Ilkogretim Online - Elementary Education Online, Year; Vol 20 (Issue 5): pp. 966-975
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.05.105

Blockchain's Contribution in the technology of Healthcare Information System

M.KASSOU, ERISI, National School of Applied Sciences, AbdelmalekEsaadiUniversiy, Tetouan, Morocco
S.BOUREKKADI, Ibn Tofail University, Kenitra, Morocco, EuRSED, Vienne, France
S.KHOULJI, ERISI, National School of Applied Sciences, AbdelmalekEsaadiUniversiy, Tetouan, Morocco
K.SLIMANI, Ibn Tofail University, Kenitra, Morocco, EuRSED, Vienne, France
H.CHIKRI, ERISI, National School of Applied Sciences, AbdelmalekEsaadiUniversiy, Tetouan, Morocco, EuRSED, Vienne, France
M.L.KERKEB, ERISI, National School of Applied Sciences, AbdelmalekEsaadiUniversiy, Tetouan, Morocco

Abstract: The aim of this paper is to propose a Healthcare system's model based on the combination of Blockchain, Big Data, and IoT technologies. A literature review was carried out to highlight the benefits of the combination of these technologies in terms of decentralization, security, privacy, and data integrity taking into account the constraints required by a medical system as a sensitive data area. Meanwhile, a list of the principal categories of participants in the healthcare system was drawn up. In addition, the current solutions in the healthcare system were analyzed. Finally, the structure and the implementation of our healthcare system's model were detailed based on the combination of the trending trio (Blockchain, Big Data, IoT), and their efficiency via a robustness analysis.

Keywords: **Block chain, Smart Contract, Big Data·IoT·Healthcare.**

I. INTRODUCTION

Several factors explain the strong acceleration in the growth of the e-health market. Demographic ageing continues accompanied by an increase in chronic diseases favored by our lifestyles. Above all, digital technology, after having colonized our personal and professional lives, is naturally making inroads into the uses of patients and healthcare professionals. From a technological point of view, we can cite Big Data and IoT as means to collect and analyze large volumes of data and extract knowledge from it.

Increasingly, health data will be collected "in real life", which is a major change from the past when most data were collected during clinical trials or hospital examinations. We have also noticed that external health data is generated by patients outside of healthcare institutions (including social media, self-quantification, including the use of smartphones/portable sensor information on patient pulse, brain activity, sleep patterns, these include: temperature, muscle movements and various other clinically useful data points), and other health-related information from insurance companies, government reports, etc. The growing exploitation of data, the volume of which would be multiplied by 10 in 5 years according to the Frost & Sullivan report, implies reinforced needs in cybersecurity, and the definition of data governance by the actors based on ethical reflection.

The Blockchain technology, could provide a new model for health information exchange by making medical data more efficient, decentralized, disintermediated and secure. It is a circulated "peer-to-peer" system, every node in the network has the chance of recording and saving operations(Lu, 2019). In theory, the data is shared by default and circulated between the nodes with no middle person or outsider mediation. In this decentralized structure, the nodes are active to participate in tasks and operations. In contrast to the centralized structure of traditional mechanisms, decentralization is a peculiar attribute of the Blockchain that increases its performance.

In addition, the data in the Blockchain is usually transparent because anyone can see and interrogate the data shown simply by using a Blockchain explorer. Each member has equal approvals and permissions, and therefore the information and the processes are all open and consistent. However, the sharing of data across nodes does not imply complete confidence among the members. The innovation is founded on shared agreement system standards that employ both decentralized and intermediary frameworks that form a reliable relationship between the network nodes and the suitable framework structures. In fact, Security assurance is an important factor of concern to the trading partners (Angraal et al., 2017).

The Blockchain, however, does not require participants to face a shared connection of trust as it uses both hash functions and the protocol of consensus to solve this problem. A key objective of Blockchain-based systems is to ensure the finality of transactions. The block containing the transaction, (the data) cannot be undone because it demands a lot of computing power, which makes it extremely doubtful that the assumption of a longer chain expansion would not involve this particular block. Therefore, once a chain is sufficiently long, it is technically impossible to reverse it. Operations may be regarded as technically permanent. This means that they are not subject to modification or deletion, and all the history is made accessible and can be searched for. This ensures the tracking of data.

Blockchain's influence is demonstrated on various levels. Three issues are regularly experienced in the Big Data environment: data security, data accuracy, and data management. One of the major issues in the use of data is data veracity. It impacts the accuracy of the analysis. The Big Data makes the accuracy and quality less measurable, and the absence of both quality and accuracy is usually the outcome of high volumes and inefficient analytical reporting.

In this paper, we will address the following points: we will draw up a list of the principal categories of participants in the healthcare system. We will review the strengths of the combination of Blockchain, Big Data and IoT technology, which are in line with the constraints required by a medical system as a sensitive data area. At the end, we will detailthe structure and the implementation of our healthcare system's model based on the combination of the trending trio (Blockchain, Big Data, IoT), and its efficiency via a robustness analysis.

