Krishna University

(Established Under A.P. Govt. Act No. 28 of 2008)
Machilipatnam-521004, Andhra Pradesh, India.

Blockchain an overview and research perspective

By

Dr. V. Srinivasa Naresh
Dean (R&D)
Sri Vasavi Engineering College
Tadepalligudem
Andhra Pradesh

Blockchain Technology

- Technologists and investors are buzzing about the potential for Blockchain technology to revolutionize everything.

- Blockchain is a peer-to-peer (P2P) distributed ledger technology for a new generation of applications that establishes transparency and trust.

- Blockchain consists of three main components: a distributed network, a shared ledger and digital transactions.

- The funding backdrop is healthy and the eco-system is growing.

- Once considered the technology behind Bitcoin, this technology has taken center stage from its crypto-currency roots.

- Blockchain is a means of recording and verifying data in a tamper and revision-proof way that is public to all.

Blockchain Technology

Distributed Network

- Blockchain is a decentralized P2P architecture with nodes consisting of network participants.
- Each member in the network stores an identical copy of the blockchain and contributes to the collective process of validating and certifying digital transactions for the network.

Shared Ledger

- Members in the distributed network record digital transactions into a shared ledger.
- To add transactions, members in the network run algorithms to evaluate and verify the proposed transaction.
- If a majority of the members in the network agree that the transaction is valid, the new transaction is added to the shared ledger.

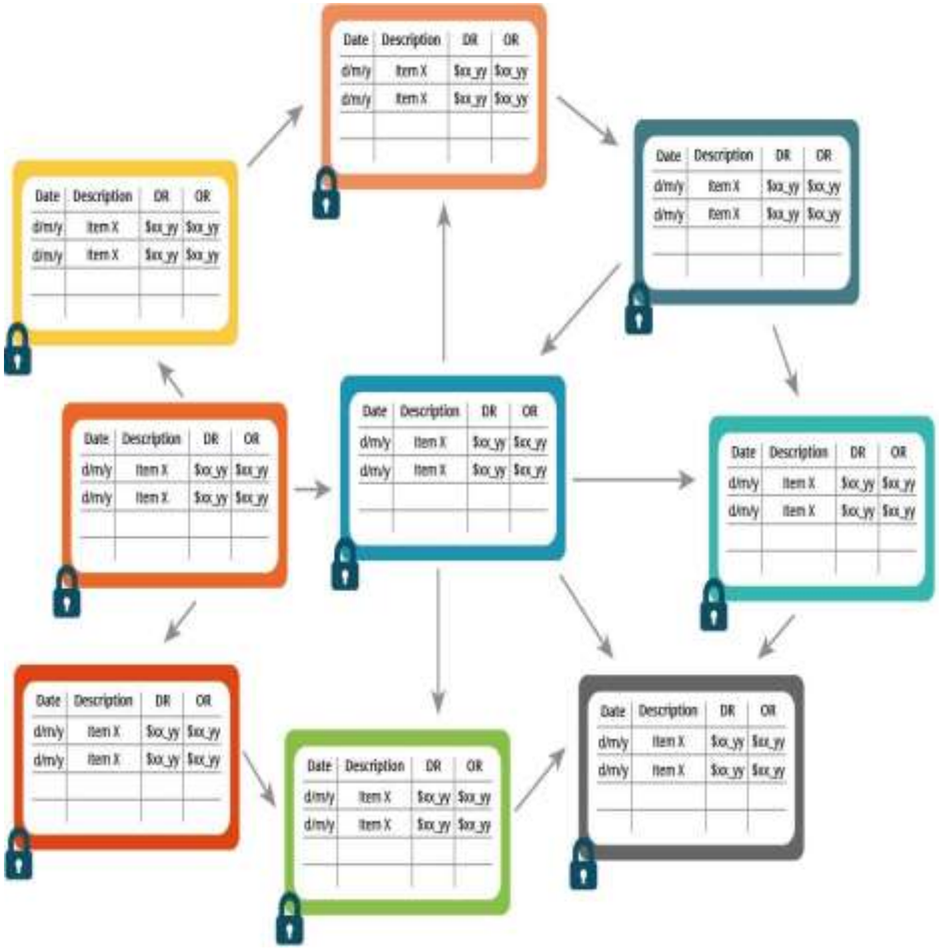
Blockchain Technology

- Changes to the shared ledger are reflected in all copies of the blockchain in minutes or, in some cases, seconds.
- After a transaction is added it is immutable and cannot be changed or removed.
- Since all members in the network have a complete copy of the blockchain no single member has the power to tamper or alter data.

Digital Transactions

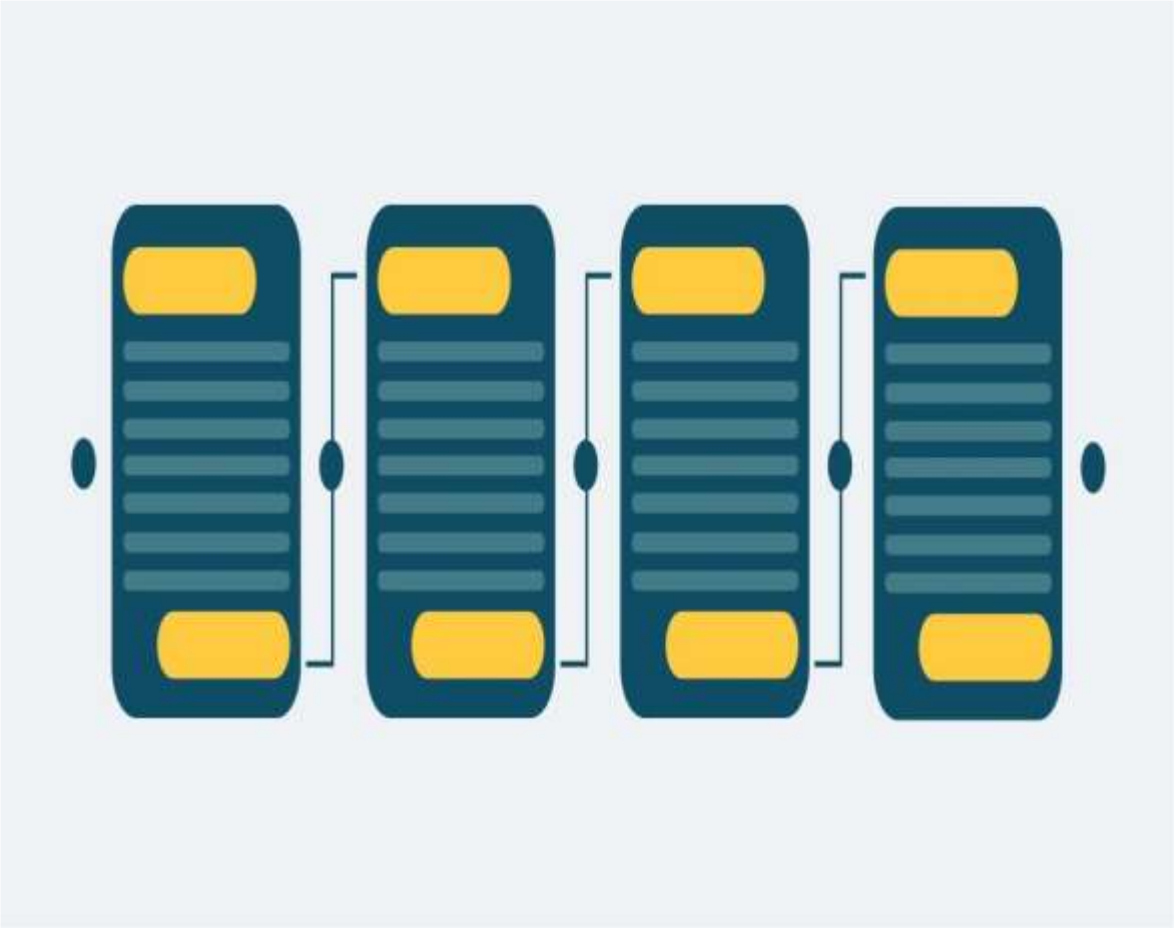
- Any type of information or digital asset can be stored in a blockchain, and the network implementing the blockchain defines the type of information contained in the transaction.
- Information is encrypted and digitally signed to guarantee authenticity and accuracy.
- Transactions are structured into blocks and each block contains a cryptographic hash to the prior block in the blockchain. Blocks are added in a linear, chronological order.

