Hindawi
Security and Communication Networks
Volume 2021, Article ID 2245808, 16 pages
https://doi.org/10.1155/2021/2245808

Research Article

Blockchain and Business Process Management in Health Care, Especially for COVID-19 Cases

Ibrahim Abunadi[1] **and R. Lakshmana Kumar**[2]

[1]*Department of Information Systems, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia*
[2]*Centre of Excellence for Artificial Intelligence and Machine Learning, Hindusthan College of Engineering and Technology, Coimbatore, India*

Correspondence should be addressed to Ibrahim Abunadi; iabunadi@psu.edu.sa

Received 8 September 2021; Revised 25 September 2021; Accepted 10 October 2021; Published 2 November 2021

Academic Editor: Thippa Reddy G

From this global health disaster, the health profession is searching for a new technology to monitor and mitigate COVID-19 infections. Accurate and reliable data are needed to surveil and prevent the diffusion of the coronavirus. However, there is a lack of consistent data on existing technologies. Various entities—for example, medical labs and public hospitals—could provide data on patients with coronavirus infection. Yet, this information might not be precise since it is not supervised and recorded correctly. This paper proposes a Blockchain and Business Process Management (BBPM) system in healthcare to solve these problems. This system could be crucial in tracing coronavirus diffusion and discovering more dangerous patients and is extremely proficient at controlling the disease. BBPM can be utilized like a digital database that includes information concurrently utilized and distributed inside a wide, decentralized, and openly accessible network. Usage of blockchains in the medical sector is anticipated to revolutionize the industry in many regions, primarily because centralization in current health technologies inhibits information sharing and causes a lack of confidentiality. Furthermore, BBPM could help supervise the diffusion of coronavirus infection worldwide by utilizing blockchain networks on the mobile devices of individuals. Protecting patient information is one of the critical strengths of BBPM. Participating BBPM nodes can be governments, hospitals, testing labs, or patients. In addition, the digital ledger has a few documents, including patient reports, consequences, the condition of treatment, and a summary of discharge. The BBPM system is categorized into four processes. In the first process, the patient is analyzed and diagnosed by a testing lab to detect any early signs of COVID-19 infection. A sample of the patients was taken. If it is positive, the second process begins. In the second process, the patient is isolated and begins treatment for a minimum of 14 days. If the patient's health condition is improving, the third process begins. In the third process, the patients were retested for COVID-19. If the patient sample is negative, the patient is discharged, and an outline is created. During discharge, the patient pays the hospital for treatment. However, if the patient sample is positive, the isolation period is continued for another 14 days. In the last process, the details of total COVID-19 are confirmed, recovered, and death cases are conveyed to the government by the testing labs and hospitals. Patient records are stored for upcoming usage; their confidentiality is maintained when distributed on a larger scale. BBPM can guarantee the security and accuracy of patients' recorded data.

1. Introduction

The whole world is battling a new disease called COVID-19 and its mutations. It was initially discovered in Wuhan, Hubei Province, China [1]. An unprecedented spread of this virus has created many challenges that make the roots of human civilization tremble [2]. Some of the most apparent challenges are described below.

(i) Social exclusion: social exclusion is a method employed to slow the disease spread and "flatten the curve" of new cases with no licensed drugs or vaccines for COVID-19 treatment and prevention. However, most everyday activities, such as medical treatment, transportation, education, banking, and shopping, require physical contact. Apart from this, controlling physical contact can lead to social

isolation and unfavourable psychological consequences.

(ii) False infodemic: the massive flow of fake data does not adhere to government policies, such as harmful self-medication or prophylactic treatments, panic behaviours, depressive disorders and social dissociation, motion restrictions, and restrictions on work and shopping hours. Furthermore, predictive models and evaluations of future claims based on such false data would be meaningless. Unfortunately, current sites and essential technologies cannot cope with this issue, becoming increasingly difficult to resist.

(iii) Continuation of necessary government services: necessary government services, for example, public utilities (sanitation, electricity, water, and so on), salaries and pensions, tax gathering, marriage, birth and death registration, elections, and visa provisions are always anticipated to be obtainable at any time. Their continued distribution and management are more challenging, as citizens and government employees are under lockdown restrictions.

(iv) Real-time data distribution: global data synchronization is a critical factor in combating the COVID-19 epidemic. Distributing necessary data, for instance, the number of infected patients, acute cases, recovered patients, deaths, and so on, should happen in real-time to raise public awareness, support quick action, and forecast future methods. However, technical challenges against the management of COVID-19 include misuse of data ownership, a lack of ways to verify data damage, the use of a single point-of-view, centralized data stores, and insufficient transparency in data transfer, as digital information is subject to security attacks.

(v) Finance and charitable distribution: some banking institutions, such as the International Monetary Fund (IMF) and the World Bank, provide loans and grants to many countries to deal with the COVID-19 economic crisis. Such financial assistance should be shared transparently with those in need. However, due to corruption and a lack of correct automation systems, multiple countries have failed to receive such assistance [3]. In addition, citizens can be encouraged to donate if they can see the final use of the money donated.

In this worldwide health disaster, the health profession seeks novel technologies for monitoring and controlling the COVID-19 (coronavirus) epidemic. Therefore, accurate and reliable data are needed to supervise and prevent the spread of COVID-19. However, in current circumstances, there is not enough reliable data with the present technology, which may provide additional accurate data regarding the outbreak of COVID-19. Certain sources, such as medical labs and public hospitals, could present data on patients with coronavirus infection [4]. However, the information will not be trusted since it was not supervised or recorded and probably not aggregated [5]. This paper proposes a blockchain and business process management system (BBPM) to track the spread of coronavirus and solve these issues quickly. The system identifies more at-risk patients and is extremely efficient in controlling the epidemic. It is described in this paper as the digital database. It includes data that can be utilized and distributed simultaneously on a comprehensive, decentralized, and openly accessible network. The use of telemedicine for people with diabetes in combating the COVID-19 epidemic has already been proven [6, 7]. Different techniques especially deep learning [8] can be used effectively to identify affected patients. In the healthcare field, deep learning [8] has been executed in numerous applications, for example, diabetic retinopathy detection [9] and lung nodule classification [10]. Many sources of medical images (for example, MRI, CT, and X-ray) create deep learning, a better technique to discover affected patients.

Blockchain is considered a digital ledger that distributes, decentralizes, and often stores public data [11]. Blockchain consists of three main parts: blocks, nodes, and miners. Chains consist of several blocks, each of which carries data, hash, and nonce information. Also, miners can construct a new chain block utilizing a procedure known as mining. Nodes are electronic devices that maintain a copy of the blockchain and keeps its network functioning.

Any user has a personal right to access a blockchain network for transfer transactions through the so-called consensus protocol. Blockchain uses a SHA256 hash to insert transactions. The NSA creates a SHA256 hash, and it is 64 characters substantial [11]. Although all transactions are recorded on a blockchain network, the public ledger does not change and is not manipulated [12]. Both transmissions are disseminated to different consumers throughout the network to transmit and modernize information [13]. A blockchain network can be copied to an individual location; for instance, in a similar capacity, networks of healthcare sharing or fractions of a global or regional information transfer scheme [14]. The blockchain data structure is a set of hierarchical blocks, illustrated in Figure 1. It shows an example of a blockchain containing n blocks. Each successive block includes the previous block's hash, timestamp, transaction data, the nonce number for the mining procedure, and other details required for the protocol to operate [15].

The blocks are attached in tuple format as the present block record values—for example, the preceding block hash, timestamp, Merkle root hash (in a blockchain network, the hash of the hashes of the entire transaction is called the Merkle root hash) and nonce number (nonce stands for "number only used once"; it is a random number utilized to secure private communications by avoiding replay attack) in its header [16]. Each block has two entities: a header and a body. The header includes the number of a block, the hash value of a previous block to protect the dependability of the chain, the hash of the present block body to preserve transaction information, honesty, nonce, timestamp, and the address of the block creator. All block bodies have numerous transactions [17]. Furthermore, distribution, durability, transparency, and audit capability are vital features of

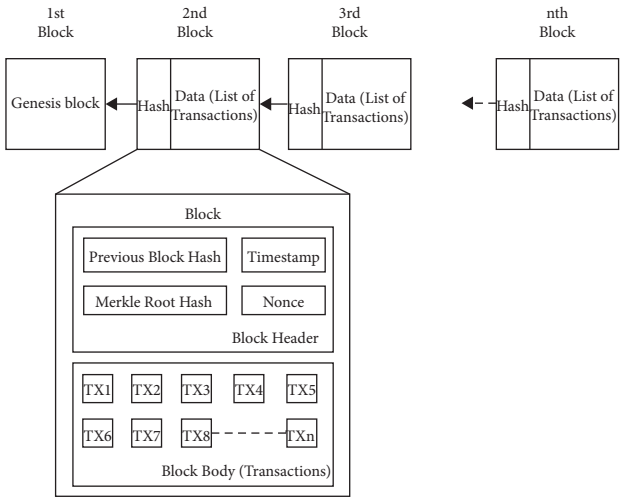

Figure 1: Structure of the blockchain.

