Karaarslan E, Konacaklı E. (2021). Decentralized solutions for data collection and privacy in healthcare. In D. Gupta, S. Bhattacharya, U. Kose, and Bao Le Nguyen (Eds.) Artificial intelligence for data-driven medical diagnosis. De Gruyter. ISBN: 978-3110667813.

Decentralized Solutions for Data Collection and Privacy in Healthcare

Enis KARAARSLAN:
Assistant Professor, Mugla Sitki Kocman University, Department of Computer Engineering, Mugla, Turkey
enis.karaarslan@mu.edu.tr

Enis KONACAKLI:
Eskisehir Technical University, Department of Computer Engineering, Eskisehir, Turkey
enisk@eskisehir.edu.tr
,

Preface

Using artificial intelligence for data-driven medical diagnosis requires processing a wide variety and massive amounts of medical data collected from different resources. Resilience, controllability, and privacy of the medical data are the most important concerns for enabling AI-based data-driven medical diagnosis. Health data storage and its security and privacy requirements emerge as one of the most important challenges. The privacy concerns and lack of trust in the system became the main barrier for collecting and storing personal medical data. The patient should be given the data ownership and the track of the collected data should be kept. The privacy and security requirements of this data can be covered by using decentralized solutions. Decentralized solutions give us the opportunity of removing the intermediaries and establish trust between peers. This chapter aims to summarize the current studies and their possible impacts on the health industry and medical studies. Possible future uses of integrating blockchain with AI are given. AI can also be used to solve the challenges in blockchain and this chapter will also address some solutions. Multi-Platform Interoperable Scalable Architecture (MPISA) model for healthcare data sharing is proposed.

Keywords: Distributed ledger technology, blockchain, medical data, AI, digital twins, IoMT.

1 Introduction

The use of artificial intelligence for data-driven medical diagnosis requires the processing of massive amounts of medical data. A wide variety of data is collected from different resources such as electronic medical records, clinical experiments, genomic data, and various (mobile, wearable, Internet of objects) devices. People use wearable and mobile devices that monitor their health information. The companies which produce these products collect this data in their data centers. Hospitals or alike keep patient records. These records are shared between various information systems of the hospitals, these systems and also with many other institutions (Karaarslan et al., 2015). These data can be used for improving the quality of treatment processes and reducing treatment costs. This data can also be used for research purposes.

Resilience, controllability, and privacy of the medical data are the most important concerns for enabling AI-based data-driven medical diagnosis. The patient can be given the data ownership; the consent management gives the patient the right to share the data by his/her own wish. It is also important to keep track and control of the collected data. Health data storage and its security and privacy requirements became one of the challenges as the privacy concerns and lack of trust in the system is the main barrier in obtaining and storing such data.

The data integrity, confidentiality, security and privacy of the data should be carefully considered while providing access to healthcare information. Only authorized people should have access to the information. It is important to monitor where and how this information is kept, and how it is shared. (Karaarslan, 2019).

We cannot be sure of any authorization and access control system that exists in the medical information systems. We are aware of serious patient information access incidents (HHS, 2019) which shows that the patient information can be accessed easily by insiders or external users. The extent of this risk can be best understood from the list of incidents of security violations in the American healthcare system. These violations are reported by the HHS office for civil rights. According to a more detailed report examining unauthorized access to health data (Protenus, 2019), more than 15 million patient records are breached in America in 2018. There were 503 health data breaches, 417 of which we have detailed information. Hackers gained 2.65 million patient records from a health system company only in one incident. There is one incident where one insider continued snooping patient records for 15 years without being caught. The discovery of such incidents takes a long time, at an average of 255 days (Protenus, 2019).

Health information contains critical information that has the potential to affect national security. The demographic intelligence of a region or a society can be obtained with this information. This health data can be used in social engineering attacks, which is the first stage of any cyber attack. This information can be used to govern people's behavior, or even to attack political targets (Karaarslan, 2019).

Privacy is a misunderstood concept. Personal information about your private life should only be available to the people you approve of. That means; you should control how your data is shared and by whom. The right to private life is a fundamental right protected by international conventions (Korkmaz, 2014). The legislation is not sufficient to protect privacy, so privacy protection technologies should be used (Karaarslan et al., 2014).

Frauds in medical devices and drugs can reach serious proportions. According to the World Health Organization's report (WHO, 2017), 10% of medicinal products (especially in developing countries) are either non-standard or counterfeit. Such frauds and risks in developing countries are discussed in detail in (Glass, 2014). Counterfeit drugs and devices can lead to serious health problems (Karaarslan, 2019).

There is a need for security services that provide trust between different parties (institutions, individuals … etc) without using any intermediaries. Decentralized solutions can be used to develop autonomous systems which satisfy the privacy and security requirements of the medical information systems. Blockchain and its derivatives can be used as a distributed ledger technologies for the solution.

This chapter aims to summarize the current studies and their possible impacts on the health industry and medical studies. Possible future uses of integrating blockchain with AI are given. AI can also be used to solve the challenges in blockchain and this chapter will also address some solutions. Multi-Platform Interoperable Scalable Architecture (MPISA) model for healthcare data sharing is proposed.

This chapter aims to summarize the current studies and their possible impacts on the health industry and medical studies. We start with a brief explanation of the need for data privacy and security need in healthcare and AI in the introduction. Decentralized technologies are described in section two. Blockchain-based healthcare systems are given in section three. The benefits of integrating blockchain with AI will be given in section four. The implementation of our MPISA model in healthcare is given in section five.

2 Decentralized Technologies

Legacy Legacy systems use client-server architecture, where there is a central node (server) which gives a service. These legacy systems may also have backup servers or more than one server to make this architecture distributed. Decentralized technologies propose solutions where each node can act as a server or a client at the same time. These solutions work as peer-to-peer (P2P), which allows direct communication between nodes (Karaarslan & Adiguzel, 2018). They do not depend on a central node and establish trust without using any intermediary. Solutions that do not need trusted third parties (banks, notary, etc) can be developed. This section continues with a brief explanation of the blockchain technology and its characteristics. Then the security services of the blockchain are explained.

2.1 Blockchain Technology

Blockchain is a (semi-)decentralized technology that is used to keep a list of records. We are using the term (semi-) decentralized because some implementations can use mining pools or some master nodes, which prevent the system to be fully decentralized. Bitcoin cryptocurrency is a live example of this technology. Records contain information about transactions. The transaction can also include program code, which is used to make the processes autonomous, increase efficiency and speed. This autonomous code was firstly introduced by the Ethereum framework and called a "smart contract". Other frameworks may call it differently, such as "chain code" in the Hyperledger Fabric framework. Decentralized applications (DAPP) are developed to use this technology efficiently (Karaarslan & Adiguzel, 2018).

A data structure called block is used to store multiple records in a time period. Cryptographic techniques are used to link each block to the previous block. This forms a chain structure, which is kept as a registry, called the ledger. The ledger is kept distributed in several devices (nodes) that are connected to each other by P2P protocols. This is called distributed ledger technology (DLT).

The records are validated by the validator nodes and then collected to form a new block. The difference between various blockchain implementations is mainly based on the anonymity and trustworthiness of the validator node. This is shown in Fig. 1 (Gür et al., 2019). Permission less means that the validator nodes can join the network without getting any permission. The validator nodes may need to get permission to join the network, which makes the system permissioned. The ledger may have open read access to everyone, which makes it public. It is private otherwise and also hybrid implementations are also possible.

