

Blockchain for global vaccinations efforts: State of the art, challenges, and future directions

Jalal Al-Muhtadi¹, Abeer Hasan¹, Kashif Saleem², Amjad Gawanmeh³,
Joel Jose Puga Coelho Rodrigues^{4,5}

¹College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia

²Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia

³College of Engineering and Information Technology University of Dubai, Dubai, United Arab Emirates

⁴College of Computer Science and Technology, China University of Petroleum, Qingdao, China

⁵Instituto de Telecomunicações, Covilhã, Portugal

Article Info

Article history:

Received Jan 3, 2023

Revised Apr 5, 2023

Accepted Apr 7, 2023

Keywords:

Blockchain

Coronavirus disease 2019

Decentralization

Ethereum

Immunization

Merkle proof

Vaccination

ABSTRACT

The emergence of the coronavirus disease 2019 (COVID-19) global crisis negatively affected all aspects of human life. One of the most important methods used worldwide to survive this global crisis is the vaccination process to circumvent the proliferation of this pandemic. Many restrictions were alleviated in many countries such as access to public facilities and events. There is a huge amount of data about vaccination campaigns that are collected and maintained worldwide. Although the vaccination data can be analyzed to find out how the alleviation of restrictions can be applied if the data management process requires preserving key aspects like trust, transparency, and availability for easy and reliable access to such data. In this regard, blockchain technology is an excellent choice for meeting the requirements and providing a secure trusted framework for global verification. In this article, the related literature on blockchain technology is surveyed and summarized for all systems that embody solutions. The pros and cons of each solution are presented and provide a comparative summary. Furthermore, a detailed analysis is given to present the current problems and provide a promising mechanism to verify the vaccinated persons anywhere in the world, in a secure manner while retaining individual privacy.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Kashif Saleem

Center of Excellence in Information Assurance, King Saud University

Riyadh-11653, Saudi Arabia

Email: ksaleem@ksu.edu.sa

1. INTRODUCTION

Throughout history, humanity witnessed many waves of pandemics, including swine flu, bird flu, and severe acute respiratory syndrome (SARS). In this era, the earth has been hit by the coronavirus disease 2019 (COVID-19) epidemic that caused 5,054,267 cumulative deaths to date according to the World Health Organization (WHO) [1]. Further harms the health and other resources at a massive scale in the individuals, society, corporate, and government [2]. The COVID-19 pandemic has unfavorably impacted almost all aspects of human life. The movement of social and other activities stopped for a long time due to lockdowns. Now individuals, governments, and enterprises are carefully redefining their activities and procedures to comply with the better guidelines in avoiding the spread of the coronavirus.

Indeed, humanity has faced many challenges in various fields due to this coronavirus. One of the most important is the partial or total ban that was imposed in many countries. The ban has an active impact

and as well negatively affected a large number of people, which heavily disrupted daily life. Due precautions imposed from physical distancing, preventing the exchange of belongings, and many other, results in changing the ways of life in every field. A more specific example is the Grand Mosque in Mecca, Saudi Arabia used to be visited by millions of Muslims from every part of the world around the year. But in the pandemic managing the huge numbers was very difficult and therefore novel policies have been forced to monitor every single person entering the premises of the Grand Mosque to prevent the spread of infection.

Accordingly, to mimic the restrictions of social distancing, many technologies are introduced and become popular that support remote communication such as Zoom and Microsoft Teams but emerges with cybersecurity issues [3]. At the government level, many customized systems and applications are developed to ensure proper and secure communication and transactions. Therefore, based on the above-mentioned challenges and many others, it is necessary to take quick action to deal with the crisis. Therefore, governments, health organizations, and scientists put all their efforts into producing vaccines for COVID-19, [1] mentioned that researchers are currently testing many vaccines in clinical trials in different stages, and 9 vaccines are approved for full use as shown in Figure 1.

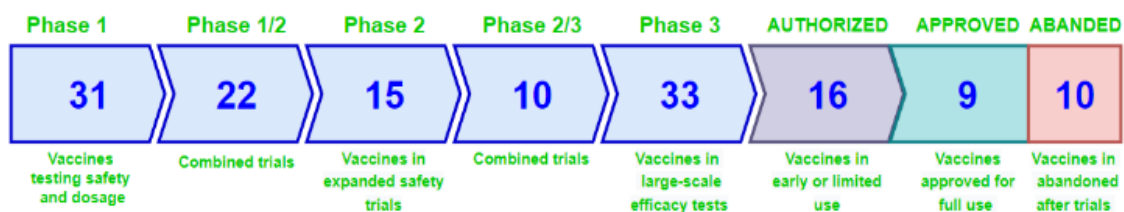


Figure 1. Coronavirus vaccine tracker

Moreover, according to the WHO [1], “as of October 28, 2021, a total of 6,838,727,352 vaccine doses have been administered”. A person should take two doses that may differ in type depending on and varies from country to country. This may lead to some difficulties, for example, a person may take a specific vaccine in one country and be classified as immunized, but then moves to another country may not recognize the vaccine type and categorize the person as not immunized. The process to manage vaccination and immunization data at the global scale is a major challenge. This issue requires a framework that confirms privacy, transparency, and availability, can ensure stakeholders’ security, and provide full proof verification of the vaccine [4]. The blockchain system is considered one of the best solutions to reduce the negative impact of the pandemic, as it has features that cover most of the requirements of this era to provide services in a safe, secure, and available manner all the time, and in particular it can be an appropriate solution to provide the requirements of vaccine management systems needed by governments and official bodies, as shown in Figure 2. The paper [5] provides a detailed assessment and analysis of the suitability of blockchain technology in meeting COVID-19 certification requirements from an ethical, legal, technical, and security standpoint. We conclude from the paper that blockchain prevents discrimination, is an available technology, protects personal data, upholds human rights, and has many other advantages.

Several studies have talked about the role of blockchain in pandemic situations, Kalla *et al.* [6] discussed some expected performance and existing implementations for blockchain-enabled use cases and the role of blockchain, and pertinent challenges for identified use cases. Also, Alam *et al.* [7] mentions 6 of the blockchain applications in the pandemic situation, the most important of which are early detection of a vulnerable population, vaccine, and essential medicine supply chain. The [8] presented an in-depth analysis of the recent blockchain-based solutions for COVID-19 contact tracing for the management of immune/vaccine certifications. Blockchain technology can help by storing in a decentralized, highly secure, and immutable manner. More precisely defined in [6] as “a collection of computing nodes that are connected in a peer-to-peer (P2P) manner and mutually verify transactions executed within the network”.

