EKNOW 2022, Porto, Portugal,
Special Track BCI (Blockchain for Industry)

Laboratory of Automation and Manufacturing, Algeria

Blockchain in eHealth

How Blockchain technology can be integrated into electronic healthcare systems to improve them and make them more secure.

REES MANGENA
AND
SAMIA AITOUCHE
Contact : mangenarees@gmail.com
: samiaaitouche@gmail.com

CONTENTS

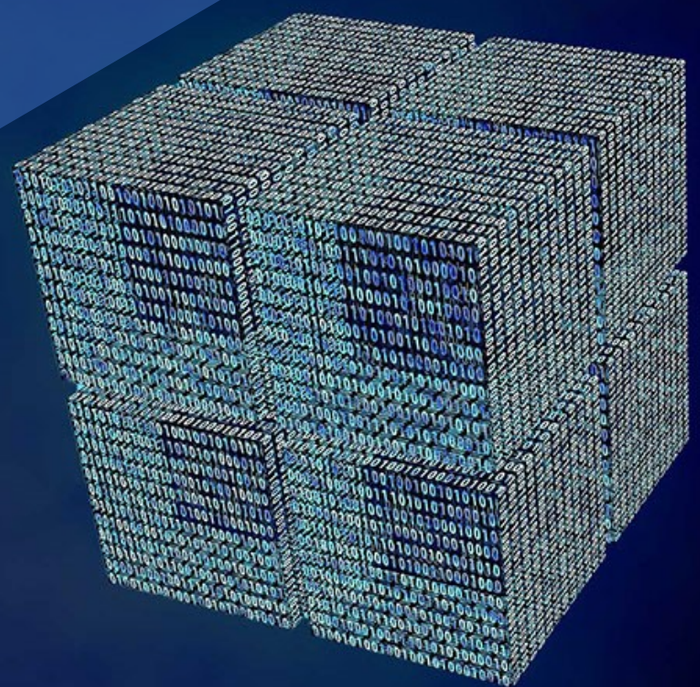
CONTENTS

(continued……)

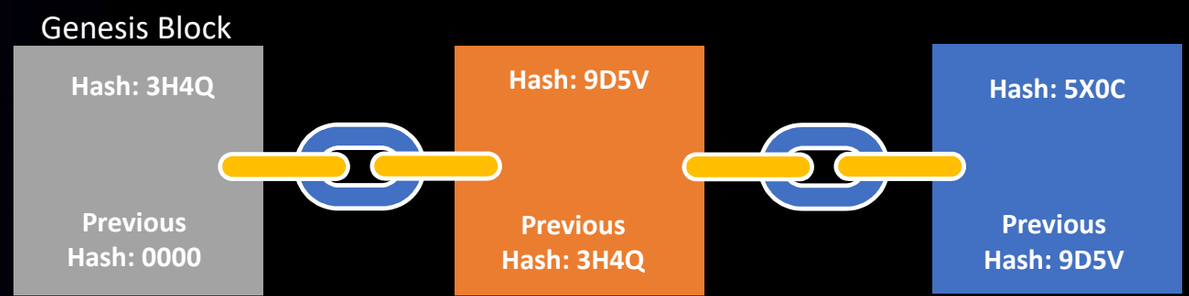
INTRODUCTION

Certain researchers consider the blockchain technology as an Industry 4.1 revolution, because it benefits from the Industry 4.0 revolution and its technologies, in a decentralized manner. Here we will address a review of the use of blockchain technology in electronic health (eHealth) because of its importance for the comfort of citizens and the promotion of a healthy society, especially after the pandemic experience of COVID-19, where the necessity and the importance of telework and Information and Communications Technology (ICT) became more essential than ever before. Healthcare has had a reputation for being a traditional business that is resistive to new ideas. Healthcare issues (such as privacy, quality of care, and information security) have gotten a lot of attention in recent years all around the world. Blockchain technology is becoming more widely recognized as a means for addressing current information mismanagement difficulties. It has the potential to improve immediate healthcare practices, such as health service delivery and care support quality.

WHAT IS BLOCKCHAIN?



- Blockchain is a shared, immutable digital ledger. It is used as method of storing data that makes it difficult or impossible to change, hack, or cheat the system. The information in a blockchain is stored in the form of a data blocks with each block connected to the next.
- It is a type of distributed ledger technology in which transactions are recorded with an immutable cryptographic signature known as a hash, each block having both its own hash and the hash of the previous block, as shown below.[1]



- Adding a block (data) to the blockchain would require the approval of all the nodes involved in the blockchain network.

