Arabian Journal for Science and Engineering (2020) 45:9895–9911
https://doi.org/10.1007/s13369-020-04950-4

REVIEW–COMPUTER ENGINEERING AND COMPUTER SCIENCE

Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System

Dounia Marbouh[1] · Tayaba Abbasi[2] · Fatema Maasmi[2] · Ilhaam A. Omar[1] · Mazin S. Debe[2] · Khaled Salah[2] · Raja Jayaraman[1] · Samer Ellahham[3]

Received: 12 June 2020 / Accepted: 17 September 2020 / Published online: 12 October 2020

Abstract
The sudden development of the COVID-19 pandemic has exposed the limitations in modern healthcare systems to handle public health emergencies. It is evident that adopting innovative technologies such as blockchain can help in effective planning operations and resource deployments. Blockchain technology can play an important role in the healthcare sector, such as improved clinical trial data management by reducing delays in regulatory approvals, and streamline the communication between diverse stakeholders of the supply chain, etc. Moreover, the spread of misinformation has intensely increased during the outbreak, and existing platforms lack the ability to validate the authenticity of data, leading to public panic and irrational behavior. Thus, developing a blockchain-based tracking system is important to ensure that the information received by the public and government agencies is reliable and trustworthy. In this paper, we review various blockchain applications and opportunities in combating the COVID-19 pandemic and develop a tracking system for the COVID-19 data collected from various external sources. We propose, implement, and evaluate a blockchain-based system using Ethereum smart contracts and oracles to track reported data related to the number of new cases, deaths, and recovered cases obtained from trusted sources. We present detailed algorithms that capture the interactions between stakeholders in the network. We present security analysis and the cost incurred by the stakeholders, and we highlight the challenges and future directions of our work. Our work demonstrates that the proposed solution is economically feasible and ensures data integrity, security, transparency, data traceability among stakeholders.

Keywords Blockchain · COVID-19 · Coronavirus · Ethereum · Trusted oracles · Smart contracts · Traceability · Tracking system · Transparency

1 Introduction

The coronavirus (COVID-19) outbreak in late 2019 caused a global health emergency around the world [1]. In just over three months, the number of coronavirus new cases has escalated to more than a million worldwide. The rapid transmission of the virus leads to new cases being reported globally by the hour. Simultaneously, the number of deaths and infections continues to rise quickly. Consequently, the COVID-19 pandemic has enforced lockdowns and social distancing guidelines affecting global economies negatively. It has led to the cancelation of many important world's activities, including sporting events such as the Tokyo Olympics [2] and Dubai Expo [3]. As a result, government officials and scientists across the globe have been rigorously working toward developing a cure and predicting the potential growth trajectory of the virus since the first few cases that were reported to the World Health Organization (WHO). In addition to forecasting the casualties and growth of COVID-19 cases, many reports also count the active and recovered cases collected from national and state government health agencies along with local media reports.

In fact, every day, a new set of baffling data points are reported concerning the number of positive and negative tests, patients hospitalized, deaths, hospital beds occupied,

✉ Khaled Salah
khaled.salah@ku.ac.ae

1 Department of Industrial and Systems Engineering, Khalifa University, Abu Dhabi 127788, United Arab Emirates

2 Department of Electrical and Computer Engineering, Khalifa University, Abu Dhabi 127788, United Arab Emirates

3 Heart and Vascular Institute, Cleveland Clinic Abu Dhabi, Abu Dhabi, United Arab Emirates

ventilator shortfalls, etc. These numbers allow the officials and public to track the progress of COVID-19 in real time and as they become available, making it a data-driven pandemic [1]. On the other hand, these numbers pose a major problem as decisions based on such data are often imperfect and incomplete. Data verification and validity in pandemic management are crucial for conclusions and recommendations given to the public that are based on recorded or reported data statistics [4]. Thus, the introduction of tracking apps becomes necessary and valuable to help prevent the spread of this virus and maintain data quality and integrity. Furthermore, tracking valid data is vital to monitor the progress of the pandemic. Tech giants, researchers, and healthcare officials started using contact-tracing mobile apps that use Bluetooth-based proximity tracing or geolocation tracking functionality to help track COVID-19 cases [5, 6]. Several organizations have even developed map-based dashboards to track information. Understanding the dynamics of the pandemic requires good data to predict how fast the disease spreads, whether the countermeasures are effective or not, and the impact it has on the lives of people. However, data available online may not be perfect as it is susceptible to data manipulation.

Hence, innovative technologies such as deep learning, machine learning, artificial intelligence (AI), and blockchain could help combat the crisis. In particular, blockchain technology has the potential to revolutionize various industries, including finance, supply chain, and the healthcare sector. Blockchain is a decentralized technology with distinct in-built features such as impenetrable information infrastructure, transparency, and cryptographic encryption tools. It is a distributed ledger containing a chain of blocks. Blockchain's decentralized platform is tamperproof due to its underlying cryptographic technology, which is used to authenticate participants in the network. Moreover, it requires a lot of resources to be able to modify transactions added to the blockchain network because once a transaction is validated and verified, then it gets chained to previous transactions with a unique hash. Hence, manipulating one transaction would change this hash, and all members would be alerted making it almost impossible to update or delete data. Furthermore, data stored on the blockchain are made available to all members of the network, ensuring transparency among participants.

Blockchain technology has several potential use cases that can help tackle the current pandemic crisis. It can be used to simplify the clinical trial processes for vaccines and drugs, raise public awareness, transparently track donations and fundraising activities, and act as a reliable data tracker. In this paper, we focus on the data tracking use case as blockchain enables confidentiality and trust to be maintained in data collection and reporting. COVID-19 data may be collected from numerous trusted sources such as WHO, the Center for Disease Control (CDC), and the Institute for Health Metrics and Evaluation (IHME). As a result, building a decentralized tracking system that retrieves publicly available information and data from authoritative sources to display on decentralized applications and dashboards is vital as this platform imposes security restrictions and data privacy.

It should be noted that building a blockchain platform to track COVID-19 transmission is essential, as many of the currently developed systems are prone to hacking and cybercriminals. Table 1 highlights the benefits of implementing a blockchain-based solution over a traditional centralized solution in various aspects, including data handling, quality assurance, fault tolerance, etc.

For instance, the World Economic Forum highlighted that hackers are using coronavirus maps to spread malware [7]. These attackers impersonate interactive maps that track the spread of the disease. By doing so, they trick users into giving their sensitive information such as user names, passwords, and credit card numbers. The hackers then use this private datum to sell it on the deep web or financially exploit people. In addition, some hackers use fraudulent mobile apps as fake coronavirus tracker apps to trap users into paying a ransom to avoid leaking their social media information [8]. Furthermore, the public is continuously exposed to misinformation and spams of fake news. Blockchain technology can eliminate the problems faced by centralized data systems. It introduces immutability and data provenance while removing single point of failure in the system. Therefore, with blockchain data tracker, any user with Internet access can learn, in a few short clicks, real-time information about the COVID-19 virus in a secure and trustable manner. The primary objectives of this paper are to review various use cases of blockchain technology for COVID-19 and develop a blockchain-based trusted data tracking system. The main contributions of this paper are summarized as follows:

- We review various blockchain applications and opportunities for combating the COVID-19 pandemic.
- We propose a framework along with the algorithms that define the working principles of the proposed blockchain-based tracking system, provided a detailed sequence diagram summarizing stakeholder interactions in the blockchain-based tracking system, tested, and validated various scenarios of the overall system functionalities.

The remainder of this paper is organized as follows: Section II details a brief background on the COVID-19 pandemic and explains the significance of utilizing blockchain platforms for handling information during outbreaks. Section III provides insights into how blockchain technology can be used in various uses cases related to the COVID-19 outbreak. Section IV details the system methodology and design architecture of the proposed system, while the implementation is discussed in Section V. Section VI demonstrates the results of testing the proposed solution. Furthermore, Section VII

Table 1 Comparison between using a traditional centralized platform and a blockchain platform

Aspects	Traditional centralized platform		Blockchain platform	
Data handling	Supports four primary operations: create, read, update, and delete	×	Only read and write options are available	✓
Authority	Controlled by the administrator (centralized)	×	Decentralized even in private blockchains	✓
Data integrity	Data can be altered	×	Data are immutable and auditable	✓
Data privacy	High chances of malicious cyberattacks	×	Data are stored using cryptography technology	✓
Transparency	Databases are not transparent	×	Data are stored in a distributed network	✓
Quality assurance	Administrators are needed to authenticate data (data provenance not applicable)	×	Data can be tracked and traced right from its origin using cryptography technology	✓
Fault tolerance	High risk of single point of failure	×	Distributed ledger is highly fault-tolerant.	✓
Cost	Easy to implement and maintain as it is an old technology	✓	Uncertainty in the operating and maintenance costs	×
Performance	Fast (more transactions processed per second) and offer great scalability	✓	Can handle minimal transactions per second, and scalability is a challenge as blockchain is at its developing stage	×

details the cost and security analysis of our proposed solution, and Section VIII presents the conclusions of our work.

2 Background

In this section, we provide background information related to the COVID-19 pandemic, and we explain the importance of adopting blockchain technology in combating this crisis.

