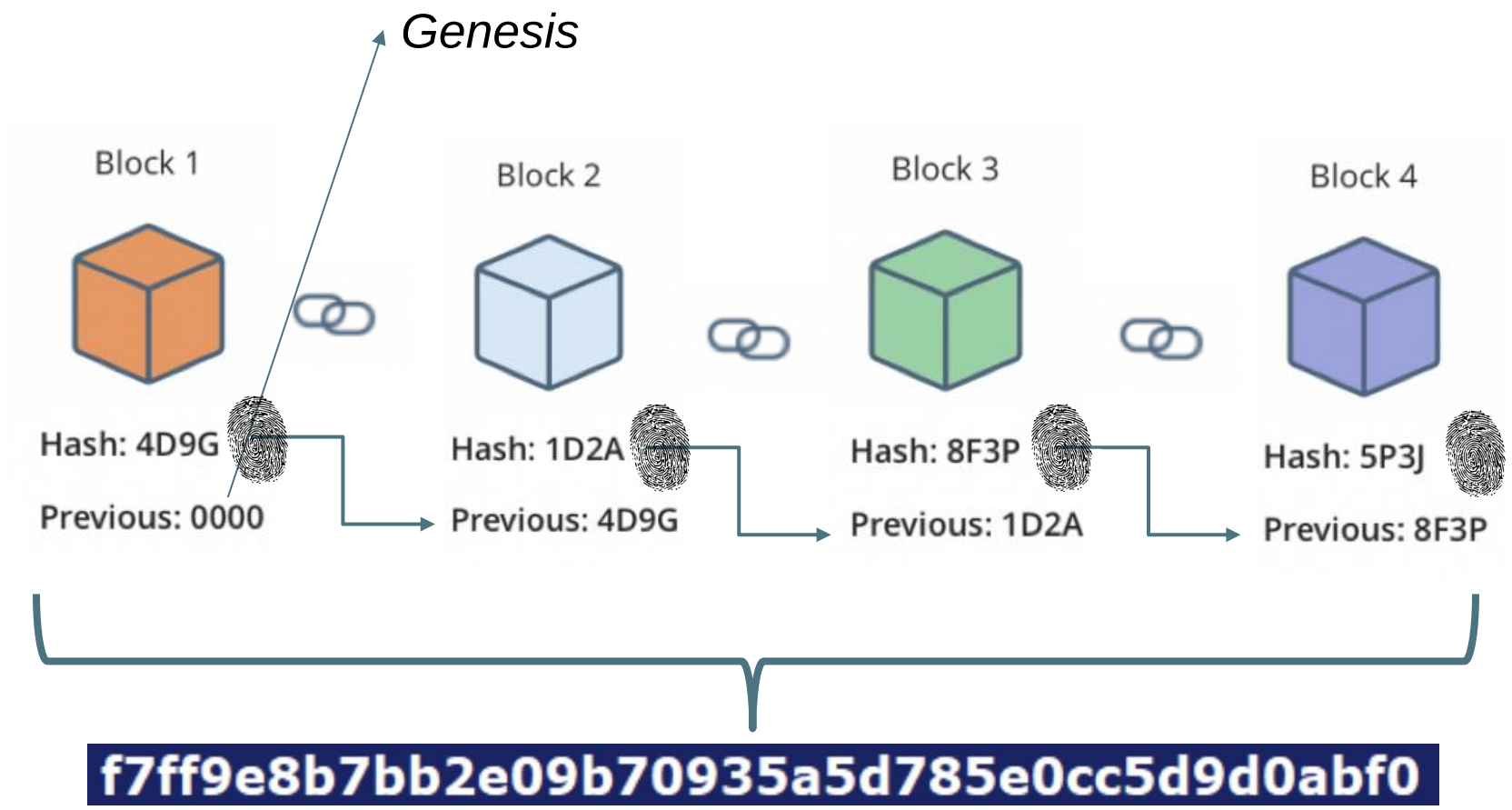
Input	Hash Function	HASH Value
Passphrase "Password1234"	**Cryptographic Key**	DFCD3454 BBEA788A 751A696C 24D97009 CA992D17

What’s in the Block?



