Healthcare Analytics 3 (2023) 100175

Contents lists available at ScienceDirect

Healthcare Analytics

journal homepage: www.elsevier.com/locate/health

HealthDote: A blockchain-based model for continuous health monitoring using interplanetary file system

Sireejaa Uppal [a], Bindiya Kansekar [a], S. Mini [a,*], Deepak Tosh [b]

[a] Department of Computer Science and Engineering, National Institute of Technology Goa, Goa 403401, India
[b] Department of Computer Science, University of Texas at El Paso, TX 79968-0518, United States of America

ARTICLE INFO

Keywords:
Blockchain
InterPlanetary file system
Internet of Things
Proof of work
Proof of stake
Directed acyclic graph
Practical byzantine fault tolerance

ABSTRACT

The Healthcare industry demands increased privacy and security to protect confidential patient information and comply with regulations. Both these features can be incorporated into the existing systems using Blockchain technology. The only challenge faced here is the ease of users, but this can be quickly resolved by integrating the Internet of Things (IoT) and blockchain. IoT-based devices overcome limited computing capacity for personal intelligent health devices. Cloud-assisted IoT devices also require limited storage capacity for devices like wearable sensors. However, it must be considered that this system still has drawbacks, leading to its inefficiency. These problems include Data Privacy and Data sharing. This paper proposes an Interplanetary File System (IPFS) based solution to these problems. Here, the users continually upload the health data collected by IoT devices and add them to blockchain transactions that the other user nodes, such as physicians, pharmacists, insurance companies, hospital authorities, etc., can access. This system ensures the well-being of the users by monitoring the data gathered every 5 min and daily. It also facilitates the alarm feature in an emergency, making it reliable. The user receives daily notifications regarding his lifestyle, and the family members receive the notifications on his behalf if there are some chances of an emergency. The authorized doctors are also notified immediately in case an emergency is detected. Apart from this feature, the user can get consultations from doctors, prescriptions from the pharmacist, funds from insurance authorities, and hospital supplies, all through the transaction on the six blockchains of HealthDote using the cryptocurrency DoteCoins, which are designed specifically for this system.

1. Introduction

The Healthcare sector can be revolutionized with the intervention of Blockchain technology equipped with IoT and IPFS storage systems. Blockchain in this sector will resolve all security and privacy concerns and eliminates fraud [1]. The IoT used in smartwatches can be configured further to enhance the user experience, and all its bulk data can be stored onto IPFS. These have been incorporated in HealthDote to provide users with a hassle-free and reliable experience in terms of Healthcare facilities.

The architecture of HealthDote consists of six blockchains, namely-UserChain, MonitoringChain, PhysicianChain, PharmacistChain, FundChain, and SCMChain. These chains interact amongst themselves with the help of DoteCoins. In this system, the patient's health-related data is continuously sensed using IoT devices [2] and is stored on the UserChain, which the MonitoringChain subsequently accesses at a regular intervals of 5 min. The data gathered is analyzed and the results are encrypted and stored in the MonitoringChain. This data is consequently accessed by the authorized Doctors or physicians who provided the diagnosis and stored in the PhysicianChain. The diagnosis further serves as a basis for the Pharmacists' prescription, consequently stored in the PharmacistChain. This succession of events is followed by the Insurance Authorities accessing the prescription to grant the relevant fund to the patient. The documents related to this are stored on FundChain. The hospital stock authorities update the remaining inventory stock by updating the SCMChain by updating inventory as per the prescription. This process gives rise to a real-time health-tracking system as described in [3].

The basic model of HealthDote is inspired by the CareBlocks architecture [4] and MapChain [5] with some additional features as CareBlocks was not feasible for emergencies if there was a case of life and death. Since the PoW(Proof of Work) is used as the consensus algorithm, it is nearly impossible for a patient to undergo this mining process before receiving any medical help. In order to overcome this shortcoming, in HealthDote, we introduce an "Alarm" feature that will automatically help the patient in case of an emergency. The alarm will be raised based on the flag value. The flag value is set by analyzing

[*] Corresponding author.
E-mail addresses: sireejaa2014@gmail.com (S. Uppal), bindiyakansekar@gmail.com (B. Kansekar), mini@nitgoa.ac.in (S. Mini), dktosh@utep.edu (D. Tosh).

https://doi.org/10.1016/j.health.2023.100175
Received 15 January 2023; Received in revised form 5 March 2023; Accepted 9 April 2023

the patient's health data after regular time intervals. The flag value is set to 1 in case of an emergency. As a result, the Alarm feature notifies the authorized doctors and the family members of the patients automatically. The flag value is set to 2 if there is some probability of a mishap. In this case, the notification is sent to the family of the patient only in order to warn them regarding an uncertain situation. The flag value is set to 3 when the system intends to inform the patient about his deteriorating habits, resulting in unwanted circumstances if persistent for a long time. The user can access the services of doctors, chemists, insurance, and hospital supplies in exchange for DoteCoins, which is the cryptocurrency created for this specific system. Further, the system's speed is enhanced by using various consensus algorithms, including PoS(Proof of Stake), DAG(Directed Acyclic Graph), and PBFT(Practical Byzantine Fault Tolerance).

The major contributions of this work are as follows:

- An Interplanetary File System (IPFS) based solution to eliminate issues related to Data Privacy and Data Sharing, is developed.
- A comparison of various consensus algorithms including Proof of Work, Proof of Stake and Directed Acyclic Graph in Blockchain based architecture, is carried out.
- Practical Byzantine Fault Tolerance algorithm is applied and compared with Proof of Stake and Directed Acyclic Graph.

The rest of the paper is organized as follows. Section 2 reviews the related work. Section 3 describes the proposed architecture of CareBlocks. The results are presented and discussed in Section 4. Concluding remarks and scope of future work in Section 5 ends the paper.

2. Related work

The foundation of HealthDote is constructed by leveraging the crucial features of some of the existing technologies which have worked wonders in their respective spheres [6,7]. One of these is the Blockchain-based system for healthcare as proposed in [4] that promises privacy preservation and data integrity. The main source of data in CareBlocks is a patient's medical records. This blockchain architecture comprises four sub-blockchains, namely — PatientChain, DoctorChain, ChemistChain, and InsuranceChain. Also, plus coins in the system act as a reward and means of exchange for the interaction of all sub-blockchains. A Hash of a patient's medical report is stored on PatientChain. Registered doctors can treat a patient and create a diagnosis report and transactions for these are stored on DoctorChain. The patient possesses the right to add or revoke a doctor. Likewise, ChemistChain maintains track of prescriptions given by the doctor to a patient, and InsuranceChain stores the record of policies availed by the patient. Here, data storage is achieved using an interplanetary file system, which simultaneously accounts for data availability and security. All these chains guarantee smooth functioning for the healthcare sector. Furthermore, future work on this model aims to integrate machine learning with blockchain so as to give better disease prediction. HealthDote extends the concept of CareBlocks in order to expand the functionalities provided to the patient along with long-term and short-term health reports, alarm facilities etc.

Blockchain-based solutions have been serving many industries [8] since its launch and healthcare is one of them. As described in [9,10], the application of blockchain in this sector has overcome the hurdles in authentication, interoperability, and record-sharing requirements [11–13] which forms the basis of patient security in HealthDote. In [14], the approach of data sharing, privacy-preserving, and data integrity are proposed for the Electronic Health Record(EHR), wherein EHR are stored securely with the access control system for the different level users [15,16]. In HealthDote these EHRs contribute to the scalability feature of online records in contrast to the off-chain storage of records. Clinical notes and laboratory results are stored in EHR. Functionalities such as patient appointment management and hospital billing are also implemented with improved security and cost-effectiveness. Though [17–19] provide the basis for implementing and storing these EHRs, they suffer from some drawbacks including interoperability, information asymmetry, and data breaches.

