International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 11, No.1 (Feb-2022)

https://dx.doi.org/10.12785/ijcds/110172

A comprehensive Survey on Blockchain-Based Solutions to Combat Covid-19 Pandemic

Fatima Ezzahra El Aidos[1], Meryem Kassab[1], Nabil Benamar[1,2] and Bouchaib Falah[1]

[1] *School of Sciences and Engineering, Al Akhawayn University in Ifrane, Morocco*
[2] *IMAGE laboratory, School of Technology, Moulay Ismail University of Meknes, Morocco*

Received 15 Sep. 2021, Revised 30 Dec. 2021, Accepted 31 Jan. 2022, Published 15 Feb. 2022

Abstract: COVID-19 pandemic has taken the world by surprise in the beginning of 2020. Initially detected in Wuhan, China, the newly discovered coronavirus has spread all over the world in a short time, which pushed the World Health Organization to declare the disease as a Public Health Emergency. The virus spread transmission primarily occurs between individuals when a contaminated person is in close contact with another person. Thus, contact tracing, the process of identifying and managing potential contacts that have been in a close contact with an infected person is a critical process toward limiting the transmission of the disease. Healthcare professionals with the help of researchers from academia investigated different techniques to deal with contact tracing. In this survey, we focus solely on Blockchain-based techniques that have been proposed so far to deal with contact tracing. We also survey existing Blockchain based applications and the privacy issues they may led to. We compare and evaluate contact-tracing applications based on a number of criteria, notably privacy, security, scalability, proximity estimation, possible attacks, latency, throughput, and resource utilization. We also present techniques that integrated Blockchain with Artificial Intelligence and we conclude this study by shedding light on the remaining limitations, challenges and future directions.

Keywords: COVID-19, Blockchain, contact tracing, pandemic, Artificial Intelligence

1. Introduction

The beginning of the third decade of this century will be definitely traced in history by the global surge of the COVID-19 pandemic caused by a newly discovered Coronavirus (SARS-CoV-2) [1]. The emergence of this virus was initially observed in the city of Wuhan, China when doctors noticed some cases of unexplained pneumonia; it has been later identified as the new form of Coronavirus family [2]. In January 30, 2020, the World Health Organization (WHO) declared the new discovered disease as a Public Health Emergency. Since then, the spread of the virus has been worldwide and led to radical changes in our daily life as well as unprecedented upheavals in every part of the globe. Globally, as of 23 July 2021, there have been 192,284,207 confirmed cases of COVID-19, including 4,136,518 deaths, reported to WHO. As of 26 July 2021, 3,694,984,437 vaccine doses have been administered [1].

At the time of writing this article, many parts of the world are experiencing a huge third wave of the pandemic due to a new variant named Covid-19 Delta. The virus spread has caused a global economic shock with major activities cessation all over the world. Various sectors have been impacted by the pandemic, from tourism to agriculture, transport and teaching. Many countries applied travel restrictions to limit the coronavirus spread, which significantly reduced travels across the world from the beginning of 2020 until this day! This has led to serious financial repercussions on the tourism industry. The Education system has not been immune and may exhibit some of the long-term consequences of the pandemic. Indeed, teaching in schools and universities switched from face-to-face to online or hybrid mode. However, Covid-19 has illuminated one of the main remaining issues in our societies: the digital divide. Many people in the world are still struggling with universal human right of internet access. Consequently, many students all over the world, and especially in rural areas and low-income communities, have not been able to get access to a decent education at the time of the pandemic.

Coronavirus has changed forever the way we learn, we work and we live. Starting 2020, working from home has become the new normal. In an attempt to stop or at least to minimize the spread of the virus, many governments were obliged to force drastic measures, such as lockdowns, mandatory sanitary measures, wearing masks, and social distancing. Although every single service has been facing the consequences of the pandemic, the healthcare infrastructures suffered the most from the coronavirus surge. Most countries have been struggling with providing necessary

E-mail address: : f.elaidos@aui.ma, m.kessab@aui.ma, n.benamar@aui.ma, b.falah@aui.ma

medication and professional staff when the number of infected patients started to increase. Based on the WHO report on the virus spread [3], SARS-Cov-2 transmission primarily occurs between individuals when a contaminated person is in close contact with another person. Contact tracing is defined as the process of identifying and managing potential contacts that have been in a close contact with an infected person to prevent the transmission of the disease. By applying contact tracing procedure, the chain of COVID-19 contamination is broken, which has been proven effective in controlling the virus [4]. Healthcare professionals with the help of researchers from academia investigated different techniques to deal with contact tracing.

Traditional Contact tracing approaches required patients to make a list of people they interacted with, and places they visited. However, one would argue that this approach is easily biased due to the unreliability of human memory. Hence, healthcare facilities and professionals are currently moving from paper records to digitized solutions to overcome the limitations and bottlenecks of the manual approach.

Furthermore, most contact tracing methods proposed so far make use of Bluetooth technology to detect patient interactions and locations. This has raised privacy and security concerns since such applications must preserve patient identities, protect their private data and not violate their overall privacy. Also, patients are generally reserved when it comes to sharing their personal data and locations. Consequently, blockchain-based solutions were proposed as an alternative to overcome such issues. Blockchain technology has been applied in different fields [5] and has proven effective in handling sensitive data transactions securely; this makes it a better choice for contact tracing and thus helping medical facilities to track coronavirus cases globally.

The current survey focuses solely on the use of Blockchain techniques to combat the spread of Covid-19. We compare and evaluate contact tracing applications based on a number of criteria, notably privacy, security, scalability, proximity estimation, possible attacks, latency, throughput, and resource utilization. Artificial intelligence-based techniques have been also widely used to combat the spread of the virus [6], [7], [8], and[9]. However, since our current survey is dedicated to Blockchain based techniques, we also surveyed the proposed solutions, available in the literature, which combined both Blockchain and AI. It is worth mentioning the existence of some dedicated surveys on AI applications to combat COVID-19 pandemic. Interested readers may find further details in [10], [11], and [12].

The remainder of the paper is organized as follows. Section 2 discusses the related surveys on the use of Blockchain in combatting COVID-19 pandemic, as well as the scope of the current survey. In Section 3, we present the main contributions of the current survey. Section 4 presents the methodology used in this work. In section 5, we summarize the background of the COVID-19 disease and the Blockchain theoretical principals. Section 6 surveys the Blockchain-based contact tracing applications. Section 7 is dedicated to AI based techniques, while Section 8 discusses in detail the privacy issues. Section 9 discusses the remaining challenges in the field of Blockchain use in contact tracing, privacy and AI. Finally, we conclude the paper in Section 10. Figure 1 illustrates the overall organization of the paper.

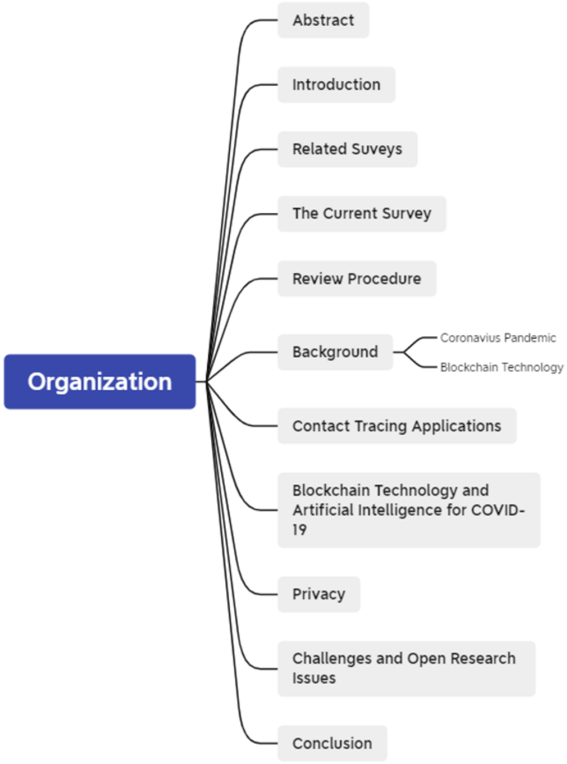

Figure 1. Organization of the survey

2. RELATED SURVEYS

Few surveys have been published recently on a variety of areas related to the use of Blockchain technology to combat COVID-19 pandemic. Chamola et al. [13] presented and discussed a considerable number of blockchain-based applications to combat COVID-19. They proposed programs for testing and reporting, recording patient details, managing the lockdown implementation, preventing the circulation of fake news, incentive-based volunteer participation, secure donation platform, and finally limiting supply chain disruptions. Moreover, the authors also examined a few challenges these applications may face, including a lack of scalability and an absence of a central authority. However, the paper did not cover the security and privacy concerns of such blockchain-based applications.

Authors in [14] and [15] presented in detail the security and data privacy issues, in addition to transaction throughput optimization and network latency. These survey papers also shed light on other applications of blockchain technology in managing the pandemic, such as E-government and handling immigration procedures. However, both papers presented a limited number of BC-applications. Ricci et al. [16] investigated how Blockchain technologies can effectively help reducing the spread of COVID-19 pandemic especially in the ara of contact tracing and vaccine/immunity passport support. This study showcased the necessity to combine Blockchain technologies with advanced cryptographic techniques to guarantee a secure and privacy preserving support to fight COVID-19. Imran et al. [17] presented a detailed survey on how the combination of artificial intelligence, blockchain, and IoT technologies can help combat the COVID-19 pandemic. Shah et al. [18] explored the challenges regarding the usage of Blockchain technologies to maintain the privacy and security of the stakeholders' data. While the previously discussed surveys covered various applications of blockchain technology, Ahmed et al. [19] covered only tracing applications, focusing on their architecture, protocols, and possible attacks. Vulnerabilities of these tracing applications were addressed but the data management aspect was not detailed. The authors proposed research directions that would ease tracing and coping with future challenges. These directions include enhancing the architecture of these applications to be fully decentralized and improving the proximity estimation.

Authors in [20] and [21] investigated the combination of artificial intelligence and blockchain technology for dealing with the COVID-19 pandemic. Nguyen et al. [20] surveyed applications, including prediction models, to estimate the outbreak size, and vaccine and drug development. Fusco et al. [21] performed a Strengths/Weaknesses/Opportunities/Threats (SWOT) Analysis of these applications and investigated the combination of artificial intelligence and blockchain technology for dealing with the COVID-19 pandemic.

Finally, Marbouh et al. [22] covered the implementation details of blockchain applications, comparing various technologies such as Ethereum smart contracts and trusted oracle networks. The authors also presented a full cost analysis that the previous papers failed to examine.

Figure 2 illustrates the most recurring keywords of existing surveys along with their connections. The size of each word represents its occurrence, while the edges constitute links and associations. We observe that "blockchain" and "covid" are large and centered; this is expected since they are the primary focus of each survey. Other keywords related to health are highly reoccurring, such as "healthcare", "outbreak", and "cases". Furthermore, words that describe blockchain applications can also be found, notably "reliable" and "security". Finally, since some review papers cover applications of artificial intelligence to handle the covid-19 pandemic, keywords describing that field are also present. Nevertheless, technical words are not highly used, which indicates that existing reviews are not extensively technical.

