Journal of Information Systems and Informatics
Vol. 5, No. 2, June 2023 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v5i2.497 Published By DRPM-UBD

Blockchain-Enabled Vaccination Registration and Verification System in Healthcare Management

Bassey Isong[1], Tshipuke Vhahangwele[2], Adnan M Abu-Mahfouz [3]

[1,2]Computer Science Department, North-West University, Mafikeng, South Africa
[3]Center for Scientific and Industrial Research, Pretoria, South Africa
Email: [1]bassey.isong@nwu.ac.za, [2]tshipukevhahangwele@gmail.com, [3]aabuMahfouz@csir.co.za

Abstract

Client-server-based healthcare systems are unable to manipulate a high data volume, prone to a single failure point, limited scalability, and data integrity. Particularly, several measures introduced to help curb the spread of Covid-19 were not effective and patient records were not adequately managed and maintained. Most vaccination-proof certificates were forged by unauthorized parties and no standard verification medium exists. Therefore, this paper proposes a blockchain-enabled vaccination management system (VMS). VMS utilizes smart contracts to store encrypted patients record, generate vaccination certificates, and verify the legitimacy of the certificate using a QR code. VMS prototype is implemented using Ethereum, a public blockchain and simulations performed based on Apache JMeter and Hyperledger Caliper to assess its performance in terms of throughput, latency and response time, and the average time per transaction. Results show VMS achieved an average: response time of 132.24 ms, the throughput of 379.89 tps, latency of 204.60 ms, and time of transactions is 10s-12s for 1000 transactions. Also, its comparison with the centralized database shows the traditional database's effectiveness in transaction processing but lacks data privacy and security strengths. We, therefore, recommend the use of blockchain in the healthcare system and other related sectors such as elections, and student records management to ensure data privacy and security and rid the system of a single point of failure.

Keywords: Covid-19, healthcare system, blockchain, patients, vaccination, security, privacy.

1. INTRODUCTION

In most developing nations, traditional healthcare is heterogeneous in nature and critical patients' healthcare records are diagonally created and maintained in diverse healthcare outlets [1]. This makes it difficult for healthcare providers to efficiently access such records internally and externally when needed for healthcare services such as diagnosis, treatment, decision-making, etc. [1]. Moreover, the traditional healthcare system generates and processes large volumes of patients' data daily and is based on the client-server architecture or the traditional

centralized database. However, a system with such an architectural orientation is unsuccessful in manipulating the high volume of patients' data and limits its scalability, development, and integrity of data as well as serving as a single point of failure [2]. Moreover, the system is prone to denial of service attacks, and reliance on third parties to handle and maintain patients' information, rendering medical data less secure[3], [4].

In recent years, digital transformation has been witnessed all around in every sector of the economy and the healthcare sector is not an exception. The healthcare sector has shown improvements and effectiveness due to advances in technologies such as the Internet of Things (IoT), blockchain, cloud computing, etc. These technologies' applications include sickness prediction, pharmaceutical traceability, electronic medical records management, patient tracking, remote patient monitoring, and the fight against contagious illnesses like the Covid-19 epidemic [3], [5]. In particular, the IoT has significantly contributed to the healthcare evolution from traditional to smart where patients are continuously monitored in real-time, diagnosed, and treated remotely. Thus, these technologies have made the majority of healthcare providers migrate from using conventional health systems to eHealth to change how information is governed and handled [6].

However, the technology adoption in most countries is slow due to reliance on two-tier or client-server architecture systems. The unanticipated outbreak of the pandemic known as Covid-19 greatly exposed the limitations of the present healthcare systems in their ability to respond to emergencies involving public health [7], [8]. Since the first cases were reported in December 2019, the healthcare sector has been under strain due to the demand for services [9]. People worked tirelessly to discover the most effective solutions in terms of creating and testing vaccines, decreasing disease transmission and promptly identifying viral carriers since coronavirus is highly contagious[1], [8], [9]. This also accelerated the development of various technologies to assist with managing the outbreak of the virus including patient tracking or contact tracing applications, symptom identification and remote monitoring applications [10]. Nonetheless, most of these methods were not effective, for instance, the apps lack a source of trustable and accurate data that could help to provide correct information about Covid-19[11]. Most clinical laboratories and general hospitals gave false information about patients affected by the Covid-19 epidemic since there were not managed, maintained or obtained based on defined criteria [3], [12]. Also, several nations advocated the use of immunity passports [13]. Nevertheless, these immunity passports pose serious scientific, practical, equitable, and legal issues[13], [14]. Most of the issued vaccination-proof certificates in several countries were forged and there were no standard ways to verify their legitimacy, and in some cases, patients' privacies were violated[14]. This resulted in several counterfeit certificates and fraudulent claims that the vaccine had been administered[15], [16]. Therefore,

there is a great need to develop cost-effective systems to deliver and deploy vaccination certificates[17], [18].

Blockchain technology is one of the promising technologies to improve the security and privacy of patient records in the healthcare system due to its decentralized distributed ledger [1], [19]. Its application in healthcare has shown promising results in terms of secure access to healthcare data. It has demonstrated the ability to improve clinical trial data management, reducing regulatory clearance delays and simplifying communication between multiple supply chain participants[4], [1]-[20]. Blockchain is a distributed, append-only, and time-stamped data structure that permits the formation of a decentralized peer-to-peer network which eliminates the need for a trusted authority and enables individuals who do not trust one another to interact with one another in a verifiable manner [21], [22]. Currently, several blockchain-based solutions enable the safe transfer of digital assets among untrustworthy clients [23]. It is an exciting new technology that has the potential to assist numerous sectors to reduce inefficiency and surmount bottlenecks such as speeding up transaction settlements, reducing costs, and offering transparency, auditability, efficiency, income, and security [24].

Therefore, this paper proposes and implemented a blockchain-based vaccination registration and verification system as a viable solution in the healthcare sector to ensure that medical data is handled in a trustworthy and secure way. In terms of proof of vaccination, which is required in almost every travel destination, this proposed system will go a long way to curb the issuance of counterfeit certificates and fraudulent activities. Moreover, throughout the epidemic, the transmission of disinformation skyrocketed dramatically, and existing platforms were unable to validate data, resulting in public fear and irrational behaviour. Consequently, developing a blockchain-based verification system is important to guarantee the dependability and credibility of information received by the public and government institutions [25], [26]. Due to the features offered by blockchain technology, the proposed system is used to register and verify vaccinated patients via a quick response (QR) code-based application. This solution idea is not only limited to vaccination but also may be applicable in other areas such as voters' registration, transmission, and storage of election results, etc. Simulations were also conducted to evaluate its performance and the results are promising.

The remaining parts of the paper are structured as follows: Section 2 presents the background information about blockchain technology, Section 3 presents some of the related works, and Sections 4 and 5 present the proposed VMS and the algorithmic design respectively. Section 5 presents the simulations which evaluate VMS's performance, Section 6 presents the paper discussion and Section 7 is the paper's conclusion.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

2. STUDY BACKGROUND

A wide variety of professionals, including those trained in chiropractic, dentistry, nursing, pharmacy, and allied health, are responsible for providing patients with healthcare. It can be administered in a wide number of locations, including hospitals, clinics, nursing homes, and other community-based settings[27], [28]. The integration of healthcare with modern technologies has attracted significant attention in academia and industry in recent years. This has resulted in the emergence of systems such as electronic health records, electronic medical records, mobile computing, telemedicine, telehealth, etc. [29]. This section presents background information on blockchain technology.