IMPORTANT PROPERTIES OF BLOCKCHAIN

Decentralization

A blockchain is not managed by a single central authority. Since it is a decentralized blockchain network, no one needs to know or trust in anyone else. A distributed ledger that contains identical data is shared by every member of the network. The majority of the network's members will reject a member whose ledger has been edited or corrupted in any way.[4]

Immutability

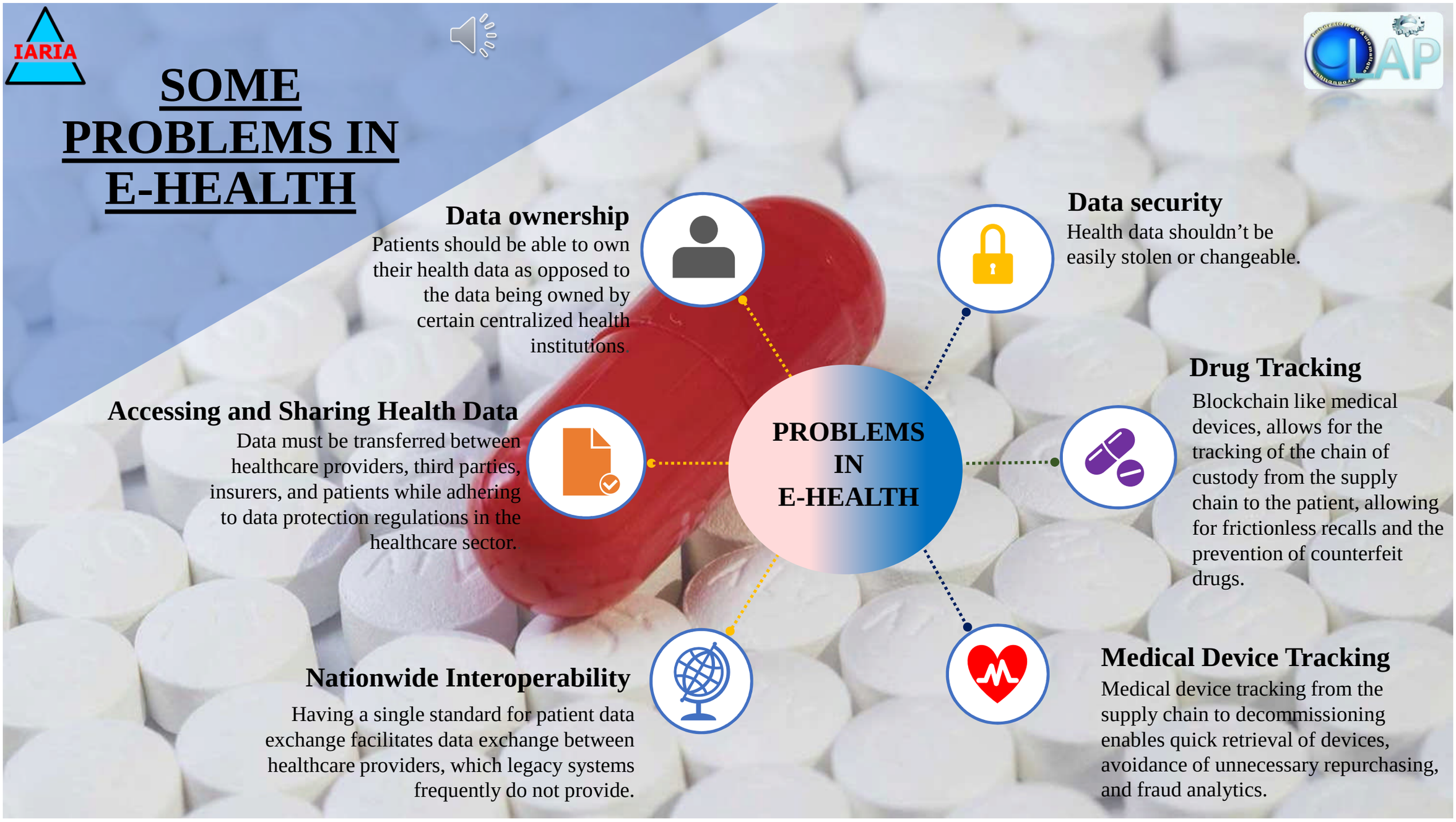
In blockchain, an immutable ledger is any record that can remain unchanged. It cannot be altered, and thus the data cannot be easily changed, ensuring that the security is quite tight. Immutability implies that it is extremely difficult to make alterations without collusion. The blockchain ledger's central idea is data security and proof that data has not been changed or altered.[5]

WHAT IS E-HEALTH?

According to the World Health Organization (WHO), eHealth is "the cost-effective and secure use of information and communication technologies in support of health and health-related fields, such as health-care services, health surveillance, health literature, and health education, knowledge, and research."
It is the use of the Internet and other associated technologies in the health-care industry to distribute health services and information.[2]

Typically, three types of cloud models are used to deliver e-Health cloud services: private, public, and hybrid clouds. Obtaining security and privacy in eHealth is critical to meeting the goals of using this modern technology. This is critical because digitizing and sharing health-related data can lead to various types of attacks. As a result, many government health institutions have developed frameworks to ensure a high level of security and privacy.

SOME PROBLEMS IN E-HEALTH



Data ownership

Patients should be able to own their health data as opposed to the data being owned by certain centralized health institutions.

Data security

Health data shouldn't be easily stolen or changeable.

Accessing and Sharing Health Data

Data must be transferred between healthcare providers, third parties, insurers, and patients while adhering to data protection regulations in the healthcare sector.

Drug Tracking

Blockchain like medical devices, allows for the tracking of the chain of custody from the supply chain to the patient, allowing for frictionless recalls and the prevention of counterfeit drugs.