3. THE CURRENT SURVEY

This section highlights the main contributions of our survey and what it adds to the current knowledge in the topic of Blockchain use in combatting COVID-19 pandemic. In this paper, we provide a detailed survey on the potential of Blockchain technology use in mitigating COVID-19 pandemic, namely in contact tracing, outbreak prediction, information protection and sharing. We also review the use of blockchain technology and artificial intelligence to handle the covid-19 pandemic. We dive into different kinds of applications, including contact tracing, virus detection, and outbreak predictions. Furthermore, we cover privacy issues related to these applications in detail, along with proposed solutions. Within these objectives, this survey makes the following contributions:

1) We put forward a comprehensive survey on the use of BC and AI to combat the covid-19 pandemic, starting from an overall comparison between existing surveys to a detailed discussion of numerous BC use cases.
2) We examine various state-of-the-art BC-based contact tracing applications related to covid-19, and compare them based on privacy, security, proximity estimation, possible attacks, throughput, and resource utilization.
3) We explore sophisticated applications that combine AI and BC to combat the covid-19 pandemic, providing virus detection, outbreak prediction, information protection and sharing, and social distancing enforcement. A table summarizing and contrasting different applications is also presented.
4) We provide a holistic discussion on the privacy advantages offered by BC technology, detailing the privacy levels of different applications based on their privacy-preserving mechanisms and self-sovereignty support.
5) We identify and highlight challenges and open issues that offer directions for future research.

Table I highlights the main contribution of this paper compared to existing surveys.

4. REVIEW PROCEDURE

As an innovative technology, Blockchain applications are far-reaching. Researchers and industries across the world leveraged the benefits that Blockchain offers to combat the current pandemic [23]. Many publications present blockchain-based solutions to fight the pandemic. However, to the best our knowledge, no survey that addresses all of these blockchain-based solutions to combat covid-19 exists; we, therefore, decided to fill this gap. The aim of this survey is to report developments, and shed light on existing and remaining challenges and open issues. We believe that our work can serve as a reference for those who would

Ref.	Journal	Covid-19 background	Blockchain Background	Contact Tracing	Covid-19 detection	Outbreak Prediction	Information Protection and Sharing	Social distancing enforcement	Privacy Issues	Use of AI	Limitations with respect to our survey
[13]	IEEE Access	✓	-	✓	✓	✓	✓	-	-	✓	The paper did not discuss applications related to social distancing enforcement and did not detail privacy issues. It also did not introduce blockchain technology
[14]	IEEE Engineering Management Review	-	-	✓	-	-	✓	-	✓	-	The paper did not examine some blockchain applications and did not cover AI applications. Furthermore, the privacy discussion was limited.
[15]	IEEE TechRxiv	-	-	✓	-	-	✓	-	-	-	The paper did not discuss some blockchain applications and did not cover AI topics. It also did not dive into privacy issues.
[16]	IEEE Access	✓	-	✓	-	-	-	-	-	-	Covers only contact tracing using Blockchain.
[17]	MDPI Electronis	✓	✓	-	-	-	-	-	-	✓	The paper did not focus on COVID-19. IT surveys emerging IoT technologies, machine learning, and blockchain for healthcare applications.The paper did not cover all Blockchain applications.
[18]	Personal and Ubiquitous Computing Electronis	✓	✓	✓	-	✓	✓	-	-	-	Does not cover the privacy issues in Blockchain. Focus more on the supply chain management, payment system, data dashboard, data sharing, security systems and vaccination.
[19]	IEEE Access	-	-	✓	-	-	-	-	✓	-	The paper did not explore all blockchain applications and did not cover AI topics. The discussion about privacy issues was limited.
[20]	IEEE Access	✓	✓	-	✓	✓	-	-	-	✓	The paper did not examine all blockchain applications. It also did not cover privacy issues.
[21]	International Journal of Environmental Research and Public Health	✓	✓	-	-	✓	-	-	-	✓	The paper did not dive into all blockchain applications and did not discuss privacy issues and solutions.
[22]	Arabian Journal for Science and Engineering	✓	✓	✓	-	-	✓	-	✓	-	The paper did not discuss AI applications, and the privacy discussion was limited.
Proposed Survey	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	-

TABLE I. Blockchain-based applications discussed in existing surveys

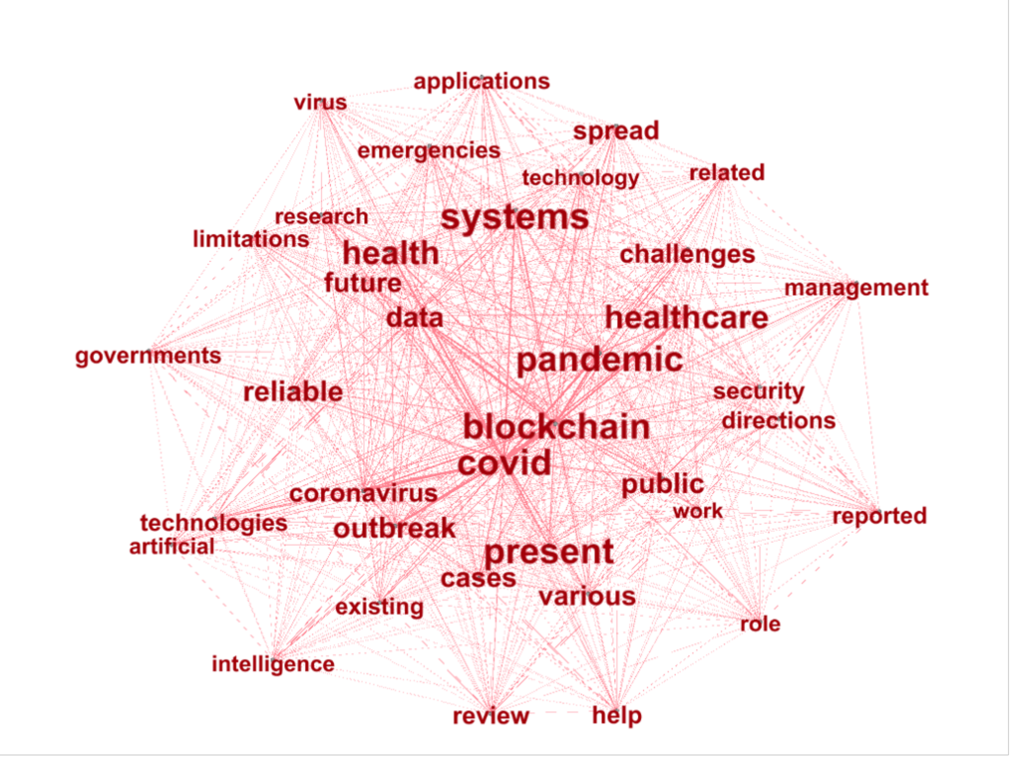

Figure 2. Keyword Mapping of Existing Surveys

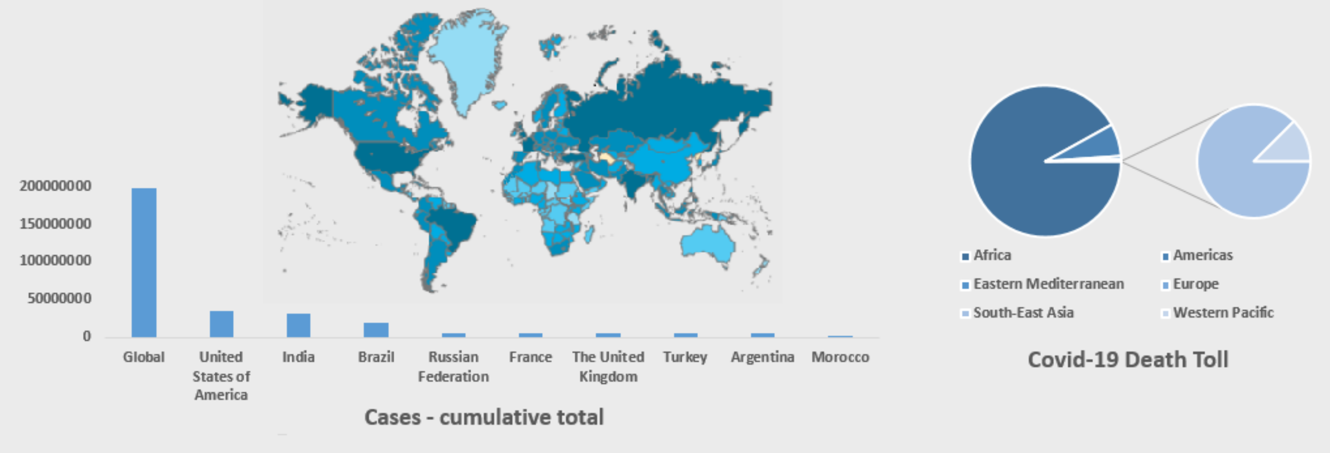

Figure 3. The cumulative total cases and deaths of the coronavirus pandemic

like to explore the use of Blockchain in Coronavirus-like pandemics.

A. Research Questions

The scope of our work has been determined by the following questions:

1) What are the different issues that arise when utilizing non-blockchain technologies to combat the pandemic?
2) How is blockchain used to combat the pandemic?
3) What solutions did the researchers propose to mitigate the issues and challenges encountered?

B. Search Strategy

The first phase of our search strategy consisted of identifying the limitations of current surveys and existing publications that propose non-blockchain solutions to fight the pandemic. This helped us to further shed light on our contribution and objectives, which are mainly associated with the use of blockchain to help in fighting Coronavirus.

The second phase was about finding relevant scientific articles on the subject; we used terminology like blockchain, and covid-19 alongside with their synonyms as shown in Table II. To find these papers and retrieve the full text versions, we mainly relied on the Google Scholar Engine in addition to databases and preprint servers, such as IEEE Xplore, ACM Digital Library, Springer Link, ScienceDirect, arXiv, bioRxiv, and medRxiv.

C. Inclusion criteria

We performed an initial quick screening of the articles we found to remove duplicates, and irrelevant papers. The remaining articles that we were able to access were then examined in order to select those that were suitable. These articles were selected if they satify the following eligibility requirements:

1) The article is available in full text version.
2) The article is written in a language that at least one of the team members can understand (French, English, Arabic).
3) The article is available as a publication or a preprint. Since the pandemic is recent, many of the relevant articles have not yet been peer-reviewed. We, therefore, decided to include Gray literature in our survey to ensure that the topic is well covered.
4) The article covers details on how Blockchain was used to combat the pandemic.
5) The article focuses on how to leverage blockchain to solve major issues such as privacy.

We relied on Excel tables to describe and summarize each of the selected articles. This process took a significant amount of time since the literature has been continuously updated with newly published papers or preprints.

5. Background

This section of the survey presents a brief overview of the coronavirus pandemic and Blockchain, a technology that is currently used to prevent and/or fight the pandemic.