Blockchain Technology



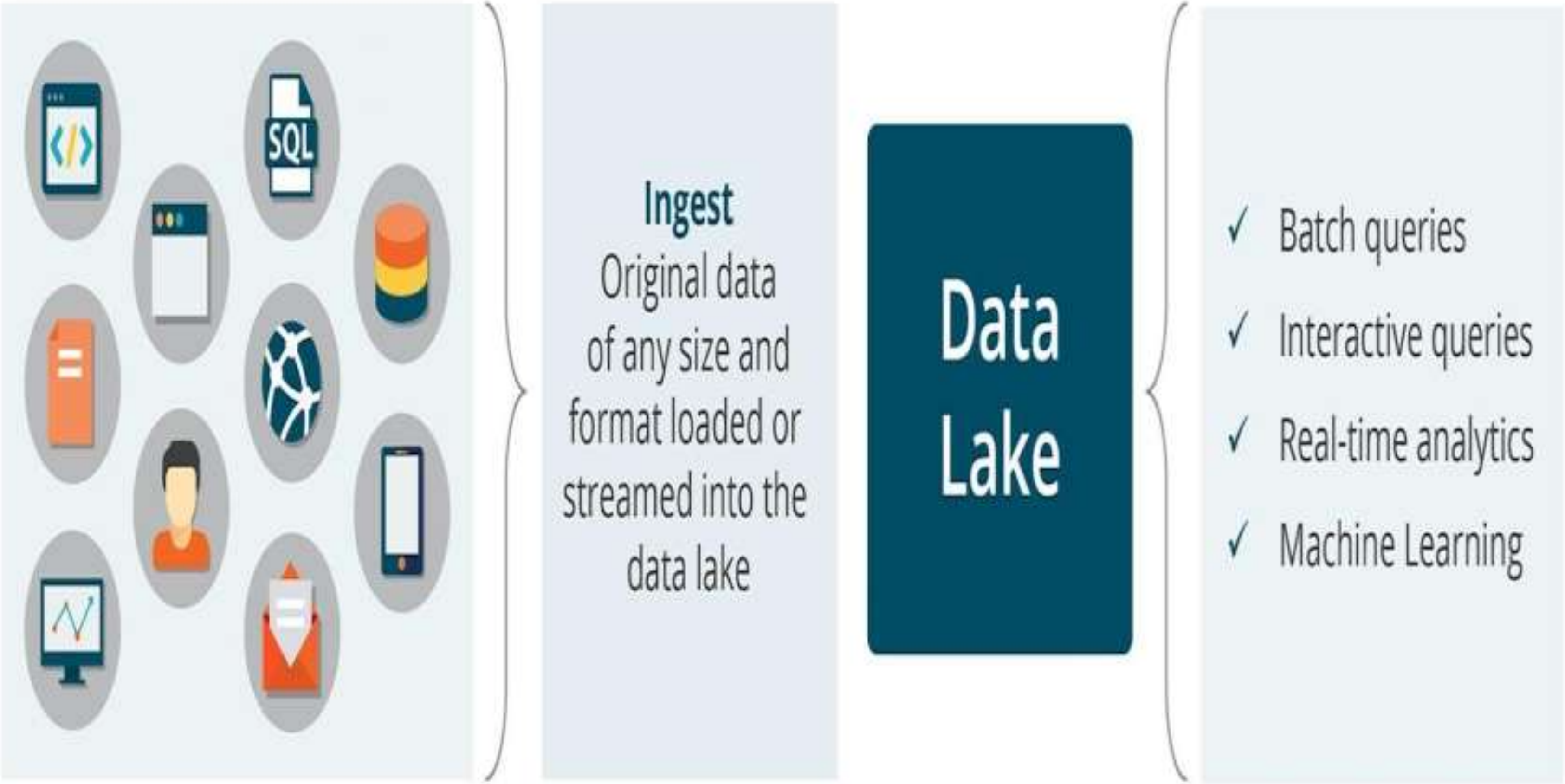
Blockchain is a decentralized P2P architecture. Members in the distributed network record digital transactions into a shared ledger. Each member stores an identical copy of the shared ledger and changes to the shared ledger are reflected in all copies.

Encryption



Transactons contain
encrypted and digitally
signed data along with
an index that points to the
prior block in the blockchain.
Transactions are structured
into blocks and recorded
in chronological order.

Data Lake

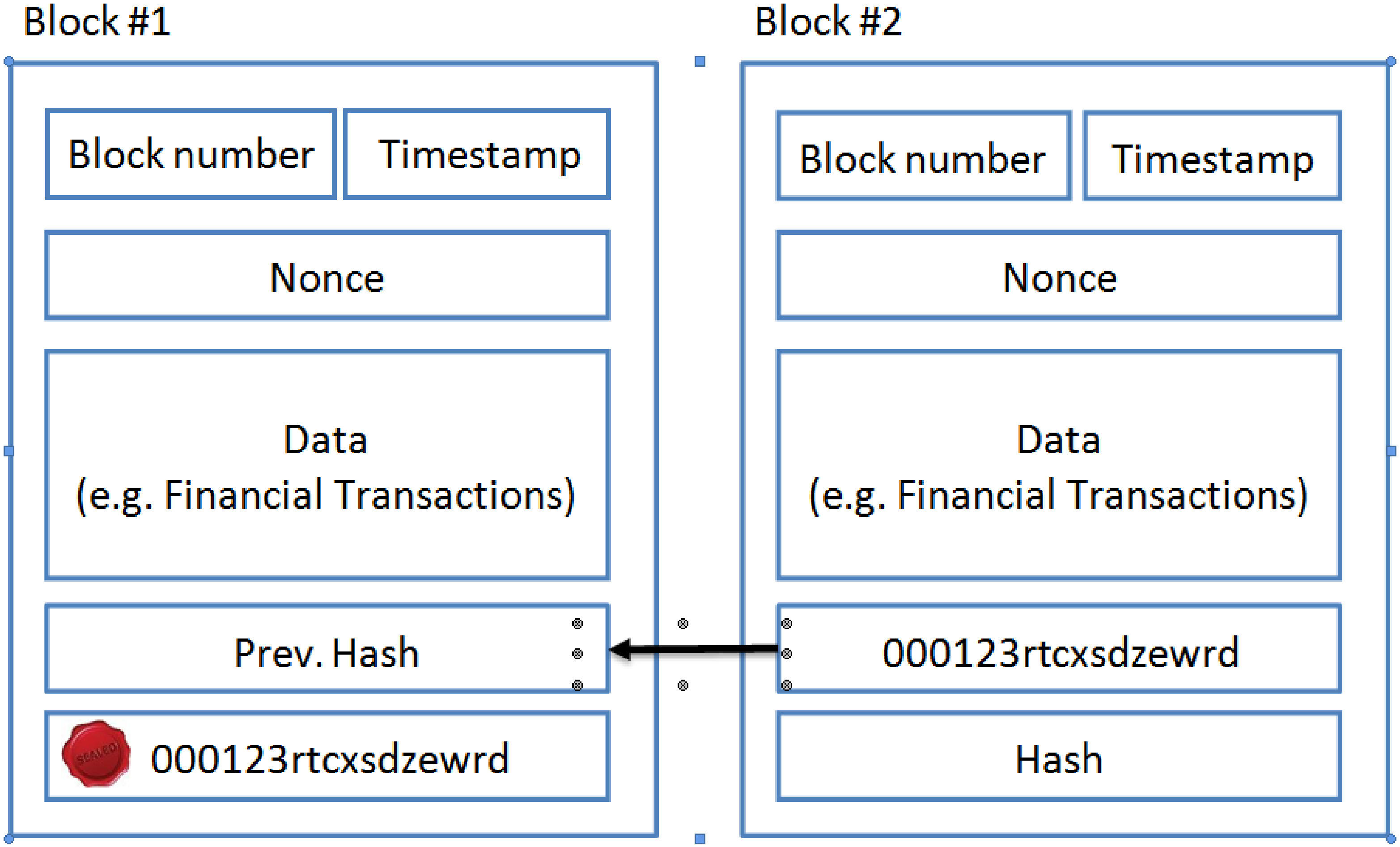


Ingest
Original data
of any size and
format loaded or
streamed into the
data lake

Data
Lake

- ✓ Batch queries
- ✓ Interactive queries
- ✓ Real-time analytics
- ✓ Machine Learning

Simple blockchain sketch



Block #1

Block number

Timestamp

Nonce

Data
(e.g. Financial Transactions)