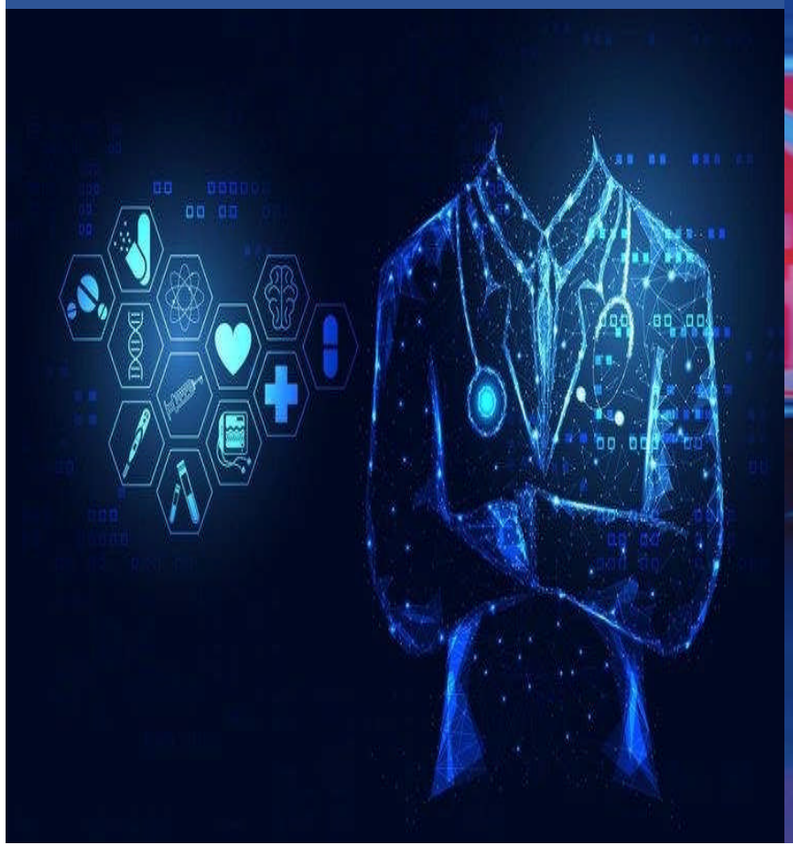
Nationwide Interoperability

Having a single standard for patient data exchange facilitates data exchange between healthcare providers, which legacy systems frequently do not provide.

Medical Device Tracking

Medical device tracking from the supply chain to decommissioning enables quick retrieval of devices, avoidance of unnecessary repurchasing, and fraud analytics.

THE USE OF BLOCKCHAIN IN E-HEALTH



There are many problems in today's healthcare that may be solved using blockchain. Two of the major focuses that must be addressed are: Data security and Data ownership. Currently, sensitive medical records lack a secure structure, resulting in data breaches with serious consequences. The second source of concern is that patients are currently unable to fully own their own medical data, a concept that is becoming more relevant with the rise of personalized medicine and wearables. Both of these issues have significant moral ramifications that must be addressed. Blockchain technology could be the answer to both these problems.

Another key challenge as tagging medical equipment with a usable ID and integrating trust in device identification and tracking. When a device, such as an infusion pump, is shown to have malfunctioned, tracking the device can reveal the source of the problem and prevent unnecessary repurchasing in the case of lost devices. These threats are likely to be reduced by a strong trust infrastructure based on medical device identification.

Blockchain can also assist the pharmaceutical industry in overcoming the growing risks associated with counterfeit and unapproved drugs. As with device tracking, smart contracts for drugs can be defined and then pill containers identified using integrated (GPS) and chain-of-custody logging.

THE USE OF BLOCKCHAIN IN E-HEALTH (Continued..)

Another use of blockchain in healthcare could be in clinical trials to overcome problems such as fraudulent results and the removal of data that does not support the researcher's bias or the funding source's intention. This will enforce clinical trial integrity.

Health insurance could also benefit from a trusted record of events surrounding the patient pathway, such as improved incident reporting and automating underwriting activities. Contracts, such as automated payments for parts of the patient pathway, could also be clearly defined and then implemented.

Pharmacists will potentially be impacted by this technology and therefore should have a strong interest in it. Pharmacists could have prescriptions that cannot be forged. Pharmacists in research laboratories could use this technology to prove the progress of their research without disclosing it. Finally, industrial pharmacists will be able to ensure the authenticity of medicines throughout their journey

Comparison of Traditional, Centralized and Blockchain supported e-Health

	Traditional Healthcare System	Centralized Telemedicine System	Blockchain Supported System
Cost	High	Low	Low
Patient Waiting Time	Very High	Low	Low
Fault Tolerance	No	No	Yes
Requirement for In-Person Visiting	Yes	No	No
Data Provenance	No	No	Yes
Health Record Manipulation	Yes	Yes	No
Documentation	Yes	Yes	No
System Administration	Centralized	Centralized	Decentralized
Audit Trails	No	No	Yes
Data Privacy & Security	Hard	Hard	Easy
Transparency	No	No	Yes
Reliability & Integrity	Low	Low	High

TYPES OF BLOCKCHAIN

Public (permissionless)

Everyone can see the data in a public chain, and anyone can join and contribute to both consensus (in theory) and changes to the core software. The public blockchain is widely used in cryptocurrencies, and the two most popular cryptocurrencies, Bitcoin and Ethereum (the main chain), are public permissionless chains.