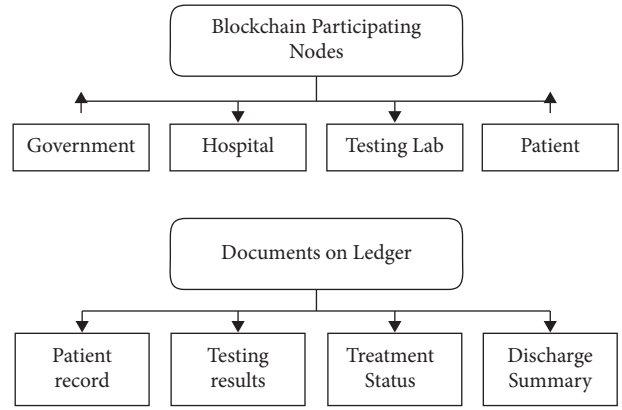

Figure 2: Blockchain participating nodes and documents on a ledger in a BBPM system.

blockchain [18, 19]. The types of blockchain are public, private, and consortium. Each archive is obtainable for the public in the public blockchain; thus, anybody can be involved in a consensus process [20]. Only a set of nodes are selected before the consensus method of a mutual network is required. In a private blockchain, only nodes from a solitary component are allowed to connect through the consensus process.

Figure 2 shows the participating blockchain nodes and documents of a distributed ledger in the proposed BBPM system. The participating BBPM nodes are testing laboratories, patients, government sites, and hospitals. In addition, the digital ledger has documents, including patient reports, consequences, the condition of treatment, and a summary of discharge.

The blockchain procedures involve the following steps: (a) collection of required data from participating blockchain nodes and (b) construction of source data converted to large amounts of information. Blockchain ensures the safety of the gathered information and assists in maintaining its confidentiality. Blockchain-protected information is examined by utilizing different solutions based on artificial intelligence. BBPM presents potential solutions to the COVID-19 epidemic, i.e., outbreak monitoring and medical supply chain management. It is utilized to set up quick, secure, and dependable data transfer with partners. Around the world, health centres and people have encountered a deficiency of medical equipment to battle the COVID-19 epidemic.

It is essential to build a BBPM to monitor COVID-19 transmission, as numerous recently implemented systems are vulnerable to hacking and cybercriminals. Table 1 illustrates the advantages of developing a BBPM-based solution instead of a conventional centralized solution in various areas, including fault tolerance, quality guarantee, data handling, and so on.

BPM is the discipline of enhancing a business process, modelling how it will perform in various situations, implementing enhancements, monitoring the advanced process, and continuously improving. A business procedure is a set of behaviours that achieve particular organizational goals. BPM is not a one-time job but a continuous function involving continuous process reengineering. BPM frequently engages spontaneous jobs in any business process, and process enhancements could occur outside of automation. A well-implemented BPM could decrease waste, decrease errors, decrease time consumption, and create superior products and services. Thus, this paper combines blockchain technology with BPM to effectively combat the COVID-19 epidemic.

The significant findings of this study can be summarized as follows. First, the patients were tested by a testing laboratory according to the early signs of COVID-19 infection. A sample of the patient is then taken, and if it is positive, the patient is isolated for a minimum of fourteen days. The BBPM is utilized for treating and monitoring the patient during the isolation period. After that, the recovery stage begins, and the patient is retested. However, if the sample of the patient is negative, the patient is released, and a summary of discharge is developed.

The rest of the paper is arranged as follows. Section 2 reviews the associated work. Section 3 describes the system with a data model. The methodology of BBPM is explained in Section 4. The results and discussion are examined in Section 5; finally, the paper's conclusion is presented in Section 6.

2. Related Work

2.1. Blockchain in Healthcare. The traditional healthcare system encounters a few issues, which include the following:

> Interoperability: this is a way to exchange data between various data systems. Data should be exchanged and used for further applications. Healthcare systems' key feature is their health information exchange (HIE) or common data distribution feature. With several EHR systems being deployed in various hospitals, they have a varying level of terminology, techniques, and functional capabilities, which means there is no universally defined standard. Moreover, medical records need to be swapped at a technical level so that more of the data can be used.

Table 1: Comparison of using a conventional centralized system and A BBPM system.

Features	Conventional centralized system	BBPM system
Fault tolerance	Huge hazard of a single point of breakdown	A distributed ledger is highly fault-tolerant
Quality quarantee	Administrators are required to authenticate data (data provenance does not apply)	Data could be tracked from its origin using cryptography technology
Transparency	Databases are not transparent	Data are stored on a distributed network
Data privacy	High chances of malicious cyber attacks	Data are stored using cryptography technology
Data integrity	The data can be changed	Data are unchanging and compatible
Control	Controlled by administrator (centralized)	Even decentralized in private blockchains
Data handling	Supports four primary functions: creating, reading, updating, and deleting	There are only read and write options

Information asymmetry: the biggest issue that critics notice in the healthcare sector is data asymmetry, which means that one contributor has better access to data than another. Health systems and the public health sector suffer from this issue because physicians can access patient records, centralizing them. If patients need to access their medical records, they have to undergo a long and arduous procedure. The data are federalized to a solitary health sector, while their regulation is delegated merely to hospitals.

Medical data breaches: an information breach of health data includes the personal health data of any individual's EHR or medical billing data from their health insurance.

Numerous health care systems are not set up to meet patients' needs or address problems associated with incompetence and poor adaptation of these systems. Some literature further suggests that the usage of health applications has had negative effects on data processing. These issues justify finding a platform that could help turn the healthcare sector into a patient-centric one—for example, blockchain, which provides a safe, obvious platform and data honesty for patients' medical records.

Blockchain technology is increasingly strengthening healthcare and operational protocols and creating the perfect foundation for a competent, proof-based decision-making procedure. Table 2 shows the SWOT analysis for model adoption based on blockchain in the medical industry. This SWOT study underscores the key advantages and disadvantages of the usual method, while the chances and risks of adoption were identified.

Disintermediation, aimed at the absence of a central authority to collect, process, and verify information or construct and distribute samples, enables us to minimize time, faults, and prices due to the effectiveness of procedures to build and update a forecast model that supports supported risk management and clinical practice. Blockchain is a combined scheme; the procedures mentioned in it are automated and consistent.

The blockchain verifies the reliability of the dealings, and the information included therein cannot be altered while enhancing the security in which the operations occur. Furthermore, with the cryptography scheme, the consistency of the information disseminated over the entire network and the lack of centralized power create more confidence in the scheme—for example, the requirement to maintain it between the contributors engaged in this procedure vanishes. Finally, the assurance between the contributors to the chain to cooperate in the execution and modernize incomplete methods is increasingly necessary through the general attention of the contributors in getting a precise, operational, and efficient forecast method.

A blockchain-based health-information-sharing network was proposed in [21]. The authors used two liberally linked blockchains to handle different health data types. They combined the storage of off-chain and authorization of on-chain to establish security and reliability criteria.

In [22], a radical user-centred healthcare information transfer technique recommended using channel creation by a decentralized and authorized blockchain to protect the privacy and improve personal security through a relationship program based on blockchain. Proof of legality with authenticity is retrieved for unspecified periods from a cloud database and embedded in the blockchain network to secure the privacy of EHR in all documents.

The safe and confidential Protected Health Information networking project based on blockchain discussed in [23] aimed to improve analysis in the e-Health program. A private consortium blockchain was formed by creating its data formation with consensus methods. The private ledger handles PHI, while the ledger society maintains a solid index of Protected Health Information.

In [24], smart contracts using blockchain were proposed to allow safe health sensor analysis and organization. They created a network using the Ethereum protocol and a private blockchain where the sensor connects to a computer that refers to the intelligent contract and records of each activity in the blockchain.

In [25], a system based on blockchain was established for secure, operational, and competent access for patients and physicians from third parties' clinical data while maintaining patient information confidentiality. Ethereum-based blockchain uses smart contracts to increase access control and encryption clarity, using modern cryptographic techniques for advanced security.

In [26], a new framework for storing blockchain-based clinical data was introduced. However, users need to keep valuable data permanently so that when there is an interruption, the originality of the data can be verified. Therefore, the authors used intelligent information administration methods and various cryptography techniques to secure consumer privacy.

Table 2: SWOT analysis for blockchain-based model adoption in healthcare.

	Positive	Negative
Internal	*Strengths* (i) Automation and disintermediation (ii) Immutability (iii) Hope (iv) Transparency (v) Confidentiality	*Weakness* (i) Operating costs (ii) Creating potential forks (iii) Lack of flexibility (iv) Data storage on local servers requires more capacity
External	*Opportunities* (i) Greater cooperation among health system operators (ii) Development of technical awareness and new expertise	*Threats* (i) Resistance to change (ii) Lack of expertise (iii) Lack of confidence in the use of new technology by health workers

MedBlock, an information administration system based on blockchain, as discussed in [27], aims to manage patients' data. The centralized MedBlock database in this scheme enables the safe entrance and reporting of medical data. In addition, an advanced consensus procedure constructs a consensus on health reports with no substantial power expenditure or obstruction of the network.