2.1 COVID-19 Pandemic

Coronavirus disease (COVID-19) is an infectious, acute, respiratory illness caused by a novel coronavirus SARS-CoV2. Coronaviruses are a family of viruses that can cause illnesses such as the common cold, severe acute respiratory syndrome (SARS), and the Middle East respiratory syndrome (MERS) [9]. Early COVID-19 cases were linked to a seafood market in Wuhan, where wild animals were traded, suggesting that the virus was primarily transmitted from animals to humans [10]. Transmission is believed to occur through respiratory droplets from coughing and sneezing, as with other respiratory pathogens. Virus discharged in respiratory secretions can infect other individuals via direct contact with mucous membranes. The virus can also persist on surfaces to varying durations and degrees of infectivity [11]. In March 2020, the World Health Organization (WHO) declared the COVID-19 outbreak a pandemic [12]. As of June 3, 2020, more than 6.5 million infection cases have been reported across 190 countries and territories, resulting in more than 384,000 deaths [13]. Figure 1 summarizes some of the pandemic's symptoms, preventive measures, mitigations efforts, and global impact in which each is explained below:

2.1.1 Symptoms

Individuals infected with COVID-19 have had a wide range of symptoms reported, ranging from mild symptoms to severe illness. Symptoms may appear two to 14 days after exposure to the virus. The symptoms and signs of COVID-19 include, but not limited to: fever or chills, cough, shortness of breath or difficulty in breathing, fatigue, muscle or body aches, headache, loss of taste or smell, sore throat, congestion or runny nose, nausea or vomiting, and diarrhea [14]. Some people may have only a few symptoms, while others may have no symptoms at all. Older adults and people who have serious underlying medical conditions like heart or lung disease, diabetes, chronic kidney, or liver disease are at a higher risk of developing more serious complications from COVID-19 illness. Complications can include pneumonia, organ failure, heart problems, unexplained blood clots, acute kidney injury, multiple organ failure, additional viral, and bacterial infections leading to death [12].

2.1.2 Preventive Measures

There is currently no vaccine to prevent COVID-19 disease or medication from treating it. Therefore, preventive measures are crucial in light of the spread of the virus to reduce the risk of encountering it. Among the preventive measures cur-

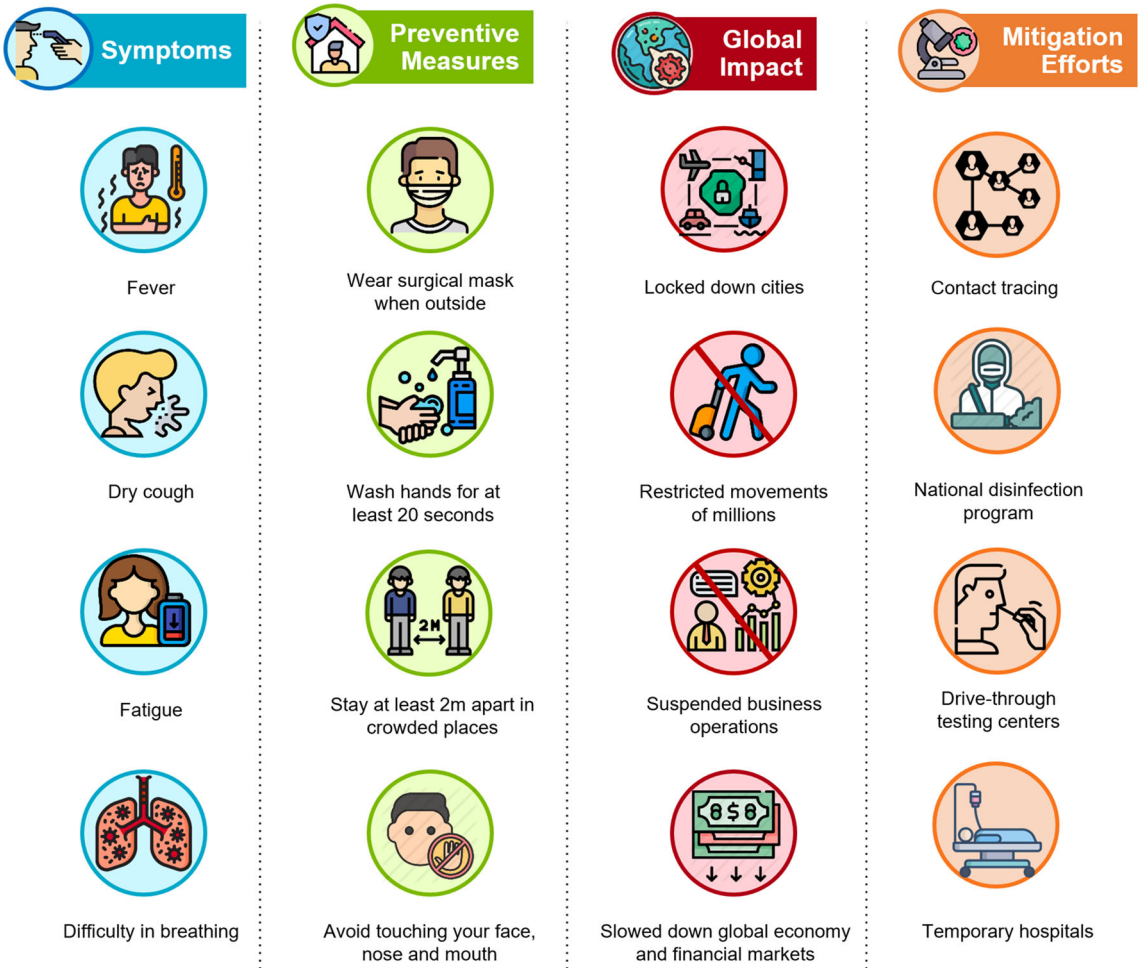


Fig. 1 Summary of COVID-19 symptoms, preventive measures, its global impact, and mitigation efforts

rently put in place: washing hands with soap or alcohol-based hand wash for at least 20 s, practicing social distancing and keeping a distance of at least 2 meters apart, wearing surgical masks, and avoiding touching the face, mouth, eyes, and nose [9] [12]. Other preventive measures include cleaning high-touch hard surfaces often, using regular household cleaners, covering coughs and sneezes, staying home, and monitoring one's health. People are advised to be alert for symptoms and watch for fever, cough, shortness of breath, or other symptoms of COVID-19 to prevent the spread of the virus and transmitting it to others [15, 16].

2.1.3 Global Impact

The virus is not only affecting the health of people but also impacting their day-to-day lives and the global economy. Many countries have declared restrictive measures, such as lockdown and stay at home orders, to contain and mitigate the pandemic. As a result, more than 3.9 billion people, or half of the world's population, had their movement restricted by early April [17]. The lockdown also implied that most factories, markets, and businesses are to be temporarily closed, most public transport suspended, and construction work halted [18]. As a result, COVID-19 not only has implications on people's health but significantly impacted businesses and the global economy. Due to the suspension of many businesses, the economic slowdown was profound, and the damage was serious. The economic damage caused by COVID-19 includes supply chain interruptions, lost tourism, spiking unemployment, defaulted loans, the likelihood of major government bailouts, and food crisis [19, 20].

2.1.4 Mitigation Efforts

In addition to the preventive measures which individuals can follow, there have been mitigation efforts put in place by governments and organizations to contain the virus. For instance, several applications across the world have been built to track COVID-19 patients and tracing their contacts. Accurate identification of cases, contact tracing, and isolation can

hardly be performed with conventional methods, and the use of targeted phone apps could highly improve the efficiency of these processes [21]. For instance, a number of leading public health authorities have built several smart solutions that detect cases of COVID-19 and control its spread. Some of these smart solutions are mobile contact-tracing applications that can detect whether an individual has been in contact with someone infected with COVID-19. These applications use the Bluetooth technology that enables users to exchange anonymized IDs stored in an encrypted form so that their health authorities can easily contact individuals at risk. These applications can also warn their users when an infected person is nearby, thereby preventing possible infection. They can also track whether an infected individual is respecting the social distancing guidelines [22]. One example of these applications is ALHOSN UAE app that can be downloaded free of charge while ensuring a high degree of privacy protection to its users, thanks to artificial intelligence and other tools [23]. In addition to the initiated applications, the United Arab Emirates (UAE) has implemented a national disinfection program that entails complete sterilization of all public utilities, public transport, metro services, and roads. The UAE has also stepped up its efforts in testing patients for COVID-19 by opening several drive-through centers across the country [24]. In addition to the disinfection program and drive-through testing centers, the UAE, like many other countries, had recourse to other mitigation strategies such as building field hospitals, imposing travel bans, canceling public activities and events, suspending places of worship and their facilities, calling for the postponement of social events, closing entertainment venues, closing public parks and beaches, and installing thermal detection systems at the entrances of malls and public areas [25].

2.2 Blockchain Technology

People from all over the world are working hard to find the best solutions concerning the development and testing of vaccines, preventing the spread of infection and quick identification of viral carriers since coronavirus is extremely contagious. In fact, blockchain potential use cases in healthcare vary accordingly to satisfy different requirements, such as data sharing, security, and data access. Other examples include blockchain platforms designed for clinical trials or precision medicine. In the current sense of epidemic management, blockchain is evolving as a crucial technology solution in providing a transparent, reliable, and low-cost solution to facilitate successful decision making, which could effectively result in contributing to quicker intervention during this crisis. Blockchain is now showing enough opportunities to become an integral part of fighting against COVID-19 as it would enable efficient tracking and monitoring solutions, ensure a transparent supply chain of vital products and donations, and secure payments. This is possible because blockchain comprises a chronologically ordered list of encrypted signatures, a secure distributed ledger containing permanent transaction records that are shared by all members in the network [26]. Moreover, adopting blockchains and public ledgers maximizes cost savings by eliminating intermediaries that handle manual transactions.

