Impact of Blockchain technology in Healthcare

AIT BENNACER Sara[1,*], SABIRI Khadija[2], AAROUD Abdessadek[1], AKODADI Khalid[1], CHERRADI Bouchaib[1]

[1] *LAROSERI Laboratory, Department of Computer Sciences, Faculty of Sciences, Chouaib Doukkali University El Jadida, Morocco*

[2] *Fraunhofer Portugal AICOS, Rua Alfredo Allen, 455/461, 4200−135 Porto, Portugal,* khadija.sabiri@aicos.fraunhofer.pt

*Corresponding author. Email: *aitbennacer.sara@gmail.com

ABSTRACT

The current healthcare systems are facing many issues in terms of data management, data sharing, information security and patient privacy, data immutability, trust, and transparency. In addition, the multiple existing healthcare systems are centralized which complicates the healthcare professionals, patients in managing their data and causes several problems. Blockchain technology as a decentralized peer-to-peer network has the power to digitalize and transform the manner that the data are managed in the healthcare industry, in this regard, is one such domain that might benefit from Blockchain technology in different manners. This paper aims to improve a review of recent works on Blockchain-based healthcare applications.

Keywords: *Blockchain technology, Healthcare, Healthcare data, data management, data sharing, security, privacy.*

1. INTRODUCTION

The world's health systems continue to encounter challenges that are frequently shown as an increase in costs or a decrease in health outcomes. The Healthcare industry becomes an important sector of information technology (IT) due to the significant change through electronic health records (EHR). This development is regarded as a primary issue faced by remote healthcare system professionals. The healthcare records collected from various sources are enormous and complex, resulting in issues with medical data quality, such as complicated analysis, diagnosis, and prediction, as well as a threat of data confidentiality, owing to an increase in cybercrime incidents [1]. Data security is a critical part of health applications, and it plays a key role in the protection of sensitive data. Healthcare data obtain patient information that should not be shared with untrustworthy third parties for reasons of data security and abuse. This data contains a list of personal patient information stored in the medical records collected from the patient's illness until his or her recovery. Blockchain technology comes to enable trust, reliability and transparency. Blockchain allows interacting various entities without a central authority. This technology offers multiple benefits to deal with challenges of healthcare. This paper aims to approve the Blockchain technology potential roles in healthcare application. This paper includes the recent related works and researches according to the blockchain technology in healthcare applications. We choose five databases: Elsevier, Springer, IEEE, MDPI, WOS. Then, we identify papers using the query: '(Blockchain OR BLOCKHAIN) AND (Healthcare OR health OR medical data OR smart contract OR data management OR data security OR data

sharing)', the total of papers is 430. After that, we remove the duplicated papers, excluding irrelevance, and including studies published to journal articles, surveys, reviews and books chapter, also we select the papers during 2016 to 2020. The final studies included in this paper are 29. In section 1, we present a Blockchain overview. The section 2 demonstrates the Blockchain for healthcare applications, the section before, resumes some related works according to the Blockchain based healthcare sector.

2. BLOCKCHAIN OVERVIEW

Satoshi Nakamoto presented Blockchain technology in 2008 through his Bitcoin cryptocurrency concept. Blockchain technology is defined as a current kind of technology that combines encryption, data management, networking, and incentive systems to permit participants to check, execute, and record the transactions. Blockchain is a technology that eliminates the need for a single, centralized authority while yet allowing to enable secure and "trustless" transactions between parties [2].

2.1.1 Data structure:

The blockchain is composed of cryptographically linked data blocks. Blocks are chained in a series, deploying the cryptographic hashes. A hash is a number of a specific length generated from a message or document. A block in a Blockchain network comprises four components: information, the current block's hash (identifying number), the previous block's hash, and the timestamp. The Blockchain is a series of blocks that contains a complete list of transaction records, like a classic public register. Block header includes, in particular: Block version, specifies which set of block validation rules to be used. Merkle tree root hash defines the hash value about all the transactions in the block. Timestamp determines the current time as in seconds using universal time, since the 1st January 1970, Block-hash presents the calculated block data hash value [3]. The figure1 bellows the blockchain's structure.