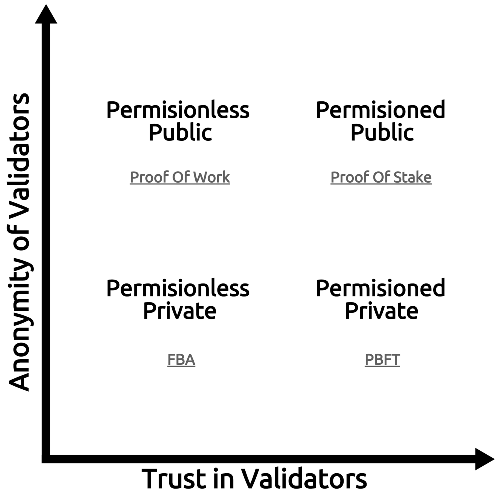

Fig. 1: Blockchain implementation types per anonymity/trust of validators

Consensus protocols are used to have a common decision on the process. Different consensus protocols are being proposed which ensure the proper usage of the system. The consensus process may involve an exhaustive process depending on the type of the validator node.

Cryptocurrency implementations mostly use permissionless and anonymous validators called miners. As the trust in the validator is low, proof of work (PoW) consensus protocol is which requires high energy and time-consuming operations (Gür et al., 2019). Other consensus protocols such as proof of stake (PoS) can be used which consume less energy and is faster than PoW (Zheng et al., 2018). The users are anonymous or pseudonymous in cryptocurrency implementations. The ledger is kept public in cryptocurrency implementations, which aim to keep the transactions transparent. All the transactions can be queried through web interfaces.

Enterprise implementations have different characteristics and different needs. Different parties deploy validator nodes. Proof of Authority (PoA), practical byzantine fault tolerance (PBFT) and alike consensus protocols, which don't need exhaustive processes, can be used as the validator nodes are identified (Zheng et al., 2018). The validators are permissioned and mostly private/public blockchains are used.

Hybrid blockchain implementations are possible where different types of implementations work together. Multiple chains can be used where public and private ledgers are used together. Multiple organizations can share information privately with each other by using federated (consortium) blockchain.

The records are immutable, which means that it is really hard to change without being noticed. The blockchain system ensures that the records are unmodifiable and inerasable (White et al., 2017). The system has no owner, no administrator. Trust is ensured with its being autonomous.

Organizations may question if they need a blockchain solution or not. This process is shown in Fig. 2 (Wüst & Gervais, 2018). Blockchain solution makes meaning when the solution needs a common dataset that is to be reachable and modifiable by more than one party. Normally this requires a trusted third party in legacy systems. The blockchain solution offers trust without using any intermediaries. The records of all activities are also kept which helps in auditing.

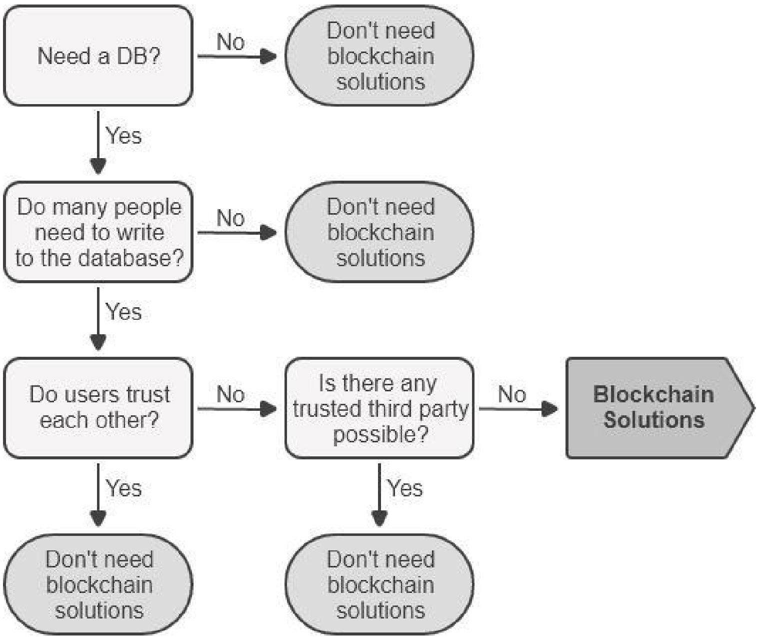
Need a DB?
No
Don't need blockchain solutions
Yes
Do many people need to write to the database?
No
Don't need blockchain solutions
Yes
Do users trust each other?
No
Is there any trusted third party possible?
No
Blockchain Solutions
Yes
Don't need blockchain solutions
Yes
Don't need blockchain solutions

Fig. 2: Do you need a blockchain?

A blockchain-based system can be developed in the following ways (from the easiest to the hardest):

- Develop it in an existent blockchain infrastructure (such as Ethereum)
- Get a blockchain as a service (BaaS) cloud service and develop by using it
- Install blockchain framework (such as Hyperledger Fabric) on your nodes and develop on it
- Clone an existent blockchain framework (such as Ethereum), deploy it on your nodes and develop on it
- Develop your own blockchain solution

IEEE Blockchain Initiative (IEEE, 2019), ISO/TC 307 technical committee (ISO, 2019), W3C community group (W3C, 2019) are the new standardization efforts (Mohan, 2019).

2.2 Security Services of the Blockchain

The blockchain system runs according to the software code and the protocol autonomously. There is no administrator of the system. It should be noted that all full nodes (the nodes which hold the whole ledger) of the system should run the same version of the blockchain software. The rules they have to follow are the same. Any change in the system will require a consensus of the community and a software update. This means that the update details are discussed and accepted before the installation. If some nodes are not updated, they are not a part of that blockchain system anymore.
The availability, data integrity and fault tolerance security services are provided by design with the blockchain technology. Privacy is not a feature by design and different levels of privacy is observed in different implementations (Halpin & Piekarska, 2017; Feng et al., 2019). The level of these security services are compared with legacy systems and are given in Table 1 (Bozic et al., 2016; Karaarslan, 2019).

Tab. 1: Comparison of the security services

	Blockchain	**Central Database**	**Distributed Da-tabase**
Integrity	High	Average	Average
Availability	High	Low	Average
Fault tolerance	High	Low	High
Privacy	Variable*	High	Average
** Privacy is not by design. Mainly depends on the implementation*			

Integrity means that the data is the same as it was recorded and its reliability can be affirmed. The design of the ledger ensures the integrity of the data. The blockchain structure is given in Fig. 3. The system uses one-way hash functions

(SHA-256, Keccak-256 … etc) which form the fingerprint of the input data. Merkle tree calculation (MTC) is used to have a cumulative hash value of the transactions in the block. The figure shows the root hash value (Tx_Root) calculation for the four-transaction scenario (Nakamoto, 2008). Each block also has the hash value of the previous one (prev_hash) and this makes each block connected to the previous ones. This data structure makes the binding so strong that, when an attacker wants to change any transaction in block n, that block and also the blocks starting from that block till the last block has to be modified. This also requires being in consensus with all other nodes and making them change their records. The attacker has to be selected in the node selection of each block and this requires that the attacker should have at least %51 of the available Graphical Processor Unit (GPU) computing power of the whole blockchain system when PoW consensus algorithm is used. The system records the selected node of each block in the ledger and this will also help in the detection of such an attack attempt (Karaarslan & Akbaş, 2016).

The availability means the system is up and giving service at all times. This feature mainly depends on the number and also geographically and network distribution of the nodes. The attacker needs to take control of the majority of the nodes when the PoW consensus protocol is used. The number of nodes will make this type of attack harder to implement. Deploying the nodes in different networks will make the system stronger against the distributed denial of service (DDOS) attacks. Fault tolerance is the ability to correct any errors and misuse. This feature is realized by the consensus protocols.

