An Integrated System of Blockchain with AL-SHIFA 3+ Healthcare Information System (HIS) in Oman

Yasmin Essam[1], Mohammed Izaan[1], Iqra Saleem[1], Aida[1] and Jitendra Pandey[1#]

[1]Middle East College, Muscat, Oman
[#]Advisor

ABSTRACT

Al-SHIFA 3+ is a healthcare information system (HIS) introduced by the Ministry of Health (MOH) in Oman in 2015, with the aim of automating all the healthcare management processes in healthcare institutions including electronic medical records, assets, inventory, and HR management, and replacing all the paper charts used in intra-departmental communication with Computerized Physician Order Entry (CPOE). Currently, this system in The Sultanate of Oman is benefiting around 85% of public healthcare seekers. However, the security of the system is a great concern, since any security gap can be exploited by attackers, therefore violating the confidentiality and integrity of patients' data. This research paper proposes integrating Blockchain technology with AL-SHIFA 3+ Healthcare Information System (HIS) in Oman, to ensure secure data access and transmission between healthcare entities. Blockchain is a technology that uses cryptographic hash functions to encrypt and secure the information that is stored in blocks, where each block is connected to the previous one in the form of chains making it tamper-proof as well as protecting it from ransomware and other cyberattacks. Thus, by implementing blockchain technology, information can be shared securely among authorized medical staff to help them make critical decisions that will improve the quality of the given healthcare services. This paper will show how to set up a blockchain environment, and the used software platforms, as well as the benefits of integrating blockchain technology with AL-SHIFA 3+ HIS along with its limitations and challenges that are likely to be faced while implementing this technology.

Introduction

Blockchain is a decentralized security technology that uses cryptographic hash functions for the encryption of information in the form of blocks to keep it secure. Every block in a blockchain is connected with the previous block forming a chain of blocks. Blockchain Technology is tamper-proof since a change made in a single block of the chain will alter the hash for all the other blocks. This makes the detection of a possible attack by an unauthorized user easier. Moreover, it is not easy to make changes in a block since blockchain works on the fundamentals of a smart contract system, and modifying data in a single block would require permission from all the users involved. Due to all such reasons, blockchain is one of the most secure ways of storing confidential and private information and carrying out day-to-day transactions. It protects organizations and users from cyberattacks such as phishing, malware, ransomware, data breaches, and data manipulation (Agbo et al., 2019).

Health Information System (HIS) is an example of storing data of various medical hospitals and clinics with the help of a digital system that uses many different tools, software, and applications. Health Information System (HIS) is adopted around the globe by various organizations to store healthcare records and patient details in an organized and systematic manner for enhancing the healthcare journey of a patient and the hospital staff. AL SHIFA 3+ is an example of a HIS system adopted by the Ministry of Health in Oman over the past few years. It has been a great success in Oman as it accomplished its aim of transforming health records from manual to automated (Al-Gharbi et al., 2015). According to Khan and Ismail (2017) nearly 200 healthcare facilities across Oman of different sizes and capabilities have implemented this system. Implementing blockchain technology in such a widely used system would be beneficial as it would secure storing of patients' data and the data transfer between hospitals or different departments in the same hospital.

The main goal of this paper is to suggest a method to implement blockchain technology in AL-SHIFA 3+ Healthcare Information System that will boost the security, efficiency, and privacy of highly sensitive healthcare data of the existing system. The paper will also discuss the different platforms required to set up the blockchain environment, and the methodology adapted to complete this project. The main objectives of the paper are: integrating a blockchain into AL SHIFA 3+ system using Ethereum IDE, investigating the types of different consensus mechanisms and the factors affecting the choice of the consensus mechanism, and restricting access to the authorized users of the system based on predefined assigned roles using RBAC (Role-Based Access Control).

The remaining research paper will consist of 6 sections. Section 2 will have a detailed analysis of related work that covers different aspects such as blockchain definition, consensus mechanisms, and integration of blockchain with EHR. Section 3 will include a SWOT analysis as well as a description of the adopted methodology in this project. Section 4 will illustrate the proposed system's architecture and the software to be used. Section 5 will have the simulation processes and the analysis of the obtained results, and section 6 will be for conclusions and further recommendations.

Related Work

What is Blockchain Technology

Blockchain technology is based on a decentralized and distributed ledger system that has gained popularity recently due to its capability to enhance security systems in various industries. According to Lemieux (2017), the technology has been hailed as a game changer due to its ability to store data in a tamper-proof and transparent manner, allowing it to have increased trust and security. It mainly uses cryptographic algorithms to guarantee data integrity and immutability. Blockchain stores data in blocks that are connected together in a chain where each block comprises the hash of the previous block which results in a counterfeit-resistant record of all transactions. A blockchain's mechanism entails triggering a transaction from one node to another, broadcasting information to all network participants, validating and verifying the transaction based on the chosen consensus algorithms by all network participants, creating a new block based on validation and verification, adding the new block to the chain, and finally sharing the information across the network. Lemieux (2017) also discusses how blockchain can help with audibility by offering an open and irrevocable record of all data changes. Moreover, it can improve accessibility by allowing users to access and verify records without the use of intermediaries. According to Junejo et al. (2021), blockchain is frequently associated with cryptocurrencies such as Bitcoin, but its potential uses extend far beyond finance such as supply chain management, healthcare, and identity management to name a few.