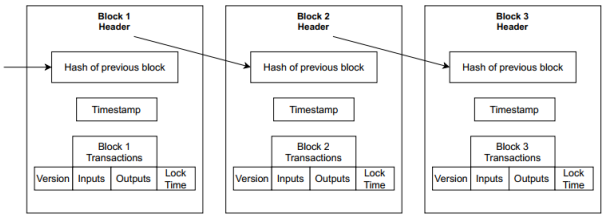

Figure 1 *Blockchain structure*

Blockchain is a distributed ledger technology (DLT). The Blockchain stores and persists a continuous set of tries in a "massive computer database." This database includes made up of multiple interconnected devices (phones, computers or embedded systems) geographically unconstrained.

Cryptography considers the use of secure hash functions; it is a crucial technique to assure the Blockchain's availability and security [4]. Hashing is a way of calculating a relatively unique output (called a message digest, or digest) given an input of nearly any size using a cryptographic hash function. Individuals can separately take input data, hash that data, and obtain the identical output, ensuring that the data has not changed. Even the smallest change in the input results in an entirely different output digest. Hash is a key element in Blockchain security. If anyone may identify an adversary attempting to change the content of a block by calculating the block's hash, and comparing it to the hash stored in the following block previous hash, to verify if there is an inconsistency.

A transaction is an exchange of information between two or more parties. A transaction in the cryptocurrency world represents a cryptocurrency transfer between Blockchain network participants. A transaction is a manner of recording activities on digital or physical assets in a business-to-business context.

2.1.2 Distributed network

The Blockchain's participants are nodes that constitute a peer-to-peer network. Participants' transactions are verified and distributed across a network of nodes. Every node has its own local copy of the blockchain. When a node retrieves the blockchain, it verifies the blocks' integrity by computing all the hashes. Every node can transmit transactions to the network and demand that they are added to the Blockchain; miners verify these pending transactions. Miners are peers who exercise their computational power to mine for blocks. To generate a block, miner nodes should solve a computational problem and use a significant quantity of computer resources. The miner who solves the problem first is the winner and gets the ability to generate a new block [5].

2.1.3 Asymmetric key cryptography

To validate transaction authentication, Blockchain employs a well-known asymmetric private/public key and hash cryptography method. Each node's transactions are signed using their private key. All transactions signed with a private key are broadcast across the whole network. To encrypt data on Blockchain, we apply asymmetric algorithms. We utilize distinct keys for plaintext encryption and ciphertext decryption in asymmetric algorithms, commonly known as public key encryption. Both the transmitter and the receiver have a public and private key pair in this form of encryption. Only the generating nodes have access to the private key, but the public key is distributed very widely throughout the network [6].

2.1.4 Digital signature

A digital signature is a mathematical technique that verifies the validity of digital messages or documents.

Every user has a private and public key pair. The transactions are signed with a private key, which must be kept secret. The digitally signed transactions are disseminated over the whole network. A basic digital signature includes two phases: the signing phase and the verification phase. The integrity of a file or message can be confirmed with digital signatures. It is a form of non-repudiation [7].

Here's an overview about how many blockchain networks employ asymmetric-key cryptography:

- Transactions are digitally signed using private keys.
- Addresses are generated with public keys.
- Signatures generated by private keys are verified using public keys.
- Asymmetric-key cryptography permits users to verify that the entity sending value to another entity has the private key needed to sign the transaction.

2.2 Blockhain deployment models

They are three categories of deployment Blockchain platform: public, private and consortium.