The term “Blockchain” expresses the basic structure, which is a chain binding a collection of blocks or ledgers so that each user connected to the network is allowed to add a block of the transaction (ledger). Besides, the block has a few specifications, each block is assigned to a cryptographic hash value that changes its value directly when the block is deleted or tampered with, which indicates possible malicious activity. The term blockchain may seem new or ambiguous to some, but it is a kind of cryptography-enabled database. At the end of the 90s, the work began on developing secure and encrypted chains of blocks. In 2008, Satoshi Nakamoto published his research entitled “Bitcoin: A peer-to-peer electronic cash system” [9], which was the beginning of the actual inception of the blockchain, or in the broadest sense, distributed ledger technology (DLT). Studies [10]–[14] explain the use of blockchain in identity management and e-voting systems and

show the importance of regulating and managing immune/vaccine certifications. Alam *et al.* [7] stated that this technology can be efficiently used to counter the shortcomings of traditional E-health record issues and to help in managing the COVID-19 pandemic issue efficiently and effectively by providing reliable, accurate, and, secure data storage and exchanges. Moreover, the work in [6] showed the key features of blockchain can address many critical issues related to health records tracing such as availability, decentralization, and scalability. This can be achieved through implementing contact tracing, vaccination records, and medical history. Figure 2 illustrated the advantages of integration of blockchain technology capabilities with COVID-19 vaccination systems.

This survey paper is the first to review the literature on the blockchain for global vaccination efforts. Moreover, the article explains and discusses the global vaccination verification framework or the mechanism that can securely share people's information on a global scale without privacy leakage. Section 2, first describes blockchain technology and the different types, then extensively review the related works, and provides a summary of the most prominent solutions. In section 3, we discuss the current issues and methods to develop the global blockchain mechanism to verify vaccinated individuals. Finally, section 4 concludes this paper with future works.

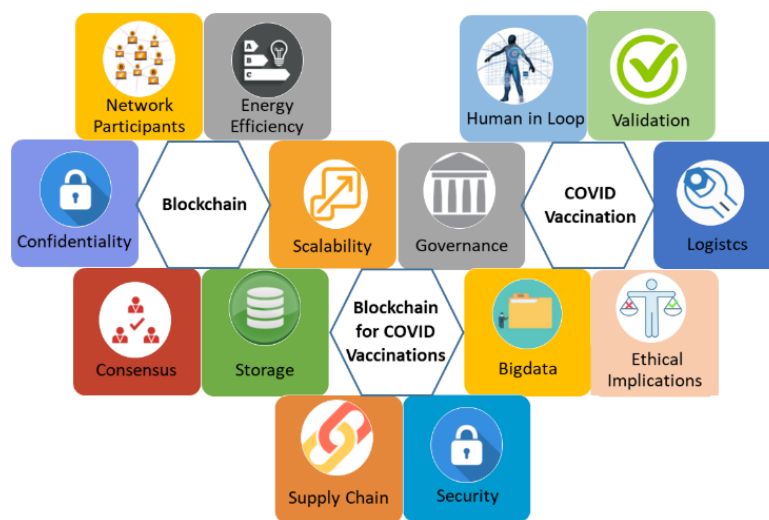


Figure 2. Blockchain for COVID vaccinations

2. LITERATURE REVIEW

In this section, blockchain technology is described including the actual structure and the different types with examples. In addition to the core concept of blockchain, this section as well elaborates on how these variations are applied in the real world. Furthermore, the related work has been reviewed and compared to show the issues, solutions, and areas covered by blockchain.

2.1. Blockchain architecture

The conventional architecture of database and World Wide Web (WWW) makes use of a client-server and distributed database servers' model. On the other hand, recently introduced blockchains use a P2P model, where each encrypted database server in the network is a part of complete the blockchain system [9]. They accept single management for not tampering with the stored ledgers. These ledgers shared the entities between the P2P network even in an untrusted situation [8]. Blockchain comprises two important structures: pointers and linked lists. A graphic representation can be seen in Figure 3 [9].

The blockchain has two main parts: the first part is the header, which contains the hash of the previous block (that is, the header of the n block contains the hash of the $n-1$ block) and it also contains the Merkle root, which can be defined as a hash value that can validate every hash of the transactions that are part of block [15]. The second part section is the body, and it contains the transaction data [16]. The main components of the blockchain [9]: i) node: network computer or user, ii) transaction: the blockchain basic unit, iii) block: a data structure used to keep a set of transactions, iv) chain: an ordered structure of blocks, v) miners: nodes that verify the process before inserting it into the architecture, vi) consensus protocol: set of operation rules, and vii) the working on blockchain.

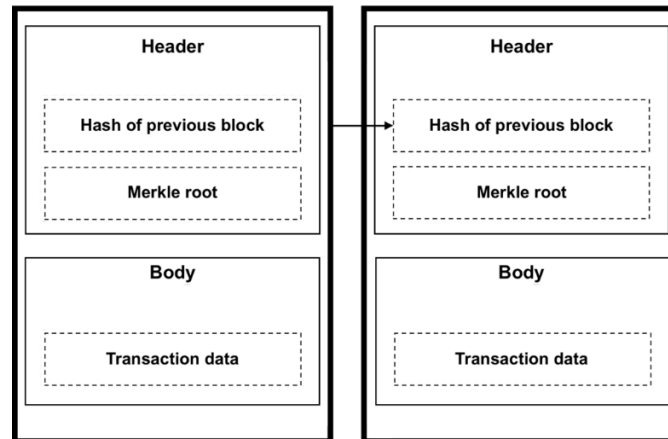


Figure 3. Blockchain architecture

2.2. Cryptography in blockchain

There are two types of cryptographic algorithms in the blockchain: hash functions and asymmetric-key cryptography. For hash functions, SHA 256 is typically used. This algorithm is used to give a single view to each participant in the network. Hash functions have many benefits to the blockchain, the most important of which are: uniqueness, deterministic (since any input will always have the same output if passed through the hash function), and quickness. Most importantly, reverse engineering is not possible. Hash functions play a key role in linking the blocks together and in maintaining the integrity of the data stored within the blocks, because any change to the data, for example, will lead to inconsistency and make the complete chain invalid [17].

Asymmetric-key cryptography is a process that uses a pair of related keys, a public key and a private key, to encrypt and decrypt. The private key is generally generated by a random number algorithm, whereas the public key is calculated by carrying out an irreversible algorithm. The public and private keys can be transmitted over unsecured channels. It is very substantial to guarantee the security of the asymmetric encryption algorithm during the transmission of data [17]. A digital signature is an important part of encryption. A digital signature gives integrity to the process and non-repudiation quality, as a signature does in real life. It also ensures the validity of the blockchain and the data is verified [17].

2.3. Blockchain types

Blockchain technology to provide privacy and security depends on network deployment. This deployment and the system architecture varies based on the actors or participants. According to the involved participants, the blockchain technology system is categorized into three different types for which the details are as follows.

