World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:17, No:2, 2023

Blockchain Technology Applications in Patient Tracking Systems Regarding Privacy-Preserving Concerns and COVID-19 Pandemic

Farbod Behnaminia, Saeed Samet

Open Science Index, Information and Communication Engineering Vol:17, No:2, 2023 publications.waset.org/10012975.pdf

Abstract—The COVID-19 pandemic has paralyzed many lives until a vaccine has been available, which caused the so-called "new normal". COVID-19 is an infectious disease. It can cause significant illness or death in anyone. Governments and health officials tried to impose rules and regulations to avoid and slow down transmission. Therefore, software engineers worldwide developed applications to trace and track patients' movements and notify others, mainly using Bluetooth. In this way, everyone could be informed whether they came in close contact with someone who has COVID-19 and take proper safety precautions. Because most of the applications use technologies that can potentially reveal the user's identity and location, researchers have debated privacy preservation and how to improve user privacy during such pandemics. We conducted a comprehensive evaluation of the literature by looking for papers in the relevant field and dividing them into pre- and post-pandemic systems. Additionally, we discussed the many uses of blockchain technology in pandemic control. We found that two major obstacles facing blockchain implementation across many healthcare systems are scalability and privacy. The Polkadot platform is presented, along with a review of its efficacy in tackling current concerns. A more scalable healthcare system is achievable in near future using Polkadot as well as a much more privacy-preserving environment.

Keywords—Blockchain, Electronic Record Management, EHR, Privacy-Preserving, patient tracking, COVID-19, trust and confidence, Polkadot.

I. Introduction

TO begin with, we should know that tracking systems entail the systematic collection of data, analysis, and interpretation, all of which are tightly interwoven with the timely transmission of these data to those responsible for preventing and controlling illness and harm. The spread of illness and other health problems are exacerbated in the midst of a humanitarian crisis.

On December 31st, 2019, the World Health Organization (WHO) was alerted about instances of pneumonia of unknown etiology in Wuhan City, China. Authorities in China announced the discovery of a new coronavirus, which they named "2019-nCoV," on January 7, 2020 [1]–[3].

The blockchain is often regarded as Bitcoin's most important technical advance since it serves as a "trustless" proof method for all network transactions. the "miner-accountants" who maintain the "public ledger" may be trusted by users, rather than needing to develop and maintain confidence with a transaction counterparty or a third-party intermediary (like a bank). The major innovation is the use of the blockchain as the framework for a new system of trustless decentralized transactions. Every form of transaction may now be completed without the need for a third-party intermediary, thanks to the blockchain [4], [5].

An infected person's connections may be identified by contact tracing, which is the process of collecting more information about these individuals. Since its inception in the early stages of epidemiology, tracking contacts has been used to prevent the spread of infectious illnesses. They depended on a list of people they had been in touch with or places they had gone recently, which was far from a thorough list. It is possible to alert people who could be approached by letters or phone calls or emails. Because of this, the list's completeness and correctness, as well as the process's speed and efficiency, are constrained by the old method of tracking down contacts [6].

Infectious disorders caused by Coronaviruses (CoV) range from the common cold to more severe conditions. Humans have not before been infected with a novel coronavirus (nCoV). In an effort to promptly discover any new 2019-nCoV cases, countries throughout the world have ramped up their monitoring. When it comes to secure data exchange, blockchain is becoming a safe and efficient network. This includes applications in the financial and healthcare industries. Blockchain has the potential to transform the healthcare industry. Confidential and authorized data can be exchanged securely through this method. In a blockchain consortium, any healthcare organization can share medical information independently of the system it uses for its native electronic health record [7].

II. Healthcare Data Sharing & Blockchain before COVID-19

Protecting sensitive health information and distributing the software across a variety of hospital contexts are two well-known difficulties. The main purpose of [8] is to answer this question whether it is possible to develop and implement a system, running on blockchain, for keeping the health records across hospitals and sharing them simply without any privacy leaks. Although blockchain provides us unique opportunities to increase the healthcare system's treatment and diagnoses efficacy, certain challenges are still in

Farbod Behnaminia and Saeed Samet are with Department of Computer Science, University of Windsor, Canada (e-mail: behnami@uwindsor.ca, saeed.samet@uwindsor.ca).

This work is partially supported by the School of Computer Science, the University of Windsor, and the Natural Sciences and Engineering Research Council of Canada (NSERC).

Open Science Index, Information and Communication Engineering Vol:17, No:2, 2023 publications.waset.org/10012975.pdf

place regrading scalability and reliability before a widely-use implementation. Reference [9] aims to introduce and review blockchain technology to the biomedical and health care areas, including its merits, drawbacks, and most recent applications.

In general, blockchain is regarded as a distributed ledger that is used to store healthcare–related data for the purposes of sharing, trading, analyzing, recording, and verifying among stakeholders. The most debated biomedical/health care application is the use of blockchains as a core tech for Health Information Exchange (HIE), or health transactions between patients, providers, payers, as well as other related personnel [9]. Cloud-based solutions and blockchain-based solutions are examples of HIE systems that are either centralized or decentralized, respectively [10].