2.2.1 Public Blockchain

It is considered a decentralized permissionless Blockchain where all network members have access to information and may participate in its approval. Furthermore, a public blockchain is an open blockchain that allows anybody to join as a node and make transactions. It also ensures great reliability and integrity by verifying the work of participants. As examples of public Blockchains, Bitcoin and Ethereum. This model of Blockchain is secure by means of its consensus process that establishes an agreement among all peers [8].

2.2.2 Private Blockchain

This kind uses Blockchain technology in a centralized structure to increase transaction security and speed. Unlike public Blockchains, private Blockchains are controlled by a single entity and not accessible to the public. This type is a permissioned network that controls which nodes are permitted to process transactions, execute smart contracts, or operate as miners. They are overseen by a single entity, which is a trusted third party [9].

2.2.3 Consortium Blockchain

Consortium Blockchain is also called federated Blockchains, in which information is available to all users, but only certain groups can modify or approve it. Consortium Blockchains, like private Blockchains, permit only authorized entities to write data and participate in the consensus processes [10]. Furthermore, this Blockchain guarantee the security of a public Blockchain while preserving the system's decentralization and providing companies with greater privacy for sensitive information. Blockchain consortiums are primarily utilized in the financial industry.

2.3 Consensus models

Blockchain technology is a distributed electronic ledger of digital data, events, or transactions that is secured cryptographically, exceedingly difficult to fake, and immutable by all connected nodes through a consensus mechanism; Inside the absence of a trusted party, nodes agree on how to confirm or reject blocks and transactions in order to avoid future disagreements.

2.3.1 Proof-of-work

PoW was proposed by Satoshi Nakamoto. Someone must be chosen to record transactions in a decentralized network. A user publishes the next block in the proof of work (PoW) paradigm by solving a computationally difficult problem first. It is structured in high complexity that make it hard to solve, however, validating a solution is simple. This allows all other complete nodes to quickly evaluate any suggested future blocks, and any recommended block that does not meet the solution's requirements will be rejected. On the other hand, it considers vulnerable to attacks. As a result, if a node desires to publish a block of transactions, it must first prove that it is unlikely to attack the network [11].

2.3.2 Proof-of-stake

The basic idea behind this consensus method is to utilize the stake to choose who gets to mine the next chain block. Using stake as proof to gain an advantage, someone with a large stake would feel more at ease. He or she would be motivated to engage in any fraudulent conduct in order to get access to the chain's many rewards [12].

2.3.3 Delegated Proof-of-stake

Participants can vote for nodes that invest resources in the Blockchain system in the DPoS system. The number of tokens a person has determined the strength of his or her vote. As a result, a small group of powerful nodes may control the network and choose the witness. The witnesses, or nodes with a larger number of votes, are in charge of creating blocks and are compensated for their efforts. Nonetheless, as the network grows, the witness must compete to keep his or her job. Voting in this protocol is a continuous process.

2.3.4 Practical Byzantine Fault Tolerance (pBFT)

BFT (Byzantine Fault Tolerance), which is derived from Byzantine general issues, seeks to obtain a consensus among nodes in a distributed network even if

some nodes fail to reply or respond with misleading information. The BFT mechanism can protect networks from failures by making collective decisions that limit the effect of faulty nodes. Practical BFT works well in dispersed networks with a limited number of nodes, however, the communication cost grows exponentially with each new node added to the network [13].

2.4 Smart contract

Nick invented the term smart contract in 1994, describing it as a computerized transaction protocol that executes the conditions of a contract. The main goals of smart contract design are to meet common contractual criteria (such as payment periods, liens, secrecy, and even enforcement), reduce malicious and unintentional exceptions, and eliminate the need for trusted intermediaries. A smart contract is a collection of self-verifying, self-executing, and tamper-resistant algorithms. Smart contracts that include Blockchain technology are able to do tasks in real time at a low cost and with a higher level of security. Smart contracts, on the other hand, take the role of trusted third parties, or intermediaries between contract participants. They make use of automated code execution in a blockchain network, which is distributed and validated by network nodes [14].