A. Coronavirus Pandemic

Tyrell and Bynoe first discovered Coronaviruses in 1966 during a search for agents that cause common cold. Coronaviruses can infect a wide range of animals as well as humans [24]. The current outbreak of the coronavirus (Covid-19) appeared, in December 2019, in Wuhan's seafood and live animals' market. The virus affects the respiratory tract and can be transmitted from one person to another through respiratory droplets [24]. Potentially infected people develop symptoms, which include but are not limited to shortness of breath, dry cough, chest pain, fever, chills, muscle aches, vomiting, diarrhea, conjunctivitis, and loss of smell and/or taste. These symptoms often appear 2 to 14 days after being exposed to the virus. Reports published by the World Health Organization (WHO), indicate that adults whose age is 60 or above are at high risk of being infected compared to young adults or children who either might show mild symptoms of the virus or even be asymptomatic [25]. To contain the virus, the Chinese government decreed containment measures on the Hubei province. Nevertheless, the pandemic kept spreading across China, and the number of infected people kept increasing at a fast pace. The virus gradually propagated and reached many other countries; this led WHO to declare the outbreak to be a global health emergency by the end of January 2020 [24]. As of January 22nd, 2020, WHO reported 580 cases across the world . Today, as shown in Figure 3, more than 180 million people were or are currently infected worldwide. The pandemic has spread to 221 countries, most of which have failed to contain its growth. Although the outbreak began in China, the United States remains at the top of the list of countries, with most infected people, with over 30 million confirmed cases, followed by India and Brazil exceeding 30 million and 18 million cases respectively [Figure 3]. Morocco recorded its first Covid-19 case in March 2019 [1]. Few days later, the first local contamination was detected; it was caused by a Moroccan citizen returning from Italy. Since then, the number of infections has been exponentially increasing. Morocco was not prepared to absorb the increase in the number of infections. Thus, to prevent the collapse of its health care system and to effectively fight the virus, the Moroccan government followed the Chinese example in containing the virus and decreed the national state of emergency. Shortly after this announcement, the authorities ordained a complete lockdown of the country. To date Morocco has surpassed 530 000 cases (see Figure 3). Although the number of patients is continuously increasing, statistics show that this increase is at a slower pace than when it first began. However, new mutations of the virus, which are reported to be more dangerous and contagious have recently, appeared in several countries threatening the efforts made by governments, universities, and research laboratories in combatting the pandemic [25]. Since the beginning of the outbreak, entities worldwide focused on finding solutions to eradicate the virus and implementing platforms to track and trace cases in almost real time, using a wide range of technologies. Several vaccines were developed by different laboratories in various countries. To address shortage of medical supplies, 3D-printing laboratories developed several prototypes of re-usable facemasks and shields as well as respiratory equipment [26]. Scholars around the world published a significant number of studies on how technologies such as Artificial Intelligence (AI), Internet of Things (IoT), and Blockchain can help in combatting the pandemic [27] , [28] [29]. In the context of AI, researchers recommended the development of deep learning models to help in accelerating the diagnosis of patients [30]. IoT also proved to be useful in this pandemic situation.

The framework proposed in [31], used IoT as well as Machine Learning algorithms to collect and process real-time health data in order to identify positive patients. Therewithal, Blokchain based solutions have also been extensively considered in fighting the pandemic. On account of the privacy and security that the technology provides,

Operator	Dimension	Keyword and synonyms
AND	Blockchain	Blockchain OR BLC OR Digital Ledger OR Distributed Ledger
	Covid-19	COVID OR COVID-19 OR CoV OR Coronavirus OR SARS-COV-2 OR Pandemic OR Epidemic
	Publication type	Survey OR Review OR Conference OR Research OR Case Study OR Report OR Meta-analysis OR State-of-the-art OR Technical Notes

TABLE II. Search keywords

Blockchain has mainly been used to track and trace infected patients, while preserving their anonymity [32]. Section 2 presents in more details Blockchain technology.

B. *Blockchain Technology*

The main goal of this section is to provide a brief overview of Blockchain and how it can be used to solve various problems in healthcare. The core concepts that shaped blockchain technology emerged with the development of the Paxos protocol by Leslie Lamport [33]. Lamport's paper delineates a consensus model for attaining an agreement on a result in a network of hosts where the network itself or the hosts may be unreliable or fallible. All participating nodes validate the information to be appended to the blockchain, and a consensus protocol ensures that the nodes agree on a unique order in which entries are appended.

Consensus protocols for tolerating Byzantine faults have gained renewed attention due to their promising results in blockchain systems. In 1991, Heber et al. [34] presented a proposal that ensures that a timestamped document could not be tampered [34]; this is achieved through a timestamping server that signs a document with the current timestamp and links it to the previous document [34]. Satoshi Nakamoto combined Lamport's, and Haber's ideas and applied them to the electronic cash system [33]. In 2008, Nakamoto published [35], which became a blueprint for most cryptocurrencies. The year of 2009 was marked by the establishment of the bitcoin cryptocurrency as the first of many blockchain applications that are used today [33].

Blockchain is a tamper-proof, distributed, digital ledger. At its basic level, Blockchain allows its users to record transactions in a shared immutable ledger. Based on their permission model, two high-level categories for blockchain networks have been identified: permissioned and permission-less [33]. Users must be granted privileges by an authority, be it centralized or decentralized, to publish blocks in a permissioned blockchain network. In such a network, only authorized individuals are maintaining the blockchain; thus, read access and transaction issuance restrictions can apply [33]. In a permissioned blockchain network, particular users are granted reading or transaction submission privileges. Whereas a permission-less blockchain network does not require permission from any authority. It is open to anyone who would like to publish blocks. Allowing anyone to publish blocks ensues that any individual that uses the permission-less blockchain network can read and/or issue transactions without restrictions. Permission-less networks might engage malevolent individuals or attackers in publishing blocks to subvert the system. To prevent this type of manipulation, such networks rely on consensus models such as Proof of Work, and Proof of Stake [33]. Despite the variations in the permissioned and the permission-less blockchains, both share core concepts. Both are distributed ledgers that contain blocks.

Figure 4 illustrates the basic structure of a Blockchain. Each block consists of a block header that holds metadata on the previous block and a block data that comprises a collection of transactions. Every block header, excluding the genesis block, which is the first block of the blockchain, carries a cryptographic link to the preceding block header. Every transaction entail one or more blockchain network users and a record of transactions that occurred. The individual who submitted the transaction digitally signs this record [33].

One of the fields where Blockchain has a significant potential is healthcare. There exist various blockchain platforms, which makes the selection of the most suitable underlying framework, one of the main tasks in a healthcare project. Blockcahin platforms are generally divided into three groups: Public Blockchain, Private Blockchain and consortium Blockchain. Ethereum and Bitcoin are two well-known public platforms, whereas GemOs and Multichain are typical private BC platforms. Hyperledger Fabric is a busines consortium BC platform. This platform has been proposed for mobile healthcare applications and for medical data storage or access applications.

Ethereum was proposed to be adopted in clinical applications such as clinical data sharing and automated remote patient monitoring. MedRec, and Patientory, both propose using an Ethereum-based BC platform for patient-managed health information exchange applications. Nebula Genomics proposes to analyze and share genomic data on an Ethereum-based blockchain platform. Blockchain is the foundation of cryptocurrency; nonetheless, it has prospects that are more extensive in various fields from banking to healthcare. Advantages of such a technology have been leveraged in the area of Electronic Health Records (EHR)

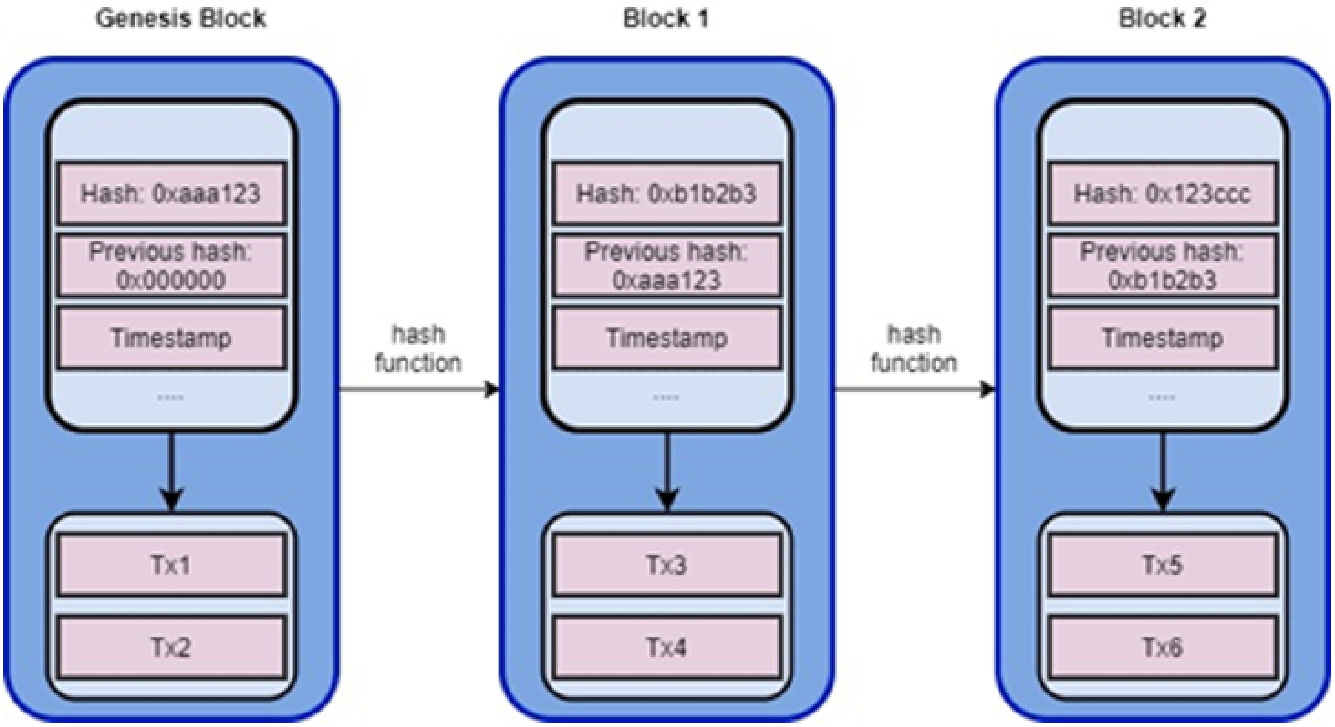

Figure 4. Blockchain structure

[36] .Over the past decades, EHR have been digitized to ease their accessibility. With this digitization, several challenges emerged; they are mainly associated to security, privacy, confidentiality and integrity [37], [38], [39], [40]. In an attempt to solve these issues, Shahnaz et al. [37] proposed a Blockchain-based framework that grants access to its users according to their role. This framework relies on hashes generated by the InterPlanetary File System (IPFS) to ensure the security of the stored data. Another area where Blockchain has proved to be beneficial is Trial and Precision Medicine. A proof of concept based on Blockchain and named “BlockTrial” has been proposed for managing the data of clinical trials [41]. BlockTrial is an Ethereumbased permissioned Blockchain in which patients and researchers are the nodes of the network. In BlockTrial, researchers request for patients’ data are added to an immutable ledger. Patients are provided with the option to determine which portion of their data can be accessed, and by whom.