Many studies and active initiatives are centered on transferring patient care data over blockchains in order to enhance medical record administration, including but not limited to Healthcare Data Gateways, MedVault, Fatcom, BitHealth, Gem Health Network. Several well-known firms, like Deloitte and Accenture, are also experimenting with blockchain technology to store health care data and manage medical records. Guardtime, a startup in Estonia that provides a blockchain-based solution to safeguard 1 million health records, is another well-known example [9].

According to [9], another important goal is to verify claim transactions in order to support health care financing tasks, such as pre-authorization payment, alternative payment models, automatic claims using Fast Healthcare Interoperability Resources and smart contracts, and Smart Health Profile to help manage Medicaid beneficiaries' constant exit and reentry due to eligibility changes.

Also, some research teams, including MedRec, Data Lake, Healthbank, and blockchain-based data sharing networks, suggest leveraging blockchain technology to speed up secondary usage of clinical data (i.e. clinical and biomedical studies and research). ModelChain also implemented blockchain to improve the security and scalability of distributed privacy-preserving health care predictive modelling across different institutions.

Many studies and projects have proposed using blockchains to store various types of health care–related data, such as genomics and precision medicine data, patient-related outcomes data, provider/patient directories and care plans data, clinical trial data, patient consent data, pharmaceutical supply chain data, and biomarker data, in addition to using them as patient care data ledgers [9].

A. Blockchain in Biomedical and Healthcare

The first significant advantage of blockchain is decentralized administration. Distributed database management systems (DDBMS) are conceptually centralized database management systems, whereas blockchain is a peer-to-peer, decentralized database management system. As a result, blockchain is appropriate for applications in which independently managed biomedical/health care parties who want to interact without relinquishing authority to a central management middleman [9].

The immutable audit trail is the second major advantage. DDBMSs, like other database systems, provide create, read, update, and delete functions, whereas blockchain only supports creation and read functions. As a result, blockchain is suited as an immutable ledger for recording vital information.

The third consideration is data provenance. On DDBMS, the system administrator can alter the ownership of digital assets, but on blockchain, the owner can only change the ownership by following the cryptographic protocols. The sources of the assets may also be traced, enhancing the re-usability of confirmed data.

The fourth advantage is that it is both sturdy and available. Although DDBMS and blockchain are built on distributed technology and so do not suffer from single-point-of-failure, achieving the high level of data redundancy that blockchain achieves would be expensive for DDBMS.

The latest main advantage of blockchain is increased security and privacy through the use of cryptographic algorithms. For example, the 256-bit Secure Hash Algorithm (SHA-256) is used as the cryptographic hash function in the hash-chain that the proof-of-work algorithm operates on in the Bitcoin blockchain.

B. Proposed Solutions & Analysis

Permissioned data sharing and the deployment of blockchain technology by [8] are discussed in this section to make cooperation across hospital systems easier.

1) Data Sharing/Security Solution: Although transactions are cryptographically signed in Blockchain, they are transparent to everyone participating in the network. So, privacy and restricted access to the health data matters. Each piece of data, in this system, has a single user (owner) who may share it with other users or groups at various degrees of access (summary versus full data). The data sharing method is based on request and response in such a way that a cryptographic object is exposed to the receiver in such a manner that only that receiver has access to data at the given access level. In the event of access revocation, there is an additional safeguard that even a receiver's private key, along with raw blockchain transaction data, would not be sufficient to gain data access. As a file storage sector, they use the InterPlanetary File System (IFPS) separately, which is a decentralized file system. It guarantees that duplication is kept to a minimum over the whole file system network [8]. In Fig. 1 we can see the overall architecture of their proposed system.

For having a robust encryption system, it would necessitate capturing the structure of submitted documents within the underlying smart contracts, such that sensitive fields are treated independently of the rest of the document.

Their solution makes use of the Ethereum platform [11] for smart contract capabilities, as well as Docker containers and microservices in a distributed design. They used the Elliptic Curve Integrated Encryption System (ECIS), a hybrid of the Elliptic Curve Diffie-Hellman (ECDH) algorithm, Concatenation Key Derivation Function (KDF), and the Advanced Encryption Standard (AES-256 in Galois Counter

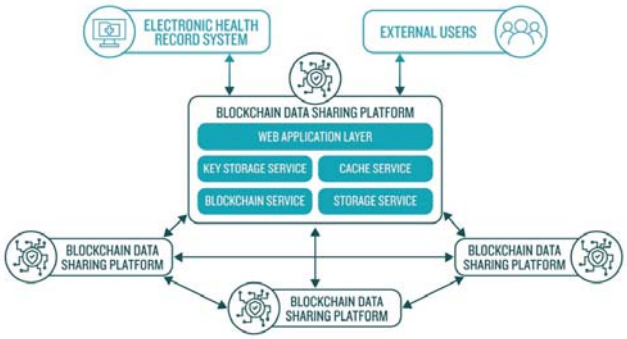

Fig. 1 An illustration of the system architecture [8]

Mode) Block Cipher for key encryption using elliptic curve primitives.

