Personal and Ubiquitous Computing
https://doi.org/10.1007/s00779-021-01610-8

ORIGINAL ARTICLE

Blockchain for COVID-19: a comprehensive review

Het Shah[1] · Manasi Shah[1] · Sudeep Tanwar[1] · Neeraj Kumar[2,3,4]

Received: 13 May 2021 / Accepted: 24 July 2021

Abstract
The rampant and sudden outbreak of the SARS-CoV-2 coronavirus also called COVID-19 and its uncontrollable spread have led to a global crisis. COVID-19 is a highly contagious disease and the only way to fight with it is to follow social distancing and Non-Pharmaceutical Interventions (NPIs). Moreover, this virus is increasing exponentially day-by-day and a huge amount of data from this disease is also generated at the fast pace. So, there is a need to store, manage, and analyze this huge amount of data efficiently to get meaningful insights from it, which further helps medical professionals to tackle this global pandemic situation. Moreover, this data is to be passed through an open channel, i.e., the Internet, which opens the doors for the intruders to perform some malicious activities. Blockchain (BC) emerges as a technology that can manage the data in an efficient, transparent manner and also preserve the privacy of all the stakeholders. It can also aid in transaction authorization and verification in the supply chain or payments. Motivated by these facts, in this paper, we present a comprehensive review on the adoption of BC to tackle COVID-19 situations. We also present a case study on BC-based digital vaccine passports and analyzed its complexity. Finally, we analyzed the research challenges and future directions in this emerging area.

Keywords Blockchain · COVID-19 · Healthcare · Contact sharing · Supply chain management

1 Introduction

Novel coronavirus disease dubbed as COVID-19 by the World Health Organization (WHO) has forced the whole world on its knees. It is a pneumonia-like infectious disease that was first seen in Wuhan, China, at the end of 2019 and has quickly spread to the rest of the world. Due to its rapid transmission, virtually every country in the world faces its threat and has overburdened the existing medical facilities. There is no cure for this virus as of now and it has infected over 25 million people and over 850,000 people have succumbed to the illness. The only definitive way of controlling the spread of the virus is by practicing social distancing and maintaining personal hygiene. The WHO recommends regularly wash hands, maintain a distance of a minimum of one meter from others, avoid visits to public places, and wear the face mask at all times.

Many countries in the world have imposed stringent measures to curb the spread of the virus, such as strict quarantine for all infected citizens, travel restrictions, and measures to maintain social distancing such as public closings places to restrict mass gathering. Despite all these measures in action, people often flout these norms and recommendations and the spread has not been contained. The only solution is that people must accept these new norms and recommendations and follow them wholeheartedly.

Information and Communication Technology (ICT) played a key role in fighting against the virus and has worked hand-in-hand with the medical industry to minimize

✉ Sudeep Tanwar
sudeep.tanwar@nirmauni.ac.in

Het Shah
17bit103@nirmauni.ac.in

Manasi Shah
17bce055@nirmauni.ac.in

Neeraj Kumar
neeraj.kumar@thapar.edu

[1] Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India

[2] Department of Computer Science Engineering, Thapar Institute of Engineering and Technology, Deemed to be University, Patiala, Punjab, India

[3] School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India

[4] King Abdul Aziz University, Jeddah, Saudi Arabia

Published online: 05 August 2021

the spread of this virus. Many governments and municipal corporations across the globe have released mobile applications to keep their citizens informed about the current spreading status of the virus. These applications include the number of cases, the number of recoveries, the areas with a high number of cases detected, nearest hospitals, government norms, and guidelines. Some countries such as South Korea [92] developed an application that can track the movements of their citizens and all those who were in contact with them in case the person tested positive. On tested positive, all the people who were in his/her contact with the infected person are tracked and also tested. This way, the spread of the virus can be contained.

Often, in these types of personal information sharing applications, there is always a concern about the security of the data and preserving the user's privacy. For example, the mobile application released by the government of Singapore known as the TraceTogether [49, 72] has faced a lot of criticism for its ignorance of the privacy of application users. In this application, nearby mobile phones share tokens via Bluetooth and also to a central server. If a citizen has been exposed to the virus, then the authorities will procure the list of all these tokens that the application received from nearby mobile phones. Further, these citizens can be tracked and checked if they are exposed to the virus or not. But this application has the following issues.

- *Privacy from Snoopers:* People trying to exploit the information of the user.
- *Privacy from Contacts:* People in Bluetooth proximity with whom the tokens were shared.
- *Privacy from Authorities:* Due to the absence of a decentralized system, the government officials and the companies tasked with creating and deploying such applications can have access to the database of the users.

The Singapore government reasonably prevented the first two problems. The transmitted tokens were randomly generated and replaced at acceptable refresh rates, preventing snooping in public places. The application provides privacy from contacts by only sharing information with the government. However, the third issue is to protect data from the authorities, which can be solved via a decentralized system [24]. Centralized architecture is adapted because of its low hardware cost and ease in information flow. But this architecture is not capable enough to handle the security and privacy of the stakeholder because of issues such as:

- Since the system is centrally located and controlled, so the data resides at one central location. Any system failure can lead to loss of all the data and it is nearly impossible to retrieve it if a good backup service is not configured.
- The centralized approach mostly works on a single operating system to manage the entire network. It might not be able to cater to the diversified needs of the users. For example, suppose some users want the data in different formats, then the system might not be able to provide it simultaneously to all the users.
- Due to lack of load sharing and load balancing functionalities in such systems, they cannot support multiple access. Hence, when essentially needed, the information is not fetched in a reasonable time frame due to the overloading of the servers.
- Despite all the security precautions taken to secure the network, there is a possibility of an attack on the centralized system since it has a central target that needs to be attacked. A complete attack to decrypt a file wholly and access its data is nearly impossible in a decentralized BC environment since the file is distributed among different storage providers [13]

These challenges of a centralized system put the security and privacy of the patients at risk.

Figure 1 shows the number of individuals affected by healthcare breaches in the years 2009 to 2019, while Fig. 2 shows the average data breach size of each attack in the same period. It can be inferred from the figure that the number of individuals affected by such data breaches is increasing over some time and has doubled (almost 40 million individuals affected) in 2019. However, this is not close to the peak, which was nearly 115 million people affected in 2015. Out of this, 78 million people alone were affected by a single breach on Anthem Inc, a US-based health insurance company [52].

Due to the increasing number of data breaches in the healthcare sector and other security issues like the authentication of the supplies as well as the supplier, online payments, etc., BC proves to be a lucrative solution, which ensures the security and privacy of the stakeholders' stored data. BC is an emerging technology that helped track the decentralized records-tracking of transactions, which cannot be tampered. This provides a secure and trustworthy way to share the personal and confidential data of the patients. BC has three major characteristics such as decentralization, immutability, and transparency. A BC is a series of logically connected blocks that store information about the transactions initiated by one party and verified by others in the network. These transactions are then added to the BC. This is how the chain expands and adds more security to the data stored in it. To change the contents of a block, the attacker needs to know the cryptographic hash value of the respective block and it is also connected to the hash value of its succeeding block. Hence, the attacker has to mutate all the succeeding blocks to perform some malicious activity, would require the control of at least

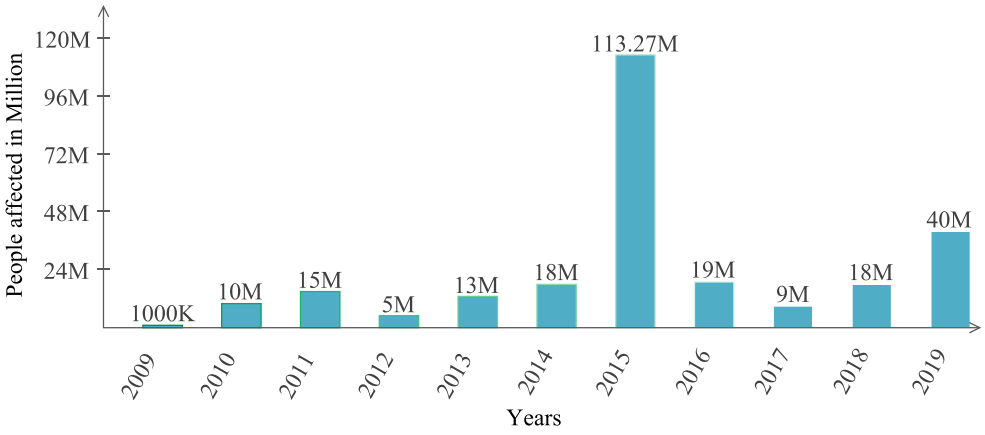

Fig. 1 Number of individuals affected from 2009 to 2019 [62]

50% of the devices employed in the chain which is tedious and time-consuming and is practically impossible and. The information stored in the blocks and their status is visible to all the network users, but there is pseudonymity ensured to protect the users' identity. BC also provides a level of access control, so that an unauthorized person cannot access data that is not meant for them. For example in the use case of the healthcare, the doctors should only have the access to a patients previous medical records. The BC has an additional characteristics which is persistence of data. Transaction once lodged in the chain, will always be recorded and can be accessed later on by an authorized person.

In this paper, we explore the challenges regarding the usage of BC to maintain the privacy and security of the stakeholders' data. We also propose a solution taxonomy to fight against COVID-19 with the adoption of BC. The solution taxonomy will discuss some areas of the COVID-19 in which the present measures implemented fall short and how BC can help overcome these issues. We also highlight open issues posed by the proposed solution taxonomy and future research directions it provides.

1.1 Comparisons with existing surveys

The possibility of integrating BC and healthcare has been a topic of investigation and has been taken by various researchers as evident from literature surveys. This section gives a comparative study of state-of-the-art works that focused on the BC and healthcare sectors and their integration, which can be helpful to tackle the COVID-19 crisis.

The authors in [59] analyzed the potential use cases of BC in healthcare. In contrast, the authors in [42] analyzed the shortcomings in the integration of BC with healthcare while discussing the limitations of BC, including the cost and complexity of implementation. The impact and the potential applications of BC were studied in [1, 78] without specifying the implementation details, while the benefits of patients utilizing BC were pointed out in [22] although its exact real-time use cases were not discussed. The authors in [11, 64] came up with a short survey on the role of BC in the case of pandemics.

The authors in [20, 21, 40, 85, 100, 112, 121] gave the use cases and applications of using ICT to tackle COVID-19 pandemic along with leveraging industry 4.0 technologies

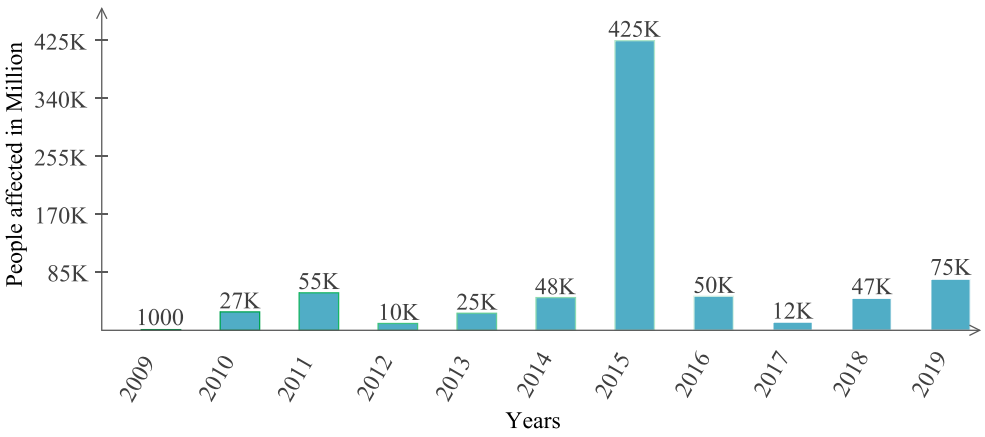

Fig. 2 Average data breach size from 2009 to 2019 [62]

such as IoT, cloud computing, Unmanned Aerial Vehicle (UAV), and Deep Learning (DL). BC was used along with AI in the solution stack that the authors presented in [79, 85, 100] utilizing the best characteristics of both technologies. Alsamhi et al. [6] came up with a novel amalgamation of drone and BC technologies to combat the pandemic.

Table 1 shows the comparison of existing surveys carried out by various researchers with the proposed survey. It also highlights their primary objective, key contributions, limitations, and open issues, which can be useful insight for beginners who want to start research in this emerging area.

1.2 Motivations and contributions

1.2.1 Motivations

Currently, research is going on to adopt BC in the healthcare industry. Several BC frameworks have been proposed by various researchers for various applications ranging from invasive technologies to critical healthcare metric prediction systems [81]. Due to the ongoing COVID-19 pandemic, some research proposals exist, which highlighted the application of BC in combating the pandemic. Most of the existing and proposed BC-based medical frameworks specialize in only one application and the healthcare industry needs an end-to-end solution to cater to its need. As per the authors' knowledge or exploration, there is no exhaustive survey exists, which provides a detailed end-to-end analysis of all potential applications of BC given the COVID-19 pandemic. Also, there is a need to analyze how the key characteristics of BC can be used as potential to combat COVID-19 situations. Motivated from these facts, in this paper, we review all the possible use cases of BC concerning the COVID-19 crisis. Table 2 shows the research questions that motivated us to conduct this survey.

1.2.2 Contributions

In this paper, we provide a detailed survey of the potential use case of BC in mitigating the COVID-19 crisis. The applications we have explored include; contact tracing, patients data sharing, supply chain management, payment system, data dashboard, security systems and vaccinations concerning utilizing BC technology and how it can be advantageous over the traditional healthcare systems. Then, we highlight integrating BC and COVID-19 and suggest future research directions for this integration. Following are the research contributions of this paper.

- We perform a comprehensive survey on the potential integration of BC and COVID-19. Moreover, we present a detailed analysis of current healthcare systems' current issues and provide background information on BC and COVID-19.
- We gave an overview of BC and also highlighted its characteristics such as privacy and security, decentralization, anonymity, accessibility, and access control, and how these characteristics can be used as a potential candidate to handle the COVID-19 situations.
- Further, we provide a solution taxonomy, which highlights an opportunity of leveraging the BC technology in the COVID-19 scenario in areas such as contact tracing, patients data sharing, supply chain management, payment system, data dashboard, data sharing, security systems and vaccination.
- We identify the main findings, the current issues and highlight the future research directions.