2.1. Blockchain Technology

Blockchain is a transparent and secure information storage and distribution platform that runs independently of a centralized authority [30]. It consists of a series of blocks which are append-only logs of time-stamped records that are interconnected and safeguarded using cryptographic techniques [31]. In the blockchain, the order of the blocks is crucial, since there are connected in a predetermined, immutable order specified by the time of the block's creation. Each block contains multiple transactions on the blockchain network that have been verified and records their hash values by the Merke tree [32]. The hash values include the block's hash value and that of the previous block, thereby maintaining a chain structure among blocks [33]. In addition, when a certain amount of time has passed, the blockchain will include a new block that is comprised of completed transactions, it must be validated by an individual known as a miner [33], [32]. A block's hash value is produced when the block is created; its value will change if the block's data is modified and it comprises the hash value of the preceding block as shown in Figure 1. The hash value is produced in such a manner that it is very hard to do reverse engineering on it and the hash is updated every minute if there is a change. Blockchain consensus mechanisms are used to approve and validate the tasks, only when the transaction has been approved that it is accepted as a permanent part of the blockchain [34], [35]. The consensus algorithm is executed by all participating nodes in the networks on the block. Thus, blockchain characteristics included immutable, distributed, anonymity, interoperability, etc.[20].

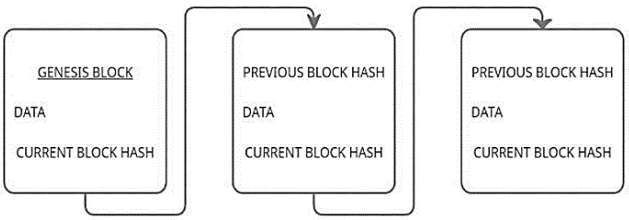

Figure 1. Blockchain structure [33]

Moreover, various classes of blockchain exist depending on the nodes' inherent permission mechanism [20]. This includes private, public (e.g. Bitcoin and Ethereum), and consortium blockchains(e.g. Hyperledger fabric)[20]. Its critical components for ensuring security and privacy in the blockchain system which are the consensus protocols include Proof of Work(PoW) common in a public blockchain, Proof of Authority(PoA), Proof of Stake(PoS), proof of familiarity(PoF), practical byzantine fault tolerance common in consortium blockchain, etc. [34], [35], [19]. These protocols are very important in terms of validating and accepting new blocks into the blockchain[34], [19].

2.2. Smart Contracts

A smart contract is a computer program that specifies the rules for managing transactions in the blockchain system or processes for automated transactions that carry out the contractual obligations of an agreement [36], [19]. As part of the transaction verification process, they are generated on the decentralized ledger and function independently. Its lifecycle includes creating, deploying, executing and completing smart contracts [19]. To generate the smart contract, a transaction on the blockchain platform (e.g., Ethereum, Hyperledger) is required, this will then add the smart contract to the blockchain network. During this particular stage, a contract is issued a unique 160-bit identification address and its code is transferred to the blockchain network [37]. When properly constructed, a smart contract composes of a balance of contracts, a contract address, present executable code, and a contracting state. The security of smart contracts is dependent on how well the contract code is written, and the integrity of the blockchain may be seriously undermined if a fault is found in the implementation logic of the contract code. The execution of each contact statement is an immutable transaction stored in the blockchain [19].

3. RELATED WORKS

This section presents some of the blockchain-based works in healthcare system ecosystems. Harris [38] proposed a blockchain solution involving storing and viewing patient status and transaction log information relevant to Covid-19 medical problems. The confidential information is only accessible to the relevant government and municipal authorities for monitoring and future action. Thippeswamy *et al.* [39] also proposed a blockchain-based approach for tracking medical reports maintained in a secure and distributed blockchain network. A patient is granted a monopoly on his/her medical records, making the system more patient-centred. The system uses two-step authentication to provide security and privacy. Similarly, Tarek *et al.* [40] suggested a secure inter-healthcare patient health records exchange architecture based on blockchain. The proposed architecture can detect and prevent any malicious activity on the eHealth records. It may also

validate the integrity and consistency of EHR queries and responses from other healthcare systems and provide them in a way that is easily comprehensible by all healthcare nodes.

Kumar *et al.* [22] also presented a solution for the off-chain distributed storage of patient diagnostic reports using blockchain and interplanetary file systems (IPFS). It was based on a consortium blockchain-based architecture that can store medical information and the IPFS has a version management technique. In this case, each report is connected with its hash value, and a peer may obtain a patient's medical report by utilizing the report's matching hash value which ensures the data is reliable and accurate. Saha *et al.*[21] also proposed a healthcare data management system based on a consortium blockchain. It is a multi-layered architecture in which various entities associated with the healthcare system would be represented by distinct components. The entities include patients, physicians, hospitals or clinics, medical records, etc. Also, Tripathi *et al.*[41] suggested a smart healthcare system based on blockchain to improve the security and integrity of smart health systems. eHealth records from clinical trials and other sensitive information acquired from a variety of sensors are encrypted and stored among several nodes in a blockchain network rather than in a centralized cloud. This allows for more decentralized access to the information. Blockchain has the potential to improve the healthcare system, however, most works done are mainly based on technical issues involving privacy, security, access control, data management and monitoring which leaves a gap to be filled in developing more decentralized systems with the help of blockchain technology. Thus, this paper focuses on such a decentralized system to boost healthcare security and privacy.

Table 1. Summary of related works

Ref.	Proposed Solution and Objective	Implementation	Consideration
[38]	A low-cost Blockchain method for storing and viewing patient status and transaction log information relevant to their COVID-19 medical problems has been presented.	Blockchain, Hyperledger Fabric, Hyperledger Composer	Trust and Security
[39]	Blockchain-Based Medical Reports Monitoring System	Ethereum Blockchain, Ganache Truffle suite, Metamask wallets, Node Js	Security, Storage, and Authorization
[40]	The blockchain-based solution to facilitate scalable and secure inter-healthcare HER exchange	Blockchain, Smart contract	Security, Integrity, and Consistency

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Ref.	Proposed Solution and Objective	Implementation	Consideration
[22]	off-chain distributed storage of patient diagnostic reports using blockchain and interplanetary file systems (IPFS)	IPFS, Blockchain, Python flask	Consistency, Integrity, and Availability
[21]	Healthcare data management system based on blockchain	Blockchain, FHIR Server	Transparency, Data replication, and availability
[41]	S2HS-smart healthcare system approach based on blockchain	-	Data integrity, Security, Privacy, and Transparency

4. METHODS

4.1. Proposed System

4.1.1 System Overview

This proposed system utilized blockchain technology to develop a secure privacy-aware and efficient vaccine management system (VMS). The system operation is twofold: patients' registration and certificate verification. To register a patient, the system operates by first executing the node, deploying the smart contract and the patient is registered by the *Registration_Authority* under normal operation of the node. However, to successfully register a patient, valid credentials must be entered for authentication. After successful registration, the patient will have a unique smart contract ID that they will use for the generation of their certificate. In the same vein, the *Verification_Authority* verifies the issued certificate. To achieve this, the verifier must have access to the system and then perform certificate verification by scanning the QR code to retrieve vaccination records. The system is straightforward and will assist in addressing the several counterfeit certificates and fraudulent claims of the vaccine having been administered.