The basic input for the EHRs consisting of vital parameters like blood pressure, body temperature and others in HealthDote is provided by the sensors and IoT devices present in the wearables accessories of the patient. Nevertheless, this is subject to data security and privacy issues [20,21]; therefore, access control plays a crucial role in HealthDote. Access control schemes based on single-server architecture function with a single point of failure limit the functionality of the blockchain architecture. Also, data can be tempered using illegal access requests.

Blockchain has been originally proposed for constructing a public distributed ledger for all transactions in Bitcoin. Over time there were significant developments like performance improvement, solving the double spending attack, and constructing efficient distributed consensus mechanisms. Blockchain is also used in vehicular networks [22], to effectively evaluate the trustworthiness of vehicles in untrusted environments. However, schemes like this can address their stated issues in specific network scenarios, but they cannot be straightly adopted in smart healthcare systems. In smart healthcare, for privacy preservation, not only the user's Health Record Data but also the doctor's diagnosis should be protected. The solutions for these issues were found in a lightweight blockchain that enables the IoT domain to deploy its network designed in [23]. Here, a DDOS attack is avoided using the public key of IoT comprising identity-based signature(IBS) to enable edge servers to filter and forward access requests initiated by validated users. The real-time off-chain policy feature is embedded in the PDP algorithm for dynamic characteristics of blockchain [24].

The application of IoT in HealthDote includes using wireless sensor networks (WSNs) to capture a person's real-time data [25] and emphasizes overall model performance utilizing multi-layer Machine Learning (ML) model [26]. Also, it provides a detailed study of body sensors for autonomous functioning and data pre-processing in a virtual network. For data transfer, [27] focuses on EMR sharing in an open network. Altogether, these algorithms aim for data quality and individual analysis of the output decisions on beneficial transactions [28]. Patient interaction with the system is a crucial point for the model success perspective as also described in [29]. A full-fledged system like HealthDote puts forth challenges for security in terms of network modeling & safety, and a related study [30] emphasizes measures to follow to avoid data breaches. [31] shows a case study of securing users' confidential data. Comprehensive survey [32] highlights a comparative study among different technological stacks to implement healthcare systems with blockchain. This can be enhanced with a continuous genetic algorithm as described in [33,34] that would be able to optimize healthcare processes based on the latest available data continuously. For example, medication dosages could be adjusted based on a patient's response to treatment, or clinical trial protocols could be adapted based on the latest research findings. Applying a continuous genetic algorithm in blockchain healthcare will improve the efficiency and effectiveness of healthcare processes [35] while ensuring patient data's security and privacy.

The study of smart wearables such as watches, glasses, and jewellery for availability, energy consumption, and communication reach has served as a baseline for including responses based on the feedback mechanism. Blockchain transaction highlighted in [36] that uses coins, and simple logic of reward-based on rules validation. The idea of system monitoring is driven by [37] where key parameters for user interface design are showcased. All these features have been incorporated into HealthDote architecture to provide patients with seamless technology that ensures a hassle-free experience.

There are broadly two different approaches to managing health conditions or promoting health, one based on clinical interventions and the other on lifestyle modifications. The clinical setup refers to the medical treatment, intervention, or management strategy used to address a specific health condition, while the lifestyle setup refers to the lifestyle modifications, behavioral changes, or non-pharmacological interventions used to improve health outcomes or prevent the onset of a particular health condition.

HealthDote is a healthcare solution that aims to provide comprehensive patient care and alleviate their suffering. The system utilizes advanced technologies such as IoT sensors and electronic medical records to monitor and manage patient health effectively. For instance, a patient with Parkinson's disease who underwent deep brain stimulation surgery to improve motor function and quality of life would benefit from the system's all-inclusive services [38]. HealthDote takes care of the entire overhead, from medicines to insurance, and ensures that the patient's medical history is readily available to the physician during consultations. Similarly, for a patient with severe depression who underwent a course of electroconvulsive therapy to alleviate symptoms, continuous monitoring of various parameters like blood and oxygen levels, sleep hours, and stress would help in monitoring their overall well-being [39]. HealthDote employs advanced IoT sensors to track these parameters and send alerts for abnormalities. Furthermore, a patient with heart failure who underwent cardiac rehabilitation, including exercise training and medication management, can benefit from the system's advanced features to improve heart function and overall health [40]. The IoT sensors check the heart rate and raise the alarm in case of abnormalities, allowing physicians to intervene early and prevent complications. Additionally, a busy executive who implemented time management strategies and regular exercise to improve mood and reduce stress can benefit from HealthDote's stress module, which monitors the user's mental state and provides suggestions if stress levels increase. If the stress levels go beyond the normal range frequently, HealthDote has a mechanism to send messages to the patient's family members.

While the existing systems offer promising solutions to various healthcare data-sharing challenges, further research and development are needed to address the healthcare industry's scalability, interoperability, and adoption challenges.

3. Proposed architecture

The architecture of HealthDote is based on five layers (Fig. 1) - The data Layer, Network Layer, Consensus Layer, Incentive Layer, and Application Layer, as stated in [4]. The Network, Consensus, and Incentive layers of CareBlocks are incorporated from Healthdote, but the following modifications and additions have been incorporated in the Data and Application layers in the upgraded version of CareBlocks. The key symbols and definitions are shown in Table 1.

3.1. Data layer

The data layer constitutes all the transactions that the various users of HealthDote have undertaken. The health records are encrypted and then hashed before storing them on the ledger in order to maintain their confidentiality as stated in [4,5]. All six blockchains operate by initializing the transactions in the data layer, as given below.

3.1.1. UserChain

The UserChain is inspired by the PatientChain of CareBlocks. The PatientChain constitutes the transaction tx_{IoT}, which is deployed to store the users' health data that is now being accessed by the MonitoringChain instead of the DoctorChain as specified in [4]. The second transaction of the PatientChain is tx_{key}, which is incorporated from CareBlocks. The IoT transaction is done at a regular interval of 2 transactions per second. It includes information regarding the heartbeat rate, ECG, blood pressure, fall detection, calories burnt, number of steps walked, oxygen levels, stress levels, etc.

Table 1
The key symbols and definition.

Symbol	Definition
ID_{ui}	User's identity key
ts_3	Transaction's current timestamp
$HEMData$	Hash of analysis data
S_i	User signed signature with private key sk_{U_i}
Ik_i	Key for encrypting IoT data
$htxI_i$	Transaction hash of all other parts (Merkle tree's left node)
ID_{C_j}	Pharmacist's Identity key
sk_{C_j}	Private key of pharmacist
ts_4	Timestamp of the transaction
$htxP_i$	Hash of the prescription
$HEpm$	Hash of encrypted prescription
S_j	Signature of Pharmacist
$htxp_j$	Hash of all other part
ID_{F_j}	Insurance authority's identity key
sk_{F_j}	Private key of insurance person
ts_5	Timestamp of the transaction
$htxI_i$	Hash of insurance documents
$HEfm$	Hash of encrypted fund
S_j	Signature of insurance authority
$htxf_j$	Hash of all other parts of transaction
ID_{E_j}	Store employee's Identity key
sk_{F_j}	Private key of Employee
ts_6	Timestamp of the transaction
$htxI_i$	Hash of updates in stock
$HESCMData$	Hash of encrypted updates in stock
S_j	Signature of store employee
$htxe_j$	Hash of all other parts of transaction

3.1.2. MonitoringChain

This blockchain stores the results of the analysis performed on the records of the UserChain. The frequency of generating a monitoring transaction is once every five minutes and every 24 h as shown in (1). Data collected is monitored every 5 min for records corresponding to sensitive heart and respiratory-related disorders. MonitoringChain is also equipped with an alarm feature to indicate an emergency, which is inspired by the features stated in [25]. The server hosts a bunch of eight algorithms for processing this data and analyzing it to produce deducible results.