There is a misunderstanding that the privacy level is low in blockchain systems. The transparency in public ledgers is used to prevent any possible misuse (Ölmez & Karaarslan, 2019). Public records of the cryptocurrency systems also do not keep any private data. Private data shouldn't be kept in the ledger even when private ledgers are used. Private data can be kept in the legacy systems and also in the cloud. Encryption should be used when some fields of the records are kept on the chain.

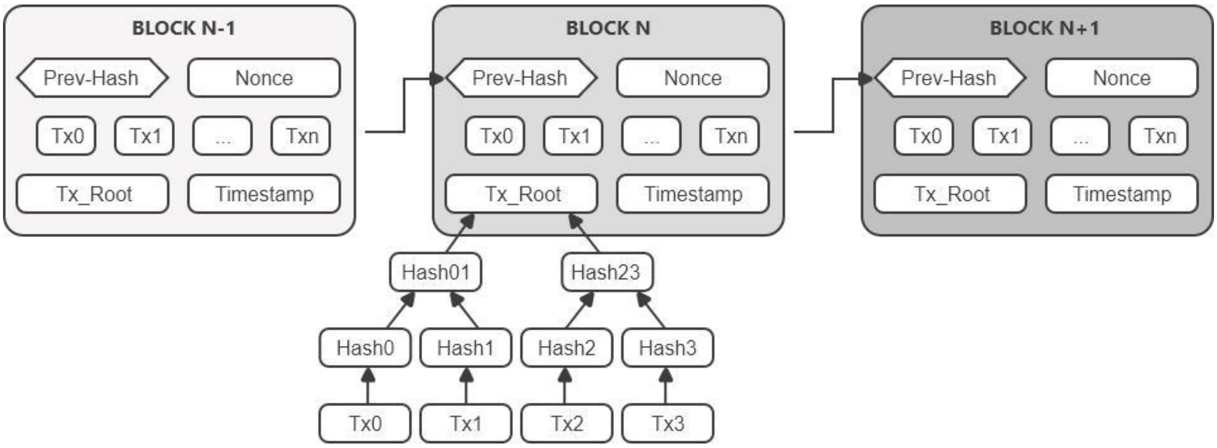

Fig. 3: Blockchain structure

3 Blockchain-based Healthcare Systems

Blockchain-based health systems have begun to emerge and we had given a comprehensive list of studies in a previous book chapter (Karaarslan, 2019). Estonia and the United States are the first countries that give importance to blockchain-based health systems.

Estonia can be called a pioneer in the e-government applications and also a pioneer in the e-health systems. Estonia has already established a proper legal infrastructure and policy for their e-government information system (https://e-estonia.com). Estonian blockchain-based health information system is a great sample for demonstrating the benefits of blockchain in health data management. Estonia uses the blockchain implementations of the Guardtime company. Estonia secures health records of over a million citizens. This system allows citizens, healthcare companies and health insurance companies to access all data related to health treatments (Heston, 2017).

There is a planned research and development process on blockchain technology in healthcare in the United States. The National Health Information Technology Coordinator (ONC) of the Ministry of Health first introduced the issue of "Using Blockchain in Health Informatics and Health-Related Research" in July 2016. The American Food and Drug Administration (FDA) and IBM Watson Health artificial intelligence unit signed a two-year joint development agreement on the secure sharing of patient data using blockchain technology for medical research and other purposes. Oncology-related information will be focused on this project (Mearian, 2017). The American Center for Disease

Control and Prevention (CDC) considers this technology to be meaningful, especially in times of epidemic diseases. CDC has also announced an additional agreement with IBM Watson Health to investigate the use of the blockchain to store and exchange medical data (Zhao, 2017).

There are new working groups and new standardization efforts. Phuse (https://www.phuse.eu/) is an independent and non-profit organization for clinical data scientists. It has a blockchain working group where usage of blockchain in pharma and healthcare is being explored. IEEE Blockchain Initiative has some standards activities for healthcare and shows the interest in the field (IEEE, 2019):

- "Blockchain for Clinical Trials" forum: IEEE initiative to build consensus on optimizing clinical trials and enhancing patient safety
- "Pharma Supply Blockchain" Forum: Working on advancing blockchain adoption within the pharmaceutical industry
- "Advancing HealthTech for Humanity" virtual blockchain workshop
- Released findings from the first detailed study of blockchain adoption in the pharmaceutical enterprise

Selected implementation areas in healthcare are given as follows with sample implementations:

- Clinical Trials: The data transparency of the clinical trials can be improved by making the process autonomous. This can be accomplished by using smart contracts and blockchain (Nugent et al., 2016).
- Fraud detection and prevention: Immutable records can be used to improve data auditing (Heston, 2017). Blockchain systems can be used to detect and prevent fraud in healthcare systems. The authenticity of medical devices and drug supply chain can be guaranteed. IBM proposes the use of crypto-anchor and blockchain technologies together to achieve this. Crypto-anchor is a new cryptographic method that is designed as digital signatures integrated into products and cannot be changed (IBM, 2018; Balagurusamy et al., 2019).
- Securing health data: Unauthorized modification of data is one of the major security risks. Systems can be developed to ensure data integrity and prevent unauthorized changes. Immutable, time-stamped and verifiable health records can be kept and shared between the parties (Wagenen, 2018). A security architecture based on blockchain for the Internet of Medical Things (IoMT) devices is proposed in a recent study (Dilawar et al., 2019).
- Eliminating duplicate data: Common data can be shared between parties. This will also solve the inconsistencies (Houlding D., 2019). There are attempts like (Azaria et al., 2016; Peterson et al., 2016) that propose blockchain-based solutions for sharing medical data. Health Nexus WEBLINK: https://github.com/Health-Nexus is an attempt (Hendren & Kuzmeskas, 2017) which is based on Ethereum to provide a blockchain system for healthcare.
- Controlling your own data: Healthbank proposes a system where users can store and manage their own data (Mettler, 2016).
- Sharing medical data: Sharing medical data can also be encouraged; Patients can give permission on the use of health data for medical research and receive a payment in return (Mettler, 2016; Gammon, 2018).
- Track medical data: SimplyVital Health company is using Nexus blockchain network and allowing patients to track their medical records (Ravindranath, 2018). Tierion uses the chain point WEBLINK: https://chainpoint.org open standard to form timestamp evidence of the data added to the blockchain. Philips healthcare solutions work with Tierion to implement such a solution in healthcare systems.
- Cloud data management: The data can be tracked in the cloud (Yue, 2017), data integrity can be provided in the cloud (Gaetani et al., 2017).

Such a system will save costs for healthcare providers. Immutable records can be used to improve data auditing. Medical care costs can be decreased when frauds are prevented and better insurance claims are issued (Heston, 2017). It is claimed that 100 billion dollar savings are possible in the health care industry by 2025 (Benartzi G., 2019).

We can design the blockchain and AI system in a layered structure as shown in Fig. 4. Each layer can be used in healthcare with the following functions (Houlding, 2017):

- Layer 0: Healthcare data is kept in silos and shared little. There is massive untapped potential.
- Layer 1: Sharing health data securely on company-to-company e-commerce (B2B) networks is implemented in this layer. Applications that run in this layer are the solutions that will complement the existing systems. A small but sufficient amount of data will be shared to meet usage requirements. Information security and interoperability of different systems are going to be aimed.
- Layer 2: Smart contracts are used for automated processes and increase efficiency and speed.
- Layer 3: Trading and incentive systems can be implemented using crypto coins and tokens.
- Layer 4: Machine learning and artificial intelligence can be used to add new insights and values. Blockchain can be used for AI; AI can be used for blockchain. Interesting usage of blockchain is to track how AI works and be sure that it works as intended (Corea, 2017).

