International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 09 – Issue 03 || May - Jun 2024 || PP. 28-35

A Heterogeneous EMR Sharing System using Blockchain

Kala Chandrashekhar, Alfiya Sama, Arushi Pundir, Ghazala Jamal, Harsh Ranjan

Dept of CSE,
SJB Institute of Technology, Bangalore, India

Abstract: Blockchain technology in recent years had made possible the use of decentralized databases with a broad range of applications. Patient identity, payment history, and other critical information require medical information, which has grown in significance. Nevertheless, prior instances of data breaches highlight the necessity for enhanced safety and isolation protocols. Furthermore, duplication of testing and resource waste occur in the present healthcare system due to hospitals' incapacity to access electronic medical records (EMRs). We suggest a safe inter-hospital EMR sharing system construct on blockchain technology to overcome these problems. Programmatic permission is achieved by this system with the use of smart contracts, which secure EMRs. Mutual authentication, data integrity, nonrepudiation, user untraceability, forward and backward secrecy, and resilience to replay attacks are all crucial features it offers. Our system makes it possible for healthcare organizations to share EMRs seamlessly by harnessing blockchain technology.

Keywords: Blockchain, Mutual authentication, nonrepudiation, untraceability, blockchain, EMR, and BAN logic.

1. Introduction

Blockchain technology has the ability to improve the logicality, security, safety and confidentiality of systems that exchange Electronic Health Records (EHRs). Unlike established centralized databases, blockchain offers a decentralized, unyielding ledger that can enhance data integrity and enable healthcare providers to exchange private patient information in a safe way. Still, classic security issues like Denial of Service (DoS) attacks and single points of failure might affect solutions that currently exist that rely on centralized databases. Moreover, previous approaches failed to adequately handle speed and scalability issues and left consumers vulnerable to privacy linkage attacks.

To address these shortcomings, we suggest a secure inter-hospital EMR sharing system in accordance with the technology of blockchain. Our solution offers a reliable and secure platform for hospitals and health care organizations to share electronic health records amongst one another by exploiting blockchain technology. The safety, isolation, and interoperability issues with standard electronic medical record (EMR) systems are dealt with by our approach by utilizing the distributed structure and cryptographic characteristics of blockchain.

Blockchain technology supports the entire system, rendering it virtually impenetrable to hackers. By preventing a single point of failure, the decentralized consensus system of blockchain reduces the possibility of data breaches and illegal access. Additionally, our solution makes use of smart contracts, which do away with the need for middlemen and guarantee transparency in data exchanges. Smart contracts make it feasible to share EMRs safely and easily by automating the application of pre-established rules.

To further ensure the confidentiality and privacy for health information, the system we store data with the Inter Planetary File System (IPFS). By distributing data over a network of nodes, IPFS is a decentralized storage structure that protects against censorship and manipulation. Our technology guarantees patient data privacy, making it available to authorized parties only, by storing EMRs on IPFS.

We will describe the scheme and execution of our blockchain-based inter-hospital electronic medical record sharing system, go over its safety and isolation measures, and assess its scalability and efficiency in this paper. Our objective is to present how blockchain technology can improve the safety and confidentiality of information, transform EMR sharing, and promote healthcare delivery.

2. Literature Survey

An innovative method to enable safe inter-hospital exchange of Electronic Medical Records (EMRs) via blockchain technology has been portrayed in A Blockchain-Based Secure Inter-Hospital EMR Sharing System [1]. The blockchain center, the patient, the hospital, and the medical index are the four main components of the system. The suggested solution is to improve efficiency, security, and confidentiality in the sharing of medical information by utilizing blockchain. Data integrity, non-repudiation, user untraceability, forward and backward secrecy, and resistance to replay attacks are all guaranteed by the system's architecture. The suggested scheme's effectiveness and safety are thoroughly examined in this study, and the validity of the solution is evaluated using

the BAN logic proof model. Potential drawbacks, however, might include the requirement for practical testing and validation, scalability constraints, potential legal difficulties, and problems integrating with the current healthcare IT system. Notwithstanding these possible drawbacks, the study advances the developing field of blockchain based safe healthcare data exchange.