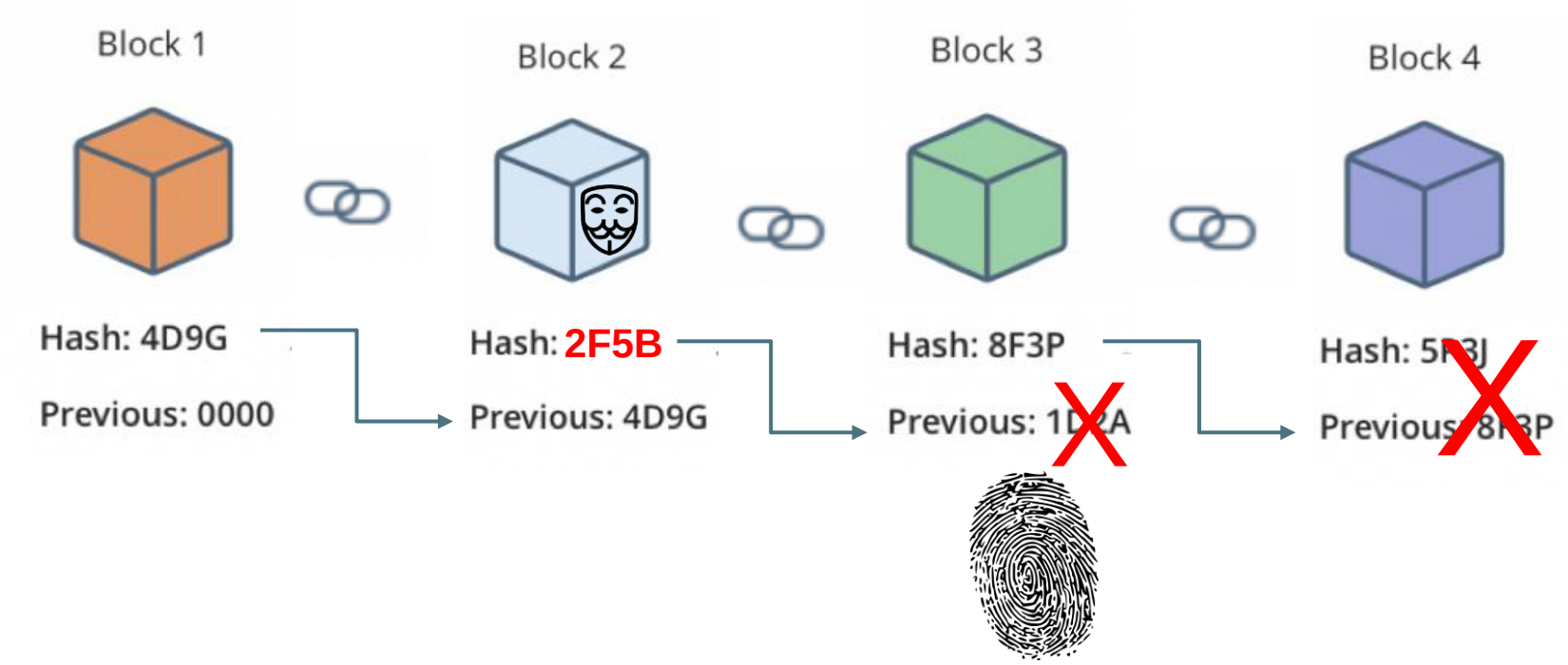
- Version (identifies the format of Blocks)
- HASH of previous Block
- HASH of the root of transaction (data structure)
- Timestamp
- Bits (data, i.e. transaction)
- Block HASH Validation (True)
- New HASH
- Link

What is Blockchain?



Cryptographic Signature (HASH)