Healthcare supply chain is another sector that leveraged Blockchain core concepts. Tracking and detecting drugs that fail to pass the quality standards set by the Food and Drug Administration (FDA) are difficult to track [42]. To ease the tracking and detection process of such drugs, Sylim et al. [42] proposed the implementation of a Blockchain-based framework that involves the following participants among others: FDA, the drugs’ manufacturers, and consumers. This framework appoints FDA to the authority role. The drug manufacturer is the participant that instigates the supply chain process; this process is recursively verified for each transaction. To review a drug’s history, a feature for scanning the barcode on purchase receipts is provided to the consumer.

6. CONTACT TRACING APPLICATIONS

The unexpected and acute spread of the COVID-19 virus created the urgent need for tracing applications. These solutions would allow health authorities and governments to track infected people, while notifying any person who came in direct or indirect contact with them. According to [32], contact tracing has been proven useful in preventing infectious diseases throughout history. However, the methods used are constantly changing, allowing for more accuracy and completeness. Traditional approaches required patients to make a list of people with whom they interacted, and places where they have been. Nonetheless, the unreliability of human memory makes this process inaccurate and defective. Healthcare facilities such as hospitals, laboratories and doctor’s offices are currently moving from paper records to EHRs. Therefore, digitized solutions were developed to overcome the limitations and bottlenecks of the manual approach. Furthermore, most methods proposed so far make use of Bluetooth technology to detect patients’ interactions and locations. However, privacy and security concerns are raised since such applications must preserve patients’ identities, protect their private data, and not violate their overall privacy. Consequently, blockchain-based solutions have been proposed to overcome such issues.

Xu et al. [32] proposed BeepTrace, a blockchain-based contact tracing scheme. Compared to existing solutions, namely Singapore TraceTogether [43], Google/Apple Contact Tracing [44], UK NHS Contact Tracing [45], and China health Code System [46], BeepTrace ensures higher security and privacy, consumes less energy, and offers a lower cost for the user. The proposed solution [32] offers strong local security, cybersecurity and privacy without sacrificing the quality of the tracing. However, compromises were made, which led to an increase in the communication and server costs, since blockchain-based decentralized solutions generally require more resources. Furthermore, and even though BeepTrace consumes less power than other existing solutions, the battery drainage problem is still present. Finally, the authors reported concerns regarding elders and minors, since the technology fails to reach such groups.

A. Khurshid [47] also discussed the BeepTrace platform, while focusing on the implementation details and privacy concerns. The author presents blockchain technology as a “Trustless system” that can enable the transparency of contracts. It allows participants to collect information anonymously thanks to the system of public and private keys. BeepTrace provides contact tracing while ensuring anonymized personal identification. Even though the contact infected person gives permission to share his location, the government authorities can never know his identity. This is achieved through the use of two chains and a public key generated by the government.

Song et al. [48] proposed another tracing solution that uses Bluetooth to save the locations visited by the user. Contrary to [32], implementation and architectural details were presented. The system architecture consists of four layers: user interaction, mobile services, smart contract, and data storage. Latency and throughput concerns were also reported, along with proposed solutions. Nevertheless, the authors failed to discuss details such as the participating nodes, the data sources and data use.

Sharma et al. [23] proposed a solution where the participating nodes are patients, testing labs, hospitals and governments. The digital ledger includes documents such as patient records, test records, online treatment status and discharge summaries. Such an application requires collecting the data from the nodes then developing it into big scale. Privacy and security concerns were not covered in details, and potential problems such as throughput and latency were not explored.

While none of the papers, presented so far in this section, discussed the specific programming languages and blockchain technologies use in their proposed solution, authors in [49] did not fail to do so. Khatoon [49] proposed a decentralized application to share authentic patient information and track relevant data, while protecting patients’ identities. It uses a private blockchain network and a distributed file system. Smarts Contracts are developed using Solidity and deployed on Ethereum. Currently, the application uses a proof-of-work algorithm; however, the developers are planning to deploy it on a platform that uses proof-of-stake for scalability. The proposed application allows to share patients’ data and track the spread of the virus without compromising the patients’ identities. Even though implementation details were presented, the authors did not cover the challenges that the platform would face, namely scalability, throughput, and accessibility.

Table III compares the different contact tracing applications discussed based on privacy, security, proximity estimation, possible attacks, throughput, and resource utilization. While “Privacy” refers to the vulnerability of a given Blockchain based application in terms of data leakage and the user’s data confidentiality, “security” refers mainly to the robustness of that solution against intrusion and other possible attacks. We adopt the following terminology in classifying and comparing the studied proposals: While “HIGH” shows that the proposed solution is secure and implements security features, “LOW” means that the security aspect is less present. Consequently, when security features are missing in a given application, the risk of possible attacks is much significant.

The papers, we covered so far, compare, and evaluate contact tracing applications based on a number of criteria including privacy, security, scalability, proximity estimation, possible attacks, latency, throughput, and resource utilization. While privacy and security are the main indicators of an application’s robustness, several authors made sure to include other indicators. We compared and classified all papers covered in this study to conclude that 27% of the proposed solutions take into account the privacy aspect, while 22.7% of them implement some security features. Figure 5 describes the occurrence rate of the different criteria.

7. BLOCKCHAIN TECHNOLOGY AND ARTIFICIAL INTELLIGENCE FOR COVID-19

According to [51], artificial intelligence is a fast-growing field that embeds itself in all aspects of life. Many papers explored and discussed the use of artificial intelligence for dealing with the COVID-19 pandemic. In this section, we dive into some applications that combine both blockchain technology and AI to cope with the pandemic. Kumar et al. [52] reported that the quick spread of the COVID-19 virus created a scarcity of testing kits. Therefore, a need for new detection mechanisms arose. In order to solve this problem, the authors proposed a collaborative network framework to develop a deep learning model for COVID-19 detection using CT images. Since the data involved should be kept private, the network model uses blockchain technology along with federated learning to collect and analyze the data in a private and secure way. This helps medical stakeholders to better train federated surveillance models with privacy protection, while social participants without mutual trusts can still share verified surveillance resources such as data and models, which could

Ref.	Privacy	Security	Proximity Estimation	Possible Attacks	Throughput	Resource Utilization
[32]	Yes	High	High	Low risk	High	Medium
[43]	No	Low	Low	High risk	Low	High
[50]	Yes	Low	Low	High risk	Low	High
[45]	Yes	Low	Low	High risk	Low	High
[46]	No	High	Medium	Low risk	High	Low
[47]	Yes	High	N/A	Low risk	N/A	N/A
[48]	Yes	High	Low	Low risk	Medium	N/A

TABLE III. Comparison between Contact Tracing Applications

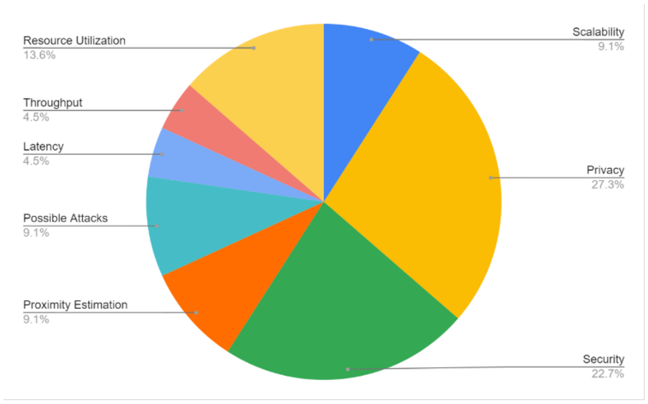

Figure 5. Occurrence rate of criteria used to evaluate contact tracing applications.

lead to the fusion of their solutions. The dataset used to train the model is gathered from different hospitals having different CT scanners. Therefore, the data normalization step is deemed necessary to handle heterogeneous data. After multiple experiments on different datasets, the authors concluded that Capsule Network-based segmentation and classification exceeds the performance of other learning models, achieving an accuracy of 98.68%.

Muhammad and Hossain [53] proposed a platform for COVID-19 detection using blockchain technology and machine learning. In addition, the platform uses the Beyond 5G (B5G) framework to process huge amounts of data in real time and utilize seamless global communication. Therefore, the platform is characterized by the three pillars of 5G, which are low latency, ultra-reliability, and massive data capacity. Blockchain technology is used to process data in a secure and private way, while preserving the confidentiality of COVID-19 patients.

Nguyen et al. [20] proposed a blockchain-AI framework for COVID-19 detection. The framework collects data from laboratories, hospitals and social media, while ensuring privacy and security using blockchain technology. Then, an AI model to detect coronavirus infections analyzes the data that has been collected. This is done through facial recognition [54], temperature detection [54] or CT imaging [55]. Finally, governments, healthcare providers, and patients can benefit from the framework's results.

While previously discussed platforms such as [52] and [53] and gave authorities the upper hand, the authors in [53] proposed a community-based system using BC and AI that allows patients themselves to self-test. Potential patients will collect liquid specimen in a tube or container, then mount it to a device that uses AI technology to analyze it against medical databases and determine whether the person is infected. The results will be communicated back to the patient.

Sujath et al. [56] proposed a linear regression, a multilayer perceptron and a vector autoregression models do predict the growth of the pandemic. The data, used to train and test the models, which represents the COVID-19 cases in India is taken from Kaggle. Since the data only takes into account the number of infected and death cases, the accuracy can be enhanced by considering the hospital where a patient is treated, the different immune systems, gender, and other metrics. This AI model can be integrated to a Blockchain platform to ensure the security of data and privacy of patients.

Aich et al. [57] explored the use of blockchain technology and AI. The authors focused on a framework to protect patients information using blockchain and federated learning. The framework allows concerned parties to use a robust AI model that protects the privacy of their data. The proposed platform is composed of four layers: the application layer, AI engine, data storage, and Blockchain. However, the authors neither implemented nor tested the proposed platform. Therefore, its accuracy and robustness cannot be quantified.

Garg et al. [58] proposed a BC-based platform for authorities to enforce social distancing by limiting the number of people present in a certain place at the same time. The application relies on the people to voluntarily sign up and give access to their location. Thus, the concerned authorities can verify whether a person is allowed to be at certain place.

Firouzi et al. [59] proposed a multi-model diagnosis, consisting of four classifiers: CT scan, ECG Signal, Cough sound, and measurements and checks. These four modalities are used to predict the risks of infection, and death. The authors test multiple machine learning models on a dataset that contains information of around 2000 patients. These models are Multilayer Perceptron (MLP), Support Vector Machines (SVM), Decision Tree using entropy, Random Forest using entropy, Logistic Regression, Adaboost, and Bagging K-Nearest Neighbors. They reported that MLP outperforms the other machine learning models, with an accuracy of 81.99 % [59].

Otoum et al. [60] proposed a framework that uses blockchain and federated learning. The authors also discussed the use of mobile edge computing and 5G and beyond networks. The proposed framework allows concerned participants to exchange data in a secure way, monitor the growth of the pandemic, and enable a fast health-authority response.

Figure 6 illustrates the general structure of a Blockchain/AI application for COVID-19.

Table IV lists the AI method used in the previously discussed papers along with their accuracy.