The blockchain platform consists of mainly three components, which are data block, distributed ledger, and consensus algorithm. Each component is explained below as follows:

2.2.1 Data Block

It can be described as a sequence of blocks interconnecting each newly updated block to its previous block until it gets linked back to its genesis block to create a secure chain. This prevents any risk of modification as each block is strongly linked to the previous one using a hash label, which builds a robust link between blocks [26].

2.2.2 Distributed Ledger

It is also known as a database that records and stores transactions generated by users. Each transaction contains a unique cryptographic signature decoupled with a timestamp, thereby making the ledger resistant to alterations. Furthermore, this ledger is shared across all members of the network simultaneously so that users are updated in real time.

2.2.3 Consensus Algorithm

No entity should be able to control the process of transacting a block over the chain so that each block is managed by all members who share equal rights to overcome security problems such as double-spending. This is achieved through the process known as consensus. From the blockchain's point of view, the consensus process establishes an agreement among entities regarding the validation of each data block. This is achieved by nodes joining in the mining process and competing with one another to verify the block to receive a fee as a reward in return for their mining effort. For example, Bitcoin uses a proof-of-work (PoW) algorithm to manage its transactions, while Ethereum uses proof-of-stake (PoS) algorithm. Also, there are various other algorithms as well, such as the Byzantine faulty tolerant (BFT) algorithm [26].

Unlike traditional database systems, blockchain technology utilizes its inherent properties to ensure transparency, immutability, and accuracy during data collection and data management transactions. Moreover, blockchain enables two or more parties to interact easily with one another in a digital environment and permits them to exchange money in the absence of a central authority. In many aspects, blockchain

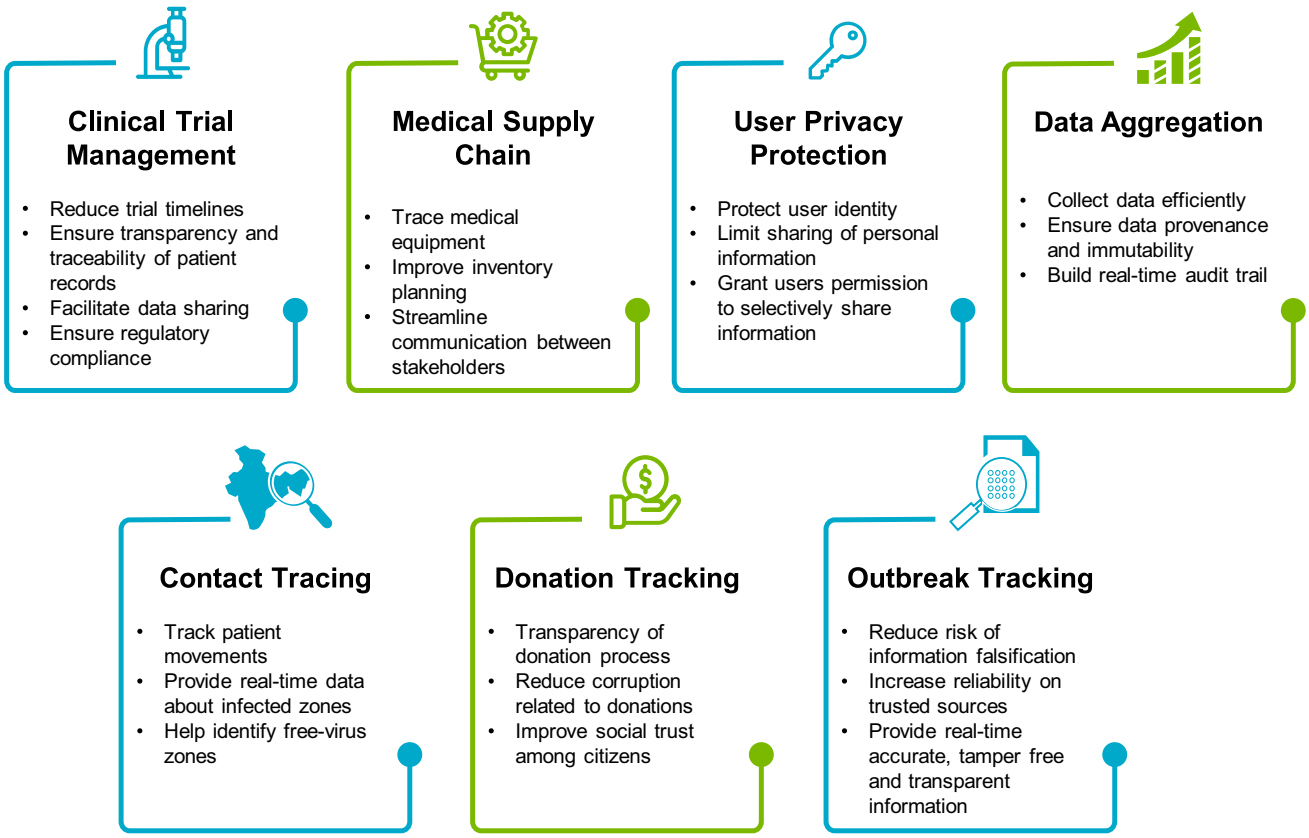


Fig. 2 Blockchain-based use cases for fighting COVID-19 pandemic along with its benefits

is transforming many industries by enabling value exchange, openness, and trust across business ecosystems. It is used in many industries such as energy, law, tourism, supply chain, banking, and healthcare. In particular, it has proved to be beneficial in the healthcare sector as it promises to enhance healthcare data privacy and secure data management. As a result, it is immensely suitable for tackling coronavirus-related healthcare problems.

3 Blockchain-Based Use Cases for COVID-19

In this section, we provide a comprehensive literature review on the prominent blockchain-based uses cases for combating the COVID-19 pandemic. Blockchain technology is capable of enhancing the healthcare sector in various areas that are affected by this outbreak, including improvements to clinical trials, managing supply chain operations, tracking donations, etc. The potential uses cases are summarized in Fig. 2.

3.1 Clinical Trial Management

Every product should be thoroughly tested to demonstrate its safety and efficiency and note possible side effects in a clinical trial, to bring new medications and medical devices into the market. Clinical trials mainly take place in four phases, out of which Phase III trials incorporate the greatest number of participants or patients, making them challenging and resource-demanding. For clinical trials to operate efficiently, they require a management system that is fair and transparent. Besides taking care of the considerable amount of information collected from each phase, the clinical protocol should be cost-proficient, regulatory compliant, auditable, safe, fast, and transparent to all stakeholders in the network [27]. The use of digital technologies and innovations can help ensure the safety and privacy of participants while reducing trial timelines. In particular, blockchain technology can aid researchers and clinicians in recording clinical data in real time as they become available. This improves accuracy, encourages data sharing, and ensures regulatory compliance [28, 29]. It can also track and keep tally of who has accessed which part of the datasets, thus creating an audit trail that improves privacy and data security [30].

Civitas, an app launched by a Canadian startup that engages in blockchain solutions, assists various government officials and local authorities in controlling the COVID-19 outbreak [31]. This app can be beneficial in managing clinical trials related to COVID-19 as it associates each person's

ID with its corresponding blockchain records anonymously without disclosing their identity. It can find out whether a person has left his home or not. This is essential as it helps in minimizing the spread of this virus. In addition, it can allow doctors to track the progress of their patients and monitor their symptoms for any side effects. In return, these doctors can send them their report with regard to the medication procedure that is to be followed.

3.2 Medical Supply Chain

The COVID-19 emergency has caused significant interruptions across worldwide supply chains. Two predominant factors play a vicious job: numerous factories closed because of safety and hygienic concerns, and there is an unparalleled demand for specific products, in particular, PPE and medical supplies. Many users are pressured to secure supplies from unknown origins or quality due to the increased demand. Lengthy supply chains cause excessive obscurity, which makes it hard to calculate and plan supply. Blockchain is the best option for supply chains as it can connect all stakeholders into one supply chain network universal source while showing transparency and being able to securely break down data silos. Therefore, huge numbers of the blockchain arrangements during the COVID-19 pandemic are in supply chain management [32]. Blockchain accelerates the validation procedure by expelling third-party delegates and innate delays in handling and processing operations. The advantages include quicker handling and processing time, reduced costs, lower operational risks, and faster settlements for all parties included. The VeChain platform is ensuring that new KN95 masks imported from China are credible and reliable while working inseparably with production offices and facilities [33]. From codes to packages, materials, all tasks related to vaccine production are noted and kept in allocated ledgers.

3.3 User Privacy Protection

In these troublesome times, the balance must be obtained between data collection and privacy assurance. Blockchain can be utilized to collect and examine patient data more productively and screen patients' movements to ensure the necessary social distancing requirements while protecting their identity simultaneously. There is no focal power, and clients are given control of their information in a blockchain platform. They can specifically share data that are significant for coronavirus relief efforts while ensuring their privacy and identity remains protected. In addition to this, governments and healthcare associations can increase data collection through coronavirus tracking, while clients can be guaranteed that their data will not be exposed or shared. A group of privacy specialists across Europe devised a blockchain-based framework for COVID-19 contact tracing utilizing Bluetooth. Moreover, German tech scale-up MYNXG has made a blockchain-based arrangement that uses cell phones while safeguarding client security [32].