II. Literature Review

According to the World Health Organization (WHO), it is difficult to specify precisely the limits of a health system, from where it begins and ends (WHO, 2000). (Fray, 2009)described the hospital as a real node of contracts between different stakeholders (see Fig1)

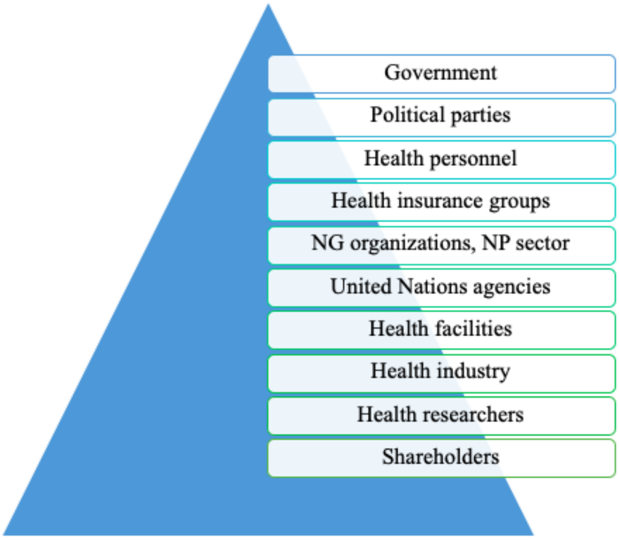


Fig1. Categories of health system stakeholders identified at the international level.

The appliance of the 5W2D in has allowed the identification of 17 groups of HSS involved at different levels with distinct roles and interests. they're all both influencing and influenced by Quality Care (QC). Nevertheless, three key HSS groups are at the core of the health system: - Patients: are the foremost important group and therefore the reason behind the existence of health systems because the target of healthcare activities(Frichi et al., 2019).

WHO emphasizes the requirement to position patients and populations at the middle of health systems by meeting their needs and expectations. Similarly, patients influence QC because the care process is initiated at the patient level; patients are who decide when and where to hunt care, and to continue or stop it. Patients and populations also play the role of contributors to finance the health system through taxes and Social Security. Furthermore, the supply and access to information has radically changed the position of patients, who are not any longer mere consumers of care, directed and guided by their physicians, but became aware and able to make choices and decisions, in a different way, patients can influence QC is through satisfaction surveys, which are the foremost widely considered indicators in QC assessment.

During this regard, some studies considered patients' experience and involvement as a chance to boost healthcare services and produce new innovative ideas in delivering care(Wu et al., 2019).- Health personnel: are the providers of healthcare services and are involved throughout the care process. This HSS group includes medical, paramedical, administrative, and other doctors, all of whom are the purpose of contact with patients and largely influence their perception of received care. Also, health personnel play a really potential role in QC through professional skills (effectiveness and safety of care), respect of patients' preferences and values (patient-centeredness), optimal use of obtainable resources (efficiency), etc. - Government: Through the Ministry of Health (Directorate of Epidemiology and Disease Control, Directorate of Hospitals and Ambulatory Care, Directorate of Medicines and Pharmacy…) and other ministries of Finance, Education, Interior, Agriculture and Transport, the government incorporates a significant impact on QC.

The government plays a leadership role within the regulation, monitoring, and improvement of QC. Generally speaking, governments play an important role in health development, through strengthening health systems and generating human and financial resources, to realize objectives of improving health, efficiency and equity in health care financing. (Leviton and Melichar, 2016)claim that improving Quality of Care (QC) requires taking into consideration the perspectives of stakeholders, that are essential for planning, implementing, and assessing QC improvement programs. Given the nice diversity and heterogeneity of the players, a worldwide perspective should be taken, to confirm efficient coordination and governance, since they play essential roles within the inputs, processes, and outputs of healthcare services.

And since several findings confirm that digital health technology may be a pivotal pillar in delivering value-based care (Philips' Future Health Index 2019), and in ensuring a decent coordination to handle the imbalance between regions and therefore the in complementarity between the private and public sectors. Then evolve effectively, it's therefore strongly recommended that the government, the Minister and every one health stakeholders collaborate, taking advantage of the strengths mentioned above, to line up a healthcare system supported information technologies (Big Data, IoT…).

2.1 Big Data in Healthcare

The Healthcare field represents a good case that ought to be considered while coping with the term of massive data and this is often thanks to the rise of the info produced by the medical organizations in terms of storage, calculation, and analysis. Recently, we haveseveral wearable devices that have hit the market like Fitbit, Samsung Gear Fit and Jawbone, these allow the patient to trace his progress, and share this information along with his doctor, who are ready to use it as a part of their diagnostic process once we visit him with an ailment. As more and more data are collected, doctors are able to give treatment options supported the info from other patients with similar conditions, genetic factors and lifestyle.