2.3.1. Public blockchain

Public blockchains are completely open since they allow all participants to read and access data to carry out transactions without relying on a third party or a central registry, so all participants contribute to the process of creating a consensus [18]. The most popular examples of public blockchains are Bitcoin (BTC) and Ethereum (ETH). Both of them are cryptocurrencies, that can be viewed and used by everyone, and anonymity is allowed here (for example anyone can buy and sell Bitcoin without revealing their identity). The biggest advantage of a public blockchain is that it is reliable as everything is recorded, and public and cannot be changed. The other major advantage is security as it increases as the public blockchain becomes more decentralized and active. Transparency is also a great advantage, as all transaction-related data is open to the public for verification. On the other hand, the public blockchain has disadvantages, the most important of which is speed. Public blockchains are slow, processing seven transactions every second. The problem of speed becomes clear when compared to Visa, which processes 24,000 transactions per second [19].

2.3.2. Private blockchain

The main difference between public and private blockchains is the access level of each participant. A private blockchain allows specific users to access a closed network, where users have certain rights and restrictions, therefore some users have full access while others have limited access, based on the network's discretion. A private blockchain is not necessarily dependent on cryptography. The most important examples

of the private blockchain are Ripple (XRP), and Hyperledger (HL) [12]. Here anonymity is not allowed because this type is used in business and corporate spheres, so the participant must be revealed.

The most important advantage of a private blockchain is speed, it can process thousands of transactions per second, while the blockchain performs only seven, and the reason for this is that the number of participants is less and thus reaching consensus is faster, and it also gives it more scalability than the other. The problem with private blockchains is that they are centralized even though the blockchain was originally invented to avoid centralization. Security is also a concern, because the number of nodes is less, and it is easier for malicious parties to penetrate security [9], [19].

2.3.3. Semi-private blockchain

The third type is called semi-private, consortium, or federated blockchain, all names refer to the same type that the consensus process is managed by preliminarily assigned nodes (ex. a consortium of 15 financial institutions, each of which controls a node and of which 10 must sign every block to validate the block). The privilege to read the blockchain can be public or restricted to the participants. R3 (banks) and EWF (Energy) are examples of consortium blockchains [9], [20]. Table 1 summarizes the main differences between the three types of blockchain [9].

Table 1. Blockchain types

Property	Public Blockchain	Semi-private Blockchain	Private Blockchain
Consensus determination	All participants	Selected set	Within one organization
Read permission	Public	Public or restricted	Public or restricted
Immutability level	Almost impossible to tamper	Could be tampered	Could be tampered
Speed	Low	High	High
Centralization	No	Partial	Yes
Encryption	General	General and customized	Customized

2.4. Blockchain-based immunization

In this section, we discuss how blockchain can support the validation of immunity passports and vaccination certificates which are formal documents confirming the users' health. An immunity passport is an official document certifying that an individual has been infected and then recovered from COVID-19. Anyway, it is much safer for the immune system to learn how to protect you from diseases through vaccination than by catching the disease and attempting to treat it. These documents have interesting uses such as allowing immune citizens to go on public transport or using them to reduce the risks related to goods delivery services for vulnerable or aged people [8].

At first, Maheswari [9] talks about an overview of blockchain technology, where it reviews its definition, history, architecture, and types. Then, the second artwork deals with the main differences between the two types of blockchain: public and private, and is keen to raise some questions for researchers in the future within this range. Based on these papers, the main characteristics of this great technology, which we see have already been applied in very many fields or at least presented as a proposal to solve serious problems, such as [10], [11], which propose blockchain as a solution to manage the identity system, as this technology covers most of the needs of identity management systems and solves most of its challenges, the most important of which are trust, scalability, and privacy. Also, a detailed technical comparison between existing solutions that rely either on Ethereum or on Quorum or other frameworks.

Blockchain is also receiving great interest in the field of electronic voting, which is considered the most important need for privacy, transparency, and reliability, and we note that all these concepts are provided by the Blockchain. Hjalmarsson *et al.* [12] presented a solution blockchain as a service for e-voting that uses a permissioned (private) blockchain, and three frameworks are considered: Exonum, Quorum, and Geth. The researchers believe that this system would enable secure and cost-efficient elections while guaranteeing voters' privacy. Similarly, the researchers introduce in Xiao *et al.* [14] the status of blockchain-based electronic voting system development that is supposed to address the problems presented by traditional voting systems, and they also present a comparison of different blockchain-based electronic voting systems. Khan *et al.* [13] presents a detailed study of performance and scalability constraints for an e-voting system. Researchers have built a blockchain-based e-voting system to examine permissioned and permissionless blockchain settings with different scenarios for voting population, block size, block generation rate, and transaction speed. So, they conclude interesting findings concerning the effect of these parameters on the efficiency and scalability of the e-voting model. Likewise, the manuscript [21] reviews blockchain technology in terms of its features, applications, and others, as well as proposes it as a developmental solution for the field of e-government, where the extent to which the technology is suitable for this dimension has been clarified.

As for the current time and the field of health, in particular, the new coronavirus has appeared in the past two years and has changed many things in life, and accordingly, new challenges have emerged that technology seeks to improve. On the other hand, the importance of blockchain technology to counter the impact of COVID-19 has emerged, and many studies have indicated this, such as “The role of blockchain to fight against COVID-19” [6], where the challenges the world faced due to the epidemic were presented, with examples from real life attached, then the features of the blockchain that can mitigate the challenges and can support proper implementation of many use cases, such as contact tracing, patient information sharing, disaster relief, and contactless delivery, were presented. Moreover, [7] is an example of one of the applications of the blockchain to counter the impact of the pandemic. Alam *et al.* [7] propose the blockchain technology be used in electronic health records, based on the needs of electronic health records that are summarized in six points: interoperability, privacy, and security, confidentiality, access control, data sharing, data integrity, and availability. Thus, it becomes clear that these needs are compatible with the advantages of the blockchain. Ricci *et al.* [8] give details about a systemic review of blockchains for COVID-19 contact tracing and vaccine support is given, and as well present different techniques such as zero-knowledge, Diffie Hellman, blind signatures, then explains how they are used with blockchain to show robust and privacy-preserving solutions. Also, a description of blockchain applications further on contact tracing and vaccine certification is presented.

Antal *et al.* [22] introduce a blockchain platform to manage the COVID-19 vaccine supply where the system allows beneficiaries to register for the vaccine, and can administer vaccines, and provide delivery services to users and medical centers whose job it is to prepare the vaccines. In addition, doctors can check the vaccines and can also follow up on patients in the event they show symptoms as a result of vaccination. The system uses the Ethereum platform and the authors have demonstrated the results, which show the increase in effectiveness with the transparency in each of the vaccine distributions.

Table 2 (see in Appendix) serves as a summary of the related work section that was used to build this research. The table is divided into two main parts. Where the first column expresses that the paper explains the history of blockchain, then the structure, which shows whether the structure was clarified by researchers. Then which type of blockchain are covered and what are the issues addressed in the related work. The applications column shows the covered platforms, and finally, the last column shows the smart contract property. Further, the relation with COVID-19 is shown, and whether the related work discusses contact tracing, immunity, and vaccination.