8. PRIVCACY

Privacy is a major concern to consider while implementing Blockchain based contact-tracing applications. Indeed, such applications collect a significant amount of critical data that contain sensitive information that should remain private. A report that IBM published in 2019 indicates that the average cost of data loss per leakage in healthcare is around 7 million per breach [61]. To preserve data privacy, particularly during the current pandemic, researchers in both the academic and industrial fields suggested different approaches and techniques. Shah et al. [18] highlighted in their survey the case of some mobile applications that faced substantial criticism for their ignorance of the user privacy. In a particular application [61], nearby mobile phones share tokens via Bluetooth as well as to a central server. If a given citizen has been exposed to the virus, the authorities are able to get all these tokens that have been received from nearby smartphones. Such a citizen can be tracked and checked if he was exposed to the virus or not. However, this application can be exploded by intruders using the Bluetooth interface and get access to personal information of the user/victim. Such vulnerability can be mitigated by restricting the information sharing with the government centralized system only.

Centralized architectures are prone to the single point of failure. To overcome this issue, decentralized architectures have been proposed, where data is stored as a hash value instead of the patient's real name [21]. Liang et al. used a private Blockchain to ensure privacy and access control to the patient's data while sharing it with other stakeholders [62]. In Kumar et al. paper [63], authors referred to the consortium blockchain and interplanetary file system (IPFS), which proposed a distributed storage framework for sharing COVID-19 patient's data. This solution can effectively mitigate the unauthorized access to the patient's sensitive data.

To overcome privacy issues that are encountered in contact tracing applications, authors in [32] developed BeepTrace. This blockchain-based solution preserves the user's privacy by using two chains and a public key for tracing, contact matching and notification. BeepTrace relies on the smartphone's Global Positioning System (GPS) to track users. Positioning data that is generated is encrypted and uploaded to the blockchain. Whenever an infection is recorded, users are assigned randomly generated IDs, which are changed on a regular basis to preserve users' identities from potential tracking and/or identification. Infected users are recorded in the blockchain using their assigned IDs. The application, then sends a notification to any other user who was in contact with the infected patient over the last 14 days.

The authors of [32] provide a detailed description of the BeepTrace architecture, functionalities and features of the involved entities. A series of tests proved the effectiveness of BeepTrace. Despite its success, BeepTrace involves many participants and complex computations. This hinders its performance as a contact tracing application that preserves the user anonymity. To improve the performance of BeepTrace, Klaine et al. [66] proposed to use the user's smartphone Bluetooth technology to collect location data. Thus, when two BeepTrace users are close to each other, the application records the location, date and time data in both phones. This data is regularly checked against the information that is available in the blockchain. Similarly to the approach presented in [32], whenever a new infection case is recorded in the blockchain, users who have been exposed are notified without disclosing identities. Although the enhanced version of BeepTrace [59] proved to be much more performant, both version [32] and [66] scored well in terms of privacy since both have demonstrated their abilities in keeping the data secure and keeping the identity of the patient anonymous.

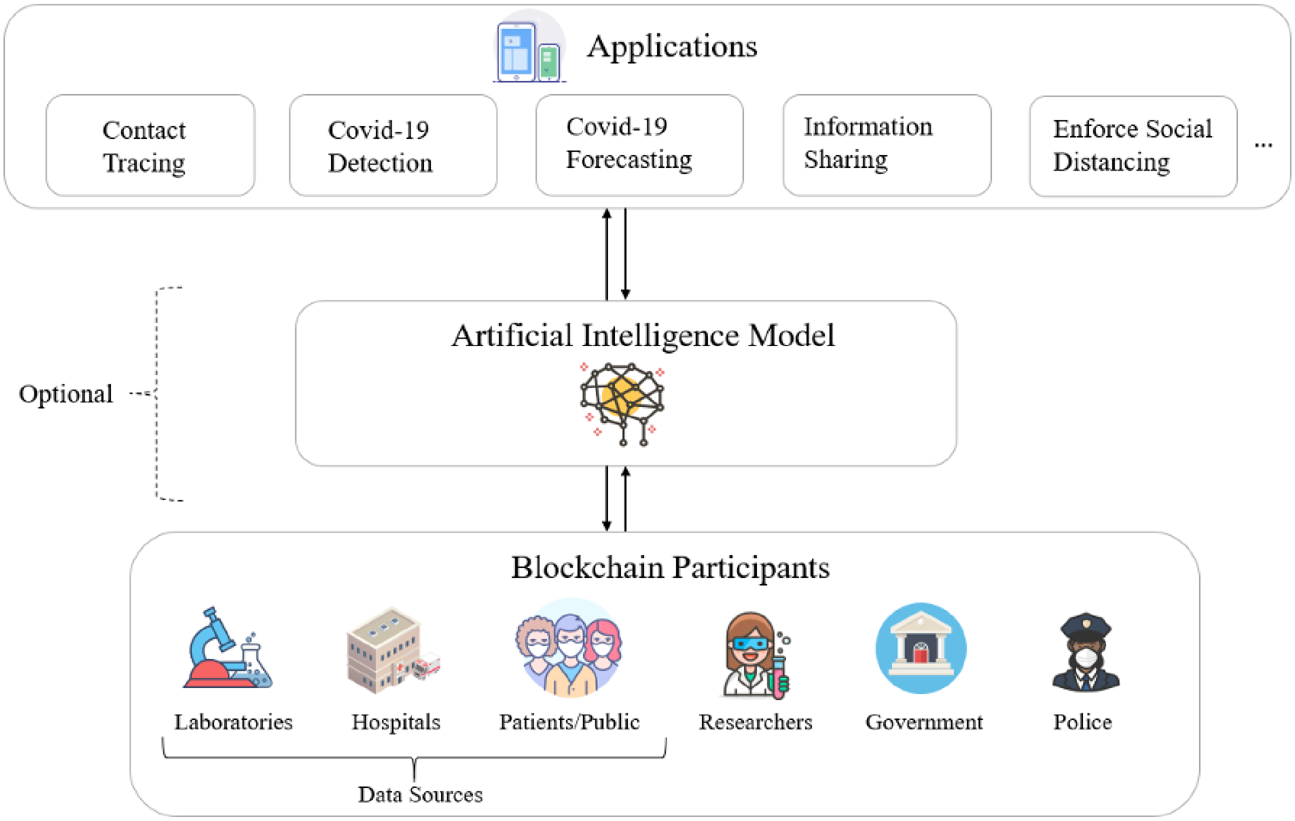

Figure 6. General structure of a Blockchain/AI application

Ref.	AI Method	Accuracy
[52]	Capsule Network	98.68 %
[53]	Convolutional Neural Network (ResNet101)	97.5 %
[56]	Linear Regression/ Multilayer Perceptron/ Vector autoregression	N/A
[57]	Federated Learning	N/A
[59]	Multilayer Perceptron	81.99 %
[60]	Federated Learning	N/A

TABLE IV. AI method used and their accuracy

Authors in [63] implemented Bychain, a decentralized permission-less Blockchain for contact tracing. These authors opted for dissociating identities and transactions by combining the zero-knowledge proof with the key escrow mechanism. Combined, these two techniques proved that it is nearly impossible to identify and associate transactions and their owners. Yet, using the escrow mechanism implies that there is still a way to associate users and transactions through private key checking which a trusted third party could achieve. This checking implies that the private keys could still be stolen or copied as even if the third party is trusted; there is no guarantee for protecting data from leakage or security attacks.

Authors in [64] proposed a Blockchain-based framework, named CovidChain, which keeps the user record anonymous. Stakeholders, including the central authority, cannot link the ledger's transactions to individuals. The central authority is granted access to the epidemiological data through a private key that relates the data in a transaction to a hash value. This hash value cannot be associated to its corresponding public key implying that stakeholders can access and analyze data without compromising patients' privacy.

In an effort to curb the spread of the pandemic while preserving privacy, authors of [66] leveraged the tamper-proof and immutability features that blockchain provides. These

Ref.	Blockchain Platform	Blockchain Type	Privacy-preserving Mechanism	Self-Sovereignty support	Privacy level
[32]	Ethereum	Private	Symmetric / Asymmetric Encryption	No	+ +
[62]	Ethereum	Private	Symmetric / Asymmetric Encryption	No	+ +
[63]	Ethereum	Public	Zero Knowledge + Escrow Mechanism	No	+ + +
[64]	Ethereum	Public	File Hashing	No	+ +
[65]	Mystiko	Private	AES / RSA encryption	Yes	+ + +
[66]	Ethereum	Public	Proof of Locations	Yes	+
[67]	Ethereum	Public	Proxy Re-encryption	Yes	+ +
[48]	Ethereum	Private	Location-based using GPS	No	+
[68]	VeChain Thor	Private	Asymmetric Encryption	No	+ +
[69]	HyperLedger Fabric	Private	Deffie-Hellman key generation + Bloom filters	No	+ + +
[70]	Hyperledger Indy/Aries	Public	Zero knowledge	Yes	+ +
[71]	Ethereum	Public	Asymmetric Encryption + PGP encryption	No	+ +
[72]	Ethereum	Private	ERC 1098 encryption provided via uPort Protocol	Yes	+ +
[73]	Ethereum	Private	AES-256-Encryption	No	+ + +
[74]	Ethereum	Public	DID Method	Yes	+ + +
[75]	Ethereum	Public	Symmetric Encryption	Yes	+ +
[76]	Indy	Public	Zero Knowledge Proof	Yes	+ + +
[77]	Indy	Public	DID Method	Yes	+ + +
[78]	Sovrin	Public	Zero Knowledge Proof	Yes	+ + +

TABLE V. Privacy metrics for covid-19 Blockchain-based applications

authors proposed a contact tracing solution that supports Self-sovereign Identity (SSI). With SSI, users have sole control on how they share or use their personal data [79]. Authors in [66] relied on registered oracles to connect the on-chain and off-chain data without involving centralized servers. To register into this decentralized application, users use their medical digital passports. After registration, the data stored on-chain only includes hashes. Accordingly, the users' identities are preserved and transactions are achieved through a digital electronic address. To further increase the privacy level, the location records are updated with a 20 minutes delay, which ensures that the user's current location is not disclosed.

Similarly to [66], Hasan et al.[72] proposed a solution that uses Ethereum smart contracts and immutable transaction logs to trace and track patients. This solution also relies on self-sovereign identity and digital medical passports. However, in terms of privacy protection, it relies on proxy re-encryption schemes, which are combined with the IPFS to store patients' data. This combination ensures to the concerned parties access to the data in a confidential manner. Abid et al. [65] proposed a blockchain-based platform, named NovidChain, for issuing and verifying test and vaccine certificates. NovidChain focuses on protecting its users' data and grant them sole control and ownership over his records. The data is stored off-chain using IPFS; the IPFS hash is the only component that is stored on-chain to ensure that sensitive records are not disclosed to other participants who are scanning the blockchain.

Similarly to [72], Christodoulou et al. [80] proposed a framework that allows the user to control his medical data and allow access to the user data. A smart contract manages references to IPFS content IDs and orchestrates access to medical data. Although identities are pseudonymous, the smart contract can associate the Ethereum public addresses to users' data such as the social security number. Song et al. [48] proposed a system that offers to its users with Bluetooth based contact tracing, location-based contact tracing and health tracing services. This system relies on Bluetooth technology to protect the user data privacy. The Bluetooth protocol randomly generates the mac addresses that the user uploads; this ensures that the user location remains anonymous.