3.4 Data Aggregation

To effectively respond to the pandemic, a key territory of opportunity is in the assortment, accumulation, and access to information necessary for the tracking of the infection, deciphering trends, and administering research. Blockchain provides the possibility of guaranteeing data accuracy by its capability to verify and store immutable real-time data. The framework of Blockchain acts as a base for new developing researches while permitting organizations and associations to share their information with innovators, scientists, and researchers to test and incorporate this information into new devices and solutions. Utilizing a blockchain-fueled platform empowers compliance management, data proprietorship, and auditability to grant flexible sharing all through different managerial levels. MiPasa, worldwide scale control and correspondence system controlled by blockchain innovation, which assists with gathering, collating, and studying data about the virus's spread and containment, was launched by WHO while collaborating with significant innovation organizations and governments. MiPasa is an asset that has expectations to help the public health officials, the scientific and business network, and people in general [34].

3.5 Contact Tracing

Contact tracing helps avoid the spread of a virus through pro-actively identifying, advising, and, where necessary, quarantining individuals who are at a higher risk than others. Using this tracing technique is useful, and smartphones aid in making the system more effective only if privacy and other issues are addressed. Governments and healthcare organizations engage in contact-tracing activities to monitor patients. However, using blockchain at every step increases the accuracy and reliability of data collected. Blockchain technology can monitor patient movements and offer updates related to affected areas in real time. Furthermore, it can be used to detect virus-free zones to inform the public about safe areas. Remember that this information can be obtained from monitoring providers using a combination of technologies such as AI and geographical information systems (GIS). Blockchain can, therefore, offer practical approaches to protect populations from the spread of the virus by complying with quarantine standards.

Coalition is a free app in the USA that users can monitor themselves if they are sick [35]. Other users are notified of potential interactions with an infected person and are encouraged to provide proper health follow-up. The solution uses Bluetooth-enabled cryptography technology to track meet-

ings and generate anonymous random IDs to protect the identity of the user with all data locally saved on a user's phone. In Europe, Africa, and Asia, similar solutions were explored. Also, the Public Health Blockchain Consortium (PHBC) announced the launch of a blockchain for systematic tracking, continuous and adequate monitoring in virus-free zones to ensure that an infected person does not enter this area [36].

3.6 Donation Tracking

The pandemic situation has presented severe hardships to humanity. To alleviate the challenges, several philanthropists have donated products and financial aid, and the entire donation process that comprises of warehousing, logistics, and distribution can be stored in the blockchain. Using this technology, the donor can verify the transfer process and receipt of donated money precisely and transparently. Consequently, blockchain will eliminate intermediaries, save costs, minimize donation exploitation, and boost social cohesion. Motivating donation practices helps to aid people facing medical or economic difficulties due to the spread of infectious diseases [37]. Hyperchain is a blockchain-based network that aims to counter the coronavirus outbreak by specializing in uniquely tracking donations [38]. This platform assists governments and healthcare organizations in the donation process for infected victims. This network ensures the donation process remains unchangeable, efficient, and traceable. It provides a transparent platform that allows donors to monitor where their funds were used. Through presenting proof of need and evidence of receipt, the blockchain charity platform ensures that the donations reach intended groups directly without intermediaries.

3.7 Outbreak Tracking

Blockchain removes the need for outsiders because of its decentralization feature, which can substantially reduce the occurrence of data modification and fictitious news and increase the reliability of information for the general population and experts in healthcare. Fraudulent data contributes to chaos and causes economic damage and psychological distress. Therefore, storing news and facts on a blockchain database prevents its modification and makes it traceable, thereby making it easier to avoid fake data and information. Blockchain technology provides a suitable coronavirus tracking platform as data handled through such a network are reliable, accurate, tamper-free, and transparent. Consequently, governments can update better on the status of coronavirus pandemic for improved planning and management, such as forecasting the outbreak, isolating possible territories, and tracking the spread of the infection. Acoer has created a HashLog dashboard from an ever-growing set of public data that allows individuals to understand the extent of infection spread and pattern over time [39]. Moreover, information collected from the CDC, WHO, and trends from social networking websites helps the Acoer Coronavirus HashLog to make data visualization models associated with clinical trial data [39].

In this paper, our primary focus is on leveraging smart contracts and oracles to validate data reporting, thereby preventing the spread of false information. This particular use case is important as there is a sudden surge in various social platforms claiming misinformation. Thus, there is a need to authenticate and monitor information and data communicated publicly. Also, it is important to track the source of the message to identify users who are engaged in spreading conspiracy theories, rumors, inflammatory remarks, and fake news. Thus, it is highly recommended to use a public blockchain platform to validate the messages as it enables all users to digitally sign their message before it gets added to the blocks making it easier to identify the source of information.

4 Proposed Blockchain-Based Data Tracking Solution

We propose a blockchain-based solution and system for tracking data relevant to COVID-19. The system connects decentralized applications (DApps), dashboards, smart contracts, oracles, and web feed sources within the same decentralized Ethereum network, as illustrated in Fig. 3. The proposed framework collects data from various web feed sources (WHO, CDC, IHME, etc.) via oracles.

The proposed system components are described below:

4.1 Ethereum Smart Contract

The second-generation blockchain platform, such as Ethereum, enables smart contracts that act as software agents to be deployed in the blockchain network [40]. Smart contracts can automatically execute the terms of the agreement and verify credible transactions without interference from third parties [41]. In our proposed solution, the blockchain system consists of three smart contracts, as shown in Fig. 3.

4.1.1 Registration Contract

This smart contract includes information about web sources and any participating stakeholders.

4.1.2 Reputation Contract

This smart contract deals with assigning a reputation score for an oracle derived from the evaluation of web sources used to retrieve data. The total reputation score of an oracle consists

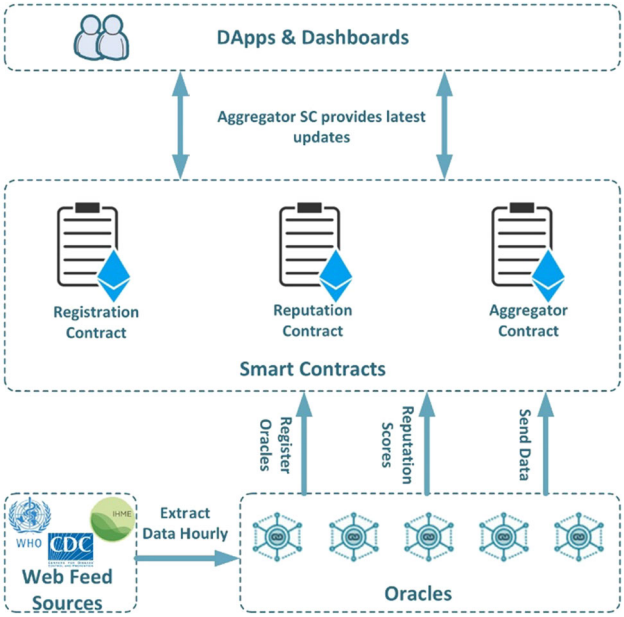


Fig. 3 System overview of a blockchain-based data tracking process using smart contracts and trusted oracles

of the credibility of the web source along with the reputation score a user has assigned to it. The reputation is, therefore, positively affected by honest and reputable websites and negatively affected by malicious ones. The reputation score of an oracle depends on its trustworthiness. If the trustworthiness of an oracle is above the threshold, its reputation score is calculated, as shown in Eq. 1.

$$Cr(A) = \frac{\text{RepScore}(A) \times T}{4 \times \text{Adj}F} \tag{1}$$

where $Cr(A)$ represents the total reputation of an oracle in which A is the address of the oracle. RepScore(A) is the reputation score of the web source, and T represents the trustworthiness of the oracle, which is the difference between the value reported by the oracle and the value computed by the smart contract, while Adj$F$ is the adjusting factor, i.e., how harsh or lenient we want to be with nodes reporting wrong values.

However, if the trustworthiness of the oracle is below the threshold, the reputation of an oracle is computed using Eq. 2.

$$Cr(A) = \frac{\text{RepScore}\ (A) \times T}{4 \times (10 - \text{Adj}F)} \tag{2}$$

4.1.3 Aggregator Smart Contract

This smart contract is concerned with retrieving the latest updates and sending them to front-end users. It will receive updates only from credible oracles with a high reputation score, while it drops updates from oracles with low scores. The reputation scores provided for every oracle are then grouped into clusters. The cluster head can be determined either by taking a member of the cluster that is approximately in the middle or considering the centroid of the values. Once the most reputable cluster is determined, the updates of the latter are sent to the front-end users through the DApps and/or dashboards.

4.2 Trusted Oracle Network

Oracles act as third-party services that feed smart contracts with external data as they are unable to fetch external information on their own. Data feeds in web APIs are usually not deterministic like blockchain and smart contracts. Therefore, oracles act as a bridge that is capable of processing external and non-deterministic information into a format that can be understood and executed by smart contracts. It should be noted that obtaining information from a single oracle is not reliable; therefore, multiple oracles are needed to report news and information feed to the smart contract. Then, smart contract validates and checks the reported data from multiple oracles to verify the trustworthiness of the reported data. This eliminates the need for trusting only one source, avoiding the occurrence of a single point of failure.