3. BLOCKCHAIN-BASED VACCINATION SYSTEM

The designs in [12], [22] together can provide a smooth platform. As the electronic voting system given in [12] uses permission enabled Go-Ethereum with Proof of Authority (PoA) to provide privacy and security, the system consisted of district node and boot node. Where every district node separately interacts with the boot node.

When the election is initiated, a voting smart contract distributes to its corresponding district node and is given permission that allows it to interact with the corresponding contract. When an individual votes, the voting data is validated by the majority of district nodes, and each vote they agree on is added to the blockchain. the second component is the boot node as shown in Figure 4. Every institution in the network hosts a boot node that helps the district nodes to find out each other and contact. To make district nodes find each other faster, boot nodes run on a static internet protocol (IP). Voters can see their votes and make sure that they have been included in the network through the transaction ID that each voter receives from his/her transaction, which gives transparency and traceability as shown in Figure 4.

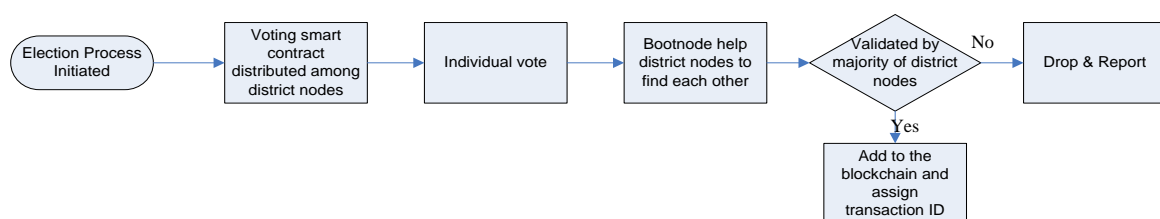


Figure 4. Blockchain based election process

Hjalmarsson *et al.* [12], in Antal *et al.* [22] presented an Ethereum blockchain system through which the vaccination supply can be managed and check their results using Etherscan. Stakeholders are divided into

5 main groups: beneficiaries, companies responsible for transmitting vaccine batches, internet of things (IoT) devices [23], [24] for monitoring, doctors who monitor patients' health and manage vaccination, and finally the medical centers [25] as shown in Figure 5. Underneath, the given system uses Merkle root (P_HASH) that becomes the payload for the Blockchain transaction. Therefore, it serves as an indication of the request of receiving the vaccine. As result, the beneficiary receives a QR code that enables him/her to avail of the services with a detailed report on the side effects. Barakat and Al-Zagheer [26] proposed vaccination systems using blockchain technology to facilitate the process of vaccination distribution by the government.

Nithin *et al.* [27] proposed an Ethereum-based decentralized application for vaccination records that is intended to reduce human effort in the digital records management process. The work does not offer a mechanism to close the loop and provide certification that can be integrated with other systems, i.e., flights, and schools. Several other works [28]–[31] presented a digital vaccine passport system, where vaccination certification is issued using blockchain technology. The methods lack a tracking process for the vaccination as well as integrating it with other applications. Hence there is a lack of presenting a comprehensive system for vaccination recording, tracking, monitoring, and validation. In particular, one that can be integrated with other systems to facilitate the use of the certificates.

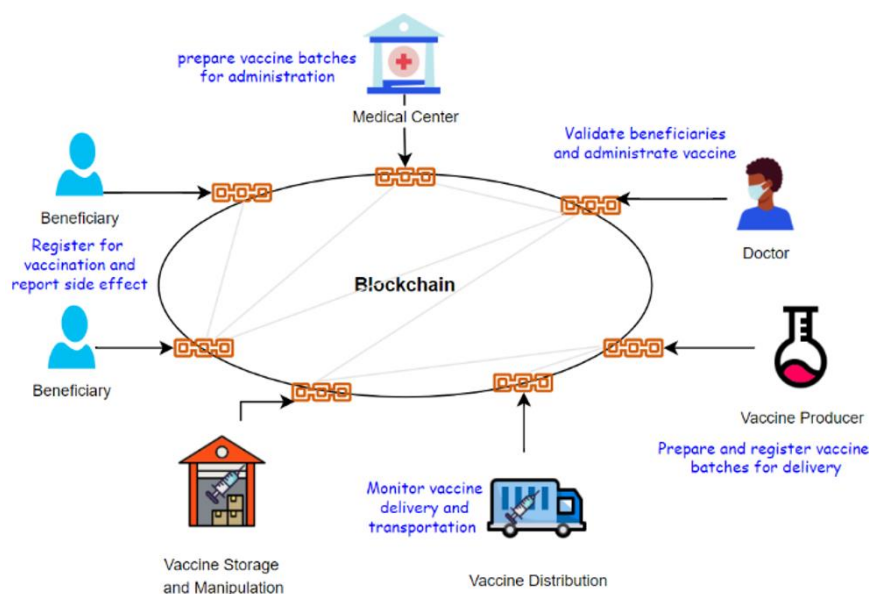


Figure 5. Blockchain-based vaccination system

All transactions are placed in the blockchain as immutable and are stored in blocks to be copied and ready to be communicated to all participants. The system aims to ensure the privacy of identities and prevent impersonation in the main by the following system. In this system the first beneficiary creates a secret key that is used later to prove identity. Further to achieve privacy, the Merkle proof is used and is calculated by (1) [15] which is based on the personal identification (PI) number for the beneficiary and the secret key (SK).

$$P_HASH = Hash(Hash(PI), Hash(SK)) \quad (1)$$

If the vaccination verification platform is based on Ethereum as well as PoA as the consensus mechanism that helps ensure the network's privacy and security. The proposed platform consists of only two main actors: beneficiaries and authorized national vaccination verifiers, which are the government bodies like immigration, border control, airlines, and police. Each participant in the network as shown in Figure 6 have a secret key and some ID number to compute Merkle root, in addition to a transaction ID that allows the follow-up. Initially, the user must create a secret key (SK) used to ensure that identity is not impersonated [22], also the authorized national vaccination verifiers and vaccination centers have identification numbers (VI). The user enters from the vaccination center for example to the system through Merkle root (P_HASH), which is calculated as (2) [15] to ensure privacy and non-impersonation and complete process is shown in Figure 7.

$$P_HASH = Hash(Hash(VI), Hash(SK)) \quad (2)$$

As for adding data, the authorized national vaccination verifiers and vaccination centers should have permission to approve and include it in the blockchain as an immutable record. After the approval of the majority, a transaction identifier (*TI*) is attached to each transaction, so it is given to the beneficiary to allow him/her to view their data. A Merkle root (*P_HASH*) is used again as well as presented in Figure 7, which is calculated as (3) [15]. In this manner, the system provides the advantage of transparency, privacy, and security.