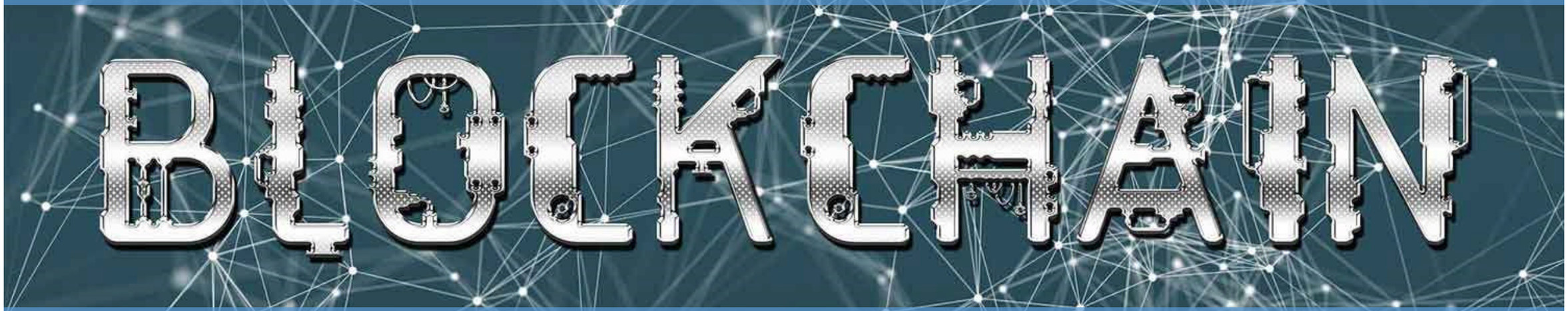
Consortium(public permissioned)

A consortium blockchain is partially centralized in the sense that only a select group of entities has access to view and participate in the consensus protocol.

Private

The network in a private blockchain is distributed but frequently centralized. Only selected nodes can participate in the network, which is frequently managed by a single central authority.

Algorithms used in e-health care systems (Consensus Mechanisms)



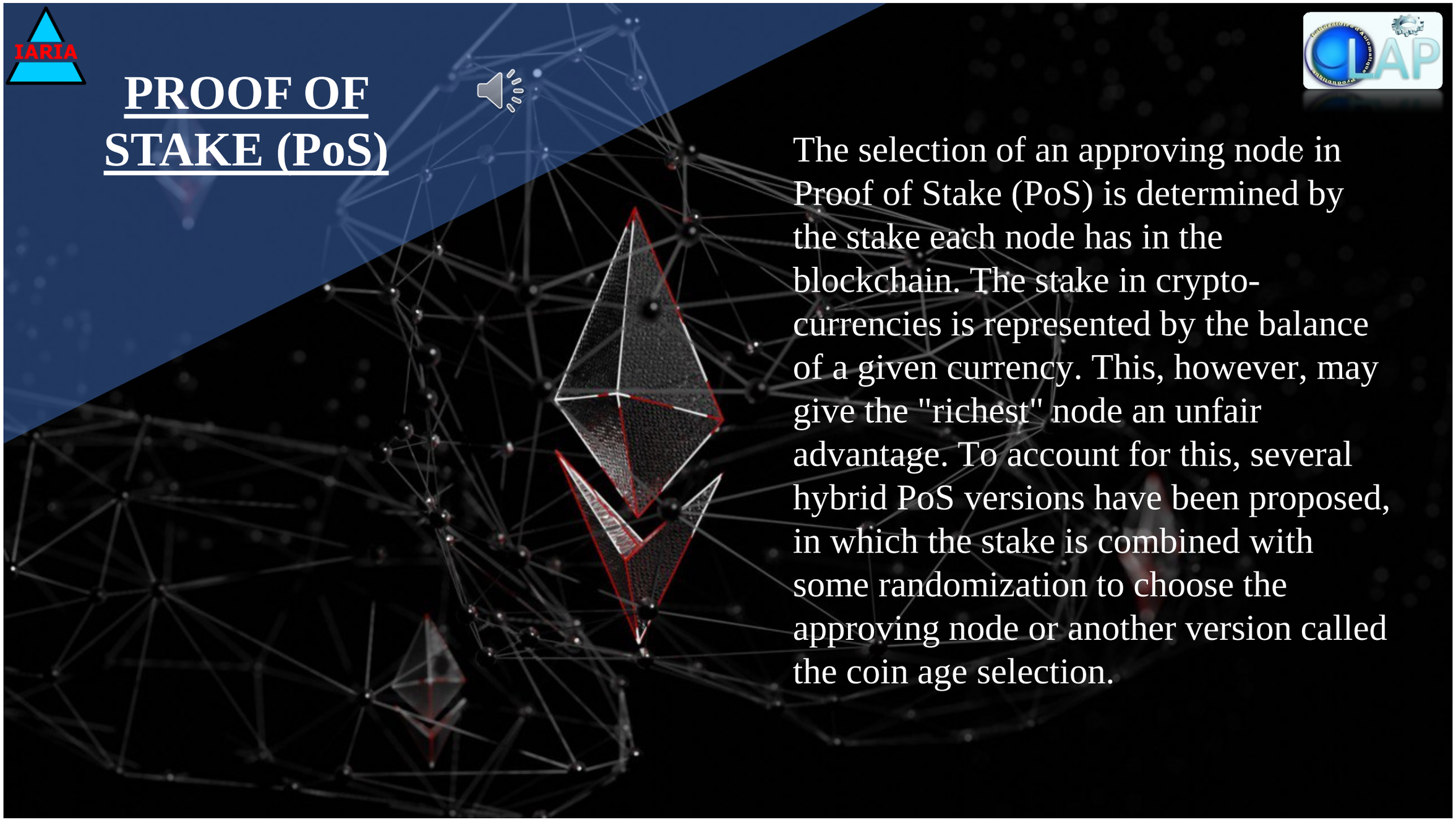
The way data entries are accepted onto the distributed ledger by a distributed consensus protocol validating the data entries is a critical component of blockchains. There are several proposed and used consensus protocols, the three most commonly used being Proof-of-Work (PoW), Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT).