In the mobile cloud, Nguyen et al. [28] recommended a novel EHR distributor framework that integrates a decentralized interplanetary file system (IPFS) with a blockchain. Notably, they developed a reliable system for controlling access using an intelligent agreement securing health records delivery between patients and health care providers. Thus, they provided an efficient solution for reliable communication in the mobile cloud while securing the necessary medical data against possible risks.

In [29], a review of the difficulties and feasibility of blockchain in healthcare applications was presented. First, they introduced the issues related to personal healthcare dealings with an organization, which will face challenges through its unique characteristics as a blockchain. They then give extended consideration to blockchain tools in the health sector and review previous work. At last, they explain the benefits and possible research chances for blockchain-associated technology to be utilized in the medical industry.

In [30], a complete outline of blockchain technology was presented. It presented a summary of blockchain structure and the advantages of blockchain, including protection [31]. In addition, they reviewed the application of blockchains in the medical industry. With the Health Information System, the authors explained how health records could be secured utilizing blockchain.

In [32], a shared program like blockchain in healthcare is described. It presented a secure data access system using blockchain to patients and doctors at a specific hospital. The security learning of their project shows that it maintains companies' honesty and resists famous attacks [33]. Subsequently, the execution consequences exemplify the feasibility of the proposed program.

MeDShare, proposed by Xia et al. [34], is a blockchain-based source of data auditing management for health data distributed in cloud storage among large data organizations. Transfers of data transmitted from one company to another are stored on MeDShare without damage. In addition, the program uses access control algorithms to effectively supervise data behaviours caused by companies when discovering data breaches [35].

Wang et al. [36] recommended a specific EHR program using blockchain technology and attribute-based cryptography. The authors used ID-based and attribute-based encryption (IBE and ABE) [37], while [38] also used ID-based signature (IBS) to generate a digital signature for encrypted health data. It helps set up the project effectively and does not require various cryptography programs for various safety needs.

In [39], a frivolous blockchain structure for Health Data Management (HDM) was recommended to slow down calculations and interaction overhead compared to the network of Bitcoin by separating network providers within clusters and keeping a ledger copy per cluster. Their framework initiates the necessity for a canal that allows secure and confidential dealings inside a collection of network providers. Furthermore, they recommended a resolution to avoid fraud in the Bitcoin network. They demonstrate the effectiveness of the authors' recommended structure in providing security with secrecy to the Bitcoin network by analyzing different attacks. They further discussed how the authors recommended structural deals for discovering attacks.

In [40], an analysis of various solutions using blockchain was provided. First, the authors explored the recent sophisticated solutions that make smart devices compatible with blockchain in various industry 4.0 devices. After that, the benefits and drawbacks of traditional security resolutions are discussed in terms of their countermeasures.

Bach et al. [41] presented comparative research into the consensus mechanisms of blockchains. In particular, Ethereum currently uses the consensus protocol known as the Proof of Work (PoW). It is a system that allows a decentralized Ethereum network to agree to deal with balances of accounts. Thus, it allows consumers to avoid "double spending" their currency and ensures that the Ethereum chain is harder to attack or overwrite.

Ying et al. [42] used attribute power to deliver keys to information consumers in the Ciphertext Policy Attribute-Based Encryption (CP-ABE) model to attain precise access control for distributing health records in the cloud. Using test surroundings in an Ubuntu Linux desktop, they assessed the proposed program with a numerical simulation, and the decentralized usage capability was avoided. In the context of

blockchains, different studies have explored the potential of blockchains to sustain e-health information distribution.

Numerous research projects are currently being conducted on the utilization of standard blockchains in health care. The most current is MedRec [43]. The MedRec method uses the Ethereum platform to set up a decentralized health proof distribution scheme for smart contracts. It distributes medical reports among various health partners and patients with any other contributor that executes health or medical reports. For example, healthcare providers could add patient records at any time, but it is up to the patient to determine what information could be accessed by other providers. MedRec recommends two mining methods. The first uses ether as an effective method. In contrast, the second recommends utilizing compiled and anonymous information like a gift to motivate investigators. The primary node going to a block is allowed access to the desired information.

2.2. Blockchain and Business Processes. We did not initially discover the application possibilities of blockchain for business processes. Many blockchains are now widely accepted in different domains to assist in the function of novel business processes. For example, a caterpillar proposed by López-Pintado et al. [44] is an open-source business process management system (BPMS) that runs on the summit of the Ethereum blockchain. Like any BPMS, Caterpillar assists in constructing procedure method events and lets consumers supervise the status of procedure events and perform their jobs. The uniqueness of Caterpillar is that the status of each processing event is kept in the Ethereum blockchain. In addition, the flow of work algorithm is executed by smart contracts created by the Business Process Model and Notation BPMN-to-Solidity compiler. The compiler assists in a broad range of BPMN configurations, containing consumer and service functions parallel to exclusive gateways, subprocesses, multiple event functions, and event handlers.

In [45], an automated BPM framework explored composing services in free commerce surroundings, and blockchain was investigated and presented to change and check trade trust. The BPM solution illustrates how blockchain technology could provide instant, dependable, and cost-efficient service and deliver quality services in workflow composition.

2.3. Use of Blockchain in Epidemic Situations. The possible use of a blockchain system for regulating and alleviating the COVID-19 situation is explained and explored in detail.

2.3.1. Data Management of Clinical Trials. Clinical trials must maintain information according to rules, for example, reports being open to shareholders, the confidentiality of reports, security, and immutability [46]. Blockchain records and makes real-time data available to physicians. It enhances data accuracy, facilitates data transfer, guarantees compliance, and provides an audit path for superior confidentiality and data security [47, 48].

Conducting clinical trials to implement the COVID-19 vaccine is a complex, time-consuming, and expensive process. The vaccine's clinical trials require close coordination and cooperation between the companies engaged and are frequently situated in geographically distributed areas. Researchers, regulators, donors, and pharmaceutical companies are instances of companies that have been seriously engaged in clinical trials to implement and administer the vaccine for COVID-19 successfully.

Traditional centralized clinical trial data management systems encounter several challenges, including compliance with course enrollment, limited effectiveness and clinical testing necessities, data confidentiality guarantees, compliance with clinical trial rules for participants' healthcare, and reliability of clinical trial data. Furthermore, centralized clinical trial management systems could provide multiple versions of clinical trial data to construct organizations' data pits. Consequently, they could guide the duplication of clinical trial information frequently recorded and handled by numerous companies.

Therefore, copying clinical test data makes it hard to access, implement, and examine consequences. Furthermore, centralization creates clinical trial data susceptible to changes by external hackers. Blockchain technology could help research institutes, and pharmaceutical companies protect clinical trial data's honesty when developing a vaccine. It ensures that a single and synchronized view of clinical trial data is obtainable to all accredited companies. Therefore, problems, such as duplication and discrepancy of clinical trial data because of the breakdown of previous centralized clinical trial management systems, could be successfully addressed.

Smart contracts could check a company's access rights before allowing the utilization of clinical trial data to protect data confidentiality and safety. The authorized contributors can digitally check that the clinical trial necessities have signed the consent form. Thus, anonymous data gathering and verifiable approval management will allow contributors to distribute their case records to authorized companies without disclosing their identities.

To keep contributors in a clinical trial, pharmaceutical companies generally provide appreciation tokens to contributors in cash or on gift cards. Smart contracts will help the payment process quickly by presenting an automated, transparent, and accountable system for converting cryptocurrencies. Accountability and transparency features ensure that data can only be utilized for the intended purpose, thus increasing user confidence.

2.3.2. Vaccine and Necessary Drug Supply Chain. Blockchains could effectively handle the healthcare supply chain, especially in epidemiological circumstances that engage important transactions across the globe. There may be instability in its distribution until an approved version of the vaccine is available to sell and advertise. Dishonest performance, for example, incorrect vaccinations, high pricing, and stock accumulation may be possible. These problems can be effectively managed to utilize a blockchain-based medical supply chain [49].

Symptomatic patients can contact remote health professionals through information technology infrastructure to reduce the risk of transmission of infectious viruses using advanced remote health practices, such as telehealth and telemedicine services. In addition, remote detection and treatment of patients could notably reduce patient access and staff limitations, thereby effectively controlling the quick rise in global COVID-19 cases of employment in remote health services.

Because they are governed and handled by a centralized authority, remote health systems can be susceptible to the point-of-failure issue, which finally infects the honesty and reliability of health records. The intrinsic features of the revolutionary blockchain technology could introduce various advantages to the remote healthcare industry. Significant features include setting up a source of electronic health records, checking the legitimacy of users, requesting patient data, verifying patient anonymity, and automating micropayments to use remote health services.

These significant features help to demonstrate self-examination clinical instruments for COVID-19 testing successfully. Following a test result, individuals whose test results are negative should generally adopt self-isolation policies to minimize the spread of the virus to the community. There is a need for safe tracking of medical items for self-isolated individuals; blockchain technology brings changes to explicitly record the timestamped location data of medical items in the ledger. Guaranteeing social exclusion and wearing masks when engaging in business behaviours can help avoid the diffusion of COVID-19.