Unlike the previously mentioned frameworks, and platforms, which are based on Ethereum, H. R. Hasan et al. [68] presented the design and the initial evaluation of a VeChain Thor blockchain based platform. This platform aims to protect sensitive health data and maintain provenance and integrity. It leverages Blockchain and Trusted Execution Environment (TEE) to provide a trusted and secure data exchange ecosystem mHealth data. Thus, the framework guarantees the information provenance and eliminates the need for trusting an authority to keep the users' data safe and private.

Authors of [65] also based their proposal, which is named Connect. It uses the Mystiko blockchain, which supports high availability, and scalability in addition of being a big data friendly blockchain [80]. Similarly to [66], the Connect platform also supports the self-sovereign identity (SSI). In Connect, every user owns a personal mobile wallet to assure a high degree of privacy. The user's activity trace records are stored his physical mobile device whereas the cryptographic identity proofs are stored in the blockchain. This way, Connect ensures that the user data is not leaked should a malicious manipulation occurs.

Ahmed et al. [15] also presented a contact tracing solution that prevents the malicious use of the user data. This privacy protection is achieved through the Diffie-Hellman mechanism and a secret sharing mechanism. To store contact information at the level of the device owner and the backend, the authors used Bloom Filters [69]. As soon as this contact information is encoded in the Bloom filter, it is deleted from the user's device. DIMY's (Did I Meet You) backend is implemented using Hyperledger fabric that provides flexibility when modeling Bloom filters on transactions.

Similarly to [15] Song et al. [48] and Bandara et al. [70] proposed a privacy aware Contact tracing application that runs on top of the Hyperledger fabric blockchain that is used as a repository for test results. Contact tracing is achieved through Bluetooth Low Energy beaconing and the user location is neither recorded nor stored. The application supports self-sovereign identity. Accordingly, users have sole control over their information, except for the diagnosis data, that needs to be shared to ensure that the application performs in a smooth manner.

In addition to contact tracing applications, researchers also leveraged blockchain to propose privacy preserving protocols for information sharing and access control that may be extended to serve the pandemic's cause. To this end, authors in [73] presented an owner-centric blockchain based data sharing model. This model overcomes several implementation challenges that are often linked to data sharing. This approach allows for Digital Twin data sharing among the concerned parties while preserving data confidentiality, integrity as well as availability. Authors in [74] designed the prototype of a protocol that can operate on public blockchain platforms. This prototype supports self-sovereign identity. It stores the user personal information off-chain, while the Digital Identifier information is recorded onto the blockchain.

Naik et al. [71]proposed uPort an open-source collection of tools and protocols for identity management. uPort is user centric, Blockchain-based and supports self-sovereign identity. It provides the users with the ability to manage their identities and any keys or data that are associated with these identities. Identity owners can grant access to data to other users. They can also allow document signing and encrypt data.

Similarly, to achieve self-sovereign identity support, authors in [76] presented Hyperledger Indy, a public distributed ledger that enables its members to manage their identities. With Indy, data is transferred through peer-to-peer encrypted links. Each link has a unique ensuring that data is not leaked from a relationship to another. Claims can be verified without disclosing any personal identity information.

Authors in [77] proposed an open-source Indy based platform for decentralized identification. This platform is public but only trustworthy participants can run nodes. To maintain identity isolation and preserve privacy, users can produce as many IDs as they need. The users have control over the generated IDs, which are governed by a separate asymmetric key pair. The solution proposed by [78] differs from the previous approaches. It is the results of the collaboration of more than 60 organizations. Their goal was to provide individuals with digital certificates, which are commonly known as immunity passports. Immunity passport holders can prove that they are covid-free or request proof from other users. Table V presents the different covid-19 blockchain contact tracing applications and protocols that focused on privacy.

Figure 7 highlights the main platforms used in the proposed applications.

9. CHALLENGES AND OPEN ISSUES

Blockchain technology promotes security and privacy thanks to its decentralized nature. Therefore, BC-based applications are distinguished by their ability to preserve people's identity and evade attacks. Moreover, since medical data such as diagnosis, CT images, and lab results are sensitive and should remain confidential, blockchain technology thrives in the medical field. However, multiple challenges can arise. Contact tracing applications such as [43], [44] and [45] need high computing power; this means that running these applications can cause cell smartphones to die faster. Furthermore, most contact tracing applications use Bluetooth; this makes cell phones vulnerable to security flaws, namely Bluetooth Low Energy Spoofing Attacks (BLESA). Bay et al. [43] instruct users to constantly patch their cell phone's operating systems. Additionally, authors in [81]

ACRONYM	DEFINITION
AI	ARTIFICIAL INTELLIGENCE
BC	BLOCKCHAIN
BLESA	Bluetooth Low Energy Spoofing Attacks
CT	COMPUTED TOMOGRAPHY
DIMY	DID I MEET YOU
EHR	ELECTRONIC HEALTH RECORD
IOT	INTERNET OF THINGS
IPFS	INTER PLANETARY FILE SYSTEM
MLP	MULTILAYER PERCEPTRON
SSI	SELF-SOVEREIGN IDENTITY
SVM	SUPPORT VECTOR MACHINE
SWOT	STRENGTHS/WEAKNESSES/OPPORTUNITIES/THREATS
WHO	WORLD HEALTH ORGANIZATION
TEE	TRUSTED EXECUTION ENVIRONMENT

TABLE VI. Acronyms

highlight scalability problems related to blockchain technology applications, especially the ones using Ethereum. Since BC is gaining huge popularity, the number of daily transactions grows exponentially, which makes BC-based applications less scalable.

AI applications also encounter several challenges. First, security attacks can alter the collected data resulting in inaccurate output. Therefore, the obtained results cannot be trusted with a high confidence. Second, authors in [36] emphasize on the importance of the data normalization stage since the data collected to train and test ML models are not unified. Hospitals do not have similar CT machines or scanners, therefore, having a standard format for such information deems necessary. Finally, combining artificial intelligence and blockchain technology to build applications creates more complexity. Authors in [47] discuss the need for using two layers of learning, which can exhaust computing resources. Furthermore, collaborations between different health institutions are crucial to obtain a decentralized network for model training and data processing.

With its distributed ledger technology and self-sovereign identity, Blockchain can easily overcome major concerns and issues such as privacy, data inconsistency, and duplication that arise in non-blockchain solutions. Preserving the user privacy is crucial particularly when using pandemic tracking applications [82]. Stakeholders might use mobile location data and other records to ease their process in containing the outbreak spread. However, to ensure that privacy is preserved, the user providing such information should have sole ownership of his data and should be the only one able to grant access to his sensitive information. Nevertheless, conflict between records collection and privacy is unavoidable and needs to be further reinforced by laws [83].

Privacy remains one of the main challenges when it comes to the use of Blockchain in healthcare. Each BC block is associated with privacy and can access to other block's data. Thus, it is of most importance to ensure that unauthorized users cannot look at a given block to deny them for seeing the whole transaction. Ring signatures blockchain remains one of the solutions based on an encrypted technology that is able to handle and mitigate privacy issues [84].

The Bluetooth protocol, primarily used in contact tracing techniques, is considered as a critical resource, which can be used against user security. Indeed, Bluetooth technology may bring exposure of the hardware identification, which raises privacy concerns considering Radio Frequency vulnerabilities. In some proposed solutions, the privacy of the user is not respected due mainly to the use of a centralized architecture where the identity of the user is generally not hidden to the authorities. Further research seems mandatory to guarantee the privacy of the user and to ensure that only relevant data is shared. Combining blockchain techniques with advanced encryption algorithms and anonymization techniques seems particularly promising in this regard. Hyperledger Fabric and Quorum are operated in controlled environment, which makes privacy easier to ensure [84], [85]. However, using a platform such as Bitcoin or Ethereum, requires much more efforts in assuring privacy since data and transactions are public. To mitigate privacy leakage risks, and to preserve the user data, developers used and/or combined several techniques such as the Zero-Knowledge proof, the Attribute Based Encryption and the Multi-party homomorphic obfuscations [14], [86], [87]. These techniques solve one part of the problem but leave the door open for carbon emission concerns, an issue that is often disregarded.

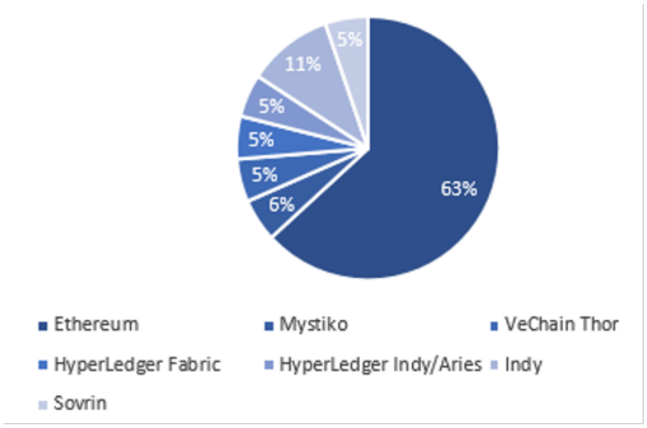

Figure 7. Blockchain Platforms used in the proposed applications/protocols to combat COVID-19 pandemic.

The pandemic requires systems handle emergencies in an efficient and timely manner. It demands consistent and close coordination and cooperation among the stakeholders that work towards curbing Coronavirus. This coordination and cooperation imply maintaining a consistent and synchronized collection of data to streamline operations of the involved parties. However, data that is generated by these parties is huge. This increases the velocity and results in difficulties to process data in fast way. In Blockchain, latency is computed based on the time needed to mine a block. Latency varies depending on the deployed blockchain platform and its specifications. The higher the latency the lower the transaction throughput. Ethereum, for instance, provides restricted transaction privacy and throughput. Ethereum can handle up to twenty transactions per second [88], [89]. Whereas, private blockchain platforms can handle hundreds of transactions per second [90], [91].

10. CONCLUSION

The COVID-19 surge is still devastating and the whole world is currently facing a new spike of the pandemic. Different causes can explain the spike in coronavirus cases, but the human behavior remains the major factor. Some respect the mandatory safety measures such as social distancing, mask wearing, and hand washing, but many are not as meticulous. Efforts in combating the pandemic have been deployed all over the world and contact tracing remains one of the most effective ways to limit the spread of the virus. Existing traditional systems have exhibited some serious vulnerabilities regarding data breaches and patients' privacy issues. In this paper, we have presented a state-of-art survey on the utilization of blockchain technology to combat the coronavirus (COVID-19) pandemic. We have first compared existing surveys in the topic to shed light on how the current survey is filling the gap. We conducted a systematic review by looking for all relevant published papers in the field and we focused solely on the use of Blockchain techniques to combat the spread of Covid-19. We compared and evaluated contact tracing applications based on a number of criteria, notably privacy, security, scalability, proximity estimation, possible attacks, latency, throughput, and resource utilization. Since Artificial intelligence-based techniques have been also widely used to combat the spread of the virus [86], [87], [88], [89], we also surveyed the proposed solutions, available in the literature that combined both Blockchain and AI. However, privacy remains a major concern in Blockchain based contact-tracing applications. Such applications collect a significant amount of critical data that contain sensitive information that should remain private. Guided by these concerns, this survey shaded light on major privacy concerns, and presented the blockchain based platforms and frameworks that have been proposed so far to enable a decentralized identification, identity isolation and thus preserving privacy. Finally, we discussed some of the remaining challenges and future directions that we hope will serve as a basis for researchers interested in developing Blockchain applications to combat the COVID-19 pandemic. We believe that the current survey highlights the main advantages of the use of Blockchain technologies compared to traditional techniques and invites the research community to investigate further on the remaining privacy issues.