- The heart rate data for the given time interval is input to the algorithm HEARTBEAT and is analyzed for values that fall above or below the specified range. The records are scanned by the algorithm for deviations from the normal range. If the deviation is more than 30 beats per minute, either positive or negative, it indicates an emergency requiring immediate medical help. Thus the flag is set to 1, and the emergency notifications are sent to the family and authorized doctors of the patient. At the same time, a deviation of 20 beats per second indicates that the patient is undergoing extensive exercise or under stress. This condition can result in either of the two possibilities.
    1. If the circumstances or surroundings of the patient change, then the heart rate may start approaching the normal range with continuously decreasing deviation.
    2. The heartbeat rate might increase further, indicating an emergency. Since the severity of the issue is not confirmed, the flag is set to 2 in both the above-stated cases and only the patient's family members are alarmed by the possibility of an emergency.

- The ECG data is input into the ECG algorithm. It studies the rhythm of the heart in order to predict diseases including Arrhythmia, cardiomyopathy, heart attacks, and coronary heart diseases. In case of abnormalities, the flag is set to 1 or two depending on the deviation of ECG values from the normal range.

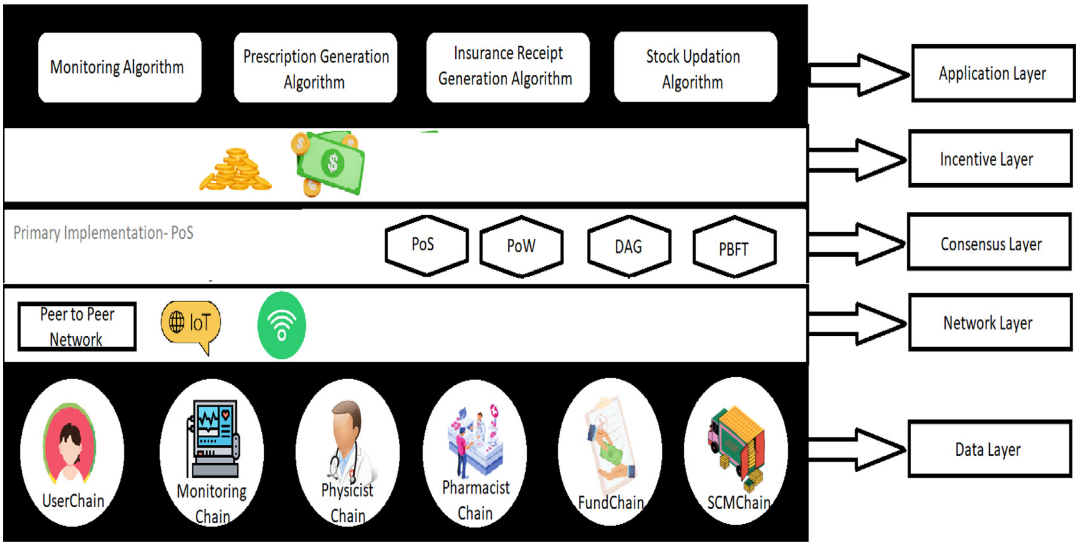

Fig. 1. Architecture of HealthDote.

- The Blood Oxygen Levels are input to the algorithm titled BLOOD. The healthy range is from 95 to 100%. The flag is set to 2 if the levels start falling below 90%, and it is set to 1 if the levels fall below 80%.
- In case of fall detection, the flag is set to 1 indicating an emergency situation. The above-stated algorithms namely HEARTBEAT, ECG, and BLOOD are executed every 5 min, and the results are stored on the MonitoringChain. Apart from these, the algorithms namely SLEEP, STRESS, CALORIE, and STEPS are used for analysis once a day. The user gets updates based on these results on a daily basis. It can be further used for monthly and weekly analysis as well. The flag for all of them is set to 3 in case of deviation of results as compared to the range of healthy body.
- The number of hours slept and quality of sleep in a day are input to the SLEEP algorithm, which outputs the recurrent trends and patterns. This analysis can be helpful for the user in the long term. Data is recorded with the help of accelerometers present in smartwatches.
- The heart rate variability is used to measure stress. This data is input to the algorithm titled STRESS, which analyzes the number of stress hours and stress magnitude. Depending on these two factors, the algorithm suggests avoiding stress and numerous methods that might help in avoiding it.
- The number of calories burnt in a day is calculated by the CALORIE algorithm. Depending on the range, it suggests if the user should rest or exercise more.
- The number of steps traveled is fed as input to the STEPS algorithm, which provides a trigger for incrementing the corresponding number of calories burnt, and in case the steps covered are too less, it suggests the users walk more in order to increase the body movements.

$$tx_{monitoring} = \{ID_{ui}, ts_3, HEMData, S_i, htxI_i\} \tag{1}$$

where,

$$S_i = Sign(sk_{ui}, H(ID_{U_i}, ts_3, HEMData)) \tag{2}$$

$$htxp_i = H(ID_{U_i}, ts_3, HEMData, S_i) \tag{3}$$

3.1.3. PhysicianChain

This chain is based on DoctorChain as specified in [4]. The Physician accesses the data of the MonitoringChain in order to give the diagnosis. This diagnosis is stored as txdiag of [4].

3.1.4. PharmacistChain

The PharmacistChain is the ledger that stores all the prescriptions. The pharmacist generates the records, and then these are encrypted using the private key of the pharmacist as cited in [41,42]. He generates the prescription after viewing the diagnosis given by the doctor. The record which consists of the prescription is hashed along with the timestamp, and Pharmacist ID. This hashed value is encrypted and stored at the IPFS node. The UserChain eventually interacts with the ChemistChain, and a certain amount of DoteCoins, depending upon the fees, is transferred from the user to the concerned pharmacist.

$$tx_{pres} = \{ID_{Cj}, ts_4, htxP_i, HEpm, S_j, htxp_j\} \tag{4}$$

where,

$$S_j = Sign(sk_{Cj}, H(ID_{Cj}, ts_4, htxI_i, HEpm)) \tag{5}$$

$$htxp_j = H(ID_{Cj}, ts_4, htxI_i, HEpm, S_j) \tag{6}$$

3.1.5. FundChain

The FundChain is used to store the insurance papers that the various insurance agencies produce. The user can authorize multiple insurance agencies to access the prescription produced by the pharmacist and grant the DoteCoins to the concerned doctor. The documents produced by the insurance agencies are encrypted using the private key of the concerned insurance authority. The insurance documents, Identification number of the insurance authority, and timestamp are hashed as a group and stored at the IPFS node.

$$tx_{ins} = \{ID_{Fj}, ts_5, htxI_i, HEfm, S_j, htxf_j\} \tag{7}$$

where,

$$S_i = Sign(sk_{Fj}, H(ID_{Fj}, ts_5, htxI_i, HEfm)) \tag{8}$$

$$htxf_j = H(ID_{Fj}, ts_5, htxI_i, HEfm, S_j) \tag{9}$$

3.1.6. SCMChain

The hospital authorities update the stock based on the prescription in the PharmacistChain. This is done with the help of txSCM transaction as described in (2). The hospital authorities deduct those supplies present in the prescription from the database of hospital by accessing the data stored in the PrescriptionChain. The quantity of all the items is checked once this transaction is done. If it is less than five, an alarm is raised to refill the particular stock.