The growing number of confirmed cases of COVID-19 worldwide, particularly in areas with the highest virus transmission rate to estimate the diffusion of COVID-19, requires the administration of drugs without contact with patients. Aerial vehicles may be utilized to transmit medicines and medical supplies to distant patients. Also, aerial vehicles could help in transporting medical supplies to hospitals located in remote locations. For example, China has used aerial vehicles to deliver medicine from one city to another during the COVID-19 epidemic.

Blockchain allows the location of aerial vehicles to be tracked, checking the level of service provided, and computing the reputation score of an aerial vehicle using its effectiveness in a reliable, responsible, and transparent manner. By executing access to control protocols and identity management, blockchain technology reduces the feasibility of attacks by enemy vehicles. Furthermore, it invariably stores orders provided by the control room on aerial vehicles (for audit purposes to check noncompliance with published orders) with measures to discover human movements and reactions by cleaning highly infected areas.

A swarm consists of several autonomous aerial vehicles that work together to attain a general aim. For example, a crowd of aerial vehicles could utilize blockchain technology to achieve the most dependable global results by trading safely in a blockchain. To take another example, a voting system based on blockchain makes it possible to discover densely populated areas where aerial vehicles can be sprayed with disinfectants.

2.3.3. Communication Tracking. Health facilities are active inpatient contact monitoring systems; however, records obtained may be misused. The utilization of blockchain will offer data stability and authenticity [50]. Networks of blockchains could monitor patient behaviour and present current updates to infected fields. In addition, records could be created for affected and potential victims through contacts. Communication tracking poses challenges to privacy, as information has to be collected, fitted, and distributed. Guaranteeing the identity protection of users with COVID-19 introduces other issues. Although participation in the exam can ensure some control, we have not yet observed how we can guarantee that merely appropriate information is distributed. Blockchain could play a neutral role in a disseminated way to separate authorized solvers from mitigating users/patients and the identity of user and place data. It could present a resolution to protect the confidentiality of technological plans before adhering to rules within the centralized scheme.

Moreover, the integration of blockchain with anonymization and encryption techniques could also defend the individuality of users. Blockchain is nonregional and provides an appropriate worldwide usage platform for detecting and controlling the COVID-19 epidemic. This explicit aspect may prevent the public from deliberately misinforming officials or other third parties.

Respecting the social distancing orders provided by the government could notably reduce the social interaction of humans to avert the spread of COVID-19. Social exclusion is activated by a public health activity called digital contract tracing, which can break a person's chain of spreading the virus. Digital communication tracking constantly monitors the affected population to quickly and efficiently discover all social communications during the incubation period of infected COVID-19 patients. It primarily uses Bluetooth or GPS to use nearby data to discover social communications with a virus-infected person.

After coming in close contact with a confirmed COVID-19 case, exposed persons should be tested, supervised, and self-isolated. The clarity and consistency of the data ensure that users' health data, for example, COVID-19 test results, cannot be changed or removed by attackers or health workers. Furthermore, the General Data Protection Regulation (GDPR) protects the confidentiality of users' information through the confidentiality rules outlined in the Privacy Act. The positioning technique parameter refers to technologies that could be utilized to discover a user's location.

The coverage area parameter explains the geographical regions in which a COVID-19 patient could detect social interactions with another person. The heavyweight designs of the Contact Tracing application are intended to utilize computer resources aggressively when identifying and verifying social interactions between people. Conversely, lightweight application design enhances computer resources by leading users and providing essential features. Digital contact tracing users' necessity promises an extended battery life of devices and greater confidentiality, safety, and transparency of data related to COVID-19.

Preferably, the digital contact tracing solution could present greater confidentiality of data, an expanded coverage region, a lightweight application plan, better data protection and clarity, and battery-friendly functionality. However, ensuring the confidentiality of an individual's health data and, at least, COVID-19 false-positive events is a significant challenge for digital communication tracking solutions. Data confidentiality is protected by encrypting a person's location and contact history and averting the dissemination of personal health information to the public.

On the occasion of close contact with a COVID-19-affected patient, users can be informed about the latest social interaction without revealing the evidence of the affected person (e.g., their name). Digital contact tracking by smartphone applications such as Google-Apple's Contact Tracing and Singapore's Trace Together uses Bluetooth to discover the close physical contacts of a person affected by the virus. However, regarding the battery barriers of smartphones, Trace Together is not user-friendly. Furthermore, Google-Apple Contact Tracing does not reveal the location and identity of users to protect data confidentiality.

Blockchain-based solutions are less reliable because they are subject to data fraud through the application administrator, given the high confidentiality and sensitivity of users' information. Unchanging and decentralized blockchain technology is a feasible alternative to digital communication tracking. It protects the confidentiality of the user's information by allowing pseudo-anonymity. Digital contact tracking with a custom exposure matching mechanism can use the blockchain site to store social contact data and enable authorized users to access the information to protect its confidentiality. An external trusted network of servers is utilized in the provided system to create anonymous addresses for users to protect data confidentiality. The organization has executed some smart agreements, for example, registration of companies, COVID-19 testing, geodata processing, query processing and approval management, automation of services, and assurance that the evidence of individuals affected by COVID-19 has not been revealed to others.

As a private blockchain-based system, all entities are registered before making a transaction on the blockchain. Geodata processor contracts assure us that the duplicate data (e.g., the location data of a user with limited mobility) are not forwarded to the contact solver to speed up the contact tracing process. COVID-19 testing contracts assisted in recording COVID-19 test results on the blockchain for each employee. Subsequently, the consent management contract seeks to legalize the location data usage of the employees of an organization. The contact solver component of the contact tracing system leverages AI-based techniques for identifying social interactions among individuals. It informs users about possible risk levels based on many factors, such as distance, mobility, and total time spent during social interaction with a COVID-19 infected person.

In a blockchain-based system, all companies are registered before creating a transaction on the blockchain. The Geodata Processor Agreement guarantees that no duplicate information (e.g., the location information of a user with limited mobility) is sent to the contact solution to expedite the contact tracking procedure. The COVID-19 test contract allows each worker to store the COVID-19 test outcomes in the blockchain. The consent management agreement aims to legitimize the use of location information by employees of a company. The Contact Solver element of the Contact Tracing System uses AI-based methods to identify social communications between individuals. COVID-19 informs users about potential risk stages using factors such as distance, movement, and total time spent during social communication with the victim.

2.3.4. Data Collection. Monitoring outbreaks by deploying, collecting, and retrieving data that respond effectively to the epidemic, understanding trends, and managing tests are vital resources. Blockchain's ability to confirm and store enduring real-time data confirms information reliability [51]. The utilization of the blockchain network presents the surveillance and communication infrastructure to assist in capturing, recording, and examining virus spread and control data.

2.3.5. Consumer Information Confidentiality. Those responsible for making the policy and health practitioners should obtain patient information through patient monitoring and other enhanced decision-making and discuss patient privacy problems. In these troubled days, a balance law must be enacted between registry management and user confidentiality management to enhance hope in the scheme. Blockchain is a viable resolution for maintaining and displaying patient data, monitoring patient processes, and setting up degrees of social isolation while protecting confidentiality.

2.3.6. Early Discovery of Susceptible People. Different triage systems based on AI can reduce patient concerns. The online bot would assist in comprehending the origin symptoms of early discovery and then guide them through preventive measurements, for example, social exclusion and hand sanitation. It would warn users about medical facilities if symptoms intensify [52]. The secrecy of patient data is vital to the protection of their social and personal values. Blockchain-based architecture could efficiently manage these safety and confidentiality problems.

2.4. Blockchain Cases of COVID-19 Epidemic. A few of the blockchain cases utilized to fight the COVID-19 epidemic are explained below.

Hyperchain is a platform based on donations created to support hospitals and governments donating to affected patients in China [53]. To solve the lack of facilities during this epidemic, numerous users could join the millions of nodes of hyperchain that could receive donated items and necessary medical equipment from factories.

PHBC: this platform based on blockchain is utilized for continuous and unknown checking of society and working places open to COVID-19 and dangerous

viruses [54]. A vital aspect of this platform based on blockchain is detecting the movement of noninfected individuals and controlling these individuals' return if they go to the affected regions.

VeChain: this is a platform using a blockchain created to supervise vaccine manufacture [55]. All behaviours associated with vaccine manufacture, from substance to codes to packages, are stored and recorded in a distributed ledger. Thus, it presents an efficient way to decrease the risk of possible changes to vaccine data.

Hashlog: this project was developed by Acoer, a Georgia-based health technology startup [56]. The Hashlog blockchain solution could be implemented through distributed blockchain ledger technology, ensuring logging and data visualization of coronavirus outbreaks from US Centers' public Data for Disease Control (CDC) and WHO.

2.5. Blockchain Security. The blockchain platform should guarantee the fundamental features of security: confidentiality, integrity, and availability that advantage the healthcare industry.