4.3 Message Sequence Diagram

A sequence diagram shows the interactions between different stakeholders while simultaneously showing various events that are triggered in the sequence of functions that are triggered within the smart contract. Each participant in the network holds an Ethereum address that enables them to interact with each other by calling functions within the smart contract. Figure 4 illustrates the sequence flow between different stakeholders, from extracting data from web sources to providing the latest updates to DApps or dashboards.

Initially, the oracle sources are registered in the registration smart contract to keep information about our stakeholders. This occurs by executing the function called *RegisterOracle(Address)*. Then, the aggregator smart contract would invoke the function *computeReputation(Address)* to check the trustworthiness, credibility, and reputation of registered oracles.

Afterward, the oracles extract data from the registered web sources by executing the function *inputOracle(infect, recover, death)*. Once the oracles extract the required attributes: number of recoveries, infections, and deaths, the extracted data go to the aggregator smart contract. The contract then approves the most reputable cluster of data that will be provided to the DApp front-end users by invoking *CalculateStatistics()* function. Through the use of these apps, front-end users would be able to access real-time data about

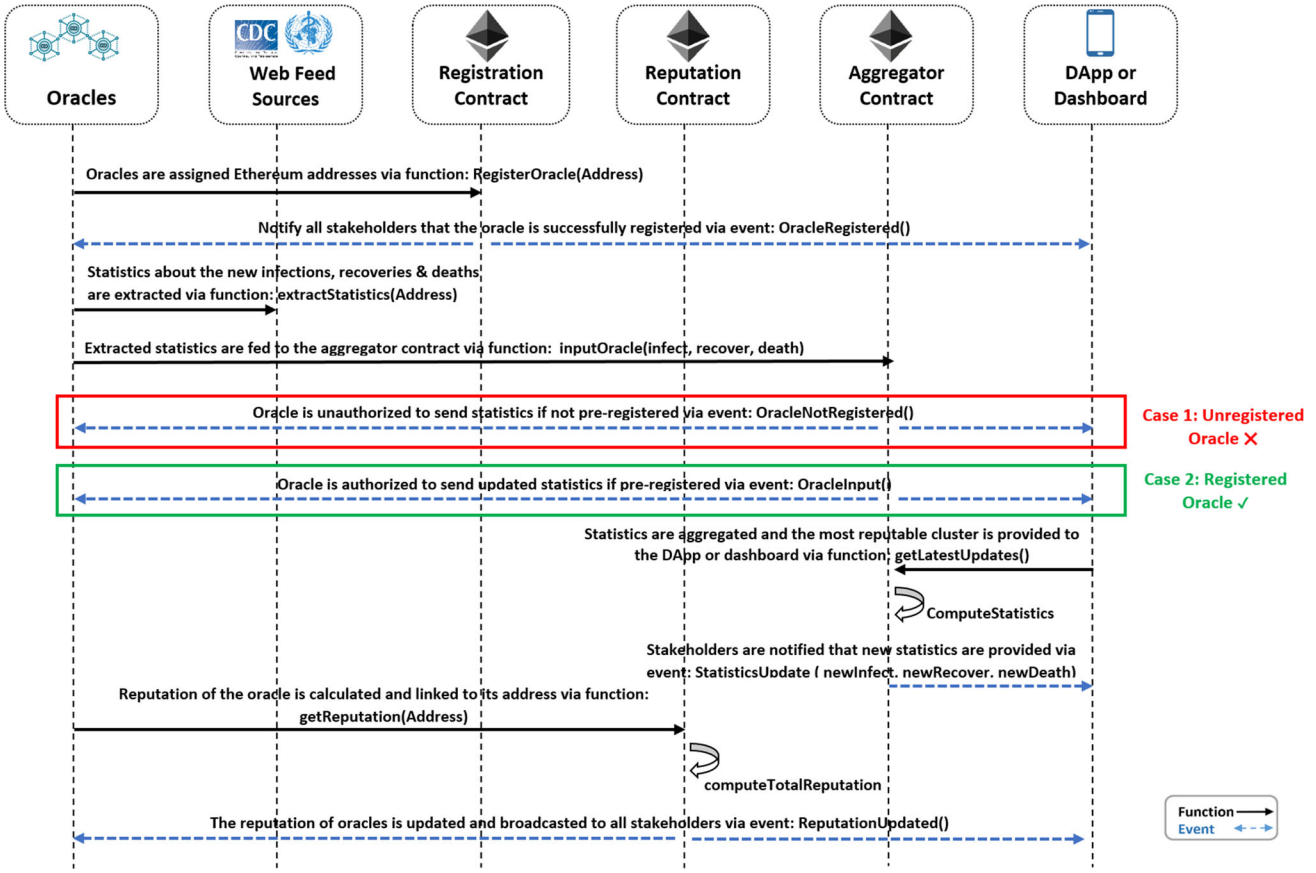


Fig. 4 Sequence diagram showing the function calls and events in a blockchain-based COVID-19 tracking system

the new recoveries, infections, and deaths in a trusted and reliable manner.

5 Implementation

We present and discuss the algorithms for implementing the blockchain-based COVID-19 tracking system that captures the working principles of our proposed solution leading to the development of the smart contract. The smart contracts were written in Solidity, which is a widely used language for Ethereum smart contracts. Compilation and execution of the contract were achieved through the use of Remix IDE, which is a browser-based compiler with an embedded debugger used for alerting and alarming the user with error notifications and warnings accordingly.

Firstly, oracles are assigned Ethereum addresses to be able to interact with the smart contracts as they act as a gateway between the blockchain platform and external data. This datum will comprise of the statistics related to the number of infected and recovered cases and deaths obtained from reliable resources. This registration process is handled by the registration smart contract.

The aggregator smart contract has the additional functionality of the registration smart contract that is necessary to register oracles. Firstly, oracles are assigned Ethereum addresses to be able to interact with the smart contract as they act as a gateway between the blockchain platform and external data. This datum will comprise of the statistics related to the number of infected and recovered cases and deaths obtained from reliable resources.

Algorithm 1 describes how only trustworthy sources are used by registering oracles under the function *registerOracle()* to check whether the address is registered or not. If the oracle is not registered, then this function is responsible for registering the oracles by appending its Ethereum address to the list of the oracles of different resources. After the process of registration, the oracle is then given an initial credibility score of 80, which can later vary based on the data provided by this oracle. After the successful registration of oracles, they are now eligible to feed the smart contract with data extracted from online sources such as IHME and CDC using the *oraclInput()* function, as shown in Algorithm 1. Then, the process of data aggregation begins by incrementing the infected, recovered, and the dead counts corresponding to that oracle.

This is followed by updating the oracle records while simultaneously triggering events to notify stakeholders with the latest updates.

Algorithm 1: Oracle Registration and data input

Input: *oracleAddress, infected, recovered, dead*

oracleAddress is the Ethereum Address of oracle that update data to smart contract.
infected, recovered, and *dead* patients since last update.
Verify if the oracle exists
if *oracle already exists* **then**
    Oracle is allowed to transfer data
else
    Initialize oracle information.
    Append the oracle to list of oracles
end
`/* Oracle Input */`
Increment number of infected, recovered, and dead as reported by this oracle.
Update the oracle records.
Announce the latest oracle updates using an event.

Then, the submitted data are processed and grouped into clusters, as demonstrated in Algorithm 2. It would ensure that information submitted is verified by using a loop to go over each registered oracle. The clustering process takes place by comparing the input data with the data that already exists in the clusters. If the new data are similar to one of the available clusters, then the oracle is added to that particular cluster accordingly else a new cluster is created. Then, the appropriate cluster is chosen by selecting the cluster with the highest number of oracles. It should be noted that the credibility of oracles is also taken into account when selecting the cluster. However, for this paper, the credibility value was fixed for simplification. Finally, the centroid of the trustworthy cluster will be found and used to update the ledger.

Algorithm 2: Update Coronavirus Statistics

clusters include similar statistics provided by different clusters.
averageInfected, averageRecovered, averageDead are the average statisics as recorded by all oracles.
foreach *oracle* **do**
    if *oracle input is similar to one of the available clusters* **then**
        Append the oracle to the appropriate cluster.
        Append the reputation score of the cluster.
    else
        Create a new cluster for the current oracle.
    end
end
Obtain the most trustworthy cluster. Statistics are updated to the average value as provied by memebers of this cluster.

Once the smart contract has aggregated the input from all oracles, the reputation of the oracles is to be updated. The input of those oracles is compared to the computed values of the infected, recovered, and deceased cases. As shown in Algorithm 3, the trustworthiness factor is computed, which is reflected in the change of the reputation scores of the oracle. If the oracle is within the most reputable cluster, it is considered a credible source of input, and its reputation increases. After many iterations, the most dependable oracles are given more weight when computing the final statistics.

Algorithm 3: Update oracle reputation scores

Input: *oracleAddress*

oracleAddress is the Ethereum Address of the oracle whose reputation is being computed.
Get latest update reported by the oracle.
Compare input of oracle with the value calculated by aggregator SC to get the trustworthiness factor.
if *trustworthiness factor* > *threshold* **then**
    Oracle reputation is incremented as shown in Equation 1.
else
    Oracle reputation is decremented as shown in Equation 2.
end
Update oracle records.