Acknowledgment

This work has been supported by the joint grant project ”A Blockchain Platform for self-sovereign Patient identity:An innovative solution to combat covid-19” under the framework of the AUI/CNRST COVID-19 program.

References

[1] “Who coronavirus (covid-19),” https://covid19.who.int/table, (Accessed May 29, 2021).

[2] “Who-convened global study of origins of sars-cov-2: China part.” https://www.who.int/publications/i/item/who-convened-global-study-of-origins-of-sars-cov-2-china-part, (Accessed Jul. 31, 2021).

[3] W. H. Organization *et al.*, “Mask use in the context of covid-19: interim guidance, 1 december 2020,” World Health Organization, Tech. Rep., 2020.

[4] M. Salathé, C. L. Althaus, N. Anderegg, D. Antonioli, T. Ballouz, E. Bugnion, S. Capkun, D. Jackson, S.-I. Kim, J. Larus *et al.*, "Early evidence of effectiveness of digital contact tracing for sars-cov-2 in switzerland," *medRxiv*, 2020.

[5] J. Abou Jaoude and R. G. Saade, "Blockchain applications–usage in different domains," *IEEE Access*, vol. 7, pp. 45 360–45 381, 2019.

[6] M. S. Nawaz, P. Fournier-Viger, A. Shojaee, and H. Fujita, "Using artificial intelligence techniques for covid-19 genome analysis," *Applied Intelligence*, vol. 51, no. 5, pp. 3086–3103, 2021.

[7] H. Mukherjee, S. Ghosh, A. Dhar, S. M. Obaidullah, K. Santosh, and K. Roy, "Deep neural network to detect covid-19: one architecture for both ct scans and chest x-rays," *Applied Intelligence*, vol. 51, no. 5, pp. 2777–2789, 2021.

[8] T. Ozturk, M. Talo, E. A. Yildirim, U. B. Baloglu, O. Yildirim, and U. R. Acharya, "Automated detection of covid-19 cases using deep neural networks with x-ray images," *Computers in biology and medicine*, vol. 121, p. 103792, 2020.

[9] I. D. Apostolopoulos and T. A. Mpesiana, "Covid-19: automatic detection from x-ray images utilizing transfer learning with convolutional neural networks," *Physical and Engineering Sciences in Medicine*, vol. 43, no. 2, pp. 635–640, 2020.

[10] V. Kumar, D. Singh, M. Kaur, and R. Damaševičius, "Overview of current state of research on the application of artificial intelligence techniques for covid-19," *PeerJ computer science*, vol. 7, p. e564, 2021.

[11] K. Raza, "Artificial intelligence against covid-19: A meta-analysis of current research," *Big Data Analytics and Artificial Intelligence Against COVID-19: Innovation Vision and Approach*, pp. 165–176, 2020.

[12] A. Abd-Alrazaq, M. Alajlani, D. Alhuwail, J. Schneider, S. Al-Kuwari, Z. Shah, M. Hamdi, and M. Househ, "Artificial intelligence in the fight against covid-19: scoping review," *Journal of medical Internet research*, vol. 22, no. 12, p. e20756, 2020.

[13] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, "A comprehensive review of the covid-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact," *Ieee access*, vol. 8, pp. 90 225–90 265, 2020.

[14] 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, 2020.

[15] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, and M. Omar, "Blockchain and covid-19 pandemic: Applications and challenges," *IEEE TechRxiv*, 2020.

[16] 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. 37 936–37 950, 2021.

[17] M. Imran, U. Zaman, J. Imtiaz, M. Fayaz, J. Gwak *et al.*, "Comprehensive survey of iot, machine learning, and blockchain for health care applications: A topical assessment for pandemic preparedness, challenges, and solutions," *Electronics*, vol. 10, no. 20, p. 2501, 2021.

[18] H. Shah, M. Shah, S. Tanwar, and N. Kumar, "Blockchain for covid-19: a comprehensive review," *Personal and Ubiquitous Computing*, pp. 1–28, 2021.

[19] N. Ahmed, R. A. Michelin, W. Xue, S. Ruj, R. Malaney, S. S. Kanhere, A. Seneviratne, W. Hu, H. Janicke, and S. K. Jha, "A survey of covid-19 contact tracing apps," *IEEE access*, vol. 8, pp. 134 577–134 601, 2020.

[20] D. C. Nguyen, M. Ding, P. N. Pathirana, and A. Seneviratne, "Blockchain and ai-based solutions to combat coronavirus (covid-19)-like epidemics: A survey," *Ieee Access*, vol. 9, pp. 95 730–95 753, 2021.

[21] A. Fusco, G. Dicuonzo, V. Dell'Atti, and M. Tatullo, "Blockchain in healthcare: Insights on covid-19," *International Journal of Environmental Research and Public Health*, vol. 17, no. 19, p. 7167, 2020.

[22] D. Marbouh, T. Abbasi, F. Maasmi, I. A. Omar, M. S. Debe, K. Salah, R. Jayaraman, and S. Ellahham, "Blockchain for covid-19: review, opportunities, and a trusted tracking system," *Arabian Journal for Science and Engineering*, pp. 1–17, 2020.

[23] A. Sharma, S. Bahl, A. K. Bagha, M. Javaid, D. K. Shukla, and A. Haleem, "Blockchain technology and its applications to combat covid-19 pandemic," *Research on Biomedical Engineering*, pp. 1–8, 2020.

[24] T. P. Velavan and C. G. Meyer, "The covid-19 epidemic," *Tropical medicine & international health*, vol. 25, no. 3, p. 278, 2020.

[25] E. Mahase, "Covid-19: What new variants are emerging and how are they being investigated?" 2021.

[26] R. Tino, R. Moore, S. Antoline, P. Ravi, N. Wake, C. N. Ionita, J. M. Morris, S. J. Decker, A. Sheikh, F. J. Rybicki *et al.*, "Covid-19 and the role of 3d printing in medicine," pp. 1–8, 2020.

[27] A. Ghimire, S. Thapa, A. K. Jha, A. Kumar, A. Kumar, and S. Adhikari, "Ai and iot solutions for tackling covid-19 pandemic," in *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*. IEEE, 2020, pp. 1083–1092.

[28] A. A. Hussain, B. A. Dawood, and F. Al-Turjman, "Iot and ai for covid-19 in scalable smart cities," in *International Summit Smart City 360°*. Springer, 2020, pp. 3–19.

[29] S. Kumar, R. D. Raut, and B. E. Narkhede, "A proposed collaborative framework by using artificial intelligence-internet of things (ai-iot) in covid-19 pandemic situation for healthcare workers," *International Journal of Healthcare Management*, vol. 13, no. 4, pp. 337–345, 2020.

[30] M. Jamshidi, A. Lalbakhsh, J. Talla, Z. Peroutka, F. Hadjilooei, P. Lalbakhsh, M. Jamshidi, L. La Spada, M. Mirmozafari, M. Dehghani *et al.*, "Artificial intelligence and covid-19: deep learning approaches for diagnosis and treatment," *Ieee Access*, vol. 8, pp. 109 581–109 595, 2020.

[31] M. Otoom, N. Otoum, M. A. Alzubaidi, Y. Etoom, and R. Banihani, "An iot-based framework for early identification and monitoring of covid-19 cases," *Biomedical signal processing and control*, vol. 62, p. 102149, 2020.

[32] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan, and M. A. Imran, "Beeptrace: Blockchain-enabled privacy-preserving contact

tracing for covid-19 pandemic and beyond," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3915–3929, 2020.

[33] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *arXiv preprint arXiv:1906.11078*, 2019.

[34] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," in *Conference on the Theory and Application of Cryptography*. Springer, 1990, pp. 437–455.

[35] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, Accessed: Jun. 30, 2021. [Online].

[36] B. Houtan, A. S. Hafid, and D. Makrakis, "A survey on blockchain-based self-sovereign patient identity in healthcare," *IEEE Access*, vol. 8, pp. 90 478–90 494, 2020.

[37] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147 782–147 795, 2019.

[38] S. V. Jardim, "The electronic health record and its contribution to healthcare information systems interoperability," *Procedia technology*, vol. 9, pp. 940–948, 2013.

[39] C. Rathert, T. H. Porter, J. N. Mittler, and M. Fleig-Palmer, "Seven years after meaningful use: Physicians' and nurses' experiences with electronic health records," *Health care management review*, vol. 44, no. 1, pp. 30–40, 2019.

[40] M. Quinn, J. Forman, M. Harrod, S. Winter, K. E. Fowler, S. L. Krein, A. Gupta, S. Saint, H. Singh, and V. Chopra, "Electronic health records, communication, and data sharing: challenges and opportunities for improving the diagnostic process," *Diagnosis*, vol. 6, no. 3, pp. 241–248, 2019.

[41] D. M. Maslove, J. Klein, K. Brohman, and P. Martin, "Using blockchain technology to manage clinical trials data: a proof-of-concept study," *JMIR medical informatics*, vol. 6, no. 4, p. e11949, 2018.

[42] P. Sylim, F. Liu, A. Marcelo, and P. Fontelo, "Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention," *JMIR research protocols*, vol. 7, no. 9, p. e10163, 2018.

[43] J. Bay, J. Kek, A. Tan, C. S. Hau, L. Yongquan, J. Tan, and T. A. Quy, "Bluetrace: A privacy-preserving protocol for community-driven contact tracing across borders," *Government Technology Agency-Singapore, Tech. Rep*, 2020.

[44] T. Duarte, "Google and apple exposure notifications system: Exposure notifications or notified exposures?" 2020.

[45] "Nhs test and trace: what to do if you are contacted - gov.uk." https://www.gov.uk/guidance/nhs-test-and-trace-how-it-works, (Accessed Jun. 23, 2021).

[46] "In coronavirus fight, china gives citizens a color code, with red flags - the new york times." https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html, (Accessed Jun. 23, 2021).

[47] A. Khurshid, "Applying blockchain technology to address the crisis of trust during the covid-19 pandemic," *JMIR medical informatics*, vol. 8, no. 9, p. e20477, 2020.

[48] J. Song, T. Gu, Z. Fang, X. Feng, Y. Ge, H. Fu, P. Hu, and P. Mohapatra, "Blockchain meets covid-19: A framework for contact information sharing and risk notification system," in *2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*. IEEE, 2021, pp. 269–277.

[49] A. Khatoon, "Use of blockchain technology to curb novel coronavirus disease (covid-19) transmission," *Available at SSRN 3584226*, 2020.

[50] "Exposure notifications frequently asked questions preliminary-subject to modification and extension," 2020.