The article "Sharing Medical Data using a Blockchain-Based Secure EHR System for New Zealand" [2] delves into the procedure of establishing a blockchain-based secure electronic health record (EHR) system in New Zealand. The document explores relevant literature, clarifies use case scenarios, and describes the prerequisites of the suggested fix. It addresses issues with the current healthcare IT systems in New Zealand and emphasizes the advantages of implementing a national EHR system. The authors stress the requirement to enhance data integration and collaboration among providers whilst promoting the possible uses of blockchain-based technologies for medical applications. The study does, however, admit many shortcomings, such as worries around data security and privacy. This study uses cryptographic approaches, including blockchain-based smart contract technology for access control and encrypting strategies, to counter these restrictions. The authors recommend using Javascript and the CryptoJS library for client-side cryptography operations, such as AES encryption and decryption, and a server for authentication to handle cryptographic resources and improve usability. Even with these developments, further study and real-world testing are essential for validation, especially in light of the possible drawbacks and practical consequences for blockchain-based EHR systems like MedBloc.

3. Proposed System

Our suggested method uses blockchain technology to cultivate a heterogeneous inter-hospital EMR sharing system. Making the secure, efficient, and interoperable transfer of electronic medical records (EMRs) across healthcare facilities is the primary objective of this system.

3.1 System Architecture

The architecture of our proposed system consists of the following key components:

[1] Blockchain Center: Owned by a public health facility, its blockchain center acts as the main hub for medical and personal mobile device administration. Using the mobile devices and institution medical devices enabling mutual verification, all patients and hospitals must sign up to the blockchain center.
[2] Patient: The patient has a personal mobile device that they have to use to store identification verification messages. They use their personal devices to prove their identity to both the hospital and themselves when seeking medical care. The medical index of the hospitals that the individual visited previously is additionally kept on the personal mobile device, which will make it available to additional hospitals in the future to be used as a medical record reference.
[3] Hospital A: Medical gadgets are utilized by the hospital's doctors to make diagnoses. Mutual authentication takes place in Hospital A and the patient when a patient presents with symptoms. In incorporation to evaluating patients, Hospital A keeps medical records on file on its system. Patients receive findings from diagnosis from Hospital A, which they retain on their mobile device together with the medical index.
[4] Hospital B: Medical gadgets are utilized by the hospital's doctors to make diagnoses. Hospital B and the patient mutually authenticate when a patient visits Hospital B for treatment of symptoms which had been noticed at Hospital A. Hospital B uses the patient's own mobile device to get Hospital A's medical index. After the patient is diagnosed, Hospital B receives the patient's medical records from Hospital A and keeps them on its system. Patients receive results from Hospital B on their diagnosis, which they retain on the mobile device along with their medical index.

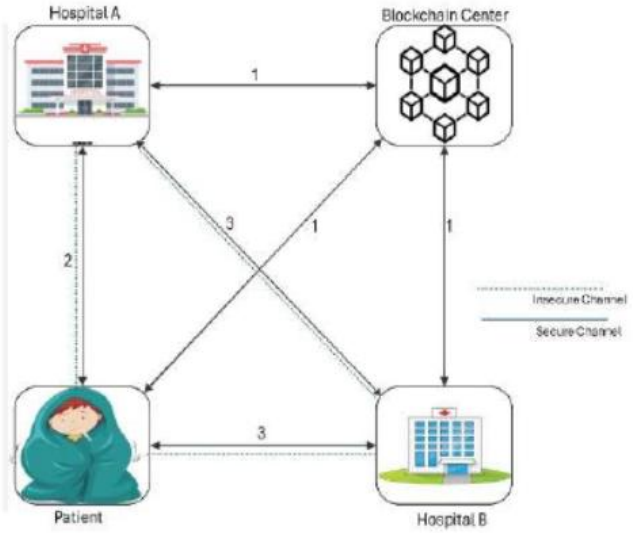


Fig 1: System Architecture

3.2 System Workflow

The workflow of the proposed system is as follows:

- **EMR Generation and Encryption:** Robust encryption methods are utilized to encrypt newly created electronic medical records (EMRs) for use by patients in medical facilities.
- **Decentralized Storage:** Next, the encrypted EMR is channeled to the decentralized storage system.
- **View Request:** A request is made via the blockchain network for access to an individual's electronic medical record (EMR) from another healthcare facility or other authorized organization.
- **Execution of Smart Contracts:** In the blockchain, smart contracts verify access requests in accordance with pre-established guidelines and authorization.
- **Decryption:** The required EMR is decrypted and given to the authorized person after validation.
- **Data Exchange:** As needed, a designated individual can access, amend, or contributes new data to the EMR.