$$P_HASH = Hash(Hash(TI), Hash(PI), Hash(SK)) \tag{3}$$

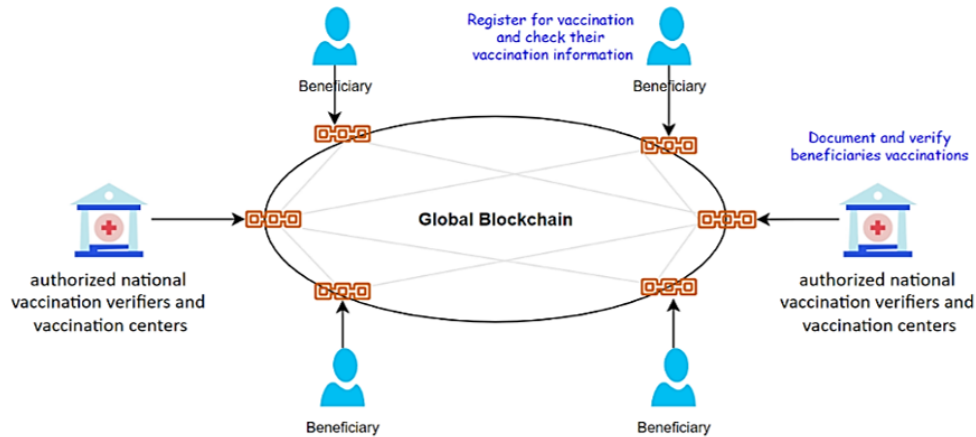


Figure 6. Global blockchain platform to validate COVID-19 vaccinations

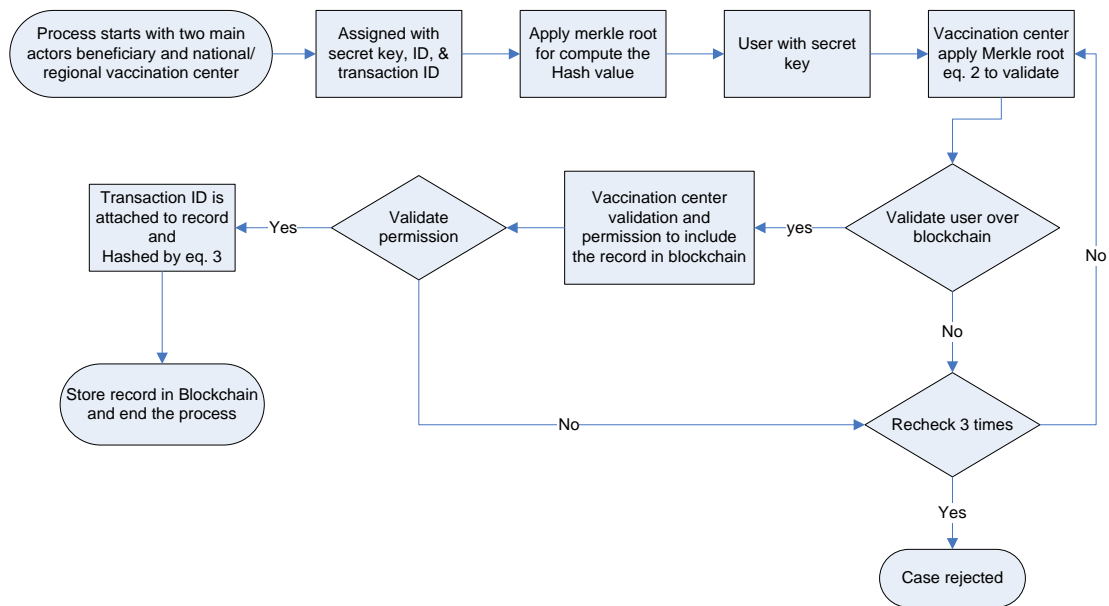


Figure 7. Flowchart of the complete process of proposed global blockchain framework to validate COVID-19 vaccinations

4. CONCLUSION

Provide this paper presents a review of platforms to record and track COVID-19 vaccinations using Blockchain technology. This article explains how Blockchain technology can be used for COVID-19 vaccination recording, tracking, and certification. The paper first presents a comprehensive review of related studies to address this problem. Existing methods are analyzed and several shortcomings were identified. In addition, based on the limitations of the existing solutions, the paper proposed a global platform to validate COVID-19 vaccinations as a solution that is based on Blockchain technology to provide a smart and secure platform for vaccine and immunization verification with complete transparency. The work presents a

high-level plan for developing the proposed platform and identifying the important elements and techniques. In light of the diversity in vaccines, the number of doses, and the huge amounts of vaccine data worldwide, this article contributes to facilitating the management of this information and presenting it more reliably and privately. In the future, the proposed idea will be deployment on real testbed to perform the experimentations and with increase the use of the novel platform to include other uses.

APPENDIX

Table 2. Related work summary

Ref.	History	Structure	Types	Covid 19	Contact tracing	Immunity and vaccination	Issues	Applications	Smart contract
[9]	N	Y	Y	N	N	N	Performance, Privacy, access control, trust	Bitcoin, Ethereum	N
[10]	N	Y	N	N	N	N	Scalability, access, motivation, trust, privacy, flexibility, UX	Bitcoin, Ethereum, Hyperledger,	Y
[11]	N	Y	Y	N	N	N	Privacy, transparency, flexibility	Go-Ethereum, quorum, co-Ethereum	Y
[12]	Y	Y	Y	N	N	N	Scalability, performance	Bitcoin, Ethereum, proposed system	N
[13]	N	Y	N	N	N	N	Scalability, Privacy, Redesign	Bitcoin and Ethereum	N
[21]	N	Y	Y	N	N	N	Scalability, Blockchain Redesign, Leak Blockchain Privacy, performance, Transparency	Business services applications, Bitcoin, Ethereum, Hyperledger platform	N
[5]	Y	Y	Y	Y	Y	Y	Scalability, redesign, leakage	Bitcoin, Ethereum, Hyperledger Fabric, R3, MedicalChain, Apla E-healthcare	N
[6]	Y	Y	N	Y	Y	Y	Privacy, data aggregation, early detection of vulnerable people	E-healthcare	Y
[7]	Y	Y	Y	Y	Y	Y	Transparency, Scalability, Privacy, Trust	E- healthcare Bitcoin, Ethereum	Y
[22]	N	Y	N	Y	Y	Y	Privacy, Transparency, Correctness, Scalability, Trust, Throughput	Ethereum	Y
[32]	N	Y	Y	Y	N	Y	Transparency, security, and accountability	Bitcoin, Ethereum and quorum	N
[33]	Y	Y	N	Y	N	Y	security, trust, economics, and auditability	Ethereum, Bitcoin and proposed system	Y
[34]	N	Y	N	Y	Y	Y	Privacy, Transparency, Scalability	proposed system	Y
[35]	N	Y	N	Y	N	N	Privacy, Transparency, Trust	E- healthcare, proposed system	N
[36]	Y	Y	N	Y	Y	Y	Privacy, Data aggregation, Trust	Ethereum	Y
[37]	Y	Y	N	Y	Y	N	Privacy, Trust, Correctness, Scalability	Ethereum	Y
[38]	N	Y	N	Y	Y	Y	Privacy, Trust, Correctness, Scalability	proposed system	N
[39]	N	Y	N	Y	Y	N	Privacy, Trust, Correctness, Scalability	Ethereum	Y
[31]	N	Y	N	Y	N	Y	Scalability, Data aggregation, Transparency	proposed system	N
[40]	N	Y	N	Y	Y	Y	Scalability, Data aggregation,	proposed system	N
[41]	N	Y	N	Y	Y	Y	Scalability, Data aggregation, performance, flexibility	proposed system	N
[42]	N	N	Y	N	Y	Y	Performance, certification, flexibility	Ethereum	Y
[43]	N	N	Y	N	Y	Y	Performance, flexibility	proposed system	N
[44]	N	N	Y	Y	N	Y	Scalability, performance, flexibility	proposed system	N
[45]	N	N	N	Y	N	Y	Scalability, Data aggregation, flexibility	proposed system	N
[46]	N	N	N	Y	N	Y	Scalability, Data aggregation	proposed system	Y
[47]	N	N	N	Y	N	N	Scalability, Data aggregation	proposed system	N
[48]	N	Y	Y	Y	N	Y	Scalability, Data aggregation	proposed system	Y
[49]	N	N	N	Y	N	Y	Scalability, certification	proposed system	N
[50]	N	N	N	Y	N	Y	Scalability, certification	proposed system	N
[51]	N	N	N	Y	N	N	Scalability, certification	proposed system	N