Several countries are getting their feet wet by gaining valuable insights from big data in the healthcare sector. in the U.S., an abundance of highly successful innovations have appeared, such as the American Indiana Health Information Exchange, which is a nongovernmental organization that uses a secure and reliable network of health information technology linking more than 90 Hospitals (Abouelmehdi and others...), long-term care services, community health centers, clinics, and other local health care providers. This allows medical information to reach the patient instead of being stored in a doctor's office or hospital system.

A further achievement is that the Kaiser Permanente healthcare network that is based in California. The network, which has more than 9 million members, is intended to handle Big Data volumes ranging from 26.5 to 44 petabytes (Mounia and Habiba, 2015). An additional example, now in Canada, at the Toronto Infant Hospital, megadata analysis is now being used to improve outcomes for children at potential risk of deadly hospital-acquired infections. Again, in Canada, a partnership involving IBM and the Ontario Technological Institute has established the Artemis project. This new surveillance platform handles the process of acquiring and storing both patient physiological data flows and the clinical records in order to be available online in real time. This involves analysis, retrospective analysis, and data processing.

In several other countries, some initiatives for the development of such data have been successful. In addition, in Italy, the Italian Medicines Agency is currently conducting clinical data collection and analysis

on high-cost new medicines as component of a national cost-effective program; on the basis of the findings, drug prices and market access conditions should be reconsidered.
The success of the technology adoption strategy within the medical sector is not limited to developed countries. India, as an example, is ranked after Morocco, based onthe social progress index (World Bank Data, 2020). But, it's played a good role in providing the telehealth (based on big Data) even to the agricultural parts of the India, with the help of HEALTHSAT, it's covered 384 hospitals with 60 specialty hospitals connected to 306 remote/rural/district/medical college hospitals and 18 Mobile Telemedicine units across the country through its geo-stationary satellite, which has marked a continual improvement in quality of healthcare in rural India. This covers diverse areas of Cardiology, Radiology, Diabetologymedicine, maternal and Child healthcare(Jarosławski and Saberwal, 2014).

2.2 IoT & Healthcare

Without a doubt, the E-health is one among the primary and foremost stakeholders of IoT today. in keeping with a recent report, The global telemedicine market size is expected to reach USD 155.1 billion by 2027, expanding at a CAGR of 15.1% over the forecast period, according to a new report by Grand View research, Inc (Grandviewresearch, 2020).

E-health solutions hold great opportunities as they assist in improving clinical management, reduce variations in diagnosis, and make effective healthcare delivery by enhancing quality and access to healthcare services.
The sudden global outbreak of coronavirus is predicted to spice up the usage of telemedicine as these solutions help caregivers to speak effectively with their patients during the pandemic and supply better solutions to their health concernsdue to social distancing implemented by various countries round the world, virtual healthcare delivery is stepping up as an efficient solution for safe and better communication.

An IoT-based healthcare system connects all the available resources as a network to perform healthcare activities like diagnosing, monitoring, and remote surgeries over the web(Deshkar, n.d.).
The adoption of this technology in Healthcare system, will allow the incapacitated and aging individuals to measure longer and healthier. it's observed that the share of the aging population is significantly increasing and it's estimated that about 20% of the globe population are going to be over 60 years old by 2050(Farahani et al., 2018). At the identical time, aging brings fast growth of varied chronic diseases (e.g., stroke, cancer, type II diabetes, and obesity).
Due to the growing acceptance of technology, in Ambient Assisted Living (AAL), IoT enables indoor positioning yet as location-aware real-time monitoring of living parameters (e.g., heart rate) and environmental conditions. The globe Health Organization (WHO) conducted a survey on disability and reported that over a billion people (equivalent to fifteen population of world) swallow disability(Maskeliūnas et al., 2019).
IoTeHealth can bring a superb deal of comfort to this vulnerable population and enhance their life significantly through automated, timely, reliable resistive technologies. For instance, variety of smart gloves are developed with low-cost inertia sensors enabling deafness to speak with those that aren't very aware of the American linguistic communication (ASL).
One of the popular applications of IoT in Healthcare system, could be a Smartphone Based m-Health System(Darshan K R and Anandakumar K R, 2015); This technique presents a brand-new Internet of Thing (IoT)-based platform to support self-management of diabetes. This approach allows for multiple care dimensions of diabetes by means of remote collection and monitoring of patient data and provision of personalized and customized feedback on a wise phone platform. The platform understands to what extent the patient’s activities accommodates their individual treatment plan, deriving rule-based health indicators, and generating appropriate warnings and support in terms of feedback advices. Another interesting application, may be a mobile system in real time to detect the OSA supported the automated extraction of a group of rules (IF ... THEN), which contained typical parameters derived from the analysis of the center rate variability obtained from an electrocardiogram (ECG)(Sannino et al., 2014).