$$tx_{ins} = \{ID_{Ej}, ts_5, htxI_i, HESCMData, S_j, htxe_j\} \tag{10}$$

where,

$$S_i = Sign(sk_{Ej}, H(ID_{Fj}, ts_6, htxI_i, HESCMData)) \tag{11}$$

$$htxf_j = H(ID_{Ej}, ts_5, htxI_i, HESCMData, S_j) \tag{12}$$

3.2. Application layer

The application layer is the interface between HealthDote and its users. There are six types of users in this system and there is a unique algorithm for each category to help them interact with the system. Since each algorithm is associated with a specific blockchain, these are described as follows:

- UserChain: The Patients interact with the system using the Health Record data Security algorithm specified in [4].
- MonitoringChain: The MonitoringChain follows the algorithm 1 for monitoring and analysis of user data. It accesses the data from UserChain and stores the corresponding analysis at IPFS.
- PhysicianChain: The Doctor accesses the Records from the MonitoringChain and stores the corresponding diagnosis in the PhysicianChain. This is done using the Disease Cure Algorithm of [4].
- The PharmacistChain is the ledger that stores all the prescriptions. The pharmacist generates the records, and then these are encrypted using the private key of the Chemist.
- The Chemist generates the prescription after viewing the diagnosis given by the doctor. The record containing the prescription is then hashed along with the timestamp, and Chemist ID, and the hashed value is encrypted and stored at the IPFS node. This provides a two-layer protection for health records as described in [43, 44]. The user eventually interacts with the PharmacistChain, and a certain amount of DoteCoins, depending upon the fees, is transferred from the user to the concerned pharmacist. The algorithm for PharmacistChain is described in Algorithm 2.

Algorithm 1 Monitoring

```
Input: User key $U_i$, IoT key $Ik_i$ and users health record data $htx$
Output: Transaction $tx_{monitoring}$
foreach record collected in last 5 minutes do
    $D_e( MData_i)$=Decrypt($EMData$,$Ik_i$)
    Decrypt the Health records stored at IPFS
    Execute HEARTBEAT algorithm → $D_1$, flag $f_1$
    Execute ECG algorithm→ $D_2$, flag $f_2$
    Execute BLOOD algorithm → $D_3$, flag $f_3$
    Execute SLEEP algorithm→ $D_5$, flag $f_5$
    Execute STRESS algorithm→ $D_6$, flag $f_6$
    Execute CALORIE algorithm → $D_7$, flag $f_7$
    Execute STEPS algorithm→ $D_8$, flag $f_8$
end
foreach flags 1 to 9 do
    if $flag == 1$ then
        Alarm
        Notify Doctor
        Notify Family Members
        Declare emergency situation
    end
    else if $flag == 2$ then
        Notify Family Member
        Declare possibility of emergency situation
    end
    else if $flag == 3$ then
        Notify user
        Provide insights and suggestions to the user
    end
end
```

- The FundChain stores the insurance papers that the various insurance agencies produce. The user can authorize multiple insurance agencies to access the prescription produced by the chemist and grant the PlusCoins to the concerned doctor. The documents produced by the insurance agencies are encrypted using the private key of the concerned insurance authority. The transaction consisting of the insurance documents, Identification number of the insurance authority, and timestamp are hashed data before storing it at the IPFS node. This is shown in Algorithm 3.

Algorithm 2 Prescription Generation

```
Input: Identity of diagnosis: chemist $C_j$, prescription $pres$ and
       prescription key $presK_{ij}$
Output: Transaction $tx_{pres}$
Encrypted prescription $Edm_j = Enc(presK_{ij}, pres)$;
Send $Edm_j$ at data storing IPFS node and generate $HEpm_j$;
Create Current timestamp $ts_4$;
Add signature to the prescription
$S_j = Sign(sk_{C_j}, H(ID_{C_j}, ts_4, htxI_i, HEpm))$;
Set $htxp_j = H(ID_{C_j}, ts_4, htxI_i, HEpm, S_j)$;
Set $tx_{pres} = \{ID_{C_j}, ts_4, htxP_i, HEpm, S_j, htxp_j\}$;
return $tx_{pres}$;
```

Algorithm 3 Insurance Receipt Generation

```
Input: Identification code of prescription $htxP_i$, insurance authority
       $ID_{F_j}$, fund $F_j$, prescription $pres$, and insurance key $fk_{ij}$;
Output: Transaction $tx_{ins}$;
Encrypted insurance papers $EFm_j = Enc(IP_j, ins)$;
Send $Efm_j$ to the IPFS storage node and get $HEfm_j$;
Generate current timestamp $ts_5$;
Add Signature to the Insurance Receipt;
Set $S_i = Sign(sk_{F_j}, H(ID_{F_j}, ts_5, htxI_i, HEfm))$;
Set $htxf_j = H(ID_{F_j}, ts_5, htxI_i, HEfm, S_j)$;
Set $tx_{ins} = \{ID_{F_j}, ts_5, htxI_i, HEfm, S_j, htxf_j\}$;
return $tx_{ins}$;
```

- The SCMChain is used to store the updations in the hospital inventory. Once the Pharmacist generates the prescription, the user gets the prescribed supplies from the hospital, and the concerned authorities update the inventory by deducting these supplies from the pertaining stock (Algorithm 4). It also checks for the quantity of the supplies falling below the limit of 5 and raises the alarm if it does so.

Algorithm 4 Stock Updation

```
Input: Identity of updation $htxU_i$, Employee Identity $ID_{E_j}$, Updation
       status $U_j$, and Updation key $Uk_{ij}$
Output: Transaction $tx_{SCM}$
Encrypted Updation data $ESCMData_j = Enc(IE_j, SCM)$;
Send $Efm_j$ to the IPFS storage node and get $HESCMData_j$;
Generate timestamp $ts_6$;
Set $S_i = Sign(sk_{E_j}, H(ID_{E_j}, ts_6, htxE_i, HESCMData))$;
Set $htxE_j = H(ID_{E_j}, ts_6, htxE_i, HESCMData, S_j)$;
Set $tx_{SCM} = \{ID_{E_j}, ts_6, htxE_i, HESCMData, S_j, htxE_j\}$;
return $tx_{SCM}$;
```

4. Results and discussion

4.1. Comparison of PoW against PoS in HealthDote

Mining new blocks consume much power due to the structure of the Proof of work algorithm. The Proof of work concept was first

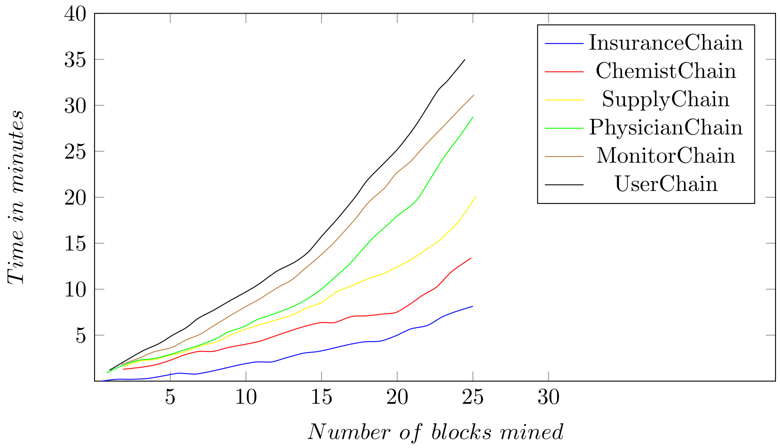

Fig. 2. Number of blocks mined vs Time (PoW).

introduced in 1993 to combat spam emails. Later, Satoshi Nakamoto incorporated Bitcoin in 1999 as this method could be used to reach a consensus between many nodes on a network. It was further used to enhance the security of the bitcoin blockchain. Nevertheless, this method requires all nodes to calculate the nonce value, which is a cryptographic puzzle. The first miner to calculate the correct value is rewarded. However, this has resulted in the development of enormous mining farms, which consume a considerable amount of the total electricity produced globally.