On the blockchain, every transaction is documented for accountability and transparency.

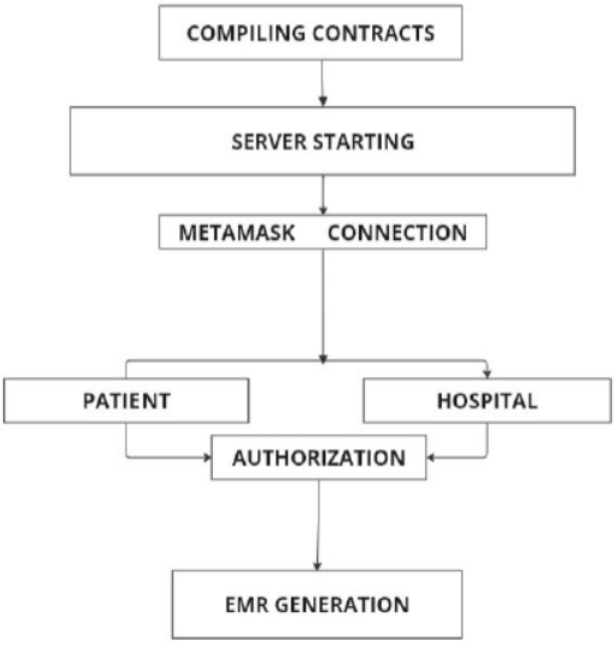


Fig 2: System Workflow

3.3 Security and Privacy Measures

Our system incorporates the following security and privacy measures:

- **Encryption:** EMRs are encrypted before being stored, and access permission is requisite to decode the data.
- **Access control:** Only certified persons are able to read or alter EMRs thanks to the enforcement of access control restrictions using smart contracts.
- **Data Integrity:** By prohibiting unwanted alteration, the blockchain guarantees the integrity of EMRs.
- **Anonymity of Users:** By making user identities anonymous, the blockchain safeguards users' privacy
- **Audit Trail:** Every transaction is updated on the blockchain, creating an irreversible audit trail that is utilized to ensure accountability.

4. Implementation

[1] Development Environment:

Truffle, Ethereum, Web3, Solidity, Ganache, and the mainnet Ethereum network will all act a part in the development of our suggested solution. With instruments for developing, testing, and implementing smart contracts, Truffle, a well-liked Ethereum development framework, will expedite the process. Ganache will operate as our local blockchain network while we're developing, making it easier to test and debug smart contracts quickly. The foundation of our system, smart contracts, will be built in Ethereum's Solidity programming language, thereby guaranteeing the construction of safe and effective smart contracts. Our front-end interface will be able to transmit with the network of Ethereum computers thanks to a JavaScript package called Web3.js.

[2] Smart Contracts:

Aspects of the EMR sharing system will be controlled by the smart contracts. Contracts pertaining to hospital registration, authentication, and medical record storage along with patient registration, authentication, and index storage will be developed by us. While data storage contracts work with IPFS to safely store and retrieve encrypted EMRs, access control contracts will enforce standards and permissions for EMR sharing.

[3] Integration with IPFS:

To secure data availability and integrity, the Inter Planetary File System (IPFS) will be incorporated for decentralized EMR storage. IPFS will work with smart contracts to securely store and retrieve encrypted EMRs. We are going to deploy the front-end application and smart contracts on the Ethereum mainnet network once the development and testing have finished.

[4] Deployment to Ethereum Mainnet:

To facilitate communication between patients, hospitals and healthcare providers in the system, an intuitive online interface will be created. Through the interface, patients will be capable to securely register, authenticate, and exchange their EMRs. Through the interface, medical personnel may check patient data, edit medical records, and request access to EMRs.

[5] User Interface:

User interface will provide an interactive way to communicate with the system. In this user, hospitals and healthcare workers will be able to get the information in one click from the blockchain.

[6] Testing and Deployment:

At every phase of the development process, thorough testing will be done to guarantee the system's operation and security. The technology will be made available for public usage on the Ethereum mainnet network when testing is finished.

5. Security and Privacy

Our proposed system integrates several safety measures to ensure the confidentiality, integrity, and accessibility of electronic medical records (EMRs).