The code was then compiled successfully and tested in the Remix environment. It was observed that the functions were executed sequentially as expected. Moreover, the code verified that only registered oracles were allowed to interact with the smart contract. We fed the data with information in which the code picked out the most trustworthy cluster based on the algorithm. This reinforces that the developed code works as intended. The full smart contract code can be found in the GitHub repository.[1]

6 Testing and Validation

The proposed solution was deployed and tested on a virtual test Ethereum network using Remix IDE. The smart contract code was implemented and debugged. All function calls can be viewed in the console to verify the functionality of the methods, the output, and the cost of execution.

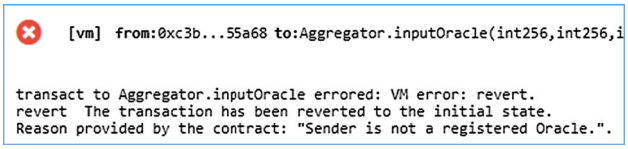
To perform the functionality testing, the registration contract was first deployed. The registration smart contract owner registered several oracles that report statistics about the number of cases. Each of these oracles has a different Ethereum address used from the available addresses in the IDE. The reputation score is initialized automatically by the smart contract and linked to the address of the oracle. Oracles can only be registered by the smart contract owner for security reasons.

After the oracles were registered, each oracle provides periodic input regarding the number of cases infected with

[1] https://github.com/MazenDB/Coronavirus.

```
"from": "0xd6fbbabc26d64533e077247d061d8d2c8cabcf1f",
"topic": "0x90d774ee83b0d97bafee24beeeb0f980a443cbceeb55fe37a5122f348e6d469f",
"event": "OracleInput",
"args": {
        "0": "0xa516bCa2E543535494A18Ab90739BE7C4Aee947f",
        "1": "34557",
        "2": "17932",
        "3": "264",
        "oracleAddress": "0xa516bCa2E543535494A18Ab90739BE7C4Aee947f",
        "newInfected": "34557",
        "newRecovered": "17932",
        "newDead": "264",
        "length": 4
```


Fig. 5 Event showing the input of an oracle



```
[vm] from:0xc3b...55a68 to:Aggregator.inputOracle(int256,int256,i

transact to Aggregator.inputOracle errored: VM error: revert.
revert  The transaction has been reverted to the initial state.
Reason provided by the contract: "Sender is not a registered Oracle.".
```


Fig. 6 Error due to input by an unregistered member

```
"from": "0x2e281c10c364bd711cfaef74453078ae7d6da663",
"topic": "0x7a31abf4cd123a966614d4ef13190885d733af663b4dfef2e80de32b9fb30730",
"event": "LatestStatistics",
"args": {
        "0": "34002",
        "1": "17309",
        "2": "264",
        "Infected": "34002",
        "Recovered": "17309",
        "Dead": "264",
        "length": 3
```


Fig. 7 Event showing the final statistics computed by the smart contract

COVID-19, the number of recovered patients, and the number of deaths. The smart contract is updated with these statistics that it records the source along with the timestamp. For instance, Fig. 5 shows an event-triggered upon receiving an update from an oracle. The event reports the oracle address as well as the updated statistics from this oracle.

The smart contract verifies the identity of the transaction's sender. In some cases, the sender is not authorized to call a certain method. As shown in Fig. 6, an Ethereum client cannot provide input to the aggregator smart contract unless it was pre-registered by the contract owner.

The final statistics are computed based on the input of all oracles, as explained previously. When this algorithm is executed, the outcome is broadcasted as an event shown in Fig. 7. The event shows the latest up-to-date statistics reported.

After the records have been updated, the reputations smart contract updates the reputation scores for the contributing oracles. The reputation of oracles is improved if their reported numbers are close to the values as computed by the aggregator smart contract.

7 Discussion and Analysis

Our proposed blockchain-based solution for tracking the COVID-19 pandemic captures the main operations required for dynamically tracking the transmission and the current number of infected, recovered, and deaths. In this section, we discuss the cost and security analysis of our proposed system. We also highlight the challenges and future directions for implementing the proposed system.

Table 2 Transaction cost incurred at an average gas price of 6 Gwei at an exchange rate of 1 ETH = 158.10 USD

Function name	Transaction gas	Execution gas	Average transaction fee (USD)
Deployment	1,521,652	1,116,836	3.21
registerOracle()	107,675	84,995	0.20
inputOracle()	50,682	28,770	0.08
calculateStatistics()	251,348	230,076	0.50
computeReputation()	36,607	13,927	0.04

7.1 Cost Analysis

For operations to get executed successfully, a gas fee is required to be paid by stakeholders in the network. Hence, every line of code that is written in Solidity requires a certain amount of gas to get executed. The Ethereum gas is the unit used to measure the computational effort required for transaction executions. Ethereum transactions incur two types of costs during their execution. First, execution cost is related to the costs of changing states in the contract and internal storage, while second is transaction cost, which includes the execution cost along with the cost of sending data such as contract deployment and transaction input cost [42].

This gas amount is calculated by considering both the gas price and gas limit, respectively. The former refers to the gas consumed in the contract, and the latter refers to the total gallons of gas placed inside the smart contract gas tank [42]. Moreover, it should be noted that as the gas price increases, the rate of adding verified transactions to each block increases. Accordingly, this price is expected to increase during high network traffic as miners compete to add transactions in the blocks to receive transaction fees. Table 2 shows the transaction and execution gases along with the corresponding transaction fees for deploying the contract and executing the major functions. The average gas price equal to 6 Gwei was obtained on April 10, 2020, according to the ETH Gas Station [43]. This transaction fee was converted to US dollars at an Ether exchange rate of 1 ETH = 158.10 USD. We notice that the cost incurred by the stakeholders does not even exceed 5 USD. This implies that implementing the proposed solution is feasible and encourages cost savings to all stakeholders in the network.

7.2 Security Analysis

In this section, we discuss the security properties of the proposed blockchain COVID-19 data tracking solution in addressing core security concerns related to integrity, accountability, authorization, non-repudiation, and resistance to cyberattacks such as distributed denial-of-service (DDoS) attack [44].

7.2.1 Integrity

It is important to guarantee integrity and maintain data consistency when obtaining information from oracles related to COVID-19 statistics. Our solution ensures that the information added to the new block is collected from the right group oracles by making sure that miners verify these transactions to assure the truthfulness and validity of data. Moreover, once information is added to the blockchain network, then it becomes very difficult to tamper with it due to its decentralized structure and combination of cryptography and sequential hashing, unlike a traditional standard database.

7.2.2 Accountability

Every user or stakeholder is held responsible for their actions on the ledger. This is because whenever a user executes a function in the smart contract, then this action call is traced back to the Ethereum caller's address.

7.2.3 Authorization

Securing data access in blockchain networks is essential for ensuring that only users with authorized access can participate and add appropriate data accordingly. Our proposed solution makes sure that all oracles are first registered using the registration smart contract and then only they are allowed to interact with the aggregator smart contract. This shows that the presented approach satisfies the authorization and authentication controls needed for a reliable tracking system. Moreover, the blockchain infrastructure ensures that each data block is fully encrypted before it gets added to the chain of existing blocks. Thus, if an attacker were to gain access to the blockchain data and network, then this does not certainly mean that the attacker would be able to retrieve and read the information due to the use of end-to-end encryption methods. Only authorized users can decrypt and see this information through the use of their private keys. This would encourage many countries to use such a system as it promotes data access control and data confidentiality by using the latest cryptographic algorithms to generate public/private key combinations that rely on solving integer factorization problems that are almost impossible to crack using current computing power.

7.2.4 Non-repudiation

All transactions are digitally signed and timestamped when added to the blockchain. This indicates that users or organizations can trace back a particular transaction at a specific time and accordingly identify the user behind that transaction using their public address. This security property reassures users since no one can duplicate their signature on a transaction that has not been created by them. This enhances the system reliability as it becomes easier to detect fraudulent transactions because every transaction stored in the ledger is cryptographically connected to its user. This auditing capability provides authenticity, transparency, and security over every transaction.

7.2.5 Resistance to Cyberattacks

Cyberattacks have become progressively more complex due to the increasing use of sophisticated malware and threat from professional cyberorganizations. Users or organizations with malicious intent attempt to steal valuable data such as financial data, personal identifiable information, intellectual property, and health records. Several strategies, such as monetizing data access through the use of advanced ransomware techniques or disrupting business operations through DDoS attacks, have been attempted. DDoS attacks, in particular, result in service disruption of websites and mobile apps, causing an increase in losses to businesses. However, such attacks are costly and difficult to execute in blockchain platforms as they would need to transact large volumes of small transactions to dominate the network. The peer-to-peer and decentralization structure of blockchain technology helps in improving its cyberdefense since the platform can prevent malicious activities through robust consensus algorithms and detect data tampering due to its inherent features such as transparency, immutability, data encryption, auditability, and operational resilience due to no single point of failure. Researchers in [45] suggest the application of chaotic systems using neural networks that generate data to be used for data encryption. This solution can be implemented on lightweight devices such as the Internet of things (IoT) devices. Some of the features that define chaotic systems, according to [46], are complexity, nonlinearity, emergence, and hierarchal growth. Table 3 describes how blockchain technology compares to those chaotic system properties.

From the table, we can conclude that since blockchain technology does not have the properties discussed above, the application of the chaotic cryptography is not feasible. Therefore, since our solution is based on the blockchain technology and is not compatible with the chaotic systems, the blockchain can be regarded as a complicated system, but not complex and thus, not chaotic.