ACKNOWLEDGEMENTS

This work is funded by FCT/MCTES through national funds and when applicable co-funded EU funds under the project UIDB/50008/2020; and by Brazilian National Council for Scientific and Technological Development-CNPq, via Grant No. 313036/2020-9.




REFERENCES

- [1] J. Holder, "Tracking coronavirus vaccinations around the world," *Covid World Vaccination Tracker-The New York Times*, 2021. https://www.nytimes.com/interactive/2021/world/covid-vaccinations-tracker.html?name=styl-coronavirus®ion=TOP_BANNER&block=storyline_menu_recirc&action=click&pgtype=Interactive&variant=1_Show&is_new=false (accessed Nov. 14, 2021).
- [2] B. M. C. Silva, J. J. P. C. Rodrigues, A. Ramos, K. Saleem, I. de la Torre, and R. L. Rabelo, "A mobile health system to empower healthcare services in remote regions," in *2019 IEEE International Conference on E-health Networking, Application and Services (HealthCom)*, 2019, pp. 1–6, doi: 10.1109/HealthCom46333.2019.9009477.
- [3] J. Al-Muhtadi, B. Shahzad, K. Saleem, W. Jameel, and M. A. Orgun, "Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment," *Health Informatics Journal*, vol. 25, no. 2, pp. 315–329, Jun. 2019, doi: 10.1177/1460458217706184.
- [4] M. A. Sahi *et al.*, "Privacy preservation in e-healthcare environments: state of the art and future directions," *IEEE Access*, vol. 6, pp. 464–478, 2018, doi: 10.1109/ACCESS.2017.2767561.
- [5] M. Foy, D. Martyn, D. Daly, A. Byrne, C. Aguneche, and R. Brennan, "Blockchain-based governance models for COVID-19 digital health certificates: A legal, technical, ethical and security requirements analysis," *Procedia Computer Science*, vol. 198, pp. 662–669, 2022, doi: 10.1016/j.procs.2021.12.303.
- [6] A. Kalla, T. Hewa, R. A. Mishra, M. Ylianttila, and M. Liyanage, "The role of blockchain to fight against COVID-19," *IEEE Engineering Management Review*, vol. 48, no. 3, pp. 85–96, Sep. 2020, doi: 10.1109/EMR.2020.3014052.
- [7] S. Alam, F. A. Reegu, S. M. Daud, and M. Shuaib, "Blockchain-based electronic health record system for efficient Covid-19 pandemic management," *2nd International Conference on Universal Wellbeing*, pp. 114–120, Apr. 2021.
- [8] L. Ricci, D. D. F. Maesa, A. Favenza, and E. Ferro, "Blockchains for COVID-19 contact tracing and vaccine support: a systematic review," *IEEE Access*, vol. 9, pp. 37936–37950, 2021, doi: 10.1109/ACCESS.2021.3063152.
- [9] J. U. Maheswari, "Blockchain technology and its applications-an overview," *International Journal for Research in Applied Science and Engineering Technology*, vol. 8, no. 8, pp. 228–232, 2020, doi: 10.22214/ijraset.2020.30837.
- [10] X. Zhu and Y. Badr, "Identity management systems for the internet of things: a survey towards blockchain solutions," *Sensors*, vol. 18, no. 12, 2018, doi: 10.3390/s18124215.
- [11] K. Gilani, E. Bertin, J. Hatin, and N. Crespi, "A survey on blockchain-based identity management and decentralized privacy for personal data," in *2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS)*, Sep. 2020, pp. 97–101, doi: 10.1109/BRAINS49436.2020.9223312.
- [12] F. P. Hjalmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjalmtýsson, "Blockchain-based e-voting system," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, Jul. 2018, pp. 983–986, doi: 10.1109/CLOUD.2018.00151.
- [13] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Future Generation Computer Systems*, vol. 105, pp. 13–26, Apr. 2020, doi: 10.1016/j.future.2019.11.005.
- [14] S. Xiao, X. A. Wang, W. Wang, and H. Wang, "Survey on blockchain-based electronic voting," in *Advances in Intelligent Networking and Collaborative Systems*, Springer International Publishing, 2020, pp. 559–567, doi: 10.1007/978-3-030-29035-1_54.
- [15] J. Frankenfield, "Merkle root (cryptocurrency) definition," *Investopedia*, 2021. <https://www.investopedia.com/terms/m/merkle-root-cryptocurrency.asp> (accessed Nov. 30, 2021).
- [16] Y.-C. Liang, *Dynamic spectrum management*. Singapore: Springer Singapore, 2020, doi: 10.1007/978-981-15-0776-2.
- [17] M. Sahu, "Cryptography in blockchain: Types and applications," *upGrad*, 2021. <https://www.upgrad.com/blog/cryptography-in-blockchain/> (accessed Dec. 02, 2021).
- [18] M. Grabisch and A. Rusinowska, "Determining influential models," *EconPapers*, 2016.
- [19] Selfkey, "Understanding public vs. private blockchain," *Selfkey*, 2020. <https://selfkey.org/understanding-public-vs-private-blockchain/>
- [20] D. Dobson, "The 4 types of blockchain networks explained," ILTA, 2018. <https://www.iltanet.org/blogs/deborah-dobson/2018/02/13/the-4-types-of-blockchain-networks-explained> (accessed Dec. 01, 2021).
- [21] O. M. AlMendah, M. A. AlZain, M. Masud, N. Z. Jhanjhi, J. Al-Amri, and M. Baz, "A survey of blockchain and e-governance applications: security and privacy issues," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 10, pp. 3117–3125, 2021.
- [22] C. Antal, T. Cioara, M. Antal, and I. Anghel, "Blockchain platform for COVID-19 vaccine supply management," *IEEE Open Journal of the Computer Society*, vol. 2, pp. 164–178, 2021, doi: 10.1109/OJCS.2021.3067450.
- [23] J. J. P. C. Rodrigues, A. Gawanmeh, and K. Saleem, *Smart devices, applications, and protocols for the IoT*. IGI Global, 2019, doi: 10.4018/978-1-5225-7811-6.
- [24] G. Zheng, R. Shankaran, M. A. Orgun, L. Qiao, and K. Saleem, "Ideas and challenges for securing wireless implantable medical devices: A review," *IEEE Sensors Journal*, vol. 17, no. 3, pp. 562–576, Feb. 2017, doi: 10.1109/JSEN.2016.2633973.
- [25] K. Saleem, A. Derhab, J. Al-Muhtadi, and B. Shahzad, "Human-oriented design of secure machine-to-machine communication system for e-Healthcare society," *Computers in Human Behavior*, vol. 51, pp. 977–985, 2015, doi: 10.1016/j.chb.2014.10.010.
- [26] S. Barakat and H. Al-Zagheer, "Blockchain tracking system of COVID-19 vaccination," *Annals of the Romanian Society for Cell Biology*, pp. 5059–5067, 2021.
- [27] G. N. Nithin, B. S. Egala, and A. K. Pradhan, "Global level smart vaccination tracking system using blockchain and IoT," in *2021 IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 450–455, doi: 10.1109/iSES52644.2021.00106.
- [28] J. L. Hernández-Ramos, G. Karopoulos, D. Geneiatakis, T. Martin, G. Kambourakis, and I. N. Fovino, "Sharing pandemic vaccination certificates through blockchain: Case study and performance evaluation," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–12, Aug. 2021, doi: 10.1155/2021/2427896.
- [29] A. K. M. B. Haque, B. Naqvi, A. K. M. N. Islam, and S. Hyrynsalmi, "Towards a GDPR-compliant blockchain-based COVID vaccination passport," *Applied Sciences*, vol. 11, no. 13, Jul. 2021, doi: 10.3390/app11136132.
- [30] A. A. Abuhashim, H. A. Shafei, and C. C. Tan, "Block-VC: A blockchain-based global vaccination certification," in *2021 IEEE International Conference on Blockchain (Blockchain)*, 2021, pp. 347–352, doi: 10.1109/Blockchain53845.2021.00055.
- [31] S. S. Nabil, M. S. Alam Pran, A. A. Al Haque, N. R. Chakraborty, M. J. M. Chowdhury, and M. S. Ferdous, "Blockchain-based COVID vaccination registration and monitoring," *Blockchain: Research and Applications*, vol. 3, no. 4, Dec. 2022, doi: 10.1016/j.bcr.2022.100092.
- [32] A. Musamih, R. Jayaraman, K. Salah, H. R. Hasan, I. Yaqoob, and Y. Al-Hammadi, "Blockchain-based solution for distribution and delivery of COVID-19 vaccines," *IEEE Access*, vol. 9, pp. 71372–71387, 2021, doi: 10.1109/ACCESS.2021.3079197.