3 BLOCKCHAIN FOR HEALTHCARE APPLICATIONS

3.1 Blockchain benefits

3.1.1 Decentralised storage

Blockchain stores data transparently and makes it available to third parties with the originator's permission. The keeping numerous copies of such information in various locations is one of the most advantageous characteristics of decentralizing information storage.

3.1.2 Transparency

In order to achieve data transparency in any technology, entities must have a trusting connection. The medical data or healthcare record in question should be safe and secure. In the Blockchain, the data are saved and spread across the network, which make it more transparent and safer against third-party interference [15].

3.1.3 Anonymity

Because Blockchain technology addressed the problem of node-to-node trust, data movement and even transactions are anonymous, all that is required is knowledge of the person's Blockchain address.

3.1.4 Immutability

A transaction added to the Blockchain ledger cannot be reversed in most cases. The most important characteristics that contributes to the integrity of Blockchain transactions are its immutability. The Blockchain immutability's is ensured using encryption [16] .

3.1.5 Security and Privacy:

Each block contains the hash of the preceding block, thus if the contents in a block are changed, the hash of the block will change, and the chain will break. To modify the data, the next blocks must also be changed in order for the chain to stay intact.

3.2 Blockchain in the healthcare application

To begin, data transformation should be performed in an assured environment. Data transformation technologies should be used to automate a variety of methodological activities, allowing entities to complete transactions more quickly. Traditional healthcare application systems are used to build a trust network, but there are two disadvantages. These circumstances frequently require greater transaction costs than public Blockchains, and they must be trusted nearly blindly, with little regard for security, internal policies, or ethics. Secondly, since the data in the distributed public ledger is securely encrypted using modern encryption, it is resistant to manipulation. In the connected objects and other kinds of networking, it eliminates the use of centralized devices, permitting connected devices to update software, handle problems, and communicate directly.

4 RELATED WORKS

This section presents related works about Blockchain technology in healthcare applications. This study [17] assume the responsibility for consent management is assured and dispersed across multiple players, each with distinct interests, this technique greatly improves confidence. Transparency is also offered since third-party auditability of consents is available. This article [18] describes a patient-centric healthcare data management system that employs Blockchain as a storage medium to ensure anonymity. The use of cryptographic methods to secure patient data ensures pseudonymity. As a result, the systems known as MediBchain guarantee accountability, integrity, pseudonymity, security, and privacy of healthcare data.

H. Kaur and M. A. Alam [19] developed a novel terme BlockCloud, which refers to the combination of Blockchain and cloud computing. The goal of using the cloud is to keep data dispersed and secure under one roof without the need of third parties. The research looked at the problems that medical practitioners and

organizations, public health agencies, healthcare service providers, and governments have when it comes to collaborating and enforcing policies. ProvChain [20] is a cloud-based provenance architecture that aims to improve data availability and privacy. This system is completely decentralized and relies on cloud computing to provide tamper-proof access through the use of Blockchain technology.

X Yue and H Wang [21] proposed the Healthcare Data Gateway (HGD) application's architecture. The Blockchain-based application allows patients to easily own, control, and share their own data in a safe manner without violating on their privacy, also they define it a new method to increase the intelligence healthcare systems while protecting patient data privacy. Patients own and manage their health data with the purpose-centric access paradigm they offer a simple, unified Indicator Centric Schema (ICS) provides an opportunity to manage all types of personal health data quickly and simply. W. Tang and J Ren [22] aim to improve trust between patients and caregivers, they suggested privacy-preserving healthcare in a trusted network. The Sybil attack is used to locate and remove the phony patient from the network. The suggested approach is utilized to grant entry to the healthcare centre to the authenticated individual. In this paper, the authors present Healthchain [23] a large-scale health data privacy-preserving system based on Blockchain technology, the healthcare data is encrypted to perform fine-grained access control. By applying user transactions for key management, individuals can effectively remove or add authorized doctors. Additionally, through using Healthchain, both IoT data and doctor diagnoses would be impossible to remove or tamper with, avoiding medical conflicts. The following table lists examples of platforms, applications and projects based on Blockchain technology applied to the healthcare sector:

Tableau 1. Blockchain in healthcare applications

Application	Platform	Description	Scenario
OmniPHR	OmniPHR Platform	Patients can access their information through a public health record (PHR). This approach was created to keep data up to date and to distinguish between electronic health records and personal health records [24] .	Data sharing Security and privacy Interoperability
MedShare	MedShare Platform	A blockchain-based system enables data provenance, auditing, and control for medical data exchanged in cloud repositories by healthcare providers, healthcare organizations, and medical researchers. Furthermore, smart contracts and an access control mechanism are used in its architecture to efficiently track the data's activities [25] .	Access control Data sharing Data security
MedChain	Ethereum	It is intended to enhance current systems by allowing patients, health care providers, and other third parties to access medical records in an interoperable, secure, and effective manner while maintaining patient privacy. Timed-based smart contracts are used by MedChain to manage transactions and limit access to electronic medical information [26].	Data sharing Security and privacy Data management
MedBlock	MedBlock Platform	It is a blockchain-based secure method for sharing electronic medical records among authorized individuals [27] .	Data shaing Data management Data security and privacy
MedRec	Ethereum	It is a decentralized record management system. It is a Blockchain model for authentication, confidentiality, data management and data sharing. Furthermore, it incorporates all the characteristics of	Data management Permission management Digital Rights Management

		Blockchain-like smart contracts as well as the notion of decentralized data [28].	Data sharing Data integrity
BloCHIE	BloCHIE Platform	The proposed platform analyses healthcare data sharing requirements, primarily for personal healthcare data and electronic medical records, and interacts with a variety of additional data types by integrating blockchains inside multiple sources [29] .	Data sharing Data storage Healthcare information interoperability Privacy and authenticability

3. CONCLUSION

Blockchain applications are being widely used, and several challenges need to be addressed. For this reason, blockchain technology will become more scalable, efficient, and sustainable. Regarded separately, the characteristics they provide are not novel, and the majority of the systems they depend on have been well known for years. However, the combination of these characteristics make them excellent for a broad range of applications, which explains the high level of interest from a variety of sectors. The current article identifies the main application areas in healthcare where blockchain technology can make a serious impact on. Furthermore, this paper discusses different blockchain-based healthcare requirements and solutions.

Références

[1] Iqbal, S. et al., «Real-time-based E-health systems: design and implementation of a lightweight key management protocol for securing sensitive information of patients,» *Health Technology,* 2018.

[2] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» 2008. Available: https://bitcoin.org/bitcoin.pdf.

[3] M. Gupta, Blockchain for Dummies, IBM Limited Edition, 2017.

[4] Maoning Wang, Meijiao Duan, Jianming Zhu, «Research on the Security Criteria of Hash Functions in the Blockchain,» *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts - BCC '18,* 2018.

[5] J. A. Kroll, I. C. Davey, and E. W. Felten, «The economics of bitcoin mining, or bitcoin in the presence of adversaries,» *Proc. WEIS,* 2013.

[6] Gautam Srivastava, Shalini Dhar, Ashutosh Dhar Dwivedi, Jorge Crichigno, «Blockchain Education,» *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE),* 2019.

[7] Weidong Fang, Wei Chen, Wuxiong Zhang, Jun Pei, «Digital signature scheme for information non-repudiation in blockchain: a state of the art review,» *EURASIP Journal on Wireless Communications and Networking,* 2020.

[8] Kim, Jin-whan, «Blockchain Technology and Its Applications: Case Studies,» *Journal of System and Management Sciences,* 2020.