Table 3 Chaotic system parameters vs. blockchain technology

Chaotic system parameters	Blockchain technology
Complexity	Algorithmically, blockchain is complicated but not complex. Furthermore, the infrastructure (miners, full nodes maintainers, and developers) presents an extremely low statistical complexity measure
Nonlinearity	Blockchain can be nonlinear, but only if regulations constrained the online exchanges from bitcoins to dollars and vice versa
Hierarchical growth	Not apparent in blockchain technology
Emergence	Not apparent in blockchain technology

7.3 Challenges

Even though blockchain has great potential in combating the COVID-19 outbreak, some challenges have to be considered. In this section, we highlight some of these major challenges, along with the recent attempts carried out to address them.

7.3.1 Shortage of Skilled Workforce

Building a blockchain platform requires a variety of skill sets ranging from security, app development to business and engineering, and other related areas. Drane reported that the blockchain industry suffers from a dearth of talent [47]. This causes problems for companies in hiring and nurturing talent. As a result, companies are finding various ways to fill this talent gap from conducting in-house training and outsourcing to hiring new collar workers [47]. Companies such as IBM are designing their private training centers to quickly train their employees to fill the vacancies of blockchain-related jobs, while other organizations are outsourcing these jobs to freelancers and agencies that specialize in this line of work. However, new collar workers, on the other hand, are a term used to describe jobs that do not require college degrees but require training instead. This approach is effective for companies that do not have the time to wait for college graduates to occupy these vacancies as they are competing in a competitive environment. As a result, several higher education institutes are offering online blockchain training courses.

7.3.2 Scalability

The blockchain network traffic becomes bulky as the number of transactions increases every day. Every node on the blockchain has to store all validated transactions, and this becomes an obstacle as there is a restriction on the block size and time interval used to create a new block. Current blockchain platforms process only a few transactions per second, which becomes problematic as millions of transactions are needed to be processed in real time. Since the block size is limited, this causes small transactions to be delayed as miners prefer to validate transactions with high transaction fees [26]. VerSum proposed a novel scheme that allows lightweight clients to subcontract expensive computations of large inputs to ensure that the computation result obtained multiple servers is correct by comparing individual results obtained [48].

7.3.3 Selfish Mining

Blockchain is vulnerable to attacks plotted by selfish miners even if only a small amount of the hashing power is used to cheat the network. The strategy used by selfish miners is that they create a private branch by mining blocks without broadcasting, and they publish the private chain only when it is longer than the current public chain [26]. They mine this chain without competitors; meanwhile, honest miners waste their resources on mining a useless branch. As a result, by doing so, selfish miners earn more revenue. To tackle this problem, ZeroBlock built a simple scheme in which each block must be created and accepted within a specific time interval. Hence, selfish miners would be unable to earn more than their expected reward [49].

7.3.4 Legal Issues

The most important concern during this COVID-19 pandemic is related to the data being accessed, stored, and shared in the blockchain network as a distributed database since there are several issues with regard to policies and laws that need to be resolved by various parties including the international health organizations, country leaders, and international policymakers to introduce new regulations related health policy, data sharing, digital health-service-related policy and issues associated with digital inequality, digital connectivity and digital divide that mainly exists in underdeveloped countries.

7.3.5 Privacy Concerns

Blockchain technology is susceptible to privacy leakage as balances and details of all public keys are made transparent to all members of the network. However, there have been two proposed solutions that are divided into mixing solution and anonymous solution to achieve anonymity in blockchains [26]. Mixing service provides anonymity by using multiple input addresses to transfer funds to multiple output addresses, while anonymous is a service that prevents transaction graph analysis by unlinking the payment origins for a transaction [26].

Table 4 Summary of security features, blockchain challenges, and their description

Security features and challenge	Description
Resistance to cyberattacks	The decentralization structure of blockchain technology can prevent malicious activities through robust consensus algorithms and detect data tampering due to its inherent features such as transparency and immutability
Authorization	Securing data access in blockchain networks is essential for ensuring that only users with authorized access can participate and add appropriate data accordingly. Thereby, only registered parties can participate in the network
Non-repudiation	In the blockchain, all transactions are digitally signed and timestamped. Therefore, users can trace back a particular transaction at a specific time and accordingly identify the user behind that transaction using their public address
Integrity	Blockchain ensures the integrity of its transactions and data. The blockchain also guarantees that data added to the new block are valid since miners verify transactions to assure their truthfulness and validity
Scalability	Every node on the blockchain must store all validated transactions, and this becomes an obstacle as there is a restriction on the block size and time interval used to create a new block
Selfish mining	Blockchain is vulnerable to attacks plotted by selfish miners. A potential solution is to build a scheme in which created blocks are accepted within a specific time interval
Legal issues	Policies and laws need to be considered by various parties considering the sensitivity of health data. These parties need to introduce new regulations related to health policy, data sharing, and digital health service
Privacy concerns	Blockchain is susceptible to privacy leakage as public keys are made transparent to members of the network. One solution is to use multiple input addresses to transfer funds to multiple output addresses while staying anonymous
Shortage of skilled workforce	Building a blockchain platform requires a variety of skill sets. Due to the lack of the needed skilled workforce, companies started designing their private training centers to satisfy their workforce needs
Accountability	Every user or stakeholder in the network is held responsible for their actions on the ledger

Table 4 summarizes the key points discussed above, along with the challenges presented in the security analysis.

7.4 Future Directions

Overall, our proposed solution is generic enough that it can be adapted to cater to data collection and report statistics on other infectious diseases, including Malaria, HIV, and TB. This is possible as blockchain encourages the sharing and reporting of data among stakeholders in a network. The proposed solution could be used to streamline communication between patients and healthcare professionals. It can connect all research and healthcare communities within the same network to use and share a trusted secure database that is tamperproof. Furthermore, the oracles in the network could be rewarded by increasing their credibility to encourage them to report accurate data. However, it should be noted that all relevant stakeholders must be involved in implementing the proposed solution so that it is sustainable, efficient, and trustworthy. This interaction is particularly important in areas with underserved communities.

8 Conclusion

In this paper, we proposed and evaluated a blockchain-based tracking system for validating the COVID-19 data from diverse sources to mitigate the spread of falsified or modified data. Our proposed blockchain-based solution promotes trust, transparency, traceability and streamlines the communication between stakeholders in the network. Our proposed solution leverages Ethereum smart contracts and oracles and demonstrates the critical application of blockchain technology for COVID-19. The developed system would update the DApps and dashboards with real-time statistics as they become available, related to the number of confirmed cases,

deaths, and recoveries. The presented system architecture, sequence diagram, and algorithms can be easily generalized for tracking various other infectious diseases. Our presented solution addresses the problems faced in the current pandemic crisis, such as miscommunication, data manipulation, and single point of failure. Furthermore, it mitigates malicious activities due to its inherent cryptography security features of blockchain technology. The smart contract code is made publicly available in GitHub. We present a detailed cost analysis to compute the transaction costs incurred by stakeholders when interacting with the smart contract. Furthermore, we present security analysis pertaining to integrity, accountability, authorization, non-repudiation, and resilience to common forms of cyberattacks, including DDoS attacks. As future work, we aim to expand the smart contract functionalities and develop DApps to enable participants to interact with Ethereum smart contracts seamlessly.

Acknowledgements This publication is based upon work supported by the Khalifa University of Science and Technology under Award No. CIRA-2019-001.