PROOF OF WORK (PoW)

Because of its integration in Bitcoin, Proof-of-Work (PoW) is the consensus protocol most strongly associated with blockchain.

When the PoW protocol is used, so-called miners compete to solve a computationally difficult puzzle. Miners use brute force to try to find a hash of the proposed block that is less than a predetermined value. The miner who computes this hash value first validates the transactions (or other entries) in the block and receives a reward.
However, a disadvantage of this method is that it consumes a significant amount of energy.

PROOF OF STAKE (PoS)



The selection of an approving node in Proof of Stake (PoS) is determined by the stake each node has in the blockchain. The stake in crypto-currencies is represented by the balance of a given currency. This, however, may give the "richest" node an unfair advantage. To account for this, several hybrid PoS versions have been proposed, in which the stake is combined with some randomization to choose the approving node or another version called the coin age selection.

PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)

A Byzantine agreement protocol underpins Practical Byzantine Fault Tolerance (PBFT). Because all nodes in PBFT must be known to the network, this consensus protocol can only be used in a public blockchain. The PBFT consensus process can be divided into three stages: pre-prepared, prepared, and commit. To progress through the three phases, each node must receive two-thirds of the votes cast by all nodes.

SMART CONTRACTS

These are self-executing contractual agreements supported by some blockchain infrastructures such as Ethereum, that formalize previously agreed-upon provisions in source code without the involvement of a third party or intermediary. Smart contracts in eHealth can be involved in [3]:

- Designing secure payment protocols by performing blockchain-based smart contract enabling the patients and hospital to reliably p ay the diagnostic and storage service efficiently
- Registration contract for immutable patient log creation
- Health Record Storage Contract for secure storage and rapid access
- Health Record Creation Contact to generate digital health records
- Update permission Contract that can provide access at emergency situations
- Viewership Permission Contract for viewing the health information by the patients for home care and future care.
- Data sharing Permission Contract for exchange of health records between different stakeholders

SMART CONTRACTS

METHODS OF ACCESSING DATA

A. Using a blockchain tree

This is done by using a principal block on the main chain containing basic information of the patient and a sub block on the sub chain containing the medical record accessed only by using Proof Of Authority (POA) protocol to ensure the registration of any successful or unsuccessful attempts of access to the records, as illustrated in Figure 1 [13].

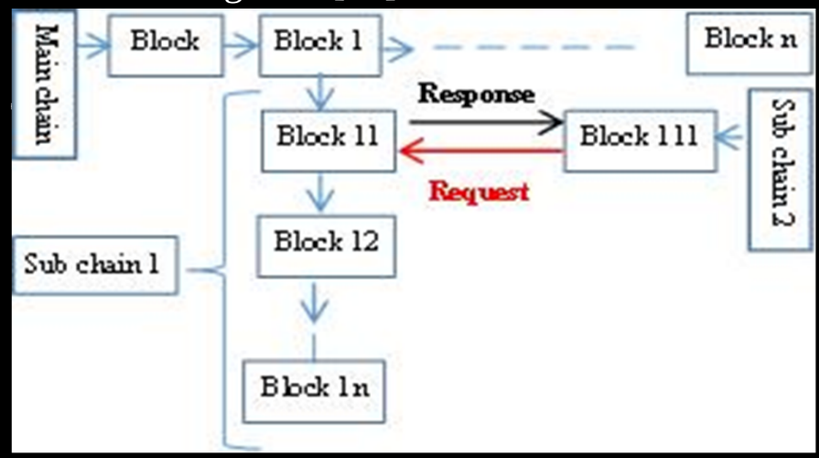


Figure 1. Blockchain tree structure

B. Practical Byzantine fault tolerance

Here, all nodes participate to the voting (2/3 must accept the transaction) which may cause a delay in the transaction processing and slow the whole operation.

METHODS OF ACCESSING DATA

C. Delegated byzantine fault tolerance

Not all nodes most vote which leads to a fast transaction acceptance but with a risk of centralization [14].

D. Adoptive leader election algorithm : (ALEA)

This algorithm is based on electing a leader via Leader Election Algorithm (LEA) to grant him permission to create, access, copy, move, edit and delete data. This type of algorithm is using bully leader election method to minimize energy consumption

Figure 2. Leader election queue

These algorithms are characterized by:

- 0% failure: due to blockchain technology if a node fails others can do the work (give access to Electronic Personal Health Record (EPHR)).
- Ownership can’t change if the owner dies or loses consciousness
- High and slow response using ALEA [15]

METHODS OF ACCESSING DATA

E. Using two types of chains :

A private one that contains the real ID of the patient and a public one which has health data of the patient under a temporary ID, under the control of a hyper ledger fabric framework, noting that only the trusted nodes can access the private chain, as shown in the figure below.