Motives to Use Blockchain Technology

There are many problems associated with using a centralized system for sharing Electronic Health Records (EHRs). According to Wang et al. (2019), some of the problems faced by centralized systems that are discussed in the article are data breaches, lack of patient control, interoperability, and standardization. As centralized EHR systems are vulnerable to data breaches, it can jeopardize the confidentiality and security of sensitive patient data. As a result, significant consequences such as medical fraud, identity theft, etc. might be faced. Wang et al. (2019) further describe how patients' privacy is compromised when their information is accessed by unauthorized parties due to patients' lack of control over who gets to access their electronic health records. This might also cause significant financial and legal consequences for healthcare providers. Furthermore, it is difficult to share patient data between different hospitals as different health institutions use different centralized EHR systems which results in a lack of interoperability. Wang et al. (2019) cite multiple studies in the article that highlighted the vulnerabilities of centralized EHR systems, including a 2019 ProPublica analysis that discovered that over 150 US healthcare institutions had their EHRs compromised in the past decade. Another study includes a Check Point Research report from 2020 that found a 45% rise in ransomware attacks on healthcare companies in the United States alone. Spence et al. (2018) also mention a Ponemon Institute report from 2017 that indicated the average cost of a ransomware attack on a healthcare firm to be $2.4 million. As a solution to the issues of EHR sharing, blockchain technology was suggested as it can create a decentralized platform that will enable secure storage and transfer of EHRs and also allow patients to have authority over their data (Wang et al., 2019).

In another article, Khalid et al. (2023) provide insight into the potential of blockchain technology as opposed to centralized systems. The article again highlights the advantages of blockchain-based storage systems which include enhanced security, privacy, and data integrity. Data is distributed across multiple nodes which eliminates the risk of data loss that might be caused due to a single point of failure such as a cyberattack or server crash. This significantly improves security. Furthermore, the cryptographic authentication method prevents data tampering and maintains the accuracy of stored or transferred data. Decentralized blockchain-based storage networks are cost-effective because they eliminate the need for expensive intermediaries such as cloud service providers or data storage providers. Also, decentralized blockchain-based storage networks can allow greater accessibility to data, as they are not limited to a single server or location. It allows users to access data from anywhere in the world. These advantages are pointed out to make blockchain-based storage systems an appropriate option for various applications in different sectors such as healthcare, finance, and social networks. (Khalid et al., 2023).

Integrating Blockchain with EHR

Blockchain implementation in healthcare was previously tested by many researchers. Azaria et al. (2016) proposed a healthcare system MedRec that used blockchain technology based on a decentralized EMR management system. It worked based on three types of Ethereum smart contracts. MedRec allowed interoperability by first authenticating the user and then allowing third parties to access patients' EHRs that were stored by different medical institutions. In another article, Xia et al. (2017) propose a system called BBDS which uses blockchain technology to facilitate the secure and transparent transfer of EHR data. BBDS utilizes a permissioned blockchain to ensure the privacy of data that allows patients to control access to their health records. The system also consists of a smart contract that assists data sharing between various healthcare providers. BBDS is a blockchain-based EMR sharing solution created primarily for cloud-based environments. BBDS employs a hybrid blockchain architecture that combines a public blockchain for hashed EMR metadata storage and a private blockchain for actual EMR data storage. This architecture is intended to strike a balance between data security and scalability, which is difficult to achieve with typical blockchain solutions. Similarly, Jabbar et al. (2020) suggested another solution named BiiMed which is also a blockchain-based solution developed for healthcare data management and sharing. BiiMed uses a permissioned blockchain network and is described as a peer-to-peer (P2P) blockchain network with existing health information exchange (HIE) standards, making it easier to integrate with existing healthcare providers to increase data security, and integrity, and enhance interoperability. To ensure compliance with relevant rules and industry standards, BiiMed combines various technologies and standards, such as HL7 FHIR and XACML.

Challenges of Implementing Blockchain Technology

However, one of the most significant challenges in implementing blockchain technology in healthcare is limited scalability. The blockchain network becomes increasingly sophisticated as the number of transactions increases, as does the time necessary to validate and verify each transaction. As a result, network participants may experience slower transaction processing times and higher fees. This scalability issue might be especially significant in healthcare, where vast volumes of data are collected daily. Another difficulty is integrating blockchain with existing healthcare

IT systems. Integrating blockchain technology with legacy EHR systems can be difficult, requiring major time and resource commitments. Furthermore, blockchain solutions demand specialized technical expertise, which may be costly for many healthcare organizations.

Methods and Methodology

Methodology

The selected methodology for this project is Agile SDLC Methodology. It is crucial for a blockchain security system to have a working system that can be tested and validated at each stage of development. Additionally, the blockchain system requires responding to threats in a fast manner as well as integrating new updates, these factors are offered by Agile methodology.

The flowchart below illustrates the stages involved in this model along with explanations.