Prev. Hash

000123rtcxsdzewrd

Block #2

Block number

Timestamp

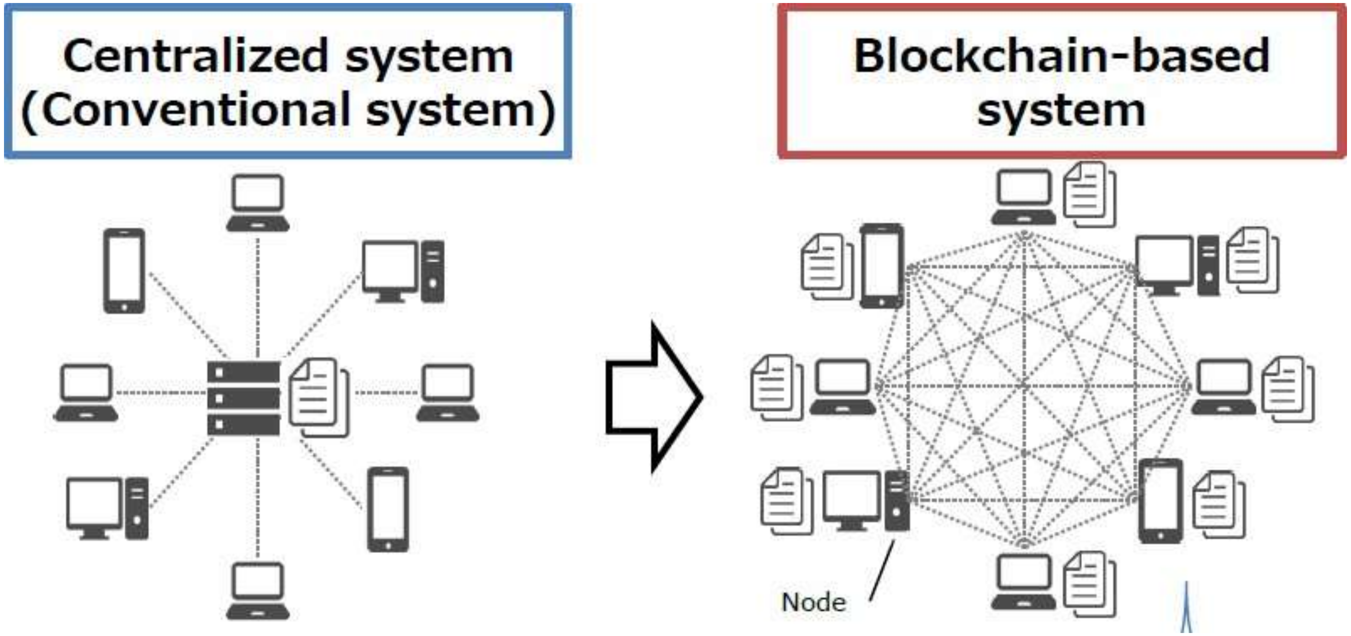
Nonce

Data
(e.g. Financial Transactions)

000123rtcxsdzewrd

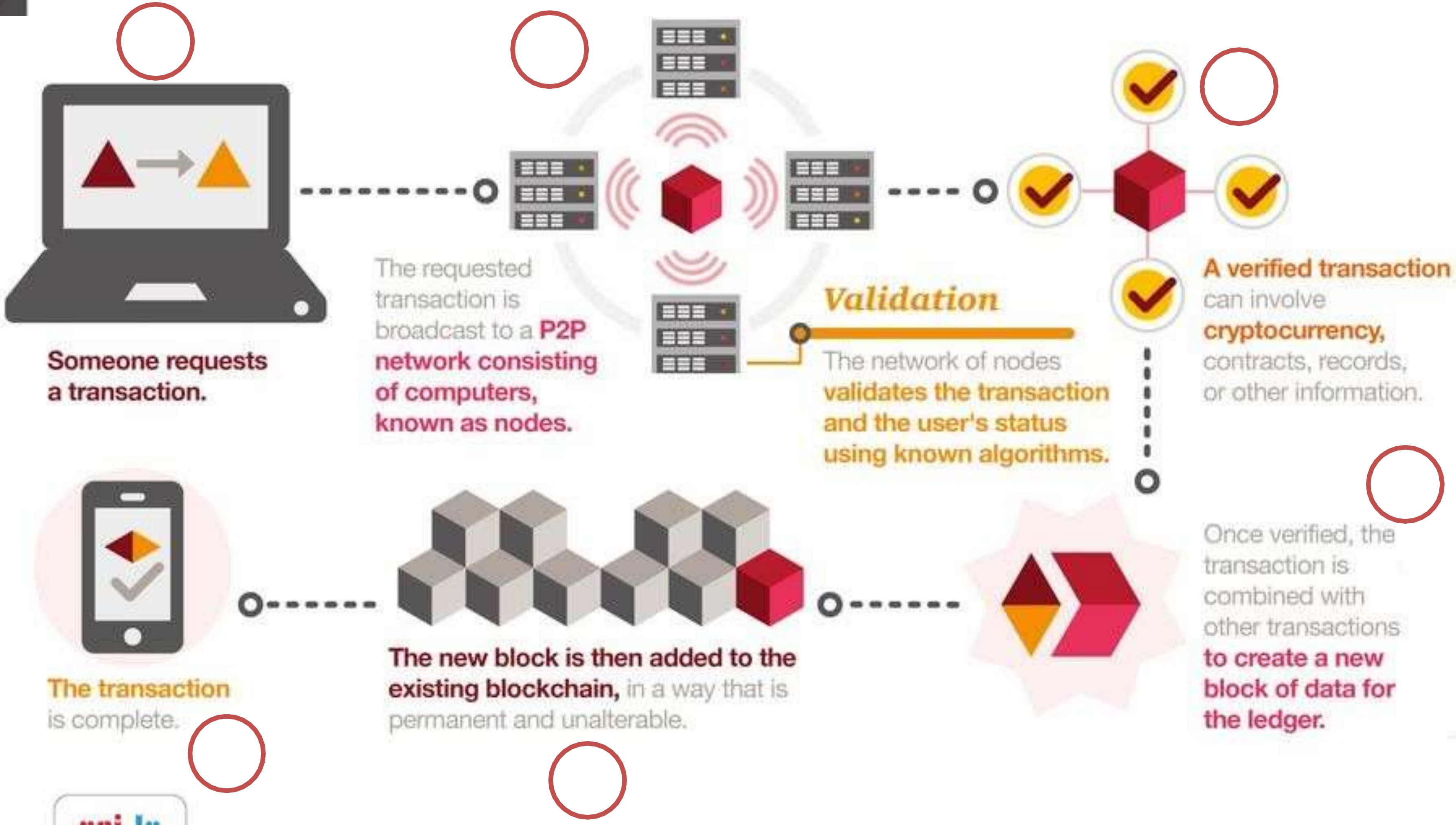
Hash

a **nonce** is an arbitrary number that may only be used once.



Centralized system (Conventional system)

Blockchain-based system



Someone requests a transaction.

The requested transaction is broadcast to a **P2P network consisting of computers, known as nodes.**

Validation

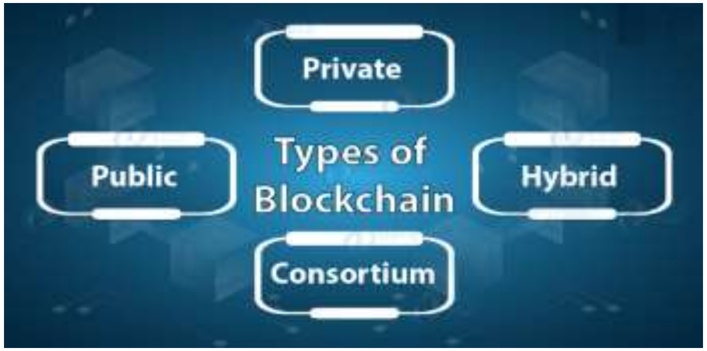
The network of nodes **validates the transaction and the user's status using known algorithms.**

A verified transaction can involve **cryptocurrency,** contracts, records, or other information.

Once verified, the transaction is combined with other transactions **to create a new block of data for the ledger.**

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

The transaction is complete.



A public blockchain is permission-less and unrestricted DLT that anyone can use this to be a part of the blockchain network as an authorized node. Some of the public blockchains are Bitcoin, Ethereum and Litecoin, etc.

A private blockchain is a permission or restricted DLT that can work only in a looped network. These are used within an enterprise or an organization where only selected members are participants in the network. The most common private blockchains are Hyperledger projects (Fabric, Sawtooth), Multichain, and Corda.

A consortium blockchain is a collaborative natured semi-decentralized DLT. In contrast to the private blockchain, it can be managed by group organizations similar in nature. Examples of consortium blockchain are; Energy Web Foundation, R3.