2.3 The Need for Integration

However, these efforts, problems with anonymity, adaptability, and integrity still have to be investigated further to realize secure decentralized data storage. Most healthcare data centers have HIPAA certification, but that certification does not guarantee patient record safety. The rationale being, HIPAA is more focused on ensuring security policies and procedures than on implementing them. Furthermore, the inflow of huge data sets from diverse sources places an additional burden on storage, processing, and communication.

Traditional security solutions cannot be directly applied to large and inherently diverse data sets. Invasion of patient privacy could be a growing concern within the domain of huge data analytics. an occurrence reported within the Forbes magazine raises an alarm over patient privacy. within the report, it mentioned that concentrate on Corporation sent baby care coupons to a teen-age girl unbeknown to her parents. This incident impels big data to think about privacy for analytics. for example, dataanonymization before analytics could protect patient identity(Abouelmehdi et al., 2017).

IoT-based applications also had these issues; the fact that personal data are going to be collected through tele-monitoring implies the necessity for strategies and mechanisms to confirm adequate security and confidentiality. "Everything" being connected, new security and privacy issues arise, as an example the confidentiality, authenticity and integrity of information detected and exchanged by "things"(AL-mawee, n.d.).

Blockchain technology is that the primitive to settle privacy and reliability concerns within the Internet of Things. It could perhaps be the solution needed by the IoT industry and may be utilized in tracking billions of connected devices, enabling the processing of transactions and coordination between devices; this allows for significant savings for IoT industry manufacturers. This decentralized approach would eliminate single points of failure, creating a more resilient ecosystem for devices to run on(Christidis and Devetsikiotis, 2016).

The cryptographic algorithms utilized by Blockchains would make consumer data more private. The ledger is tamper-proof and cannot be manipulated by malicious actors because it does not exist in any single location, and man-in-the-middle attacks cannot be staged because there is no single thread of communication, which will be intercepted. Blockchain makes trustless, peer-to-peer messaging possible. for instance, by leveraging the Blockchain, IoT solutions can enable secure, trustless messaging between devices in an IoT network(Baliga, 2017).

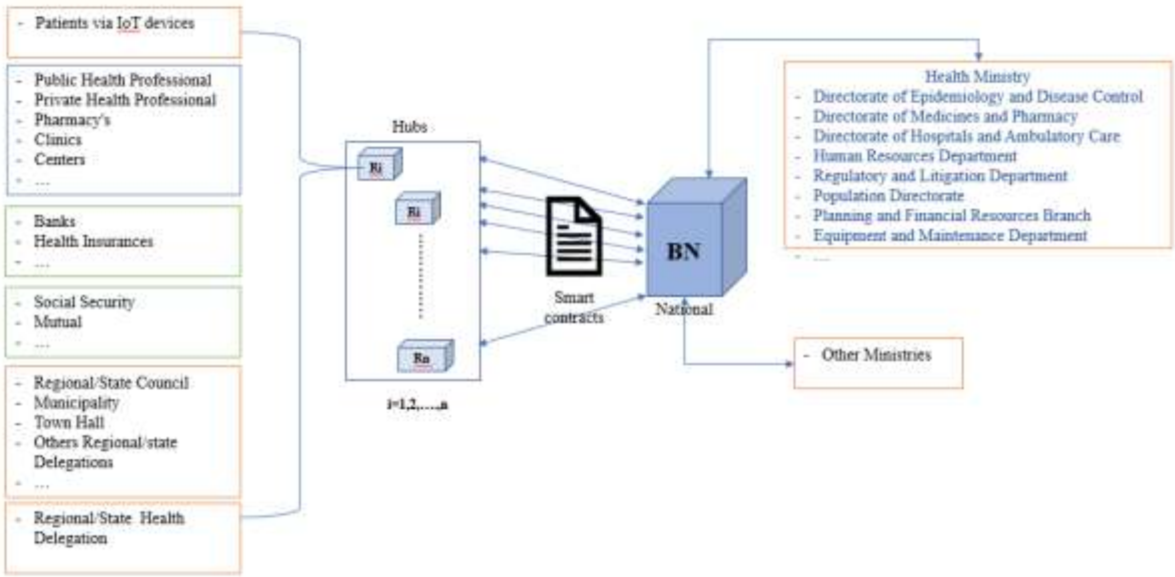
Combining the Blockchain and Big Data, on the other hand, is potentially a more effective way to address this issue, as the quality of Big Data analysis results is always affected. Based on consensus algorithms, the Blockchain is a robust, safe, and tamper-proof distributed data system. This system is a data repository that will be checked and authored by the participants in this unified ecosystem, while maintaining its consistency and integrity. The federated ecosystem registers all incidents as the identity holder goes through various steps and gives each licensed user a reviewable record (Bhuiyan et al., 2018). In this way, the log can be expanded and checked without limit, and the Blockchain maintains a permanent track of every action recorded, avoiding the tiring but critical first stage (data cleaning) of the classic Big Data infrastructure. The inclusion of the Blockchain in the Big Data governance framework resolves the security issue through mathematically testable encrypted signatures. The Blockchain is unchangeable because of the use of the Merkle tree. This means that when data is included in the Blockchain, the data cannot be changed. Because of this unchangeable property, the Blockchain can be used to generate data in a very secure way. In addition, the Blockchain's transparent capability is in line with the fashionable Open Data trend in two areas: Legitimate Data Openness, indicating that data access is legal, as well as processing and distribution (Liu, 2016).