Moreover, the Proof of Work scheme is more biased towards the miners possessing better equipment; the higher the hash weight, the more the chances of mining the next block onto the blockchain. In other cases, the miners can form mining pools to combine their hashing powers and thereby distribute the awards evenly among themselves and navigate the blockchain towards its centralized behavior instead of the decentralized form. Fig. 2 shows the throughput in terms of the number of blocks mined vs. time for all the six blockchains in the case of PoW.

The disadvantages of the Proof of Work(PoW) are :

- Consumption of large units of electricity
- Encouraging the formation of mining pools.

To solve these issues, Proof of Stake(PoS) was introduced. In this ideology, the validator is chosen by election randomly instead of the miners competing against each other for mining a block onto the blockchain. In PoS, the validator has to invest a certain amount of money into the network as a Stake which is considered a security deposit in the real-world scenario. The deposit size determines the chances of the validator being elected for mining the next block. It is a linear correlation, as shown in Fig. 3 for all the blockchains. It turns out to be perfectly linear in ideal conditions as the probability of selecting a validator is directly proportional to the stakes he has invested in the network. Here, the UserChain requires more time in mining as the volume and the number of transactions, both, are more significant when compared to the rest of the blockchains. This Chain is followed by the MonitoringChain and then the rest of the chains—PhysicianChain, PharmacistChain, FundChain, and SCMChain as they require only one transaction per file.

The throughput of the Proof of work algorithm decreases considerably as the network size increases due to frequent collisions of the blocks being mined by different nodes at the same instance of time. Still, the Proof of Stake overcomes this problem with no simultaneous mining. Instead of the mining concept, the validators are elected to add blocks to the blockchain.

Assuming that the same nodes are used for both PoW and PoS consensus algorithms, the computational requirements of PoW would lead to a steady increase in the energy needed to validate each transaction as more transactions are added to the blockchain. This would result in a curve that increases roughly linearly over time. As the computational requirements continue to grow, the cost per transaction may become prohibitively high, making the blockchain less practical. On the other hand, PoS algorithms generally require less computational power and can validate transactions more efficiently. This would result in a curve that increases slowly over time, leveling off as the network becomes more established and efficient. As a result, PoS can support a more significant number of transactions with a lower overall cost per transaction.

It is important to note that this is a hypothetical scenario, and the actual behavior of PoW and PoS would depend on many factors, including the specific implementation details of each algorithm and the particular characteristics of the network being used. Table 2 shows the differences between PoW and PoS.

4.2. Pros of incorporating directed acyclic graph (DAG) in HealthDote

DAG (Directed Acyclic Graph) is a consensus algorithm used in blockchain platforms such as IOTA and Nano. Unlike PoS and PoW, DAG does not rely on miners to validate transactions. Instead, each user verifies two previous transactions before adding their own transaction to the network. The result is a graph-like structure of transactions that users rather than miners verify. The main advantage of DAG is that it can process transactions in parallel, which makes it faster than PoS and PoW. However, DAG can also suffer from scalability issues, and its security depends on the assumption that most users are honest.

The rules of DAG consensus algorithms are based on a directed acyclic graph (DAG), a data structure used to represent a set of transactions in a distributed ledger. In a DAG-based consensus algorithm, the rules for adding transactions to the ledger are as follows:

- **Validity**: Before a transaction can be added to the ledger, it must be validated to ensure it meets specific criteria. This may include checking that the transaction is appropriately formatted, that the appropriate parties sign it, and that it does not conflict with any other transactions in the ledger.
- **Ordering**: Once a transaction has been validated, it must be placed in a specific order relative to other transactions in the ledger. This is typically done by linking each transaction to one or more previous transactions in the DAG. The order of transactions in the DAG is crucial because it determines the ledger's state at any given point in time.
- **Consensus**: For the DAG to be used as a distributed ledger, all nodes in the network must agree on the order of transactions in the DAG. This is achieved through a consensus algorithm, which allows nodes to reach a shared agreement about the ledger's state.

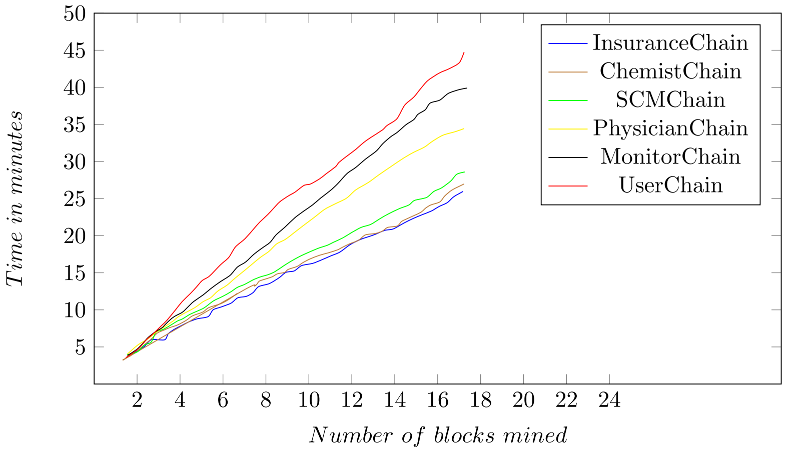

Fig. 3. Number of blocks mined vs Time (PoS).

Table 2
Comparison of PoW and PoS.

Factor	Proof of Work (PoW)	Proof of Stake (PoS)
Consensus mechanism	Nodes compete to solve complex mathematical problems to validate transactions and earn rewards	Nodes are chosen to validate transactions based on the amount of cryptocurrency they “stake” or hold
Energy consumption	High energy consumption due to the need for powerful computing equipment to solve mathematical problems	Low energy consumption since no complex mathematical problems need to be solved
Security	High security due to the difficulty and cost of performing a 51% attack	Security relies on the economic incentives of node operators and the cost of acquiring enough cryptocurrency to perform a 51% attack
Decentralization	High degree of decentralization due to the distributed nature of mining	Decentralization can be affected by the concentration of cryptocurrency ownership among a small number of users
Scalability	Limited scalability due to the high computational requirements of mining	Potentially higher scalability due to the low energy consumption and less complex consensus mechanism
Block time	Long block time, typically around 10 min	Shorter block time, typically a few seconds to a few minutes
Block rewards	Block rewards decrease over time as the cryptocurrency’s total supply approaches its maximum limit	Block rewards remain relatively constant, with transaction fees & becomes more important over time
Inflation	Inflationary, with a constant creation of new coins to reward miners	Can be either inflationary or deflationary depending on the design of the cryptocurrency
Forks	Hard forks can occur due to differences in consensus rules	Soft forks are more common since there is less disagreement on the rules
Environmental impact	High environmental impact due to the large amount of energy consumption	Low environmental impact due to the reduced energy consumption
Implementation difficulty	High implementation difficulty due to the complexity of mining	Lower implementation difficulty since there is no mining required
Governance	Less formal governance structures since the mining community determines the direction of the network	More formal governance structures, with node operators and cryptocurrency holders playing a larger role in decision-making
Adoption	Widely adopted and used by most cryptocurrencies, such as Bitcoin and Ethereum	Increasing in popularity, but not yet widely adopted by major cryptocurrencies
Examples	Bitcoin, Ethereum	Cardano, Polkadot

Consensus algorithms may be based on voting, proof-of-work, or other mechanisms.