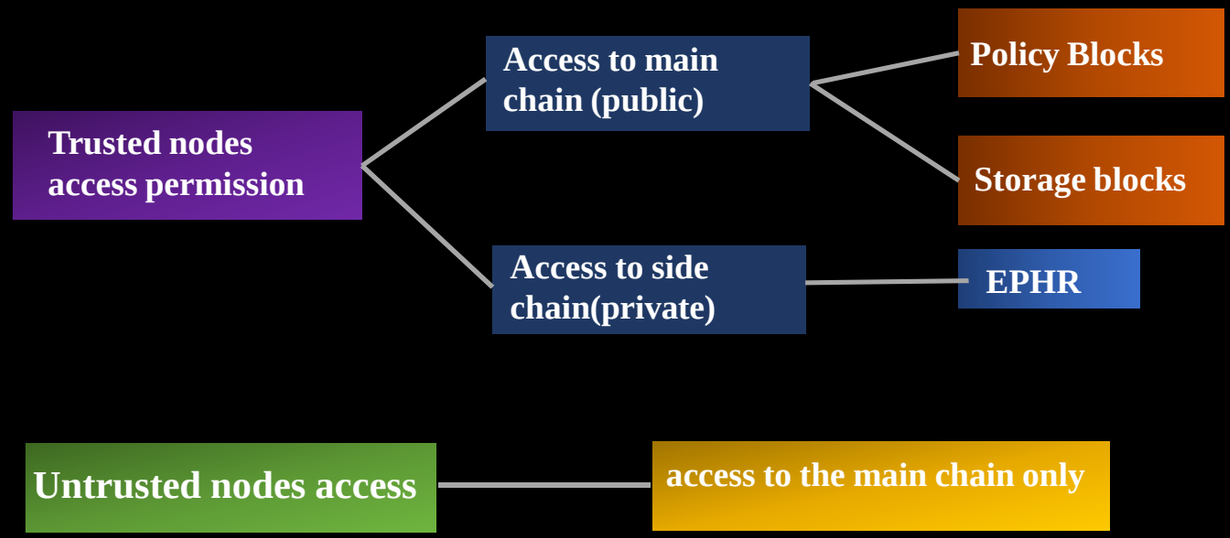


Figure 3. Types of permission for trusted and untrusted nodes

***Storage block*: The main chain is used to secure the data from modification as it creates storage blocks containing the temporary ID, patient digital signature approving the transaction, medical institution signature and information about the current block and the previous one.**
***Policy block*: it contains a form of contract about the storing policies of the institution who store the data, signed by both it and the patient then approved by the trusted nodes and broadcasted on the main chain [16].**

USING IOT IN E-HEALTH

We will see how can we introduce IOT and blockchain to the health care system. The general idea is to equip patients, post-hospitalization, with equipment easy to use that collect data for example heart rate, blood pressure, etc. and puts them on the blockchain while having a well put web platform that offers the link for authorized persons (medical staff) to access the patients' data and monitoring his medical status leading to the lowering of the cost of post-hospitalization.