4.1.2 System Architecture

This subsection presents the architecture of the proposed VMS. This is presented in Fig. 1 and the components involved are discussed as follows.

1) Patient: Any individual who is going to receive the vaccine from the healthcare facility. Once the patient gets to the healthcare facility, a vaccination dose will be administered to the patient and the vaccination details will be stored on the VMA.
2) Registration_Authority: A person or organization who handles the registration of vaccinated patients in the VMS. He/she must ensure that

the blockchain node is running correctly, must be registered, and verified in the VMS to have access.

3) Verification_Authority: A person or organization who handles all the verification processes. They must also be registered in the VMS to be able to verify the certificate via scanning of the QR code.
4) Blockchain-based smart contract: This is the suggested method for safely storing the information on the distributed ledger. Once patient data has been collected and added to the blockchain, all the other parties involved, including patients and verifiers, will have a more secure means of accessing it. Its features include elements such as data integrity, immutability, transparency, and availability, all of which are among the system's most notable distinguishing characteristics [54].

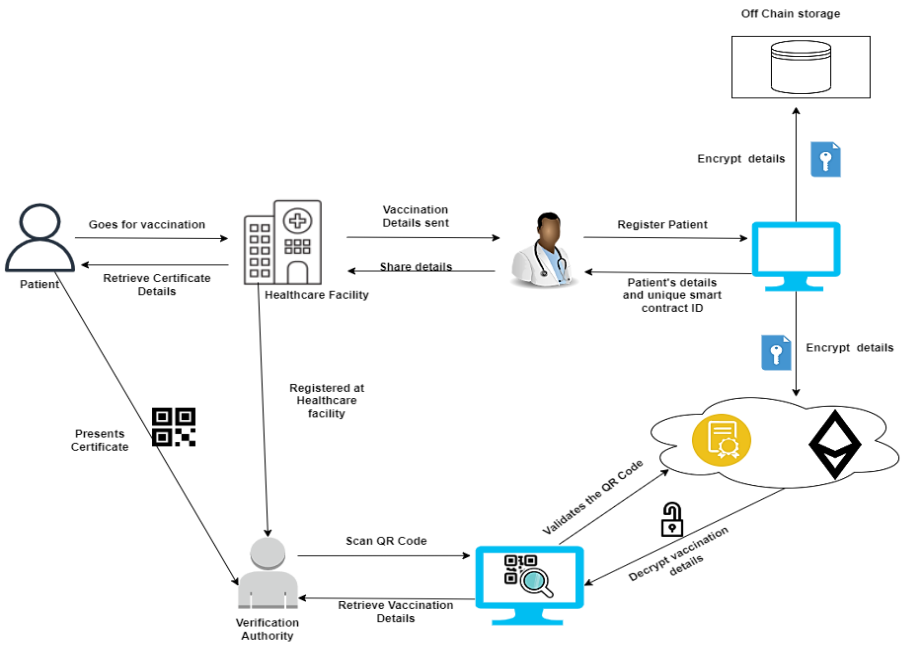

Figure 2. System architecture

4.2 Algorithmic Design

This section presents the algorithmic design which explains how different operations performed in the proposed system happen from the time of patient registration until the verification phase.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

4.2.1 System Operation

As shown in Fig. 3, the proposed VMS starts by executing the node and then is followed by deploying the smart contract. If the node is running without any errors, then the Registering_Authority will be permitted to register the patient, or else if the node is not running an error message will display alerting the administrator to restart the node. A patient is successfully registered when the Registering_Authority enters the valid credentials for authentication. Once registration is successful, a patient can log in with the issued credentials which will be verified to access, request, and view the certificate. However, the requested certificate can be verified by Verification_Authority after logging in with their credentials. Once the credentials are correct, Verification_Authority is allowed to scan the QR code and retrieve vaccination details. In both cases, the blockchain-based smart contract is deployed, the core technology that ensures transparency, integrity, confidentiality, privacy, immutability, and other desirable characteristics of patient's healthcare information.

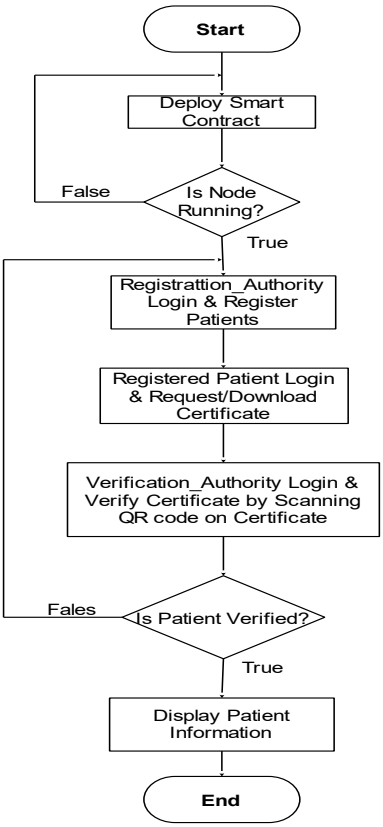

Figure 3. Algorithm for system operations

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

In the proposed VMS, the blockchain node must be operational for the smart contract to be deployed. The correct execution of the smart contract was checked using the hardhat command to build the API and bytecode. Once no error is flagged, the hardhat instruction is executed to invoke the smart contract and generate a unique address. Furthermore, a database is generated by constructing a docker container which is accessible from the API which is launched by Prisma to establish a connection to the database. Also, for effective security, symmetric data encryption is done during registration and decrypted during verification. The process involved in both cases is captured in Fig. 4 and discussed in-depth.

4.2.2 Registration process

This is an activity involving the addition of patients and their vaccination into the VMS by the Registering_Authority. In this process, once a vaccination dose is administered to the patient, personal information such as the national ID and vaccination details of the patient will be collected and stored in the VMS. To achieve this, the Registration_Authority must be registered and verified with the VMS to log in. That is, he/she is required to log in and an access token is automatically created for post request to the API and the token validity will then be checked. It is valid, a 128-bit key will be generated and stored on the database and the plaintext will be encrypted using the generated key while a JSON object will be returned with a ciphertext, as shown in Fugure 4.