All in all, the data are kept in an external storage solution, and the system's blockchain component is in charge of executing Smart Contracts. Constraints might be introduced to the system to guarantee that data files are standardized according to healthcare-related standards.

2) Ease of Deployment and Implementation: In order to achieve an ease of access, their system utilizes a virtual machine deployment. By using containers, they gain a better installment, maintenance, and portability. In the application layer, user's queries are monitored and contains the main business logic which allows us to create and interact with the smart contracts on the blockchain.

Features such as: flexibility on data specifications, easier parallel development, ability of using different programming languages, were made possible via a distributed microservice design in which total resource use is split over several computer instances.

III. Blockchain in Pandemic Management

Although previous works have preciously offered some insight on the present COVID-19 scenario, they provide a short and incomplete picture of the precise issue [12]–[17]. The authors of [18] offer a complete assessment of the COVID-19 pandemic, which will assist readers in acquiring a better knowledge of the current worldwide situation resulting from the COVID-19 pandemic.

One of the primary benefits of adopting blockchain-enabled apps, according to experts, is blockchain's capacity to validate continually changing data. This capability might be pretty valuable in dealing with the fast-developing COVID-19 issue. Two blockchain-based solutions are discussed; "*Civitas*" and "*MiPasa*" [18]. A Canadian start-up specializing in blockchain solutions has just released Civitas, a safety system in the form of an app that may help local authorities in many countries worldwide limit the impact of the COVID-19. Civitas includes built-in telemedicine capabilities that allow doctors to watch their patients' symptoms and provide comments about the medications to be taken and healthcare plans to be followed. This software compares people's official IDs to blockchain data to determine if they have permission to leave their houses. This software also identifies the best time and day for persons with COVID-19 symptoms to go out and buy necessary things, reducing the chance of infecting others. According to the firm, the app ensures that people's data is safe and secure. MiPasa is a Hyperledger Fabric-based data streaming platform. This platform also makes use of the IBM blockchain and cloud platforms to allow the sharing of verified health and location data among individuals, authorities, and hospitals. This program functions by gathering data from numerous medical organizations, public health officials, and other persons. The WHO recently recognized this app as an excellent platform for assisting clinicians in gaining access to verifiable information. The data on this platform can assist hospitals in determining future action plans and efficiently allocating resources to mitigate the effect of the COVID-19 epidemic.

The pandemic's nature is spreading. As a result, distributed ledger technologies, such as blockchain, can be highly beneficial in dealing with this problem. Blockchain technology enables individuals and businesses worldwide to join a single linked network that allows for the secure sharing of data. The tamper-proof characteristic of blockchain makes it resistant to unauthorized modifications, and the use of consensus algorithms and smart contracts reduces the possibility of propagating fake data and fraudulent information. Blockchain-based apps can be used to digitally monitor and manage COVID-19 patients, alleviating part of the strain on hospital staff and other healthcare workers [18]. Some of the significant ways in which blockchain technology can aid in the fight against the COVID-19 are described as:

1) Increasing Testing and Reporting Capabilities
2) Keeping Track of COVID-19 Patients' Information
3) Managing the Implementation of Lockdown
4) Preventing the Spread of False News
5) Providing an Incentive-Based Volunteer
6) Participation Platform Providing a Secure Donation for Supporters
7) Reducing Supply Chain Breakdowns

In Fig. 2 we can see the contact tracing applications for COVID-19, especially in Blockchain.

A. Increasing Testing and Reporting Capabilities

To guarantee efficacy, testing must be done intelligently, and reliable data on the number of tests completed must be kept. To that aim, blockchain technology can aid in the establishment of distributed check-in sites for testing patients who exhibit COVID-19-related symptoms. All of these check-in sites' coordinators can function as nodes in the same distributed blockchain network. These nodes on this network can continually update data about the number of tests done and the number of laboratory-confirmed cases in their local check-in site. Because blockchain is irreversible, data saved in the network will be tamper-proof and can thus be trusted by all healthcare practitioners and government agencies.

Open Science Index, Information and Communication Engineering Vol:17, No:2, 2023 publications.waset.org/10012975.pdf

Open Science Index, Information and Communication Engineering Vol:17, No:2, 2023 publications.waset.org/10012975.pdf