1.3 Review of security systems in place during COVID-19

Most of the companies and organizations have transitioned to work-from-home mode due to the pandemic. Due to the sudden onset of the pandemic most of the organizations do not have an adequate cybersecurity policy in place. Employees often use their own personal device to work. This has often lead to increased cybersecurity attacks such as malware, phishing and Denial-of-Service attacks that have caused monetary losses. During the pandemic, the number of successful cybersecurity attacks have increased by 600% [16].

In addition, healthcare organizations also face security risks from hackers. There have been many ransom-motivated attacks on hospitals during the pandemic. The hospital administration lost access to the systems during the attack and it was serious risk to patient safety as well. Huge ransoms had to be paid to regain access [126].

To reduce the risks of such cybersecurity attacks, some of the methods have been adopted include [3, 82, 98]:

- *Employee Awareness*: Employers should conduct seminars educating the employees on cybersecurity practices such as importance of strong passwords.
- *Virtual Private Network*: Home networks used by employees may be vulnerable to such attacks, but Virtual Private Networks can provide an encrypted mode of communication over the internet
- *Multi-Factor Authentication*: This allows for an additional layer of security. While accessing a resource with Multi-Factor Authentication in addition to the username and password, a one-time code that would be send to mobile phone would be required to log-in.

Table 1 Relative comparison of the existing surveys with the proposed survey

Related surveys	Year	Objective	Key contributions	Limitations and open issues
[42]	2018	Review of the scope and the possible shortcomings in the integration of BC and healthcare	The authors present a systematic review of the potential opportunities of BC integration and its possible challenges	The limitations of BC such as cost, absence of legislation, trust issues, and privacy concerns are not considered
[59]	2018	Review of the potential BC use case in healthcare	The authors analyzed the increasing use of BC technology in the healthcare industry	Prototype design and its implementation details are not present in their study
[22]	2019	Potential applications of BC for the patients	The authors explored the potential use cases for implementation of BC as an improvement over the legacy systems present for the patients such as data ownership, access control, remote monitoring and sharing of medical data	The cost associated with BC and the security concerns of BC such as susceptibility to 51% attacks
[1]	2019	Impact of BC in the healthcare industry	The authors reviewed the current and the ongoing research works in the domain of BC and healthcare	The effectiveness of the proposed models cannot be evaluated due to the lack of implementations of such the prototype models
[78]	2019	Potential applications of BC in healthcare	The authors explored the possible use case of BC applications in the healthcare industry	Mining incentives were not defined
[21]	2020	How BC can be helpful in the COVID-19 Pandemic	The authors presented the shortcoming of the current system and presented the ways BC can help overcome such shortcomings	Lacks in real-time implementation.
[85]	2020	Present AI and BC-based Solutions to combat COVID-19	The authors presented a novel architecture utilizing both BC and Artificial Intelligence(AI) technology	Challenges of AI and Blockchain integration were not considered.
[121]	2020	How digital tools can be helpful in the COVID-19 pandemic	The authors presented a wide range of digital technologies such as IoT, big data, AI, and BC and their potential applications in public health measures	The acceptance of such digital technology by the general public
[20]	2020	How new technologies can aid in managing the impact of COVID-19	The authors presented a comprehensive review about the potential use case of IoT, UAV, BC, AI and 5G	The limitations of each technology were not discussed
[112]	2020	Present the current IT trends and how they contribute to the fight against COVID-19	The author discussed almost all present IT trends such as AI, IoT, Big data, data analytics, BC, 3D printing, and drones. The authors did not discuss	The challenges of integration of these technologies.
[100]	2020	Role of AI and BC to flatten the COVID-19 curve	The authors presented a mobile application incorporating AI and BC components which can be used against the COVID-19 pandemic	The performance of the proposed application in real-time scenario was not considered.
[11]	2020	Potential role of BC in case of a pandemic	The authors explored the potential role of BC in data storage and its management in case of pandemics	Security and privacy of the healthcare data is still a primary concern among the stakeholders.
[40]	2021	Fusion of BC, AI and IoT technologies to combat the pandemic	The authors explored the potential fusion of new cutting edge technologies to control the pandemic	Challenges of AI and Blockchain integration were not considered

Table 1 (continued)

Related surveys	Year	Objective	Key contributions	Limitations and open issues
[6]	2021	Fusion of BC and Drone technologies to combat the pandemic	The authors explored the potential integration of BC in multi-drones to increase scalability and task collaboration among drones	Security issues by new joiner to a consensus and limited processing capacity of drones
[2]	2021	BC use cases in telehealth and telemedicine	The authors explored the potential opportunities of BC in digital healthcare to prevent frauds, ensure privacy and to verify credentials	Overall penetration of BC in healthcare industry is still in infancy stage
[64]	2021	BC use cases in pandemics	The authors explored the potential use cases of BC in pandemics like COVID-19 and how these measures can offer protection	Computational issues that arise with dealing so much healthcare data and the lack of confidence among general population for widespread adaption
Proposed Survey	2021	Provide a comprehensive review of applications of BC in COVID-19	The authors presented a systematic and detailed review of all BC applications to combat the COVID-19 pandemic situation	–

- *Antivirus software*: Ensure that antivirus databases are up-to-date and can protect against recent malware and virus attacks as well.
- *Updating Systems*: Legacy systems that are no longer supported and do not get security patches are the most vulnerable to such attacks. Updating the legacy systems and firmware to the latest version can also offer a layer of protection.

1.4 Methods and materials

For the proposed comprehensive survey, we need a broad overview of all the topics about the BC and COVID-19, so we explored only standard peer-reviewed journal databases (for example, ACM Digital Library, MDPI, Springer, IEEEXplore, Science Direct) for searching all the electronic data and literature as suggested in [65, 66]. We

Table 2 Research questions and discussions

Research questions	Motivation
What are the current challenges in the healthcare domain?	The current traditional healthcare systems are susceptible to cyber-attacks, exposing the patient data and records. Since such systems use a centralized approach, privacy and performance issues have been raised.
What is the key requirement of the healthcare domain?	The key requirement of the healthcare domain is to prevent unauthorized access to patient records, ensure smooth and transparent data sharing between different healthcare provider entities, and ensure monetary transactions to be completed smoothly.
What is the importance of security in the healthcare domain?	Security is the foremost requirement of the healthcare industry and its patients' privacy and prevents their data from malpractice.
What are the key characteristics of BC?	There is a requirement to explore the characteristics of BC, which includes decentralization, transparency, autonomy, persistency, and immutability
What is the potential application of BC for COVID-19	Potential application of BC includes tackling the current issues in the healthcare domain such as data interchange, nationwide interoperability, mobility, supply chain management, drug tracking, and payment frauds
What are the advantages of integrating BC with the healthcare system over the traditional healthcare systems?	BC offers security, decentralized architecture, user data privacy, and access control as well as immutability, and scalability.
What is the current research direction in the BC- healthcare domain?	Over the previous years, the applications of BC have expanded beyond its initial use as a digital currency. Its application in the healthcare domain has been getting attention among researchers and industry professionals.

explored other resources like white papers, technical books about the topic, predicting websites, patents, and online blogs and websites related to the existing surveys.

In this criteria, search using keywords like *Blockchain techniques for COVID-19*, *Blockchain in healthcare* and *Digital technology for COVID-19* and others. Our search string was not present in the title or abstract of several research papers and this case, we have performed a manual search. BC can be used in various application areas, so the search string *Blockchain for COVID-19* often gave papers irreverent to be used in the proposed survey. To gain complete insight into the current research trends and to have an adequate number of papers, we also included papers from 2020 early access. We also included data from other resources such as white papers and surveys conducted by renowned companies, survey articles, technical papers, and patents to broaden the research field.

1.5 Structure of this survey

The rest of the paper is organized as follows. Table 3 shows the acronyms table of the paper. Section 2 presents the background of BC and COVID-19 while highlighting the characteristics of BC and its possible application in the pandemic scenario. Then, the security challenges of COVID-19 are presented and the opportunities brought by BC to overcome them. In Section 3, we proposed a solution taxonomy for the adoption of BC to tackle COVID-19 situations. In Section 4, we present a case study on digital vaccine passports. Section 5 highlights all the main findings, challenges, and future research directions in this domain.

Table 3 Acronyms

AI	Artificial Intelligence
BBDS	Blockchain Based Data Sharing
BC	Blockchain
CSP	Cloud Service Providers
DHP	Digital Health Passport
DL	Deep Learning
FDA	Food and Drug Administration
ICT	Information and Communication Technology
IoT	Internet of Things
IVS	Infection Verifier Subsystem
NPI	Non-Pharmaceutical Interventions
OECD	Economic Co-operation and Development
P2P	Peer-to-Peer
PoS	Proof of Stake
PoW	Proof of Work
RFID	Radio Frequency Identification
SARS-CoV-2	COVID-19
UaV	Unmanned Aerial Vehicle
WHO	World Health Organization

Finally, Section 6 concludes the paper. Table 3 shows the acronyms used in this survey.

2 Blockchain and COVID-19: background, definition and motivation

2.1 Blockchain

BC technology has gained popularity in recent times due to the success of Bitcoin. For example, Dinh et al. [32] suggested how BC has made its way outside the cryptocurrency world to support user-defined models in various domains [94]. Li et al. [73] also describes that BC is a decentralized system that does not need any trusted third party for authorization. Instead, it adopts decentralized consensus mechanisms to ensure the authenticity and persistency of the data and transactions. Li et al. [73] define the four major consensus mechanisms to be used in the smart solutions, which are as follows.

- *Proof of Work (PoW)*: It is a puzzle-based method wherein the authenticity is verified when the node creating a block computes a puzzle and then broadcasts to the same other nodes in the network [73].
- *Proof of Stake (PoS)*: In this method, before creating and broadcasting a block, the node needs to pay some minimal cryptocurrency, i.e., to hold the stake and if the block can be authenticated, then the cryptocurrency is refunded back to the node [73].
- *Practical Byzantine Fault Tolerance (PBFT)*: It allows a maximum of 1/3 malicious byzantine replicas where a primary node chosen in every round has to order the transactions. If it receives 2/3 of votes from the other nodes, it enters into the next phase; otherwise, reaching the common consensus is difficult. This is based on Byzantine agreement consensus [84].
- *Delegated Proof of Stake*: It is similar to PoS, but here the different organizations present in the BC network choose their respective representatives, which are involved in the consensus mechanism [84].

BC maintains a distributed ledger, which maintains a set of global transactions whose existence, values, histories, and order are agreed upon by all network nodes. Each node has a replica of the data, which helps to verify the transactions. Moreover, BC is also defined as an append-only data structure managed and maintained by a set of nodes in the network that offers greater security than the existing centralized systems since it can tolerate arbitrariness of the nodes [32, 44].

Zheng et al. [138] proposed architecture of a typical BC along with the structure of a block, in which every block in the BC is connected to its parent block, as shown in Fig. 3,

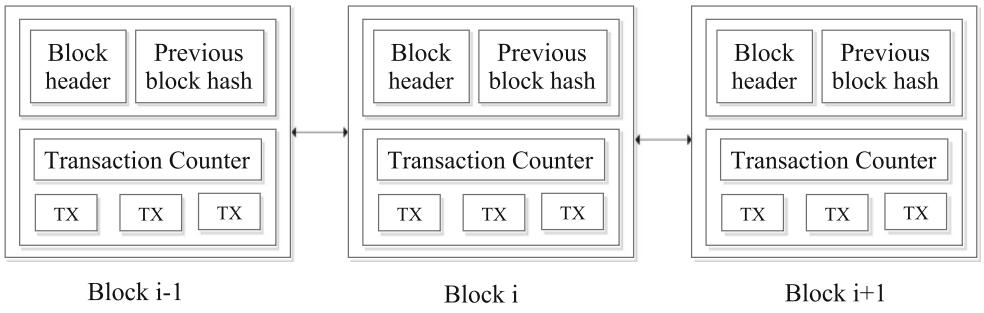

Fig. 3 A typical BC architecture

through a hash value. However, the first block has no parent and it is called the genesis block.

Figure 4 shows a block in BC, which consists of the block header and the block body. In general, the block header includes [138]:

- *Block version*: It describes the type of the block and its corresponding validation rules.
- *Merkle tree root hash*: It stores the calculated hash values of all the transactions in the block.
- *Timestamp*: It represents the time in seconds in Universal Time Coordinated format at which the last transaction was stored.
- *nBits*: It gives the threshold value for a valid block hash that can be used to identify a transaction uniquely.
- *Nonce*: It shows the number of transactions in the block; it generally starts with 0 and increases as and when a new hash value is calculated for the incoming transaction and stored in this a 4-byte field.
- *Parent block hash*: It is a 32-bit hash value of the previous block to which it points to form a logical link.

The block body is comprised of two components: transaction-counter and the various transactions that the block stores [116]. There is an upper limit to the number of transactions that can be stored in a block, which is decided based on each transaction's block size and size. The validation of these transactions is carried out by asymmetric cryptographic methods to check their authenticity [48, 138].

Zheng et al. [138] categorized the existing BC systems into three categories: public, consortium, and private. These categories are differentiated based on their accessibility control over the BC system. The accessibility control gets tighter hierarchically, going from public BC system to consortium BC system and private BC system. [138].

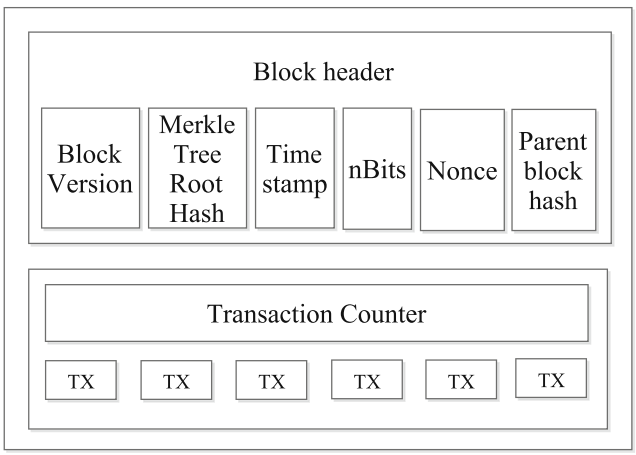

Fig. 4 The structure of a block

2.2 COVID-19

Novel coronavirus, which was first discovered in Wuhan, China, at the end of 2019, belongs to the family of coronaviruses. It presents with pneumonia-like symptoms and it is communicable by the air and is spread due to close contact with an infected person. The spread of this virus is so fast and the WHO has forced to enforce its status as a global pandemic after a month of its spread. This virus has caused a massive scare among the people globally and has compelled business owners worldwide to scale down their operations or even shut them down in cases such as tourism and transport. It is forecasted by many global institutions such as Organisation for Economic Co-operation and Development (OECD), that this pandemic will slow down the economy and the world will see its lowest economic growth rate since 2009 [38].