Confidentiality could be attained by ensuring that the application is on a personal blockchain and that users have restricted access. It will reflect the certification needed in the healthcare field, such as becoming a physician, with the proper qualifications needed. Likewise, in the business network, the accounts of the physicians should be constructed by the medical entity. In addition, blockchain network data should be allowed to protect confidentiality. In addition, contributors will have various roles and privileges. In addition, encryption should ensure that the data between the blockchain and the user is safe. Confidentiality is further mandatory in this business network; however, it directly battles data breaches and phishing attacks [44].

Integrity: integrity is about ensuring that information is reliable and accurate. Blockchain attains this in two different methods: (1) hashing and (2) shared distributed ledger. Strong collision-resistant and safe hashing algorithms should be utilized to ensure integrity. Likewise, privacy and access control ensure that the data are reliable by controlling the number of individuals who could damage the data.

Availability: significantly, there is dependable and simple access to data on the blockchain. Ensuring that the network of blockchains is fault-tolerant decreases the number of failed links to information in the blockchain. In addition, the data in a blockchain are a shared ledger; thus, there is a variety of copy information that ensures that the data do not disappear. The network of blockchains should run on the newest version of HyperLedger to ensure that errors do not impact the system's availability.

Berdik et al. [45] presented an extensive review of the use of blockchain as a service for applications within today's data systems. This review provides the reader with an in-depth foresight on how blockchains can help to protect and handle today's data systems. The review includes detailed reports on the various examples of blockchain studies and applications presented through the investigation group and their implications for blockchain and other applications or their use in scenarios. A few of the very significant discoveries this review highlights are the framework of blockchain and the latest cloud and edge computing examples that are important in allowing the extensive adaptation and implementation of blockchain technologies for novel players in today's unparalleled vibrant global market.

3. System Model

This section discusses the BBPM system model and the notations utilized in this model. Here, Figure 3 illustrates the system model. It has four entities.

Participating nodes in BBPM are testing laboratories, patients, government sites, and hospitals. In addition, the digital ledger has documents, including patient reports, consequences, treatment conditions, and a summary of discharge. Figure 4 demonstrates the necessary steps utilized in BBPM to trace and store the data's active COVID-19 patients. (1) Patient visits a testing lab. (2) First, the patients were analyzed by a testing lab according to the early signs of COVID-19. The testing lab is an important node in the network of blockchains. It acts as a miner. (3) The patient sample is taken, and if it is negative, the patient may be discharged; a summary of discharge is also constructed. (4) However, if the result of the patient sample is positive, the patient is isolated for a minimum of 14 days. (5) During the time of isolation, BBPM is used to treat and monitor the patient. (6) After that, the recovery stage begins, and the patient is retested for COVID-19 after 14 days. (7) If the patient dies during treatment, the body of the deceased will be disposed. (8) After recovery, the patient pays the hospital for treatment. (9) Details of total COVID-19 confirmed cases are informed to the government through the testing lab. 10) Details of recovered and death cases are informed to the government through the hospital. The government records patient data for upcoming usage; its confidentiality is maintained and provided when required to be demonstrated on a large scale. Figure 4 demonstrates the workflow of the BBPM scheme.

BBPM provides a guarantee of the accuracy of the patient's stored information. Table 3 shows the notations used in the proposed system model.

4. Proposed Methodology

This section discusses the Blockchain and Business Process Management (BBPM) system in health care methodology. One of the major issues has been the requirement for current information on the epidemic and the spread of COVID-19. BBPM helps solve this problem more efficiently. One significant benefit of this system is that it provides provable and safe information utilizing its peer-to-peer networking features and distributed ledger technology. This technology plays a vital role in recording patient data on COVID-19

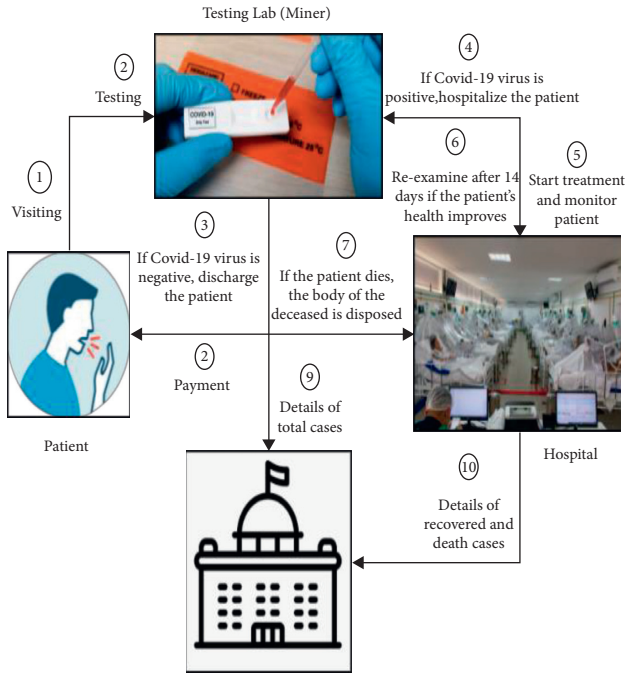

Figure 3: Proposed system model.

signs, locations, and records of health situations during the infection. BBPM helps distribute, encrypt, and securely record digital transactions. It is anticipated to revolutionize calculations in numerous regions, mostly where centralization is unnatural; moreover, privacy is necessary. By establishing a network of blockchains on citizens' mobile devices, it could be improved internationally to monitor the spread of COVID-19.

In general, there are three kinds of nodes: miner nodes, full nodes, and light nodes. A miner node could suggest blocks and contain a whole blockchain history. Full nodes contain the entire blockchain history, although without presenting novel blocks. Meanwhile, light nodes depend on the full node blockchain history. In the BBPM scheme, the miner nodes are the testing lab, and the hospital is a full node; the patient and government also play the role of light nodes. In the BBPM system, many patients, testing labs, and hospitals are obtainable. Thus, control of access is essential. Their BBPM scheme presents access control. The collection, use or disclosure of personal health data without the consent of individuals is generally called as unauthorized access or "snooping." Unauthorized access involves viewing personal health data in electronic data systems and can be triggered by a number of factors, including individuals' conflicts, interests, personal gain, or concerns about their health and well-being. As a health data protector, we must take reasonable steps to guarantee that personal health data are protected against theft, loss and unauthorized access and disclosure, and that records containing data are protected against unauthorized copying, alteration or removal. We must take reasonable steps to guarantee that personal health data are not collected without authority and that records of personal health data are retained, altered, and disposed of in a secure manner. Protecting privacy should be integrated into the provision of health care and should be embedded in the culture of each health care system. To overcome this problem, access control is proposed in this BBPM.

At BBPM, the patient could merely see his or her digital ledger; moreover, nobody else could see his or her ledger.

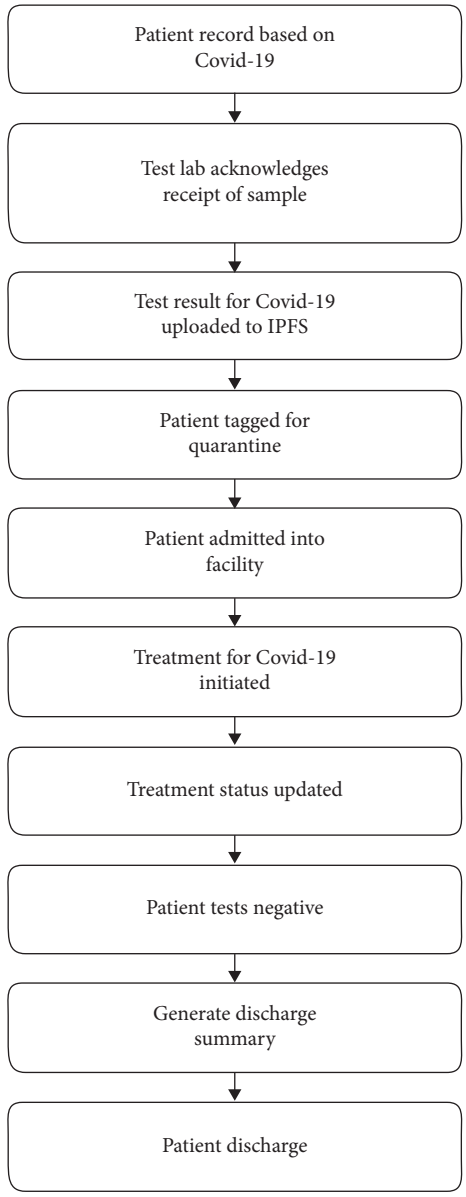

Figure 4: Workflow of the BBPM system.

Table 3: Notations.

Notation	Description
BH	Block header
BB	Block body
Bid	Block ID
EB	Encrypted block body
DS	Discharge summary
DD	Discharge date
PD	Patient details
TD	Treatment details

Furthermore, a testing lab can only see the ledger of the patients it has tested. Like the testing lab, the hospital can only see the ledger of the patients it has treated. Finally, the government cannot look at any patient's ledger. They can only view statistical information, such as total, recovered, and death cases.