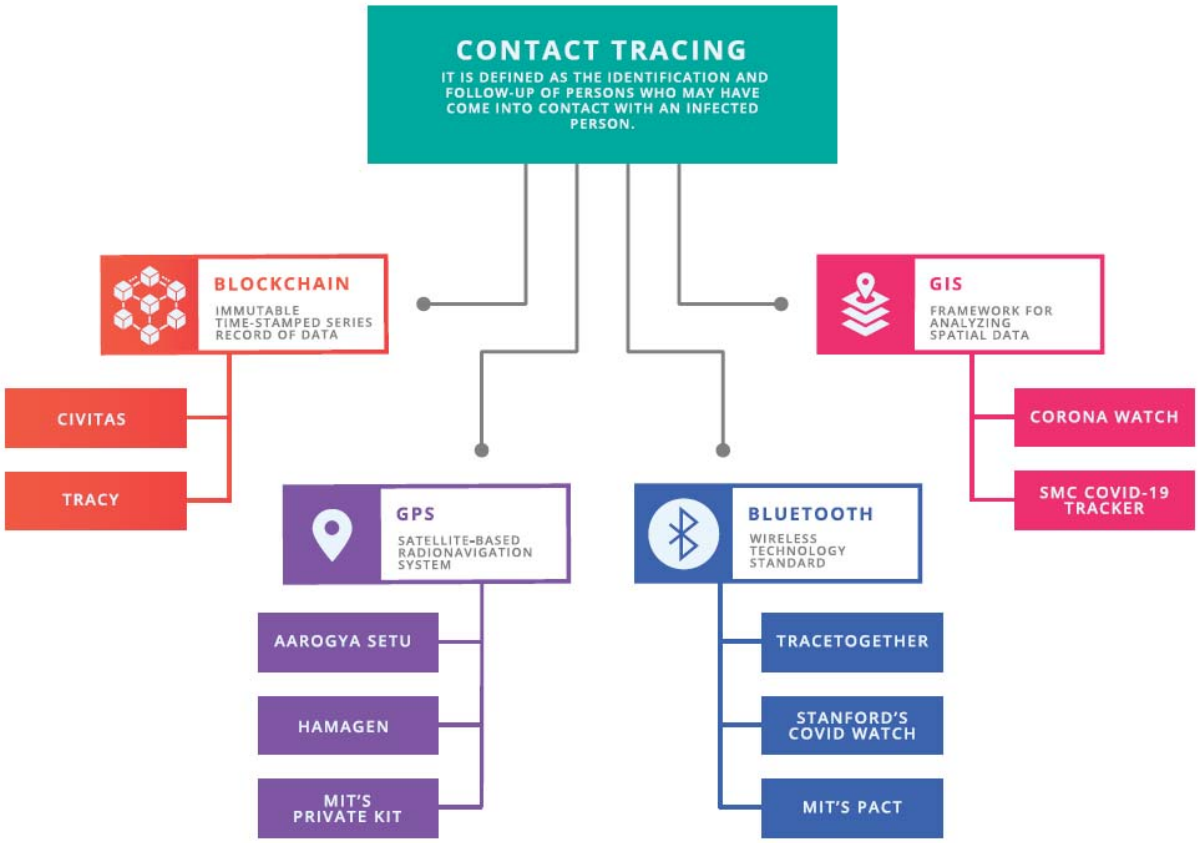

Fig. 2 Contact tracing applications for COVID-19 [18]

B. Keeping Track of COVID-19 Patients' Information

When a person tests positive for COVID-19, all of their information, including sex, age, medical history, underlying health problems, the severity of the disease, the symptoms acquired, and the suggested course of treatment, is safely uploaded to the network. Soon, every health center dealing with a confirmed case of COVID-19 will be able to refer to these studies to predict the type of facilities and medications needed to cope with the issue at hand.

C. Managing the Implementation of Lockdown

To accomplish the desired outcomes of the lockdown, people from the police department, healthcare department, Non-Governmental Organizations (NGOs), and other volunteers must work hand in hand with government officials. Blockchain technology can let the government and non-governmental organizations monitor the needs of people in different parts of the nation and efficiently manage lockdown implementation. All participating nodes in the blockchain network are permitted to check for the requirements indicated by nodes from various regions, after which the targeted organizations may take necessary measures to meet those needs.

D. Preventing the Spread of False News

Because numerous social platforms are presently in use, authorities find it difficult to check the validity of the information published on each site. The usage of a public blockchain network for information exchange can be an up-and-coming solution for limiting the spread of rumors, conspiracy theories, fake news, and derogatory remarks.

E. Providing an Incentive-Based Volunteer

A blockchain-based reward structure might be extremely beneficial in encouraging a large number of individuals to volunteer for COVID-19 crisis management. To honor their efforts and inspire them to engage even more enthusiastically, all blockchain network participants can be awarded tokens or certificates of gratitude.

F. Participation Platform, Providing a Secure Donation for Supporters

To dispel concerns about the legitimacy and transparency of existing donation platforms and, as a result, empower more individuals to give monetary assistance, a secure and transparent donation platform is necessary. Blockchain-based systems can ensure the secure collecting of funds, while also ensuring transparency in terms of where the contributed funds are used.

Open Science Index, Information and Communication Engineering Vol:17, No:2, 2023 publications.waset.org/10012975.pdf

G. Reducing Supply Chain Breakdowns

Several initiatives have been undertaken in recent years by companies across the globe to incorporate blockchain into their supply chains in order to enhance supply chain visibility, miss of which is recognized as the major cause of supply chain breakdowns. Permission blockchains enable suppliers to transmit and receive data without revealing the identities of their partners.

IV. Proposed Systems after the COVID-19

Some of the previous main works include Singapore TraceTogether, Google/Apple Contact Tracing, UK NHS Contact Tracing, China Health Code System [19]–[22]. The first three solutions use Bluetooth technology with a high-power demand because the user is obliged to keep the device in an active broadcasting mode under this system, which consumes the user device's battery. All Bluetooth-based contact tracing systems are subject to threats such as spying, sniffing, and jamming due to the Bluetooth technology's vulnerable wireless interface. There is a significant possibility of replay attacks on the contact tracking network, resulting in widespread fear among the population.