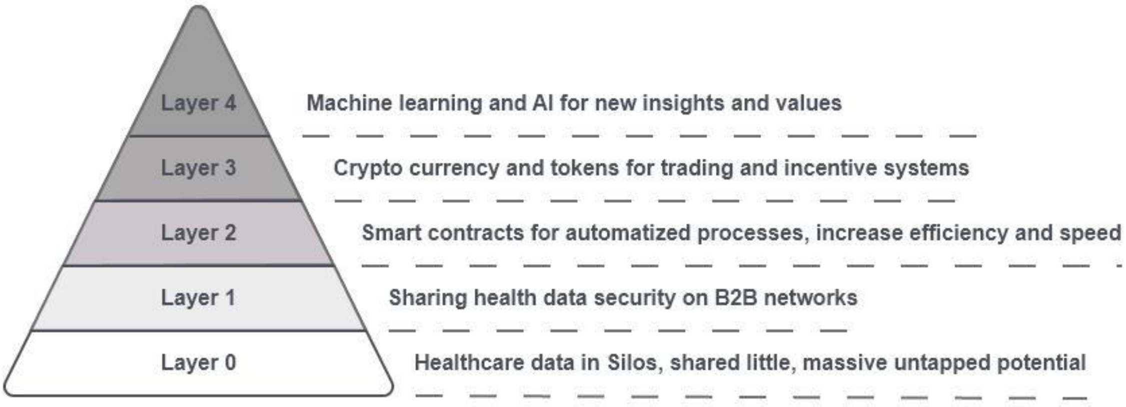
Layer 4
Machine learning and AI for new insights and values
Layer 3
Crypto currency and tokens for trading and incentive systems
Layer 2
Smart contracts for automatized processes, increase efficiency and speed
Layer 1
Sharing health data security on B2B networks
Layer 0
Healthcare data in Silos, shared little, massive untapped potential

Fig. 4: The layered design of blockchain and AI for health care

Ravindranath, referring to the views of the US HHS authorities; stated that the health sector is not currently ready for the blockchain technology. He claimed that the technology is not sufficiently understood and it is not that clear how to use it in health care (Ravindranath, 2018). As stated in another publication (Radanović & Likić, 2018), it is clear that we should do awareness-raising about the potential of this transformer technology in the field of healthcare. The academic studies are not enough in this field. More studies and experiments should be performed in order to see the contribution of technology to healthcare. This book chapter is also an attempt to clarify misunderstandings and describe how this technology can be used by and with AI.

4 The need for AI and Blockchain Cowork

Current developments of AI technology ought to be attributed to the recent advances in the processing powers. Basically, it is a discipline that aims to enable computers to learn and make decent predictions as humans. Machine learning and deep learning are remarkable techniques that can be used to enable AI solutions. Deep learning is the latest machine learning algorithm that can be applied to very large data sets and supports advanced decision-making processes (Najafabadi et al., 2015). Detection of a disease can be much faster and easier with these classification algorithms and prediction techniques in healthcare (Wahl et al., 2018). The basic ingredients of machine learning and deep learning are data, model selection, and training. These processes require a lot of real patient's medical information about a specific disease to discern generalizations and patterns, which are then used to offer a prediction. Health data is confidential and this data can not be shared publicly by law. Professionals must get permission for the collection and usage of this data (Krittanawong et al., 2018). This permission is often for a very limited period of time (Kin, 2019). These conditions can lead to obtaining fewer data than the required amount for training the AI algorithms. If AI algorithms cannot be trained properly, their prediction mechanisms cannot work sufficiently to give the expected solutions (European Parliament, 2018). Thus, legitimate legal and technical regulations have to be established to enable the processing of huge datasets while protecting individual rights.

Blockchain secured medical data can overcome the lack of data management problems. AI blockchain integration also has the potential to provide solutions and has benefits in many subjects. Benefits of integrating blockchain with AI can be summarized as (Dinh & Thai, 2018; Salah et.al., 2019):

- Enhanced data security
- Improved trust
- Privacy-preserving personalization
- Collective decision making
- Decentralized intelligence
- Scalable blockchains
- High efficiency

Systems that are using blockchain technology ensure the highest capability of consent management, security, immutability, transparency, unchangeability, and irremovability. AI blockchain collaborated systems have the potential to create the world's most reliable technology-enabled resilience decision-making system that will produce decent insights and predictions for the health sector (Balthazar et al., 2018).

4.1 Blockchain for AI

One of the biggest challenges in data science today is the collection of a proper dataset, which can be used to train AI algorithms. Blockchain can boost the capability of AI in novel ways and in different areas. This technology is the ideal solution for protecting and sharing sensitive data. All important data is secured within a successively encrypted ledger, and distributed within the peers, which each of them acts as the separate servers of a large private network. All actions leave an unchangeable and irrevocable secure trail. Blockchain and AI have the capacity to add revolutionary value to medical analysis and healthcare sectors by advancing the whole process, improving predictive analytics techniques and providing the patients new means to manage their own data (Mamoshina et al., 2018). This merger may help patients to monetize their private personal data with incentive benefits to have continuous monitoring of their health. After enabling blockchain secured private network for medical AI systems, personalized medical prescriptions will be possible by detailing records of patients' health history for health professionals, with the help of the data acquired not only from patients past clinical diagnosis story but also the data collected from various medical sensors such as smartwatches, scanning preexisting health conditions in daily routine (Woods, 2018).

The benefits of AI and Blockchain cowork scenario is shown in Figure 5 (Salah et al., 2019). Such a system will allow many parties such as patients, drug manufacturers, lab technicians, medical researchers, physician and radiologists to share data simultaneously in a secure and trusted environment. Cryptocurrency implementations are available and will probably be used after the regulations. IPFS will be used to store MRI data securely on the cloud. Only the hash values will be kept as a record. Other benefits will be given in the following sections. The benefits of using blockchain architecture for AI technology for medical information systems can be given as follows:

- Improved Trust, Collective Decision Making and Use of Diverse Data Sets
- Autonomous Security, Protection and Storage
- Ensure Proper Consent Management
- Data Monetization