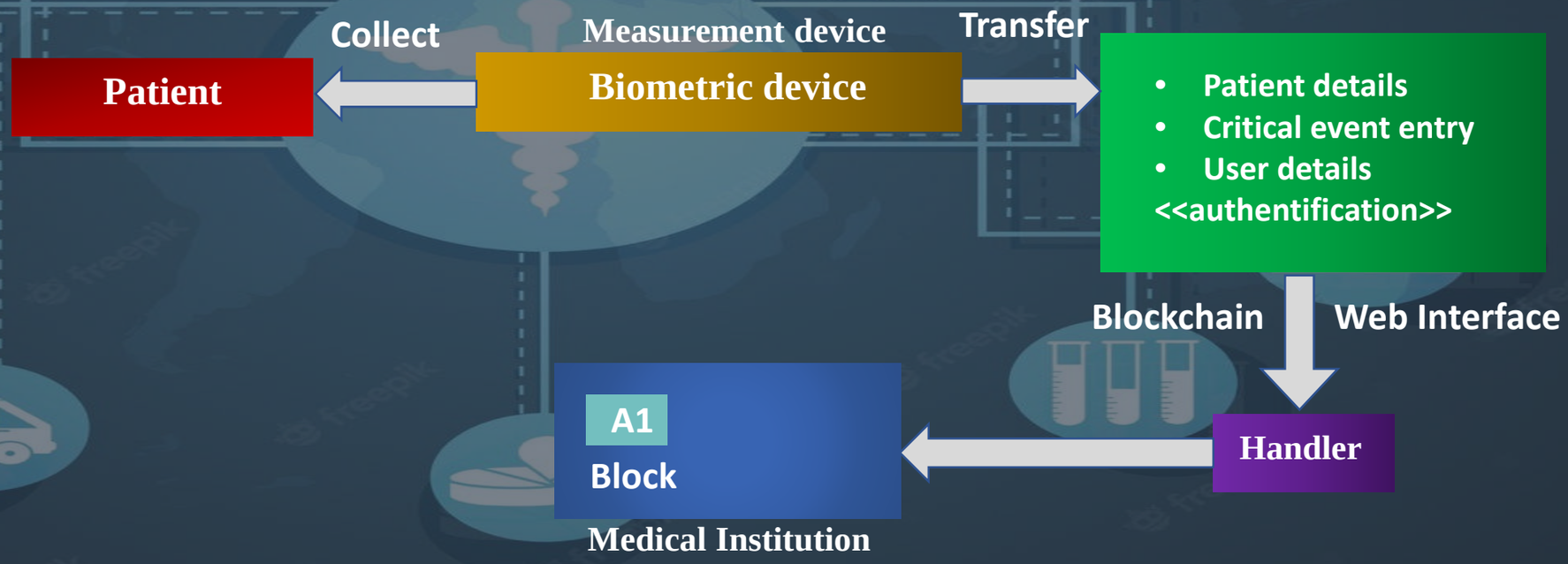


Figure 4. IOT and blockchain health platform

USING IOT IN E-HEALTH

One of many developed methods of collecting patient data and storing them or delivering them in real time to medical institution to ensure the best performance of health care towards the patient is Wireless Body Area Network (WBAN). It is mainly a collection of wireless sensors placed on or in a human body and is used to exchange data from patient to remote stations (noting that this network has a very small range, one we show in Figure 5 below). Afterwards, all these data are then transferred using blockchain technology to ensure proper security and confidentiality.

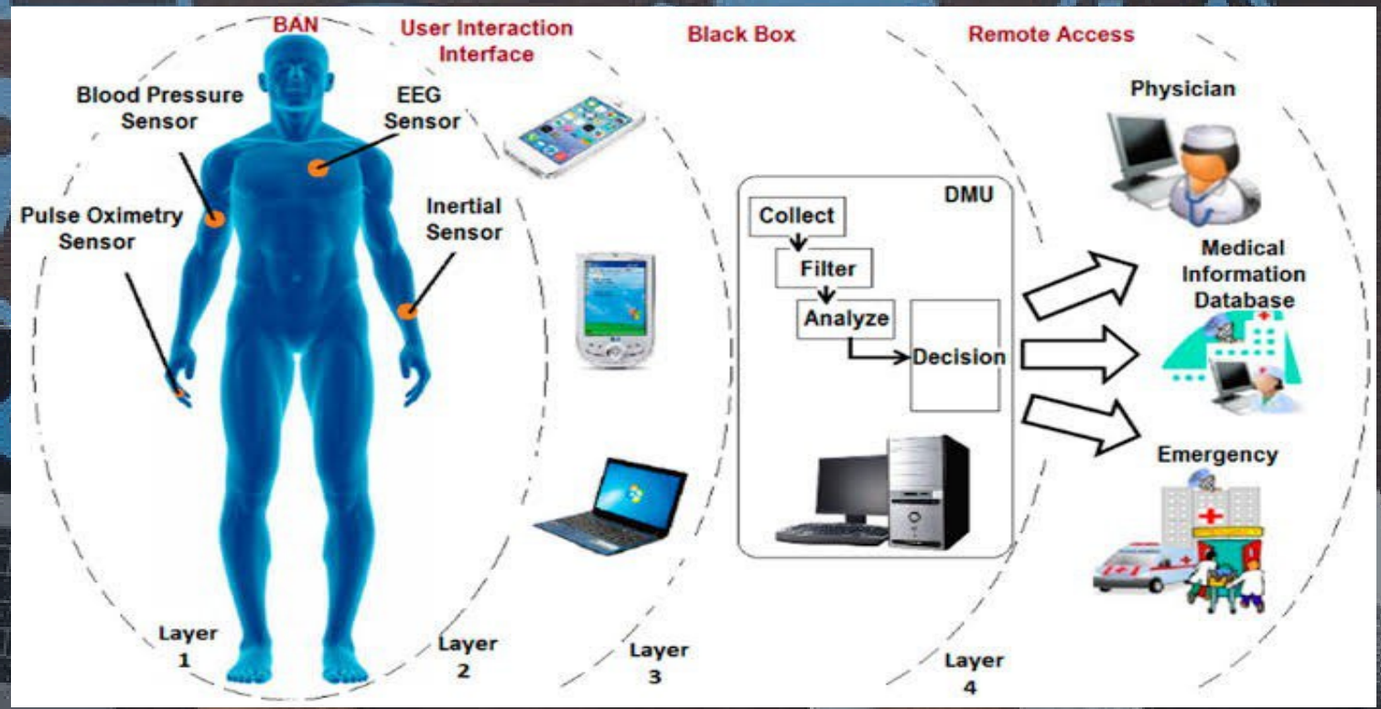


Figure 5. Wireless body area network scheme

HEALTH RECORDS AND THE INTEGRATION OF BLOCKCHAIN TECHNOLOGY

In a general point of view, e-health is an integration of computing methods and systems to provide solutions to the industry of health care, such as managing patient files but due to the huge amount and diversity of files provided by medical institutions, it has become a challenge to share and store data without failing or breaking the rules of privacy [9]. These files are called EHRs, i.e., a digital format of a patient information such as medical history, current and past medication, etc., that are sourced to cloud but cloud based EHRs aren't secure enough and their current cryptographic methods aren't sufficient enough [11]. Thus, blockchain technology has emerged as a promising solution in terms of privacy and data security since it is independent of third parties such as governments or banks. However, this doesn't mean that it is an optimal solution since it is in its early years and needs more development in terms of performance, energy consumption and offering guaranteed confidentiality since in medical health care no one is allowed to read or see patient files without the proper permission [10].

