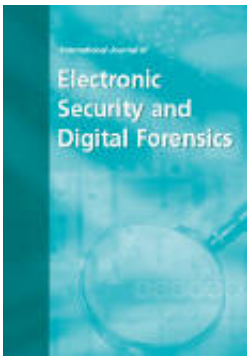
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research




**International Journal of Electronic Security and Digital Forensics**

ISSN online: 1751-9128 - ISSN print: 1751-911X
https://www.inderscience.com/ijesdf

# A novel scalable and cost efficient blockchain solution for managing lifetime vaccination records based on patient preference

Neetu Sharma, Rajesh Rohilla

**DOI:** 10.1504/IJESDF.2025.10063362

**Article History:**

| | |
|---|---|
| Received: | 20 May 2023 |
| Last revised: | 26 August 2023 |
| Accepted: | 21 September 2023 |
| Published online: | 23 December 2024 |

# A novel scalable and cost efficient blockchain solution for managing lifetime vaccination records based on patient preference

Neetu Sharma* and Rajesh Rohilla

Delhi Technological University,
110042, India
Email: neetusharma85@gmail.com
Email: neetu_2k19phdec25@dtu.ac.in
Email: rajesh@dce.ac.in
*Corresponding author

**Abstract:** This study aims to design a novel, cost-efficient blockchain-based solution for managing lifetime vaccination records based on patient preference. The proposed design reduces fraud in vaccination certification by providing QR code-based validation. The proposed system stores the cryptographic-hash of vaccination certificates on the blockchain for security and integrity validation. For scalability, availability, and store-house cost reduction, vaccination records have been stored off-chain through a private interplanetary file system (IPFS) based on patient preference. The smart contract is successfully deployed and tested over the Remix IDE environment. Performance has been evaluated by analysing execution costs at different transaction sizes. Moreover, we have evaluated the probability of data availability for a private IPFS network, which was not done in any previous work. Furthermore, we have analysed the network parameters to get optimal data availability at a low storage cost. The comparative analysis proves that the proposed scheme is better than existing schemes.

**Keywords:** blockchain; vaccination; security; IPFS; scalable; Ethereum; smart contract.

**Reference** to this paper should be made as follows: Sharma, N. and Rohilla, R. (2025) 'A novel scalable and cost efficient blockchain solution for managing lifetime vaccination records based on patient preference', *Int. J. Electronic Security and Digital Forensics*, Vol. 17, Nos. 1/2, pp.108–137.

**Biographical notes:** Neetu Sharma is currently a full time PhD Scholar at the Delhi Technological University, India. She is PG certified in blockchain technology from IIT Bangalore. Earlier, she worked as an Assistant Professor for ten years. She received her MTech and BE in Electronics and Communication Engineering from RGPV, Madhya Pradesh Technical University, India in 2010 and 2007 respectively. Her research interests include blockchain technology, IOT, machine learning, deep learning, image processing and VLSI. She is gold medallist in MTech and has received Srijin award for good teaching. She has co-guided 10+ MTech thesis and has 38 research papers publications.

Rajesh Rohilla is currently a Professor in Delhi Technological University, India. He received his PhD, MTech and BE in Electronics and Communication Engineering. His research interests include computer vision, machine learning, embedded system, robotics and digital design.

## 1 Introduction

Vaccinations play a crucial role in protecting public health against infectious diseases. Vaccination needs to be a mandatory requirement imposed by the government on the public (Fiquaro et al., 2021). As governments seek to ensure widespread vaccination coverage, it is essential to explore mandatory vaccination requirements to protect communities from transferable diseases (Yong et al., 2020). In the context of pandemics, vaccines not only save lives but also contribute to economic resilience (Deka et al., 2020). Vaccines develop antibodies to protect the body against spreadable diseases (Carniel et al., 2021). The immunised public can contribute to a bigger umbrella of group invulnerability by preventing the spread of disease to individuals who are not fully vaccinated.

Digitisation has provided a practical solution for patients to access and manage their vaccination records efficiently. It has also facilitated the concept of immunity passports, serving as essential documentation for medical consultations, migration, education, and employment (Eisenstadt et al., 2020). Digitisation of vaccination records has alleviated the practical challenge of managing hardcopy records from various sources, enabling seamless record-keeping. However, this digital transformation has introduced new challenges related to data privacy and healthcare system integration. Despite these advancements, improper management of vaccination data can lead to delayed or incorrect treatment, ultimately affecting public health. In the last decade, there has been a significant increase in the exchange of digital information (Khan et al., 2023). Resolving the issues with sharing personal information is significant (Mariga and Moturi, 2023). A mechanism is required for maintaining data validity in a trustworthy and secured manner (Nacer et al., 2023). The lack of synchronisation among different healthcare sector members working independently poses a significant challenge in integrating digital copies of individual records into a united repository (Houtan et al., 2020).

Moreover, traditional healthcare systems rely on centralised databases to store vaccination records, which can be susceptible to single point failures and vulnerable to various cyberattacks like distributed denial of service (DDoS) attacks and ransomware incidents (Sharma and Rohilla, 2020). These security weaknesses and lack of data integrity and interoperability in centralised systems may lead to record blocking and breaches, eroding public trust in healthcare providers (Sharma and Rohilla, 2022). To restore and enhance this trust, it is essential to leverage technology and implement innovative strategies for tracking and validating vaccination records by authorised entities.

The COVID-19 has shown the importance of reliable systems (Zhu et al., 2021; Marbouh et al., 2020). It has brought distributed technologies, such as blockchain, for the handling of data on multiple nodes (Udokwu and Norta, 2021). The applications of blockchain in Cryptocurrencies and the token marketplace are flourishing in the business community (Naseer et al., 2021) blockchain is also well suited for healthcare applications such as drug supply chain and drug discovery chain management systems (Sharma and Rajesh, 2023). Moreover, the integration of blockchain with artificial intelligence presents an innovative business environment for healthcare management (Omar et al., 2021). Blockchain eliminates the requirement of a third trusted party (TTP) in environments that are prone to cybercrime (Benarous et al., 2020). Centralised systems have no distributed controlling power (Sai et al., 2021), but blockchain guarantees distributed control so no one can alter data (Sharma and Rohilla, 2020). The optimisation

of storage pressure is required to utilise blockchain benefits in securing sensitive vaccination records and data obtained from smart devices (Li et al., 2021). Moreover, To fully realise the potential of blockchain for vaccination record management, governance policies are critical (Dursun and Üstündağ, 2021). By leveraging blockchain technology and fostering collaborative efforts, healthcare systems can establish a reliable, secure, and interoperable framework for vaccination record management.

### *1.1 Motivation*

The current system of scattered vaccination records in centralised health organisations poses risks of tampering and loss. Although blockchain has the potential to be a smart solution to problems in existing centralised systems, its use in vaccination management is still in its early stages. Public blockchains are preferred over private or consortium blockchains for managing vaccination records because they offer enhanced security, availability, integrity, and validity. Additionally, public blockchains possess a global reach, which ensures that vaccination certificates issued on these platforms are widely recognised, accepted, and validated across international borders. There are few COVID-specific Ethereum-blockchain-based systems (Deka et al., 2020; Carniel et al., 2021; Eisenstadt et al., 2020; Ait Bennacer et al., 2022; Nabil et al., 2022) and very few Hyperledger-blockchain based systems (Fiquaro et al., 2021; Yong et al., 2020) are available. These existing works have limited smart contract functionality, scalability, high execution costs, and storehouse cost issues. Also, the existing blockchain based systems use PoW consensus engines that are very energy-consuming. A proper information security policy is needed to govern the data shared with stakeholders. It can be done by adding access controls as security provisions as part of the contract. This work is focused on PoA consensus-based Ethereum blockchain for patients' lifetime vaccination record management. We intend to create novel smart contract algorithms that will cover the entire vaccination process for a low execution fee. For improved security, privacy, scalability, availability, and decreasing storehouse costs, we only store the hash of the vaccination record on the Ethereum blockchain. The actual data is stored in the private Interplanetary file system (IPFS) based on the patient preference. We implement a QR code-based validation mechanism so that vaccination certificates can be verified by any requesting identity globally. Additionally, the study investigates data availability in the private IPFS network based on patient preference. Network parameters are examined to achieve optimal data availability at a low storage cost.

### *1.2 Contributions*

The key contributions are listed below:

- Proposal of a decentralised model: This study introduces a scalable and cost efficient decentralised model for managing patients' lifetime vaccination records, utilising the Ethereum blockchain to enhance decentralisation and network security. The hash of vaccination certificates is stored on the Ethereum blockchain, ensuring integrity validation.
- Development of a novel smart contract algorithm: A novel smart contract algorithm with access control checks is developed, enabling complaints against health organisations and their removal when necessary. This ensures smooth governance of

the vaccination process over the blockchain network, with a focus on low-cost execution for different transaction sizes.

- Off-chain vaccination record storage: Vaccination records are stored off-chain in private IPFS based on patient preference, ensuring scalability, availability, and reduced storage costs.
- Successful deployment of a smart contract: A smart contract has been successfully deployed over the remix IDE, and its performance has been evaluated through analysis of execution costs with varying transaction sizes.
- Utilisation of the PoA consensus engine: The research employs the PoA consensus engine to reduce resource consumption and accelerate validation.
- Evaluation of data availability probability: The research evaluates the probability of data availability in a private IPFS network based on patient preference, a novel aspect not addressed in previous work. Network parameters are also analysed to optimise storage costs.
- Fraud reduction through QR code validation: The proposed design implements QR code-based validation, for effectively reducing fraud in vaccination certification. This also empowers requesting identities to verify vaccination certificates globally in order to accept and trust them.
- Comparative analysis: A comparative analysis demonstrates that the proposed blockchain-based scheme outperforms existing schemes across various performance metrics.

## 2 Blockchain technology

A blockchain is a decentralised computer network based on cryptography (Patil et al., 2021). Blockchain nodes are computers that keep copies of the transactions and maintain the blockchain network. Blockchain is primarily used for recording or securely sharing transactions across multiple nodes (Wang et al., 2021) and for building trust. Satoshi Nakamoto founded the blockchain technology (Fu et al., 2021), and the bitcoin blockchain is the first application of the blockchain technology that evolved in 2008 for cryptocurrency transactions (Platt and McBurney, 2021).