In addition, the technical openness signifies that no technical obstacles to the processing of the data should exist. In most cases, the data that is open is simply impersonal data. Basically, the data contains no information about people for clear privacy reasons. Furthermore, the Blockchain combination assures that policy, as it is consistent with the principle of anonymity and every single node in this system is identified by an address. The Blockchain's handling ability to store public data in a secure, clear, and unchangeable manner removes the chance of tampering or modification by the wrong parties, while at the same time fostering the continuous protection and accessibility of the data, as the Blockchain construct does not constitute the single point of failure (SPOF) concern.

III. Result

This section mainly introduces the architecture design and implementation of Big Data-IoT-Block chain network in the Healthcare system.

3.1 Model Design



- Patients via IoT devices
- Public Health Professional
- Private Health Professional
- Pharmacy's
- Clinics
- Centers
- …
- Banks
- Health Insurances
- …
- Social Security
- Mutual
- …
- Regional/State Council
- Municipality
- Town Hall
- Others Regional/state Delegations
- …
- Regional/State Health Delegation
Hubs
Ri
Ri
Rn
i=1,2,….n
Smart contracts
BN
National
Health Ministry
- Directorate of Epidemiology and Disease Control
- Directorate of Medicines and Pharmacy
- Directorate of Hospitals and Ambulatory Care
- Human Resources Department
- Regulatory and Litigation Department
- Population Directorate
- Planning and Financial Resources Branch
- Equipment and Maintenance Department
- …
- Other Ministries

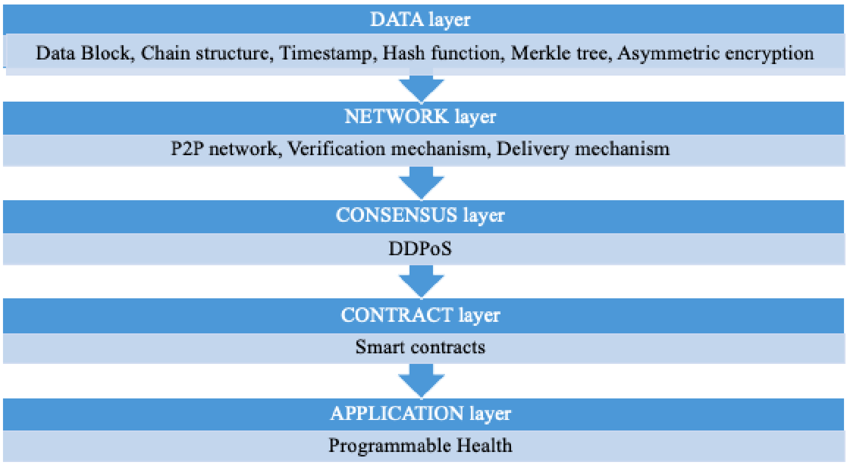
Figure 2.Overview of the infrastructure of our system combining Blockchain, Big Data and IoT.

In the concern for de-concentration and decentralization Figure 1:

The proposal is to provide for a Hub (R i) at the level of each administrative division or territorial autonomy, thus enabling the collection and efficient use of data and decision-making at the local level, and a general Hub at the national level, granting the central government the right to manipulate centralized data for the design of various state policies.

3.2 Model Implementation

The infrastructure of the Blockchain system is split into six layers: data layer, network layer, consensus layer, incentive layer, contract layer, and application layer. The Blockchain infrastructure of our model is shown in Fig.3.



DATA layer

Data Block, Chain structure, Timestamp, Hash function, Merkle tree, Asymmetric encryption

NETWORK layer

P2P network, Verification mechanism, Delivery mechanism

CONSENSUS layer

DDPoS

CONTRACT layer

Smart contracts

APPLICATION layer

Programmable Health

Figure 3.The Blockchain infrastructure of our model.

3.3 Data Storage Protocol Based on Blockchain

Our framework is a distributed system that comprises of a constant succession of blocks, by holding a total rundown of exchange records

- ***The Construction of Data Blocks (Data layer):***

A block comprises of the block header and the block body as appeared in Figure 4. Specifically, the block header incorporates Block version: indicates which set of block validation rules to follow.
Block version: demonstrates which set of block approval rules to follow.
Merkle tree root hash: the hash value of the considerable number of exchanges in the block.
Timestamp: current time as seconds in widespread time since January 1, 1970.
nBits: target edge of a substantial block hash.
Hash of the preceding block: a 256-bit hash value that points to the previous block.