By scanning the QR code connected with the user, China Health Code System is based on relational cross-match. Because of the centralization of this system, user privacy is not protected, and the user's identity is not hidden from the authorities. On the other hand, this QR code is only scanned when passing checkpoints, saving the user's phone energy and consuming no data.

In this section, some of the proposed blockchain-based systems are introduced briefly.

A. BeepTrace

Here a detailed explanation of the architecture behind the BeepTrace is provided, including entities, functions and interfaces, and the workflow of the BeepTrace [6].

1) Entities, Functions & Interface:

- Users: refers to the people who utilize a contact tracing app on a mobile device. For self-matching, all users will submit their encrypted TraceCode to the tracing blockchain and read from the notification blockchain.
- Diagnosticians: diagnose and approve validated COVID-19 users' geodata with a signed prefix before sending to the tracing blockchain for solver matching.
- Geodata solvers: are the trustworthy third party or user's server or server cluster, interacts with the geodata and gives endorsement on the notification chain; reads raw data from the tracing blockchain and compares it to the data on the notification blockchain.
- Public Key Infrastructure (PKI)/Certified Authority (CA): Key delivery to the user, diagnostician, and solvers are handled by a trusted third party (e.g., governments, public health agencies).
- Positioning service providers: are GPS, Bluetooth, Cellular Tower, and Wi-Fi, to name a few, if the user's device supports them.
- Tracing blockchain: is one of two chains that accept TraceCode registration from both the user and the diagnostician. The solver reads it as well for geodata matching.
- Notification blockchain: is the chain dedicated to risk registration to the TraceCode of the impacted users.
- TraceCode: is a mask name for the blockchain address. It consists of two parts: the front portion is the user pseudonym, known as the prefix, and the back part is geodata cipher-text, known as the suffix.

2) Workflow of the BeepTrace: PKI/CA gives the keys to the above parties as to the first stage of BeepTrace. Users will obtain raw geodata from positioning service providers (Step 2) and produce several local private keys over time (for example, once a day), which will be kept in users' local storage, ideally on an encrypted chip (Step 3). This encryption will be strong enough to safeguard users' privacy from known threats while avoiding human error. These keys will be used to produce a pseudonym, used as the prefix of a TraceCode blockchain address. In step 4, the user, on the other hand, produces a new cipher-text using a public key that has been validated by a CA (a trusted party) to encrypt its current geographical or topological position data with a timestamp, forming the back portion of TraceCode. This geodata is referred to as cipher-text, and it will be utilized as the suffix of a blockchain address connected with the pseudonym, as described in Step 5. The initial link between a user pseudo-identity and geodata in the form of blockchain addresses is successfully constructed at this stage. In Step 6, the user will announce the address on the blockchain network after being produced. As a result, the address may be indexed by a trustworthy third party using its suffix, and the users' privacy is secured owing to the pseudonym's anonymous identity.

Once a diagnostician has diagnosed a user, the user can exchange existing pseudonyms with the current handler by granting the patient's approval in step 7. After getting all of the pseudonyms from the users, this diagnostician uses the prefix to trace down all of the connected addresses. The trustworthy one must validate the pseudonyms during the pseudonym exchange. Meanwhile, this trustworthy individual decouples the user's private key-related prefixes from the geodata suffix and replaces the pseudonym section with another private key encrypted cipher-text specified to the diagnosticians. The diagnostician creates a new blockchain address by re-coupling the new prefix and suffix, which can be done with a man-made drifting/noise encryption mechanism for added security, and then endorses it on the blockchain network, as described in step 8. Anyone with access to the tracing blockchain, after the confirmed patient's status has been updated, will be able to read the ciphertext and know the update made by the diagnostician. However, access to the geodata is limited to the geo private keyholder, issued by a public trusted party with the previously mentioned public keys. At step 9, the data once again has no access to user information. At the same time, the user is the only one who knows about the pseudonym's link.

Step 10: Any interested parties/users who have been allowed by the CA can begin decrypting the geodata and timestamp from confirmed patients who the diagnosticians have marked.

Open Science Index, Information and Communication Engineering Vol:17, No:2, 2023 publications.waset.org/10012975.pdf