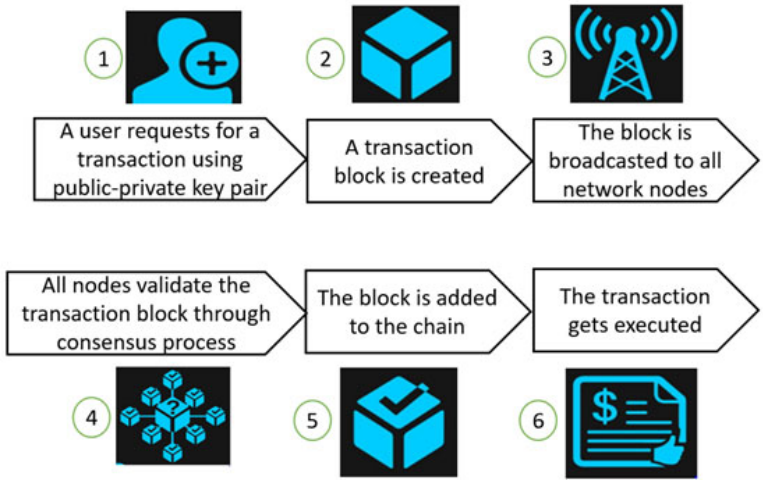
In a blockchain network, transactions are recorded inside the blocks. Every block is added after the consensus process. Blockchain databases are always online and transparent. So all permitted members with internet facilities can access transactions. Moreover, blockchain eliminates mediators, making systems cheaper and more streamlined. The basic features of this technology are security, integrity, immutability, transparency, and transaction availability (Khan et al., 2021). The detailed features are listed below:

- The blockchain enables verification without the need of any third-party (Alam et al., 2021).
- It is immutable. So, the data cannot be altered or deleted (Wu et al., 2021).

- It uses asymmetric cryptography to secure the data blocks (Sharmila and Jaisankar, 2021). Also, the current block is dependent on its previous block to complete the encryption process.
- All the transactions attach to the block after the process of trust verification through broadcasting, consensus, and auditing.
- All the blocks in the blockchain ledger are time stamped.
- The data is shared across each node in the blockchain network. It is decentralised and allows lifetime data availability.
- The transactions that take place are visible to all authorised participants. It is transparent and preserves integrity and trust.
- The records can be traced back to their origin.
- Consensus mechanisms are needed to verify the transaction data, It avoids the hazard of a duplicate record.
- Automatic transactions can be triggered with smart contracts using pre-set conditions.

Figure 1 Illustrates a blockchain transaction. Whenever any user places a digitally signed transaction request, the requested transaction is flooded to all the nodes of the network through gossip protocol (Arnold and Longley, 2021).

**Figure 1** Illustrates a blockchain transaction (see online version for colours)




Blockchain uses a public-private key pair to sign transactions (da Silva, 2021). A transaction encrypted by a private key can only be decrypted by a corresponding public key, and vice versa. The private key is owned by the individual member-only and the public key is shared among all members across the blockchain network.

The blocks are encrypted by hashes and each block hash depends on the previous block hash, current block data, and nonce (Sharma and Rohilla, 2020). The procedure of generating a valid hash for new block creation is known as mining. Mining involves

complex math for finding a good nonce, satisfying difficulty and obtaining an acceptable hash . The difficulty level needs to be fulfilled to add blocks to the chain. Then a new transaction block is created by the consensus process and broadcast to all other validator nodes. When all validator nodes come to a consensus, a new block is added to the existing chain, and the transaction is executed. Any change in the block data of the ledger requires re-mining all of the blocks that come after.

### *2.1 Types of blockchain*

There are three kinds of blockchain: public, private, and consortium (Al-Marridi et al., 2021; Pandey and Litoriya, 2021). The public blockchain is non-restrictive in that anyone can join as an authorised node to perform, verify, and record transactions. E.g., bitcoin is a public blockchain because anyone in the entire world can join as a node. Bitcoin cryptocurrency is the first and most popular digital asset (Saxena et al., 2023). The private blockchain is a restrictive one that only authorised users can join. The advantage of a private blockchain is that it has high transaction speeds. The weakness is that it is less secure and transparent. A consortium blockchain is a permissioned blockchain in which multiple organisations run a blockchain platform.

### *2.2 Consensus in blockchain*

In the blockchain network, mathematical algorithms are used to validate transactions and transaction blocks. These algorithms are called consensus mechanisms. The three most elementary consensus engines are PoW, PoA, and proof of stake (PoS) (Patil et al., 2021). Every consensus mechanism has its uses, benefits, costs, and trade-offs. The consensus mechanism that involves complex mathematical algorithms and enormous computing power to confirm transaction blocks is known as PoW. The benefits of the PoW consensus engine are the high degree of decentralisation and security. Its limitation is that it consumes a lot of energy (Li and Xu, 2021; Goyat et al., 2020). The PoS resolves the issue of energy consumption existing in the PoW (Liu et al., 2021). The benefits of the PoS are low block creation time and energy consumption. But, PoS is less secure and requires a monetary stake to validate the new block (Khalid et al., 2020). PoA is an improved version of the PoS consensus protocol for reaching consensus through authorised validators. In this consensus mechanism, a limited number of nodes have block sealing power, and the validator's identity is at stake, so any faulty behaviour can damage the sealer's reputation. PoA is a viable alternative to PoW and PoS because of its cost-effectiveness, throughput, fault tolerance capability and scalability features (Liu et al., 2019). It is well-suited for applications that require users to trust validators.

## 3 Related work

In this section, we cover the work related to blockchain-based health data management systems, with a specific focus on vaccination record systems. To fully leverage the potential of blockchain technology, addressing scalability is a critical area that requires further research (Sanka and Cheung, 2021). The existing vaccination process-based schemes are summarised in Table 1.

**Table 1** Summary of existing vaccination process-based schemes

| *Existing scheme* | *Objective* | *Limitation* |
|---|---|---|
| Fiquaro et al. (2021) | Created a blockchain-based prototype of vaccination system | Restricts certificate validation right |
| Yong et al. (2020) | Proposed an intelligent system for vaccine supply using blockchain | Restricts certificate validation right |
| Deka et al. (2020) | Presented the methodology for storing vaccination records using blockchain | Not cost efficient |
| Carniel et al. (2021) | Described usability of blockchain in supporting vaccination process | Scalability is not addressed, not cost efficient, lacks cost analysis |
| Eisenstadt et al. (2020) | Proposed an app for COVID-19 vaccination certification | Scalability is not addressed, lacks cost analysis |
| Ait Bennacer et al. (2022) | Presented digital health passport using blockchain | Privacy issues due to use of public IPFS network |
| Nabil et al. (2022) | Proposed digital vaccine passport system using blockchain | Scalability is not addressed |
| Proposed | Proposed cost-efficient and scalable blockchain-based vaccination record management system using private-IPFS network | Addressed scalability, cost efficiency and evaluated data availability |

A prototype of a blockchain-based system aimed at securing the vaccination process has been developed in Fiquaro et al. (2021), and a blockchain-based approach for vaccine supply monitoring is proposed in Yong et al. (2020). However, the performance of these works has not been analysed. Moreover, both of these systems utilise a private blockchain, which restricts the right to validate vaccination certificates to authorised individuals only. Another design, presented in Deka et al. (2020), attempts to manage vaccination records, but it is not a cost-efficient approach. Similarly, the use of blockchain technology to improve the vaccination process is explored in Carniel et al. (2021), and in Eisenstadt et al. (2020), a decentralised application is developed to support the record-keeping of COVID-19 test reports and vaccination certificates. However, these designs lack in terms of scalability, lack of cost analysis, and limited functionality; thus, they are not entirely cost-efficient. Digital passport systems using blockchain are proposed in Ait Bennacer et al. (2022) and Nabil et al. (2022). The first system raises concerns about privacy issues due to its reliance on the public IPFS network, and the second system faces challenges related to scalability.

In the review of applications of blockchain in healthcare information management in Berdik et al. (2021), the system is found to focus on theoretical contributions, lacking practical implementation. Additionally, a cloud-supported electronic health (eHealth) system proposed in Zhang et al. (2021) fails to address scalability concerns. In Motohashi et al. (2019), a blockchain-based system for health data management is designed and validated, but it lacks performance analysis. Moreover, in Kumar and Chand (2021), a healthcare data securing and exchanging system is suggested, but the use of a private blockchain restricts validation rights. The proposal in Miyachi and Mackey (2021) introduces a cost-efficient healthcare data security system using on-chain and off-chain storage, but it lacks performance analysis. Similarly, the architecture for

deploying blockchain technology in the healthcare domain presented in Shahnaz et al. (2019) lacks both cost analysis and validation mechanisms.

In contrast, the proposed work in this study adopts a PoA Consensus-based blockchain for managing patients' lifetime vaccination records. It boasts more smart contract functionalities, providing coverage of the entire vaccination process at a lower execution fee. Moreover, to enhance scalability, availability, and reduce storage costs, the actual data is stored off-chain based on patient preference, and only the hash of the vaccination record is stored on the Ethereum blockchain. We have also presented the performance evaluation. Additionally, the study investigates data availability on the private IPFS network based on patient preference. Network parameters are examined to achieve optimal data availability at a low storage cost.

Thus, this section emphasises that blockchain design plays a crucial role in ensuring the security, immutability, transparency, trust, and accessibility of recorded data. The studies suggest that blockchain can prove to be the most effective tool for vaccination record management. By addressing existing limitations and incorporating advanced functionalities, blockchain technology can significantly improve various aspects of healthcare data management and ultimately enhance the vaccination process and public health outcomes.

## 4 Preliminaries

### *4.1 Ethereum blockchain*

Ethereum is an open-source platform for building blockchain-based distributed applications. Ethereum was founded by Vitalik Buterin in 2013 and is popular for executing smart contracts. Smart contracts have increased blockchain applications tremendously (Liu et al., 2021). Smart contracts are computer programs stored on a distributed ledger that execute transactions automatically when certain conditions are met. The Ethereum virtual machine (EVM) facilitates machines running smart contracts that are compiled into the EVM bytecode. Smart contracts are put on the Ethereum network using contract creation transactions. The Ethereum transaction includes the following components:

- From: 20-byte address of transaction sender.
- To: 20-byte address of transaction recipient.
- Value: Amount (wei) that is sent from sender to recipient.
- Data: It contains transaction inputs.
- Gas: Gas is a unit to measure the fee required for executing a transaction.
- Gas price: Amount of ether per unit of gas that sender is willing to pay for running transaction.
- Gas limit: Maximum gas set by the sender for the transaction.