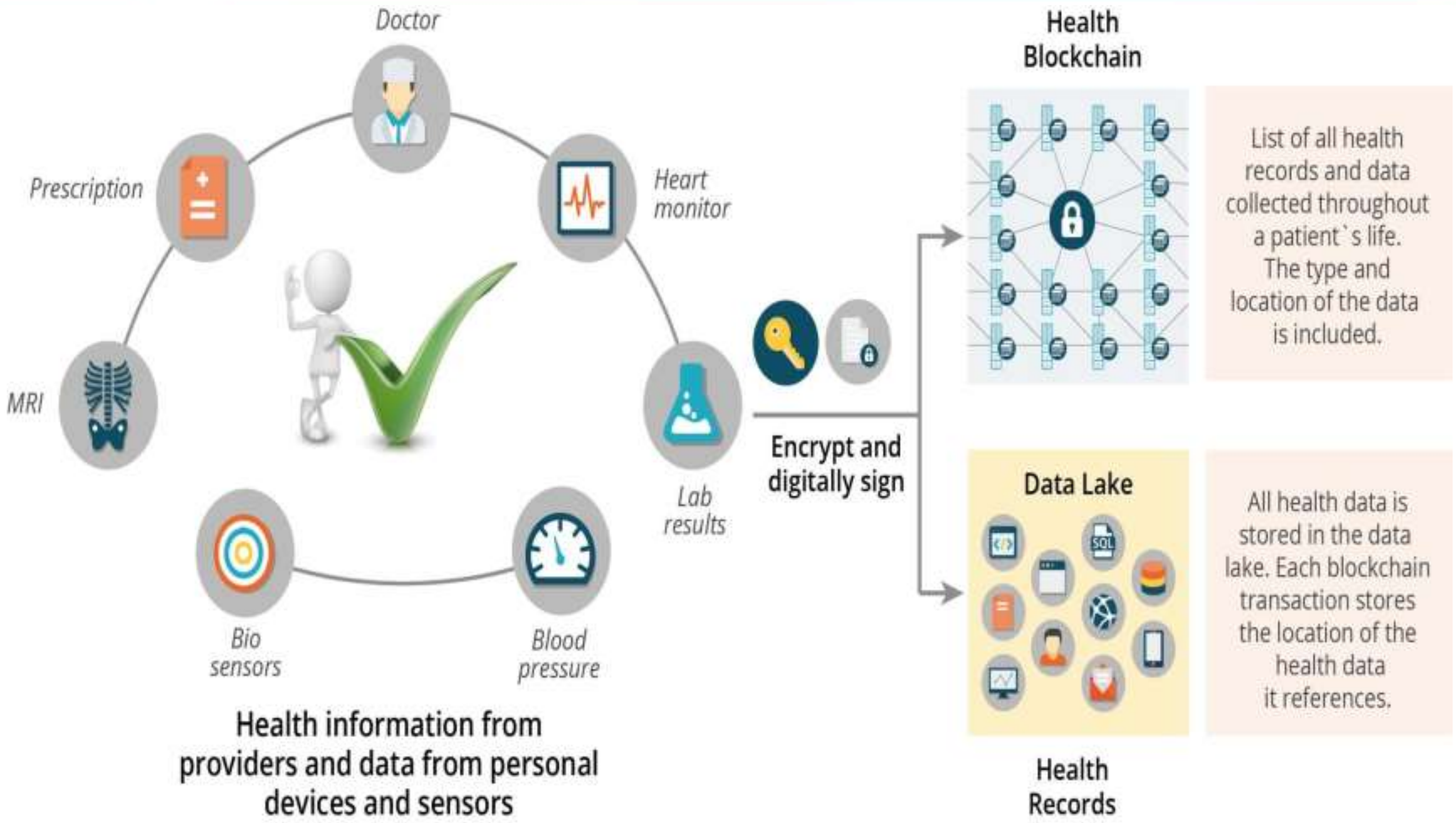
- **A hybrid blockchain** is a combination of the private and public blockchain. It uses the features of both types of blockchains that is one can have a private permission-based system as well as a public permission-less system. Only a selected section of data or records from the blockchain can be allowed to go public, keeping the rest as confidential in the private network. An example of a hybrid blockchain is Dragonchain.

- In thiswork, we adopted consortium blockchain because of its collaborative nature. It can work with multiple healthcare organizations such as hospitals, research institutes, insurance companies, Governments, and, Universities etc.

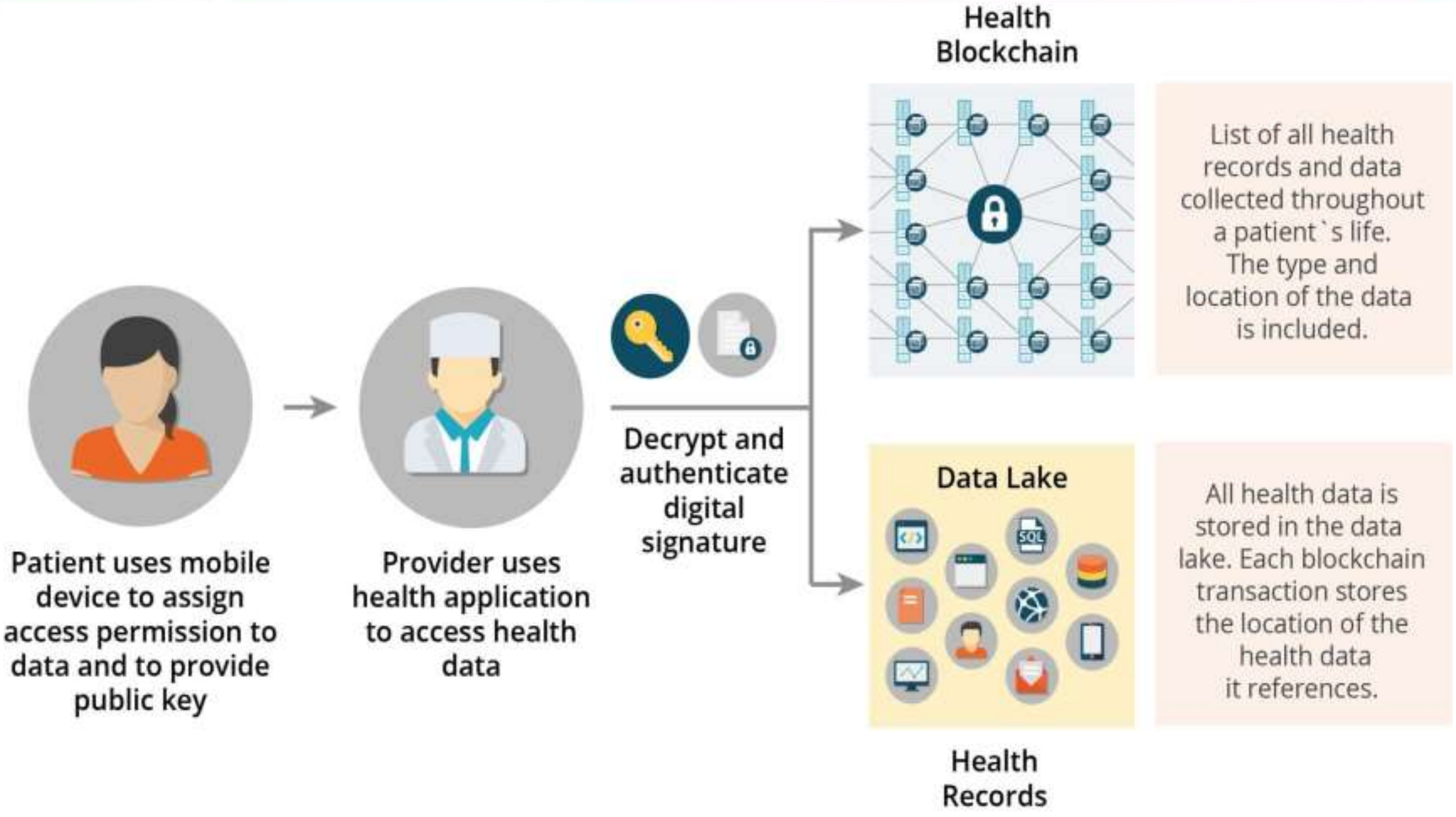
USE CASE: HEALTHCARE

Blockchain-Based Security, Privacy and Trust in in Healthcare

Health Care Blockchain


Doctor
Prescription
Heart monitor
MRI
Lab results
Bio sensors
Blood pressure
Health information from providers and data from personal devices and sensors
Encrypt and digitally sign
Health Blockchain
List of all health records and data collected throughout a patient`s life. The type and location of the data is included.
Data Lake
SQL
All health data is stored in the data lake. Each blockchain transaction stores the location of the health data it references.
Health Records