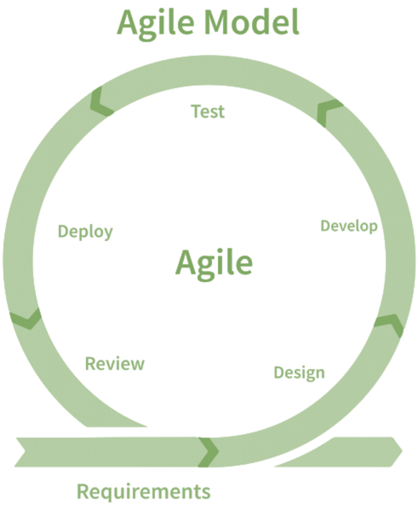


Figure 1.

(InterviewBit, 2021)

Note: Fig 5 from InterviewBit, 2021. "Agile Model: Overview, Manifesto, Principles, Methodology, and More" https://www.interviewbit.com/blog/agile-model/

- Requirement Gathering(the planning phase): During this phase, we calculated the time and effort that was required for the completion of the project. We also recognized the security requirements of the blockchain system.
- Design the requirement: The features and functions of the project are designed virtually according to customer needs. We intend to design the system to be robust and unaffected by attacks using a virtual machine such as Ethereum VM.
- Develop/Iteration: During this phase, our team would work to create the blockchain security system using an approach using increments. The compiled codes using Ethereum will be deployed in the blockchain.
- Test: We will use specific testing techniques to identify any vulnerabilities in the system, if present, and to check the functionality and quality of our system. We will send the data of a block and check if the transaction is made successfully. We can also add new blocks to the blockchain for the testing phase.
- Deployment: When the testing is passed we are assured that the blockchain is secure under various conditions so the product will be released to the customer in the deployment phase.

- Review / Feedback: The customer and user will provide their feedback and they will review the product if it is accepted.

Software Platforms

In the following section, some components and software platforms required to set up a blockchain environment such as: Smart contracts, Ganache, Truffle and MetaMask are explained.

- Smart contracts: A smart contract is a small self-executing computer program that is stored in a blockchain that contains the predefined terms and conditions of an agreement. They are tamper-proof, cryptographically secure, transparent automatic contracts that are executed once the predefined conditions of a transaction are met. They also eliminate the use of third parties in between the peers, which helps speed up transaction processes. Smart contracts are created using Solidity, which is a high-level programming language that contains all the functions needed to create accurate conditions needed on a blockchain. After compiling the programmed operations, they can be deployed and checked on the Ethereum blockchain during run-time. To convert the solidity code to bytecode that can be interpreted by the Ethereum Virtual Machine (EVM), a command-line compiler such as Solidity Compiler (Solc) will be used. Either Solc or Solcjs can be used depending on the environment. For instance, Remix IDE Ethereum uses Solcjs as a compiler since it is more appropriate in Node.js and browser environments.
- Ganache: is a local ethereum blockchain development tool used to test smart contracts and decentralized apps (Dapps) in a safe controlled environment before deploying them in the real network. It allows the developers to identify and fix errors before running the blockchain on the network, which ensures the intended security and reliability as achieved as well as lowering the costs of deploying smart contracts on the main network. It provides fake Ethereum addresses with 100 ETH in each to enable a GUI simulation of blockchain network.
- Truffle: is an open-source development framework for building decentralized applications (dApps) on the Ethereum blockchain. It provides a suite of tools and utilities that make it easy for developers to create, test, and deploy smart contracts and dApps on the Ethereum network. It includes several key components, including a smart contract compiler, a testing framework, a development console, and a build pipeline. These tools enable developers to write and test their smart contracts and dApps in a sandbox environment before deploying them to the Ethereum network.
- MetaMask: is a popular web3 wallet that enables users to interact with the Ethereum blockchain and decentralized applications (dApps) from their web browser. It is a browser extension that functions as a bridge between the user's browser and the Ethereum blockchain, providing a secure and user-friendly interface for managing Ethereum accounts, sending and receiving Ether tokens, and interacting with dApps. It includes several key features, including support for multiple Ethereum networks, custom gas fees, and the ability to import and export private keys.

System Architecture

EHR System Model

Figure 2 shows how different agents interact in the system. Via a web application, different agents will access the system with the aim of providing or requesting information. After being authenticated, the smart contract of the required transaction will be executed depending on the user type. For instance, when a doctor or a patient tries to access the system for performing a specific task, the request will be sent to the smart contract, after the verification of their account address and role, they will be given access to the corresponding predefined operations of their roles. The EMR smart contract will be executed once the account address and role match the requested operation. To ensure transparency, the transaction will be broadcasted to all the nodes on the peer-to-peer network for verification. Once the transaction is verified by all the nodes using consensus algorithms (known as the mining process), the new block will be added to the blockchain network, and the results will be displayed to the user. In this process, immutability, transparency, and efficiency are achieved making the patient's data more secure and easily accessible to authorized entities.

How Do Different Entities in The System Communicate?

To start the communication of the entities with the system these steps are conducted:

Firstly, Registration of the agent: The admin will assign the new agent an account and a role. Using Ganache Ethereum, a private key will be used to create the account since each different account will be assigned a unique private key. The added role will be saved in the RBAC (Role Based Access Control) so that it can be used to determine the level of authority and the operations this account has access to perform. After verifying the account address using MetaMask (ETH Wallet), the account will be connected to the blockchain network and the agent information such as their ID and account will be added through a smart contract to allow successful registration to the blockchain.