### 4.2 Blockchain scalability

Currently, the blockchain has a scalability issue that limits its usability in various applications (Sharma and Rohilla, 2023). Scalability means the limited capability of a highly distributed network to handle a huge number of transactions and update ledgers in a short amount of time. The transaction per second can be calculated using the following mathematical formula:

$$\text{Transactions persecond} = \text{transactions per block} / \text{block generation time} \quad (1)$$

The above equation shows that to increase transaction speed, transactions per block should be high and block generation time should be low. But block generation time is generally fixed by the blockchain platforms to maintain the network. The transaction per block can be calculated using a mathematical formula:

$$\text{Transactions perblock} = \text{block size} / \text{average transaction size} \quad (2)$$

The above equation shows that transactions per block can be increased either by increasing block size or by decreasing the average transaction size. An increase in block size can destroy the harmony in the blockchain network by splitting the community. The PoW which is a traditional cryptocurrency-based is an energy-inefficient consensus engine (Haouari et al., 2022; Song et al., 2021). So the throughput can be improved by switching from PoW to PoA. PoA increases transaction speed, reduces the wastage of energy by all validators, and also prevents the 51% attack. On-chain scaling increases the block size, and optimising consensus mechanisms degrades the decentralisation and security. Hence, the storage efficiency of smart contracts needs to be improved to increase the overall throughput (Spataru et al., 2021). This can be done by creating a lightweight blockchain (Ekanayake and Halgamuge, 2021) using off-chain storage.

### 4.3 Interplanetary file system

The IPFS is a peer-to-peer file-sharing system for off-chain storage of large amounts of data (Patil et al., 2021). Off-chain scaling can be done through IPFS without the involvement of a blockchain network. It is a protocol for peer-to-peer secure data storage, as all the data files kept on IPFS are encrypted by a cryptographically generated hash value. It reduces the computational overhead of mining large data files. IPFS allows users to store and share data files in the network by their content address instead of their location address. Everyone can access the data on the public IPFS network. Patients need complete control over their information, so making it publicly accessible is not an option. Private IPFS permits only connecting to other peers who have a shared secret key. With private IPFS networks, privacy can be achieved.

## 5 Method

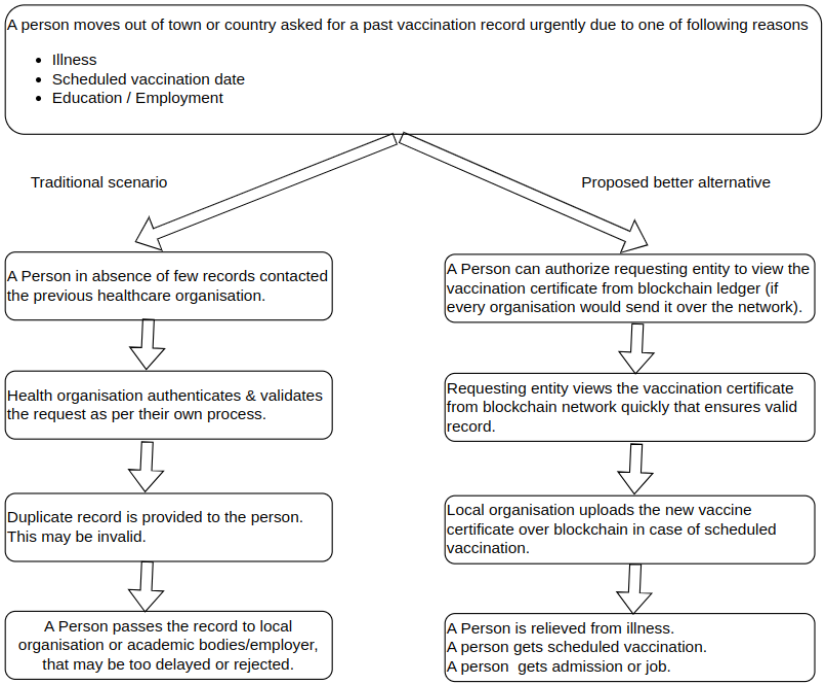
### 5.1 Overview of proposed work

In today's world, people move a lot from one place to another frequently, and it is almost inevitable that one or more vaccinations are missed, either due to a lost physical copy or a poorly managed online record. In cases of unavailability at times of need like scheduled

vaccinations, illness, migration, education, or employment purposes, the patient attempts to contact the concerned health organisation for those records to present them to the requesting entity. But current health organisations maintain data in a centralised manner that can be altered or lost by cyber-attacks. The process of transferring the vaccination data from the hospital often requires multiple hospital-to-patient communications, leading to delays, that can be unbearable in the case of an illness.

Moreover, patients visit many hospitals to take various kinds of vaccines in their lifetime. Some of which are Hepatitis A, Hepatitis B, Rotavirus, Haemophilus, Influenzae type b, Poliovirus, Diphtheria, Tetanus, Pertussis, Pneumococcal, Meningococcal, Influenza, Measles, Mumps, Rubella, Varicella, Human Papillomavirus, Covaxin, Covishield, etc. The scattering of vaccination records makes it difficult to manage and retrieve them. Bringing together different hospitals on a centralised system cannot be a solution, as the database will remain in the custody of one administrator and can be tampered with or lost. So in this situation, it is a necessity that the health ministry initiate a decentralised system to maintain immutable and trustworthy vaccination records that can be easily accessible by any requesting entity throughout their life.

**Figure 2** Illustrates the traditional and proposed use case scenarios (see online version for colours)



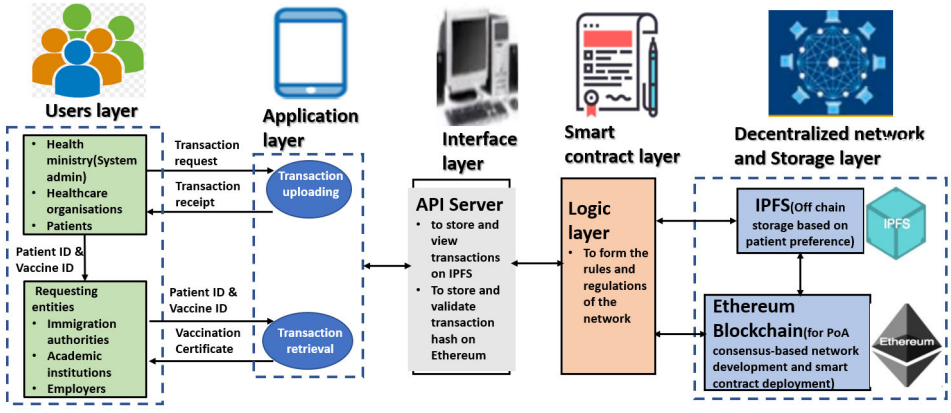

In this scenario, a person moves out of town or country and has been asked for a past vaccination record urgently due to one of the following reasons: person is sick, the person has a scheduled vaccination date, or the person has applied for education or employment. In the traditional scenario, the person, in the absence of a few records, contacts the old health organisation that provided vaccination earlier. The organisation takes time to provide a duplicate copy of the vaccination certificate to the person. The integrity of this

certificate has no guarantee. The person might not be able to submit vaccination certificates on time. In the proposed scenario, the person gives authorisation to view the vaccination record over the blockchain network to the requesting entities. That could be possible if the health ministry makes the uploading of vaccination records over the blockchain network mandatory for all health organisations. The requesting entity quickly views the authentic vaccination records on the blockchain network.

## *5.2 System architecture*

A blockchain-based vaccination system allows users to update and retrieve vaccination records from anywhere and at any time. The aim is to guarantee accurate record accessibility for scheduled vaccinations or illnesses in order to protect the patient from diseases. The proposed blockchain-based model for vaccination record management works without a central authority. At the same time, it ensures record accessibility for all requesting entities. The architecture of the proposed system shown in Figure 3 has the following layers:

**Figure 3** Architecture of proposed system (see online version for colours)



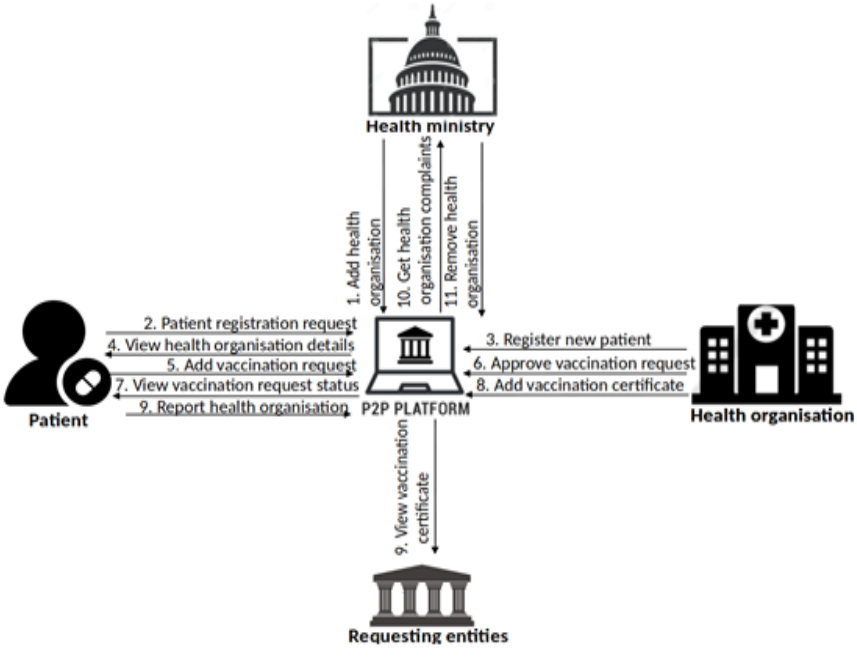

- Users layer consists of the Health Ministry, health organisations, patients, and requesting entities that invoke transactions on the blockchain network. The health ministry acts as an admin to govern the entire network. A patient can authorise requesting entities to view the vaccination certificate using the patient ID and vaccination ID.
- Application layer forms the front end of the application. In the proposed model, this user interface is to create an environment for interacting with the blockchain-IPFS network. It allows users to upload and retrieve transactions. After transaction completion, a transaction receipt containing transaction details is received by the sender through this interface.
- Interface layer is the set of API's that has been used to communicate with the blockchain and get the required result such as retrieval of data, the addition of data, etc.