Since vaccines are not available for this new strain of coronavirus, so the treatment options mainly consist of two options: suppression and mitigation. The main goal of suppression is to reduce the spread of the virus and eradicate the virus's human-to-human transmission. The objective of the mitigation is not to stop the growth, but to reduce the health impact brought on by the pandemic [37].

The virus has now spread to over 188 countries and most of the governments are implementing NPIs to curb the growth of the virus. NPI policy advocates the principle of social distancing and avoiding physical gathering in large numbers. This type of strategy successfully prevented the spread of the virus in previous pandemics, such as the Influenza pandemic of 1918 [37]. However, such strict measures often have a huge impact on the economy. Hence,

countries across the globe are trying to find the right balance between them. Social distancing norms worldwide are being phased out and relaxed to allow economic activities to occur. It aims to save lives and at the same time ensure that economy is not slowed down drastically [132].

Governments across the globe are also compelled to the wide-scale surveillance of their citizens to carry out contact tracing. Contact tracing is pinpointing whether a person has come in close vicinity with an infected person or not [39]. This is a proven method to prevent the spread of such infectious diseases. Previously contact tracing was achieved by relying on the people, but nowadays, it is implemented using smartphones to track and trace the users. However, this approach faced some criticisms also, as it violates the privacy of the users and puts a risk of exposing the person's data [24].

COVID-19 pandemic can only be brought under control through effective data sharing and its management. The drawback of using a centralized system to tackle COVID-19 situations is that there is continuous data loading by different organizations that work under one central authority, which makes it ineffective. Also, data security is an issue. A BC can help to overcome these obstacles since it does not work on a single centralized system [60].

This pandemic has brought a new challenge and the world is dependant more than ever on technologies to overcome these challenges. In this paper, we discuss the possible use case of BC technology to overcome the challenges brought by COVID-19.

2.3 Potentials of the Blockchain and COVID-19 integration

2.3.1 Definition of integration of Blockchain and COVID-19

BC technologies are gaining more prominence as they offer a wide range of applications in various domains. Researchers are also exploring its potential in the healthcare domain [138]. However, the use of BC in the healthcare domain was made first in 2011, where a common database was created for doctors, nurses, pharmacies, and other stakeholders in the sector [50, 104]. Many institutions and companies worldwide are working on integrating BC in their solution space to counter the effect of COVID-19. The main aim of integrating BC is to combine all the verifiable and trusted data sources. One of the unique advantages of BC is that it can continuously validate data even in real time, which is immensely important to fight against COVID-19.

Current issues in the healthcare domain as identified by Bell et al. [12], McGhin et al. [78] and Kumar et al. [67]includes:

- *Healthcare data interchange*: Patient data which is to be exchanged between various stakeholders must have some protection mechanism in it [61].
- *Nationwide Interoperability*: Legacy healthcare systems often have the patient data stored in fragments in a centralized system, which does not allow easy sharing of data between stakeholders.
- *Mobility*: As patients are becoming more mobile due to the era of smartphones, they expect their healthcare records to meet the same level of mobility, i.e., so patients need real-time access to their data from anywhere on any device.
- *Supply chain management*: Stock management and authentication is a big concern in healthcare as its timely delivery and authenticity determine the successfulness of the treatment.
- *Drug tracking*: Drugs mix-ups between patients are frequent in the medical domain [127] and also the presence of counterfeit drugs.
- *Payment frauds*: Double payments and insurance frauds are high-risk issues, especially when hospitals are under chaos in times of pandemic like COVID-19.

BC can be a viable solution to handle the aforementioned issues and it offers a secure end-to-end solution to the end-users.

2.3.2 Security challenges in COVID-19

The world is under the threat of a pandemic like COVID-19, and in this pandemic, the healthcare sector has the most important role to play. The cases have been increasing exponentially and also the data. Handling this ever-growing data securely is a big challenge for healthcare professionals.

Patient data is the most valuable resource in the healthcare sector. Despite knowing the privacy drawbacks of online access of their healthcare records, 90% of the Americans still prefer online access [135]. The information is gathered over the years by physicians and patients, which, if combined and made accessible to both the parties without having to give it to a trusted third party for management, is highly demanded [135]. Medical information is of two kinds: historical data of the patient and the real-time monitoring data, and its security is of the highest concern [118]. Centralized systems are inadequate to secure this data and the data breaches have serious consequences (e.g., malicious attacks are a risk to the patient's privacy) [78].

Some of the major security challenges to be overcome in the fight against COVID-19 as set out by McGhin et al. [78], Azim et al. [11], and Nguyen et al. [85] are as follows.

- *Data integrity*: The data of the positively tested patients is not only important to the hospitals where the doctors are treating them but also to the R&D department to aid

them in their work of finding the vaccine for COVID-19 [78]. As COVID-19 has spread around the world, rumors are also spreading, which may lead to false conclusions [11].
- *Interoperability*: Centralized systems do not support it. Looking at the situation that this pandemic has created, there is an immense generation of records daily at different locations, which is stored centrally at different hospitals and may lead to fragmentation of data, loss of data, and slow access of data [78]. The other sources of data relevant for coronavirus are clinical labs, inventories, financial institutions [85, 111]. Sharing these scattered data without being prone to attacks along with maintaining integrity is the key challenge. Also, it may be possible that different encryption standards are used by the various data stakeholders, which refrain others from accessing the data [78].
- *Immutability*: For the containment of the virus, it is required to trace the contact history of patients and the public to determine the origin of the infection and prevent its further spread. Inaccuracy or change in this data may neglect some of the potential sources of the virus and hence the disease would spread more [11].
- *Transparency*: If all the information is not available due to the government's extra secrecy, it may lead to the degradation of public decision-making power. This, in turn, prevents the citizens from having a controlling power, which hampers the balance between the society and governance [69]. Therefore, maintaining the transparency of pandemic data together with anonymity, respecting the patients' privacy, during world public health emergencies is needed for public decision-making and good governance [11].

2.3.3 Opportunities brought by Blockchain to COVID-19 pandemic

BC is one of the emerging technologies which shows great promise for a variety of applications. We have identified some key characteristics of BC and explored how they can be advantageous in tackling the COVID-19 pandemic. Table 4 shows the various characteristics of BC and their potential applications that can help tackle the COVID-19 crisis, further explained below.

- *Decentralization*: BC has a peer-to-peer (P2P) decentralized architecture wherein each member has access to the entire network and takes part in verification and validation of the transactions. The advantage of such an architecture concerning the COVID-19 pandemic can be when independent stakeholders want to collaborate; they can do so without giving full control to a central

Table 4 Main characteristics of Blockchain and their potentials to COVID-19

Characteristics of BC	Description	Potential applications to COVID-19 pandemic
Decentralization	Users have complete authority over their data as there is no central third party to validate and perform the transactions [86].	Unwanted disclosure of the sensitive patient data to the third party, which might exploit the data is prevented with the decentralized architecture.
Increased capacity	A higher storage capacity and computational power for the whole network as many low processing computers work in parallel.	Accommodate the heavily increasing data of COVID-19 patients. Also, high computational power adds to the rate at which analysis and decision-making are carried out.
Transparency	The data stored in the BC system is accessible to each node in the network. Any registered user can check the contents and review the status of any transaction at any time [75].	As the data is visible to every computer in the BC network, tracking potential patients will be easier due to easy access of patient data and sharing of new treatment methodologies between researchers.
Autonomy	As a result of the consensus algorithms, every node on the BC system can control the data without any interventions [75].	Preserves integrity of the data and gives a free hand to the nodes in the network to decide its data access controls.
Persistency	Transactions are verified on the spot and the invalid transactions can be discarded [138].	Faster validation and correction enable quicker decision-making, which is needed in the times of a pandemic.
Immutability	The records once inserted in the BC are preserved forever and cannot be changed [75, 108].	Susceptible patient data and records are protected from being exploited, which helps in efficient data sharing.
Anonymity	Each user is assigned a general address with which they interact with the network. This assigned address cannot be matched with the identity of the user [138].	BC supports pseudonymity, which solves the various stakeholders in COVID-19 like patients, hospitals, and inventories, not to disclose their identity entirely due to security reasons.

authority [71]. Also, this decentralized architecture is not prone to a single point of failure than traditional centralized systems. In the case of a decentralized system, if any node goes down, the working of other nodes is not affected [30]. In such cases, the healthcare system must always be functioning. The inability of the system to do so can be potentially life-threatening. Also, due to the absence of a central authority, all the data ownership belongs to the patient and they have full access to it. The working of this distributed architecture also ensures the user's privacy because data is stored using hash value instead of patient's actual names.

- *Increased Capacity*: The main advantage of P2P networks is that all the data is stored in a vast network of geographically isolated computers as opposed to being stored in a few centralized servers. The capacity of such types of networks is always increasing; as a new node will join the network, it will also start contributing to the network's total capacity. This increased capacity can be useful in this pandemic to store the vast amount of ever-growing patient data. The increased computational power can be used to reduce the time in verifying the transactions, thus allowing more transactions per second. The computational power can also aid in creating a vaccine for this pandemic by helping run-time simulations. FoldingCoin is an initiative by Stanford University, which exchanges crowdsourced computing power for cryptocurrency as a reward [110]. For COVID-19 research, the COVID-19 HPC consortium was created to accelerate research across the globe. It currently has 483 petaflops of computing power [28], which is almost double the capacity of Summit, the fastest supercomputer exist the world [58].
- *Transparency*: BC networks offer transparency like no other network. In such networks, the ledger is shared and is available for every member node to access. Nugent et al. [87] presented a BC-based smart contracts system implemented on the Ethereum network for medical clinical trials. The credibility of such trials is often undermined due to missing data, data loss when passed from one entity to another, or discrediting the data due to data snooping. Also, in healthcare, there is a trade-off between providing transparency and maintaining the privacy of the patient since the miner has a complete ledger of all the data in the network [136].
- *Autonomy*: As there is no single central authority governing the transactions, all the member nodes of the BC can access the data and add another data without any external source watching. Since the patients can access the data on the network and they can also connect with other patients across the globe who may be suffering from the same medical condition. The architecture ensures that patients have complete autonomy over their data and they can choose to whom they want to share their data [114].
- *Persistency*: The BC network can quickly validate all the transactions and allows only the valid transactions to enter into the network. Once the transaction has entered in the network, the network does not allow rollback or deletion of any transactions [138]. This characteristic enables faster and correct decision-making, which is required to tackle the COVID-19 situations. This characteristics of BC can also help in management of supply chain of COVID-19 vaccines.
- *Immutability*: Records once entered into the BC network can never be removed or deleted. This characteristic ensures that all the transactions are stored in the BC forever. The advantage of this to tackle the COVID-19 pandemic is that if a patient is referred to another doctor, the second doctor will have access to the entire patient history. However, a potential shortcoming here is the 51% attack. In such attacks, a single entity controls more than 51% of the total nodes and has complete access to the network and makes changes [75, 108].

3 Blockchain for COVID-19: a solution taxonomy

In this section, we present a solution taxonomy abstracted in to seven phases such as contact sharing, patient data sharing, supply chain management,payments, dash board, security of data, and vaccination. The description of each phase with a relative comparison of state-of-the-art is explained as follows. Figure 5 shows the various aspects considered for the proposed solution taxonomy of integrating BC to tackle the COVID-19 crisis.

3.1 Contact tracing

The most significant part in the battle against COVID-19 is contact tracing since it is a highly infectious disease. Until any vaccine is made public, it is vital to trace down the source of infection and thus limit the spread. A total lockdown employed by some countries has influenced the economy unfavorably, and hence it is needed that the economic activities keep at pace.

Considering the economic condition, the social distancing norms have been eased by various governments to recover from this downfall. However, it should not be forgotten that the coronavirus still prevails and hence keeping track of the contact history of people is very critical [132]. Choudhury et al. [25] suggested that the contact tracing

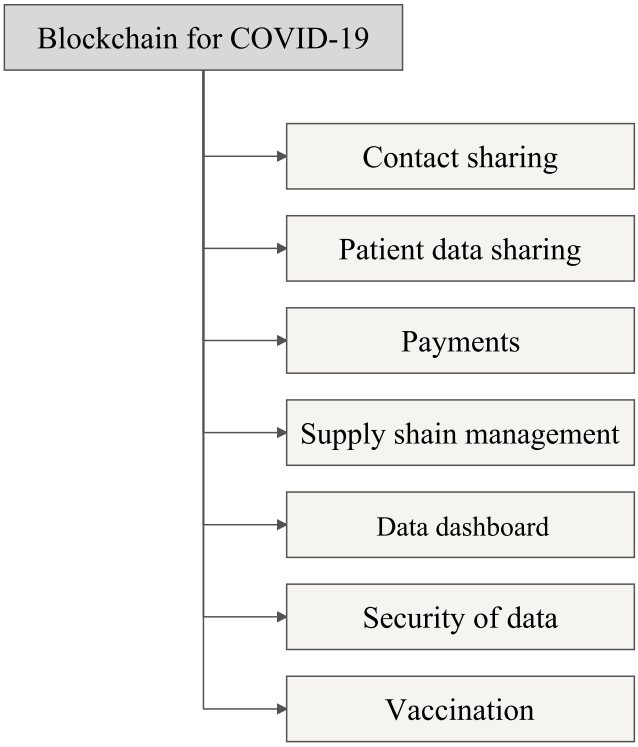

Fig. 5 Blockchain for COVID-19: A Solution Taxonomy

applications must alert the people about the vicinity of the virus and about the people they plan to meet or places they plan to visit in the future, along with showing statistics of several infected people and status of various regions. These applications can be proven to be beneficiary through large public participation and hence the users must be assured of their privacy [25].