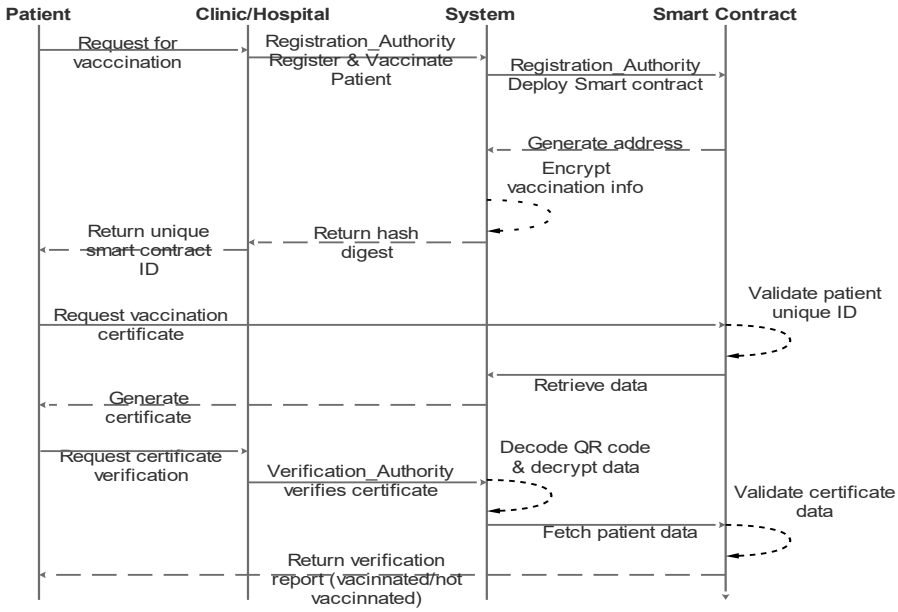

Figure 4. Registration and verification processes

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Once all details are entered into the system, the data will be encrypted and saved into the blockchain smart contract as well as the off-chain storage and a unique QR code is automatically be generated alongside a certificate. The Registration_Authority will then assign the unique smart contract ID generated by the VMS to the patient for the generation of the certificate for verification. The information will be safely stored on the blockchain node for potential use in the future or verification by the relevant authorities. Moreover, a patient can request a certificate of vaccination or registration proof using the unique smart contract ID obtained after registration. It is a valid ID that creates the QR code and encodes it with a vaccinationHash and makes it available for download.

4.1.3 Verification process

Once a patient has successfully registered and been issued a valid certificate, the certificate can be verified for authenticity. To achieve this with the VMS, the Verification_Authority must log in to the system to have its credential's authenticity and user role checked. It is valid, access will be granted, and the 128-bit key will be used to decrypt the data, returning a plaintext from a JSON object. As access is granted, he/she activates the camera and uses it to scan the QR code embedded in the certificate. The data extracted from the QR code will then be translated into a string format and saved into a local variable. Once achieved, the smart contract is then invoked and a request for the vaccine hash is made for the smart contract to provide the saved information. If information is unavailable, an error message will be flagged, otherwise, the smart contract will return all relevant information about the user and the vaccine administered.

5. RESULTS AND DISCUSSION

5.1 Sumulation

This section presents the evaluation of the proposed system prototype to determine its effectiveness and performance.

5.1.1 Setup

In this paper, after the implementation of the proposed VMS prototype, we conducted a series of simulations to evaluate its effectiveness and performance. The performance has been tested based on Apache JMeter and Hyperledger Caliper[42] using metrics: latency, throughput, and response time. The simulations executed between 0 and 1000 threads with a ramp-up speed of one second. The benchmarks were carried out in a PC with Windows 10 Home, a 64-bit operating system, having an intel Core-i5-8265U CPU 1.80GHz, 8GB DDR4 RAM, and 500GB HDD. More three scenarios were involved.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

5.1.2. Tools

As stated above, Apache-JMeter 5.4.5 and Hyperledger Caliper were used to simulate and evaluate the proposed solution. The Apache JMeter is open-source software based on a Java application built to assess functional behaviour and perform load testing. It assesses the performance of apps and online resources that is either static or dynamic on the web. It also simulates high demand on a server, group of servers, network, or item to test the item's resilience or investigate the item's overall performance under a variety of different sorts of loads [43]. In the same vein, the Hyperledger Caliper is a blockchain benchmarking tool used to evaluate how well a blockchain implementation works based on a set of use cases that have already been set up. It was introduced by Hyperledger and is to show how well the blockchain systems, Hyperledger Iroha, Hyperledger Burrow, Hyperledger Fabric, Hyperledger Besu, Hyperledger Sawtooth, Ethereum work and FISCO BCOS. Currently, it can handle performance measures like transaction/read throughput, success rate, transaction/read latency (minimum, maximum, average), and resource consumption (CPU, memory, network) [44].

5.2 Results and Analysis

This section presents the results and analysis of the simulations. The analysis is based on the two simulations scenarios 1, 2 and 3. Scenario 1 employs the Apache JMeter and scenario 2 is Hyperledger Caliper tests while scenario 3 compares VSM to centralized database system performances in terms of the response time, throughput, latency, etc. per the number of threads.

5.2.1 Scenario 1. Apache JMeter tests with and without blockchain

The results for VMS's performance with integrated blockchain based on Apache JMeter are presented in Fig. 5. As shown in Fig. 5, the response time or throughput or latency is directly proportional to the number of threads. Thus, the average response time is 132.24 ms while the average latency calculated was 204.60 ms, and the average throughput calculated is 379.89 tps. However, in terms of latency, once it reaches a certain peak it becomes linear and starts increasing again. The rationale could be that current blockchain architectures do not allow them to scale up to thousands of transactions per second rates. This is in line with literature where scalability is a blockchain challenge [31], [25]. Moreover, in terms of the average time per transaction, the relationship with the number of threads is directly proportional since it increases with the number of threads. Nonetheless, the proposed VMS is capable of processing 1000 transactions in about 10-12 s which signifies VMS is efficient since it can process many transactions in a short time.

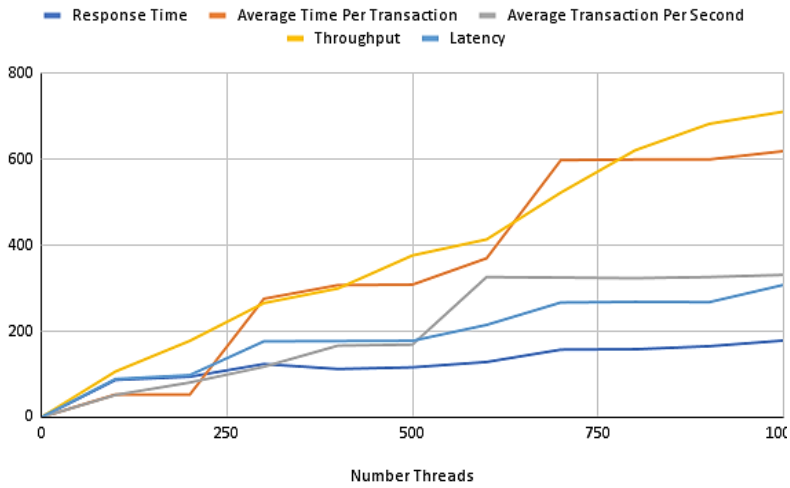

Figure 5. Apache test with blockchain

In the same vein, Fig. 6 presents the Apache JMeter tests where the blockchain was not integrated. That is, VMS was implemented in an off-chain environment but evaluated with the same performance measures. As shown in Fig. 6, the response time or the latency or throughput also increases with the increased number of threads. The average time is 4.77ms, the average latency of 15.18ms and the average throughput is 105.62tps. However, the latency is very low without blockchain. In terms of the average time per transaction, the average time per transaction increased with the number of threads.