- The smart contract layer forms the logic of the network and ensures that the blockchain network follows all the rules and regulations to govern the proposed application.
- Decentralised network and storage layer comprise the Ethereum blockchain and private IPFS. The Ethereum platform has been used to form the base of the blockchain network and ledger for holding transaction data. The PoA consensus mechanism has been utilised for mining purposes. The hash of the transactions has been stored on the blockchain, and the complete transactions are on off-chain storage. Each transaction sender runs both a blockchain node and an IPFS node by using an API (application program interface) server as middleware. When publishing off-chain data, this middleware stores the original data in IPFS, then creates a blockchain transaction containing that data's hash. The middleware extracts the hash from the blockchain, then uses this hash to fetch the complete content from IPFS. The local IPFS node automatically verifies the retrieved content against the hash to ensure it hasn't been changed. IPFS has been used with the blockchain for scalability and patient preference feature to reduce storehouse costs.

## *5.3 Workflow*

The workflow diagram for all parties involved in the proposed system is shown in Figure 4.

**Figure 4** Workflow diagram of proposed system

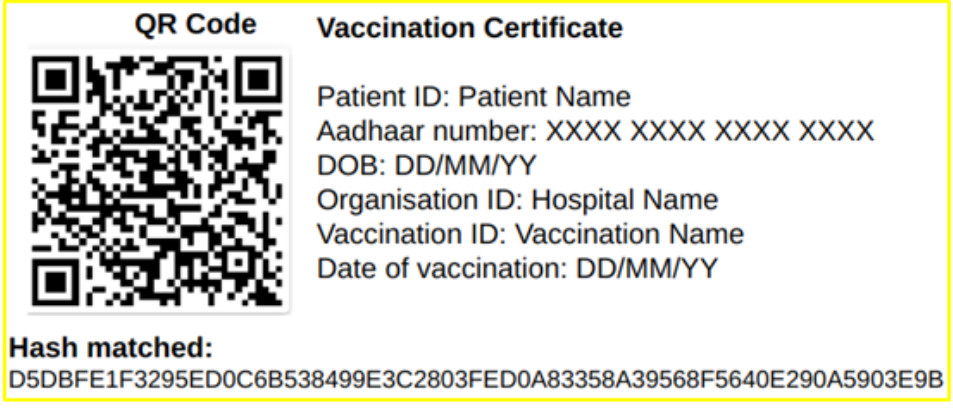



Initially, the health ministry adds the health organisations that have vaccination facilities. The patient invokes registration requests on the network. Health organisations register

new patients in response to registration requests. Now patients can view all health organisation details to check the address, available vaccines, and date-time slots. After viewing the organisation details, the patient places a vaccination request with any suitable health organisation to get an appointment for vaccination. The health organisation then accepts the vaccination request by including an approved status. After that, the patient views the transaction request status and visits the health organisation physically. After the vaccination process, the health organisation uploads the vaccination certificate, which any authorised requesting entity can access. Patients can report a complaint against health organisations in cases of issues faced during the vaccination process. The health ministry can retrieve complaints reported against any organisation. The health ministry can remove health organisations against which reported complaints exceed the predefined value.

After vaccination, the patient's vaccination certificate is generated with a QR code. The hash of the vaccination certificate is added to the blockchain and the actual data is stored on the private IPFs network. The user gets the vaccination certificate with a QR code that can also be used as a vaccination proof. This helps with requesting authorities to permit cross-border travel, the next vaccination, and recruiting individuals. The requesting entities can view the vaccination certificate and scan the QR code to verify it on the blockchain. Figure 5 represents the QR code and information of vaccination certificate The vaccination certificate contains the following information: patient ID, Aadhaar number, date of birth, organisation ID, vaccination ID, and date of vaccination. In response to the QR code scanning, requesting entities will get the hash of the vaccination certificate if it matches the stored hash on the blockchain. The proposed design reduces fraud in vaccination certification by providing QR code-based validation on the blockchain.

**Figure 5** QR code and information of vaccination certificate (see online version for colours)




The functionalities of the involved parties with access controls are defined inside the smart contracts. Algorithm 1 shows the smart contract functionality of the health ministry. The health ministry can invoke the following functions:

- addHealthOrganisation(): This function has been defined to add health organisations. It contains the organisation ID, address, registration number, and list of available vaccines with the date and time slots.

- getHealthOrganisationComplaints(): This function has been defined to get complaints reported against health organisations. It contains the organisation ID.
- removeHealthOrganisation(): This function has been defined to remove health organisations in the event that complaints are reported by more than one-third of the vaccinated patients. It contains the field of organisation ID.

**Algorithm 1** Smart contract functionality of the health ministry

```
1   function addHealthOrganisation(Organisation ID, Address, Registration number,
    Available Vaccines slots)
2       if msg.sender == Health ministry then
3         if organisation ID does not exist then
4             Add health organisation to the Health organisation asset
5         else
6             Invalid transaction
7         end if
8       end if
9   end function
10  function getHealthOrganisationComplaints(Organisation ID)
11      if Organisation ID exist then
12          return Complaints reported against health organisation
13      else
14          Invalid Organisation ID
15      end if
16  end function
17  function removeHealthOrganisation(Organisation ID)
18      if Organisation ID exist then
19          if Complaint reported > 1/3(Vaccination count of organisation) then
20            remove health organisation
21          else
22            Invalid Organisation ID
23        end if
24      end if
25  end function
```

Algorithm 2 shows the smart contract functionality of a health organisation. The health organisations can invoke the following functions:

- RegisterNewPatient(): This function has been defined to register new pa tients. Any health organisation can register a new patient. It contains patient ID, Aadhaar number, age, and data availability choices.
- approveVaccinationRequest(): This function has been defined to accept vaccination requests and include the ‘approved status’. It contains patient ID, date and time, requested vaccination, and status.

- addVaccinationCertificate(): This function has been defined to upload vaccination certificates and increment the vaccination count. It contains organisation ID, vaccination ID, patient ID, vaccination certificate.

**Algorithm 2** Smart contract functionality of health organisation

```
1   function registerNewPatient(Patient Name, Aadhaar Number, Age, Data Availability
    choice)
2       if Patient ID does not exist then
3           Add patient to the registered patient asset
4       else
5           Invalid transaction
6       end if
7   end function
8   function ApproveVaccinationRequest(patient name, Date Time, Re quested vaccination,
    status)
9       if Patient ID exist then
10          Approve vaccination request by adding 'approved' status
11        else
12          Invalid transaction
13        end if
14  end function
15  function AddVaccinationCertificate(Organisation ID, Vaccination ID, patient ID,
    Vaccination certificate)
16        if patient ID and vaccination ID exist then
17          add vaccination certificate and increment vaccination count of organisation
18        else
19          Invalid transaction
20        end if
21  end function
```

Algorithm 3 shows the smart contract functionality for patients. The patients only have access control to invoke the following functions (in the case of a child patient, this function can be invoked by a parent):

- patientRegistrationRequest(): This function has been defined for placing registration requests. It contains the fields of patient ID, Aadhaar number, age, and data availability choice.
- viewHealthOrganisationDetails(): This function has been defined to view health organisation details. It contains the field of organisation ID. – addVaccinationRequest(): This function has been defined to place vacci nation requests. It contains the fields of patient ID, date and time, requested vaccination, and organisation ID.
- ViewHealthorganisationStatus(): This function has been defined to view the status of vaccination requests. It contains the field of organisation ID. –

reportHealthOrganisation(): This function has been defined to report complaints against health organisations by incrementing the reported complaints. It contains the field of organisation ID.

**Algorithm 3** Smart contract functionality of patients

```
function patientRegistrationRequest(Patient ID, Aadhaar Number, Age, Data Availability choice)
        if Patient ID does not exist then
          Add patient to the registration request asset
        else
          Invalid transaction
        end if
end function
function Viewhealthorganisation(Organisation ID)
        if Organisation ID exist then
          return Health organisation details
        else
          Invalid Organisation ID
        end if
end function
function addVaccinationRequest(patient ID, Date Time, Requested vaccination, Organisation ID)
      if patient ID exist then
          add vaccination request to the vaccination request asset
      else
          Invalid transaction
        end if
end function
function viewVaccinationRequestStatus(Patient ID)
        if Patient ID exist then
          return Vaccination request status
        else
          Invalid Patient ID
        end if
end function
function ReportHealthOrganisation(Organisation ID)
        if Organisation ID exist then
          Increment complaint reported
        else
          Invalid transaction
        end if
end function
```

Algorithm 4 shows the smart contract functionality of the requesting entity. Any requesting entity with a valid patient ID and vaccination ID can invoke the below functions:

- View vaccination certificate(): This function has been defined to view the vaccination certificate. It contains the fields of patient ID and vaccination ID.

**Algorithm 4** Smart contract functionality of requesting entity

```
1  function viewVaccinationCertificate(Patient ID, vaccination ID)
2      if Patient ID and vaccination ID exist then
3          return Vaccination certificate
4      else
5          Invalid Patient ID and vaccination ID
6      end if
7  end function
```

**Table 2** Summary of notations

| *Symbol* | *Description* |
|---|---|
| TN | Total number of nodes in the network |
| TDN% | Total number of data nodes in % |
| TIAN% | Total number of inactive nodes in % |
| IADN% | Number of inactive data nodes in % |
| TDN | Total number of data nodes |
| TIAN | Total number of inactive nodes |
| IADN | Number of inactive data nodes |
| (TN, TDN, TIAN, IADN) | Set of private IPFS-network parameters |
| Q | Possible ways to get number of inactive-data nodes from total number of inactive nodes |
| R | Possible ways to get number of active-data nodes from total number of active nodes |
| S | Possible ways to get total number of data nodes from all nodes |
| P | Probability of data availability |

## *5.4 Patient preferences of data availability*

In the proposed system, the patients specify their vaccination data availability choices as HIGH, MODERATE, or LOW in the transaction request. Based on given preferences, the system stores the data at the desired number of nodes in off-chain storage. In this section, Table 2 lists the notations used in the paper and their descriptions. We have first calculated the possible ways to get inactive data nodes from total inactive nodes, active data nodes from total active nodes, and total data nodes from total nodes. This gives the probability of data unavailability as:

$$\mathrm{TIAN}_{\mathrm{CIADN}} *^{\mathrm{TN-TIAN}} \mathrm{C}_{\mathrm{TDN-IADN}} /^{\mathrm{TN}} \mathrm{C}_{\mathrm{TDN}} \tag{3}$$

So the probability of data availability can be calculated as

$$P = 1 - [({}^{TIAN}C_{IADN} *^{TN-T\,IAN} C_{TDN-IADN}) /^{TN} C_{TDN}] \quad (4)$$

Suppose that TN = 100, TDN = 90, IAN = 10, and IADN = 0, which gives the probability of data availability P equal to 1.