Health Care Blockchain



Patient uses mobile device to assign access permission to data and to provide public key

Provider uses health application to access health data

Decrypt and authenticate digital signature

Health Blockchain

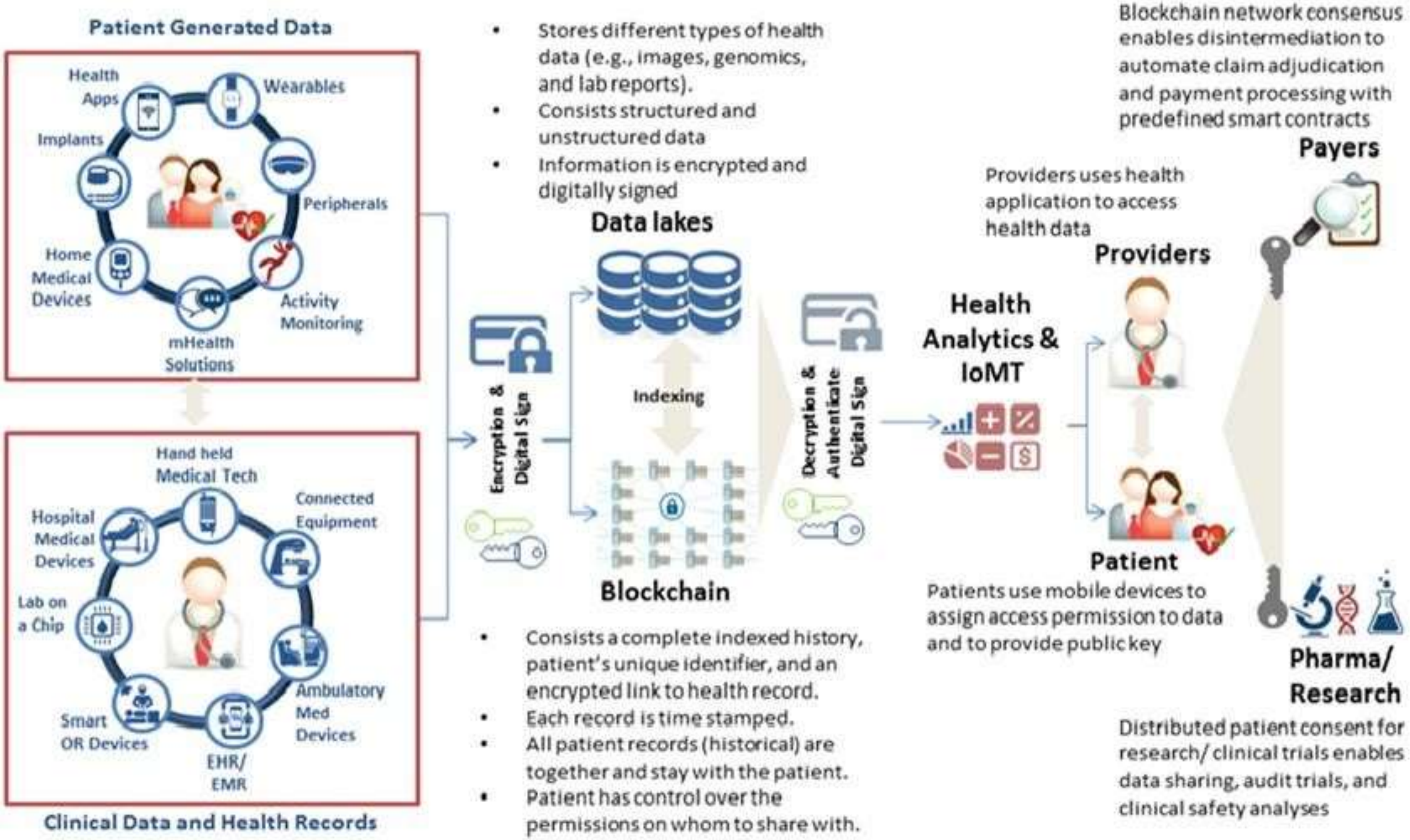
List of all health records and data collected throughout a patient`s life. The type and location of the data is included.

Data Lake

Health Records

All health data is stored in the data lake. Each blockchain transaction stores the location of the health data it references.

Health Care Blockchain



- Stores different types of health data (e.g., images, genomics, and lab reports).
- Consists structured and unstructured data
- Information is encrypted and digitally signed

- Consists a complete indexed history, patient's unique identifier, and an encrypted link to health record.
- Each record is time stamped.
- All patient records (historical) are together and stay with the patient.
- Patient has control over the permissions on whom to share with.

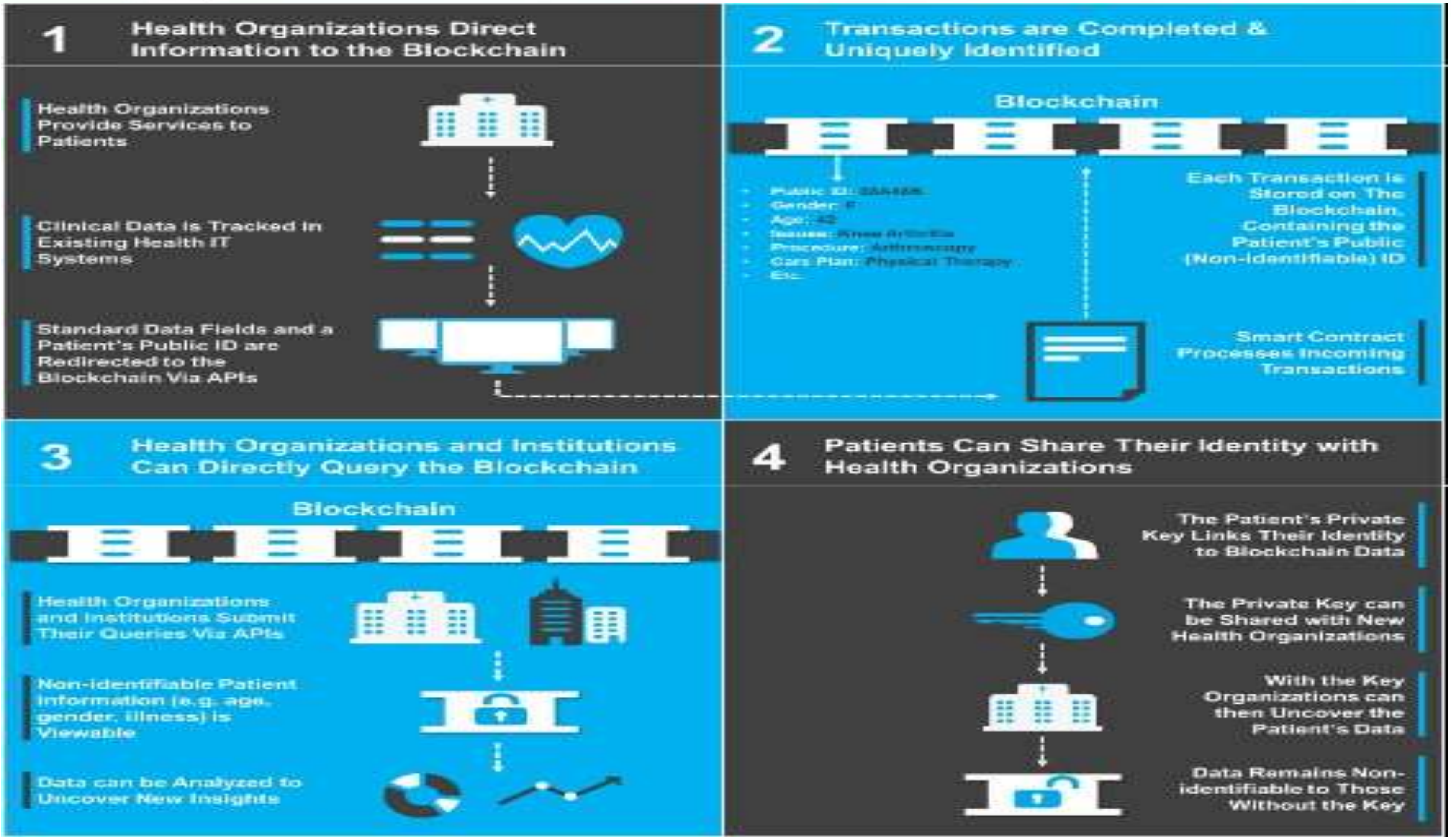
Blockchain network consensus enables disintermediation to automate claim adjudication and payment processing with predefined smart contracts

Providers uses health application to access health data

Patients use mobile devices to assign access permission to data and to provide public key

Distributed patient consent for research/ clinical trials enables data sharing, audit trials, and clinical safety analyses

Health Care Blockchain



1 Health Organizations Direct Information to the Blockchain

Health Organizations Provide Services to Patients

Clinical Data is Tracked in Existing Health IT Systems

Standard Data Fields and a Patient's Public ID are Redirected to the Blockchain Via APIs

2 Transactions are Completed & Uniquely Identified

Blockchain

- Public ID: [illegible]
- Gender: F
- Age: 42
- Issues: Knee Arthritis
- Procedure: Arthroscopy
- Care Plan: Physical Therapy
- Etc.