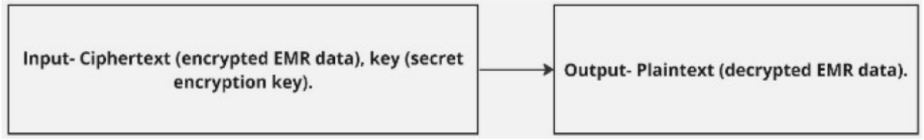
5.1 Encryption Algorithm

Our system's encryption technique makes sure that EMRs are safely encrypted before being transferred or stored. We use the Advanced Encryption Standard (AES), a symmetric encryption method that is renowned

for its security and efficiency. EMR data in plaintext is encrypted and then transformed into cipher text using a secret encryption key. This make sure that anyone who are not allowed to view the data will be unable to decrypt it without the encryption key.

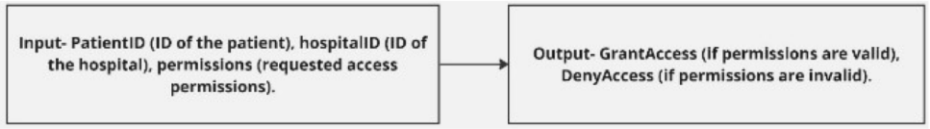
5.2 Decryption Algorithm

For reading or processing, authorized parties can decode ciphertext EMRs back into plaintext using the decryption technique. For this operation the same secret encryption key that is used for encryption is needed, which is encryption in reverse. The original EMR data can only be retrieve by those who possess the proper decryption key.



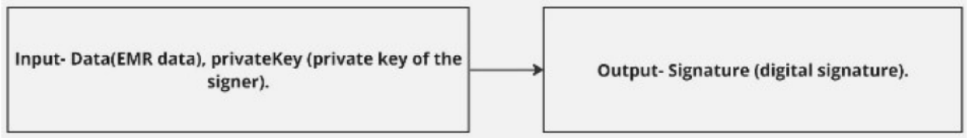
5.3 Access Control Algorithm

To guarantee that only certified healthcare practitioners have authority to patient EMRs, access control is essential. The access control algorithm checks if a hospital has the right to access a patient's electronic medical record. Based on established rules and permissions, it verifies the validity of the requested access permissions. Access is given, enabling the hospital to read or edit the EMR, if the permissions are legitimate. In the event that access is refused, patient data is shielded from unwanted access.



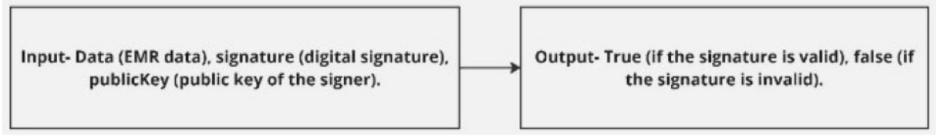
5.4 Digital Signature Algorithm

EMR data integrity and validity are confirmed by digital signatures. Our approach employs the generally used Elliptic Curve Digital Signature method (ECDSA) for electronic signatures. Every time a healthcare provider creates or modifies an electronic health record (EMR), they use the private key to create a digital signature. The EMR data includes this signature, which anybody who have access to the public key of the provider may validate. Verifying that the signature is legitimate verifies that the EMR data is authentic and comes from the physician who signed it.



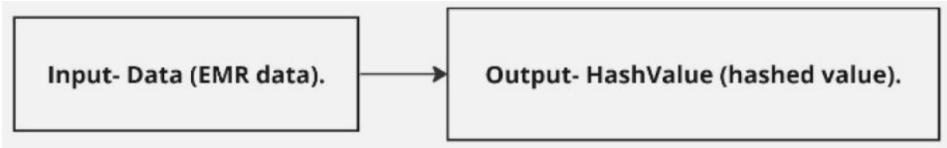
5.5 Verification Algorithm

The verification technique verifies the reliability of digital signatures associated with EMR data. It ensures that the signature was developed by the purported signer and that the data hasn't been altered since the signature was applied. The method of verification uses the signer's public key to validate the signature against the EMR data. The reliability and fairness of the data are confirmed by the signature's validity, providing confidence that the EMR data is real and unmodified.



5.6 Hashing Algorithm

Hash values, unique identifiers for EMR data, are produced using hashing. Our system uses the SHA-256 hashing technique, a cryptographic hash function well known for its security characteristics. When EMR data is encrypted a fixed-length of hash value is generated, that serves as a unique representation to the data. Data consistency, illegal alteration detection, and integrity verification of EMR data are all achieved by hashing.