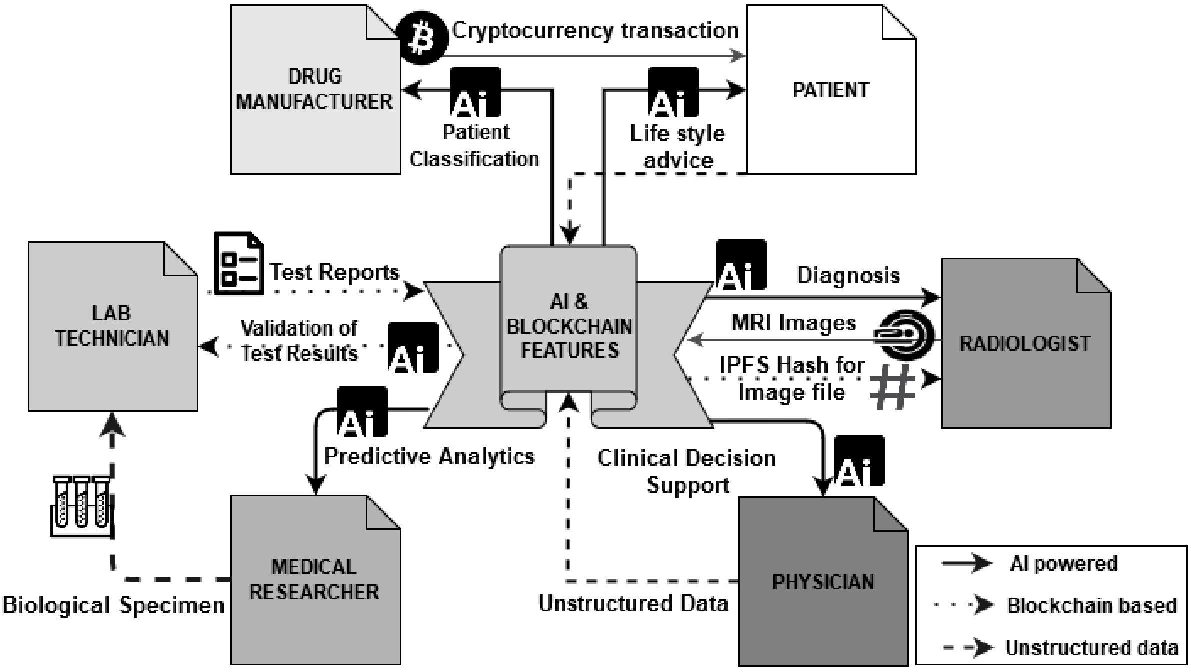

Fig. 5: AI & Blockchain-based Scenario

4.1.1 Improved Trust, Collective Decision Making and Use of Diverse Data Sets

Unlike legacy systems, blockchain technology can create suburbanized, secure transparent networks that can be publicly accessed. Such systems will allow different AI agents to communicate and interact with each other and run on distinct datasets concurrently. Creating such diverse datasets with blockchain technology will enable collective decision-making applications on decentralized architectures. The IoMT systems, which are the agents responsible to collect data about patients' realtime health conditions using their sensors, can be made to trust each other without using any intermediaries. This will also increase machine-to-machine interaction and allows them to share data directly (Campbell, 2018).

AI service providers can enrich the data set with successful diagnosis achievements. This will optimize the machine learning and the precision of the AI models. Health professionals could compare their diagnoses with the results published on the blockchain. As the service providers are incentivized for every accurate diagnosis, they are bound to improve the precision of their machine learning algorithms. The whole process will improve trust and collective decision making. This will create a snowball effect on the diagnosis which will enhance prediction while shortening the diagnosis time (Peterson et al., 2016). This renovation may also benefit the radiology and CT scan images (Xu et al., 2014). These big files can be stored securely in the cloud. The improved trust and collective decision making will enhance data science analytics. This can be used to find out the next course of treatment by interpreting the outcomes.

The ability to create and manage diverse data sets with blockchain boosted AI solutions can play a significant role in healthcare assistance for robotic systems (Lotfi et al., 2018). Medical assistive robots can turn into secure, resilient, smart medical supervisory systems, with enabled trust between peers. Socially assistive robots can be one of the most promising technologies that can act as a medical information help center interface. These can be used to determine the needs of the aged or seriously ill patients, where there is a need for professional assistance and supervision at all times.

4.1.2 **Autonomous Security, Protection and Storage**

AI techniques are efficient for classifying and analyzing large datasets with huge volumes of raw medical data. This data is not only fed by clinical diagnosis records but also from connected sensors of the IoMT devices. Storage, security, and protection of this sensitive data is an important concern for the patients and AI service providers (Leeming et al., 2018). It is also risky to trust a robotic agents' decisions and expertise in the medical field since these devices are also vulnerable to attacks and open to manipulation. All medical records should be ensured to be accurate and tamper-proof during critical decision-making processes.

Blockchain technology is an ideal solution for the autonomous security, protection, and storage of highly sensitive, private medical data. Encrypted data can be stored and separation of personal data from medical data can be ensured. This will also eliminate the confidentiality risk from the outsider attacks and also possible insider attacks including the technical administrators' accessibility rights.

All actions leave unchangeable and irremovable records on the blockchain. This may benefit AI architectures by enabling the traceability of predictions and reasons for the decisions made by AI thinking processes. This will give a chance to advance the algorithms of current AI models. AI decision-making processes can also be monitored and logged and can be traced back to investigations if needed. The information can be securely stored on a distributed, decentralized and immutable patient ledger. Also, a graph-based relationship database can be formulated for storing unstructured data and the relationships amongst the data. Blockchain can implement an invincible record of the complete diagnosis reports of both service providers and hospitals.

The merger of blockchain and AI technology could personalize medicine, quadrate treatments and health recommendations based on a patient's medical history, genetic lineage, stress levels, place of residence (atmospheric conditions during record), past medical conditions.

4.1.3 **Ensure Proper Consent Management**

Digital health care systems share medical information between different healthcare providers to create a common medical record that every patient can access online. Thus, one of the main challenges for digital healthcare systems is to facilitate transparency and interoperability of the data while satisfying the expectations users' privacy and security concerns. Consent management is basically a term attributed to a process or set of policies for allowing users to determine which health information to share, and the parties to give access permission (IBM, 2020). This process should be implemented by establishing a transparent health information sharing platform between the related peers.

Blockchain models provide opportunities to solve the well-known challenges of the users; consent management, privacy, and confidentiality. These systems have the ability to establish semi-private and private networks that give the clients total control of their own data while enabling personalized secure access to their medical records. Patients will be able to hide or share their personal data with specific health professionals. This is also available in some legacy systems, but the patients are only given limited access control on sharing.

The separation of the personal information(name, parents' information, DNA records, blood type, etc.) from the medical data (health background, past illnesses, CT records, etc.) can be ensured by smart codes that enable the system to run autonomously (Mamoshina et al., 2019).

Consent management is important for the AI service providers and researchers since these structures enable the collection of sufficient data resources with proper consent management. Blockchain architectures facilitate to reach and use of medical information and ensures privacy by establishing consent management. Blockchain systems will be promising technologies for not only meeting the requirements of privacy concerns but also conforming to the information governance rules (such as EU's General Data Protection Regulations (GDPR) on data science programs), organizational needs and priorities, public expectations.

4.1.4 Data Monetization

Getting enough quantities of data and validation of that information is important for the precision of AI models. Millions of mammograms are needed to detect breast cancer. However, this data can not be obtained because of privacy laws. Using cryptocurrencies for monetizing medical data may be a solution. Getting a profit from it can be a motivation for the patients to share their private data willingly (Maxmen, 2018).

Developing and feeding AI datasets is very expensive for corporations that need private medical data, who want to make a profit from AI business. Creating an efficient dataset from raw data is an extremely time-consuming process that needs long training hours. An example pricing for such a research service is 105 Eur per hour (Statistics Finland, 2020). Editing unprocessed data needs high-performance computing (HPC) for processing it. This means extra IT and labor costs for service providers, and data processing is being priced at an hourly rate. Blockchain-powered systems will let AI service providers buy raw data directly from its source (patients). This process has the potential to decrease the total health expenses of the service providers. The system can also be made to allow patients to make their health payments by using their data profits. This process may also be used by governments to decrease total health expenses.

4.2 AI for Blockchain

Conventional blockchain systems come up with a bunch of challenges that limit the use of border capabilities of this technology. The core challenges can be summarized as (Karaarslan & Konacakli, 2019):

- High energy consumption
- Slow transaction and confirmation times which causes delays
- Scalability
- Interoperability

Enabling sufficient user privacy may be assumed as another challenge, depending on the type of blockchain protocol. Cryptology and security of ledger against high processing powers is a new upcoming challenge in the age of quantum computing.

AI has the capacity to burst the power of blockchain and totally change the administration of blockchain networks to make them more efficient. A smart consensus protocol, which has the ability of thinking and making its own decisions, can manage its blockchain system better than the conventional methods. Thus, merging AI algorithms with blockchain structures will help the current blockchain architecture in managing its confirmation, authorization and transaction processes. AI collaboration with effective management of these processes will be able to benefit the issues written in subsections below.