- **Conflict resolution**: Because transactions in the DAG are linked to one another, there is a possibility of conflicts arising when two transactions try to update the same data simultaneously. DAG-based consensus algorithms must have mechanisms in place to resolve disputes and ensure that the ledger remains consistent across all nodes in the network.

These rules are designed to ensure that transactions are adequately validated, ordered, and agreed upon by all nodes in a distributed network. This allows the DAG to function as a secure and reliable ledger for storing and managing digital assets.

The asymptotic behavior of consensus algorithms depends on various factors, such as the number of nodes in the network, the amount of cryptocurrency held by users, and the computational power of miners. DAG is generally expected to scale better than PoS and PoW, but its

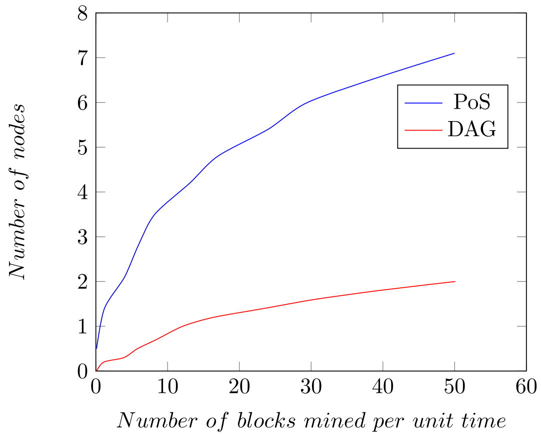

Fig. 4. Number of blocked mined per unit time vs Number of nodes used for mining in case of PoS and DAG.

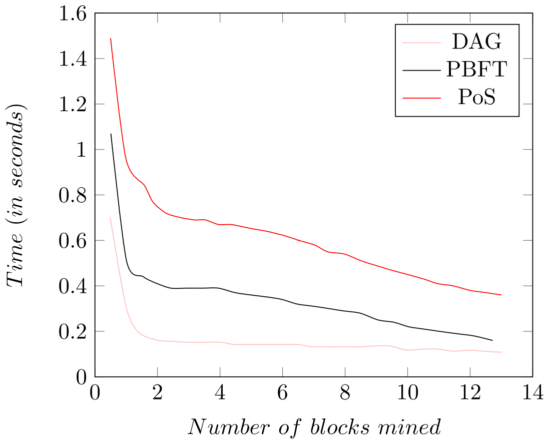

Fig. 5. Number of blocked mined per unit time using PoS, PBFT and DAG.

security is more challenging to analyze. PoS is expected to be more energy-efficient than PoW, but it may suffer from centralization if a small group of users holds a large amount of cryptocurrency. PoW is a proven and secure method of validating transactions, but it is very energy-intensive and may also suffer from centralization.

With the advent of time, the number of transactions that are supposed to be recorded on the blockchain increased abruptly. This gives rise to the urgent need to improve the processing rate, overcome by using DAG. It is a consensus algorithm that overcomes the downside of the slow speed of PoW and PoS. This is made possible because the DAG facilitates a parallel validation process, resulting in improved throughput. Tangle is the first DAG-based blockchain. It is a data structure that makes use of topological ordering. As opposed to PoW and PoS, there is no competition between the peers in the DAG algorithm. The speed of mining blocks or, in other words, for confirming a transaction in ascending order for these consensus algorithms is — PoW, PoS, and DAG.

The confirmation rate and Transaction Per Second (TPS) are much higher in DAG than PoW and PoS when the new transaction arrival rate is fast. The significant advantages of using DAG as the consensus algorithm are:

- Instantaneous transaction processing
- Faster growth of blockchain
- Zero transaction fees
- More scalable
- Elimination of double spending
- Efficient for smaller transactions
- Lightweight i.e., less bulky chain as the transaction is added to a node of a graph instead of the typical propagating blockchain

Since HealthDote uses the IPFS to store fixed-sized transactions, i.e., 64-bit hash, the DAG is a comparatively more efficient consensus algorithm than PoS. As DAG is used to store only one specific transaction in a particular block, using this data structure as the structural foundation can make the entire CareBlocks' operational speed boost up. This is shown in Fig. 4.

4.3. Comparison of PBFT against PoS and DAG

Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm used in distributed systems to ensure that all nodes agree on a particular state. It was developed in 1999 by Miguel Castro and Barbara Liskov and is designed to tolerate up to one-third of the nodes in the network behaving maliciously.

In PBFT, a leader is elected to propose a new block of transactions to the network. The other nodes in the network then vote on the proposed block, and if two-thirds of the nodes agree, the block is added to the blockchain. If the leader is faulty, the other nodes can detect this and replace the leader with a backup node. PBFT is designed for high-performance systems and can achieve consensus quickly, even in large networks. However, it requires more communication between nodes than other consensus algorithms, making it less efficient in networks with high latency. It also requires a trusted set-up, where all nodes in the network must be pre-determined and known to each other. Additionally, it assumes that up to one-third of the nodes in the network are malicious, which may not always be the case in practice. Overall, PBFT is a robust consensus algorithm well-suited for high-performance systems where a trusted setup is possible and the number of malicious nodes in the network is relatively small.

The PBFT consensus algorithm has high performance compared to traditional consensus mechanisms like PoW and PoS. The algorithm's robustness makes it stand apart from the previously discussed algorithms. Fig. 5 shows its implementation, where the number of blocks mined per unit of time is used as a parameter to compare the three consensus algorithms — PoS, PBFT, and DAG.

Though the PBFT algorithm outperforms the PoS and PoW algorithms, comparatively, it is still slower than DAG. Nevertheless, PBFT is often chosen favorably over DAG because it assures a significant percentage of trustworthy records in the network, unlike DAG, where a malicious node can add false transactions onto the network.

The four consensus algorithms — DAG (Directed Acyclic Graph), PoS (Proof of Stake), PoW (Proof of Work) and PBFT(Practical Byzantine Fault Tolerance) are compared against each other based on several factors in Table 3.

4.4. File size vs no of transactions

The records pertaining to all six blockchains are stored in encrypted format at the IPFS. Each record stored contains the following 4 entries:

1. Mining node id
2. Hash of the transaction
3. Hash of the previous transaction
4. Timestamp

HealthDote consists of a fixed set of nodes capable of mining the blocks onto the blockchain. Each one is uniquely identified using an identification number called the node id. Transaction consisting of the sender's address, recipient's address, and number of DoteCoins transferred is encrypted using the SHA 256 Algorithm, and the hash of all these fields is stored in the blockchain. A Hash of the previous transaction is required to link the blocks in chronological order. The timestamp is used to resolve conflicts in consensus algorithms and for bookkeeping purposes.

Table 3
Comparison of PoW, PoS, PoW and PBFT.