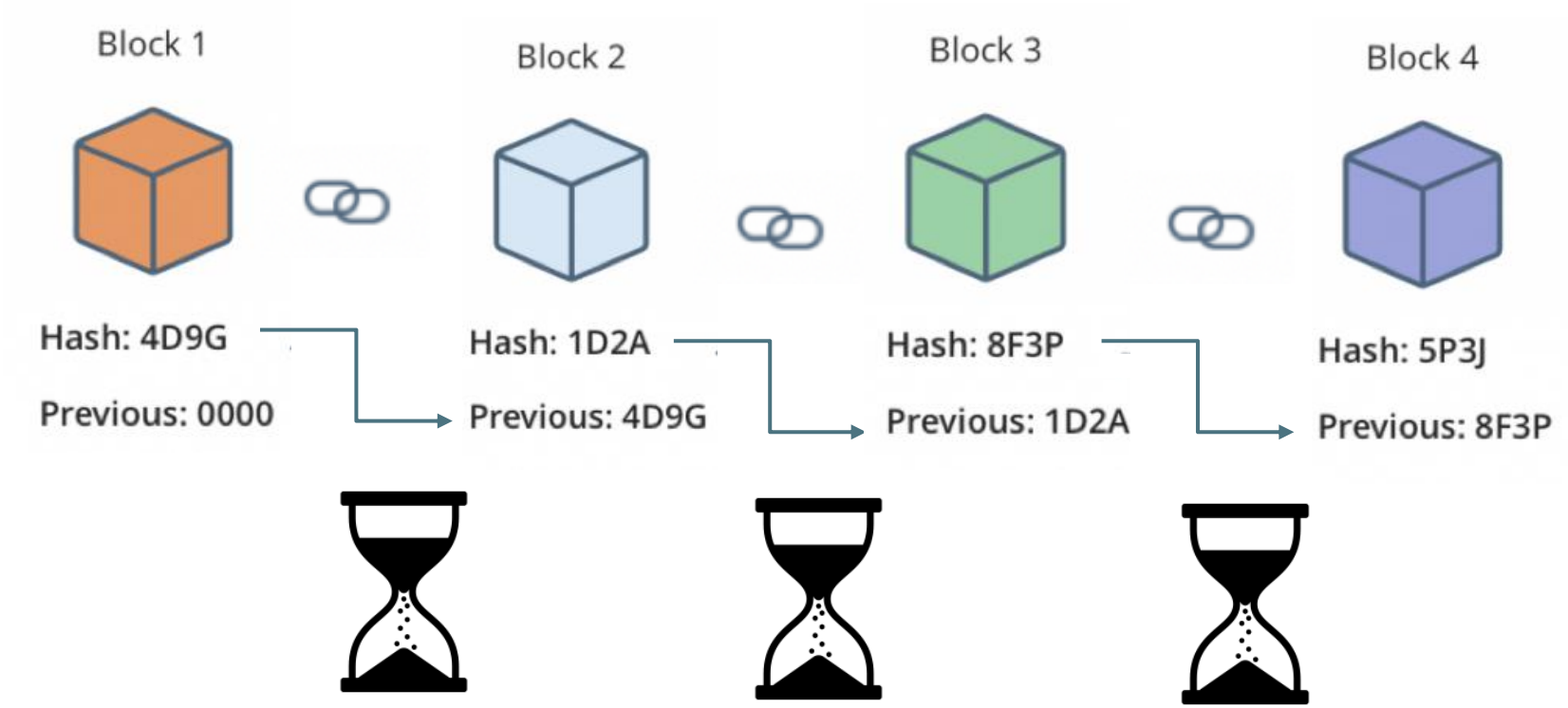
Tempering with the Blockchain



If The “Fingerprint” changes – it is no no longer valid

Proof-of-Work Mechanism

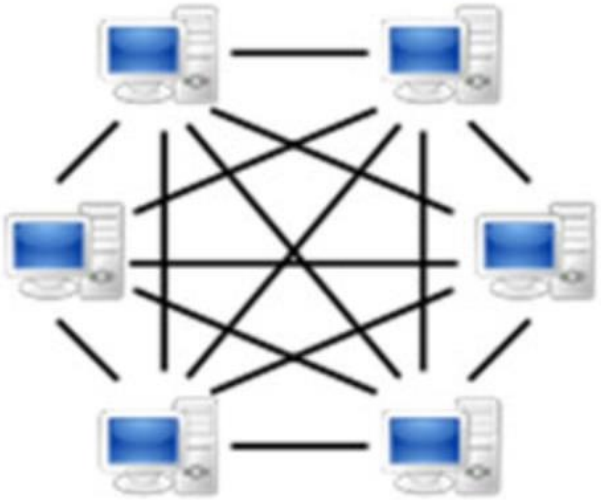
Operations are validated by “Crypto Miners” and take about 10 min on average to validate



This operation is called “Proof-of-Work (PoW)

Distributed Networks

No Centralized Management Entity



Peer-2-Peer Networks

All “Peers” share a copy of the ledger

Crypto Mining

- Cryptocurrency mining includes two functions, namely: adding transactions to the blockchain (securing and verifying) and also releasing new currency. Individual blocks added by miners should contain a proof-of-work, or PoW.
- Mining needs a computer and a special program, which helps miners compete with their peers in solving complicated mathematical problems. This would need huge computer resources.
- In regular intervals, miners would attempt to solve a block having the transaction data using cryptographic hash functions.
- In the case of gold mining, electricity is just one of many resources in a process which has a lot of constraints which result in nonrenewable resources being used such as coal and oil which have far reaching environmental repercussions.

Crypto Mining Facilities

What is Digital Wallet?