Each Transaction is Stored on The Blockchain, Containing the Patient's Public (Non-identifiable) ID

Smart Contract Processes Incoming Transactions

3 Health Organizations and Institutions Can Directly Query the Blockchain

Blockchain

Health Organizations and Institutions Submit Their Queries Via APIs

Non-identifiable Patient information (e.g. age, gender, illness) is Viewable

Data can be Analyzed to Uncover New Insights

4 Patients Can Share Their Identity with Health Organizations

The Patient's Private Key Links Their Identity to Blockchain Data

The Private Key can be Shared with New Health Organizations

With the Key Organizations can then Uncover the Patient's Data

Data Remains Non-identifiable to Those Without the Key

Advantages

- Blockchain technology offers many advantages for health care IT.
- Blockchain is based on opens source software, commodity hardware, and Open API’s.
- These components facilitate faster and easier interoperability between systems and can efficiently scale to handle larger volumes of data and more blockchain users.
- The architecture has built-in fault tolerance and disaster recovery, and the data encryption and cryptography technologies are widely used and accepted as industry standards.
- The health blockchain would be developed as open-source software.

Advantages

- It is reliable and robust under fast changing conditions that cannot be matched by closed, proprietary software.
- Open-source solutions also drive innovations in the applications market. Health providers and individuals would benefit from the wide range of application choices and could select options that matched their specific requirements and needs.
- Blockchain technology offers many advantages to medical researchers, health care providers, care givers and individuals.
- Creation of a single storage location for all health data, tracking personalized data in real-time and the security to set data access permissions at a granular level would serve research as well as personalized medicine.

- The most efficient and effective approach for advancing interoperability objectives would be to establish a national technology infrastructure for health IT based on open standards.
- Open API's based on industry best practices are vital and essential to addressing interoperability.
- However, open API's are essential but not sufficient.
- A shared distributed infrastructure that provides a comprehensive view of an individual's health data across a lifetime is an equally essential component of interoperable health IT systems.

- Blockchain technology addresses **interoperability** challenges, is based on open standards, provides a shared distributed view of health data and will achieve widespread acceptance and deployment throughout all industries.
- **Utilization of the proposed health blockchain** described in this work has the potential to engage millions of individuals, health care providers, health care entities and medical researchers to share vast amounts of genetic, diet, lifestyle, environmental and health data with guaranteed security and privacy protection.
- **The acquisition, storage and sharing** of this data would lay a scientific foundation for the advancement of medical research and precision medicine, help identify and develop new ways to treat and prevent disease and test whether or not mobile devices engage individuals more in their health care for improved health and disease prevention.

Uses of Blockchain in Health Care

- Blockchain has the potential to substantially impact the health care industry

- As a whole and payers, providers and patients with respect to drug traceability, clinical trials and research, and data management.

Blockchain can provide authentication and prevent modification:

- Provides proof of existence for and verification of trial data and transparency
- Would include the trial protocol, results, site information, required consents, etc.
- Allows reproducibility and secure data sharing among research communities
- Trial protocol may have a unique signature recorded on the blockchain

Patient Data Management

Managing patient data requires complete access the individual medical records to be shared among various clinicians and other professionals and to and from various locations.

- No standards for collection, storage or disclosure of such information
- Social networks and physician portals are not always secure
- Patients do not control their data

Patient Date Management

Blockchain can provide a secure structure:

- Users share information
- Information can be stored in smart contracts containing permissions and conditions for release
- Patients control access – private keys unlock access or third parties authorized by the patients can do so
- Can pull in other information from wearables and registries
- Companies are building personal health records (PHR) to align all stakeholders through patient engagement platforms and utilizing blockchains to implement

Patient Data Management

ONC issued an informational blockchain challenge to address the sensitive nature health data and challenges of interoperability, patient record matching and information exchange.

- **Critical issues include:**
  - Creating a trusted environment for determining how multiple providers can view, edit and share patient data while maintaining up-to-date records – that EHRs were not designed to manage
  - Allowing providers to add new records and patients to authorize sharing

Patient Data Management

- **Blockchain can:**
  - Address patient consent for data sharing not addressed by HIEs
  - Provide more tailored consents and update as desired
  - Create a system of “smart contracts” for a rule-based method for access

Patient Data Management

Store certain data on the blockchain but still allow certain data to be accessed by secure links:

- On blockchain data could include age, gender and other personally identifiable information; be of the size and type to be stored and be immediately viewable
- Off blockchain data could include images and medical notes of any size or format that may have different requirements for the need to view.

Patient Data Management

- Blockchain could also collect information from web-based and mobile applications or other devices and becomes very important for digital health
- Development and other costs, concern of patients, scability,
  storage limits and capacity are obstacles to be addressed

Blockchain for EHR Interoperability and Exchange of Big Data

Blockchain provides the validation that health care industry needs, and delivers in a way all parties can trust. No single entity is in charge of holding the data, but all participants are responsible for ensuring data integrity and security.

If no one can change a record without all stakeholders approving the changes, and no unauthorized party can access the health record without the participants giving collaborative permission, the health care industry can avoid two of its most dangerous big data risks at the same time.

Patient care may benefit from the idea that a readily available verifiable record is instantaneously shared among stakeholders and does not rely on manual data reconciliation prone to human error.

Blockchain for EHR Interoperability and Exchange of Big Data

- Health care organizations may need to limit the number of authorized participants in a single blockchain to a patient, and his or her care team and approved family members.
- This collaborative approach to creating and sharing data would eliminate many of the challenges of HIEs, including the question of how much to trust the middleman.
- While some HIEs have already taken a decentralized approach to their data architecture, the validation piece has been missing.
- Patients and providers have had to trust that the HIE knows what it's doing, and take it on faith that the records moving back and forth between hospitals, specialists, or care facilities are the best possible
version of the patient's history.

- When using a blockchain approach to sharing a patient’s record, the question of trust is irrelevant since every participant is known and has been approved.

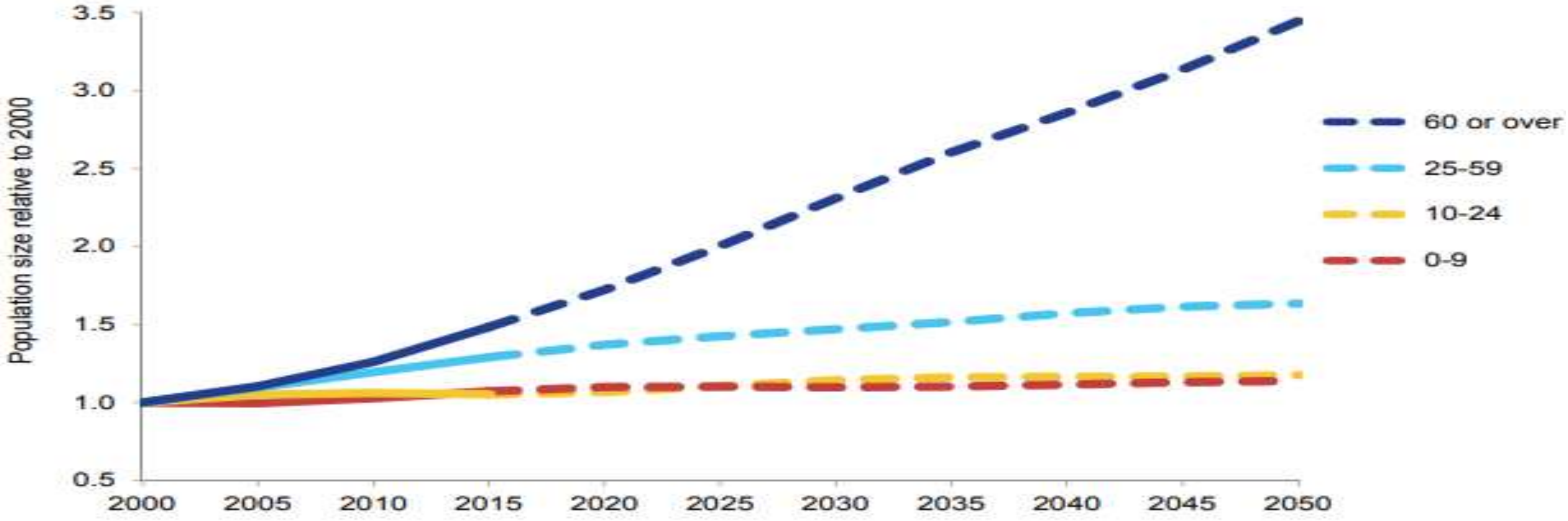
- The implications of blockchains for population health management, patient matching, and care coordination are massive.