4.1. Algorithm Design. Algorithm 1 explains the proposed Blockchain for Business Process Management (BBPM) in healthcare.

4.2. Benefits of BBPM System in the COVID-19 Pandemic. This section discusses the benefits of the proposed BBPM system in the COVID-19 pandemic, as shown in Figure 5.

4.2.1. Enhancing Transparency When Treating Affected Patients. Transparency is one of the most significant aspects of BBPM. It is essential to protect personal data and information regarding patients undergoing treatment. The spread of false information on social websites creates fear against untested data. The ability to verify BBPM data and modernize current information could present a viable way to guarantee the analysis of data accuracy. Thus, it could aid the change from an organization powered by interoperability to patient-centred interoperability.

4.2.2. Traceability. Diagnosis refers to the monitoring of affected patients. Controlling the spread of the coronavirus is essential. With BBPM, one could trace the activities of affected patients; present modern information regarding total confirmed, recovered, and death cases; and report direct combating efforts. This tracking could be completed through the transaction of the blockchain network's storing and tracking capabilities.

4.2.3. Enhanced Healthcare Protection. BBPM operates on platforms that deal with reasonable and excellent healthcare security. It could present a viable solution for monitoring coronavirus outbreaks to defend numerous patients from this infection. It monitors affected patients by regular testing to ensure timely and appropriate treatment. If hospitals have a safe and dependable health record database, it will reduce the risk of misdiagnosis.

4.2.4. Record and Exchange Treatment-Associated Data. Keeping a record of the gathered information and transmission of treatment-associated information are some of the very serious and difficult jobs during the COVID-19 epidemic. From July 2020 to June 2021, an average of 3,343,448 health records was breached each month. The BBPM system could maintain an incorruptible, decentralized, and obvious record of patient information. BBPM lets healthcare providers, doctors, and patients distribute similar data rapidly and securely.

4.2.5. Enhancing the Recovery of Affected Patients. Timely treatment can improve the recovery rate of affected patients. In addition, BBPM helps to monitor isolated cases in hospitals effectively. In a COVID-19 infection, the blockchain patient's symptoms, location, and historical health status can be recorded with high privacy. The data block spreads over distributed networks of end-users, governments, and health professionals.

4.2.6. Disease Control. To control and prevent the spread of infection, effective and accurate disease monitoring is essential. BBPM could be utilized worldwide to monitor the spread of COVID-19 infection in humans. In the COVID-19 pandemic, BBPM must sustain the victims of the virus by immutably storing patient disease signs.

5. Experimental Results

The effectiveness of the proposed work is examined in this section. The intensity of COVID-19 was high that the World Health Organization (WHO) had to announce COVID-19 as an epidemic within a week of its complete growth. The greatest difficulty many governments face is a shortage of accurate methods for diagnosing recently affected cases and predicting the danger of the coronavirus pandemic. Therefore, this paper proposes the Blockchain and Business Process Management system to resolve this COVID-19 disaster. This experiment uses a blockchain constructed utilizing POJO in Java. Blockchain makes dealing easier among unreliable groups. The blockchain is a collection of blocks, including many transactions. Each block is hashed, a hash is added, the hash is reconnected, and the hash is rehashed until there is a hash and Merkle root. Each block stores the hash of an ex-block by linking the blocks. Thus, it ensures that a block will not alter without altering the adjacent blocks. However, the experiment grasps a string of data that contains anything you can envision, including smart contracts based on the style of Ethereum. The experiment driving this BBPM system also calculates the performance of the BBPM system with a primary evaluation metric, namely, execution time.

5.1. Execution Time. Execution time (ET) is explained as the period (in a sec) between the transaction confirmation (TC) and its execution (TE) in the blockchain network shown in the following equation:

$$ET = TE - TC. \tag{1}$$

The time of execution increases as the number of transactions is raised. These transactions perform a variety of operations contained in the smart contract algorithm as explained in Algorithm 1. For example, when merely one consumer is utilizing the system, operations at a time, including testing records, hospital allocation records, treatment and monitoring records, re-examination records, corpse disposal records, discharge summary records, payment records, and statistics records, it would take 1 min 20 seconds, 30 seconds, 50 seconds, 1 min 10 seconds,

```
Testing Lab (Miner)
Res = Take a sample of the patient and examine and diagnose COVID-19 in the testing lab
if (Res == positive) then
    Patient registration
    The private key and public key generation for a patient using RSA algorithm
    Select hospital for patient isolation and treatment
    BB = Generate block body using patient details with hospital name, testing lab name, and date of testing
    EB = Encrypt BB based on the public key of the hospital
    Hash = Generate hash based on HmacSHA1 algorithm
    Timestamp = Get current date and time
    Nonce = Generate random numbers
    BH = Generate block header using previous block hash, timestamp, and nonce
    Block = Add BH with EB
    Upload Block to Blockchain
Else
    DS = Generate Discharge Summary of the patient
    DD = Get current date and time//Discharge Date
    BB = Generate block body using patient details with hospital name, testing lab name, date of testing, DS, and DD
    EB = Encrypt BB based on the public key of patient
    Hash = Generate hash based on HmacSHA1 algorithm
    Timestamp = Get current date and time
    Nonce = Generate random numbers
    BH = Generate block header using previous block hash, timestamp, and nonce
    Block = Add BH with EB
    Upload Block to Blockchain
End
Hospital
The hospital can only access the ledger of the patients who should be treated
EB = Extract EB from a block of the blockchain
BB = Decrypt EB based on the private key of the hospital
PD = View details of patient, testing lab name, and date of testing from BB
TD = Get details of treatment using patient monitoring
if (the patient health improves) then
    //Take a sample of the patient and re-examine the request to the testing lab
    BB = Generate block body using PD and TD
    EB = Encrypt BB based on the public key of testing lab
    Hash = Generate hash based on HmacSHA1 algorithm
    Timestamp = Get current date and time
    Nonce = Generate random numbers
    BH = Generate block header using previous block hash, timestamp, and nonce
    Block = Add BH with EB
    Upload Block to Blockchain
else//if the patient is death
    Dispose of the body of the patient
End
Patient
The patient can only see his or her digital ledger
EB = Extract EB from a block of the blockchain
BB = Decrypt EB based on the private key of patient
PD = View details of patient, testing lab name, date of testing, hospital name, treatment details, and discharge summary from BB
Government
Government can only see the details of statistics to ensure the patient's privacy
```

Algorithm 1: Blockchain and Business Process Management (BBPM) algorithm.

40 seconds, 30 seconds, 25 seconds, and 15 seconds, respectively, for these operations to be performed. This time would increase when 100 consumers are utilizing the system concurrently. The experiment assessed the effectiveness of the BBPM system using a comparison between the average size of EHRS or blocks and the average execution time for accessing EHR from centralized storage or accessing blocks from the blockchain using existing BSF-EHR [57] and the proposed BBPM algorithms, as shown in Figure 6.

Figure 6 compares centralized storage and the existing BSF-EHR algorithm, and the proposed BBPM algorithm works quickly. Furthermore, Figure 7 shows the

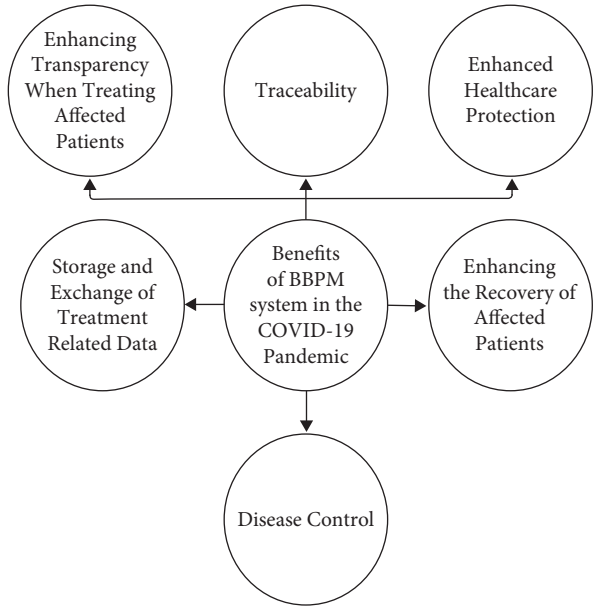

Figure 5: Benefits of BBPM system in the COVID-19 pandemic.

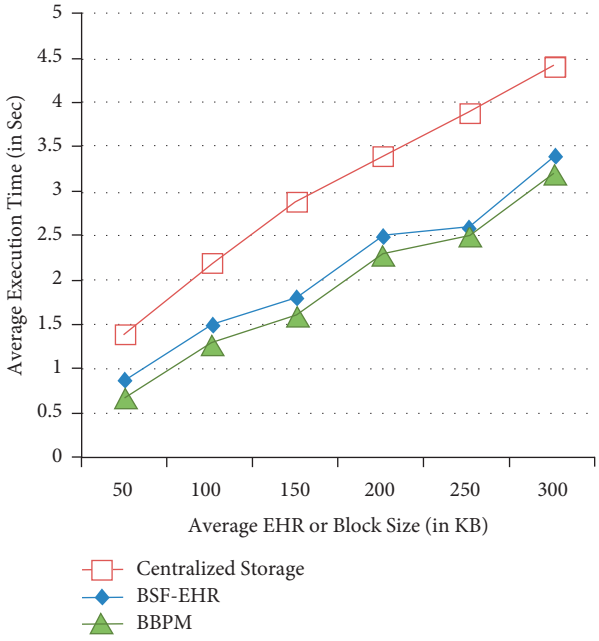

Figure 6: Average EHR or block size vs. average execution time.

effectiveness of the BBPM scheme using a comparison between the number of user requests and execution time for accessing EHR from centralized storage [28] or accessing blocks from the blockchain using the existing BSF-EHR and the proposed BBPM algorithms.