- A “Crypto Wallet” is an application that stores the public and private keys which can be used to receive or spend a cryptocurrency.
- Digital or crypto wallets can be desktop application, a mobile app, hardware tokens.
- Most commercially available crypto wallets are:
  - Bread wallet (Mobile Bitcoin Digital)
  - Mycelium (Mobile Multiple Crypto Currencies)
  - Ledger Nanos (Hardware Token)
  - Jaxx (Desktop Wallet – Good to manage Digital Assets)
  - Coin Payments (Online Wallets – over 1200 Crypto Currencies)

Roadmap and Applications

- Blockchain Technology “Will Affect Our Future”
- Applications of “Blockchain” go beyond Bitcoin systems:
  - Personal Identification
  - Legal Contracts Signatures
  - Healthcare
  - Supply Chain
  - Cross-Border Payments
  - Internet-of-Things (IoT)
  - Music and Video Industries
  - Government (Digital Personal Identities) – Government IDs, Passports, Birth, Wedding, and Death Certificates

Challenges

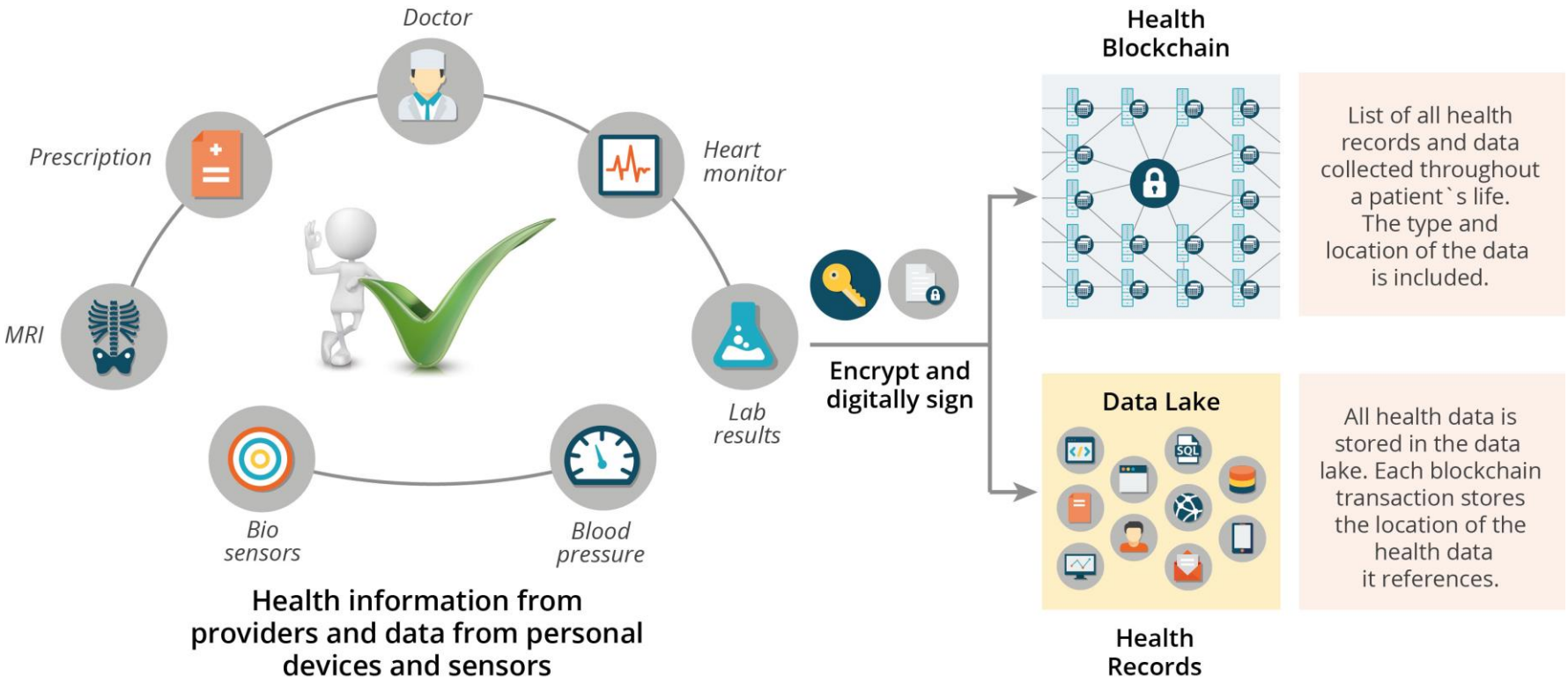
- **Regulatory and legal acceptance**: Blockchains have no legal framework. There is no single ownership, so a legal framework on territoriality for issues like jurisdiction and the applicable law needs to be there. This is important as each network node may be in a different geography with a different legal law or enforcement.
- **Central administrator for blockchains**: Today there is no central administration or administrating body responsible for the distributed ledger. This may lead to a concern that there is no person, party, group, or organization eventually responsible for the functioning of distributed ledgers and the information contained within.
- **Validity of the information stored**: There is a need for a legal deed declaration of ownership of the existence of an asset on the node or of the information with a genuine backing of the proof of ownership or existence of the said asset.
- **Standardization**: Standards are required to facilitate the interoperability between blockchains. This will also enable security and compliance for enterprises to interact and share solutions and transactions.