4.2.1 Enhanced energy consumption and smart computing

PoW consensus protocol uses nodes called miners. AI can help improve computations to reduce the miner responsibility which can result in lower latency and faster transactions. The energy spent by the miners could also be reduced if AI machines replace the work done by miners (Sgantzos, 2019).

As the blockchain ledger increases with every transaction, AI algorithms can be used for optimizing data storage. Some blockchain protocols support pruning that allowing users to delete raw data blocks after the entire ledger has been down-loaded and validated, keeping only a small subset of the data. This process is a very effective method for the management of the length of the total ledger. Machine learning models have the ability to make pruning for the unwanted breaches of decision trees (Hoare, 2020). A promising future usage is using AI blockchain merger structures to make data pruning automatically. Thus, AI favors data storage containers, lessens CPU and GPU used for the validation processes and reduces energy consumption. AI-based systems can provide even new decentralized learning solutions such as federated learning or new data-sharing techniques that can make the system much more efficient.

4.2.2 **Enhanced data security**

The addition of AI thinking capability to blockchain technology has the potential to come up with safer applications and to implement new patterns created by AI on the decentralized infrastructures. AI algorithms have the ability to predict fraud in the transactions and can decide on further steps like blocking or investigation. This will increase the efficiency of the transactions and confirmation processes of the overall system. This will eventually speed up the validation processes.

AI and blockchain integration can also increase system security and provide a stronger defense against the attacks. Blockchain architecture can be set to automatically remove bugs and fraudulent data sets effectively with the help of the AI algorithms. AI algorithms can create automation among the collected data while ensuring trust and transparency between peers. AI algorithms can be used to enhance the cryptographic algorithms that will handle the emerging security challenges of post-quantum computing.

All steps from data entry to the predictions can be observed with appropriate AI-powered blockchain programming. It can be monitored whether data had tampered or not. This will build trust within the predictions drawn by the AI schemes.

5 MPISA for Healthcare Data Sharing

Multi-Platform Interoperable Scalable Architecture (MPISA) model which we have described in (Karaarslan & Konacakli, 2019) involves integrating multiple platforms and is an attempt to solve the scalability and interoperability issues. The main goal when applying MPISA to healthcare systems should be sharing the common data in the blockchain and leaving the private data in data silos of the organization. This is shown in Fig 6 (Houlding D., 2019).

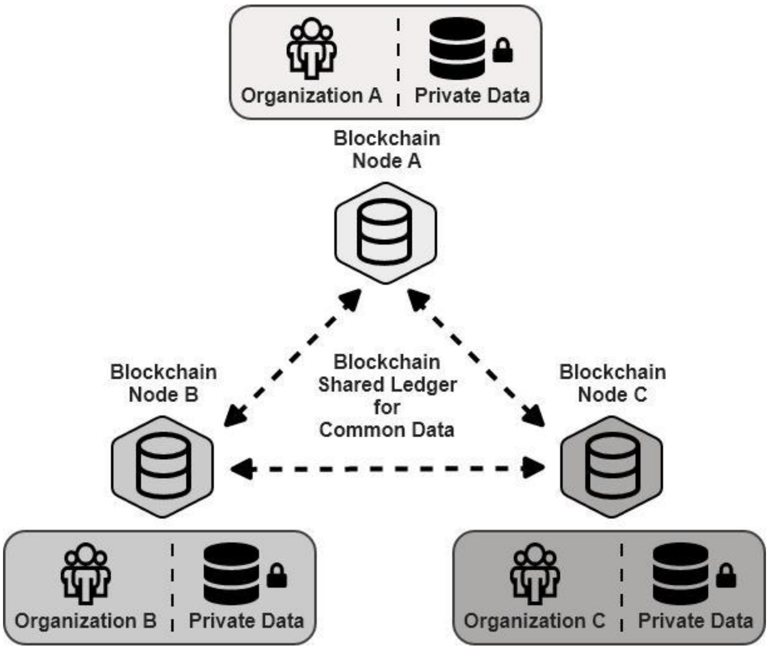

Fig. 6: Blockchain architecture for sharing common Data

The healthcare blockchain system can be multi-chain and each chain may serve different medical sectors or the government. There should also be some interoperability platforms which interconnect these chains and the DID (Decentralized identity) system (Bakre et.al., 2017). A simplified implementation of this architecture is shown in Figure 7. The legacy healthcare system and legacy software implementation is still used. The integration to the decentralized world is implemented by the smart contracts which are added to the patient and health staff (doctor, nurse, lab technician … etc) applications. A usage scenario can be summarized as the following steps:

- Appointment request: The patient forms an appointment request using a mobile application in step 1. The appointment needs an ID check. The smart contract of the patient implements an ID check with the DID system which is shown in step 2. This process ends with a connection to the legacy hospital information system and getting an affirmation as shown in step 3.

- Health Service: Health staff and patients use the legacy information system in step 4. The smart contract of the patient implements the consent management that decides on which parts of the private data are to be shared with the health staff with which conditions. This step is shown in step 5 and that shared data is used by the smart contract of the healthcare professional in step 6. The outcomes of the treatment are recorded on the healthcare blockchain system in step 8. The protocol and privacy rules are implemented and ensured by the autonomous code. The data is kept on the cloud, only the reference to this data is kept on the blockchain.
- AI-based Healthcare analytics: AI-based analytics is implemented in the cloud by using the data in the blockchain and the cloud.

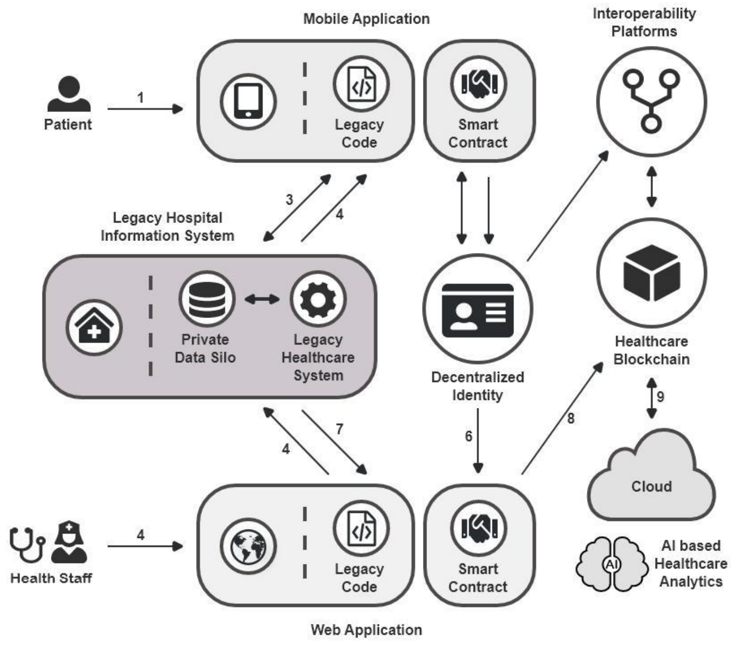

Fig. 7: Health service scenario with blockchain

6 Conclusion

There are several benefits of integrating blockchain with AI. This chapter summarized the current studies and their possible impacts on the health industry and medical studies. Data-driven medical diagnosis requires a wide variety of medical data collected from different resources. Data privacy and security for these medical data should be satisfied. The patient should have control of his/her data. Lack of trust in the system is the main barrier in obtaining and storing such medical data. Decentralized technologies can be used as solutions for these concerns.