Secondly, Authentication of agent: To start interacting with the system the registered users should authenticate themselves. Using their account address, the RBAC will be checked to give them access to operations matching their assigned roles.

Lastly, to perform an operation such as accessing and modifying patient records, the agent will send an access request throughout the smart contract that checks the requestor's identity and level of authority and if it matches with their predefined rights, they will be authorized to perform the needed tasks, otherwise the request will be rejected.

System Entities and their Roles

The proposed system will have three main entities: an administrator, a doctor, and a patient. Each entity will have different roles assigned to them based on their authority level and the information they need to perform their tasks. The administrator has access to all the actions since he is the highest authority in the health care system. He will be able to perform different system management tasks including adding doctors, managing, and verifying users' accounts, assigning roles, and managing the security of the whole system. A doctor will be able to perform tasks related to their job only such as viewing, editing, and updating patients' records, checking appointments, and changing their personal details. A patient will have limited access to only view his records, modify his personal details, and make appointments.

Login Pages

On the administrator login page, once he tries to access the system, he will be asked for the private key of his account to authenticate his identity. This key should match the assigned key to the Ethereum wallet from Ganache Ethereum. After confirming his identity via the Ethereum Wallet, he will be given access to lots of system management tasks. The admin can add patients, add doctors, delete records, check appointments with the doctor, and confirm any needed updates.

For the doctor, after authenticating his identity using the appropriate information and private key, he will be granted access to several operations. In addition to viewing the appointments which is allowed for an admin as well, he will be given more responsibilities. A doctor can view and update their personal information such as phone number or photo. He can view the patients' records to evaluate their condition based on previous prescriptions, scanning, or allergies. Also, he can alter and change those records if needed depending on the current patient's condition, or even delete the unnecessary records.

For the patient to log in, they should enter the needed information and their private key. If that key was not matching and did not get confirmation from the Ethereum Wallet, the access will be rejected, and the patient will be asked to re-enter his correct password. Once logged in the patient can perform the actions required to complete his tasks. Patients can view their personal details, view their medical records including any previous prescriptions or scanning, and make appointments.

Figure 3 shows the login page of the web-based Al-Shifa HIS that will allow the users to log in to the system. Figure 4 shows the mobile application version of Al-Shifa HIS once a patient has successfully logged in. It will show the patient's personal information, such as civil ID, age, height, and weight. Figs 5-7, show some data included in the system. Previous health records, medical history, prescriptions, lab investigations, and immunization details will be shown.

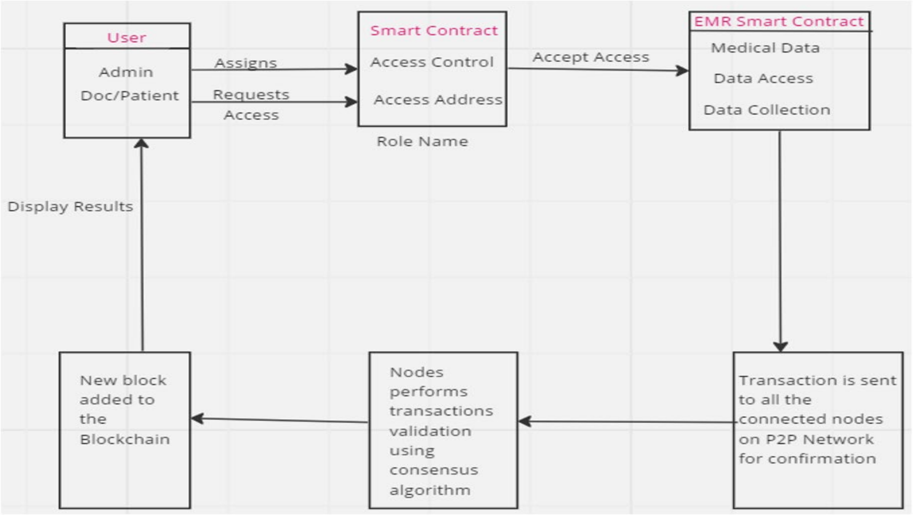
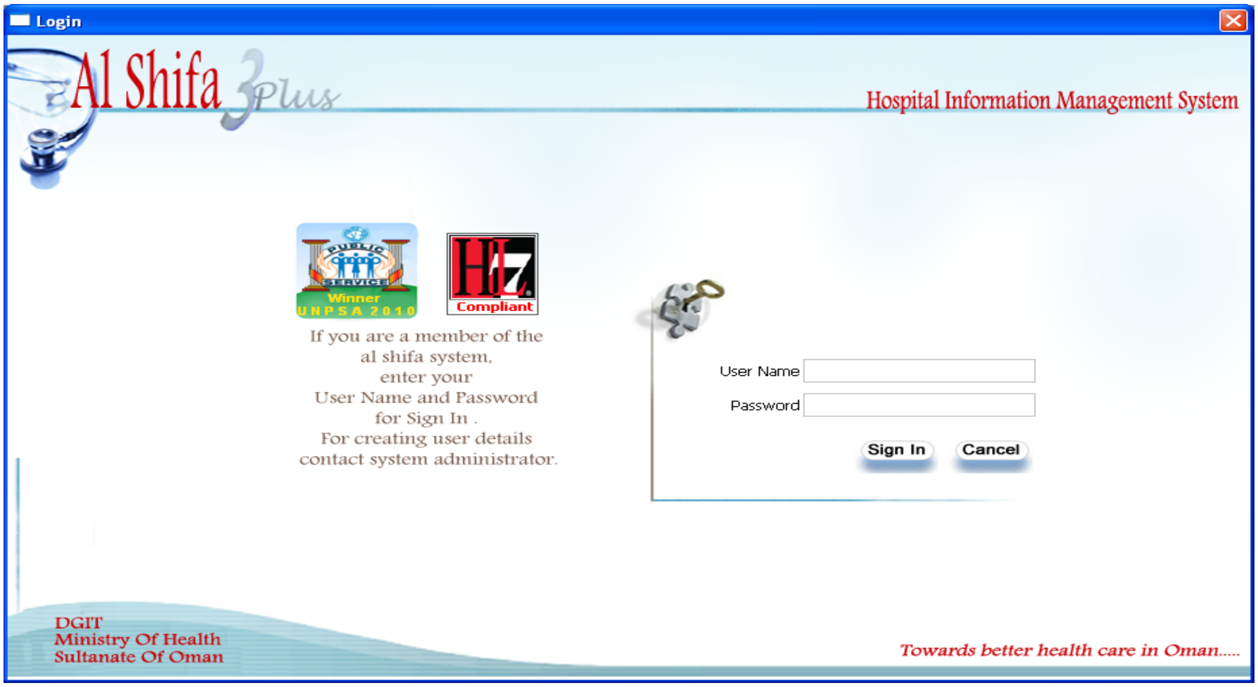