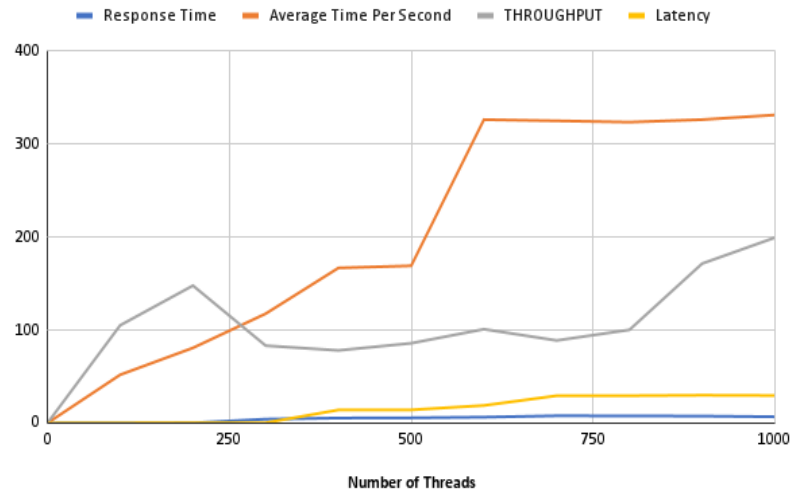

Figure 6. Apache test without blockchain

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

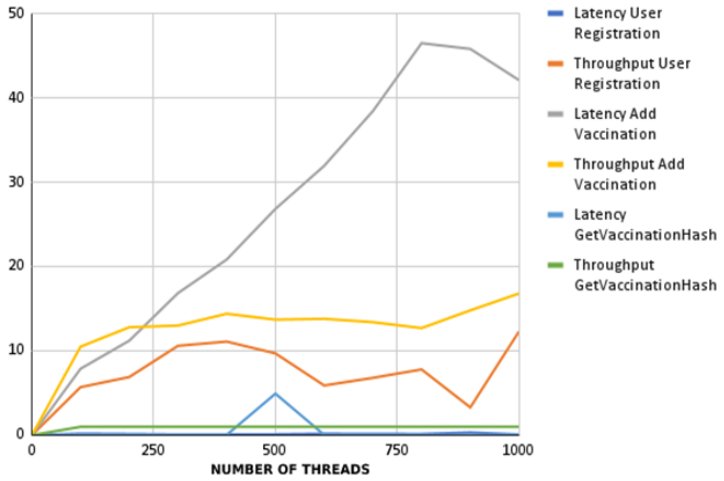

Figure 7. Hyperledger Caliper tests

5.2.2 Scenario 2. Hyperledger Caliper tests.

This subsection presents the results of the system's performance using Hyperledger Caliper which assesses several blockchain systems with distinct use cases and generates performance reports [45]. To achieve this, we evaluated the performance in terms of patient registration using about 1000 different transactions. With the registration activity that executes the smart contract on the blockchain network, Fig. 7 presents the latency and throughput per the number of transactions involved. Accordingly, the latency seems to be directly proportional to the number of transactions, but this proportion remains constant between 250 and 800 transactions. Buts as the number of transactions reached 1000, there was a significant decrease in the latency which could be due to the server restriction. Thus, a latency of 0.114 seconds on average across all runs was achieved. Similarly, for throughput, from 0 to 400 transactions, there was a significant increase in throughput which then decreases gradually to a certain level. Also, as the transactions increase beyond 850, they started decreasing and immediately started increasing towards 1000 transactions.

Thus, the throughput showed haphazard behaviour with the number of transactions, having an average of 8.01 transactions per second. This shows scalability is still an issue in blockchain [46]. According to [31], blockchain was not designed to hold vast volumes of data; as a result, scalability issues must be taken into consideration when combining blockchain technology with the IoT. Moreover, in terms of the vaccinationHash retrieval process, as shown in Fig. 7, the time taken to acquire the vaccine hash does not change. However, for above 450 transactions, the latency begins to increase, and at a certain peak, it begins to

decrease until it reached a constant. Hence a latency of 0.0529 seconds was expended in retrieving the vaccine hash from the blockchain. The throughput showed a direct proportionality with the number of transactions, but as the number of transactions exceeds a particular threshold, it remains constant. In this case, about one transaction was completed every second on average. In terms of how long it took to register a user on the blockchain-based smart contract and the amount of data processed, Fig.6 shows that the latency or throughput is directly proportional to the number of transactions. However, for more than 300 transactions, the throughput remains constant. Thus, the average latency is 28.8 seconds while the average throughput is 13.59 TPS.

5.2.3 Scenario 3. Blockchain-enabled VMS compared to a centralized database system

This section presents the comparison between the blockchain-based system and the traditional database system. The goal was to compare and assess the performance and effectiveness of both systems based using the same measures as shown in Fig. 8. In this scope, the response time is proportional to the number of threads for both systems. However, the traditional system has a better response time as compared to the blockchain-based system. This is due to the execution of smart contracts and other consensus mechanisms in the blockchain system. Also, in terms of average time per transaction, the traditional system can process 1000 transactions in 0.20 seconds while the blockchain-based system can process 1000 transactions in 10-20 seconds. Moreover, though throughput increases as the number of threads increases in both systems, the average throughput of the traditional system seems to be lower than that of the blockchain system.

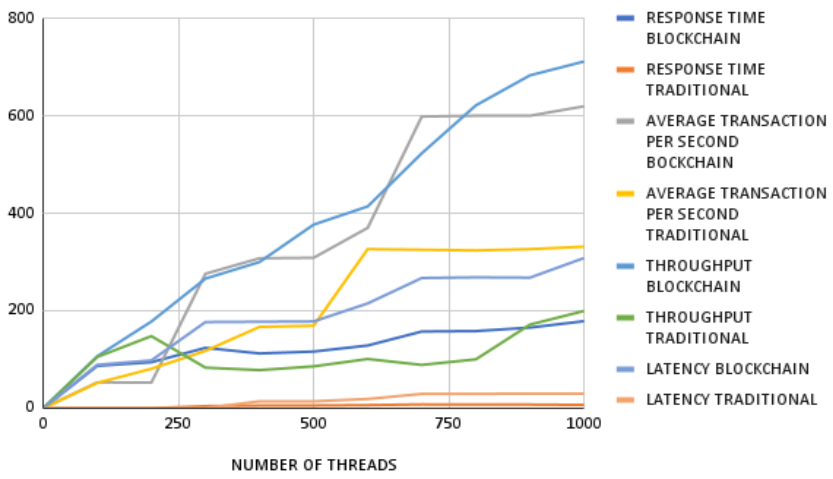

Figure 8. Traditional vs blockchain system

Journal of Information Systems and Informatics
Vol. 5, No. 2, June 2023
p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

5.3 Implementation

This section presents the system prototype of the implemented blockchain-enabled VMS. We designed and implemented a system using a public blockchain because of its availability in research. The blockchain was implemented on a local computer using the hardhat client to host the node. To store the database, an API using REST was implemented. The system's front end was designed using material UI, ReactJS and CSS.