- In addition. Health Care organizations will not compete for, or be unwilling to share, data since they will all have exactly the same information.

Significance

- Increased life expectancy results in a large aging population in the next two decades coupled with
- Inability of Elderly and disabled people to Afford Medication
- Emphasizes the need for **smart, secure , reliable and cost effective health care systems.**

Increase in world population relative to 2000, by broad age group, 2000-2050



Data source: United Nations (2015). *World Population Prospects: The 2015 Revision.*

Project Significance

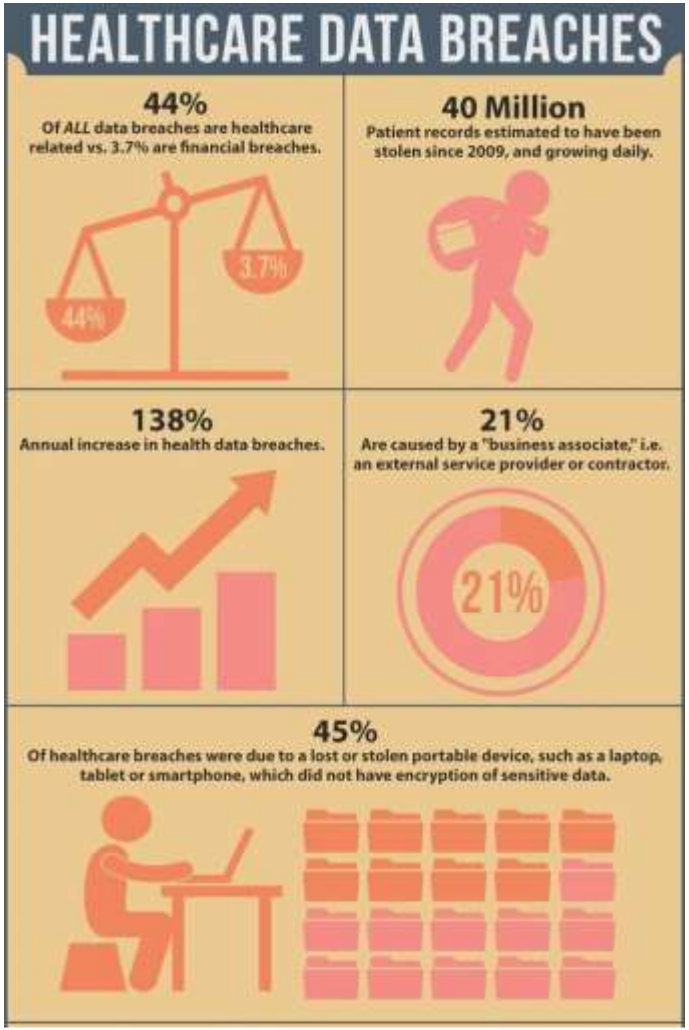
✓Increase in Healthcare data breaches

✓Lack of **reliability, availability, privacy, security and interoperability** with the existing centralized systems

✓ To Ensuring trust in medical community, scientist and in pharmaceutical is essential to improve the quality of healthcare.

✓To save Massive loss of time, money and eventually life.

✓We proposed a **blockchain integrated decentralized secure and smart health care system**



SOURCES: http: //www. govhealthitcom/ news/5-ways-health-data-breaches-are-far-worse-financial-ones

Benefits to elderly and Disabled

✓Blockchain facilitates personalized and integrated approach to service delivery for the elderly

✓Allow **longitudinal data of the elderly** to be securely stored on the blockchain which they can grant access to the service providers they had engaged.

✓ Link all product and **service providers** for eldercare with the elderly, their **families and care givers** together to form a seamless ecosystem where relevant information are readily accessible by them.

✓Improve efficiency and save cost for the service providers and the elderly by leveraging on **smart contract** for eldercare products and service

Project uniqueness from Existing Solutions

Existing Solution	Proposed Solution
We need to trust intermediary [third party] to store our health records	Third parties can be eliminated by establishing a distributed ledger which has built in trust mechanism [blockchain]
Cost per transaction is very high as lot of intermediaries are involved.	Reduces transaction costs due to disintermediation, as well as near-real time processing.
No standard method for Patient identity	Uses Private and public keys identifiers which creates a singular, more secure method of protecting patient identity
No health data interoperability between systems	Shared data enables real-time updates across the network to all parties
Limited Access to health data	Distributed, secure access to patient health data across the distributed ledger
Inconsistent rules and permissions	Smart contracts creates a rule-based method for accessing patient data that can be permissioned to selected organizations

Objectives

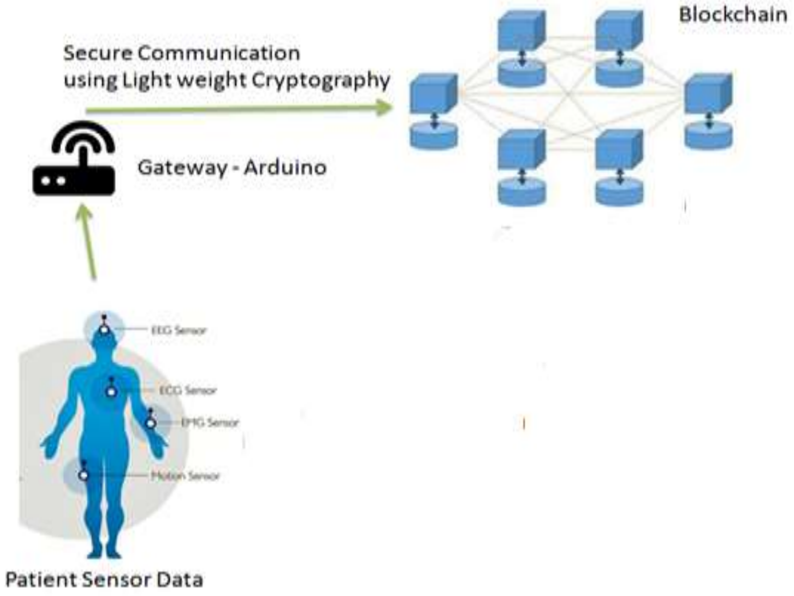
✓To build a BLOCKCHAIN INTEGRATED SMART AND SECURE HEALTH CARE SYSTEM while ensuring system reliability, security and privacy, Interoperability of the data.

✓To provide enhanced security for storage and Privacy-Preserving Data Sharing using Blockchain .