## 6 Results

To test the performance of the proposed framework, we have conducted experiments using the Intel Core i5, an 8th generation CPU, on a Ubuntu 64-bit operating system with 12.00 GB of RAM. We have used the Ethereum Geth environment to create the blockchain network. We have built a smart contract in the Solidity programming language. The smart contract of the proposed design has been deployed and tested over the remix IDE. The set of APIs to communicate with the blockchain has been written in node JS. The algorithms to compute the IPFS network parameters and probability of data availability have been written in JavaScript.

### *6.1 Computation of IPFS-Network parameters*

In this section, the private IPFS-network parameters have been calculated and are shown in Algorithm 5. Initially, the preferences for data availability of patients have been fetched from the ledger. This algorithm performs the following functions:

- getTotalDataNodes(): This function takes the patient preference for data availability and a total number of nodes as inputs and returns the total number of data nodes as an output.
- getTotalInactiveNodes(): This function takes the total number of nodes and inactive nodes in % of all nodes as an input, and returns the total number of inactive nodes as an output.
- getInactiveDataNodes(): function takes the total number of nodes and in active data nodes in % of all nodes as an input and returns the total number of inactive nodes as an output.

**Algorithm 5** Computation of private IPFS-network parameters

```
1    INPUT: PPDA, TN, TIAN%, IADN%
2    OUTPUT: TDN, TIAN, IADN
3    function getTotalDataNodes(PPDA, TN)
4        if PPDA == 'HIGH' then
5            TDN% = 90
6            TDN= TDN%*TN/100
7            return TDN
8        else if PPDA == 'MODERATE' then
9            TDN% = 75
10           TDN= TDN%*TN/100
11           return TDN
```

```
        else if PPDA == 'LOW' then
            TDN% = 50
            TDN= TDN%*TN/100
            return TDN
        else
            TDN% = 50
            TDN= TDN%*TN/100
            return TDN
        end if
    end function
    function getTotalInactiveNodes(TN,TIAN%)
        TIAN= TIAN%*TN/100
        return TIAN
    end function
    function getInactiveDataNodes(TN,IADN%)
        IADN= IADN%*TN/100
        return IADN
    end function
```

## 6.2 Computation of probability of data availability

In this section, the probabilities of data availability have been calculated and are shown in Algorithm 6. This algorithm performs the below functions:

- getProbabilityofDataAvailability() This function takes the set of IPFS network parameters (TN, TDN, IAN, and IADN) as an input and returns the probability of data availability as an output. This function performs the following operations: it determines the total number of data nodes, determines the total number of inactive nodes, determines the number of inactive data nodes, determines possible ways to get inactive data nodes from total inactive nodes, active data nodes from total active nodes, and total data nodes from total nodes, and finally determines the probability of data availability.

**Algorithm 6** Computation of probability of data availability

```
INPUT: Set of IPFS-network parameters(TN, TDN, TIAN, IADN)
OUTPUT: Probability of data availability
function getProbabilityofDataAvailability(TN, TDN, TIAN, IADN)
Q= combination(TIAN,IADN)
R= combination((TN-TIAN), (TDN-IADN))
S = combination(TN, TDN)
P = (Q*R)/S
return P
end function
```

### *6.3 Data availability analysis*

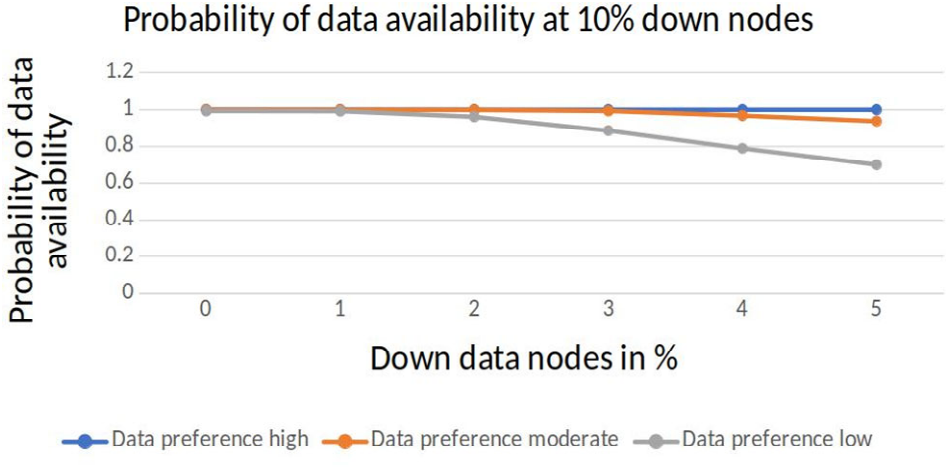
The patients can specify the data availability preference as HIGH, MODERATE, or LOW. Based on preference, the system stores the data at the desired number of network nodes. If the preference is high, data is shared with 90% of the total number of network nodes. If the preference is moderate, data is maintained at 75% of the total number of network nodes. If the preference is low, data is maintained at 50% of the total number of network nodes. The probability of data availability can be calculated by Equation 4 for different patient preferences. We have calculated the probability of data availability for each patient preference by considering the total number of nodes, the total number of inactive nodes (TIAN%) in % of all nodes, and the number of inactive-data nodes (IADN%) in % of all nodes. In our investigation, TN is kept at 100, and TDN can be 90%, 75%, or 50% according to the patient preference. The IAN values have been taken as 10%, 20%, and 30%, and the IADN has been taken as 0%, 1%, 2%, 3%, 4%, and 5%. First, we have investigated the probability of data availability for different patient preferences at 10% of inactive nodes and 0–5% of inactive-data nodes, which is shown in Table 3.

**Table 3** Probability of data availability at 10% down nodes

| *Down data nodes in %* | *Preference high* | *Preference moderate* | *Preference low* |
|---|---|---|---|
| 0 | 1 | 0.999980908 | 0.993472384 |
| 1 | 1 | 0.999942144 | 0.992763175 |
| 2 | 0.99999999 | 0.999183445 | 0.962006667 |
| 3 | 0.999999186 | 0.993562236 | 0.886903568 |
| 4 | 0.999969002 | 0.968548839 | 0.788586783 |
| 5 | 0.999864321 | 0.936827418 | 0.694371652 |

Figure 6 illustrates the data availability probability with different user preferences at 10% inactive nodes.

**Figure 6** Probability of data availability at 10% down nodes (see online version for colours)



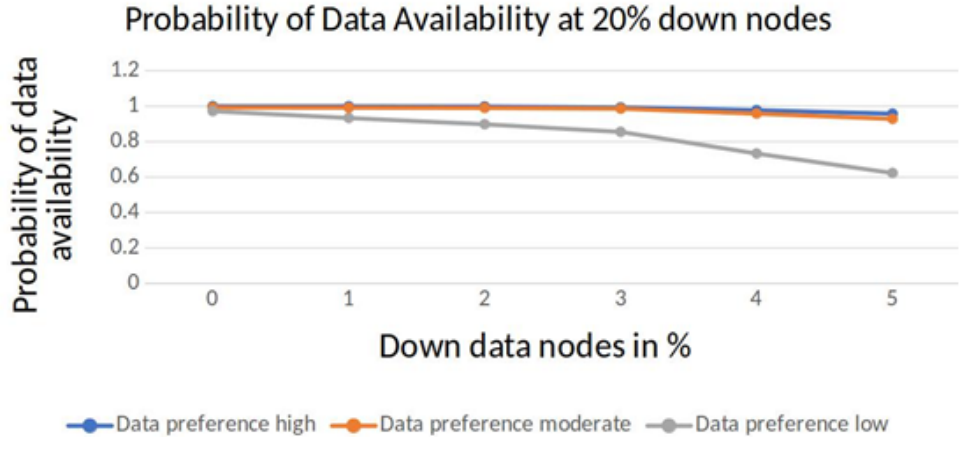
Next, we have investigated the probability of data availability at 20% of inactive nodes and 0–5% of inactive data nodes, which is shown in Table 4.

**Table 4** Probability of data availability at 20% down nodes

| *Down data nodes in %* | *Preference high* | *Preference moderate* | *Preference low* |
|---|---|---|---|
| 0 | 0.999964426 | 0.992999224 | 0.972194988 |
| 1 | 0.999732146 | 0.991977004 | 0.933869161 |
| 2 | 0.998476583 | 0.990632066 | 0.898397569 |
| 3 | 0.993371798 | 0.98645864 | 0.855391381 |
| 4 | 0.977762382 | 0.95846853 | 0.733128782 |
| 5 | 0.959678436 | 0.92646497 | 0.626173786 |

Figure 7 illustrates the data availability probability with different user preferences at 20% inactive nodes.