Factors	DAG	PoS	PoW	PBFT
Network scalability	High	High	Low	High
Security	Medium	High	High	High
Decentralization	High	High	Low/Medium	Low
Energy efficiency	High	High	Low	Low
Transaction speed	Medium/High	High	Low/Medium	Medium/High
Forking probability	Low	Low	High	Low
Consensus mechanism	Asynchronous	Synchronous	Synchronous	Synchronous
Finality	Probabilistic	Deterministic	Probabilistic	Deterministic
Fault tolerance	Low/Medium	High	High	High
Nodes required for consensus	Less	Many	Many	Many

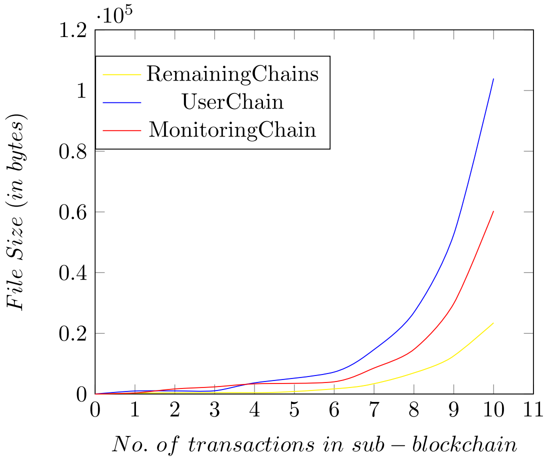

Fig. 6. Number of transactions in various blockchains of HealthDote vs File Size.

Fig. 6 shows the variation in file size storing the various blockchains at the IPFS against the number of transactions. Initially, the file is observed to be 0 bytes for all six blockchains without any data. After inserting the header, i.e., the titles for all four columns, the file size increases to 35 bytes. Each record in the file is of fixed size, i.e., 158 bytes. Hence the relationship between file size at IPFS and the number of transactions is linear. The UserChain has the most significant file size of all because, for every 0.5 s, a new IoT transaction is generated by the user. All the transactions for one minute are clubbed together into one file and stored at the IPFS in an encrypted format. Thus while mining a block for this chain, the file size is 18960+35 bytes. The next bulkier file size is of the MonitoringChain as it consists of 5.00347 records every 5 min. The remaining chains have a file size of 158 bytes with a 35-byte header.

The following are some advantages of HealthDote:

- Decentralized access control: HealthDote uses a decentralized access control mechanism that allows patients to control who has access to their health data. This can improve patient privacy and security while ensuring patients have more control over their health information. The need for a centralized server to manage access control is eliminated, allowing for greater scalability and improved efficiency.
- Health Data Integration: HealthDote offers integration with various healthcare data sources, including Electronic Health Records (EHRs), Personal Health Records (PHRs), and wearables. This gives a more comprehensive and accurate view of a patient's health status.
- Incentive-Based Model: HealthDote offers an incentive-based model that rewards patients for sharing their health data. This incentivizes patients to engage with the system and improve their health outcomes.
- AI-Enabled Analytics: HealthDote leverages AI-enabled analytics to identify health trends and patterns in patient data. This can help healthcare.
- Providers make better-informed decisions. This can improve the accuracy of diagnoses and treatment plans.
- Data integrity: Using blockchain technology in HealthDote helps ensure the integrity of health data. Each transaction is recorded on a distributed ledger, which cannot be altered without consensus from the network. This helps prevent data tampering, a problem in traditional healthcare systems.
- Cost savings: HealthDote can help reduce costs associated with traditional healthcare systems, such as administrative costs and duplicative testing. By reducing the need for intermediaries and improving coordination between healthcare providers, HealthDote can lower overall healthcare costs.
- Increased access to care: HealthDote can improve access to care for patients in remote or underserved areas. Real-time monitoring and AI-enabled analytics can help healthcare providers remotely monitor and diagnose patients, reducing the need for in-person visits.
- Improved clinical trials: HealthDote can be used to improve the efficiency and transparency of clinical trials. Blockchain technology can help streamline the data collection and analysis process, reducing administrative burdens and ensuring the accuracy of results.
- Secure communication: HealthDOte can facilitate secure communication between healthcare providers, patients, and other stakeholders. The decentralized access control mechanism ensures that only authorized parties can access health data, reducing the risk of data breaches and improving overall security.

The potential disadvantages include limited adoption, complexity, high energy consumption, regulatory challenges, lack of standardization, scalability issues, limited functionality, dependence on third-party vendors, and legal and ethical concerns. As a new technology, blockchain is still being adopted, and healthcare professionals must become more familiar with the technology to use it effectively. Moreover, regulatory compliance and data standardization could also pose challenges to the adoption of blockchain technology in healthcare. As such, healthcare organizations must carefully evaluate the potential benefits and risks before using blockchain technology in healthcare.

5. Conclusion and future work

In this paper, we proposed a blockchain-based model, HealthDote, to deal with enormously vast amounts of health data stored on the six blockchains. These blockchains are used to ensure that users' health data, monitoring data, doctors' diagnoses, chemists' prescriptions, insurance documents, and SupplyChain Data are not modified and accessed by unauthorized authorities in order to avoid medical disputes in the future. The encrypted data is decoupled, and the corresponding keys are used to achieve flexible key management. The patients are eligible to revoke any of the doctors at a given instant by generating a new set of keys for the rest of the authorized doctors. The decentralized nature of blockchain technology makes it possible to access health records and data stored on the sub-blockchains by the authorized authority. This model can be used to monitor diseases and the patient's report in case of outbreaks and in real-time. We aim to extend the model by creating and linking additional Machine Learning algorithms for disease diagnosis. The algorithm will read the user records from the UserChain and predict the disease to the concerned doctor, thereby enhancing the healthcare system in case of a disease outbreak. The doctor can review the efficiency of the algorithm in order to train the model to give better results in the future. In future, an additional database can help in supporting the blockchain architecture to store enormous amounts of data. Numerous types of databases can serve the demand, including IPFS and BIGchain.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] R. Zhou, Z. Lin, A privacy protection scheme for permissioned blockchain based on trusted execution environment, in: International Conference on Blockchain Technology and Information Security, ICBCTIS, 2022, pp. 1–4.

[2] N. Saxena, D.S. Chakravarthi, A.N. Venkatesh, N. Soni, S. Kant, The future of blockchain technology and the internet of things in healthcare, in: International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems, ICSES, 2022, pp. 1–9.

[3] T. Lavigne, B. Mbarek, T. Pitner, A real time healthcare tracking system based on blockchain application, in: IEEE/ACS 18th International Conference on Computer Systems and Applications, AICCSA, 2021, pp. 1–8.

[4] Sireejaa Uppal, Bindiya Kansekar, Prajwalita, S. Mini, Deepak Tosh, CareBlocks: A blockchain-based health information sharing framework for medical IoT, in: International Conference on Signal Processing and Integrated Networks, SPIN, 2021.

[5] U. Demirbaga, G.S. Aujla, MapChain: A blockchain-based verifiable healthcare service management in IoT-based big data ecosystem, IEEE Trans. Netw. Serv. Manag. (2022).

[6] P.P. Ray, D. Dash, K. Salah, N. Kumar, Blockchain for IoT-based healthcare: Background, consensus, platforms, and use cases, IEEE Syst. J. 15 (1) (2021) 85–94.

[7] J. Zhang, Y. Yang, X. Liu, J. Ma, An efficient blockchain-based hierarchical data sharing for healthcare internet of things, IEEE Trans. Ind. Inform. 18 (10) (2022) 7139–7150.

[8] C. Liu, et al., Blockchain technology in healthcare: A scientific and technological driving force, in: 34th International Symposium on Computer-Based Medical Systems, CBMS, 2021, pp. 550–555.