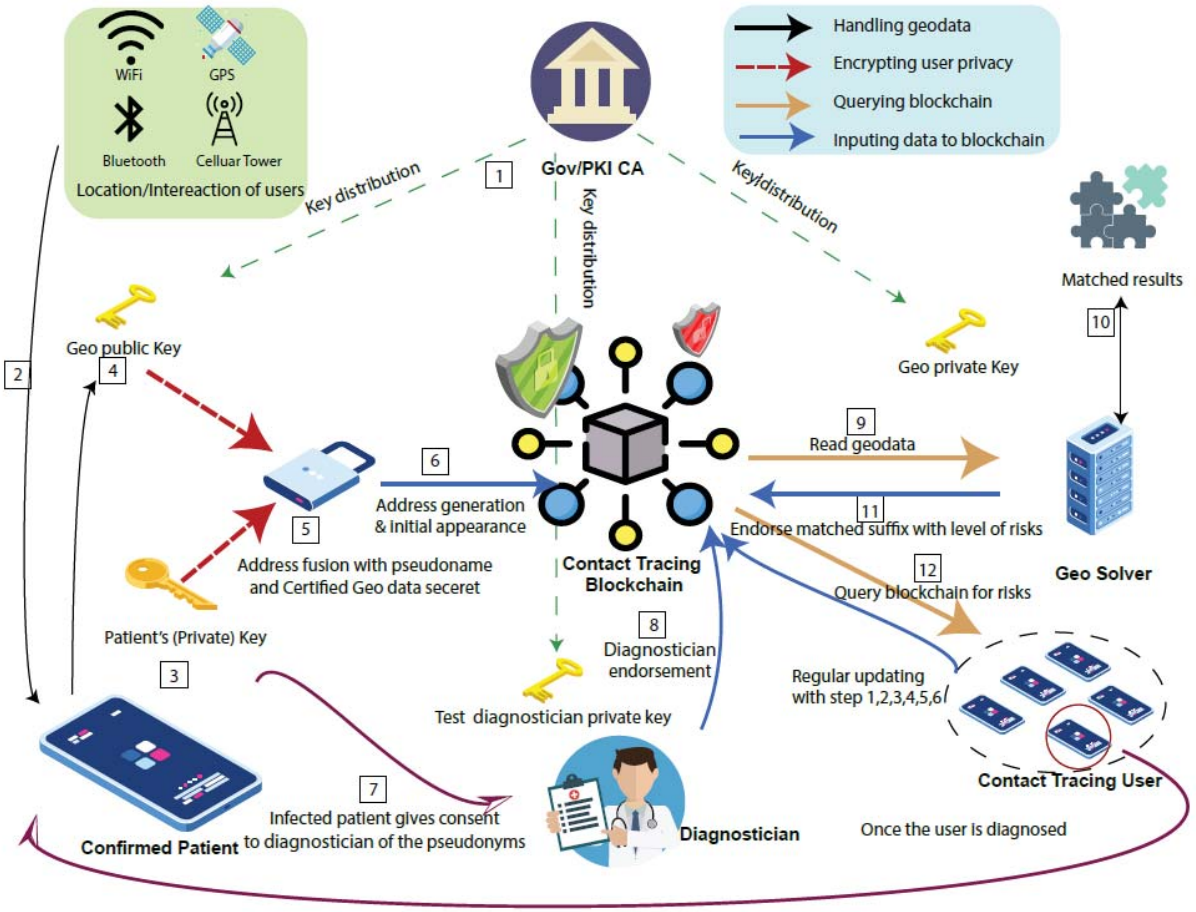

Fig. 3 BeepTrace Framework [6]

If cross-infection between several blockchain addresses is possible, the solvers will update the risk level for connected addresses by seeking up the suffix and endorsing it on the blockchain. In Step 11, the highlighted addresses are re-declared on the notification blockchain. When the user is using the tracing App and the notification download has been completed locally in Step 12, the user can look up its addresses on the notification blockchain, which is a separate chain dedicated to risk level notification, and the users are now passively notified once the addresses match with endorsements made to any of the users' addresses [6].

B. Blockchain-Based Digital Contact Tracing App

Authors [23] describe the digital contact tracking technique and the applications built so far to tackle the COVID-19 epidemic in this article. On the other side, they investigate how adopting a blockchain-based decentralized network for managing the app may give users with privacy-preserving contact tracking without sacrificing speed and efficiency.

1) Solution: Because users' data are gathered, tracked, tallied, and broadcasted to the network, it is vital to protect user privacy and avoid identity theft. Assurances to users that only data essential to tracking COVID-19 propagation is being

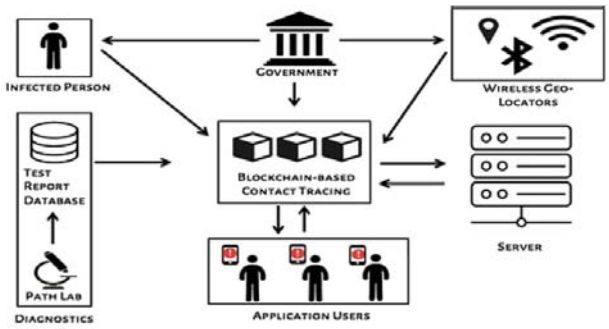

Fig. 4 Blockchain-based contact tracing app structure [23]

recorded are still inadequate. Blockchain technology may help contact tracing by enabling dispersed peer-to-peer network communication between users and app management [24].

Sharing data for decision-making processes is also problematic in a centralized network, owing to the hazards of data tampering. The blockchain-based solutions might manage this, since the network is dispersed and the users' identities are initially hidden.

Currently, decentralized applications are only accessible

Open Science Index, Information and Communication Engineering Vol:17, No:2, 2023 publications.waset.org/10012975.pdf

for limited geographical networks, which is inconvenient for individuals who travel often for business. So a blockchain-based decentralized network can give worldwide accessibility and traceability while connecting people from all over the world.