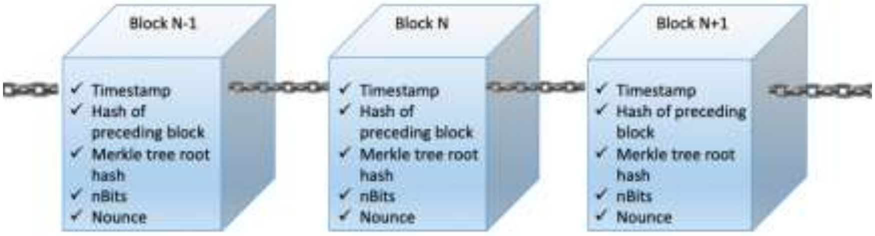
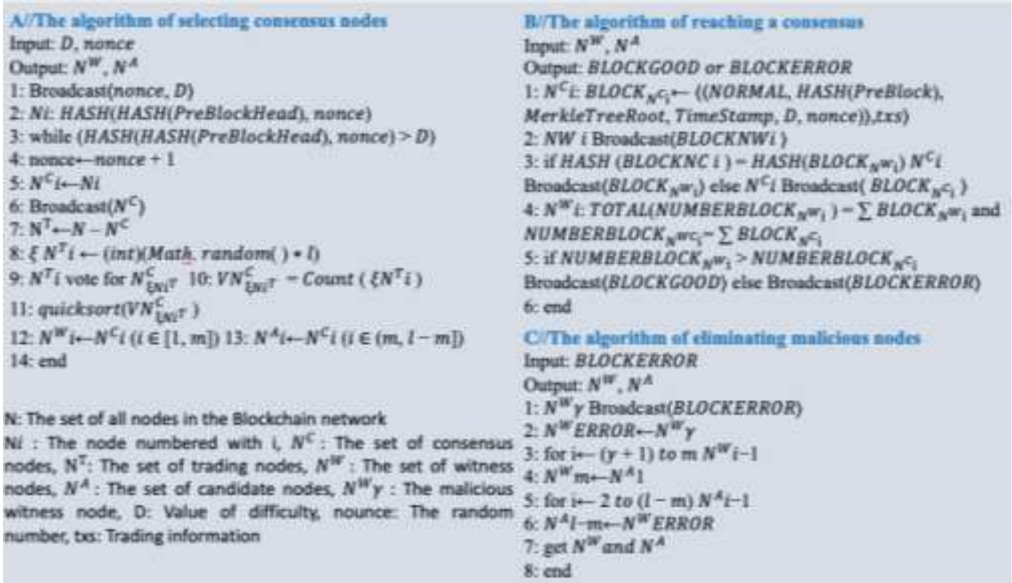


Figure 4. The construction of Data Block.

3.4 DDPosAlgorithm forBlock Verification (Consensus Layer)

Consensus algorithms have an important role to play in guaranteeing the Blockchain's safety and effectiveness. The implementation of a proper algorithm results in a considerable performance improvement of the Blockchain system following a comparative study, our ecosystem is based on an effective consensus algorithm named Delegated Proof of Stake with Downgrade DDPoS (based on the combination of PoW and DPoS's advantages)(Yang et al., 2019), detailed in Fig.5, which ensures:Lower resource consumption, higher operating efficiency and stronger security of the Blockchain.



```
A//The algorithm of selecting consensus nodes
Input: $D$, $nonce$
Output: $N^W$, $N^A$
1: Broadcast($nonce$, $D$)
2: $Ni$: $HASH(HASH(PreBlockHead), nonce)$
3: while ($HASH(HASH(PreBlockHead), nonce) > D$)
4: nonce←nonce + 1
5: $N^C i$←$Ni$
6: Broadcast($N^C$)
7: $N^T$←$N - N^C$
8: $\xi N^T i \leftarrow (int)(Math.random() \bullet l)$
9: $N^T i$ vote for $N^C_{\xi Ni^T}$  10: $VN^C_{\xi Ni^T} = Count(\xi N^T i)$
11: $quicksort(VN^C_{\xi Ni^T})$
12: $N^W i \leftarrow N^C i$ ($i \in [1, m]$) 13: $N^A i \leftarrow N^C i$ ($i \in (m, l - m]$)
14: end
```