- [33] Y. Madhwal, Y. Yanovich, and I. Chumakov, "CoVID-19 vaccination certificate supply verification based on blockchain," in *2021 4th International Conference on Blockchain Technology and Applications*, 2021, pp. 88–93, doi: 10.1145/3510487.3510500.
- [34] A. W. D. Edridge *et al.*, "Coronavirus protective immunity is short-lasting," *medRxiv*, 2020.
- [35] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *Journal of Medical Systems*, vol. 43, no. 1, Jan. 2019, doi: 10.1007/s10916-018-1121-4.
- [36] D. Resiere, D. Resiere, and H. Kallel, "Implementation of medical and scientific cooperation in the Caribbean using blockchain technology in coronavirus (Covid-19) pandemics," *Journal of Medical Systems*, vol. 44, no. 7, Jul. 2020, doi: 10.1007/s10916-020-01589-4.
- [37] A. Khatoun, "A blockchain-based smart contract system for healthcare management," *Electronics*, vol. 9, no. 1, Jan. 2020, doi: 10.3390/electronics9010094.
- [38] A. Bansal, C. Garg, and R. P. Padappayil, "Optimizing the implementation of COVID-19 'Immunity certificates' using blockchain," *Journal of Medical Systems*, vol. 44, no. 9, Sep. 2020, doi: 10.1007/s10916-020-01616-4.
- [39] D. Pavithran, K. Shaalan, J. N. Al-Karaki, and A. Gawamneh, "Towards building a blockchain framework for IoT," *Cluster Computing*, vol. 23, no. 3, pp. 2089–2103, Sep. 2020, doi: 10.1007/s10586-020-03059-5.
- [40] P. Bradish, S. Chaudhari, M. Clear, and H. Tewari, "CoviChain: A blockchain based COVID-19 vaccination passport," in *Lecture Notes in Networks and Systems*, Springer Nature Switzerland, 2023, pp. 195–206, doi: 10.1007/978-3-031-28076-4_17.
- [41] J. Chen, X. Chen, and C.-L. Chen, "A traceable blockchain-based vaccination record storage and sharing system," *Journal of Healthcare Engineering*, vol. 2022, pp. 1–15, Mar. 2022, doi: 10.1155/2022/2211065.
- [42] A. Razzaq, S. A. H. Mohsan, S. A. K. Ghayyur, N. Al-Kahtani, H. K. Alkahtani, and S. M. Mostafa, "Blockchain in healthcare: a decentralized platform for digital health passport of COVID-19 based on vaccination and immunity certificates," *Healthcare*, vol. 10, no. 12, 2022, doi: 10.3390/healthcare10122453.
- [43] Y. Ai, C.-L. Chen, W. Weng, M.-L. Chiang, Y.-Y. Deng, and Z.-Y. Lim, "A traceable vaccine supply management system," *Sensors*, vol. 22, no. 24, 2022, doi: 10.3390/s22249670.
- [44] T. Khanna, P. Nand, and V. Bali, "BEVDS: A blockchain model for multiparty authentication of COVID-19 vaccine beneficiary," in *Innovative Data Communication Technologies and Application*, Springer Nature Singapore, 2022, pp. 857–869, doi: 10.1007/978-981-16-7167-8_63.
- [45] N. Kumar, K. Upreti, S. Upreti, M. S. Alam, and M. Agrawal, "Blockchain integrated flexible vaccine supply chain architecture: Excavate the determinants of adoption," *Human Behavior and Emerging Technologies*, vol. 3, no. 5, pp. 1106–1117, 2021, doi: 10.1002/hbe2.302.
- [46] H. Hu, J. Xu, M. Liu, and M. K. Lim, "Vaccine supply chain management: an intelligent system utilizing blockchain, IoT and machine learning," *Journal of Business Research*, vol. 156, Feb. 2023, doi: 10.1016/j.jbusres.2022.113480.
- [47] T. Wang, C. Li, H. Li, and Z. Li, "Urban monitoring, evaluation and application of COVID-19 listed vaccine effectiveness: a health code blockchain study," *BMJ Open*, vol. 12, no. 7, Jul. 2022, doi: 10.1136/bmjopen-2021-057281.
- [48] Y. Kamenivskyy, A. Palisetti, L. Hamze, and S. Saberi, "A blockchain-based solution for COVID-19 vaccine distribution," *IEEE Engineering Management Review*, vol. 50, no. 1, pp. 43–53, Mar. 2022, doi: 10.1109/EMR.2022.3145656.
- [49] P. R. Agbedanu *et al.*, "BLOCOVID: A blockchain-based COVID-19 digital vaccination certificate verification system," in *2022 International Conference on Engineering and Emerging Technologies (ICEET)*, 2022, pp. 1–6, doi: 10.1109/ICEET56468.2022.10007366.
- [50] L. Cui, Z. Xiao, F. Chen, H. Dai, and J. Li, "Protecting vaccine safety: An improved, blockchain-based, storage-efficient scheme," *IEEE Transactions on Cybernetics*, vol. 53, no. 6, pp. 3588–3598, Jun. 2023, doi: 10.1109/TCYB.2022.3163743.
- [51] N. R. Pradhan, R. Mahule, P. K. Wamuyu, P. K. Rathore, and A. P. Singh, "A blockchain and ai based vaccination tracking framework for coronavirus (COVID-19) epidemics," *IETE Journal of Research*, pp. 1–13, Jun. 2022, doi: 10.1080/03772063.2022.2058630.