**Figure 7** Probability of data availability at 20% down nodes (see online version for colours)



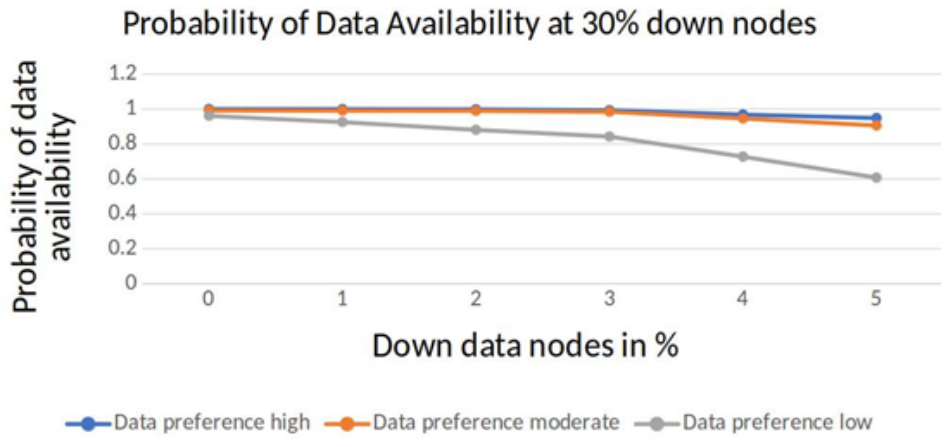

Finally, we have investigated the probability of data availability for different patient preferences at 30% of inactive nodes and 0–5% of inactive-data nodes, which is shown in Table 5.

**Table 5** Probability of data availability at 30% down nodes

| *Down data nodes in %* | *Preference high* | *Preference moderate* | *Preference low* |
|---|---|---|---|
| 0 | 0.999998264 | 0.991999594 | 0.961331795 |
| 1 | 0.999642144 | 0.990995976 | 0.925382448 |
| 2 | 0.998083445 | 0.989968671 | 0.881029357 |
| 3 | 0.993262236 | 0.984806468 | 0.842788793 |
| 4 | 0.968548839 | 0.946043199 | 0.727516847 |
| 5 | 0.946325827 | 0.904382465 | 0.606825345 |

Figure 8 illustrates the data availability probability with different user preferences at 30% inactive nodes.

**Figure 8** Probability of data availability at 30% down nodes (see online version for colours)




The obtained results show that relatively better data availability has been achieved at IADN = 0–-3%. For high data availability, it is between 0.9999 and 1.0000 at 10% inactive nodes, 0.9933 and 0.9999 at 20% inactive nodes, and 0.9932 and 0.9999 at 30% inactive nodes. For moderate data availability choice, it is between 0.9935 and 0.9999 at 10% inactive nodes, 0.9864–0.9929 at 20% inactive nodes, and 0.9848–0.9919 at 30% inactive nodes. For low data availability, it is between 0.9934 and 0.9869 at 10% inactive nodes, 0.8553 and 0.9721 at 20% inactive nodes, and 0.8427 and 0.9613 at 30% inactive nodes. The probability of data availability obtained is above 90% at 10% down nodes and 0-3% inactive-data nodes. So we have concluded that the optimal probability of data availability is possible at a low storage cost by ensuring that the down data nodes should not be more than 3% of total network nodes.

**Table 6** Execution cost of smart contract functions

| *Function* | *Transaction size (in bytes)* | *Execution cost (in Gas)* |
|---|---|---|
| reportHealthOrganisation | 202 | 49854 |
| approveVaccinationRequest | 522 | 76191 |
| registerNewPatient | 650 | 84395 |
| patientRegistrationRequest | 692 | 119616 |
| addVaccinationRequest | 778 | 121448 |
| addHealthOrganisation | 806 | 128498 |
| addVaccinationCertificate | 906 | 212253 |

## *6.4 Execution cost analysis*

We have built the proposed Ethereum smart contract in the Solidity programming language. The smart contract of the proposed design has been compiled and deployed in

the remix environment for testing. We have assessed the execution cost of smart contract functions, which is shown in Table 6.

Figure 9 shows the remix IDE interface representing the smart contract functions defined in the workflow.

**Figure 9** Remix ide interface representing the smart contract functions (see online version for colours)

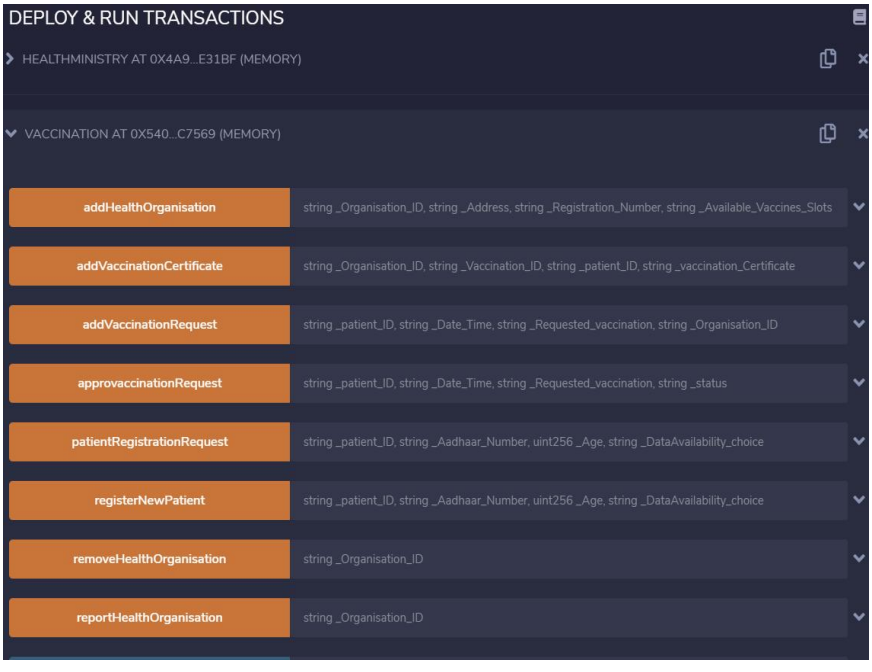
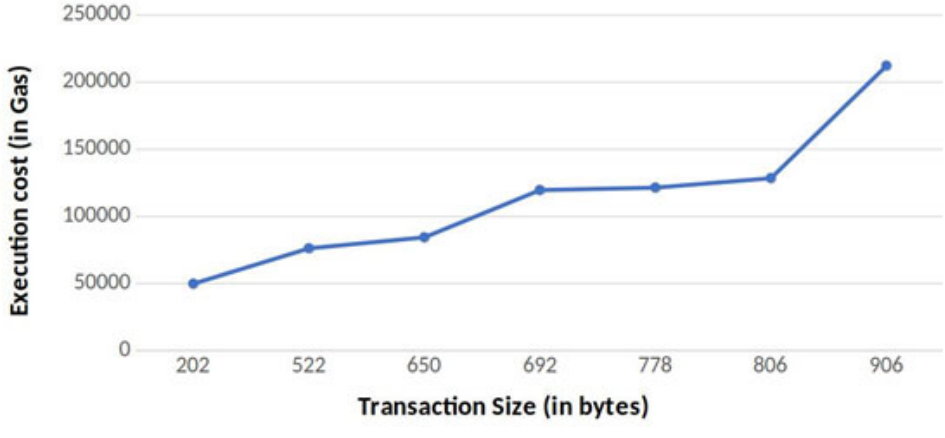



Figure 10 represents the execution costs of different transaction sizes. The maximum execution cost is in the transaction of the contract, which is equal to 4291404 gas and all transaction functions have low costs.

**Figure 10** Execution cost vs. transaction size (see online version for colours)

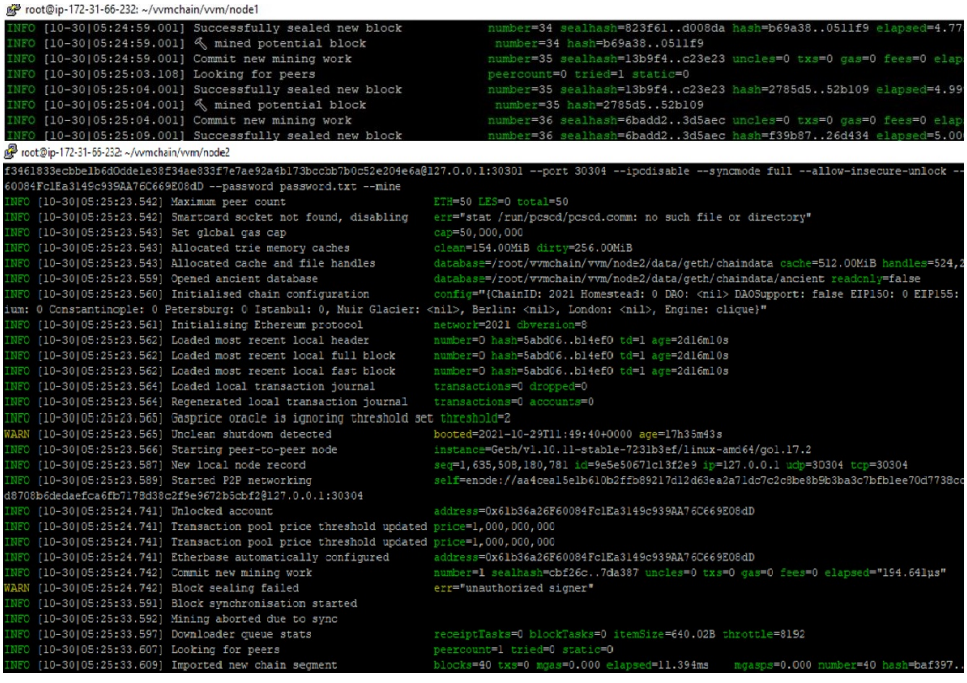


Furthermore, during the testing phase, we decreased the execution fees by introducing various checks in the smart contract. These checks revert invalid transactions to avoid unnecessary execution fees due to the wastage of computation power. For scalability and cost reduction, vaccination records have been stored off-chain through IPFS based on patient preference. The execution cost can be reduced further by batching multiple transactions into a single transaction.

## *6.5 Energy efficiency analysis*

For blockchain network development, we have created 1 boot node and 4 peer nodes representing the users (health ministry, health organisation, patient, requesting entity) in the Ethereum Geth environment. The PoA consensus mechanism has been utilised for mining in the proposed system. Using the puppeth tool, only one admin node representing the health ministry has been authorised to mine blocks. Because the mining process is not completed by all peers, wastage of energy is reduced. Figure 11 represents the block sealing process at node1 and node2.

**Figure 11** Block sealing process at node 1 and node 2 (see online version for colours)




It is clear from this figure that node 1 seals a new block successfully by committing new mining work. As only node1 has been authorised to seal a new block, when node2 or any other node commits new mining work, block sealing fails with the error message 'Unauthorised signer'. In this scheme, only one node out of four consumes energy when mining a new block. Hence, the proposed PoA consensus-based system reduces the energy consumption in sealing new blocks by a factor of 4 as compared to the same system designed using the PoW consensus engine.