Figure 7 concludes that the proposed BBPM algorithm quickly responds to any user request compared with centralized storage and the existing BSF-EHR algorithm. Figure 8 compares the blockchain hash generation time of different algorithms using blockchain in healthcare, specifically Shynu et al. [58], the BSF-EHR algorithm of Abunadi et al. [57], and the proposed BBPM.

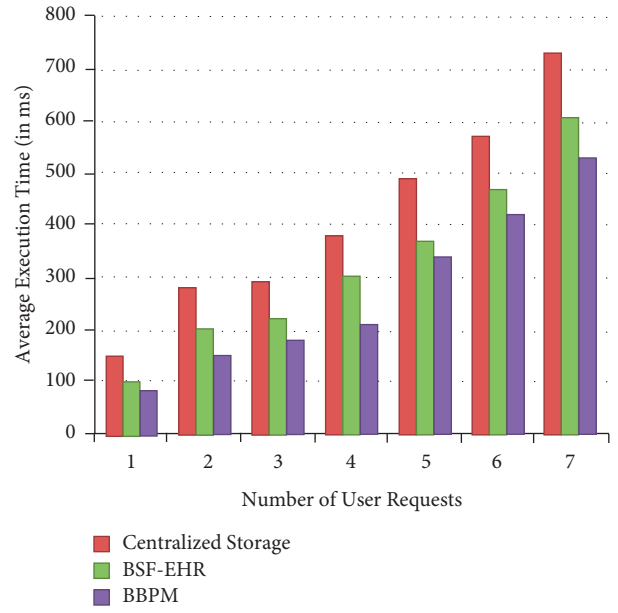

Figure 7: A comparison between the number of user requests and average execution time.

Figure 8 concludes that the BBPM algorithm takes less time for hash generation than other algorithms as BBPM used lightweight hash generation algorithm, namely, HmacSHA1. This lightweight hash generation algorithm takes less time for hash generation than others. The experiment calculates the execution time for accessing health records, from demanding information to getting information. In centralized storage, health records are recorded on a centralized server. If the hospital desires to access a patient's health record, it creates a health record demand. Now, we note the present time (PT1), and they send the health record demand to a centralized server. After receiving the health record demand from the hospital, the centralized server search also obtains the patient's health record and transmits it to the requested hospital. We then note the present time again (PT2). Thus, the execution time for using health records = (PT2 – PT1) secs.

Moreover, the execution time is frankly relative to the size of the health record. If the size of the health record is very large, the time taken to access the health record is important. On the other hand, if the size of the health record is small, the time taken for accessing the health record is little. Therefore, the execution time varies depending on the size of the health record. At BBPM, each hospital and testing lab maintains the blockchain. This blockchain contains the EHR of any patient in an encrypted format. After decryption, the testing lab or hospital can access the EHR of the patients it has tested or treated. Compared with centralized storage and the existing BSF-EHR, the proposed BBPM takes the smallest amount of time. The experiment's consequences regarding various sizes of health records show that BBPM is better than centralized storage based on execution time. This outcome also demonstrates the efficiency of the BBPM system. Table 4 shows an evaluation of BBPM by comparison with some associated works [57].

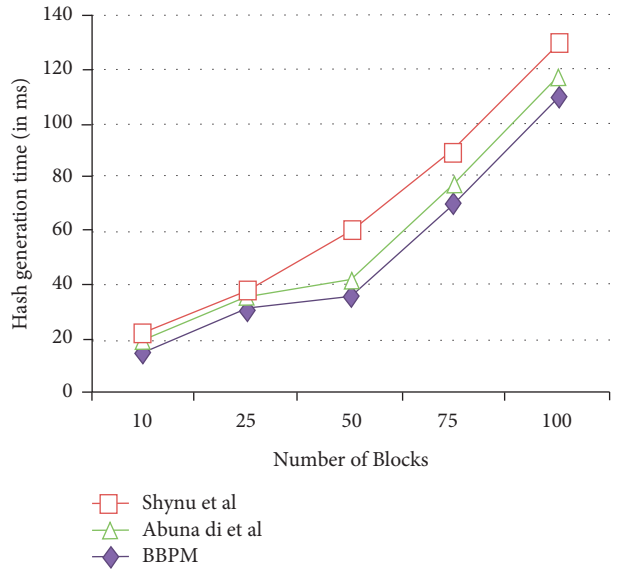

Figure 8: Comparison between the number of blocks and hash generation.

Table 4: Comparison of BBPM with some associated works.

Associated works	Decentralized access	User authentication	Identity management	Data privacy	Flexibility	Availability	Integrity
Ying et al. [42]	No	Yes	Yes	Yes	No	No	Yes
Ramani et al. [32]	Yes	Yes	No	Yes	No	No	Yes
Xia et al. [34]	Yes	Yes	Yes	Yes	No	Yes	Yes
Liang et al. [22]	Yes	No	No	Yes	Yes	Yes	Yes
BBPM	Yes	Yes	Yes	Yes	Yes	Yes	Yes

6. Conclusion

This paper presented a Blockchain and Business Process Management System (BBPM) for combating the COVID-19 epidemic. The existing blockchain or business process management system is used separately to mitigate the COVID-19 pandemic. But, this paper integrates the blockchain and business process management system for COVID-19 epidemic mitigation. In this way, the benefits of both technologies can be obtained simultaneously. The main role of the BBPM system is to assist in managing the diffusion of this epidemic. The system could assist us during this epidemic disaster by presenting the advanced resolution, explosion monitoring, user privacy protection, donation monitoring, and secure daily operations. The BBPM system should minimize network delays by offering a safe environment for recording and transmitting sensitive data. A lightweight blockchain plan is essential in the medical industry to improve information confirmation and transactional communication. Creating modified ledgers that could be located on neighbouring servers in the blast region increases blockchain performance. BBPM system consumes a lot of energy because every transaction needs robust hardware resources. Scalability is the main limitation of this BBPM system. Another drawback of this BBPM system is the complexity of blockchain and the need for a comprehensive network of users. In the future, to deal with the above problems, a novel, energy-efficient and scalable BBPM system is needed. Furthermore, the final mixture of the BBPM system with other growing techniques, such as big data and artificial intelligence, will efficiently manage deadly epidemics similar to the coronavirus.

Data Availability

The data that support the findings of this study are unavailable in any public repositories.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

The authors would like to acknowledge the Prince Sultan University for its support, which facilitated the publication of this paper.

References

[1] S. S. Vedaei, A. Fotovvat, M. R. Mohebbian et al., "COVID-SAFE: an IoT-based system for automated health monitoring and surveillance in post-pandemic life," *IEEE Access*, vol. 8, pp. 188538–188551, 2020.

[2] F. Hu, J. Liu, L. Li, M. Huang, and C. Yang, "IoT-based epidemic monitoring via improved gated recurrent unit model," *IEEE Sensors Journal*, 2021.

[3] H. Wang, J. Tan, and X. Li, "Global NO2 dynamics during the COVID-19 pandemic: a comparison between two waves of the coronavirus," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 14, pp. 4310–4320, 2021.

[4] S. Nisar, M. A. Zuhaib, A. Ulasyar, and M. Tariq, "A privacy-preserved and cost-efficient control scheme for coronavirus outbreak using call data record and contact tracing," *IEEE Consumer Electronics Magazine*, vol. 10, no. 2, pp. 104–110, 2020.

[5] X. Chen, S. Jiang, Z. Li, and B. Lo, "A pervasive respiratory monitoring sensor for COVID-19 pandemic," *IEEE Open Journal of Engineering in Medicine and Biology*, vol. 2, pp. 11–16, 2020.

[6] X. Ding, D. Clifton, N. Ji et al., "Wearable sensing and telehealth technology with potential applications in the coronavirus pandemic," *IEEE reviews in biomedical engineering*, vol. 14, pp. 48–70, 2020.

[7] A. Romanovs, E. Sultanovs, E. Buss, Y. Merkuryev, and G. Majore, "Challenges and solutions for resilient telemedicine services," in *Proceedings of the 2020 IEEE 8th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, pp. 1–7, Vilnius, Lithuania, April 2021.

[8] S. Bhattacharya, P. K. Reddy Maddikunta, Q.-V. Pham et al., "Deep learning and medical image processing for coronavirus (COVID-19) pandemic: a survey," *Sustainable cities and society*, vol. 65, Article ID 102589, 2021.