Together, these safety and isolation measures make certain that patient data is kept private, unchangeable, and only available to those who have permitted authorization to our blockchain-based inter-hospital EMR sharing system.

6. Results

The below given pictures/figures provide some incites of our project.

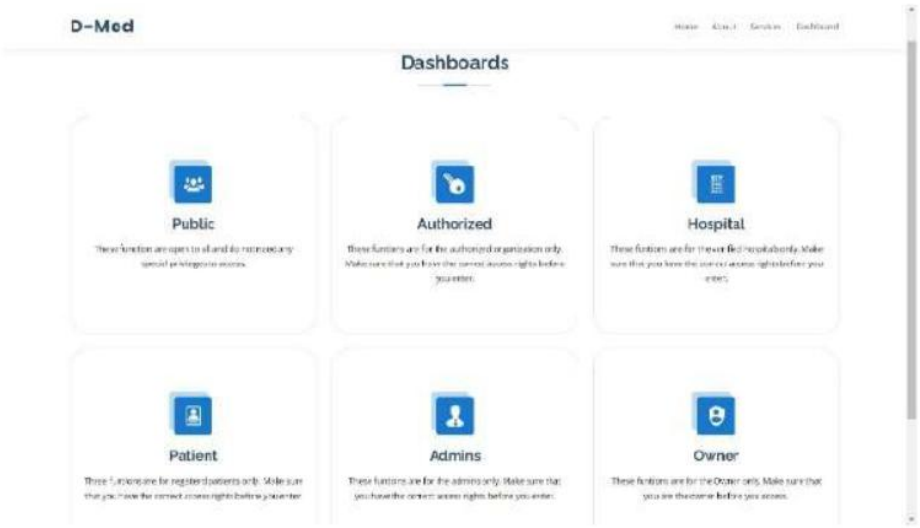


Fig 3: Main Dashboard

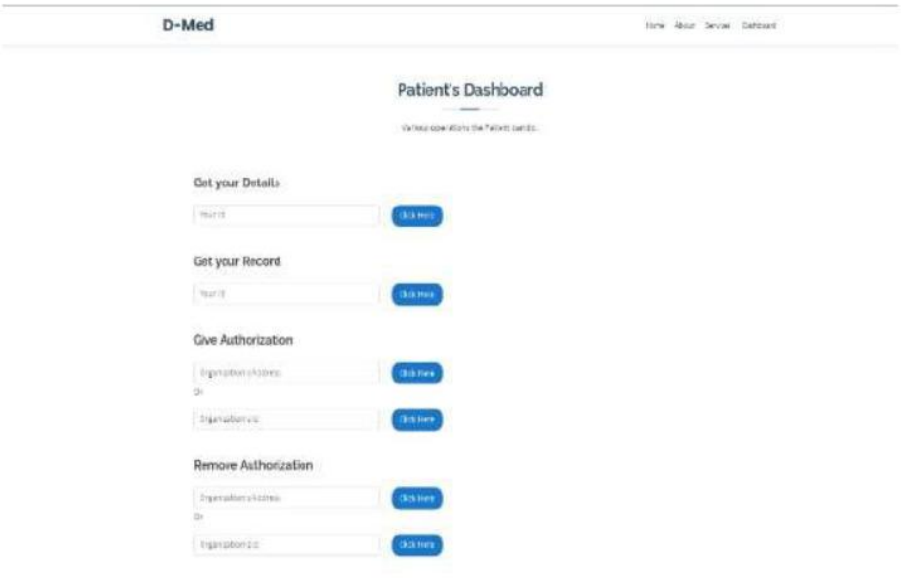


Fig 4: Patient's Dashboard

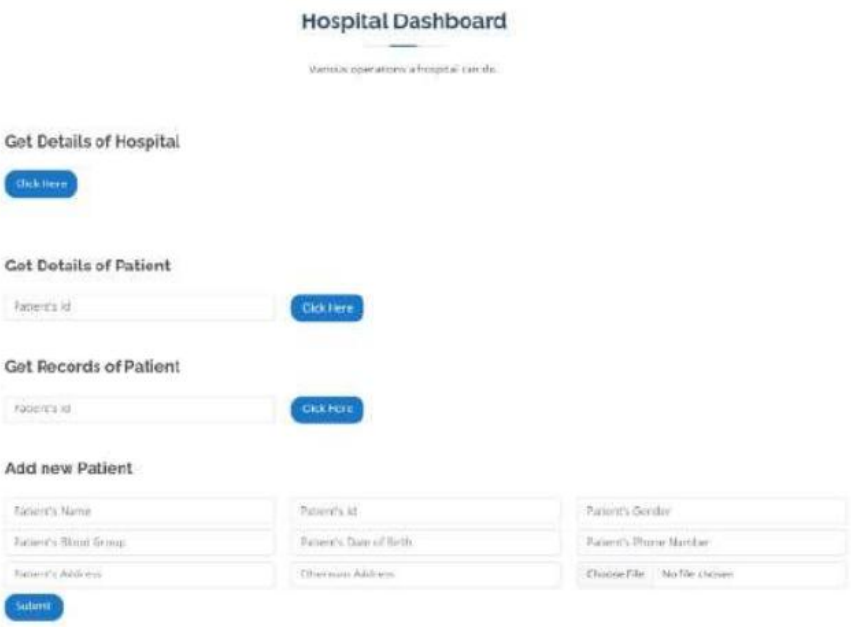


Fig 5: Hospital Dashboard

7. Conclusion

The significance of medical data, such as patient identities, payment histories, and medical records, has grown significantly with the advancement of medical technology. This information is very private, though, and there have been notable breaches of private information due to factors like operational errors and hacker attempts. Studying patient privacy protection and medical data security has become essential.

Furthermore, individuals' medical records are not quickly accessible between hospitals under the present medical system. Medical resources go unused and unnecessary exams result from this absence of interoperability. Access to medical records between hospitals must thus be made possible.

To overcome these issues, our study suggests a blockchain-based secure inter-hospital Electronic Medical Record (EMR) sharing system. In our proposed approach, the blockchain center provides identity verification keys to the members of medical alliance, considering that hospitals and patients are in same group. As a result, patient's medical records are available across organizations and alliance members can interact legally and exchange data. This method increases the effectiveness and quality of medical care while preventing the waste of medical resources.

We have made confident that our suggested plan complies with multiple security regulations. The suggested method works well in regard of computing and communication costs when assessed according to BAN logic proof model.