Some of the popular contact tracing mobile applications developed by various countries such as Singapore's TraceTogether, UK's NHS Contact Tracing App, Google/Apple's Contact Tracing App, China's Health Code System, and India's Aarogya Setu App [25]. All these applications use Bluetooth signals from smartphones for contact tracing. But Bluetooth alone is not adequate for sharing information because it has security issues like bugging, sniffing, and jamming, which does not guarantee the protection of the user's privacy. The integration of BC with such contact tracing applications can solve security and privacy issues while keeping the transparency of the data intact [132]. Also, the authors in [63] have compared the centralized and decentralized approach for contact tracing, highlighting pros and cons of each approach, and have presented an analysis on role of BC in the contact tracing application.

Xu et al. [132] proposed a BC framework for contact tracing named *BeepTrace*. The diagnostician verifies a positively tested person and alerts the others who might have come in his/her contact. In this approach, the users first have to register to the Certified Authority (CA) for obtaining their keys, which would be used for encryption and verification. The user's pseudonym is determined by the encrypted version of his/her allotted keys and the current encrypted location. When a person is diagnosed and verified to be tested positive, then the diagnostician signs the pseudonym of the diagnosed user. The updated data is visible to everyone in an encrypted form, but only a registered user can decrypt it using his/her private key. Thus, the concerned user can look at the history of the infected patient and see the risk level analysis updated by the trusted third party involved in managing all this. Although in their proposed approach uses a trusted party, the user's privacy is also protected since only pseudonyms are used for identification [132].

Hassanein et al. [122] presented a novel BC-based framework to combat the spread of coronavirus. Their framework is an amalgamation of four subsystems, which work in harmony — Infection Verifier Subsystem (IVS), P2P Mobile App, BC Platform, and Mass Surveillance System. Here, the user's anonymity is preserved as it uses regular expressions to represent its user. The data of infected people and the people or place they might have infected are stored in the BC using IVS. An infected person is represented by *infection pattern* as a regular expression and the patterns obtained from this regular expression, named *infection instances*, represent the people and places the concerned patient has infected. The verification of an infected instance belonging to a particular infection pattern is done via a finite automaton. The P2P Mobile App is engaged in intimidating the potential catchers of the virus. The Mass Surveillance System carries out contact tracing of the users. However, they have left it open for thought to implement this surveillance system [122].

Public Health BC Consortium (PHBC) is a BC-based framework used for monitoring the spread of the infection. It has additional functionality to recognize the zones without the verified reports based on real-time updates from the surveillance systems with AI and geographical positioning systems. This approach performs tasks such as keeping track of contact of the users and intimidating the potential patients to the virus [95].

Another BC-based framework was proposed by Choudhury et al. [25], which is named *CovidChain*. Like other proposals, this approach also helps track and alert people of their possibility of coming in contact with an infected person. Besides, it also enables users to check the record of people with whom they might interact closely using a digital pass that stores their contact and visits history. All the data is stored in the BC in a distributed manner, so the proposed framework ensures transparency. The stakeholders are also ensured of their anonymity and privacy as no backtracking of a transaction to its origin is possible except when

the authorities assemble and invest a significant amount of public resources due to the immutability property of BC [25].

Peng et al. [96] have proposed a BC-based privacy-preserving solution for contact tracing which they called *P^2B-Trace*. The main four players in this system architecture are the following: (i) *workers*: who verify data through consensus and then add a block to the blockchain; (ii) *patients*: people who have positively tested for COVID-19; (iii) *clients*: people whose COVID-19 report is not known to the system; and (iv) *authority*: the healthcare center or the hospital for checking vacancy of beds for the patients to get admitted. They adopt a zero-knowledge proximity verification scheme for privacy preservation. This approach uses Bluetooth for generation and exchange of tokens in proximity which are regularly updated and once the contact-matching with an infected person is confirmed by the workers, users are notified on their local devices.

Ricci et al. have described in their review the three types of BC-based contact tracing techniques: (i) Proximity-based Contact Tracing, (ii) Location-based Contact Tracing, and (iii) Mobile Operator Contact Tracing. The authors have also given a comparison between the various BC-based contact tracing solutions taking into considerations attributes like the communication infrastructure, cryptographic technologies, the actors, type of blockchain and its role in the system [105].

Constantinos et al. [7] have thought a step forward and looked into helping the economy come back to play. They have proposed a Digital Health Passport (DHP) to enable international travel to assure safety. Digital Contact Tracingis a local thing, and most of its approaches are dependent on a smartphone being carried all the time by the users. Whereas in DHP, it is just verification without being worried about privacy. A local Testing Health Facility issues the DHP after testing the person. Based on the test result, he/she is issued a DHP. This DHP is then registered, verified, and added to the global DHP BC by the National Health Security of the country. Then, the issued DHP of the user is verified by the airlines before boarding, and on satisfactory hygiene result, the passenger is allowed to board the aircraft [7]. Table 5 gives a relative comparison of Blockchain techniques' potentials in contact tracing.

3.2 Patient data sharing

In COVID-19 pandemic situations, sharing of information over a network securely is of paramount importance. The data to be shared can be in the form of patient medical records, researcher-specific records, or about the supply chains, etc. BC technology can aid in all aspects of data sharing.

Medical records play a critical role in diagnosis and treatment methodologies employed and must be shared

Table 5 A relative comparison of Blockchain techniques potentials in contact tracing

Author	Year	Objective	Key characteristics
Xu et al. [132]	2020	Proposed a BC-based framework called *BeepTrace* for contact tracing in times of COVID-19	Privacy-preserving data sharing using encryption techniques with the psuedonymity property of BC to preserve the users' identity.
Choudhury et al. [25]	2020	Proposed a BC-based contact tracing framework called *CovidChain*	It issues a digital pass, which enables user to check the record of the people they are planning to meet.
Torky and Hassanein [122]	2020	Proposed a four system BC-based framework for verifying and detecting the positive cases of COVID-19	Regular expressions are used for the data processing in the BC and data storage.
PHBC-Public Health BC Consortium [95]	2020	Proposed a framework for contact tracing based on the BC	It can identify the zones in real time without waiting for the verified reports.
Constantinos et al. [7]	2020	Proposed a digital health passport for safe international travel	It works on a global BC network where after a person is tested and verified by local healthcare, then he/she is issued this digital password, which is uploaded to the BC.
Peng et al. [96]	2021	Proposed a BC-based privacy-preserving approach called *P^2B-Trace*	Uses Bluetooth for proximity checking and have employed admins for double verification of data before adding to the blockchain.
Ricci et al. [105]	2021	Presented various types of BC-based contact tracing techniques	Highlighted the working, advantages and disadvantages of each technique and their future works.

among various parties such as insurance companies, healthcare providers, and pharmacies to dispense the required medicines and the patient and their family for their follow-up to the treatment. Such records must be kept up-to-date. Also, the entire records are not available for everyone to view, so it is a tedious task to design a proper access control mechanism [36]. An AI and BC-based mobile application was proposed by the authors of [77], which can help in self-testing in the COVID-19 pandemic. The AI component was utilized for the diagnosis, whereas the BC component of the application was used to facilitate data sharing and data amalgamation [77].

Azaria et al. [10] proposed a BC-based framework for medical data access and permission management, which they dubbed as *MedRec*. It was build using the Ethereum BC. The implementation combines all the fragmented data into one, then logs it in the network and provides the patients with a comprehensive log of their medical history. It also facilitates the data exchange between healthcare providers and provides them a single point of reference to get the updates. The proposed solution is built on a decentralized system, but it cannot guarantee the security of individual nodes [10].

Another approach proposed by Xia et al. [130] which combined cloud computing along with BC to facilitate medical data sharing. As the world is moving towards cloud-based storage over the traditional in-house storage system, they proposed a framework called *MedShare* to allow data sharing among Cloud Service Providers (CSP) securely. *MedShare* exploits several properties of BC, such as all records are stored in the network in a tamper-proof manner, prevents malicious access of data by invalidating transactions and revoking access to entities on detecting unauthorized access of data. *MedShare* also gave better performance compared with current data sharing models among CSPs while providing better security [130]. Xia et al. [131] also proposed another BC-based solution for cloud-based data sharing of medical information called *Blockchain Based Data Sharing (BBDS)*. The network only allows access to invited users and it allows access to data only after their identities are verified using cryptographic keys. When compared to the BC network, BBDS is lightweight and is scalable due to the support of the cloud [131].

To accelerate the COVID-19 research, an unconventional approach was proposed by Celesti et al. [18] which leveraged the technical benefits of the cloud, IoT, and BC. A group of hospitals forms a federated cloud over which all the data regarding the clinical trials is shared. The medical examinations are performed using IoT devices for the safety of lab technicians. The data is uploaded to the cloud, which can be accessed by any hospital doctor present in the federation. BC technology is used for various features such as immutability, smart contracts functionality, and ensuring the validity of all the transactions [47]. The data is shared in the form of Electronic Health Record (EHR) only and it cannot be traced back to the concerned patient, thus ensuring anonymity and privacy of the user. Both public and hybrid implementations of BC were tested via the Ethereum network. They concluded that the hybrid approach performed better in terms of cost and the average response time [17, 18].

Over the previous few years, due to the advent of wearable technology, complete and comprehensive personal healthcare data is available to healthcare providers, which can aid them in the proper diagnosis. However, sharing of this data must be carried out securely while being convenient at the same time. Liang et al. [74] proposed a healthcare data sharing model, which is a mobile application that periodically collected and synchronized the data from the wearable technology and uploaded it to a cloud platform for easy access to the healthcare entities such as healthcare providers and insurance companies. To maintain integrity of data, the proof of integrity is attached to the BC network; to ensure privacy, an access control mechanism was put in place; and for security, a channel formation scheme was used [74] in their approach.

Donawa et al. [33] identified scalability issues in traditional BC networks of large-scale healthcare systems, which can generate up to 7.5 million medical records per day and proposed a BC-based system capable of handling over 30 million records daily as a solution for the prevailing scalability issue [54]. To achieve this, they proposed a sidechain and the main network to relieve its load and prevent bottlenecking. A sidechain is a child BC connected to the parent BC via a two-way connection. It provides the ability to disburden the parent chain and also provides a platform for testing the new features before implementing them in the main chain. In the proposed architecture, they allotted each patient an individual sidechain, hence adding records to one patient independent of others. The main chain performs tasks such as handling the joining/leaving of the patients in the network and produce a discharge summary at the end of the patient visit. Their proposed model can revolve the scalability issue of the BC when dealing with a large amount of transactions [33].

GlobeChain is a data sharing architecture for a global level that uses BC, which was proposed by the authors Biswas et al. [15]. The architecture designed works primarily at three levels: (i) *Physical Level*: collection of the patient's data, (ii) *National Peer Level*: maintaining healthcare data of patients at national-level in a BC, and (iii) *Global Peer Level*: cross-border data exchange through multinational BC centers called peers. Such maintenance and regulation of healthcare data at global-level makes it easy for the authorities in times of emergencies to alert

the crowd of an outbreak and thus immediate preventive measures can be taken [15].

All the aforementioned approaches discuss the patient data sharing model between healthcare service provider entities. Still, a secure method is needed to share the patient data between researchers working on developing and performing clinical trials on new drugs. *FHIRChain* model was proposed by Zhang et al. [137] which is a BC-based architecture for collaborative clinical data sharing. The main advantage of this model includes preventing the vendor lock-in issue found in the conventional system as the data is stored in a decentralized manner while maintaining the data ownership. This model only exchanges reference pointers, which refer to the BC component instead of exchanging actual data; hence data ownership is maintained. One of the potential issues with this prototype is that it cannot prevent clinical malpractices. It only facilitates the sharing of information and it is assumed that all the information shared is authentic and accurate [137]. Table 6 gives a relative comparison of Blockchain-based techniques used in patient data sharing.

3.3 Payments

BC technology was initially conceived as a new and safer platform for financial transactions. Bitcoin, a cryptocurrency, was the first implementation of BC, which was used as a payment system.

Since the pandemic has put a strain on healthcare resources; the industry needs volunteers' help to ease the burden of the scarcity of medical equipment and affordability by underprivileged people. It has been found that more people would be attracted to the volunteering program if some incentive is associated with it [20]. He et al. [56] proposed a distributed P2P BC-based system, which incentivize the volunteers using cryptocurrency [56]. Another incentive mechanism was proposed by Xuan et al. [133] based on smart contracts. The smart contracts

Table 6 A relative comparison of Blockchain-based techniques used in patient data sharing

Author	Year	Objective	Key characteristics
Azaria et al. [10]	2016	Proposed a BC framework build on the Ethereum BC called *Medrec*	Facilitates data access and control and allows the amalgamation of all the fragmented data. All records are stored with a unique reference number to identify them
Xia et al. [130]	2017	Proposed a BC and cloud computing-based approach for data sharing	All the data is stored in the cloud while exploiting BC properties such as immutability and verification.
Xia et al. [131]	2017	Proposed a lightweight BC and cloud computing-based approach for cloud-based data sharing	Access is granted only after identity is verified using the crytographic keys.
Liang et al. [74]	2017	Proposed a data sharing model using BC for wearable technology	Mobile application periodically uploads the data to the cloud, which can be accessed by healthcare provider entities only after verification. Proof of integrity is put in the blocks to ensure the integrity of the uploaded data.
Zhang et al. [137]	2018	Proposed a patient data sharing model using BC dubbed as *FHIRchain*	Decentralized architecture to avoid vendor lock-in problem. Anonymity is maintained as the reference to the data are only shared and not the actual data itself.
Donawa et al. [33]	2020	Identified the scaling issues while employing BC for healthcare and proposed a solution for the same	Proposed solution used the concept of side chains and was able to handle up to 30 million transactions daily
Mashamba et al. [77]	2020	Proposed a mobile application based on AI and BC for self-testing	AI was used for diagnosis and BC was used for efficient data sharing
Celesti et al. [18]	2020	Proposed a multi-disciplinary approach consisting of cloud computing, IoT and BC for data sharing	IoT is used to avoid human touch, the cloud is used to store the information and BC was utilized to ensure security, the validity of transactions and preserve anonymity
Biswas et al. [15]	2021	Proposed a global-level architecture for data sharing called *GlobeChain*	Enables healthcare data maintenance at global-level enabling easy analysis and alerting of an outbreak to the masses.

were based on evolutionary game theory and they could dynamically reward the participants to encourage the volunteers [46, 133]. The volunteers are to work side-by-side with the government to mitigate the COVID-19 crisis.