[9] P. Banerjee, S. Bilgaiyan, A. Tikmani, Application of blockchain technology in healthcare: An analysis, in: International Conference on Computing, Communication and Power Technology, IC3P, 2022, pp. 254–259.

[10] A. Sinha, A. Patel, M. Jagdish, Application of blockchain in healthcare, in: First International Conference on Artificial Intelligence Trends and Pattern Recognition, ICAITPR, 2022, pp. 1–4.

[11] M.N. Bhuiyan, M.M. Rahman, M.M. Billah, D. Saha, Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities, IEEE Internet Things J. 8 (13) (2021) 10474–10498.

[12] J. Zhou, G. Feng, Y. Wang, Optimal deployment mechanism of blockchain in resource-constrained IoT systems, IEEE Internet Things J. 9 (11) (2022) 8168–8177.

[13] M. Haghi, et al., A flexible and pervasive IoT-based healthcare platform for physiological and environmental parameters monitoring, IEEE Internet Things J. 7 (6) (2020) 5628–5647.

[14] Ayesha Shahnaz, Usman Qamar, Ayesha Khalid, Using blockchain for electronic health records, IEEE Access 7 (2019) 147782–147795.

[15] S. Namasudra, P. Sharma, R.G. Crespo, V. Shanmuganathan, Blockchain-based medical certificate generation and verification for IoT-based healthcare systems, IEEE Consum. Electron. Mag. (2022).

[16] J.A. Alzubi, O.A. Alzubi, A. Singh, M. Ramachandran, Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning, IEEE Trans. Ind. Inform. 19 (1) (2023) 1080–1087.

[17] R. Schoenberg, C. Safran, Internet-based repository of medical records that retains patient confidentiality, Br. Med. J. 321 (7270) (2000) 1199–1203.

[18] S.N.G. Gourisetti, M. Mylrea, H. Patangia, Evaluation and demonstration of blockchain applicability framework, IEEE Trans. Eng. Manage. 67 (4) (2020) 1142–1156.

[19] S. Chauhan, H.K. Singh Tanwar, Application of blockchain technology in healthcare: A systematic review, in: 2022 International Conference on Applied Artificial Intelligence and Computing, ICAAIC, 2022, pp. 1–5.

[20] D.M. Rind, I.S. Kohane, P. Szolovits, C. Safran, H.C. Chueh, G.O. Barnett, Maintaining the confidentiality of medical records shared over the internet and the world wide web, Ann. Internal Med. 127 (2) (1997) 138–141.

[21] X. Li, Z. Ma, S. Luo, Blockchain-oriented privacy protection with online and offline verification in cross-chain system, in: International Conference on Blockchain Technology and Information Security, ICBCTIS, 2022, pp. 177–181.

[22] K.O.-B.O. Agyekum, Q. Xia, E.B. Sifah, C.N.A. Cobblah, H. Xia, J. Gao, A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain, IEEE Syst. J. 16 (1) (2022) 1685–1696.

[23] Shuang Sun, Rong Du, Shudong Chen, Weiwei Li, Blockchain-based IoT access control system: Towards security, lightweight, and cross-domain, IEEE Access 9 (2021) 36868–36878.

[24] W. Javed, F. Aabid, M. Danish, H. Tahir, R. Zainab, Role of blockchain technology in healthcare: A systematic review, in: International Conference on Innovative Computing, ICIC, 2021, pp. 1–8.

[25] R.W. Grant, J.S. Wald, E.G. Poon, J.L. Schnipper, T.K. Gandhi, L.A. Volk, B. Middleton, Design and implementation of a web-based patient portal linked to an ambulatory care electronic health record: Patient gateway for diabetes collaborative care, Diabetes Technol. Ther. 8 (5) (2006) 576–586.

[26] W. Song, et al., Blockchain data analysis from the perspective of complex networks: Overview, Tsinghua Sci. Technol. 28 (1) (2023) 176–206.

[27] A.N. Gohar, S.A. Abdelmawgoud, M.S. Farhan, A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and IoT, IEEE Access 10 (2022) 92137–92157.

[28] D. Li, Q. Guo, D. Bai, W. Zhang, Research and implementation on the operation and transaction system based on blockchain technology for virtual power plant, in: International Conference on Blockchain Technology and Information Security, ICBCTIS, 2022, pp. 165–170.

[29] M. Younis, W. Lalouani, N. Lasla, L. Emokpae, M. Abdallah, Blockchain-enabled and data-driven smart healthcare solution for secure and privacy-preserving data access, IEEE Syst. J. 16 (3) (2022) 3746–3757.

[30] Y. Zhao, et al., Correction to privacy-preserving blockchain-based federated learning for IoT devices, IEEE Internet Things J. 10 (1) (2023) 973.

[31] S. Banaeian Far, A. Imani Rad, PP-DENT: A privacy-preserving framework for blockchain-based mobile/roaming transactions, IEEE Netw. Lett. 4 (4) (2022) 204–207.

[32] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, E. Hossain, A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes, IEEE Access 8 (2020) 118433–118471.

[33] Zaer Abo-Hammour, Omar Abu Arqub, Shaher Momani, Nabil Shawagfeh, Optimization solution of troesch's and bratu's problems of ordinary type using novel continuous genetic algorithm, Discrete Dyn. Nat. Soc. 6 (2014) 401656–401696.

[34] Omar Abu Arqub, Zaer Abo-Hammour, Shaher Momani, Nabil Shawagfeh, Solving singular two-point boundary value problems using continuous genetic algorithm, Abstr. Appl. Anal. 12 (2012) 205391–205429.

[35] Omar Abu Arqub, Zaer Abo-Hammour, Numerical solution of systems of second-order boundary value problems using continuous genetic algorithm, Inform. Sci. 279 (2014) 396–415.

[36] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F.-Y. Wang, Blockchain-enabled smart contracts: Architecture, applications, and future trends, IEEE Trans. Syst. Man Cybern. Syst. 49 (11) (2019) 2266–2277.

[37] C.K. Da Silva Rodrigues, V. Rocha, Towards blockchain for suitable efficiency and data integrity of IoT ecosystem transactions, IEEE Lat. Am. Trans. 19 (7) (2021) 1199–1206.

[38] L. Goetz, et al., Deep brain stimulation of the Pedunculopontine Nucleus Area in parkinson disease: MRI-based anatomoclinical correlations and optimal target, Neurosurgery 2 (2019) 506–518.

[39] Repetitive transcranial magnetic stimulation for people with treatment-resistant depression: A health technology assessment, Ont Health Technol. Assess. 4 (2021) 1–232.

[40] S.A. Lear, Ignaszewski, Cardiac rehabilitation: a comprehensive review, Curr. Control Trials Cardiovasc. Med. 2 (2001) 221–232.

[41] D. Gritzalis, C. Lambrinoudakis, A security architecture for interconnecting health information systems, Int. J. Med. Inform. 73 (3) (2004) 305–309.

[42] S. Bonacina, S. Marceglia, M. Bertoldi, F. Pinciroli, A web-based system for family health record, in: 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2007, pp. 3652–3656.

[43] L. Ibraimi, M. Asim, M. Petković, Secure management of personal health records by applying attribute-based encryption, in: Proceedings of the 6th International Workshop on Wearable, Micro, and Nano Technologies for Personalized Health, 2009, pp. 71–74.

[44] Jie Xu, Kaiping Xue, Shaohua Li, Hangyu Tian, Jianan Hong, Peilin Hong, Nenghai Yu, Healthchain: A blockchain-based privacy-preserving scheme for large-scale health data, IEEE Internet Things J. 6 (2019).