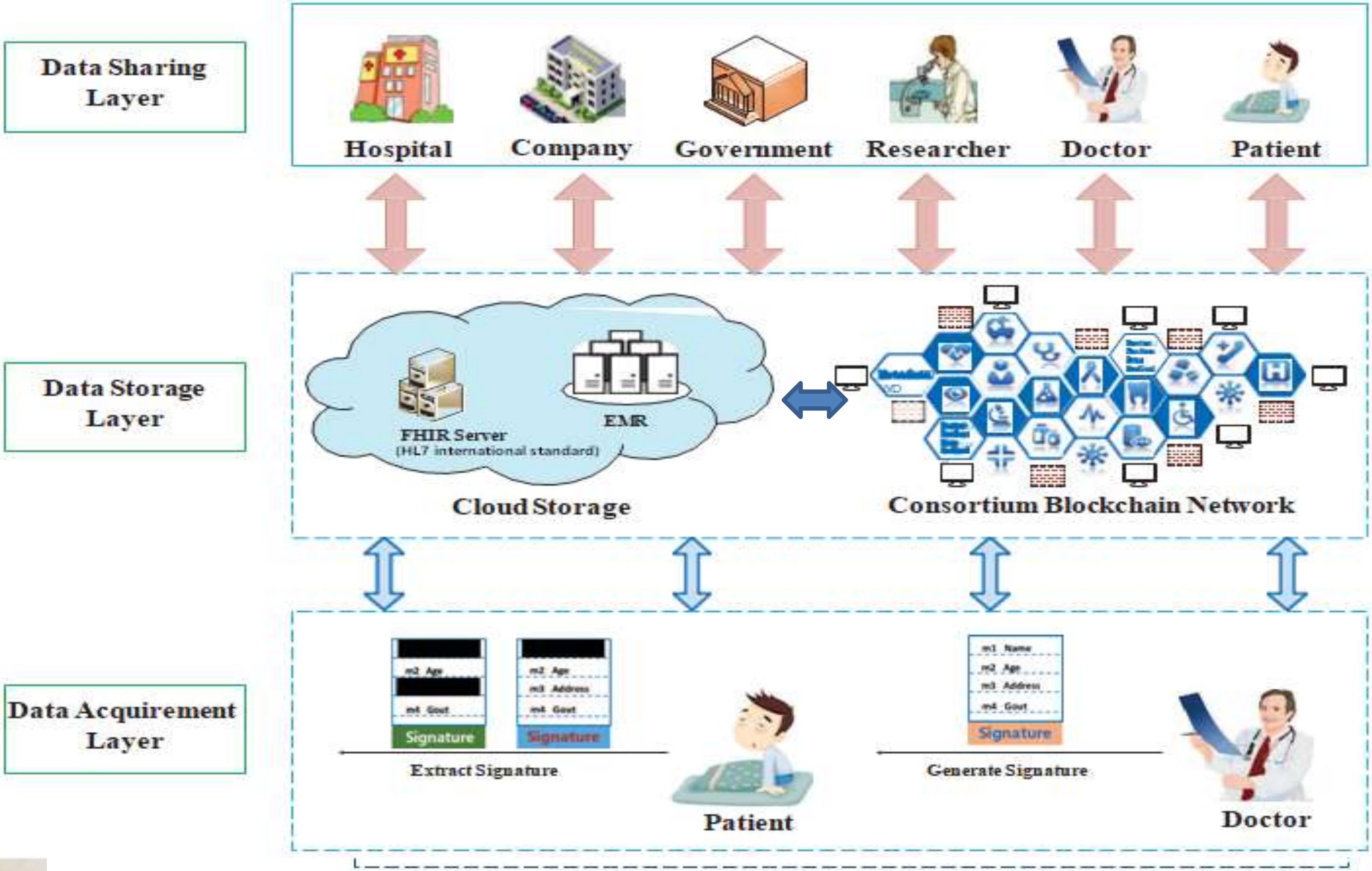
✓To collaborate with doctors from hospitals they engaged for taking preventive measure for any abnormalities.

METHODOLOGY

1. Pulse
2. Oxygen in blood (SPO2)
3. Airflow (breathing)
4. Body temperature
5. Electrocardiogram (ECG)
6. Glucometer
7. Galvanic skin response (GSR - sweating)
8. Blood pressure (sphygmomanometer)
9. Patient position (accelerometer)
10. Muscle/electromyography sensor (EMG)



BLOCKCHAIN BASED PRIVACY-PRESERVING DATA SHARING(BDPS) FOR Electronic Medical Records(EMR)



BPDS System Architecture

The function of each layer is described as follows.

Data Acquirement Layer

✓EMRs are created by data providers such as doctors.

✓Doctors sign patients’ EMRs using their private key and send them to the patients.

✓Patients are the owners of EMRs and can completely control them.

Data Storage Layer

✓***Fast Healthcare Interoperability Resources (FHIR):*** The standard was created and is managed by the Health Level Seven International (HL7) healthcare standards organization.

✓***Cloud Storage:*** The cloud stores patients' encrypted EMRs Which solves limited storage capacity of blockchain.

▪In order to avoid privacy information is leaked in the process of data sharing, patients can remove sensitive information of EMRs and generate valid extraction signatures.

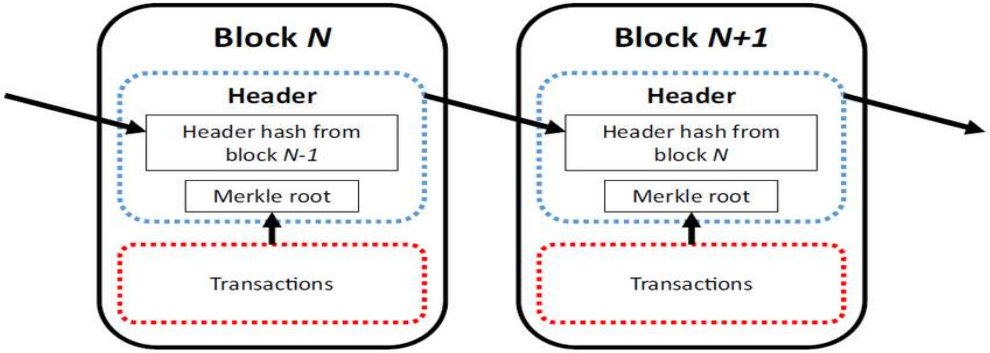
▪***Data Sharing Layer***

✓The authorized patients, medical workers and healthcare institutions can request patients’ EMRs and utilize them for making personal health plans, getting better clinic treatment or carrying out medical research.

✓ The patient predefined access permissions in the smart contracts to ensure data sharing securely.

A. Immutability (Tamper Proof)

- Every transaction is hashed using SHA256 algorithms
- Each Block is also hashed and linked to previous block
- All the transactions are again grouped and a Merkle Root of the transactions are calculated and stored in the block.
- As Merkle root is created which contains all the transaction hashes it is highly impossible to tamper / modify any transaction which ensure Immutability / Data integrity



B. Privacy Preservation

-- Anonymity. Each participant generates a unique account with *a* ***random public key***. Therefore, each transaction on the blockchain is anonymous.
-- Confidentiality. The original EMRs are **encrypted** and stored in the cloud storage.
-- Content Extraction Signature(CES) Any entities cannot forge extraction signatures without the signer's private key.
-- Improved DPoS. BPDS uses the improved DPoS consensus to realize the trust between a certain number of preselected nodes in the consortium blockchain. In the improved DPoS, the selected medical organizations are reputable and reliable, which guarantees the reliability of data sharing.

C.Data Secure Storing and Sharing

Confidentiality and Integrity : The use of **symmetric encryption technology guarantees** the of EMRs generated by doctors.

-- Authentication, Integrity, and non-repudiation are provided for each transaction through the **digital signature**

-- Data Sharing. In BPDS, the data access permissions are preset in the **smart contracts**. Only authorized users or institutions can use the EMRs.

Work Flow of BPDS

- The elderly and disabled Patient(P) healthcare sensor data securely send to the Doctor(D)
- D integrates related EMR of P
- Upon receiving EMR'S, P stores them to the cloud FIHR server and submits the indexes of EMR to B.C with the list of authorized data users
- Data sharing:- For secure EMR sharing to healthcare stakeholders, P pre-sets access permission in the smart contracts with time period

Blockchain Further Reading

1. Blockchain Use Cases in Healthcare; Anca Petre – 1/30/17
2. IBM Watson, FDA Collaborate on Healthcare Blockchain Research; Elizabeth O’Dowd; HIT Infrastructure.com
3. Advancing Healthcare and Clinical Research with Blockchain: Florence and Verady Farm Partnership; Press Release 9/25/17; newsine.com
4. Blockchain Technology for Improving Clinical Research Quality; Mehdi Berchoufl and Phillippe Ravaud; *Trials*
   (2017)
5. Fudging Clinical Trial Data Made Impossible by Blockchain Technology Gautham; Bitcoin News
6. Is Blockchain The Solution to Drug Traceability?; Bob Celeste, Pharmaceutical Online, 7/17/17
7. Three Reasons for Leveraging The Blockchain for Clinical Trials; Gordon Tampol, GP{MS 8/22/16
8. Improving Data Transparency in Clinical Trials Using Blockchain Smart Contracts; Timothy Nugent, David Upton, Mihai Cimpoesu, F1000Research 5:2541 2016

9.Expoloring the Use of Blockchain for EHRs, Healthcare Big Data; Jennifer Bresnick; Intelligent

Media 10.Is Blockchain the Answer to Healthcare’s Big Data Problems; Jennifer Bresnick;

Intellignet Media 4/27/16

11.Five Blockchain Uses for Healthcare Payers, Providers; Jennifer Bresnick; Intelligent Media; 10/10/17

THANK YOU