The COVID-19 crisis has brought in donations from across the globe for providing aid to people who are facing a hard time due to the pandemic. The donations are in monetary form or in-kind and often, corruption by officials associated with it makes it all in vain. BC can be used to bring transparency to a donation by storing the entire process of donation. The donors will have complete information about where their donations are being utilized [21]. Binance charity seeks donations in the form of BC cryptocurrency, which would then be utilized to purchase goods and supplies for the worst affected regions [85].

Smart contracts in the case of BC can be tailor-made to create a value-based payment system. In such a payment system, the payment is made only after requirements are fulfilled in the BC system. This eliminates the mistrust factor between the doctor and the patient. Smart contracts can also be programmed to impose a financial penalty on the doctors if some error has occurred, thus making the doctors more responsible for their actions [134].

Sirisha et al. [113] proposed a donation platform called *Charity-Chain* which was build on top of the Ethereum network. The primary aim of this platform was to ensure that the donor has full knowledge of the current state of his/her donations and bring transparency to the process [113]. The advantages of using BC for philanthropy include transactions at higher speeds and lower costs, and also increased visibility and traceability of the transactions [70]. The primary issue while utilizing BC is the high energy consumption that is incurred due to the crypto-mining process, which leaves a large carbon footprint and that criminals may use BC for illegal activities such as tax evasion [125].

Wu et al. [129] proposed an end-to-end BC mechanism to manage the charity donations during COVID-19 pandemic. The proposed system was build on top of the Ethereum network and can facilitates information sharing, allocate the funds as well as internal management. The authors in [102] presented a BC-based Charity 4.0 using the example of Charity Wall as a case study. The study presents the shortcoming of the platform and drawing comparisons to how BC technology help in preventing them. Table 7 gives a relative comparison of Blockchain-based techniques used in payment mechanisms.

3.4 Supply chain management

The supply chain management of drugs monitors all the phases in the life cycle of drugs, starting from research going through clinical trials to licensing and its production and distribution. Counterfeiting of drugs is the most serious problem, which can be resolved to ensure the legitimacy and quality of drugs that are distributed and consumed as it risks the lives of patients [14]. The traditional approaches used Radio Frequency Identification (RFID) which is wireless and has individual identification. But creating a unique identification from the database is easy for any attacker and hence this approach is prone to counterfeiting. BC is one of the best solutions to prevent counterfeiting as it does not support mutability and hence fraudulently produced drugs cannot enter the legitimate supply chain [123]. Dinh et al. [85] have summarized the key solutions that BC offers to assist the drug supply chain as product requirements, supply creditability, transportation tracking and customs certificate [85, 93].

The authors of [83] have highlighted the drawbacks of circular economy prevailing in the traditional supply chains. They also have pointed out the urgent need for redesigning of the current structure of supply chains and include localization, agility and digitization. These can be

Table 7 A relative comparison of Blockchain-based techniques used in payment mechanism

Author	Year	Objective	Key characteristics
He Y et al. [56]	2018	P2P BC-based incentive mechanism	Used cryptocurrency to incentivize the donors
Sirisha et al. [113]	2019	Proposed BC framework called Charity-Chain	Build on the Ethereum network and provides the donor with complete knowledge of their donation
Yaeger et al. [134]	2019	Eliminate mistrust using smart contracts	Fine is levied on the doctor if mistake is made
Xuan et al. [133]	2020	Incentive mechanism based on smart contracts	Dynamically hand out rewards to encourage the volunteers
Wu et al. [129]	2020	End-To-End BC framework to manage charity contributions	Information sharing, donation allocation, internal management
Rangone et al. [102]	2021	Proposed BC-based Charity 4.0	Case-study to point out advantages of BC

achieved by integrating BC to the supply chain management system and thus create resilience, minimize waste, and support a more sustainable supply chain [83].

Patrick et al. [115] suggested a drug supply chain management system based on BC technology which they called Pharmacosurveillance BC System. The system works on the very popular and open-source Ethereum BC. It has five main actors: the manufacturer, the wholesaler, the retailer, the Food and Drug Administration (FDA), and the last node, which takes care of the customer service, which is a portal website to enable the consumer to have a look at the drug distribution history and be assured of the authenticity of the drugs they are being given. Each drug has its sub-chain in the main BC that consists of all separate actors. Thus, monitoring becomes easier as it is organized and easily accessible due to the transparency characteristic of BC while adhering to the Drug Supply Chain Security Act (DSCSA) standards [115].

Ijazul et al. [53] proposed a solution to overcome the counterfeiting of drugs in the drug supply chain. The manufacturer gives a unique identification number (hash value) to each product, registered on the BC from where it can be easily tracked. The transfer of drugs from one entity to another is done physically while simultaneously registering this transaction in the BC, i.e., the manufacturer, when handing over the drugs to the wholesaler also registers this transaction on the BC and the same is followed by the wholesaler when giving it is to the distributor who further gives it to the pharmacy through the same procedure. The customer can check for the availability and authenticity of the drug on the mobile application and then purchase it from the pharmacy. This transaction is also recorded on the BC [53, 68]. Thus, there is a transparent flow of the drugs from the manufacturer to the end-customer.

Another BC-based approach named *LifeCrypter* has been proposed Manuela et al. [109] to curb the counterfeiting in the supply chain of drugs. It helps to disincentivize the counterfeiting of drugs by assuring integrity, traceability, and transparency in the supply chain. Smart contracts on the BC are used to transfer ownership from the supplier to the consumer and at every intermediate stage, verified by a unique identification tag given to each medicine item. Moreover, it makes the whole process of drug distribution more efficient and reliable. Also, the users can themselves verify the legitimacy of drugs through a simple mobile application [109].

GCoin is a preventive measure against double-spending used to combat the counterfeiting of drugs. This was proposed by Jen-Hung et al. [123] wherein the *G* in the name stands for global governance. The government's involvement as a supervisor is important since surveillance of a lot of resources simultaneously is required, which cannot be achieved when there is distrust among the public. A hash value is obtained by mathematical manipulation on the data related to a drug like its batch number or quantity produced. All such drug information is used to generate a QR Code, which becomes the unique identity of that drug. This system is immune to the counterfeiting of drugs since authorized actors are registered to the *GCoin BC* and only they can carry out the transaction as they possess a private key, which is only known to them [117]. Each transaction carried out between any two parties in the supply chain is recorded on the BC, verified. Then the transaction data is stored in the *GCoin BC* after carrying out encryption using hashing on the transaction data [123].

Omar et al. [89] have proposed a BC-based group purchasing organization (GPO) contract solution using Ethereum smart contracts for healthcare supply chain management. All the stakeholders involved in the supply chain are registered on the BC using registration contracts. A contract passes through all the stakeholders where it is verified and authorized at each point, and then is uploaded to the decentralized storage when all the stakeholders confirm the contract. This ensures that there is no price discrepancy among the stakeholders and streamline communication. Only registered stakeholders can take part in the supply chain, thus data privacy and security is taken care of [89]. Table 8 gives a relative comparison of Blockchain-based techniques used in supply chain management.

3.5 Data dashboard

Currently, most of the information regarding COVID-19 is made available to the public by the government agencies in the form of news bulletins. Johns Hopkins Researchers also created a website that automates some aspects of data collection and displays it. It was found that such websites often lag behind the real statistics and so, these statistics are manually updated frequently by taking note of Twitter news feed, local news services, and the statistics that were sent to the website directly by volunteers [34].

BC can be used to supplement this process, make it tamper-proof and also ensure transparency. *MiPasa* is a BC network build using hyperledger fabric to share and collect the data regarding COVID-19. Its main goal is to provide a secure platform for collecting and integrating various data sources, identifying the mislabeled or misreported data, and ensuring smooth integration of data from various sources. All this information can be made available to hospitals separately beside the common man; then they can work on their action plan [20, 97].

Genobank.io [55], a private company, which has partnered with the Telos Foundation, integrated their platform on the telos sidechain BC and developed the app called *Agerona*. *Genobank* offers the services of personal

Table 8 A relative comparison of Blockchain-based techniques used in supply chain management

Author	Year	Objective	Key characteristics
Ijazul et al. [53]	2017	Proposed a drug supply chain management for local requirements	At every stage of the supply chain, the authentication is carried out before adding the transaction to the BC so that only legitimate actors can participate and take the registration to the BC process ahead.
Hung et al. [123]	2018	Proposed a preventive approach against counterfeiting of drugs named *GCoin* which has global governance over the BC network	Access granted only to authorized users who possess the private key and the items of the supply chain are identified by a unique QR Code thus maintaining the integrity of the items shared along the supply chain.
Patrick et al. [115]	2018	Proposed a BC-based drug supply chain management system	Each item has its own sub-chain which is linked to the main chain thus making it easy to keep a track and monitor the activities taking place on the main chain easily.
Manuela et al. [109]	2018	Proposed an approach called *LifeCrypter* to combat counterfeiting of drugs in drug supply chain	Smart contracts in BC are used for transaction verification as the supply chain moves forward at every stage. Also, the users can check the authenticity through the mobile application.
Nandi et al. [83]	2021	Proposed a new design for supply chain management in healthcare	Integrating BC with currently existing supply chains of circular economy to achieve localization, agility and digitization which can make the process hassle free and reliable.
Omar et al. [89]	2021	Proposed a BC-based group purchasing organization (GPO) contract solution using Ethereum smart contracts	Registration and authorization at each point when data passes through stakeholders ensures high security and privacy of data, as well as eliminates any discrepancies that can take place between the stakeholders.

COVID-19 testing. Users of the app will be able to order the kit online, and upon receiving the kit, the user will scan the kit's barcode and will get registered anonymously on the *Telos BC*. The kit is then sent to a lab and the results are lodged in the BC, which the user can then access. Researchers will be able to see the results available on the BC but would not be able to link them to an individual hence maintaining privacy [55].

Algorand has launched the *iReport-Covid* App worldwide, which is based on the BC technology. It depends on a survey filled out by citizens from across the globe. Their responses are stored on the BC and kept anonymous. This app allows changing the answers of the survey if the symptoms change. Each survey answer is accessible only by the random survey number, which is generated on submission of the survey by the user [29].

Ouyang et al. [91] presented a BC- and smart contract-based framework build on Ethereum chain to function as a early warning and alert system using crowdsourced data. Dhillon et al. proposed a BC-based wellness tracker for healthcare workers using data from health devices. The data present in COVID-19 hot-stops can be analyzed and working hours can be allocated accordingly.

Table 9 gives a relative comparison of Blockchain-based techniques used in the data dashboard.

3.6 Security of data

Although BC is very secure and less prone to successful attacks, but the confidentiality of the patient's data is a concern. The data stored and shared via a BC network must be secured and hence some encryption techniques have to be applied to the data before storing it on the network.

Axin et al. [128] proposed an efficient, privacy-preserving, and traceable attribute-based encryption for BC. It employs fast ciphertext generation due to pre-computation and hence pre-encryption can be performed, a hidden policy which removes the mapping function between access control structures and attributes through an attribute bloom filter, and also whenever a private key of any party in the network is abused, a random third party from the network can conclude the origin of the private key [128].

Table 9 A relative comparison of Blockchain-based techniques used in data dashboard

Author/company	Year	Objective	Key characteristics
Pham et al. [97]	2020	Data collection model build on the hyper-ledger Fabric	Ensure smooth integration of data from various sources and ensure the authenticity of the data.
GenoBank.io [55]	2020	Mobile application called *Agerona* build on the *Telos BC*	*GenoBank* offers testing services and this app will gather all the results anonymously and share with the researchers to help them for obtaining accurate results for their research.
Algorand [29]	2020	*iReport-Covid* App to collect information from all around the world and have a global place to store and get data about the scenarios in different parts of the world	Users are asked to fill the survey and the responses are stored in the BC. The responses cannot be traced back to the user. This data can be used in contact tracing and also shared with doctors for their better knowledge of the symptoms and effects of the virus.
Ouyang et al. [91]	2021	BC-based collaborative dashboard for early warning and alert system that can enable common man to be updated about the situation in his/her surrounding and take relevant steps	BC-based Federated Learning with privacy protection
Dhillon et al. [31]	2021	BC-based healthcare workers tracker that enables to keep a watch on our frontline workers' health	Using data from healthcare devices such as Fitbit to track health parameters of front line workers so that immediate help and assistance can be given to them as they are the saviours in this pandemic situation.

Chen et al. [23] developed a novel approach in which RFID and BC technologies were integrated to facilitate sharing the records of physiological signals between different medical institutes. They have proposed an eight-step mechanism based on fog and BC architecture to facilitate data sharing securely [99]. The control of the medical data consisting of physiological signals remains in the hands of the patients. The eight steps include communications between the patient, the hospital and the attending physician in the form of https request and responses, to prevent eavesdropping [23].

The approach proposed by Joseph et al. [76] for contact tracing is privacy-preserving and zero-knowledge. Moreover, it maintains privacy with the authenticity of the users of their application. This approach discloses the private information of the positively tested patient with the government and his/her doctor, but they have zero knowledge about the patient's contact history [35]. Moreover, the people who have come in contact with this patient are intimidated by the application. Still, they do not know who they might have been infected with, thus ensuring the said zero-knowledge policy. The security of this system is handled by standard cryptographic policies that are driven by some required assumptions [76].

MediBchain was proposed by Abdullah et al. [5], which helps in sharing the data securely while maintaining privacy, authenticity, and integrity. Due to the use of BC, any unauthorized access to the data is prohibited. The parties' identity is protected and the data is stored in an encrypted form for its security. There is a ten-step procedure to be followed before the data is stored in the BC. All these steps use basic key distribution and encryption techniques to share and store the data securely [5].

Similar to DHP proposed by Constantinos et al. [7], Chris et al. [57] have proposed *SecureABC*, which is a BC-based system for verifying antibodies certificates and can be used as an immunity passport. The *SecureABC* protocol works in three phases: setup, issue, and authentication. It is a three-party protocol, which includes the healthcare provider, the user and the verifier. Here, it is assumed that the healthcare provider makes no deliberate blunders in issuing the certificate; cryptographic systems handle the rest for authentication and verification [120].