N: The set of all nodes in the Blockchain network
Ni : The node numbered with i, N^C : The set of consensus nodes, N^T: The set of trading nodes, N^W : The set of witness nodes, N^A : The set of candidate nodes, $N^W y$: The malicious witness node, D: Value of difficulty, nounce: The random number, txs: Trading information

```
B//The algorithm of reaching a consensus
Input: $N^W$, $N^A$
Output: $BLOCKGOOD$ or $BLOCKERROR$
1: $N^C i$: $BLOCK_{N^C i} \leftarrow ((NORMAL, HASH(PreBlock),$
   $MerkleTreeRoot, TimeStamp, D, nonce)), txs)$
2: $NW i$ Broadcast($BLOCKNWi$)
3: if $HASH(BLOCKNC i) = HASH(BLOCK_{N^W i})$ $N^C i$
   Broadcast($BLOCK_{N^W i}$) else $N^C i$ Broadcast($BLOCK_{N^C i}$)
4: $N^W i$: $TOTAL(NUMBERBLOCK_{N^W i}) = \sum BLOCK_{N^W i}$ and
   $NUMBERBLOCK_{N^W C i} = \sum BLOCK_{N^C i}$
5: if $NUMBERBLOCK_{N^W i} > NUMBERBLOCK_{N^C i}$
   Broadcast($BLOCKGOOD$) else Broadcast($BLOCKERROR$)
6: end

C//The algorithm of eliminating malicious nodes
Input: $BLOCKERROR$
Output: $N^W$, $N^A$
1: $N^W y$ Broadcast($BLOCKERROR$)
2: $N^W ERROR \leftarrow N^W y$
3: for i← (y + 1) to m $N^W i$-1
4: $N^W m \leftarrow N^A 1$
5: for i← 2 to (l − m) $N^A i$-1
6: $N^A l{-}m \leftarrow N^W ERROR$
7: get $N^W$ and $N^A$
8: end
```

Figure 5. DDPoS Algorithm for Block verification

3.5 Data Circulation Protocol Based on Smart Contract (Contract layer)

In this model, we designed intelligent contracts that support two kinds of inquiries: the first is to storing data inquiries, while the second is the data demand inquiry, to improve: Data reliability, data security, and data management. and others for allocating digital contracts between two IoT devices, in order to prevent the same processing task from being executed multiple times, ensure that the execution of a contract among IoT devices can be proved retrospectively and that processing records are traceable.
When the participant A needs to share data to the participant B (see Fig.5); Our model use an asymmetric key encryption,the public-key_private-key pair, “x- X” is the private-key_ public-key par for the participant A, “y-Y” is the private-key_ public-key par for the participant B. Public_key is published(as Pseudonyms ensuring anonymity for patients), and the private-key is kept safe and locked. Instead of sending, will send a simple request, the participant A will send a transaction data Figure encrypted by A’s private_key, and then encrypted by B’s public_key.
B will first decrypt the data using its own private_key, then use A’s public key to decrypt assigned transaction data. This procedure, will ensure that only B can decrypt and receive the data, and that only A could have sent the data.

IV. Discussion

Our proposed system addresses the aforementioned vulnerabilities associated with data storage and privacy. So, integrity, anonymity, security, and privacy of healthcare data must be maintained by the systems. Nowadays, in developing countries, patients are losing their interest in electronic health record systems as privacy and security are threatened in EHR systems. Anonymity of patient is imperative, as personal healthcare data are sensitive. We briefly describe each ofthose properties within the context of our system below:
◦ Privacy: The smart contract is that the authoritative guarantee of the safety of data circulation. it's a computerized transaction protocol, which is totally automatic and not must be supervised. At the identical time, the Blockchain network can monitor the status of the smart accept real time and execute the contract by verifying the external data source and confirming that the particular trigger condition is satisfied. In our case, the info producer can store the info within the Blockchain by calling the shop interface of the contract. the information requester initiates an information authorization request to the contract owner through the contract address and therefore the APIcall query interface.
• Security: Emerging, Blockchain Big Data and IoT, solves the matter of security via mathematically verifiable cryptographic signatures (Public-key, Private-key pair). Blockchain's capability to safely, transparently, and permanently retain information reduces the threat of falsification or corruption by the wrong parties, and ensures the continuous protection and accessibility of the data, as the Blockchain approach does not constitute the Single Point of Failure (SPOF) issue.

• Data Integrity: Blockchain is not only a data structure but also a timekeeping mechanism for the information structure so proof of the history of information is definitely reportable and updated to the second. Merkle tree may be a fundamental component of Blockchains, which uses cryptographic hash functions. Every block stores transaction data within the variety of a tree, a Merkle tree that may be an organization. In it, hashes of kid nodes are combined into the parent node's header and this system continues iteratively until a final, or root, node is reached. This root node acts sort of a fingerprint for the whole tree containing all the data.

• Anonymity: Our system ensures that the Patient's identity is reduced to a public key containing a string of letters and numbers, from 20 to 160 bytes, usually generated from the private key generated by using the tree structure for computing the hash.

• Interoperability: Our proposed Model ensures interoperability between the various health organizations. and since interoperability is increasingly patient-centric, our system allows patients to higher control their data.