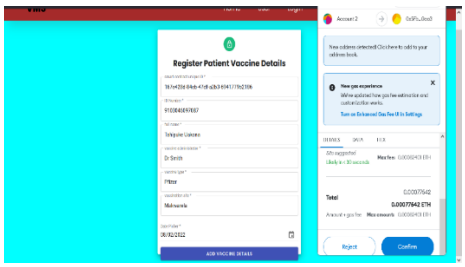

Figure 9. Registration and data confirmation

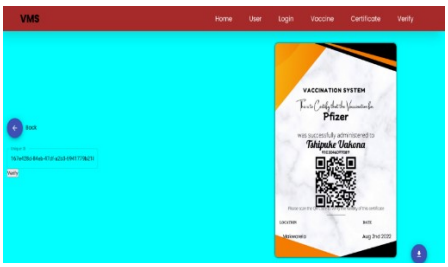

Figure 10. QR code and certificate generation

Moreover, for the front-end and smart contract interaction, we utilized ethers.js and web3.js which assisted in providing effective communication between them. Fig. 9 presents the form for entering a patient's vaccination details by the Registering_Authority. To this end, details such as smart contract ID, patient's ID number, patient's full name, vaccination administrator, vaccine type and number, vaccination site and date, etc. are required for a successful registration. Similarly, Fig. 9 also presents the communication between the VMS and the smart contract. This is achieved by the Registrating_Authority entering all the information about a patient and performing wallet confirmation that confirms the transaction to the smart contract.

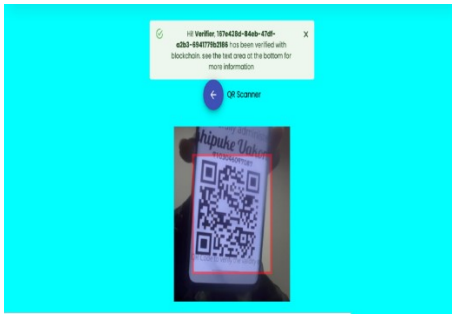

Figure 11. QR code scanning for verification

Figure 12. Successful data retrieval from blockchain

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

In the proposed VMS, upon successful login, patients can view or request their certificates using their unique smart contract ID and can download their certificate embedded with a QR code as shown in Fig. 10. To verify a patient's registration to avoid counterfeit and fraudulent claims, Fig. 11 presents how the QR code is scanned by the Verification_Authority on the certificate provided by the patient verifies its legitimacy. On scanning the QR code, all the details stored on the blockchain-based smart contracts will be retrieved as proof that the patient has been vaccinated as shown in Fig. 12 which consists of transaction hash, vaccination hash and stored collected records.

5.4 Discussion

The centralization of data in the traditional system opens up a lot of possible fraud as data can easily be stolen and modified. Therefore, this paper proposes and presented a decentralized system to minimize or eliminate fraudulent activities surrounding healthcare data. The implemented VMS runs on a local blockchain network, which allows the registration of patients and the storage of vaccination details to the smart contract deployed on the blockchain then encrypts the data using symmetric encryption before the data is stored on the smart contract. The system will eliminate the risk of cyber-attacks and provides security and privacy for patient's medical information in the healthcare system. In addition to the immutability attribute of the blockchain, the security is enhanced using an encryption scheme to encrypt data before storage in the blockchain, making it a cyber-attack-resilient system. Moreover, the proposed VMS was evaluated via a series of simulations to assess its performance and effectiveness. Parameters such as latency, throughput, and response time were used and results were compared to related implementations such as [47] and [48]. The results obtained confirm previous studies such as; latency, response time and throughput increase with the number of transactions. However, it varies with different testing servers, and this might be due to blockchain scalability issues. This shows the results are consistent with other previous studies' findings. Consequently, it shows that blockchain technology has the potential to improve the security, privacy, and effectiveness of healthcare systems. Furthermore, the security analysis of the proposed system was theoretically performed on the data confidentiality, integrity, privacy, availability, access control and transparency. This includes:

1) Confidentiality: The protection of patients' information is one of the core goals of the proposed system. blockchain technology was utilized due to the embedded cryptographic as well as the widely held belief that blockchain networks are exceptionally secure, reliable, and sturdy[49].
2) Privacy: In the context of the VMS, the Ethereum blockchain based on a public blockchain was utilised. Nonetheless, the solution can also be applied to the permissioned blockchain network, thereby, increasing the privacy level. Moreover, blockchain is renowned for its high degree of anonymity because it conceals its public keys [50][51]. In this case, the proposed VMS

encrypts the data before it sends it to the smart contract which provides an additional layer of privacy.

3) Data integrity: This is an essential security component that is core to the system. Due to the cryptographic underpinnings upon which it is constructed, blockchain is inherently protected against tampering and so maintains its integrity. In this case, once the information has been added to a blockchain, it becomes impossible for any party to edit or alter it in any way. As a result of the immutability of user access control rolls and challenges that are issued with the user's private key, the system forbids adjustments to any of these elements[49],[48],[52]. With that being said data integrity is well maintained in our system.
4) Availability: This is also a core security component and our system design guarantees that any data that is pertinent to the verification and authentication processes that are kept on the blockchain is always available to users. In this case, the transaction data is replicated and kept up to the current by each node. The functionality of the network as a whole will not be affected in any way, regardless of whether a node was removed from the network mistakenly, deliberately, or for any other cause [48],[52],[50]. Thus, our system will provide an extremely high degree of availability
5) Access control: On the blockchain, users are authorized to make transactions, but before using the system, each user is required to go through the authentication process. Because in our system just the registration authority is required to register the user, and the vaccination authority is required to validate the certificate, access control is quite crucial [49],[51]. Thus, the system will not allow access to any authorized user organizations to submit transactions.
6) Transparency: This is the characteristic of a blockchain network in which all of its nodes have access to the system's records and in which any alterations to those records are visible to users [53]. Thus, our system is transparent and will not allow unauthorized changes to be made in the blockchain network.

In summary, this analysis shows that our blockchain-based VMS can enhance healthcare systems' security, privacy, transparency, etc. Similar results were obtained in previous studies such as [30], [48], [54], making our system consistent with previous studies.

6 CONCLUSION

This paper proposed and implemented a blockchain-based VMS prototype that registers and verifies the legitimacy of vaccination certificates. Both smart contracts and encryption techniques were utilized to improve the security, privacy and transparency, etc. of the healthcare system. VMS's performance was assessed using simulations based on latency, response time and throughput against transactions performed. Also, a detailed theoretical security analysis was

performed and the simulation results were compared and presented. The results showed that the throughput, latency and response time were directly proportional to the number of transactions performed. Nevertheless, the traditional database system outperformed the blockchain-based system in terms of response time while the security evaluation shows the superiority of the blockchain-based systems. The overall findings show that blockchain can be integrated successfully into healthcare systems to achieve data security, privacy and operational transparency etc., thereby eliminating cyber-attacks and counterfeit documents. The findings corroborated the findings in the existing literature in terms of blockchain scalability issues.