In COVID-19, managing the ever-growing data is a big task. The authenticity of this data determines the successfulness of the treatment employed and the statistics of the number of cases that decide the overall public panic and reaction towards this pandemic.

Al-Aswad et al. [4] proposed a four-layered BC-based zero knowledge proof model to be used in IoT smart cities to increase healthcare security. The authors proposed a model to be used in the Kingdom of Bahrain by the public and private healthcare providers for a reliable way of sharing medical data. In addition, the zero knowledge proof model can be used in combination with smart contracts to allow for automatic medicine dispensation in pharmacies. Table 10 gives a relative comparison of Blockchain-based techniques used to secure the stakeholder's data.

3.7 Vaccination

The COVID-19 pandemic has again proven that it should not be taken lightly, and strict and conscious measures have to be implemented as fast and as globally as possible. With the passing time, this virus is getting stronger and its new variants are continuously emerging. The most effective way to curb all of this in short span of time is a mass vaccination drive carried out throughout the globe.

Carrying out a global vaccination drive over a short period of time comes with its own problems. The major hurdle is the production-distribution ratio. The production of vaccine doses have to be increased at a higher rate to fulfill the demand, but this is a tough task. So, the already produced vaccine doses have to very carefully and judiciously be distributed. This job can be seamlessly handled by the BC. Frauds in distribution and counterfeiting of the vaccine doses can be ensured not to take place when BC comes in to picture. Thus, the vaccine doses produced can be assured to reach to the citizens with full authenticity.

Leonardo et al. [101] proposed a method for a secure BC-based supply chain mechanism for the COVID-19 vaccine doses. It takes place in five phases: vaccine generation, where the chemical composition, expiration date, and other details about the vaccine along with its serial number are stored on the BC; then, there is international delivery of these vaccine boxes [45], where the quantity received and sent along with a serial number of the box is stored; the third phase is inventory development, where the log of received

Table 10 A relative comparison of Blockchain-based techniques used to secure the stakeholders data

Author	Year	Objective	Key characteristics
Abdullah et al. [5]	2017	Proposed an approach called *MediBchain* which focuses on maintaining privacy, authenticity, and integrity while data sharing	A ten-step procedure of key distribution and encryption before the data is shared via the BC or even stored hence making sure that the key reaches to the required and assigned stakeholder, making it difficult for the attacker to decode the key even if he can successfully extract the key from the network.
Axin et al. [128]	2019	Proposed an encryption method for BC that adds additional security to the data stored in the BC	It enables fast encryption due to pre-computational powers and also can catch when the private key of any user in the network has been abused.
Chen et al. [23]	2020	Proposed a secure way of data sharing by integrating RFID and BC	Eight-step encryption technique to secure the health data among various authorized stakeholders where the physiological signals are used for communication among the health centers.
Joseph et al. [76]	2020	Proposed a privacy-preserving contact tracing approach	It is a zero-knowledge mechanism which means although the positively tested patient's all data is disclosed; the authorities have zero knowledge about his/her contact history; also the people in his/her contact are intimidated about the positive case, they do not know from whom they may have acquired.
Chris et al. [57]	2020	Proposed a secure framework based on BC for verifying antibodies in immunity passport	It employs a three-phase protocol to issue this immunity passport, which cannot be hampered and provide authenticate information
Al-Aswad et al. [4]	2021	Proposed a zero knowledge BC framework for the IoT smart cities of Bahrain	Four-Layer BC framework that can used in IoT smart cities providing reliable way of patient data sharing

and sent boxes of vaccine is maintained in the BC; then comes vaccine application where the details such as time and date of application of vaccine, location of application of vaccine, data about who applied for the vaccine and to whom it was applied are stored in the BC; and lastly monitoring the patient to whom the vaccine was applied for the symptoms and result of the vaccine. Since, BC is used in each phase; so it is a highly secure and reliable approach [101].

Antal et al. [8] have put forward the reasons to use BC in vaccine supply management cycle — from manufacturers to distributors, from distributors to medical centers, from medical centers to doctors, and lastly from doctors to the patients or beneficiaries. A very close monitoring and tracking is required for the vaccine doses especially when they have go through multiple nodes until they reached to the common man. From the time, the vaccine doses leave the manufacturing place, they have to be monitored for their surroundings as they are very temperature sensitive and so transport is also a big issue to be tackled, which can be taken care by IoT — sensors and actuators. BC can help in maintaining the trust when multiple participants are involved, confidentiality is required, real-time data monitoring is necessary, and also having all of this data recorded and maintained at a central point is risky as this data has to be protected and cannot be afforded to be deleted; thus, a distributed ledger system comes handy in such cases [106]. So, the authors of [80, 107] suggested a IoT integrated BC solution, named *BlockColdChain*, *Go-Win* respectively, for efficient vaccine distribution, where temperature sensors and the corresponding monitoring system take care of the well-being of the vaccine doses when they are being transported or stored, while BC takes care of the supply management — authenticity, security and privacy.

The next step is to have an authorized and authenticated proof of vaccination. Vaccine certificates or passports must be issued once the dose is given to a patient. Now, the problems that occur are again the same — authenticity, privacy, and security of this information. With hackers becoming more stronger, the frauds are increasing — fake certificates, black marketing of vaccine doses, etc. To handle the aforementioned problems, Tsoi et al. [124] proposed a BC-based solution of vaccine passports. BC proves to be one of the safest way to store and share this sensitive data required for monitoring the patient post vaccine to know its side effects, how long the vaccine provides protection from the virus and alert about any new variants emerging out there despite the vaccine being taken. Table 11 gives a relative comparison of Blockchain-based techniques used in vaccination supply chain.

4 BC-based digital vaccine passports: a case study

To demonstrate the usefulness and versatility of BC techniques in the COVID-19 pandemic, we present a case study. In this case study, we specifically focus on applying BC techniques for the administration of COVID-19 vaccines. Since the emergence of COVID-19 in November 2019, the researchers worldwide have been teaming up

Table 11 A relative comparison of Blockchain-based techniques used in vaccination supply chain

Author/company	Year	Objective	Key characteristics
Leonardo et al. [101]	2020	Proposed an early BC-based supply chain management system for the COVID-19 vaccine	Keeping track of production, distribution, details of the patient who gets the vaccine, and also details of the person who injects the vaccine.
Antal et al. [8]	2021	Explained the reasons to use BC in vaccine supply chain	Described the role of each actor, actions that take place at each actor, and how the chain proceeds further with double verification at each point.
Mendonca et al. [80]	2021	Proposed a BC and IoT-based vaccine supply system called *BlockColdChain*	Protection of vaccine doses using temperature sensors and actuators due to their temperature sensitivity and BC used to authenticate and secure the distribution of these doses.
Dr. S. Saranya [80]	2021	Proposed a IoT-integrated BC solution called *Go-Win* from a secured supply chain of vaccine doses	A system architecture to safely deliver the vaccines to health centers with cloud services and smart IoT monitoring system.
Tsoi et al. [124]	2021	Proposed a BC-based technique to issue vaccine passports to vaccinated individuals for prevention of frauds and analysis of post vaccination scenarios	The vaccine passport consists of all the data required to check, analyze, monitor and alert on the basis of post effects of the vaccine taken.

for developing an effective vaccine for inoculation against COVID-19 [27]. Numerous governments worldwide have endorsed fast-track approval of vaccines based on clinical studies. This has led to vaccines with efficacy as high as 95% [19].

The discovery and licensing of vaccinations have resulted in the launch of mass vaccination campaigns around the world and the expansion of vaccine manufacturing facilities. Because these COVID-19 vaccinations were produced quickly and tested on a limited group of people, some patients have experienced side effects after receiving the vaccine, and some of these side effects have been permanent in nature [26]. Most of the countries offer WHO-approved vaccines via government-run healthcare centers. After a citizen has been fully inoculated, then they get a certificate from the agency that can act as a proof of vaccination. However this method has potential pitfalls, such as:

- If a batch of vaccines is bad and citizens were jabbed with it. Trying to locate such citizens can prove to be a mammoth task.
- If the proof of first dost of vaccination is lost by the citizen, then it might be hard for them to obtain the second dose
- Due to the scarcity of vaccines, black marketing of vaccines has emerged, and various cases have been reported the citizen getting the vaccine in-spite of non-eligibility [41].
- While travelling international, the certificates might not be recognized by the foreign country.

BC has the potential to eliminate all the aforementioned pitfalls using a BC-based digital vaccine passport. Each person of the world can be assigned a digital vaccine passport that can act as an authentication mechanism and proof of vaccination. All the digital passports can be stored on Ethereum blockchain and contain the information about the owner, vaccination information such as date, place, time, and batch number. Since the solution is BC-based so it has the advantages of immutably, transparency, persistency and anonymity. From the chain, citizens jabbed with the bad batch can be tracked by the concerned authority in a secure manner. The persistency of BC ensures the records are never lost by the citizen and smart contracts written in the block can ensure that black marketing of the vaccines does not take place. The digital vaccine passport system can be implemented on a global scale that can ensure that these are accepted by all the participating countries. The digital vaccine passport can be of the form of a smartphone application and be linked to each user by their countries passport number. The implementation challenge is not big, but the real challenge lies in worldwide acceptability and standardization.

5 Main findings, challenges and future research directions

5.1 Blockchain for COVID-19

The integration of BC with the healthcare working model has gained high momentum in this era of COVID-19. Several researchers are working to inculcate the advantageous properties of a BC network in the working models of healthcare sectors. We have analyzed and summarized the literature that is necessary for the fight against this crisis. The major parts include contact tracing, data sharing, payments, supply chain management, and data security.

The major three promising characteristics of BC, which are decentralization, transparency, and immutability, have enabled successful amalgamation of BC with the healthcare sector. After going through the existing literature, we conclude that the current centralized systems on which these healthcare models are working have high vulnerabilities to unwanted attacks, resulting in unavoidable consequences such as harming the users' privacy and identity. The main support that BC provides is efficient, fast, and secured form of data sharing among different stakeholders for better decision-making. Also, BC helps in the authorization and verification of the stakeholders of the application that preserve the integrity of the data shared over the network.

Many researchers across the globe are working to find the ways how the BC technology can be used to combat COVID-19, but some proposed BC-based approaches have been simulated like *BeepTrace* [132] and *CovidChain* [25] for contact tracing; *MedRec* [10] and *MedShare* [130] for data sharing; smart contract incentive [133] and *Charity-Chain* [113] for payment; *GCoin* [123] and *LifeCrypter* [109] for supply chain management etc.; and *BlockColdChain* [80] and *Go-Win* [107] for vaccination management.

5.2 Challenges and open issues

The sudden outbreak of COVID-19 has given ways to the research community across the globe to develop infrastructure of a data sharing model in the healthcare sector with better efficiency and security. BC seems to be a viable solution, keeping in mind the continuously growing data, management, privacy, and security. Although the existing works are potential solutions, they pose some challenges and throw open issues that need to be shaped and made full-proof before deploying them into the real world.

Some of the challenges posed by BC in the fight against COVID-19 are as follows:

- First and foremost, the initial hurdle in adapting to BC technology would be the hesitation of doctors and healthcare workers to switch from the traditional paper-records to the advanced BC technology, and the technical difficulties they would face due to lack of skill and knowledge of the new technology would also hinder the onset of BC-based solutions in healthcare [103].
- There is a possibility of legal and regulatory issues when deploying a new BC network in the entire healthcare fraternity. These issues include the type of content being exchanged and stored in the BC network, privacy, integrity threats, copyright issues, etc. [85].
- The different stakeholders have their databases with different attributes and they interact through a BC network. So, managing the data comprising of various databases is also a challenge [85], i.e., interoperability issues. Hence, open standards need to be adopted by these stakeholders for smooth functioning [1].
- Since many functions are to be carried out in a short period and considering the widely spread network; it isn't easy to have every aspect in full control. One of the main challenges could be key management and fear of the keys being abused [43] which in turn affects the security of data.
- Due to mobile recording gadgets and the advent of EHR, the frequency of taking readings is very high and hence there is a change in the patient's data very frequently. But BC has the property of immutability. Therefore, every time a new reading is taken, it must be registered as a new transaction since the previous record cannot be modified. However, it pertains to the same patient. This also gives rise to scalability and storage issues [90].
- With inclusion of IoT in healthcare services, more sensors and actuators are required. And to run these devices, power is needed. Power scarcity cannot be afforded when the life of a person is at stake. Hence additional arrangements for the same have to be made for proper and accurate monitoring of the patient and health data collection [103].
- Lastly, the most harmful issue and challenge of adoption of BC in COVID-19 are mining attacks, which are architecture sensitive and their vulnerabilities differ accordingly.

5.3 Future research directions

Motivated by our detailed survey on research studies on the convergence of BC and COVID-19 pandemic, we point out possible research directions, which should be considered in future works.

5.3.1 From simulation to implementation

Most of the proposed solutions of integrating BC with healthcare to tackle COVID-19 are under the simulation phase. Moreover, these proposals concentrate on any one of the challenges posed in times of COVID-19, but a thorough solution, which covers all aspects in fighting against COVID-19 is missing. After exploring the existing literature, we found that systems are available that combines the characteristics of BC to tackle COVID-19. They proposed various solutions such as proposed by Hiten et al. [25] for contact tracing, *MedShare* by Xia et al. [130] for a reliable framework for sharing of patient data, Hung et al.'s [123] proposed *GCoin* for the supply chain management. Integrating parts and pieces of these proposals may prove to be a potential solution to fight the COVID-19 pandemic through such promising technologies.

There have been cases reported where a person tested positive for the COVID-19 virus even after he/she is vaccinated though the severity is not so high. But now the next step has to be making specific drugs for treating this virus and their trials. The data produced during drug discovery and trials is also very sensitive. No researcher wants his/her work being copied, manipulated and taken credit of. The information about the molecules and their combination he/she has used to develop this drug must be protected and shared only to relevant and legitimate stakeholders [88]. Thus, BC can make this process of data sharing as hassle free. The same can be applied for data collected and shared during the trials of this drug.