In conclusion, there is an increasing chance that blockchain-based technology will be used in the medical industry. In addition to safeguarding individual privacy and enabling the exchange of medical resources, our suggested method also questions the effectiveness of blockchain transactions. This creates opportunities for comparativing blockchain-based platforms in regard of evaluation of performance through future study.

8. References

[1]. Blockchain Technology of Healthcare: A Comprehensive Review and Directions for Future Research" by Zhang et al. (2018).
[2]. Azaria et al. (2016) "Achieving Interoperability in Health Record Systems: A Blockchain Approach."
[3]. Yue et al. (2020) "Security and Privacy on Blockchain-Based Electronic Health Record Systems."
[4]. Li et al. (2018) "Blockchain-Based Access Control for Healthcare Systems."
[5]. Li et al. (2019) propose "A Scalable Blockchain-Based Platform for Healthcare Data Access Control."
[6]. Krawiec et al. (2019) "Blockchain: The Evolutionary Next Step for Healthcare Interoperability."
[7]. Understanding Users' Intention to Continue Using Mobile Health Apps: A Privacy Calculus Model and Trust Transfer Perspective by Zhang et al. (2021). Nguyen et al. (2020) present "
[8]. A Blockchain-Based Design for Collaborative DDoS Mitigation with Smart Contracts."

[9]. Blockchain-based smart contracts: https://www.geeksforgeeks.org/ The design ideas for transitioning from old systems to blockchain systems in 202001 may be found at : https://www.geeksforgeeks.org/smart-contracts-inblockchain/
[10]. https://blockchain.ieee.org/images/files/pdf at https://blockchain.ieee.org Nakamoto, S. (2008),
[11]. A peer-to-peer electronic cash system is called bitcoin. taken from the bitcoin.org/bitcoin.pdf website.
[12]. Lippman, A., Vieira, T., Ekblaw, A., & Azaria, A. (2016). MedRec: Blockchain Technology for Medical Data Access and Permission Control. On pages 25–30, in the 2nd International Conference on Open and Big Data (OBD). IEEE.
[13]. Jiang, W., Jin, D., Yue, X., Wang, H., and Li, M. (2016). Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. Medical Systems Journal, 40(10), 218