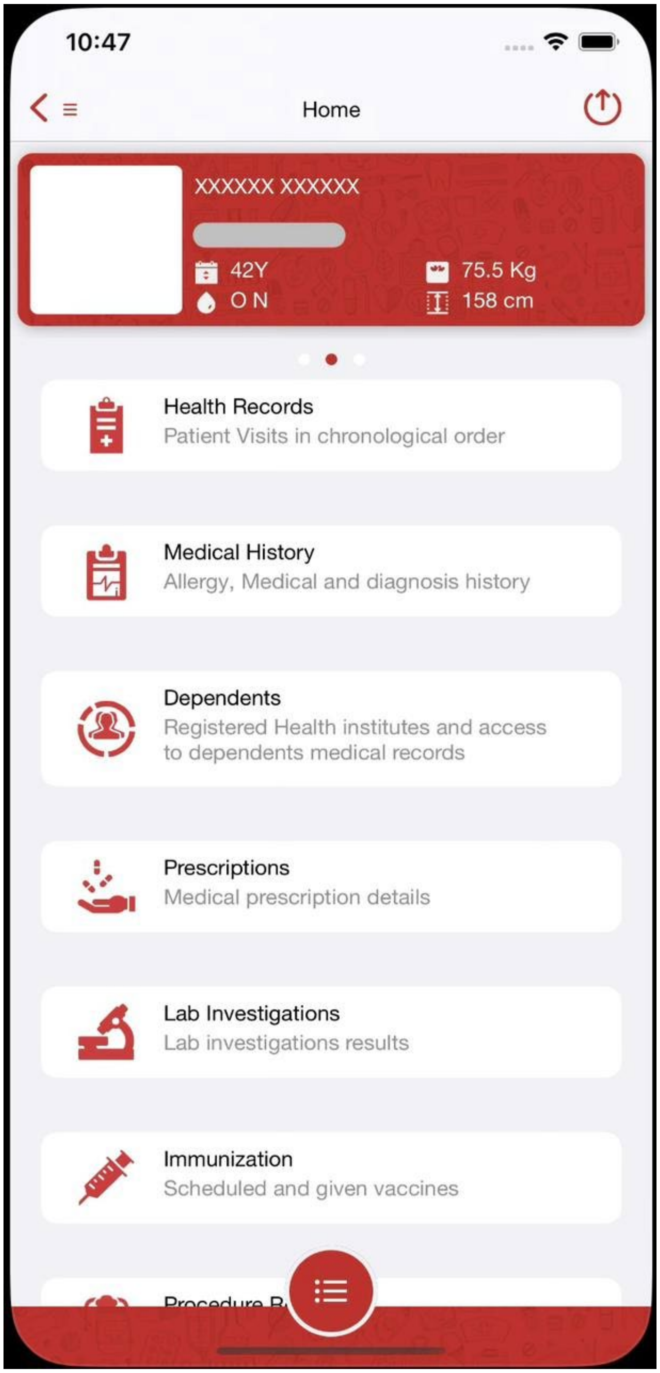
Figure 2.



If you are a member of the
al shifa system,
enter your
User Name and Password
for Sign In .
For creating user details
contact system administrator.