In future, we intend to implement a complete VMS with more features and deploy it in a real-world environment to very whether the vaccine has been approved by pharmaceutical authorities as well verify the identity of the patient. Moreover, the proposed solution can be implemented on a private blockchain and tested on a real-world server such as the Rinkeby testnet to compare the performances to the public blockchain and local servers. Also, different data encryption algorithms can be utilized and tested against several cyber-attacks as well as apply a good privacy model into VMS such as anonymizers to make it more privacy-aware. VMS's idea can also be applied to ensure fair and transparent elections, students' record management, especially exams and results, etc.

REFERENCES

[1] R. Zhang, R. Xue, and L. Liu, "Security and Privacy for Healthcare Blockchains," *IEEE Trans. Serv. Comput.*, pp. 1–18, 2021, doi: 10.1109/TSC.2021.3085913.

[2] S. Devi *et al.*, "Utilizing Blockchain to Enhance the Privacy and Block Validity in Healthcare Systems," *CITISIA 2021 - IEEE Conf. Innov. Technol. Intell. Syst. Ind. Appl. Proc.*, 2021, doi: 10.1109/CITISIA53721.2021.9719915.

[3] W. Yang, E. Aghasian, S. Garg, D. Herbert, L. Disiuta, and B. Kang, "A Survey on Blockchain-Based Internet Service Architecture: Requirements, Challenges, Trends, and Future," *IEEE Access*, vol. 7, pp. 75845–75872, 2019, doi: 10.1109/ACCESS.2019.2917562.

[4] T. K. Mackey *et al.*, "'Fit-for-purpose?' - Challenges and opportunities for applications of blockchain technology in the future of healthcare," *BMC Med.*, vol. 17, no. 1, pp. 1–17, 2019, doi: 10.1186/s12916-019-1296-7.

[5] K. Azbeg, O. Ouchetto, S. J. Andaloussi, and L. Fetjah, "A Taxonomic Review of the Use of IoT and Blockchain in Healthcare Applications," *Irbm*, vol. 1, 2021, doi: 10.1016/j.irbm.2021.05.003.

[6] M. Sookhak, M. R. Jabbarpour, N. S. Safa, and F. R. Yu, "Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues," *J. Netw. Comput. Appl.*, vol. 178, no. July 2020, p. 102950, 2021, doi: 10.1016/j.jnca.2020.102950.

[7] A. I. Sanka *et al.*, "Blockchain-Empowered Multi-Robot Collaboration to Fight COVID-19 and Future Pandemics," *IEEE Access*, vol. 8, no. 1, pp. 10474–10498, 2021, doi: 10.1109/ACCESS.2021.3051051.

[8] A. Kalla, T. Hewa, R. A. Mishra, M. Ylianttila, and M. Liyanage, "The Role of Blockchain to Fight against COVID-19," *IEEE Eng. Manag. Rev.*, vol. 48, no. 3, pp. 85–96, 2020, doi: 10.1109/EMR.2020.3014052.

[9] E. Of, "Sustainable D Evelopment of C Ritical," *Textb. Influ.*, vol. 24, no. 8, pp. 0–63, 2014, doi: http://dx.doi.org/10.1002/9781118636817

[10] W. Y. Ng *et al.*, "Review Blockchain applications in health care for COVID-19 and beyond : a systematic review," *Lancet Digit. Heal.*, vol. 3, no. 12, pp. e819–e829, 2021, doi: 10.1016/S2589-7500(21)00210-7.

[11] T. Singhal, "A Review of Coronavirus Disease-2019 (COVID-19)," *Indian J. Pediatr.*, vol. 87, no. 4, pp. 281–286, 2020, doi: 10.1007/s12098-020-03263-6.

[12] M. Filali Rotbi[1], S. Motahhir[2], and A. El Ghzizal[1], "Blockchain technology for a Safe and Transparent Covid-19 Vaccination."

[13] A. L. Phelan, "COVID-19 immunity passports and vaccination certificates: scientific, equitable, and legal challenges," *Lancet*, vol. 395, no. 10237, pp. 1595–1598, 2020, doi: 10.1016/S0140-6736(20)31034-5.

[14] L. Ricci, D. Di Francesco Maesa, A. Favenza, and E. Ferro, "Blockchains for covid-19 contact tracing and vaccine support: A systematic review," *IEEE Access*, vol. 9, pp. 37936–37950, 2021, doi: 10.1109/ACCESS.2021.3063152.

[15] C. M. Angelopoulos, A. Damianou, and V. Katos, "DHP Framework: Digital Health Passports Using Blockchain -- Use case on international tourism during the COVID-19 pandemic," 2020, doi: 10.1111/j.1365-2966.2005.08922.x.

[16] H. John Leon Singh, D. Couch, and K. Yap, "Mobile Health Apps That Help With COVID-19 Management: Scoping Review," *JMIR Nurs.*, vol. 3, no. 1, p. e20596, 2020, doi: 10.2196/20596.

[17] D. Marbouh *et al.*, "Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System," *Arab. J. Sci. Eng.*, vol. 45, pp. 9895–9911, 2020, doi: 10.1007/s13369-020-04950-4.

[18] K. K. F. Tsoi, J. J. Y. Sung, H. W. Y. Lee, K. K. L. Yiu, H. Fung, and S. Y. S. Wong, "The way forward after COVID-19 vaccination: Vaccine passports with blockchain to protect personal privacy," *BMJ Innov.*, vol. 7, no. 2, pp. 337–341, 2021, doi: 10.1136/bmjinnov-2021-000661.

[19] Q. Liu, Y. Liu, M. Luo, D. He, H. Wang, and K. K. R. Choo, "The Security of Blockchain-Based Medical Systems: Research Challenges and Opportunities," *IEEE Syst. J.*, vol. 16, no. 4, pp. 5741–5752, 2022, doi: 10.1109/JSYST.2022.3155156.

[20] T. McGhin, K. K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw.*

Comput. Appl., vol. 135, no. September 2018, pp. 62–75, 2019, doi: 10.1016/j.jnca.2019.02.027.

[21] S. Saha, A. Majumder, T. Bhowmik, A. Basu, and A. Choudhury, "A Healthcare Data Management System on Blockchain Framework," *2021 Int. Conf. Smart Gener. Comput. Commun. Networking, SMART GENCON 2021*, pp. 1–5, 2021.

[22] R. Kumar, N. Marchang, and R. Tripathi, "Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain," *2020 Int. Conf. Commun. Syst. Networks, COMSNETS 2020*, pp. 1–5, 2020, doi: 10.1109/COMSNETS48256.2020.9027313.

[23] M. S. Ferdous, M. J. M. Chowdhury, and M. A. Hoque, "A survey of consensus algorithms in public blockchain systems for crypto-currencies," *J. Netw. Comput. Appl.*, vol. 182, no. February, p. 103035, 2021, doi: 10.1016/j.jnca.2021.103035.

[24] A. I. Sanka, M. Irfan, I. Huang, and R. C. C. Cheung, "A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research," *Comput. Commun.*, vol. 169, no. December 2020, pp. 179–201, 2021, doi: 10.1016/j.comcom.2020.12.028.