5.3.2 Integrating machine learning with Blockchain for COVID-19

The integration of machine learning with BC can prove to be a breakthrough idea in the era of COVID-19. Although BC handles the storage, sharing, verification, integrity, and security, the data processing and decision-making have to be done separately and then stored in the BC network. By integrating machine learning with BC, the decision-making can be done in real time and hence faster appropriate actions can be taken, which are highly required to handle the COVID-19 pandemic [9]. Also, due to mobile medical sensors such as smartwatches and wristbands, the readings from such devices can give a lot of information, making diagnosis easy and efficient. Using machine learning algorithms on this data, the disease can be detected from early symptoms and necessary precautions and treatment procedures can be started [51].

5.3.3 Blockchain for big data in COVID-19

The unexpected exponential expose to the coronavirus has led to an outburst of the amount of data being generated daily. Necessary information extraction, performing various analyses, and then taking appropriate actions by analyzing this huge set of data is a task and highly demanded in such circumstances. It is very necessary to incorporate big data analytics into the BC-based approaches to curb COVID-19. BC can help with the storage and security concerns of big data while ensuring the authenticity of the data [86, 119].

6 Conclusion

BC has come a long way since it has been introduced alongside bitcoin. Researchers across the globe are working to explore the potentials of BC in a variety of domains. Its application in the healthcare sector is very interesting as in this sector, data control and access must be closely monitored. Existing traditional systems are often vulnerable to data breaches, which puts the patients' privacy at risk. BC has several benefits, such as an effective sharing model and immutability, which make its use very compelling. As the world is fighting against the once-in-a-century pandemic, BC could be the key factor that can decrease the impact of the pandemic.

In the proposed survey, we discussed the possible use cases of BC to tackle the COVID-19 situations like contact tracing, which is of utmost importance in an easily transmitted disease like COVID-19 and hence its high accuracy and integrity is demanded, which can be solved by BC; an efficient and privacy-preserving patient data sharing model in BC; payments method; and security of the data flowing in the BC network. All these aspects are not covered in a single proposed framework, which leads the studies in the future towards the amalgamation of these aspects into a single framework and presents a working model for the real world.

Although the research on the possibilities of COVID-19 and BC is just in the initial phases. It can be seen that the BC brings many novel features to the table, which bring significant improvements to the systems currently being used. We believe the proposed survey can elucidate the possible implications of BC technology in the times such as these and will motivate further research in this domain. In the future, we would like to conduct a detailed survey on the BC techniques currently deployed and used around the world to tackle the COVID-19 pandemic.

Declarations

Conflict of interest The authors declare no competing interests.

References

1. Agbo CC, Mahmoud QH, Eklund JM (2019) Blockchain technology in healthcare: a systematic review. In: Healthcare, vol. 7, p. 56. Multidisciplinary Digital Publishing Institute
2. Ahmad RW, Salah K, Jayaraman R, Yaqoob I, Ellahham S, Omar M (2021) The role of blockchain technology in telehealth and telemedicine. Int J Med Inf 148:104399
3. Ahmad T (2020) Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity Available at SSRN 3568830
4. Al-Aswad H, El-Medany WM, Balakrishna C, Ababneh N, Curran K (2021) Bzkp: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain iot smart cities and covid-19 risk mitigation. Arab J Basic Appl Sci 28(1):154–171
5. Al Omar A, Rahman MS, Basu A, Kiyomoto S (2017) Medibchain: A blockchain based privacy preserving platform for healthcare data. In: International conference on security, privacy and anonymity in computation, communication and storage, pp 534–543. Springer
6. Alsamhi SH, Lee B, Guizani M, Kumar N, Qiao Y, Liu X (2021) Blockchain for decentralized multi-drone to combat covid-19 and future pandemics: Framework and proposed solutions. Trans Emerg Telecommun Technol e4255. https://doi.org/10.1002/ett.4255
7. Angelopoulos CM, Katos V (2020) Dhp framework: Digital health passports using blockchain-use case on international tourism during the covid-19 pandemic. arXiv:2005.08922v2 [cs CY]
8. Antal C, Cioara T, Antal M, Anghel I (2021) Blockchain platform for covid-19 vaccine supply management. IEEE Open J Comput Soc 2:164–178
9. Ashraf I, Alnumay WS, Ali R, Hur S, Bashir AK, Zikria YB (2021) Prediction models for covid-19 integrating age groups, gender, and underlying conditions. Comput Mater Continua 67(3):3009–3044
10. Azaria A, Ekblaw A, Vieira T, Lippman A (2016) Medrec: Using blockchain for medical data access and permission management. In: 2016 2nd International conference on open and big data (OBD), pp. 25–30
11. Azim A, Islam MN, Spranger PE (2020) Blockchain and novel coronavirus: Towards preventing covid-19 and future pandemics. Iberoamerican Journal of Medicine (AheadOfPrint) 2:0–0
12. Bell L, Buchanan WJ, Cameron J, Lo O (2018) Applications of blockchain within healthcare. Blockchain in healthcare today
13. Benisi NZ, Aminian M, Javadi B (2020) Blockchain-based decentralized storage networks: A survey. J Netw Comput Appl 162:102656
14. Bhattacharya P, Tanwar S, Bodke U, Tyagi S, Kumar N (2019) Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications. IEEE Transa Netw Sci Eng 8:1–1
15. Biswas S, Li F, Latif Z, Sharif K, Bairagi AK, Mohanty SP (2021) Globechain: An interoperable blockchain for global sharing of healthcare data-a covid-19 perspective. IEEE Consumer Electronics Magazine
16. Borkovich DJ, Skovira RJ (2020) Working from home: Cybersecurity in the age of covid-19. Issues Inf Syst 21(4)
17. Budhiraja I, Tyagi S, Tanwar S, Kumar N, Rodrigues JJPC (2019) Tactile internet for smart communities in 5g: An insight for noma-based solutions. IEEE Trans Industr Inform 15(5):3104–3112
18. Celesti A, Ruggeri A, Fazio M, Galletta A, Villari M, Romano A (2020) Blockchain-based healthcare workflow for tele-medical laboratory in federated hospital iot clouds. Sensors 20(9):2590

19. Chagla Z (2021) The bnt162b2 (biontech/pfizer) vaccine had 95% efficacy against covid-19≥ 7 days after the 2nd dose. Ann Intern Med 174(2):JC15
20. Chamola V, Hassija V, Gupta V, Guizani M (2020) A comprehensive review of the covid-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact. IEEE Access 8:90,225–90,265
21. Chang MC, Park D (2020) How can blockchain help people in the event of pandemics such as the covid-19? J Med Syst 44:1–2
22. Chen HS, Jarrell JT, Carpenter KA, Cohen DS, Huang X (2019) Blockchain in healthcare: A patient-centered model. Biomed J Scient Tech Res 20(3):15,017
23. Chen X, Zhu H, Geng D, Liu W, Yang R, Li S (2020) Merging rfid and blockchain technologies to accelerate big data medical research based on physiological signals. J Healthcare Eng 2020
24. Cho H, Ippolito D, Yu YW (2020) Contact tracing mobile apps for covid-19: Privacy considerations and related trade-offs. arXiv:2003.11511
25. Choudhury H, Goswami B, Gurung SK (2020) Covidchain: An anonymity preserving blockchain based framework for protection against covid-19. arXiv:2005.10607
26. Cirillo N (2021) Reported orofacial adverse effects of covid-19 vaccines: the knowns and the unknowns. J Oral Pathology Med 50(4):424–427
27. CLEVE M (2021) What the lightning-fast quest for covid vaccines means for other diseases. Nature 589
28. Consortium CH (2020) Covid-19 hpc consortium. https://covid19-hpc-consortium.org/. ([Online; accessed on 9-September-2020]
29. iReport Covid App (2020) Covid-19 worldwide survey - ireport-covid app. https://ireport.algorand.org/en/about. [Online; accessed on 15-June-2020]
30. De Filippi P (2016) The interplay between decentralization and privacy: the case of blockchain technologies. J Peer Production Issue (7)
31. Dhillon V, Xu T, Parikh C (2021) Blockchain enabled tracking of physician burnout and stressors during the covid-19 pandemic. Frontiers in Blockchain 3:62
32. Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, Wang J (2018) Untangling blockchain: A data processing view of blockchain systems. IEEE Trans Knowl Data Eng 30(7):1366–1385
33. Donawa A, Orukari I, Baker CE (2020) Scaling blockchains to support electronic health record systems for hospitals. arXiv:2001.05525
34. Dong E, Du H, Gardner L (2020) An interactive web-based dashboard to track covid-19 in real time. Lancet Inf Dis 20(5):533–534
35. Doss S, Nayyar A, Suseendran G, Tanwar S, Khanna A, Hoang Son L, Huy Thong P (2018) Apd-jfad: Accurate prevention and detection of jelly fish attack in manet. IEEE Access 6:56,954–56,965
36. Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F (2017) Secure and trustable electronic medical records sharing using blockchain. In: AMIA annual symposium proceedings, vol 2017, p 650. American Medical Informatics Association
37. Ferguson N, Laydon D, Nedjati Gilani G, Imai N, Ainslie K, Baguelin M, Bhatia S, Boonyasiri A, Cucunuba Perez Z, Cuomo-Dannenburg G, et al. (2020) Report 9: Impact of non-pharmaceutical interventions (npis) to reduce covid19 mortality and healthcare demand
38. Fernandes N (2020) Economic effects of coronavirus outbreak (covid-19) on the world economy Available at SSRN 3557504
39. Ferretti L, Wymant C, Kendall M, Zhao L, Nurtay A, Abeler-Dörner L, Parker M, Bonsall D, Fraser C (2020) Quantifying sars-cov-2 transmission suggests epidemic control with digital contact tracing. Science 368:6491
40. Firouzi F, Farahani B, Daneshmand M, Grise K, Song JS, Saracco R, Wang LL, Lo K, Angelov P, Soares E, et al. (2021) Harnessing the power of smart and connected health to tackle covid-19: Iot, ai, robotics, and blockchain for a better world. IEEE Internet of Things Journal
41. Goel RK, Nelson MA, Goel VY (2021) Covid-19 vaccine rollout—scale and speed carry different implications for corruption. J Policy Model 43(3):503–520
42. Gökalp E, Gökalp MO, Çoban S, Eren PE (2018) Analysing opportunities and challenges of integrated blockchain technologies in healthcare. In: Eurosymposium on systems analysis and design, pp 174–183. Springer
43. Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T (2018) Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J Med Syst 42(7):130
44. Gupta R, Kumari A, Tanwar S A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles. Trans Emerg Telecommun Technol n/a(n/a), e4009. https://doi.org/10.1002/ett.4009. https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4009
45. Gupta R, Shukla A, Mehta P, Bhattacharya P, Tanwar S, Tyagi S, Kumar N (2020) Vahak: A blockchain-based outdoor delivery scheme using uav for healthcare 4.0 services. In: IEEE INFOCOM 2020 - IEEE conference on computer communications workshops (INFOCOM WKSHPS), pp 255–260
46. Gupta R, Shukla A, Tanwar S (2020) Aayush: A smart contract-based telesurgery system for healthcare 4.0. In: 2020 IEEE International conference on communications workshops (ICC Workshops), pp 1–6
47. Gupta R, Tanwar S, Al-Turjman F, Italiya P, Nauman A, Kim SW (2020) Smart contract privacy protection using ai in cyber-physical systems: Tools, techniques and challenges. IEEE Access 8:24,746–24,772
48. Gupta R, Tanwar S, Kumar N, Tyagi S (2020) Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. Comput Electr Eng 86:106,717. https://doi.org/10.1016/j.compeleceng.2020.106717. http://www.sciencedirect.com/science/article/pii/S0045790620305723
49. Gupta R, Tanwar S, Tyagi S, Kumar N (2019) Tactile internet and its applications in 5g era: A comprehensive review. Int J Commun Syst 32(14):e3981. https://doi.org/10.1002/dac.3981. https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.3981. E3981 dac.3981
50. Gupta R, Tanwar S, Tyagi S, Kumar N (2019) Tactile-internet-based telesurgery system for healthcare 4.0: An architecture, research challenges, and future directions. IEEE Netw 33(6):22–29. https://doi.org/10.1109/MNET.001.1900063
51. Gupta R, Tanwar S, Tyagi S, Kumar N (2020) Machine learning models for secure data analytics: A taxonomy and threat model. Comput Commun 153:406–440. https://doi.org/10.1016/j.comcom.2020.02.008. http://www.sciencedirect.com/science/article/pii/S0140366419318493
52. Gupta R, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Sadoun B (2019) Habits: Blockchain-based telesurgery framework for healthcare 4.0. In: 2019 International conference on computer, information and telecommunication systems (CITS), pp. 1–5. https://doi.org/10.1109/CITS.2019.8862127
53. Haq I, Esuka OM (2018) Blockchain technology in pharmaceutical industry to prevent counterfeit drugs. Int J Comput Appl 975:8887