User Name
Password

Figure 3. Al-Shifa3+ login page



10:47

Home

XXXXXX XXXXXX

42Y	75.5 Kg

O N	158 cm

Health Records
Patient Visits in chronological order

Medical History
Allergy, Medical and diagnosis history

Dependents
Registered Health institutes and access to dependents medical records

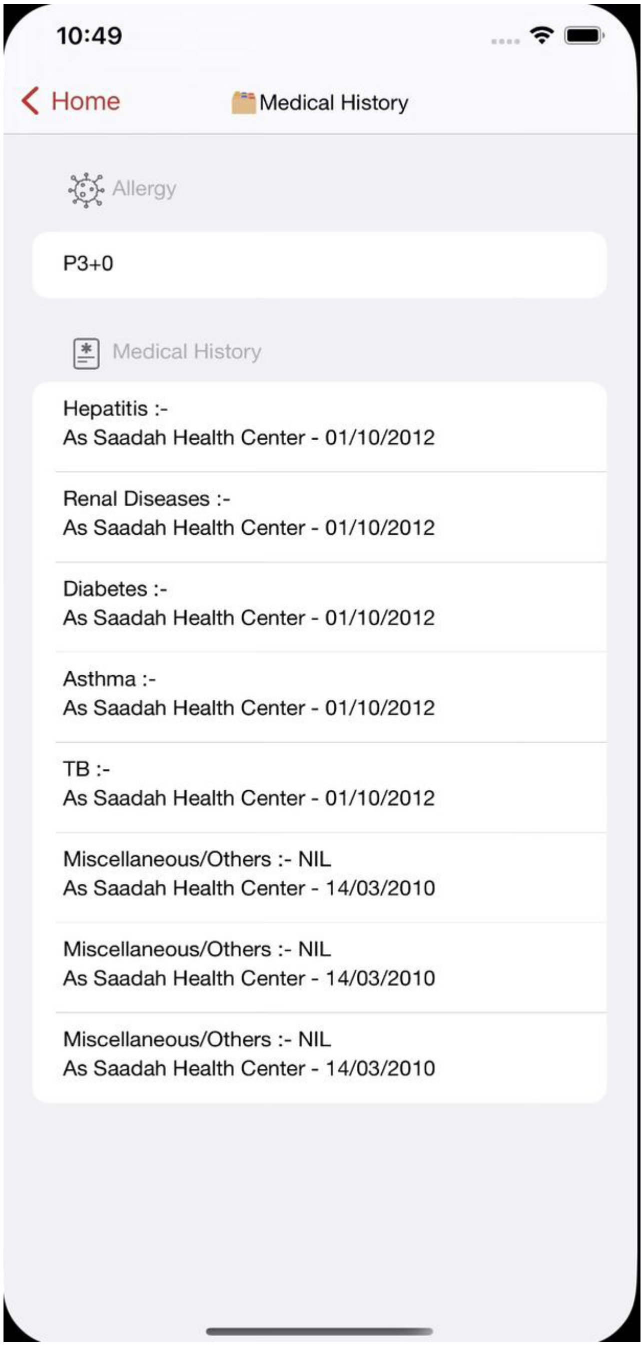
Prescriptions
Medical prescription details

Lab Investigations
Lab investigations results

Immunization
Scheduled and given vaccines

Procedure R

Figure 4. Al-shifa3+ Home page



10:49

Home	Medical History

Allergy

P3+0

Medical History

Hepatitis :-
As Saadah Health Center - 01/10/2012

Renal Diseases :-
As Saadah Health Center - 01/10/2012

Diabetes :-
As Saadah Health Center - 01/10/2012

Asthma :-
As Saadah Health Center - 01/10/2012

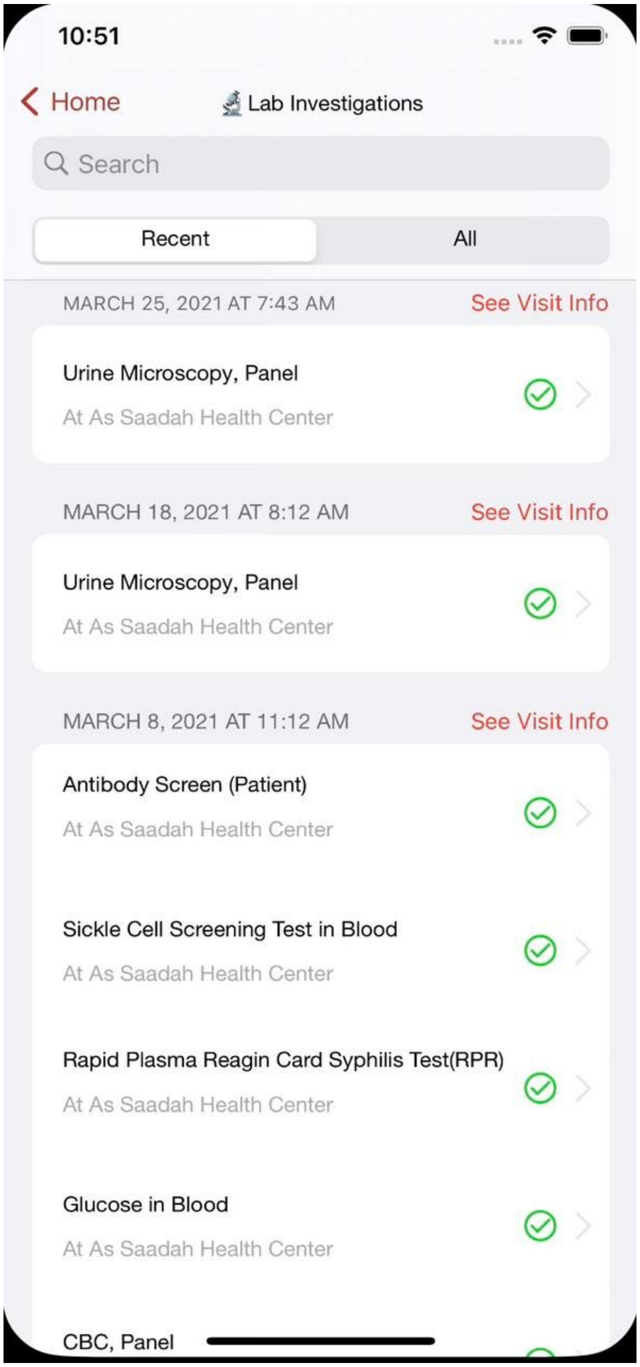
TB :-
As Saadah Health Center - 01/10/2012