V. Conclusion

This document reviews the current digital solutions in the Health system, lists the key stakeholders who play a vital role in the system, and details the untapped assets that encourage the adoption of information technology in the HealthCare sector. It also presents a Model of a Distributed Healthcare system based on the combination of Blockchain, Big Data and IoT technologies. By analyzing the protocol, we showed the strengths of this system. The concerns over integrity, anonymity, security, and privacy have also been addressed in this paper. In our future research, we will deploy this whole system.

REFERENCES

1. Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., Saadi, M., 2017. Big data security and privacy in healthcare: A Review. Procedia Comput. Sci. 113, 73–80. https://doi.org/10.1016/j.procs.2017.08.292
2. AL-mawee, W., n.d. Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey 57.
3. Angraal, S., Krumholz, H.M., Schulz, W.L., 2017. Blockchain Technology: Applications in Health Care. Circ. Cardiovasc. Qual. Outcomes 10. https://doi.org/10.1161/CIRCOUTCOMES.117.003800
4. Baliga, D.A., 2017. Understanding Blockchain Consensus Models. In Persistent.
5. Bhuiyan, M.Z.A., Zaman, A., Wang, T., Wang, G., Tao, H., Hassan, M.M., 2018. Blockchain and Big Data to Transform the Healthcare, in: Proceedings of the International Conference on Data Processing and Applications - ICDPA 2018. Presented at the the International Conference, ACM Press, Guangdong, China, pp. 62–68. https://doi.org/10.1145/3224207.3224220
6. Christidis, K., Devetsikiotis, M., 2016. Blockchains and Smart Contracts for the Internet of Things. IEEE Access 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
7. Darshan K R, Anandakumar K R, 2015. A comprehensive review on usage of Internet of Things (IoT) in healthcare system, in: 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT). Presented at the 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), IEEE, Mandya, India, pp. 132–136. https://doi.org/10.1109/ERECT.2015.7499001
8. Deshkar, S., Thanseeh, R. A., & Menon, V. G. (2017). A review on IoT based m-Health systems for diabetes. International Journal of Computer Science and Telecommunications, 8(1), 13-18.
9. Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., Mankodiya, K., 2018. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Gener. Comput. Syst. 78, 659–676. https://doi.org/10.1016/j.future.2017.04.036
10. Fray, A.-M., 2009. Nouvelles pratiques de gouvernancedans le milieu hospitalier : conséquencesmanagériales sur les acteurs. Manag. Avenir 28, 142. https://doi.org/10.3917/mav.028.0142
11. ichi, Jawab, Boutahari, 2019. The Mixed-Method 5W2D Approach for Health System Stakeholders Analysis in Quality of Care: An Application to the Moroccan Context. Int. J. Environ. Res. Public. Health 16, 2899. https://doi.org/10.3390/ijerph16162899
12. Jarosławski, S., Saberwal, G., 2014. In eHealth in India today, the nature of work, the challenges and the finances: an interview-based study. BMC Med. Inform. Decis. Mak. 14, 1. https://doi.org/10.1186/1472-6947-14-1

13. Leviton, L.C., Melichar, L., 2016. Balancing stakeholder needs in the evaluation of healthcare quality improvement. BMJ Qual. Saf. 25, 803–807. https://doi.org/10.1136/bmjqs-2015-004814
14. Liu, P.T.S., 2016. Medical Record System Using Blockchain, Big Data and Tokenization, in: Lam, K.-Y., Chi, C.-H., Qing, S. (Eds.), Information and Communications Security, Lecture Notes in Computer Science. Springer International Publishing, Cham, pp. 254–261. https://doi.org/10.1007/978-3-319-50011-9_20
15. Lu, Y., 2019. The Blockchain: State-of-the-art and research challenges. J. Ind. Inf. Integr. 15, 80–90. https://doi.org/10.1016/j.jii.2019.04.002
16. Maskeliūnas, R., Damaševičius, R., Segal, S., 2019. A Review of Internet of Things Technologies for Ambient Assisted Living Environments. Future Internet 11, 259. https://doi.org/10.3390/fi11120259
17. Mounia, B., Habiba, C., 2015. Big Data Privacy in Healthcare Moroccan Context. Procedia Comput. Sci. 63, 575–580. https://doi.org/10.1016/j.procs.2015.08.387
18. Sannino, G., De Falco, I., De Pietro, G., 2014. Monitoring Obstructive Sleep Apnea by means of a real-time mobile system based on the automatic extraction of sets of rules through Differential Evolution. J. Biomed. Inform. 49, 84–100. https://doi.org/10.1016/j.jbi.2014.02.015
19. Wu, J., Wang, Y., Tao, L., Peng, J., 2019. Stakeholders in the healthcare service ecosystem. Procedia CIRP 83, 375–379. https://doi.org/10.1016/j.procir.2019.04.085
20. Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N.N., Zhou, M., 2019. Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism. IEEE Access 7, 118541–118555. https://doi.org/10.1109/ACCESS.2019.2935149