## 6.6 Comparative analysis

There is limited work related to blockchain-based vaccination systems, almost all of which focuses on COVID vaccination records and COVID vaccine supply schemes. In this work, we have proposed a novel blockchain-based, scalable, and optimal vaccination record management model. It is not limited to COVID-19 vaccination but is aimed toward creating the vaccination record throughout the patient's life, i.e., from childhood to death. A comparison of the proposed blockchain-based vaccination system with related work in terms of different metrics is shown in Table 7.

**Table 7** Comparison of the proposed vaccination scheme with prior works

| *Qualitative metrics* | *Fiquaro et al. (2021)* | *Yong et al. (2020)* | *Deka et al. (2020)* | *Carniel et al. (2021)* | *Eisenstadt et al. (2020)* | *Ait Bennacer et al. (2022)* | *Nabil et al. (2022)* | *Proposed work* |
|---|---|---|---|---|---|---|---|---|
| Ethereum based | × | × | √ | √ | √ | √ | √ | √ |
| Smart contract | √ | √ | √ | √ | × | √ | √ | √ |
| Cost analysis | × | × | √ | × | × | √ | √ | √ |
| Energy efficient | × | × | × | × | √ | × | × | √ |
| Scalability | × | × | √ | × | × | √ | √ | √ |
| Cost efficient | × | × | × | × | × | √ | √ | √ |
| Availability analysis | × | × | × | × | × | × | × | √ |
| Validation mechanism | × | × | × | × | × | √ | √ | √ |

Note: ×: Unavailable, √: available.

The comparison of proposed work with prior works in terms of various performance metrics is summarised as follows:

- Ethereum-based: For managing vaccination records, public blockchains such as Ethereum are preferred over private or consortium blockchains because they provide improved decentralisation, security, availability, integrity, and validity. Furthermore, because public blockchains have a global presence, vaccination certificates issued on these systems are guaranteed to be widely acknowledged, accepted, and validated across national boundaries. There are few Ethereum blockchain-based systems (Deka et al., 2020; Carniel et al., 2021; Eisenstadt et al., 2020; Ait Bennacer et al., 2022; Nabil et al., 2022) and very few Hyperledger blockchain based-systems (Fiquaro et al., 2021; Yong et al., 2020) available. The proposed system is deployed over the Ethereum blockchain for enhanced decentralisation and global validation.

- Smart-contract: The smart contract functionalities used in the proposed system cover the entire vaccination process with access controls, which were missing in the existing papers. A novel smart contract algorithm with access control checks is developed, enabling complaints against health organisations and their removal when necessary. This ensures smooth governance of the vaccination process over the blockchain network, with a focus on low-cost execution for different transaction sizes.
- Cost-analysis: Execution cost is the amount of computational resources, measured in gas, required to perform a transaction or execute a smart contract on the network. In the proposed system, within the smart contract, various checks are introduced to lower the execution cost. These checks revert invalid transactions to avoid incurring unnecessary execution fees due to computation power waste. The execution costs of various functionalities with different transaction sizes are presented for the proposed system. It was not evaluated in most of the existing works and was not analysed to make it lower.
- Energy-efficient: PoA is an improved version of the PoS consensus protocol for reaching consensus through authorised validators. In this consensus mechanism, a limited number of nodes have block sealing power, and the validator's identity is at stake. The proposed system is energy efficient in comparison to the existing systems because it is based on the PoA-consensus mechanism, whereas all others are based on PoW.
- Scalability: Scalability is the ability of a blockchain network to handle an increasing number of transactions or users efficiently and without compromising its performance, security, or decentralisation. Scalability is a major issue in the adoption of blockchain technology, and most of the existing work has not addressed it. In the proposed work, we have provided a scalable solution using private IPFS as off-chain storage. Private IPFS was not used in the existing work but has been used with the patient preference option in the proposed scheme.
- Cost-efficient: In the proposed scheme, vaccination certificates are stored off-chain in private IPFS based on patient preference, and the hashes of the vaccination certificates are stored on the Ethereum blockchain. Hence, execution cost reduction as well as storehouse cost reduction are achieved in the proposed work in comparison to the existing works.
- Availability analysis: Data availability analysis is for ensuring that the data stored is accessible and retrievable by anyone who needs it. We have analysed the parameters for a private IPFS network to get optimal data availability at a low storage cost. This aspect has not been addressed in any previous work.
- Validation mechanism: Validation mechanisms are for ensuring that the vaccination certificates presented by patients are accurate. This prevents the introduction of incorrect or faulty data into the system. Most of the existing works lack validation mechanisms. We have implemented a QR code-based validation mechanism so that vaccination certificates can be verified by any requesting identity globally.

## 7 Conclusions

This study presents a novel blockchain solution for vaccination record management based on the PoA consensus mechanism. Unlike prior blockchain-based models, this system is not limited to COVID-19 vaccination records but aims to maintain vaccination records throughout a patient's lifetime. The proposed system enables healthcare organisations to securely upload vaccination records, allowing requesting entities to access trustworthy vaccination data. As a result, the system proves beneficial in protecting public health and fulfilling non-medical requirements such as education or employment. The smart contract implemented in this system covers the entire vaccination process and incorporates various checks to minimise execution fees. This approach ensures cost efficiency while maintaining the integrity and security of the records. For scalability, availability, and cost reduction, vaccination records are stored off-chain using a private IPFS, as per patient preference. The proposed design ensures the authenticity of vaccination records and reduces fraud through QR code-based validation. All smart contracts are successfully tested in the Remix IDE environment. The performance analysis, considering various transaction sizes, indicates low execution costs for all transaction functions. During testing, the introduction of various checks in the smart contract significantly reduced execution fees by identifying and rejecting invalid transactions, thereby optimising computational power usage. Additionally, the study has investigated data availability in the private IPFS network based on patient preference. Network parameters are examined to achieve optimal data availability at a low storage cost. It is found that maintaining down data nodes at no more than 3% of the total network nodes ensures optimal data availability at a cost-effective storage rate. Comparative analysis demonstrates that the proposed scheme offers scalability, cost efficiency, and energy efficiency when compared to existing solutions.

## References

Ait Bennacer, S., Aaroud, A., Sabiri, K., Rguibi, M.A. and Cherradi, B. (2022) 'Design and implementation of a new blockchain-based digital health passport: a Moroccan case study', *Informatics in Medicine Unlocked*, Vol. 35, No. 2022, p.101125, https://doi.org/10.1016/j.imu.2022.101125.

Alam, S., Shuaib, M., Khan, W.Z., Garg, S., Kaddoum, G., Hossain, M.S. and Zikria, Y.B. (2021) 'Blockchain-based initiatives: current state and challenges', *Computer Networks*, Vol. 198, No. 2021, p.108395, https://doi.org/10.1016/j.comnet.2021.108395.

Al-Marridi, A.Z., Mohamed, A. and Erbad, A. (2021) 'Reinforcement learning approaches for efficient and secure blockchain-powered smart health systems', *Computer Networks*, Vol. 197, No. 2021, p.108279, https://doi.org/10.1016/j.comnet.2021.108279.

Arnold, R. and Longley, D. (2021) 'Continuity: a deterministic byzantine fault tolerant asynchronous consensus algorithm', *Computer Networks,* Vol. 199, No. 2021, p.108431, https://doi.org/10.1016/j.comnet.2021.108431.

Benarous, L., Kadri, B. and Bouridane, A. (2020) 'Blockchain-based privacy-aware pseudonym management framework for vehicular networks', *Arabian Journal for Science and Engineering*, Vol. 45, No. 8, pp.6033–6049.

Berdik, D., Otoum, S., Schmidt, N., Porter, D. and Jararweh, Y. (2021) 'A survey on blockchain for information systems management and security', *Information Processing and Management*, Vol. 58, No. 1, p.102397, https://doi.org/10.1016/j.ipm.2020.102397.

Carniel, A., Leme, G., de Melo Bezerra, J. and Hirata, C.M. (2021) 'A blockchain approach to support vaccination process in a country', in *ICEIS*, Vol. 1, No. 1, pp.343–350, ISBN: 978-989-758-509-8; ISSN 2184-4992, SciTePress, DOI: 10.5220/0010520003430350.

da Silva, R.C.K. (2021) 'Analyzing blockchain integrated architectures for effective handling of IoT-ecosystem transactions', *Computer Networks*, Vol. 201, No. 2021, p.108610, https://doi.org/10.1016/j.comnet.2021.108610.

Deka, S.K., Goswami, S. and Anand, A. (2020) 'A blockchain based technique for storing vaccination records', in *2020 IEEE Bombay Section Signature Conference (IBSSC)*, IEEE, pp.135–139.

Dursun, T. and Üstündağ, B.B. (2021) 'A novel framework for policy based on-chain governance of blockchain networks', *Information Processing and Management*, Vol. 58, No. 4, p.102556, https://doi.org/10.1016/j.ipm.2021.102556.

Eisenstadt, M., Ramachandran, M., Chowdhury, N., Third, A. and Domingue, J. (2020) 'Covid-19 antibody test/vaccination certification: there's an app for that', *IEEE Open Journal of Engineering in Medicine and Biology*, Vol. 1, pp.148–155, Electronic ISSN: 2644-1276, DOI: 10.1109/OJEMB.2020.2999214.

Ekanayake, O.A. and Halgamuge, M.N. (2021) 'Lightweight blockchain framework using enhanced master-slave blockchain paradigm: fair rewarding mechanism using reward accuracy model', *Information Processing and Management,* Vol. 58, No. 3, p.102523, https://doi.org/10.1016/j.ipm.2021.102523.

Fiquaro, M.A., Zahilah, R., Othman, S.H., Arshad, M.M. and Saad, S.M.S. (2021) 'Vaccination system using blockchain technology: a prototype development', in: *2021 3rd International Cyber Resilience Conference (CRC)*, IEEE, pp.1–6.

Fu, W., Wei, X. and Tong, S. (2021) 'An improved blockchain consensus algorithm based on raft', *Arabian Journal for Science and Engineering*, Vol. 46, No. 9, pp.8137–8149.