Miscellaneous/Others :- NIL
As Saadah Health Center - 14/03/2010

Miscellaneous/Others :- NIL
As Saadah Health Center - 14/03/2010

Miscellaneous/Others :- NIL
As Saadah Health Center - 14/03/2010

Figure 5. Medical Records page



MARCH 25, 2021 AT 7:43 AM See Visit Info

Urine Microscopy, Panel
At As Saadah Health Center ✓

MARCH 18, 2021 AT 8:12 AM See Visit Info

Urine Microscopy, Panel
At As Saadah Health Center ✓

MARCH 8, 2021 AT 11:12 AM See Visit Info

Antibody Screen (Patient)
At As Saadah Health Center ✓

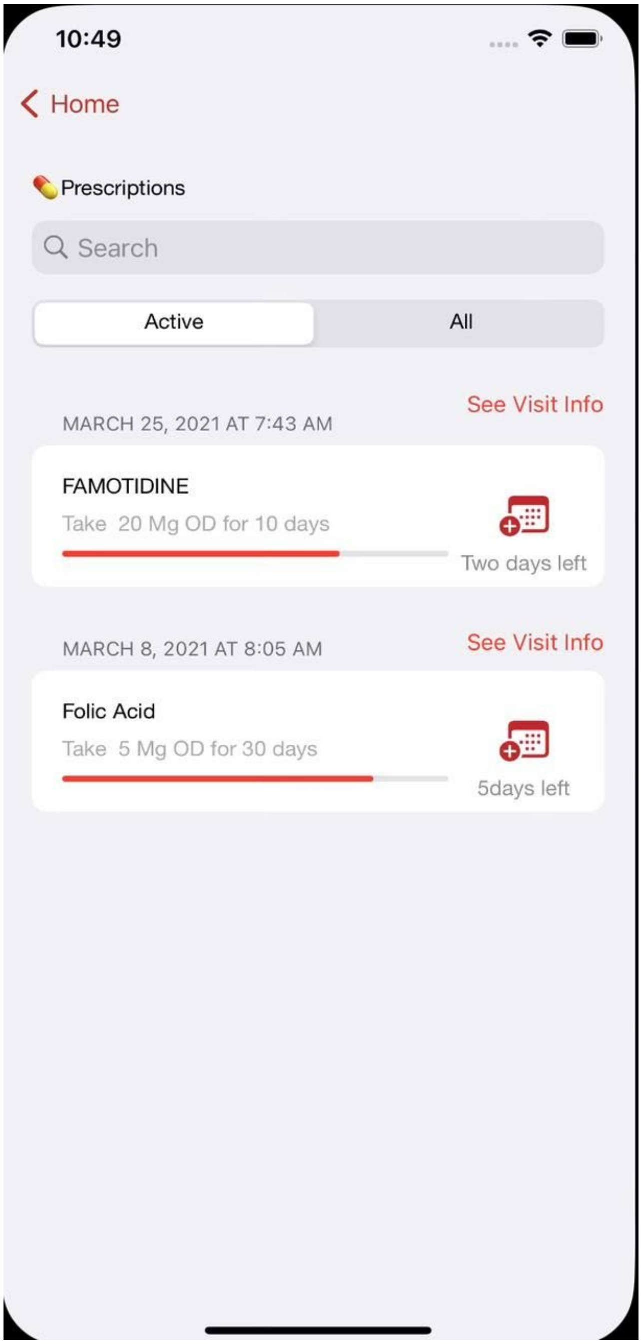
Sickle Cell Screening Test in Blood
At As Saadah Health Center ✓

Rapid Plasma Reagin Card Syphilis Test(RPR)
At As Saadah Health Center ✓

Glucose in Blood
At As Saadah Health Center ✓

CBC, Panel

Figure 6. Lab investigations page



MARCH 25, 2021 AT 7:43 AM See Visit Info

FAMOTIDINE
Take 20 Mg OD for 10 days
Two days left

MARCH 8, 2021 AT 8:05 AM See Visit Info

Folic Acid
Take 5 Mg OD for 30 days
5days left

Figure 7. Prescriptions page

Implementation and Results

The following simulation of a blockchain environment was performed on an 11th Gen, intel core i7, 2.80 GHz processor, with 16 GB RAM, running on Microsoft Windows 10 PRO.