[25] Y. Himeur *et al.*, "Blockchain-based recommender systems: Applications, challenges and future opportunities," *Comput. Sci. Rev.*, vol. 43, p. 100439, 2022, doi: 10.1016/j.cosrev.2021.100439.

[26] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology," *Multimed. Tools Appl.*, vol. 79, no. 15–16, pp. 9711–9733, 2020, doi: 10.1007/s11042-019-07835-3.

[27] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, and G. Dhiman, "Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives," *J. Food Qual.*, vol. 2021, 2021, doi: 10.1155/2021/7608296.

[28] E. M. Adere, "Blockchain in healthcare and IoT: A systematic literature review," *Array*, vol. 14, no. January, p. 100139, 2022, doi: 10.1016/j.array.2022.100139.

[29] M. Massaro, "Digital transformation in the healthcare sector through blockchain technology. Insights from academic research and business developments," *Technovation*, vol. 120, no. May 2021, p. 102386, 2021, doi: 10.1016/j.technovation.2021.102386.

[30] T. Frikha, A. Chaari, F. Chaabane, O. Cheikhrouhou, and A. Zaguia, "Healthcare and Fitness Data Management Using the IoT-Based Blockchain Platform," *J. Healthc. Eng.*, vol. 2021, no. ii, 2021, doi: 10.1155/2021/9978863.

[31] S. Saxena, B. Bhushan, and M. A. Ahad, "Blockchain based solutions to secure IoT: Background, integration trends and a way forward," *J. Netw. Comput. Appl.*, vol. 181, no. December 2020, p. 103050, 2021, doi: 10.1016/j.jnca.2021.103050.

[32] P. Drakatos, "Blockchain Data Management for IoT Applications," in *Proceedings - IEEE International Conference on Mobile Data Management*, 2022, vol. 2022-June, pp. 337–339, doi: 10.1109/MDM55031.2022.00076.

[33] P. Varma Kakarlapudi, Q. H. Mahmoud. "A Systematic Review of Blockchain for Consent Management," 2021, doi: 10.3390/healthcare.

[34] T. Rathee and P. Singh, "A systematic literature mapping on secure identity management using blockchain technology," *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2021, doi: 10.1016/j.jksuci.2021.03.005.

[35] P. Dutta, T. M. Choi, S. Somani, and R. Butala, "Blockchain technology in supply chain operations: Applications, challenges and research opportunities," *Transp. Res. Part E Logist. Transp. Rev.*, vol. 142, no. August, p. 102067, 2020, doi: 10.1016/j.tre.2020.102067.

[36] Z. Zheng *et al.*, "An overview on smart contracts: Challenges, advances and platforms," *Futur. Gener. Comput. Syst.*, vol. 105, pp. 475–491, 2020, doi: 10.1016/j.future.2019.12.019.

[37] B. Hu *et al.*, "A comprehensive survey on smart contract construction and execution: paradigms, tools, and systems," *Patterns*, vol. 2, no. 2, p. 100179, 2021, doi: 10.1016/j.patter.2020.100179.

[38] P. Harris, "Blockchain for COVID-19 Patient Health Record," *Proc. - 5th Int. Conf. Comput. Methodol. Commun. ICCMC 2021*, no. Iccmc, pp. 534–538, 2021, doi: 10.1109/ICCMC51019.2021.9418443.

[39] M. N. Thippeswamy, B. M. Sai Kiran, P. R. Tanksali, M. Hegde, and P. R. Naik, "Blockchain based medical reports monitoring system," *Proc. 4th Int. Conf. IoT Soc. Mobile, Anal. Cloud, ISMAC 2020*, pp. 222–227, 2020, doi: 10.1109/I-SMAC49090.2020.9243573.

[40] O. Ajayi, M. Abouali, and T. Saadawi, "Secured Inter-Healthcare Patient Health Records Exchange Architecture," *Proc. - 2020 IEEE Int. Conf. Blockchain, Blockchain 2020*, pp. 456–461, 2020, doi: 10.1109/Blockchain50366.2020.00066.

[41] G. Tripathi, M. A. Ahad, and S. Paiva, "S2HS- A blockchain based approach for smart healthcare system," *Healthcare*, vol. 8, no. 1, p. 100391, 2020, doi: 10.1016/j.hjdsi.2019.100391.

[42] R. Abbas and Z. Sultan, "Comparative Analysis of Automated Load Testing Tools : Apache JMeter, Microsoft Visual Studio (TFS), Load Runner, Siege," pp. 39–44, 2017.

[43] Halili and H. Emily "Apache JMeter," *Birmingham: Packt Publishing*, 2008.

[44] P. Charles, "A blockchain benchmark framework to measure performance of multiple blockchain solutions", [Online] https://github.com/hyperledger/caliper (accessed Jul. 18, 2022).

[45] W. Choi and J. W. K. Hong, "Performance Evaluation of Ethereum Private and Testnet Networks Using Hyperledger Caliper," *2021 22nd Asia-Pacific Netw. Oper. Manag. Symp. APNOMS 2021*, pp. 325–329, 2021, doi: 10.23919/APNOMS52696.2021.9562684.

[46] T. McGhin, K. K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, no. January, pp. 62–75, 2019, doi: 10.1016/j.jnca.2019.02.027.

[47] S. S. Nabil, M. S. A. Pran, A. A. Al Haque, N. R. Chakraborty, M. J. M. Chowdhury, and M. S. Ferdous, "Blockchain-based Covid Vaccination Registration and Monitoring," 2021.

[48] M. Abubakar, P. McCarron, Z. Jaroucheh, A. Al Dubai, and B. Buchanan, "Blockchain-based Platform for Secure Sharing and Validation of Vaccination Certificates," *Proc. - 2021 14th Int. Conf. Secur. Inf. Networks, SIN 2021*, 2021, doi: 10.1109/SIN54109.2021.9699221.

[49] H. R. Hasan *et al.*, "Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates," *IEEE Access*, vol. 8, no. December, pp. 222093–222108, 2020, doi: 10.1109/ACCESS.2020.3043350.

[50] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11717–11731, 2021, doi: 10.1109/JIOT.2021.3058946.

[51] A. Chowdhary, S. Agrawal, and B. Rudra, "Educational Certificate Verification," pp. 916–921, 2021.

[52] K. S. Malik, D. Rani, C. Science, P. C. L. S. Govt, and C. Karnal, "IoT System with Blockchain for Data Security and Protection : A Review," *Int. Res. J. Eng. Technol.*, pp. 1572–1580, 2021.

[53] W. M. A. Al-Rubaye and S. Kurnaz, "Blockchain and Smart Contracts to Improve Dental Healthcare for Children in Primary School," *2021 Int. Conf. Adv. Comput. Appl. ACA 2021*, pp. 62–67, 2021, doi: 10.1109/ACA52198.2021.9626789.

[54] M. H. Chinaei, H. Habibi Gharakheili, and V. Sivaraman, "Optimal Witnessing of Healthcare IoT Data Using Blockchain Logging Contract," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 10117–10130, 2021, doi: 10.1109/JIOT.2021.3051433.