[51] B. Williams, "Principles of autonomy and decision making."

[52] R. Kumar, A. A. Khan, J. Kumar, A. Zakria, N. A. Golilarz, S. Zhang, Y. Ting, C. Zheng, and W. Wang, "Blockchain-federated-learning and deep learning models for covid-19 detection using ct imaging," *IEEE Sensors Journal*, 2021.

[53] G. Muhammad and M. S. Hossain, "A deep-learning-based edge-centric covid-19-like pandemic screening and diagnosis system within a b5g framework using blockchain," *IEEE Network*, vol. 35, no. 2, pp. 74–81, 2021.

[54] M. N. Wernick, Y. Yang, J. G. Brankov, G. Yourganov, and S. C. Strother, "Machine learning in medical imaging," *IEEE signal processing magazine*, vol. 27, no. 4, pp. 25–38, 2010.

[55] O. Gozes, M. Frid-Adar, H. Greenspan, P. D. Browning, H. Zhang, W. Ji, A. Bernheim, and E. Siegel, "Rapid ai development cycle for the coronavirus (covid-19) pandemic: Initial results for automated detection & patient monitoring using deep learning ct image analysis," *arXiv preprint arXiv:2003.05037*, 2020.

[56] R. Sujatha, J. Chatterjee *et al.*, "A machine learning methodology for forecasting of the covid-19 cases in india," 2020.

[57] S. Aich, N. K. Sinai, S. Kumar, M. Ali, Y. R. Choi, M.-I. Joo, and H.-C. Kim, "Protecting personal healthcare record using blockchain & federated learning technologies," in *2021 23rd International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2021, pp. 109–112.

[58] C. Garg, A. Bansal, and R. P. Padappayil, "Covid-19: prolonged social distancing implementation strategy using blockchain-based movement passes," *Journal of Medical Systems*, vol. 44, no. 9, pp. 1–3, 2020.

[59] F. Firouzi, B. Farahani, M. Daneshmand, K. Grise, J. S. Song, R. Saracco, L. L. Wang, K. Lo, P. Angelov, E. Soares *et al.*, "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*, 2021.

[60] S. Otoum, I. Al Ridhawi, and H. T. Mouftah, "Preventing and controlling epidemics through blockchain-assisted ai-enabled networks," *IEEE Network*, vol. 35, no. 3, pp. 34–41, 2021.

[61] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "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)*. IEEE, 2017, pp. 1–5.

[62] D. J. Leith and S. Farrell, "Coronavirus contact tracing app privacy: What data is shared by the singapore opentrace app?" in *Inter-*

national Conference on Security and Privacy in Communication Systems. Springer, 2020, pp. 80–96.

[63] R. Kumar and R. Tripathi, “A secure and distributed framework for sharing covid-19 patient reports using consortium blockchain and ipfs,” in *2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC)*. IEEE, 2020, pp. 231–236.

[64] “Cost of a data breach report 2020 — ibm,” https://www.ibm.com/security/digital-assets/cost-data-breach-report//, (Accessed May 29, 2021).

[65] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, “Novidchain: Blockchain-based privacy-preserving platform for covid-19 test/vaccine certificates,” *Software: Practice and Experience*, 2021.

[66] P. V. Klaine, L. Zhang, B. Zhou, Y. Sun, H. Xu, and M. Imran, “Privacy-preserving contact tracing and public risk assessment using blockchain for covid-19 pandemic,” *IEEE Internet of Things Magazine*, vol. 3, no. 3, pp. 58–63, 2020.

[67] H. Choudhury, B. Goswami, and S. K. Gurung, “Covidchain: an anonymity preserving blockchain based framework for protection against covid-19,” *Information Security Journal: A Global Perspective*, pp. 1–24, 2021.

[68] H. R. Hasan, K. Salah, R. Jayaraman, J. Arshad, I. Yaqoob, M. Omar, and S. Ellahham, “Blockchain-based solution for covid-19 digital medical passports and immunity certificates,” *IEEE Access*, vol. 8, pp. 222 093–222 108, 2020.

[69] T. Hardin and D. Kotz, “Amanuensis: Information provenance for health-data systems,” *Information Processing & Management*, vol. 58, no. 2, p. 102460, 2021.

[70] E. Bandara, X. Liang, P. Foytik, S. Shetty, C. Hall, D. Bowden, N. Ranasinghe, and K. De Zoysa, “A blockchain empowered and privacy preserving digital contact tracing platform,” *Information Processing & Management*, vol. 58, no. 4, p. 102572, 2021.

[71] N. Naik and P. Jenkins, “Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology,” in *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*. IEEE, 2020, pp. 90–95.

[72] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, M. Omar, and S. Ellahham, “Covid-19 contact tracing using blockchain,” *IEEE Access*, vol. 9, pp. 62 956–62 971, 2021.

[73] E. Bandara, W. K. Ng, K. De Zoysa, N. Fernando, S. Tharaka, P. Maurakirinathan, and N. Jayasuriya, “Mystiko—blockchain meets big data,” in *2018 IEEE international conference on big data (big data)*. IEEE, 2018, pp. 3024–3032.

[74] N. Ahmed, R. A. Michelin, W. Xue, G. D. Putra, S. Ruj, S. S. Kanhere, and S. Jha, “Dimy: Enabling privacy-preserving contact tracing,” *arXiv preprint arXiv:2103.05873*, 2021.

[75] W. Song, R. N. Zaeem, D. Liau, K. C. Chang, M. R. Lamison, M. M. Khalil, and K. S. Barber, “Self-sovereign identity and user control for privacy-preserving contact tracing.”

[76] B. Putz, M. Dietz, P. Empl, and G. Pernul, “Ethertwin: Blockchain-based secure digital twin information management,” *Information Processing & Management*, vol. 58, no. 1, p. 102425, 2021.

[77] “A decentralized, open source solution for digital identity and access management.” https://jolocom.io/wp-content/uploads/2019/12/Jolocom-Whitepaper-v2.1-A-Decentralized-Open-Source-Solution-for-Digital-Identity-and-Access-Management.pdf, (Accessed Jun. 25, 2021).

[78] N. Naik and P. Jenkins, “uport open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain,” in *2020 IEEE International Symposium on Systems Engineering (ISSE)*. IEEE, 2020, pp. 1–7.

[79] W. Lv, S. Wu, C. Jiang, Y. Cui, X. Qiu, and Y. Zhang, “Towards large-scale and privacy-preserving contact tracing in covid-19 pandemic: A blockchain perspective,” *IEEE Transactions on Network Science and Engineering*, 2020.

[80] K. Christodoulou, P. Christodoulou, Z. Zinonos, E. G. Carayannis, and S. A. Chatzichristofis, “Health information exchange with blockchain amid covid-19-like pandemics,” in *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, 2020, pp. 412–417.

[81] “Hyperledger indy.” https://github.com/hyperledger/indy-sdk, (accessed Jun. 25, 2021).

[82] A. Tobin and D. Reed, “The inevitable rise of self-sovereign identity,” *The Sovrin Foundation*, vol. 29, no. 2016, 2016.

[83] “Covid-19 credentials initiative: Home,” https://www.covidcreds.org/, (accessed Jun. 25, 2021).

[84] X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, “A blockchain privacy protection scheme based on ring signature,” *IEEE Access*, vol. 8, pp. 76 765–76 772, 2020.

[85] X. Li, B. Tao, H.-N. Dai, M. Imran, D. Wan, and D. Li, “Is blockchain for internet of medical things a panacea for covid-19 pandemic?” *Pervasive and Mobile Computing*, p. 101434, 2021.

[86] D. Wang, J. Zhao, and Y. Wang, “A survey on privacy protection of blockchain: The technology and application,” *IEEE Access*, vol. 8, pp. 108 766–108 781, 2020.

[87] 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, pp. 1–2, 2020.

[88] D. S. W. Ting, L. Carin, V. Dzau, and T. Y. Wong, “Digital technology and covid-19,” *Nature medicine*, vol. 26, no. 4, pp. 459–461, 2020.

[89] M. Muzammal, Q. Qu, and B. Nasrulin, “Renovating blockchain with distributed databases: An open source system,” *Future generation computer systems*, vol. 90, pp. 105–117, 2019.

[90] G. Wood *et al.*, “Ethereum: A secure decentralised generalised transaction ledger,” *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[91] D.-J. Munoz, D.-A. Constantinescu, R. Asenjo, and L. Fuentes, “Clinicappchain: A low-cost blockchain hyperledger solution for healthcare,” in *International Congress on Blockchain and Applications*. Springer, 2019, pp. 36–44.

NABIL BENAMAR NABIL BENAMAR received the B. E., M.Sc., and Ph.D. degrees from the University of Moulay Ismail in 1998, 2001, and 2004, respectively. He is currently a Professor of computer sciences with the School of Technology, Department of Computer Engineering, Moulay Ismail University, and the School of Sciences and Engineering at alAkhawayn University on Ifrane, Morocco. He is also Director of the IMAGE laboratory. His main research topics are IPv6, vehicular networks, ITS, IoT, and Service Function Chaining. He has authored several journal papers and IETF Internet Drafts. He is a reviewer for Computer Communications (Elsevier), JKSUCS (Elsevier), Adhoc (Elsevier), IJWIN (Springer), AJSE (Springer), and IEEE ACCESS. He is also a TPC Member in different IEEE conferences, such as Globecom, ICC, and PIMRC. He is an IPv6 Expert (he.net certified) and a Consultant with many international organisms, such as Academic Agency for Francophonie, AFRINIC, and MENOG. He is also an expert in Internet Governance after completion the ISOC Next generation e-learning programme: “Shaping the Internet, History and Futures” in 2012. He is an ISOC Ambassador to IGF from 2012 to 2013, a Google Panelist in the first Arab-IGF, an ISOC Fellow to IETF and ICANN Fellow. He is a member of Task Force for Arabic IDNs which is a part of Global Stakeholder Engagement endorsed by ICANN. He is a member of G6 association for IPv6 and one of the contributors to the IPv6 MOOC.

Bouchaib Falah Bouchaib Falah is an Associate Professor at the AlAkhawayn University in Ifrane. Offering more than 20 years of combined experience developing and implementing computer science and technical/math curriculum for different colleges and universities as well as web designs for multimillion-dollar organizations in USA and researcher in different projects, Dr. Falah is currently an Assistant Professor at Al Akhawayn University, teaching graduate and undergraduate software engineering courses, School of Science and Engineering. Beside teaching high school level math in Morocco and college mathematics and computer science at Harrisburg Area Community College in Pennsylvania, Suny Orange Community College in New York, Pennsylvania State University in Pennsylvania, Central Pennsylvania College in Pennsylvania, Concordia College in Minnesota, and North Dakota State University in North Dakota, Dr. Bouchaib Falah has an extensive industrial experience with Agri-ImaGIS, Synertich, and Commonwealth of Pennsylvania Department of Environmental Protection. He holds a doctoral degree in Software Engineering from North Dakota State University, in 2011, a master degree in Computer Science from Shippensburg University, in 2001, and a bachelor degree/teaching certificate from Ecole Normale Superiere in Morocco, in 1990.