References

1. WHO. Rolling updates on coronavirus disease (COVID-19). World Health Organization. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen. Accessed 25 May 2020
2. Ramsay, G.: Japanese PM and IOC chief agree to postpone 2020 Olympics until 2021. CNN, 24 March 2020. https://edition.cnn.com/2020/03/24/sport/olympics-postponement-tokyo-2020-spt-intl/index.html. Accessed 25 May 2020
3. BIE Member States confirm one-year postponement for Expo 2020. Expo 2020 Dubai UAE. https://www.expo2020dubai.com/en/whats-new/expo-stories/bie-announcement. Accessed 25 May 2020
4. Houston, L.; Probst Y.; Humphries, A.: Measuring data quality through a source data verification audit in a clinical research setting. Stud Health Technol Inform (2015)
5. Bischoff, P.: COVID-19 App Tracker: Is privacy being sacrificed in a bid to combat the virus?. CompariTech, 20 April 2020. https://www.comparitech.com/blog/vpn-privacy/coronavirus-apps/. Accessed 25 May 2020
6. Warner, K.; Nowais, S.A.: Coronavirus: Doctors urge public to help track COVID-19 cases with tracing app. The National, 28 April 2020. https://www.thenational.ae/uae/health/coronavirus-doctors-urge-public-to-help-track-covid-19-cases-with-tracing-app-1.1012267. Accessed 25 May 2020
7. Tangermann, V.: Hackers are using coronavirus maps to spread malware. World Economic Forum, 14 March 2020. https://www.weforum.org/agenda/2020/03/hackers-are-using-coronavirus-maps-to-spread-malware?fbclid=IwAR06Xux96s2GTy_-Ttew1Cuy96YV4ng9Z4eGd0kFVa-a_QbapumxgFO6DmU. Accessed 25 May 2020
8. Villas-Boas, A.: A fake coronavirus tracking app is actually ransomware that threatens to leak social media accounts and delete a phone's storage unless a victim pays $100 in bitcoin. Business Insider, 16 March 2020. https://www.businessinsider.com/coronavirus-fake-app-ransomware-malware-bitcoin-android-demands-ransom-domaintools-2020-3. Accessed 25 May 2020
9. Tesini, B.L.: MSD Manual. May 2020. https://www.msdmanuals.com/professional/infectious-diseases/respiratory-viruses/coronaviruses-and-acute-respiratory-syndromes-covid-19,-mers,-and-sars#v47572273. Accessed 3 June 2020
10. Readfearn, G.: How did coronavirus start and where did it come from? Was it really Wuhan's animal market?. The Guardian, 28 April 2020. https://www.theguardian.com/world/2020/apr/28/how-did-the-coronavirus-start-where-did-it-come-from-how-did-it-spread-humans-was-it-really-bats-pangolins-wuhan-animal-market. Accessed 3 June 2020
11. Cennimo, D.J.: Coronavirus Disease 2019 (COVID-19). MedScape, 1 June 2020. https://emedicine.medscape.com/article/2500114-overview#a9. Accessed 3 June 2020
12. Coronavirus disease 2019 (COVID-19). MayoClinic, 22 May 2020. https://www.mayoclinic.org/diseases-conditions/coronavirus/symptoms-causes/syc-20479963. Accessed 3 June 2020
13. COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE). Johns Hopkins University, 2020. https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6. Accessed 3 June 2020
14. Coronavirus Disease 2019 (COVID-19). CDC Center for Disease Control and Prevention, May 2020. https://www.cdc.gov/coronavirus/2019-ncov/symptoms-testing/symptoms.html. Accessed June 2020
15. Coronavirus disease (COVID-19): Prevention and risks. Government of Canada, 29 May 2020. https://www.canada.ca/en/public-health/services/diseases/2019-novel-coronavirus-infection/prevention-risks.html. Accessed 3 June 2020
16. How to Protect Yourself & Others. CDC Center of Disease Control and Prevention, 24 April 2020. https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/prevention.html. Accessed 4 June 2020
17. Sandford, A.: Coronavirus: Half of humanity now on lockdown as 90 countries call for confinement. Euronews, 3 April 2020. https://www.euronews.com/2020/04/02/coronavirus-in-europe-spain-s-death-toll-hits-10-000-after-record-950-new-deaths-in-24-hou. Accessed 4 June 2020
18. Wright, R.: The world's largest coronavirus lockdown is having a dramatic impact on pollution in India. CNN, 1 April 2020. https://edition.cnn.com/2020/03/31/asia/coronavirus-lockdown-impact-pollution-india-intl-hnk/index.html. Accessed 4 June 2020
19. Chico Harlan, S.P.: Italy extends coronavirus lockdown to entire country, imposing restrictions on 60 million people. Washington Post, 10 March 2020. Chico Harlan and [Accessed 4 June 2020
20. Carmen, R.S.; Reinhart, M.: How can we prevent a COVID-19 food crisis? World Economic Forum, May 2020. https://www.weforum.org/agenda/2020/05/preventing-a-covid-19-food-crisis/. Accessed 4 June 2020
21. A. F. et al.: Simulating SARS-CoV-2 epidemics by region-specific variables and modeling contact tracing App containment. MedRxiv (2020)
22. M. I.,. M. B.,. S. D.,. L. F. R. F. Chiara Farronato, "Harvard Business Review," 15 July 2020. Chiara Farronato, Marco Iansiti, Marcin Bartosiak, Stefano Denicolai, Luca Ferretti and Roberto Fontana
23. MoHAP: Ministry of Health and Prevention. 25 April 2020. https://www.mohap.gov.ae/en/MediaCenter/News/Pages/2385.aspx
24. National Disinfection Programme and testing for COVID-19. UAE Government, 1 June 2020. https://u.ae/en/information-and-services/justice-safety-and-the-law/handling-the-covid-19-outbreak/disinfection-and-testing-for-covid-19. Accessed 4 June 2020
25. Khalid, T: UAE's latest measures to contain the spread of the coronavirus: All the facts. Al Arabiya English, 21 March 2020.

https://english.alarabiya.net/en/News/gulf/2020/03/21/UAE-s-latest-measures-to-contain-the-spread-of-the-coronavirus-All-the-facts. Accessed 4 June 2020
26. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H.: An overview of blockchain technology: architecture, consensus, and future trends. In: IEEE 6th International Congress on Big Data, Honolulu (2017)
27. Rao, R.; Jain, H.: Improving Integrated Clinical Trial Management Systems through Blockchain. Genetic Engineering & Biotechnology News, Nov. 2019. https://www.genengnews.com/insights/improving-integrated-clinical-trial-management-systems-through-blockchain/. Accessed 27 May 2020
28. Glover, D.G.; Hermans, J.: Improving the Traceability of the Clinical Trial Supply Chain. Applied Clinical Trials, pp. 36–38, Nov./Dec. 2017
29. Nugent, T.; Upton, D.; Cimpoesu, M.: Improving data transparency in clinical trials using blockchain smart contracts. F1000Research **5**, 1–4 (2017)
30. Benchoufi, M.; Ravaud, P.: Blockchain technology for improving clinical research quality. BioMed Central **18**, 1–5 (2017)
31. Wright, T.: Blockchain App Used to Track COVID-19 Cases in Latin America. Coin Telegraph: The future of money, 6 April 2020. https://cointelegraph.com/news/blockchain-app-used-to-track-covid-19-cases-in-latin-america. Accessed 29 May 2020
32. Dragov, R.; Croce, C.L.; Hefny, M.: How Blockchain Can Help in the COVID-19 Crisis and Recovery. IDC-Analyze the Future, 4 May 2020. https://blog-idcuk.com/blockchain-help-in-the-covid-19-and-recovery/. Accessed 27 May 2020
33. Blockchain And Crypto Firm VeChain Utilized to Confirm Authenticity of Coronavirus KN95 Masks. Blockchain Magazine, 20 April 2020. https://www.blockchainmagazine.net/blockchain-and-crypto-firm-vechain-utilized-to-confirm-authenticity-of-coronavirus-kn95-masks/. Accessed 27 May 2020
34. Singh, G.; Levi, J.: MiPasa project and IBM Blockchain team on open data platform to support Covid-19 response. IBM, 27 March 2020. https://www.ibm.com/blogs/blockchain/2020/03/mipasa-project-and-ibm-blockchain-team-on-open-data-platform-to-support-covid-19-response/. Accessed 27 May 2020
35. Coalition: Help stop the spread. https://www.coalitionnetwork.org/. Accessed 27 May 2020
36. Joshi, M.: PHBC announces blockchain monitor to track virus-free zones. Cryptopolitan, 19 March 2020. https://www.cryptopolitan.com/phbc-blockchain-monitor-for-virus-free-zones/. Accessed 27 May 2020
37. Chang, M.C.; Park, D.: How can blockchain help people in the event of pandemics such as the COVID-19? J. Med. Syst. **44**(102), 2020 (2020)
38. Zhang, J.: Chinese startup launches blockchain platform to improve donation efficiency," Tech in Asia, 14 Feb. 2020. https://www.techinasia.com/china-blockchain-platform-donation. Accessed 27 May 2020
39. Acoer. Providing daily tracking and visualizations of the pandemic. Coronavirus (COVID-19) Tracker. https://www.acoer.com/coronavirus. Accessed 27 May 2020
40. Buterin, V.: Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. White Paper, 2013. http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. Accessed 19 Jan. 2020
41. Hasan, H.; Salah, K.: Blockchain-based solution for proof of delivery of physical assets. In: Proceedings of the 2018 International Conference on Blockchain (ICBC 2018). Springer LNCS, Seattle, USA, June 25–June 30, 2018
42. Optimizing your Solidity contract's gas usage. Medium, 5 April 2018. https://medium.com/coinmonks/optimizing-your-solidity-contracts-gas-usage-9d65334db6c7. Accessed 9 March 2020
43. Eth Gas Station. https://ethgasstation.info/calculatorTxV.php. Accessed 10 April 2020
44. Piscini, E.; Dalton, D.; Kehoe, L.: Blockchain & Cybersecurity Point of View. Deloitte, 2017. https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf. Accessed 2 June 2020
45. Tlelo-Cuautle, E.; Díaz-Muñoz, J.; González-Zapata, A.; Li, R.; León-Salas, W.; Fernández, F.; Guillén-Fernández, O.; Cruz-Vega, I.: Chaotic image encryption using hopfield and hindmarsh-rose neurons implemented on FPGA. Sensors **20**(5), 1326 (2020)
46. Salah, K.; Nizamuddin, N.; Jayaraman, R.; Omar, M.: Blockchain-based soybean traceability in agricultural supply chain. IEEE Access **7**(1), 73295–73305 (2019). https://doi.org/10.1109/ACCESS.2019.2918000
47. I. d. Marco. 3 ways organizations are dealing with the blockchain developer shortage. Venture Beat, 28 Jan 2018. https://venturebeat.com/2018/01/28/3-ways-organizations-are-dealing-with-the-blockchain-developer-shortage/. Accessed 1 June 2020
48. van den Hooff, J.; Kaashoek, M.F.; Zeldovich, N.: VerSum: verifiable computations over large public logs. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York (2014)
49. Solat, S.; Potop-Butucaru, M.: ZeroBlock: Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin. May 2016