[9] T. R. Gadekallu, N. Khare, S. Bhattacharya et al., "Early detection of diabetic retinopathy using PCA-firefly based deep learning model," *Electronics*, vol. 9, no. 2, p. 274, 2020.

[10] S. H. Ebenuwa, M. S. Sharif, M. Alazab, and A. Al-Nemrat, "Variance ranking attributes selection techniques for binary classification problem in imbalance data," *IEEE Access*, vol. 7, pp. 24649–24666, 2019.

[11] I. Ezzine and L. Benhlima, "Technology against COVID-19 A blockchain-based framework for data quality," in *Proceedings of the 2020 6th IEEE Congress on Information Science and Technology (CiSt)*, pp. 84–89, Agadir-Essaouira, Morocco, June 2021.

[12] S. Singh, A. S. Hosen, and B. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed iot network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021.

[13] G. Karame and S. Capkun, "Blockchain security and privacy," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 11-12, 2018.

[14] A. S. Musleh, G. Yao, and S. M. Muyeen, "Blockchain applications in smart grid-review and frameworks," *IEEE Access*, vol. 7, pp. 86746–86757, 2019.

[15] H. Halpin and M. Piekarska, "Introduction to security and privacy on the blockchain," in *Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 1–3, Paris, France, April 2017.

[16] Z. Liehuang, G. Feng, S. Meng et al., "Survey on privacy-preserving techniques for blockchain technology," *Journal of Computer Research and Development*, vol. 54, no. 10, Article ID 2170, 2017.

[17] Y. Lu, "Blockchain: a survey on functions, applications and open issues," *Journal of Industrial Integration and Management*, vol. 3, no. 4, Article ID 1850015, 2018.

[18] A. Lamba, S. Singh, S. Balvinder, N. Dutta, and S. Rela, "Mitigating IoT security and privacy challenges using distributed ledger-based blockchain (Dl-BC) technology," *International Journal for Technological Research in Engineering*, vol. 4, no. 8, 2017.

[19] M. Attaran, "Blockchain technology in healthcare: challenges and opportunities," *International Journal of Healthcare Management*, pp. 1–14, 2020.

[20] J. H. Lee, "BIDaaS: blockchain-based ID as a service," *IEEE Access*, vol. 6, pp. 2274–2278, 2017.

[21] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "BlocHIE: A BLOCkchain-based platform for healthcare information exchange," in *Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, pp. 49–56, Taormina, Italy, June 2018.

[22] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–5, Montreal, Canada, October 2017.

[23] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-Health systems via consortium blockchain," *Journal of Medical Systems*, vol. 42, no. 8, 2018.

[24] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of Medical Systems*, vol. 42, no. 7, p. 130, 2018.

[25] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable Cities and Society*, vol. 39, pp. 283–297, 2018.

[26] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-based data preservation system for medical data," *Journal of Medical Systems*, vol. 42, no. 8, p. 141, 2018.

[27] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: efficient and secure medical data sharing via blockchain," *Journal of Medical Systems*, vol. 42, no. 8, 2018.

[28] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based E-health systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019.

[29] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: research challenges and opportunities," *Journal of Network and Computer Applications*, vol. 135, pp. 62–75, 2019.

[30] S. B. Wagh and J. K. Murthy, "Securing health care data for medical research using blockchain technology," *Journal of Advancement in Electronics Design*, vol. 1, no. 3, pp. 17–23, 2018.

[31] I. Abu-Elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-Alrazaq, "The benefits and threats of blockchain technology in healthcare: a scoping review," *International Journal of Medical Informatics*, vol. 142, Article ID 104246, 2020.

[32] V. Ramani, T. Kumar, A. Bracken, M. Liyanage, and M. Ylianttila, "Secure and efficient data accessibility in blockchain-based healthcare systems," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, pp. 206–212, Abu Dhabi, UAE, 2018 Dec 9.

[33] K. M. Khan, J. Arshad, and M. M. Khan, "Secure digital voting system based on blockchain technology," *International Journal of Electronic Government Research*, vol. 14, no. 1, pp. 53–62, 2018.

[34] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[35] H. Es-Samaali, A. Outchakoucht, and J. P. Leroy, "Blockchain-based access control for big data," *International Journal of Computer Networks and Communications Security*, vol. 5, no. 7, p. 137, 2017.

[36] H. Wang and Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," *Journal of Medical Systems*, vol. 42, no. 8, p. 152, 2018.

[37] K. Balasubramanian and M. Rajakani, "Implementation of algorithms for identity based encryption and decryption," *International Journal of Chemical Reactor Engineering*, vol. 1, no. 1, pp. 52–62, 2019.

[38] J. Sun, L. Ren, S. Wang, and X. Yao, "Multi-keyword searchable and data verifiable attribute-based encryption scheme for cloud storage," *IEEE Access*, vol. 7, pp. 66655–66667, 2019.

[39] L. Ismail, H. Materwala, and S. Zeadally, "Lightweight blockchain for healthcare," *IEEE Access*, vol. 7, pp. 149935–149951, 2019.

[40] U. Bodkhe, S. Tanwar, K. Parekh et al., "Blockchain for industry 4.0: a comprehensive review," *IEEE Access*, vol. 8, pp. 79764–79800, 2020.

[41] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *Proceedings of the 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1545–1550, IEEE, Opatija, Croatia, May 2018.

[42] Z. Ying, L. Wei, Q. Li, X. Liu, and J. Cui, "A lightweight policy preserving EHR sharing scheme in the cloud," *IEEE Access*, vol. 6, pp. 53698–53708, 2018.

[43] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: using blockchain for medical data access and permission management," in *Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD)*, pp. 25–30, Vienna, Austria, August 2016.

[44] A. Le Bris and W. El Asri, *State of Cybersecurity & Cyber Threats in Healthcare Organizations*, ESSEC Business School, Cergy, France, 2016.

[45] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A survey on blockchain for information systems management and security," *Information Processing & Management*, vol. 58, no. 1, Article ID 102397, 2021.

[46] D. R. Wong, S. Bhattacharya, and A. J. Butte, "Prototype of running clinical trials in an untrustworthy environment using blockchain," *Nature Communications*, vol. 10, no. 1, pp. 917-918, 2019.

[47] D. G. Glover and J. Hermans, "Improving the traceability of the clinical trial supply chain," *Applied Clinical Trials*, vol. 26, no. 11/12, pp. 36–38, 2017.

[48] I. A. Omar, R. Jayaraman, K. Salah, M. C. E. Simsekler, I. Yaqoob, and S. Ellahham, "Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts," *BMC Medical Research Methodology*, vol. 20, no. 1, pp. 1–17, 2020.

[49] A. Chawla and S. Ro, "Coronavirus (COVID-19)—is blockchain a true saviour in this pandemic crisis," 2020, https://thelivinglib.org/coronavirus-covid-19-is-blockchain-a-true-savior-in-this-pandemic-crisis/.

[50] M. M. Arifeen, A. Al Mamun, and M. Shamim Kaiser, "Blockchain-enabled contact tracing for preserving user privacy during COVID-19 outbreak," pp. 1–11, 2020, http://www.preprints.org.

[51] D. S. W. Ting, L. Carin, V. Dzau, and T. Y. Wong, "Digital technology and COVID-19," *Nature Medicine*, vol. 26, no. 4, pp. 459–461, 2020.

[52] T. P. Mashamba-Thompson and E. D. Crayton, "Blockchain and artificial intelligence technology for novel coronavirus disease-19 self-testing," *Diagnostics*, vol. 10, no. 4, p. 198, 2020.

[53] M. Shuaib, S. Alam, M. S. Nasir, and M. S. Alam, "Immunity credentials using self-sovereign identity for combating COVID-19 pandemic," *Materials Today: Proceedings*, 2021.

[54] I. Zhou, I. Makhdoom, M. Abolhasan, J. Lipman, and N. Shariati, "A blockchain-based file-sharing system for academic paper review," in *Proceedings of the 2019 13th International Conference on Signal Processing and Communication Systems (ICSPCS)*, pp. 1–10, IEEE, Gold Coast, Australia, December 2019.

[55] Nasdaq, *VeChain Announces Blockchain Vaccine Tracing Solution for China*, https://www.nasdaq.com/articles/vechain-announces-blockchain-vaccine-tracing-solution-china-2018-08-16, 2018.

[56] H. Hedera, "Acoer coronavirus tracker, powered by hedera hashgraph, now freely available to general public with added clinical trial data," *Hashgraph Hedera*, vol. 11, no. 2, pp. 1–6, 2020.

[57] I. Abunadi and R. L. Kumar, "BSF-EHR: blockchain security framework for electronic health records of patients," *Sensors*, vol. 21, no. 8, Article ID 2865, 2021.

[58] P. G. Shynu, V. G. Menon, R. L. Kumar, S. Kadry, and Y. Nam, "Blockchain-based secure healthcare application for diabetic-cardio disease prediction in fog computing," *IEEE Access*, vol. 9, pp. 45706–45720, 2021.