False information and rumors circulating among individuals might cause panic and should be stopped. To minimize inaccuracies or discrepancies in data, health care institutions must have trustworthy authority to review and authenticate it. So, the blockchain network is the greatest alternative, since it allows for transparent contact tracking while protecting anonymity.

Any activity inside a blockchain-based architecture is requested and represented as a block. These blocks of transactions are broadcast to all network nodes and verified only if all network nodes verify them. Fig. 4 illustrates a typical blockchain-based contact tracing app structure.

The transaction flow may be like this: all app users, even infected ones, will submit encrypted data to the blockchain network and do match on their own devices. Infected users may use the blockchain contact tracing software to map their contacts with the server's support. The network executes the mapping using the geographical data provided and feeds the results back to the blockchain. The servers receive geographical data from users using wireless technologies such as Wi-Fi, Bluetooth, or GPS. In addition, the government tracks all data transfers between users, path labs and servers.

C. Combining Solutions with GIS

Patients' COVID-19 symptoms, whereabouts, and health history are all recorded with utmost secrecy using blockchain technology during the epidemic. COVID-19-related data and information may now be shared more easily because to the recent emergence of several platforms that make use of this new technology. In a virus-free zone, this technology may also be used to monitor people's movements. Making the public surveillance system more effective and resilient may be achieved by combining blockchain technology with AI and Geographic Information Systems (GIS).

Patients, testing and clinical labs, hospitals, and government sites employ blockchain technology nodes. The digital ledger also contains patient data, test results, treatment status, and discharge summaries.

Fig. 5 depicts the basic stages employed in blockchain technology to monitor COVID-19 active patients. Initially, the patient is assessed and diagnosed with COVID-19 pre-symptoms. The patient is isolated for at least 14 days if the test results are positive. During this time, the patient is treated and monitored using blockchain technology. The patient is then re-examined for COVID-19. If the sample is negative, the patient is released with a discharge report. The patient data are saved for future reference, kept private, and supplied as required. The blockchain technology ensures the patient's data is accurate.

Healthcare, finance, politics, economics and education have all been hit hard. Blockchain technology can help manage the post-COVID-19 future. Some of the most common use cases

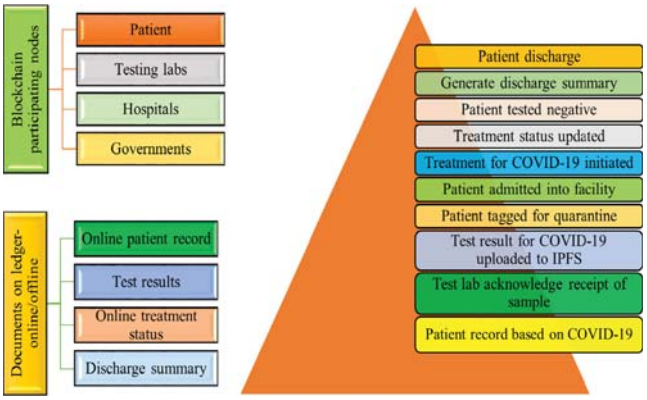

Fig. 5 Role of Blockchain Technology for COVID-19 [25]

for blockchain technology are call tracking, disaster assistance and medical data exchange. Others include automated surveillance, contactless delivery and online education.

When a patient is diagnosed with COVID-19, it is important to identify everybody who had intimate contact with them during the incubation period. It is achievable via contact tracing, which tries to find the patient's social connections during that time. Various apps employing Bluetooth Low Energy (BLE) technology have been created to record intimate contacts between mobile phones, wearables, and the Internet of Things (IoT). Because contact tracing data is maintained in a centralized cloud, consumers may lose control of their data. Thus, blockchain technology can help protect users' data by offering a decentralized system that gives consumers complete control over their data. Therefore, permitting pseudo-anonymity protects the patient's privacy.

The COVID-19 epidemic has hampered global trade. Achieving a new kind of working environment that incorporates social separation and working with a small number of people to avoid physical touch is increasingly harder. It caused a supply and demand issue. Demand for medical equipment and pharmaceuticals is increasing. Another explanation for the spike in demand for particular things such as food is panic purchasing. Blockchain technology can enable parties connect and build provenance and transparency chains. This can assist create smart contracts with tight access constraints and automation.

A good dataset for COVID-19 research requires sharing relevant data with healthcare colleagues nationally and globally. The privacy of patients must be protected, and the sharing method must not breach national or international data-sharing legislation. Medical IoT devices may gather detailed data on blood oxygen levels, medicines, and more. Blockchain can facilitate real-time data exchange between hospitals and medical practitioners. Using blockchain may assist solve issues like data forgery and mutation. Blockchain allows decentralised storage. Thus, improving data security and privacy helps retain stakeholder confidence.