Trusted autonomous systems can be developed for healthcare. Smart contracts and consensus protocols make these systems possible. Decentralized solutions give us the opportunity of removing the intermediaries and establish trust between peers. This technology also promises security services such as data integrity, availability and fault tolerance (Bozic et.al., 2016).

Blockchain technology will enable the sharing of medical data in a trusted way. Clinical trials and fraud detection in the pharmaceutical industry are the current popular implementation areas. Blockchain-based systems may help in mitigating these frauds (Bharadwaj, 2016). Records which show the user, time and details of any transaction can be kept on an immutable ledger. The transparency and visibility of the transactions will help in the detection of fraudulent data and will allow faster measures. Blockchain technology can be used for further improvement of audit processes and ensure compliance with the rules. These attempts are the proof of concept works of this technology, showing beyond doubt that it has a meaning as a solution.

Blockchain can be used for the AI, especially in forming a trusted environment of sharing data. Revolutionary changes are possible by advancing the whole process. AI blockchain collaborated systems have the potential to create the world's most reliable technology-enabled resilience decision-making system that will produce decent insights and predictions. The obtained data can be used to increase AI precision, broaden applicable treatments. Diagnoses can be made faster and more accurate. Predictive analytics can be improved and the patients can be given new means to manage their own data.

After enabling blockchain secured private network for medical AI systems, personalized medical prescriptions will be possible with using detailed records of the patients. That kind of system will allow many parties such as patients, drug manufacturers, lab technicians, medical researchers, physician and radiologists to share data simultaneously in a secure and trusted environment. An AI-Blockchain architecture has the potential to enable the monetization of private data and this can be used to decrease the total health expenses of the service providers. Blockchain establishes perfect infrastructure to achieve and facilitate to reach and use of medical information. It can be used to ensure privacy by establishing consent management. The ability to create and manage diverse data sets with blockchain boosted AI solutions can play a significant role in healthcare assistance with robotic systems.

AI blockchain cooperation has the capability to come up with safer applications. AI algorithms can predict fraud in the transactions and can decide on further steps such as blocking or investigation. This will increase the efficiency of the transactions and the confirmation processes of the overall system. This will also speed up the validation processes.

Multi-Platform Interoperable Scalable Architecture (MPISA) model for data sharing is applied to the healthcare and a use scenario is given. Blockchain can also be used to control AI and ensure that it works as it is intended.

However, decentralized solutions are not perfect. There are challenges to be solved with decentralized technologies. AI can help develop consensus protocols with lessening miner responsibilities. This will lead to lower latency and faster transactions. The energy spent by the miners will also be reduced. A promising future usage may be the ability to achieve automatic data pruning that will also optimize the efficiency of blockchain data storage schemes. AI can be used to strengthen enterprise blockchain implementations such as Hyperledger, Corium and Corda by optimizing their transaction and validation processes. AI technology can be a cutting edge technology that will strengthen blockchain technology against the power of quantum computing that will threaten the security of current cryptographic algorithms.

Future will probably bring implementations of digital twins in health care. All the data of the patients will be collected in the cloud and simultaneously updated with IoMT devices. Possible cures will firstly be tested on these digital twins. These systems and personalized medicine will be based on AI and will probably be protected with blockchain-based solutions.

Acknowledgements

We would like to thank MSKU Blockchain Research Group (http://wiki.netseclab.mu.edu.tr/index.php?title=MSKU_BcRG) member Cemal Dak for his contribution to the graphics used in this chapter.

Bibliography

Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. 2016, August. Medrec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data. 25-30. IEEE.

Balagurusamy, V., Cabral, C., Coomaraswami, S., Delamarche, E., Dillenberger, D., Dittmann, G., and Kumar, A. D. 2019. Crypto Anchors. IBM Journal of Research and Development.

Balthazar, P., Harri, P., Prater, A., and Safdar, N. M. 2018. Protecting your patients' interests in the era of big data, artificial intelligence, and predictive analytics. Journal of the American College of Radiology. 580-586.

Bakre A., Patil N. and Gupta S. 2017. Implementing decentralized digital identity using blockchain. International Journal of Engineering Technology Science and Research, 4(10), pp. 379-385

Benartzi G. 2019. Introducing Blockchain Impact Award Winner SimplyVital Health. Newsweek, https://www.newsweek.com/2019/03/08/blockchain-impact-award-winner-simplyvital-health-1339345.html

Bharadwaj S. 2016. Fraud Prevention in Healthcare using Blockchain, https://www.linkedin.com/pulse/fraud-prevention-healthcare-using-blockchain-saketh-bharadwaj/.

Bozic, N., Pujolle, G., and Secci, S. 2016, December. A tutorial on blockchain and applications to secure network control-planes. In 2016 3rd Smart Cloud Networks & Systems (SCNS) (pp. 1-8). IEEE.

Campbell, D. 2018. Combining AI and blockchain to push frontiers in health-care. http://www.macadamian.com/2018/03/16/combining-ai-and-blockchain-in-healthcare/, vol. online.

Corea F., 2017. The convergence of AI and Blockchain: what's the deal?. https://medium.com/@Francesco_AI/the-convergence-of-ai-and-blockchain-whats-the-deal-60c618e3accc

Dilawar, N., Rizwan, M., Ahmad, F., and Akram, S. 2019. Blockchain: Securing Internet of Medical Things (IoMT). Int J Adv Comput Sci Appl, 10(1).

Dinh, T. N., and Thai, M. T. 2018. Ai and blockchain: A disruptive integration. Computer, 51(9), 48-53.

European Parliament . 2018. Artificial Intelligence: Challenges for EU Citizens and Consumers, Briefing, IP/A/IMCO/2018-16, ISBN 978-92-846-4508-4, doi:10.2861/441665, QA-01-19-044-EN-N

Feng, Q., He, D., Zeadally, S., Khan, M. K., and Kumar, N. 2019. A survey on privacy protection in blockchain system. Journal of Network and Computer Applications, 126, 45-58.

Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., and Sassone, V. 2017. Blockchain-based database to ensure data integrity in cloud computing environments. In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy.

Gammon, K. 2018. Experimenting with blockchain: Can one technology boost both data integrity and patients' pocketbooks?.

Glass, B.D. 2014. Counterfeit drugs and medical devices in developing countries. Research and Reports in Tropical Medicine, 11-22.

Gür, A. Ö., Öksüzer, Ş., and Karaarslan, E. 2019, April. Blockchain based metering and billing system proposal with privacy protection for the electric network. In 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG) (pp. 204-208). IEEE.

Halpin, H., and Piekarska, M. 2017. Introduction to Security and Privacy on the Blockchain. In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 1-3). IEEE.

Hendren, L. and Kuzmeskas, K. 2018. Health Nexus (Version 1.0). https://crushcrypto.com/wp-content/uploads/2018/03/HLTH-Whitepaper.pdf

Heston, T. 2017. A Case Study in Blockchain Healthcare Innovation, Authorea Working Paper No AUTHOREA_213011_3643634. Available at SSRN: https://ssrn.com/abstract=3077455

HHS 2019 Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. U.S. Department of Health and Human Services (HHS) Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Hoare J. 2020. Machine Learning: Pruning Decision Trees. https://www.displayr.com/machine-learning-pruning-decision-trees/

Houlding D. 2019. A Data Centric View of Blockchain, https://www.linkedin.com/pulse/data-centric-view-blockchain-david-houlding-cissp-cipp/

IBM 2018. Five Innovations that will help change our lives within five years: Crypto-anchors and blockchain, http://research.ibm.com/5-in-5/crypto-anchors-and-blockchain/

IBM 2020. Overview of Consent Management, https://www.ibm.com/support/knowledgecenter/en/SSWSR9_11.6.0/com.ibm.mdmhs.overview.doc/consentmanagementoverview.html

IEEE 2019. IEEE Blockchain Standards. https://blockchain.ieee.org/standards

ISO . 2019. ISO/TC 307 technical committee on blockchain and distributed ledger technologies, https://www.iso.org/committee/6266604.html

Karaarslan, E., Eren, M.B., Koç, S. 2014. Çevrimiçi Mahremiyet: Teknik ve Hukuksal Durum İncelemesi [Online Privacy: Technical and Legal Situation Review], 19th Internet Conference, Istanbul, s.188-195.