Blockchain in Healthcare

- Healthcare data is distributed and highly fragmented
- Peoples' Identities and personal Information is spread across diverse ecosystems:
  - Healthcare Providers
  - Hospitals
  - Insurance Companies
  - Healthcare Systems
  - Billing Companies

- Blockchain in healthcare can address a variety of problems, such as care coordination, data security, and interoperability issues.
- Significant challenges exist to blockchain adoption in healthcare, such as technical challenges and question of ownership.

Blockchain in Healthcare



Concerns

Blockchain may address a threat that is rapidly approaching: integrity-based attacks. In these attacks, malicious insiders or external actors modify data -- such as by adding or removing drug allergy information -- in such a way that is not trackable, leading to major patient safety and institutional trust concerns.

- Challenges with Blockchain include:
  - Fundamental blockchain-related changes to how we store health data may, in the future, address some of these challenges, but that is still quite a ways off.
  - The problems that cybersecurity has within the realm of blockchain and cryptocurrencies are two-fold. One is with the effectiveness of third-party users in providing this same level of security over their products.
  - Recent events have shown that while the number of cryptocurrency wallets and exchanges is increasing over time. The level of security they provide is wanting when because over the years, millions of dollars in different cryptocurrencies have been stolen.
  - In a single-ledger model, anyone who treats patients becomes a new and dangerous threat vector from a privacy and security standpoint. Everyone has the keys to the kingdom.

Open Source Blockchain

Hyperledger is a multi-project open source collaborative effort hosted by The Linux Foundation, created to advance cross-industry blockchain technologies.

Eris - A dependable on the Blockchain or any smart contract technology that you use. A government can use these smart contracts to do business with Eris automatically.

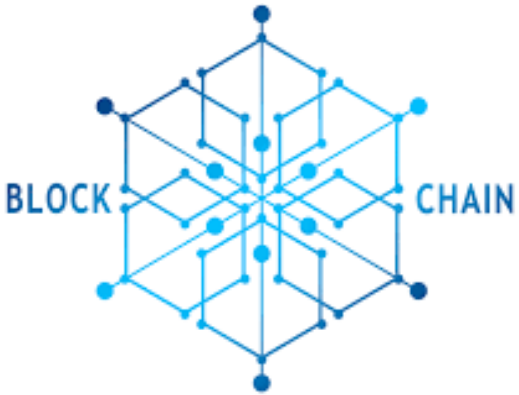
OpenChain - An open source distributed ledger technology which stands alone. It is mainly suited for companies which are interested in managing their digital assets in a robust and flexible manner.

IBM Blockchain Platform Targets Banks and Financial Institutions.

IBM also published a fully interoperable Blockchain platform for **Hyperledger**

Summary

- Blockchain is a simple concept to understand.
- Blockchain presents opportunities which can be applied in many industries.
- Challenges with legal issues, platform standardization and digital identities.
- Blockchain Cybersecurity issues are still not fully explored and many solutions that are being deployed may pose privacy and security concerns.



Research

- Researches have published articles on Blockchain including:
  - Blockchain Technology: Applications in Health Care Suveen Angraal, Harlan M. Krumholz, and Wade L. Schulz (2017)
  - Deloitte (2017) Blockchain risk management Risk functions need to play an active role in shaping blockchain strategy.
  - Devon, Connor-Green (2017). Blockchain in Healthcare Data. 21 Prop. & Tech. L. J. 93
  - Hölbl, M., Kompara, M., Kamišalić, A., & Zlatolas, L. N. (2018). A systematic review of the use of blockchain in healthcare. *Symmetry*, *10*(10).
  - Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf. Accessed January 15, 2017.Google Scholar
  - Pirtle, C., & Ehrenfeld, J. (2018). Blockchain for Healthcare: The Next Generation of Medical Records? *Journal of Medical Systems*, *42*(9), 1–3.

Questions?