54. Hathaliya J, Sharma P, Tanwar S, Gupta R (2019) Blockchain-based remote patient monitoring in healthcare 4.0. In: 2019 IEEE 9th international conference on advanced computing (IACC), pp 87–91. https://doi.org/10.1109/IACC48062.2019.8971593
55. de Havilland P (2020) Telos blockchain and genobank.io partner to tackle coronavirus testing — crypto briefing. https://cryptobriefing.com/telos-blockchain-genobank-io-partner-tackle-coronavirus-testing/. [Online; accessed on 15-June-2020]
56. He Y, Li H, Cheng X, Liu Y, Yang C, Sun L (2018) A blockchain based truthful incentive mechanism for distributed p2p applications. IEEE Access 6:27,324–27,335
57. Hicks C, Butler D, Maple C, Crowcroft J (2020) Secureabc: Secure antibody certificates for covid-19. arXiv:2005.11833
58. Hines J (2018) Stepping up to summit. Comput Sci Eng 20(2):78–82
59. Hölbl M, Kompara M, Kamišalić A, Nemec Zlatolas L (2018) A systematic review of the use of blockchain in healthcare. Symmetry 10(10):470
60. Hueber O (2020) Blockchain and health
61. Jayalakshmi M, Garg L, Maharajan K, Jayakumar K, Srinivasan K, Bashir AK, Ramesh K (2021) Fuzzy logic-based health monitoring system for covid'19 patients. Comput Mater Continua 67(2):2431–2447
62. Journal H (2019) Healthcare data breach statistics. https://www.hipaajournal.com/healthcare-data-breach-statistics/. [Online; accessed on 10-June-2020)
63. Kassab M, Destefanis G (2021) Blockchain and contact tracing applications for covid-19: The opportunity and the challenges. In: 2021 IEEE International conference on software analysis, evolution and reengineering (SANER), pp 723–730. IEEE
64. Khubrani MM, Alam S (2021) A detailed review of blockchain-based applications for protection against pandemic like COVID-19. Telkomnika 19(4):1185–1196. https://doi.org/10.12928/TELKOMNIKA.v19i4.18465
65. Kitchenham B, Brereton OP, Budgen D, Turner M, Bailey J, Linkman S (2009) Systematic literature reviews in software engineering–a systematic literature review. Inf Softw Technol 51(1):7–15
66. Kitchenham B, Charters S (2007) Guidelines for performing systematic literature reviews in software engineering
67. Kumar T, Ramani V, Ahmad I, Braeken A, Harjula E, Ylianttila M (2018) Blockchain utilization in healthcare: Key requirements and challenges. In: 2018 IEEE 20th International conference on e-health networking, applications and services (Healthcom), pp 1–7. IEEE
68. Kumari A, Gupta R, Tanwar S, Kumar N (2020) Blockchain and ai amalgamation for energy cloud management: Challenges, solutions, and future directions. J Parall Distrib Comput 143:148–166. https://doi.org/10.1016/j.jpdc.2020.05.004. http://www.sciencedirect.com/science/article/pii/S074373152030277X
69. Kumari A, Gupta R, Tanwar S, Tyagi S, Kumar N (2020) When blockchain meets smart grid: Secure energy trading in demand response management. IEEE Netw 1–7
70. Kumari A, Shukla A, Gupta R, Tanwar S, Tyagi S, Kumar N (2020) Et-deal: A p2p smart contract-based secure energy trading scheme for smart grid systems. In: IEEE INFOCOM 2020 - IEEE conference on computer communications workshops (INFOCOM WKSHPS), pp 1051–1056
71. Kuo TT, Kim HE, Ohno-Machado L (2017) Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc 24(6):1211–1220
72. Leith DJ, Farrell S (2020) Coronavirus contact tracing app privacy: What data is shared by the singapore opentrace app. Retreived from https://www.scss.tcd.ie/Doug.Leith/pubs/opentrace_privacy.pdf
73. Li X, Jiang P, Chen T, Luo X, Wen Q (2020) A survey on the security of blockchain systems. Futur Gener Comput Syst 107:841–853
74. Liang X, Zhao J, Shetty S, Liu J, Li D (2017) Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), pp 1–5
75. Lin IC, Liao TC (2017) A survey of blockchain security issues and challenges. IJ Netw Secur 19(5):653–659
76. Liu JK, Au MH, Yuen TH, Zuo C, Wang J, Sakzad A, Luo X, Li L (2020) Privacy-preserving covid-19 contact tracing app: A zero-knowledge proof approach. IACR Cryptol ePrint Arch 2020:528
77. Mashamba-Thompson TP, Crayton ED (2020) Blockchain and artificial intelligence technology for novel coronavirus disease-19 self-testing
78. McGhin T, Choo KKR, Liu CZ, He D (2019) Blockchain in healthcare applications: Research challenges and opportunities. J Netw Comput Appl
79. Mehta P, Gupta R, Tanwar S (2020) Blockchain envisioned uav networks: Challenges, solutions, and comparisons. Comput Commun 151:518–538. https://doi.org/10.1016/j.comcom.2020.01.023
80. Mendonça RD, Gomes OS, Vieira LF, Vieira MA, Vieira AB, Nacif JA (2021) Blockcoldchain: Vaccine cold chain blockchain. arXiv:2104.14357
81. Mohan S, A J, Abugabah A, M A, Kumar Singh S, Kashif Bashir A, Sanzogni L An approach to forecast impact of covid-19 using supervised machine learning model. Software: Practice and Experience n/a(n/a). https://doi.org/10.1002/spe.2969
82. Muthuppalaniappan M, Stevenson K (2021) Healthcare cyberattacks and the covid-19 pandemic: an urgent threat to global health. Int J Qual Health Care 33(1):mzaa117
83. Nandi S, Sarkis J, Hervani AA, Helms MM (2021) Redesigning supply chains using blockchain-enabled circular economy and covid-19 experiences. Sustain Prod Consum 27:10–22
84. Nawari NO, Ravindran S (2019) Blockchain technologies in bim workflow environment. In: Computing in civil engineering 2019: Visualization information modeling, and simulation. American Society of Civil Engineers Reston, VA, pp 343–352
85. Nguyen D, Ding M, Pathirana PN, Seneviratne A (2020) Blockchain and AI-based solutions to combat coronavirus (covid-19)-like epidemics: A survey
86. Nguyen DC, Pathirana PN, Ding M, Seneviratne A (2020) Blockchain for 5g and beyond networks: A state of the art survey. J Netw Comput Appl p 102693
87. Nugent T, Upton D, Cimpoesu M (2016) Improving data transparency in clinical trials using blockchain smart contracts. F1000Research 5
88. Olsson C, Toorani M (2021) A permissioned blockchain-based system for collaborative drug discovery. In: ICISSP, pp 121–132
89. Omar IA, Jayaraman R, Debe MS, Salah K, Yaqoob I, Omar M (2021) Automating procurement contracts in the healthcare supply chain using blockchain smart contracts. IEEE Access 9:37,397–37,409
90. Onik MMH, Aich S, Yang J, Kim CS, Kim HC (2019) Blockchain in healthcare: Challenges and solutions. In: Big data analytics for intelligent healthcare management, pp 197–226. Elsevier
91. Ouyang L, Yuan Y, Cao Y, Wang FY (2021) A novel framework of collaborative early warning for covid-19 based on blockchain and smart contracts. Inform Sci 570:124–143

92. Park S, Choi GJ, Ko H (2020) Information technology–based tracing strategy in response to covid-19 in south korea—privacy controversies. Jama
93. Patel K, Mehta D, Mistry C, Gupta R, Tanwar S, Kumar N, Alazab M (2020) Facial sentiment analysis using ai techniques: State-of-the-art, taxonomies, and challenges. IEEE Access 8:90,495–90,519
94. Patel MM, Tanwar S, Gupta R, Kumar N (2020) A deep learning-based cryptocurrency price prediction scheme for financial institutions. J Inf Secur Appl 55:102,583. https://doi.org/10.1016/j.jisa.2020.102583. http://www.sciencedirect.com/science/article/pii/S2214212620307535
95. PBBC (2020) Phbc - public health blockchain consortium. https://www.phbconsortium.org/. [Online; Accessed on 23-August-2020]
96. Peng Z, Xu C, Wang H, Huang J, Xu J, Chu X (2021) P2b-trace: Privacy-preserving blockchain-based contact tracing to combat pandemics. In: Proceedings of the 2021 international conference on management of data, pp 2389–2393
97. Pham QV, Nguyen DC, Hwang WJ, Pathirana PN et al (2020) Artificial intelligence (ai) and big data for coronavirus (covid-19) pandemic: A survey on the state-of-the-arts
98. Pranggono B, Arabo A (2021) Covid-19 pandemic cybersecurity issues. Int Technol Lett 4(2):e247
99. Prasad V, Bhavsar M, Tanwar S (2019) Influence of monitoring: Fog and edge computing. Scalable Comput 20:365–376. https://doi.org/10.12694/scpe.v20i2.1533
100. Prieto Tejedor J, Corchado Rodríguez JM et al (2020) Blockchain and ai to flatten the curve
101. Ramirez Lopez LJ, Beltrán Álvarez N (2020) Blockchain application in the distribution chain of the covid-19 vaccine: a designing understudy
102. Rangone A, Busolli L (2021) Managing charity 4.0 with blockchain: a case study at the time of covid-19. Int Rev Public Nonprofit Market 1–31
103. Ratta P, Kaur A, Sharma S, Shabaz M, Dhiman G (2021) Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. J Food Qual 2021
104. Resiere D, Resiere D, Kallel H (2020) Implementation of medical and scientific cooperation in the caribbean using blockchain technology in coronavirus (covid-19) pandemics. J Med Syst 44:1–2
105. Ricci L, Maesa DDF, Favenza A, Ferro E (2021) Blockchains for covid-19 contact tracing and vaccine support: A systematic review. IEEE Access 9:37,936–37,950
106. Rotbi MF, Motahhir S, Ghzizal AE (2021) Blockchain technology for a safe and transparent covid-19 vaccination. arXiv:2104.05428
107. Saranya S (2021) Go-win: Covid-19 vaccine supply chain smart management system using blockchain, iot and cloud technologies. Turk J Comput Math Educ (TURCOMAT) 12(12):1460–1464
108. Sayeed S, Marco-Gisbert H (2019) Assessing blockchain consensus and security mechanisms against the 51% attack. Appl Sci 9(9):1788
109. Schöner MM, Kourouklis D, Sandner P, Gonzalez E, Förster J (2017) Blockchain technology in the pharmaceutical industry. Frankfurt School Blockchain Center: Frankfurt, Germany
110. Shae Z, Tsai JJ (2017) On the design of a blockchain platform for clinical trial and precision medicine. In: 2017 IEEE 37th international conference on distributed computing systems (ICDCS), pp 1972–1980. IEEE
111. Sheth K, Patel K, Shah H, Tanwar S, Gupta R, Kumar N (2020) A taxonomy of ai techniques for 6g communication networks. Comput Commun 161:279–303. https://doi.org/10.1016/j.comcom.2020.07.035. http://www.sciencedirect.com/science/article/pii/S0140366420318478
112. Singhal N, Prakash S (2020) A fight against covid-19: Major it trends Available at SSRN 3601504
113. Sirisha NS, Agarwal T, Monde R, Yadav R, Hande R (2019) Proposed solution for trackable donations using blockchain, pp 2019 International conference on nascent technologies in engineering (ICNTE), pp 1–5. IEEE
114. Siyal AA, Junejo AZ, Zawish M, Ahmed K, Khalil A, Soursou G (2019) Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography 3(1):3
115. Sylim P, Liu F, Marcelo A, Fontelo P (2018) Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention. JMIR Res Protocols 7(9):e10,163
116. Tanwar S (2018) Verification and validation techniques for streaming big data analytics in internet ofthings environment. IET Netw. https://digital-library.theiet.org/content/journals/10.1049/iet-net.2018.518
117. Tanwar S, Bhatia Q, Patel P, Kumari A, Singh PK, Hong W (2020) Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward. IEEE Access. (8) 474–488 https://doi.org/10.1109/ACCESS.2019.2961372
118. Tanwar S, Obaidat MS, Tyagi S, Kumar N (2019) Online Signature-Based Biometric Recognition, pp. 255–285. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-98734-7_10
119. Tanwar SS, Tyagi NK (2019) Multimedia Big Data Computing for IoT Applications. Concepts, Paradigms and Solutions. Springer
120. Tanwar S, Vora J, Kanriya S, Tyagi S, Kumar N, Sharma V, You I (2018) Human arthritis analysis in fog computing environment using bayesian network classifier and thread protocol. IEEE Consumer Electr Mag
121. Ting DSW, Carin L, Dzau V, Wong TY (2020) Digital technology and covid-19. Nature Med 26(4):459–461
122. Torky M, Hassanien AE (2020) Covid-19 blockchain framework: innovative approach. arXiv:2004.06081
123. Tseng JH, Liao YC, Chong B, Liao SW (2018) Governance on the drug supply chain via gcoin blockchain. Int J Environ Res Public Health 15(6):1055
124. Tsoi KK, Sung JJ, Lee HW, Yiu KK, Fung H, Wong SY (2021) The way forward after covid-19 vaccination: vaccine passports with blockchain to protect personal privacy. BMJ Innovations 7(2):337–341
125. Vogel P (2019) The benefits and drawbacks of blockchain for philanthropy. https://www.imd.org/research-knowledge/articles/could-blockchain-revolutionize-philanthropy/. [Online; accessed 29-August-2020]
126. Williams CM, Chaturvedi R, Chakravarthy K (2020) Cybersecurity risks in a pandemic. J Med Int Res 22(9):e23,692
127. Wong ZSY (2016) Statistical classification of drug incidents due to look-alike sound-alike mix-ups. Health Inform J 22(2):276–292
128. Wu A, Zhang Y, Zheng X, Guo R, Zhao Q, Zheng D (2019) Efficient and privacy-preserving traceable attribute-based encryption in blockchain. Ann Telecommun 74(7-8):401–411
129. Wu H, Zhu X (2020) Developing a reliable service system of charity donation during the covid-19 outbreak. IEEE Access 8:154,848–154,860

130. Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M (2017) Medshare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 5:14,757–14,767
131. Xia Q, Sifah EB, Smahi A, Amofa S, Zhang X (2017) Bbds: Blockchain-based data sharing for electronic medical records in cloud environments. Information 8(2):44
132. Xu H, Zhang L, Onireti O, Fang Y, Buchanan WB, Imran MA (2020) Beeptrace: Blockchain-enabled privacy-preserving contact tracing for covid-19 pandemic and beyond. arXiv:2005.10103
133. Xuan S, Zheng L, Chung I, Wang W, Man D, Du X, Yang W, Guizani M (2020) An incentive mechanism for data sharing based on blockchain with smart contracts. Comput Electr Eng 83(106):587
134. Yaeger K, Martini M, Rasouli J, Costa A (2019) Emerging blockchain technology solutions for modern healthcare infrastructure. J Sci Innov Med 2(1):1–7
135. Yue X, Wang H, Jin D, Li M, Jiang W (2016) Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J Med Syst 40(10):218
136. Zhang P, Schmidt DC, White J, Lenz G (2018) Blockchain technology use cases in healthcare. In: Advances in computers, vol 111, pp 1–41. Elsevier
137. Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST (2018) Fhirchain: applying blockchain to securely and scalably share clinical data. Comput Struct Biotechnol J 16:267–278
138. Zheng Z, Xie S, Dai H, Chen X, Wang H (2017) An overview of blockchain technology: Architecture, consensus, and future trends. In: 2017 IEEE international congress on big data (BigData congress), pp 557–564. IEEE