[9] Marko Hölbl, Marko Kompara, Aida Kamišali´c, Lili Nemec Zlatolas, «A Systematic Review of the Use of Blockchain in Healthcare,» *Symmetry ,* 2018.

[10] Adetomike Adeyemi, Mingyu Yan, Mohammad Shahidehpoura, Cristina Botero, Alba Valbuena Guerra, Niroj Gurung, Liuxi (Calvin) Zhang, Aleksi Paasob, «Blockchain technology applications in power distribution systems,» *The Electricity Journal,* 2020.

[11] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, «An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,» *2017 IEEE 6th International Congress on Big Data,* 2017.

[12] S.Velliangiri, P. Karthikeyan, «Blockchain Technology: Challenges and Security issues in Consensus algorithm,» *2020 International Conference on Computer Communication and Informatics (ICCCI -2020),* 2020.

[13] V. Gramoli, «From blockchain consensus back to byzantine consensus,» *Future Generation Computer Systems,* 2017.

[14] Daniel Macrinici, Cristian Cartofeanu, Shang Gao, «Smart Contract Applications within Blockchain Technology: A Systematic Mapping Study,» *Telematics and Informatics,* 2018.

[15] Ayesha Shahnaz, Usman Qamar, And Ayesha Khalid, «Using Blockchain for Electronic Health Records,» *IEEE Access,* 2019.

[16] OECD Blockchain Primer, https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf, 2018.

[17] Philippe Genestier, Sajida Zouarhi, Pascal Limeux, David Excoffier, Alain Prola, Stephane Sandon, Jean-Marc Temerson, «blockchain for consent management in the ehealth environment: a nugget for privacy and security challenges,» *Journal Of The International Society For Telemedicine And Ehealthgenestier,* 2017.

[18] Abdullah Al Omar, Mohammad Shahriar Rahman, Anirban BasuShinsaku Kiyomoto, «MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data,» *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage,* 2017.

[19] Harleen Kaur, M. Afshar Alam, Roshan Jameel, Ashish Kumar Mourya, Victor Chang, «A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment,» *Journal of Medical Systems,* 2018.

[20] Liang, Xueping, Sachin Shetty, Deepak Tosh, Charles Kamhoua, Kevin Kwiat, and Laurent Njilla, «Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability,» *In Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing,* 2017.

[21] X Yue, H Wang, D Jin, M Li, W Jiang, «Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control,» *Journal of medical systems,* 2016.

[22] Wenjuan Tang, Ju Ren, Yaoxue Zhang, «Enabling Trusted and Privacy-Preserving Healthcare Services in Social Media Health Networks,» *IEEE Transactions on Multimedia ,* 2018.

[23] ie Xu, Kaiping Xue, Shaohua Li, Hangyu Tian, Jianan Hong, Peilin Hong, Nenghai Yu, «Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data,» *IEEE Internet of Things Journal,* 2019.

[24] Alex Roehrs, Cristiano Andréda Costa, Rodrigoda Rosa Righi, Valter Ferreirada Silva, José RobertoGoldim, Douglas C.Schmidt, «Analyzing the performance of a blockchain-based personal health record implementation,» *Journal of Biomedical Informatics,* 2019.

[25] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du et M. Guizani, « MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain,» *IEEE Access ,* 2017.

[26] Bingqing Shen, Jingzhi Guo, and Yilong Yang, «MedChain: Efficient Healthcare Data Sharing via Blockchain,» *Applied sciences,* 2019.

[27] Kai Fan, Shangyang Wang, Yanhui Ren, Hui Li, Yintang Yang, «MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain,» *Journal of Medical Systems ,* 2018.

[28] Azaria, Asaph, et al., «MedRec: Using Blockchain for Medical Data Access and Permission Management,» *International Conference on Open and Big Data (OBD),* 2016.

[29] Jiang, Shan, et al., «BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange,» *IEEE International Conference on Smart Computing,* 2018.