Karaarslan, E., Ergin, A.M., Turğut, N., Kılıç, Ö. 2015. Elektronik Sağlık Kayıtlarının Gizlilik ve Mahremiyeti [Confidentiality and Privacy of Electronic Health Records], 20th Internet Conference, Istanbul, s.215-220.

Karaarslan, E., and Adiguzel, E. 2018. Blockchain Based DNS and PKI Solutions. IEEE Communications Standards Magazine, 2(3), 52-57.

Karaarslan E., and Akbaş, M.F. 2016. Blok Zinciri Tabanlı Siber Güvenlik Sistemleri [Blockchain Based Cyber Security Systems]. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Volume 3, Issue 2, Pages 16-21, DOI:10.18640/ubgmd.373297, http://dergipark.gov.tr/ubgmd/issue/33645/373297.

Karaarslan E. 2019. Usage of Blockchain Technology in the Health Sector [Sağlık Sektöründe Blokzinciri Teknolojisinin Kullanımı]. Advanced Technology Applications in Health [Sağlıkta İleri Teknoloji Uygulamaları] Book, Nobel Publishing House,

Karaarslan, E., Konacaklı, E. 2019. Data Storage in the Decentralized World: Blockchain and Derivatives. “Who Run The World: DATA" Book. Istanbul University Press, 2020 (in press)

Kin Y.Z. 2019. Legal Issues in AI Deployment, The Singapore Law Gazette, https://lawgazette.com.sg/feature/legal-issues-in-ai-deployment/

Korkmaz, A., 2014. İnsan Hakları Bağlamında Özel Hayatın Gizliliği Ve Korunması [Privacy and Protection of Private Life in the Context of Human Rights], Karamanoğlu Mehmetbey Üniversitesi Sosyal Ve Ekonomik Araştırmalar Dergisi, Cilt: 2014, Sayı: 3, ss 99-103, DOI: 10.18493/kmusekad.97442.

Krittanawong, C., Bomback, A. S., Baber, U., Bangalore, S., Messerli, F. H., & Tang, W. W. 2018. Future direction for using artificial intelligence to predict and manage hypertension. Current hypertension reports, 20(9), 75.

Leeming, G., Cunningham, J., and Ainsworth, J. 2019. A ledger of me: personalizing healthcare using blockchain technology. Frontiers in medicine, 6.

Lotfi, A., Langensiepen, C., and Yahaya, S. 2018. Socially assistive robotics: Robot exercise trainer for older adults. Technologies, 6(1), 32.

Mamoshina, P., Ojomoko, L., Yanovich, Y., Ostrovski, A., Botezatu, A., Prikhodko, P., & Ogu, I. O. 2018. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget, 9(5), 5665.

Maxmen, A. 2018. AI researchers embrace Bitcoin technology to share medical data. Nature, 555(7696).

Mettler, M. 2016. Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-3). IEEE.

Mearian, L. 2017. IBM Watson, FDA to explore blockchain for secure patient data exchange. CIO. Last modified January, 12.

Mohan, C. 2019, June. State of public and private blockchains: Myths and reality. In Proceedings of the 2019 International Conference on Management of Data (pp. 404-411).

Nakamoto, S. 2019. Bitcoin: A peer-to-peer electronic cash system. Manubot.

Najafabadi, M. M., Villanustre, F., Khoshgoftaar, T. M., Seliya, N., Wald, R., & Muharemagic, E. 2015. Deep learning applications and challenges in big data analytics. Journal of Big Data, 2(1), 1.

Nugent, T., Upton, D., and Cimpoesu, M. 2016. Improving data transparency in clinical trials using blockchain smart contracts. F1000Research, 5.

Ölmez A.C., Karaarslan, E. 2019. Blockchain Based Adoption and Fostering System Proposal for Animal Shelters:BAdopt. UBMYK 2019.

Peterson, K., Deeduvanu, R., Kanjamala, P., and Boles, K. 2016, September. A blockchain-based approach to health information exchange networks. In Proc. NIST Workshop Blockchain Healthcare Vol. 1, pp. 1-10.

Protenus Inc. & DataBreaches.net 2019. Breach Barometer 2019 Annual Report, https://email.protenus.com/hubfs/Breach_Barometer/2018/2019%20Breach%20Barometer%20Annual%20Report.pdf

Radanović, I., and Likić, R. 2018. Opportunities for use of blockchain technology in medicine. Applied health economics and health policy, 16(5), 583-590.

Ravindranath, M. 2018. Health isn’t ready for blockchain. https://www.politico.com/newsletters/morning-ehealth/2018/02/16/health-isnt-ready-for-blockchain-109346

Salah, K., Rehman, M. H. U., Nizamuddin, N., and Al-Fuqaha, A. 2019. Blockchain for AI: review and open research challenges. IEEE Access, 7, 10127-10149.

Sgantzos, K., and Grigg, I. 2019. Artificial intelligence implementations on the blockchain. Use cases and future applications. Future Internet, 11(8), 170.

Statistics Finland, 2020. Pricing for research data and services https://www.stat.fi/tup/hinnat/tutkimuspalvelut_en.html

Xu, Y., Mo, T., Feng, Q., Zhong, P., Lai, M., Eric, I., and Chang, C. 2014, May. Deep learning of feature representation with multiple instance learning for medical image analysis. In 2014 IEEE international conference on acoustics, speech and signal processing. ICASSP. pp. 1626-1630. IEEE.

Yue, L., Junqin, H., Shengzhi, Q., and Ruijin, W. 2017, August. Big data model of security sharing based on blockchain. In 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM) pp. 117-121. IEEE.

Zhao, W., 2017. CDC to Trial Blockchain With IBM in Bid to Manage Medical Data. https://www.coindesk.com/cdc-trial-blockchain-ibm-bid-manage-medical-data/

Zheng, Z., Xie, S., Dai, H. N., Chen, X., and Wang, H. 2018. Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

Wahl, B., Cossy-Gantner, A., Germann, S., and Schwalbe, N. R. 2018. Artificial intelligence (AI) and global health: how can AI contribute to health in resource-poor settings?. BMJ global health, 3(4), e000798.

W3C (2019).The Web Ledger Protocol 1.0, Draft Community Group Report 18 June 2019, https://w3c.github.io/web-ledger/

White, M., Killmeyer, J., and Chew, B. 2017. Will blockchain transform the public sector? Blockchain basics for government. Deloitte Center for Government Insights. Deloitte University Press.

WHO. 2017. 1 in 10 medical products in developing countries is substandard or falsified. World Health Organization (WHO), http://www.who.int/en/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified

Woods, J. 2018. Blockchain: Rebalancing amplifying the power of AI and machine learning (ML). URL: https://medium.com/crypto-oracle/blockchain-rebalancing-amplifying-the-power-of-ai-and-machine-learning-ml-af95616e9ad9, vol. Online

Wüst, K., and Gervais, A. 2018, June. Do you need a Blockchain?. In 2018 Crypto Valley Conference on Blockchain Technology CVCBT. pp. 45-54.IEEE.