Goyat, R., Kumar, G., Rai, M.K., Saha, R., Thomas, R. and Kim, T.H. (2020) 'Blockchain powered secure range-free localization in wireless sensor networks', *Arabian Journal for Science and Engineering*, Vol. 45, No. 8, pp.6139–6155.

Haouari, M., Mhiri, M., El-Masri, M. and Al-Yafi, K. (2022) 'A novel proof of useful work for a blockchain storing transportation transactions', *Information Processing and Management*, Vol. 59, No. 1, p.102749, https://doi.org/10.1016/j.ipm.2021.102749.

Houtan, B., Hafid, A.S. and Makrakis, D. (2020) 'A survey on blockchain-based self sovereign patient identity in healthcare', *IEEE Access*, Vol. 8, No. 2020, pp.90478–90494.

Khalid, S., Maqbool, A., Rana, T. and Naheed, A. (2020) 'A blockchain-based solution to control power losses in Pakistan', *Arabian Journal for Science and Engineering*, Vol. 45, No. 8, pp.6051–6061.

Khan, A., Khan, M.M., Khan, K.M., Arshad, J. and Ahmad, F. (2021) 'A blockchain-based decentralized machine learning framework for collaborative intrusion detection withinuavs', *Computer Networks*, Vol. 196, No. 2021, p.108217, https://doi.org/10.1016/j.comnet. 2021.108217.

Khan, A.A. et al. (2023) 'Cloud forensics-enabled chain of custody: a novel and secure modular architecture using blockchain hyperledger sawtooth', *International Journal of Electronic Security and Digital Forensics*, Vol. 15, No. 4, pp.413–423, https://dx.doi.org/10.1504/ IJESDF.2023.131959.

Kumar, M. and Chand, S. (2021) 'Medhypchain: a patient-centered interoperability hyperledger-based medical healthcare system: regulation in COVID-19 pandemic', *Journal of Network and Computer Applications*, Vol. 179, No. 2021, p.102975, https://doi.org/10.1016/j.jnca.2021. 102975.

Li, C., Zhang, J., Yang, X. and Youlong, L. (2021) 'Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices', *Information Processing and Management*, Vol. 58, No. 4, p.102602, https://doi.org/10.1016/j.ipm.2021.102602.

Liu, X., Zhao, G., Wang, X., Lin, Y., Zhou, Z., Tang, H. and Chen, B. (2019) Mdp-based quantitative analysis framework for proof of authority', in *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, IEEE, pp.227–236.

Liu, Y. and Xu, G. (2021) 'Fixed degree of decentralization dpos consensus mechanism in blockchain based on adjacency vote and the average fuzziness of vague value', *Computer Networks*, Vol. 199, No. 2021, p.108432, https://doi.org/10.1016/j.comnet.2021.108432.

Liu, Y., Lan, Y., Li, B., Miao, C. and Tian, Z. (2021) 'Proof of learning (pole): empowering neural network training with consensus building on blockchains', *Computer Networks,* Vol. 201, No. 2021, p.108594, https://doi.org/10.1016/j.comnet.2021.108594.

Marbouh, D., Abbasi, T., Maasmi, F., Omar, I.A., Debe, M.S., Salah, K., Ja yaraman, R. and Ellahham, S. (2020) 'Blockchain for covid-19: review, opportunities, and a trusted tracking system', *Arabian Journal for Science and Engineering*, Vol. 45, No. 12, pp.9895–9911.

Mariga, J. and Moturi, C.A. (2023) 'Improving credit information sharing in small economies using blockchain technology', *International Journal of Blockchains and Cryptocurrencies*, Vol. 4, No. 2, pp.171–185, https://doi.org/10.1504/IJBC.2023.132707.

Miyachi, K. and Mackey, T.K. (2021) Hocbs: a privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design', *Information Processing and Management*, Vol. 58, No. 3, p.102535, https://doi.org/10.1016/j.ipm.2021.102535.

Motohashi, T., Hirano, T., Okumura, K., Kashiyama, M., Ichikawa, D. and Ueno, T. (2019) 'Secure and scalable mhealth data management using blockchain combined with client hashchain: system design and validation', *Journal of Medical Internet Research,* Vol. 21, No. 5, p.e13385.

Nabil, S.S., Alam Pran, M.S., Al Haque, A.A., Chakraborty, N.R., Chowdhury, M.J.M. and Ferdous, M.S. (2022) 'Blockchain-based covid vaccination registration and monitoring', *Blockchain: Research and Applications*, Vol. 3, No. 4, p.100092, https://doi.org/10.1016/j.cra.2022.100092.

Nacer, M.I., Prakoonwit, S. and Prakash, E. (2023) 'Missa: a regional approach to maintain validity', *International Journal of Blockchains and Cryptocurrencies*, Vol. 4, No. 1, pp.26–64, https://dx.doi.org/10.1504/IJBC.2023.131658.

Naseer, O., Ullah, S. and Anjum, L. (2021) 'Blockchain-based decentralized lightweight control access scheme for smart grids', *Arabian Journal for Science and Engineering*, Vol. 46, No. 9, pp.8233–8243.

Omar, I.A., Jayaraman, R., Salah, K., Yaqoob, I. and Ellahham, S.Applications of blockchain technology in clinical trials: review and open challenges', *Arabian Journal for Science and Engineering*, Vol. 46, No. 4, pp.3001–3015.

Pandey, P. and Litoriya, R. (2021) 'Securing e-health networks from counterfeit medicine penetration using blockchain', *Wireless Personal Communications*, Vol. 117, No. 1, pp.7–25.

Patil, P., Sangeetha, M. and Bhaskar, V. (2021) 'Blockchain for iot access control, security and privacy: a review', *Wireless Personal Communications*, Vol. 117, No. 3, pp.1815–1834.

Platt, M. and McBurney, P. (2021) 'Sybil attacks on identity-augmented proof-of-stake', *Computer Networks*, Vol. 199, No. 2021, p.108424, https://doi.org/10.1016/j.comnet.2021.108424.

Sai, A.R., Buckley, J., Fitzgerald, B. and Gear, A.L. (2021) 'Taxonomy of centralization in public blockchain systems: a systematic literature review', *Information Processing and Management*, Vol. 58, No. 4, p.102584, https://doi.org/10.1016/j.ipm.2021.102584.

Sanka, A.I. and Cheung, R.C. (2021) 'A systematic review of blockchain scalability: issues, solutions, analysis and future research', *Journal of Network and Computer Applications*, Vol. 195, No. 2021, p.103232, https://doi.org/10.1016/j.jnca.2021.103232.

Saxena, R., Deepak, A. and Vishal, N. (2023) 'Efficient blockchain addresses classification through cascading ensemble learning approach', *International Journal of Electronic Security and Digital Forensics*, Vol. 15, No. 2, pp.195-210, https://dx.doi.org/10.1504/IJESDF.2023.129278.

Shahnaz, A., Qamar, U. and Khalid, A. (2019) 'Using blockchain for electronic health records', *IEEE Access,* Vol. 7, No. 2019, pp.147782–147795.

Sharma, N. and Rajesh, R. (2023) 'A novel hyperledger blockchain-enabled decentralized application for drug discovery chain management', *Computers and Industrial Engineering*, p.109501, https://doi.org/10.1016/j.cie.2023.109501.

Sharma, N. and Rohilla, R. (2020) 'Blockchain based approach for managing medical practitioner record: a secured design', in *International Advanced Computing Conference*, Springer, pp.73–82.

Sharma, N. and Rohilla, R. (2022) 'Blockchain based electronic health record management system for data integrity', in *Proceedings of International Conference on Computational Intelligence*, Springer, pp.289–297.

Sharma, N. and Rohilla, R. (2023) 'A multilevel authentication-based blockchain powered medicine anti-counterfeiting for reliable IoT supply chain management', *J. Supercomput*., https://doi.org/10.1007/s11227-023-05654-w.

Sharmila, A.H. and Jaisankar, N. (2021) 'Edge intelligent agent assisted hybrid hierarchical blockchain for continuous healthcare monitoring and recommendation system in 5g wban-IoT', *Computer Networks*, Vol. 200, No. 2021, p.108508, https://doi.org/10.1016/j.comnet.2021.108508.

Song, H., Zhu, N., Xue, R., He, J., Zhang, K. and Wang, J. (2021) 'Proof-of-contribution consensus mechanism for blockchain and its application in intellectual property protection', *Information Processing and Management*, Vol. 58, No. 3, p.102507, https://doi.org/10.1016/j.ipm.2021.102507.

Spataru, A.L., Pungila, C-P. and Radovancovici, M. (2021) 'A high-performance native approach to adaptive blockchain smart-contract transmission and execution', *Information Processing and Management*, Vol. 58, No. 4, p.102561, https://doi.org/10.1016/j.ipm.2021.102561.

Udokwu, C. and Norta, A. (2021) 'Deriving and formalizing requirements of decentralized applications for inter-organizational collaborations on blockchain', *Arabian Journal for Science and Engineering*, Vol. 46, No. 9, pp.8397–8414.

Wang, X., Chen, Y. and Zhang, Q. (2021) 'Incentivizing cooperative relay in utxo based blockchain network', *Computer Networks*, Vol. 185, No. 2021, p.107631, https://doi.org/10.1016/j.comnet.2020.107631.

Wu, Y., Wang, Z., Ma, Y. and Leung, V.C. (2021) 'Deep reinforcement learning for blockchain in industrial IoT: a survey', *Computer Networks*, Vol. 191, No. 2021, p.l108004, https://doi.org/10.1016/j.comnet.2021.108004.

Yong, B., Shen, J., Liu, X., Li, H., Chen, F. and Zhou, Q. (2020) 'An intelligent blockchain based system for safe vaccine supply and supervision', *International Journal of Information Management*, Vol. 52, No. 2020, p.102024.

Zhang, G., Yang, Z. and Liu, W. (2021) 'Blockchain-based privacy preserving e health system for healthcare data in cloud', *Computer Networks*, https://doi.org/10.1016/j.comnet.2021.108586.

Zhu, P., Hu, J., Zhang, Y. and Li, X. (2021) 'Enhancing traceability of infectious diseases: a blockchain-based approach', *Information Processing and Management*, Vol. 58, No. 4, p.102570, https://doi.org/10.1016/j.ipm.2021.102570.