Blockchain Technology and The GDPR Rules

After the rise of blockchain technology, all over the world, a tension was created between this technology and the GDPR. This tension was mainly because of two overarching factors.

First, the GDPR is based on assuming that there is always someone who controls data thus adding more protection as commanded by data subjects; however, blockchain has a philosophy of decentralization, which means there is no more governance but many players who control these data, which can make accountability difficult.

Secondly, the GDPR requires the possibility to erase or modify data in certain circumstances (article 12 GDPR) but blockchains are designed for the exact opposite purpose where they make the modification or deletion data difficult or even impossible, which makes it hard to reconcile with GDPR requirements [12].

CONCLUSION

Blockchain is an immutable ledger that records data entries in a decentralized manner. This new technology has the potential to disrupt a variety of data-driven industries, including the healthcare sector. Cloud-assisted eHealth systems have played an essential role in the administration and management of healthcare data, allowing patients to save their EHRs in an efficient and convenient manner [7]. The efficient management of EHRs is critical for patient telecare, which includes medicine for chronic patients, long-term telecare for special patients, and study of patients infected with a specific disease, among other things. The sharing of EHRs with medical practitioners can improve diagnosis accuracy; however, the system's privacy and security preservation of patients' records are drawbacks. Blockchain technology, due to its immutability, has recently been offered as a promising method for accomplishing EHR sharing while maintaining privacy and security [6]. There are several other areas of healthcare and well-being that could be enhanced using blockchain technologies. Accessing and sharing health data, device tracking, clinical trials, pharmaceutical tracing, and health insurance are just a few examples.

We tried to give a review about the usage of blockchain in eHealth to resolve problems of central bureaucratic authority, replaced by a peer-to-peer network allowing decentralized responsibility, even including the end user in certain blockchain solutions, while maintaining patient privacy and protecting the confidentiality of their health folder. Blockchain is still promising in the future of the healthcare domain as well as in other domains

REFERENCES

[1] Euromoney Learning [online] [retrieved: May, 2022]. Available on: https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain

[2] eHealth: Definition, History, Characteristics, Scope, Benefits and Challenges, September 5, 2019

[3] U. Chelledurai, S. Pandian, and K. Ramasamy, A blockchain based patient centric electronic health record storage and integrity management for e-Health systems. Health Policy and Technology, 2021, 10.4: 100513

[4] Todaro, Joseph Edward. “Blockchain.” Amazon, Cherry Lake Publishing, 2019, https://aws.amazon.com/blockchain/decentralization-in-blockchain/.

[5] Solulab, “What Is Immutable Ledger in Blockchain and Its Benefits.” Blockchain Technology, Mobility, AI and IoT Development Company USA, Canada, 16 Aug. 2021, [retrieved: May, 2022]. Available on: https://www.solulab.com/what-is-immutable-ledger-in-blockchain-and-its-benefits/.

[6] S. Shamshad, Minahil, K. Mahmood, S. Kumari, and C. M. Chen, A secure blockchain-based e-health records storage and sharing scheme. Journal of Information Security and Applications, 2020, 55: 102590

[7] A. Hasselgren, et al. Blockchain in healthcare and health sciences—A scoping review. International Journal of Medical Informatics, 2020, 134: 104040

[8] G. Zhang, Z. Yang, and W. Liu, Blockchain-based privacy preserving e-health system for healthcare data in cloud. Computer Networks, 2022, 203: 108586

[9] F. Yahmed and M. Abid, "Trust Execution Environment and Multi-party Computation for Blockchain e-Health Systems." International Conference on Smart Homes and Health Telematics. Springer, Cham, 2020.

[10] F. Michèle, Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?, Panel for the Future of Science and Technology EPRS | European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 634.445 – July 2019 ENEPRS

[11] M. R. Yuce and J. Khan, eds. Wireless body area networks: technology, implementation, and applications. CRC Press, 2011.

[12] B. Arunkumar and G. Kousalya, "Blockchain-Based Decentralized and Secure Lightweight E-Health System for Electronic Health Records." Intelligent Systems, Technologies and Applications. Springer, Singapore, 2020. 273-289

[13]. L. Hirtan, P. Krawiec, C. Dobre, and J. M. Batalla, Blockchain-based approach for e-health data access management with privacy protection. In: 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). IEEE, 2019. p. 1-7.

[14]. T. Hyla and J. Pejas, eHealth integrity model based on permissioned blockchain. Future Internet, 2019, 11.3: 76.

[15]. L. Xu, A. Bagula, O. Isafiade, K. Ma, and T. Chiwewe, Design of a Credible Blockchain-Based E-Health Records (CB-EHRS) Platform. In: 2019 ITU Kaleidoscope: ICT for Health: Networks, Standards and Innovation (ITU K). IEEE, 2019. p. 1-8.

[16]. B. Assiri, Using Leader Election and Blockchain in E-Health, Advances in Science, Technology and Engineering Systems Journal, vol. 5, no. 3, pp. 46-54