BIOGRAPHIES OF AUTHORS






Jalal Al-Muhtadi    is the Director of the Center of Excellence in Information Assurance (CoEIA) at King Saud University, and an Associate Professor at the Department of Computer Science, King Saud University. His areas of expertise include cybersecurity, information assurance, privacy, and Internet of Things. He received his Ph.D. and M.S degrees in Computer Science from the University of Illinois at Urbana-Champaign, USA. He has published over 50 scientific papers in the areas of cybersecurity and internet of things. He can be contacted at email: jalal@ksu.edu.sa.






Abeer Hasan    received the B.S in Information Technology-Security and Networks from King Saud University in 2018. She is currently a M.S degree student in cybersecurity at the King Saud University, Saudi Arabia. She can be contacted at email: 442203014@student.ksu.edu.sa.






Kashif Saleem    received a B.Sc. degree in computer science from Allama Iqbal Open University, Islamabad, Pakistan, in 2002, a PGD degree in computer technology and communication from Government College University, Lahore, Pakistan, in 2004, and the M.E. degree in electrical engineering electronics and telecommunication and the Ph.D. degree in electrical engineering from the University of Technology Malaysia, in 2007 and 2011, respectively. Since 2012, he has been with the Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia, where he is currently an Associate Professor. He is also an Adjunct Professor with the Department of Computer Sciences and Engineering, College of Applied Studies and Community Service, King Saud University. He is professionally certified by the Massachusetts Institute of Technology (MIT) in cybersecurity, the University of the Aegean in information and communication security, Institut Mines-Télécom in queuing theory, IBM in security intelligence analyst, and Microsoft and Cisco in computer networks. He acquired several research grants in Saudi Arabia, EU, and other parts of the world. He has authored or co-authored over 140 papers in refereed journals and international conferences. His research interests include ubiquitous computing, mobile computing, the internet of things (IoT), machine-to-machine (M2M) communication, wireless mesh networks (WMNs), wireless sensor networks (WSNs), and mobile ad hoc networks (MANETs), intelligent autonomous systems, information security, and bioinformatics. He served as a technical program committee member and organized numerous international workshops and conferences. He is providing services as an Associate Editor mainly to Alexandria Engineering Journal, Journal of Multimedia Information System (JMIS), IEEE ACCESS, International Journal of E-Health and Medical Communications (JJEHMC), and International Journal of Cyber-Security and Digital Forensics (IJCSDF). He can be contacted at email: ksaleem@ksu.edu.sa.



Amjad Gawanmeh (SM'17)    is an Associate Professor and Director of Undergraduate Programs at the University of Dubai, UAE and Affiliate Adjunct Professor at Concordia University, Montreal, Canada. He received his Ph.D. degrees from Concordia University in 2008; respectively. He has two edited books, 3 book chapters, more than 40 peer reviewed Scopus indexed journal papers, and more than 65 peer reviewed conference papers. He worked at Khalifa University from 2010 until 2019, before joining the University of Dubai on January 2020. He was visiting scholar at Syracuse University, University of Quebec, and Concordia University. He is the Editor in Chief for the International Journal of Cyber-Physical Systems (IJCPS) IGI, an associate editor for IEEE Access Journal, and for Human-centric Computing and Information Sciences Journal, Springer. He acted as guest editor for several special issues. He is on the reviewer board for several journals in IEEE, Elsevier, Wiley, and many others. He acted as a member of the executive committee for IPCCC conference. He has co-chaired several conference workshops and special sessions organized in key conferences including Globecom, ICC, ICDCS, IPCCC, Healthcom, WoWMoM, ISNCC, and WiMob. He is senior IEEE member. He can be contacted at email: amjad.gawanmeh@ieee.org.



Joel Jose Puga Coelho Rodrigues [Fellow, IEEE and AAIA]    is with the College of Computer Science and Technology, China University of Petroleum, Qingdao, China; Senac Ceará, Brazil; and senior researcher at the Instituto de Telecomunicações, Portugal. Prof. Rodrigues is a Highly Cited Researcher (Clarivate), N. 1 of the top scientists in computer science in Brazil (Research.com), the leader of the Next Generation Networks and Applications (NetGNA) research group (CNPq), Member Representative of the IEEE Communications Society on the IEEE Biometrics Council, and the President of the scientific council at ParkUrbis-Covilhã Science and Technology Park. He was Director for Conference Development-IEEE ComSoc Board of Governors, an IEEE Distinguished Lecturer, Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, a Past-Chair of the IEEE ComSoc Technical Committee (TC) on eHealth and the TC on Communications Software, a Steering Committee member of the IEEE Life Sciences Technical Community and Publications Co-Chair. He is the editor-in-chief of the International Journal of E-Health and Medical Communications and editorial board member of several high-reputed journals (mainly, from IEEE). He has been general chair and TPC Chair of many international conferences, including IEEE ICC, IEEE GLOBECOM, IEEE HEALTHCOM, and IEEE LatinCom. He has authored or coauthored about 1,150 papers in refereed international journals and conferences, 3 books, 2 patents, and 1 ITU-T Recommendation. He had been awarded several Outstanding Leadership and Outstanding Service Awards by IEEE Communications Society and several best papers awards. Prof. Rodrigues is a member of the Internet Society, a senior member ACM, and Fellow of AAIA and IEEE. He can be contacted at email: joeljr@ieee.org.