Steps to create the blockchain environment:

Create a virtual workspace in Ganache, where all the transactions, blocks and smart contracts of the network will be shown. Several account addresses will be given along with their private keym with 100ETH in each account. The account address is a 42-character string that functions as a unique identifier for an Ethereum account. It is derived from the account's public key and is used to send and receive Ether and interact with smart contracts on the Ethereum network. It is used to identify the owner of a smart contract and to verify transactions on the blockchain. A private key is a 64-character hexadecimal string that is mathematically linked to the account address. Using private key, the owner will get access to their Ethereum account also, it can be used to sign transactions, to send Ether or interact with smart contracts. A private key should never be shared, while the account address is shared to interact with others.

1- In MetaMask, the blockchain network will be created. To connect that network to the Ganache workspace, the RPC Server URL will be used, with the chain ID 1337.
2- To add a user on the Metamask wallet, a new account will be created using the private keys provided from Ganache Workspace.
3- In the cmd of the repository, the following commands will be entered: Truffle install (to install truffle), Truffle version(to check that truffle latest version is installed), Truffle compile (to compile the contracts), Yarn install (to install Yarn which will manage the dependencies), Yarn start (To run the network)
4- The URL shown after entering the command Yarn start will be opened in browser to open the simulation EHR system.
5- The commands truffle migrate and truffle deploy were entered in the cmd to deploy the contracts. The name of the network, ID, transaction hash, number of block, and total cost of transaction were shown.
6- All the transaction details will be shown in ganache workspace, such as: the block number, the hash of the block and the transaction details.

Conclusion

Blockchain is a trending technology. It is still a new and developing concept which follows the decentralized method of storing data. Many organizations and individuals are doing research on blockchain around the globe for different purposes. In our research paper we have done research on how blockchain can be used in the healthcare industry for storing data. The example taken here is of AL SHIFA 3+ system which is an HIS used in Oman. We have proposed a plan for integrating blockchain with the AL SHIFA 3+ system thereby increasing its security levels. This research can be a crucial step towards incorporation of blockchain with healthcare. The proposed research has covered all the important aspects related to Blockchain. In this research paper the concept of blockchain was clearly discussed and the steps to build a blockchain environment was showcased. Methodology and System Architecture describes the aspects of different approaches used and the basic outline of the system. Literature review of various similar article was done which highlights the importance of blockchain, shows its strengths and background. By implementing our idea, not only AL SHIFA 3+ system but the entire Blockchain community and various other projects which are related to blockchain will benefit. The main strength of our project is how each and every step of using blockchain from scratch is explained, which is not found in most of the journal articles available on the internet too. The use of different applications and software such as Solidity, Ethereum, Ganache and many more is elaborated. The proposed research consists of everything related to Blockchain with main focus on its basics. At the end we can conclude that Blockchain requires more attention and research for gaining success in the upcoming time.

References

Agbo, C., Mahmoud, Q., & Eklund, J. (2019). Blockchain Technology in Healthcare: A Systematic Review. Healthcare, 7(2), 56. https://doi.org/10.3390/healthcare7020056

Al-Gharbi, K. N., Gattoufi, S. M., Al-Badi, A. H., & Al-Hashmi, A. A. (2015). Al-Shifa Healthcare Information System in Oman: A Debatable Implementation Success. The Electronic Journal of Information Systems in Developing Countries, 66(1), 1–17. https://doi.org/10.1002/j.1681-4835.2015.tb00471.x

Khan, S. F., & Ismail, M. Y. (2017). Al-Shifa: Case study on Sultanate of Oman's National Healthcare Information System. Indian Journal of Science and Technology, 10(17), 1–4. https://doi.org/10.17485/ijst/2017/v10i17/113060

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. 2016 2nd International Conference on Open and Big Data (OBD), 25–30. https://doi.org/10.1109/obd.2016.11

Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. (2020). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). https://doi.org/10.1109/iciot48696.2020.9089570

Khalid, M. I., Ehsan, I., Al-Ani, A. K., Iqbal, J., Hussain, S., Ullah, S. S., & Nayab. (2023). A Comprehensive Survey on Blockchain-Based Decentralized Storage Networks. IEEE Access, 11, 10995–11015. https://doi.org/10.1109/ACCESS.2023.3240237

Lemieux, V. L. (2017). Blockchain recordkeeping : A SWOT ANALYSIS. Records Management Journal, 27(2), 110–132.

Junejo, A., Maqbool, M., Memon, M., Junejo, M., Talpur, S., & Memon, R. (2021). Blockchains Technology Analysis: Applications, Current Trends and Future Directions—An Overview. https://doi.org/10.1007/978-981-15-3284-9_47

Spence, N., Bhardwaj, N., Paul, D. L., & Coustasse, A. (2018). Ransomware in Healthcare Facilities: A Harbinger of the Future? Ransomware in Healthcare Facilities: A Harbinger of the Future?

Wang, Y., Zhang, A., Zhang, P., & Wang, H. (2019). Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain. IEEE Access, 7, 136704–136719. https://doi.org/10.1109/access.2019.2943153

Xia, Q., Sifah, E., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. Information, 8(2), 44. https://doi.org/10.3390/info8020044