To combat new coronavirus (COVID-19) sickness, it is vital to socially isolate, wear face masks, protective shields, and monitor symptoms like fever and cough. But humans are not used to these actions. Alerts must be continual and automatic

Open Science Index, Information and Communication Engineering Vol:17, No:2, 2023 publications.waset.org/10012975.pdf

to save human lives. Furthermore, COVID-19 transmission is quite high in many places, necessitating contactless delivery for food and medication. Blockchain-powered UAVs and robots may be used for surveillance and delivery. In high-speed transmission zones, blockchain-powered UAVs and robots can successfully function without human interference.

D. AYUSH

The suggested solution uses blockchain technology to create a transparent health record chain. When a patient transfers from one hospital to another, he/she authorizes the transfer of data. If the new hospital generates new health data, they first upload it to the IPFS file system. Its hash is added to the blockchain. The suggested approach is patient-centric, meaning the patient has control over his/her data. This is because the system requires a permissioned network, which would be Hyperledger Fabric. The architecture of the proposed system, AYUSH, will be discussed in this section [26].

1) AYUSH Platform: The AYUSH platform encapsulates Hyperledger Fabric and IPFS implementation details and exposes API module functions. Modules in the AYUSH network include: Fabric client, IPFS interface, Auth module, Membership module, Application logic and database.

Fabric client uses Hyperledger Fabric which, in contrast to other widely used distributed ledger or blockchain technologies, is an open-source business-grade permissioned DLT platform built for usage in corporate settings. Fabric offers a secured network. In a permissioned network, the resources exchanged are permissioned, meaning only authorized users may access them. While members may not entirely trust one another (they may be rivals in the same business, for example), a network may be run using a governance model based on mutual trust, such as a formal agreement or framework for managing disputes [27].

A communication interface with the InterPlanetary File System (IPFS) is used to upload or download data from the IPFS network. The Auth module is used to verify a user's identity, enabling only genuine users to connect with the platform and communicate with other users. A membership module is a software component designed to provide an abstraction of the architecture of a membership service. All cryptographic techniques and protocols that are involved in issuing, verifying, and authenticating certificates are abstracted away. Peers utilize the certificates it provides to join the Hyperledger Fabric network. The platform's general operation will be handled by the Application Logic and Database module, which includes a local database as well.

In Fig. 6 we can see the detailed designed architecture.

2) Methodology Analysis: Every AYUSH patient will have a public and private key established upon registration. Patients' data are encrypted using their private key. It requires decryption using their private key. So, patient decrypts the private key and chooses which health data to disclose. Then the client decrypts the chosen data. To guarantee that only the necessary service provider gets the data, the decrypted data are encrypted again using the service provider's public key. The recipient may verify the file's integrity by recalculating the hash and comparing it to the original hash on the AYUSH blockchain network. They examine previous data after obtaining shared files from the service provider. Symptoms are posted to the blockchain after sufficient inspection. The patient's treatment records may be large, making it harder to store them on the blockchain and increasing calculation time. This may lower transaction rates. To circumvent this, the hefty records are encrypted with the patient's public key and saved on IPFS. The original field's hash is uploaded to the blockchain to verify the file's integrity if shared with another service provider. IPFS generates the hash of the encrypted file after uploading it. This helps IPFS identify files and prevents repeated uploads. The record has now been disseminated to all nodes in the network. The IPFS system now has trustworthy and immutable data. Only the patient possesses the matching private key pair, thus only he can decode the data. The new record is now part of the patient's personal health records. Similar steps may be used to distribute this data to others, if desired. To improve security, all encryption, decryption, and key creation are done at the client [26].

V. Blockchain & IoMT against COVID-19

Blockchain, when used with asymmetric cryptographic techniques and digital signatures, can safeguard IoMT. Decentralization of blockchain systems also reduces the possibility of single-point failures and malicious assaults. Blockchain can protect IoMT data privacy by using privacy-preserving technologies like homomorphic obfuscation and differential privacy. So blockchain is a great IoMT carrier. Thus, deep integration of blockchain and IoMT may improve IoMT systems [28].

A. Blockchain-Enabled IoMT

Blockchain and IoMT integration may solve security and privacy problems. We call this blockchain-enabled IoMT. Fig. 7 depicts a blockchain-enabled IoMT. This design has four layers: device, edge computing, blockchain network, and data analytics [28].

The device layer contains IoMT devices such as heat sensors, thermal cameras, wristband sensors, thermometers, and RFID tags. The intermediate layer integrates communication networks and edge computer services. Nodes at base stations, Wi-Fi APs, and IoT gateways may gather and preprocess IoMT data. The blockchain network layer also acts as a middleware to provide reliable resource management across the lower levels. The data analytics layer comprises cloud computing, data storage, and Artificial Intelligence (AI) and Machine Learning (ML) or Deep Learning (DL) algorithms. Notably, edge computing facilities and entities in the data analytics layer are all linked to nodes in the blockchain network layer. Thus, blockchain-enabled IoMT can effectively authenticate and regulate access both at the edge computing and blockchain network layers.

Features of this multi-layer architecture:

- *Providing layer abstraction*. The edge computing and blockchain network layers act as middleware, hiding the complexity of IoMT devices and communications. To

Open Science Index, Information and Communication Engineering Vol:17, No:2, 2023 publications.waset.org/10012975.pdf

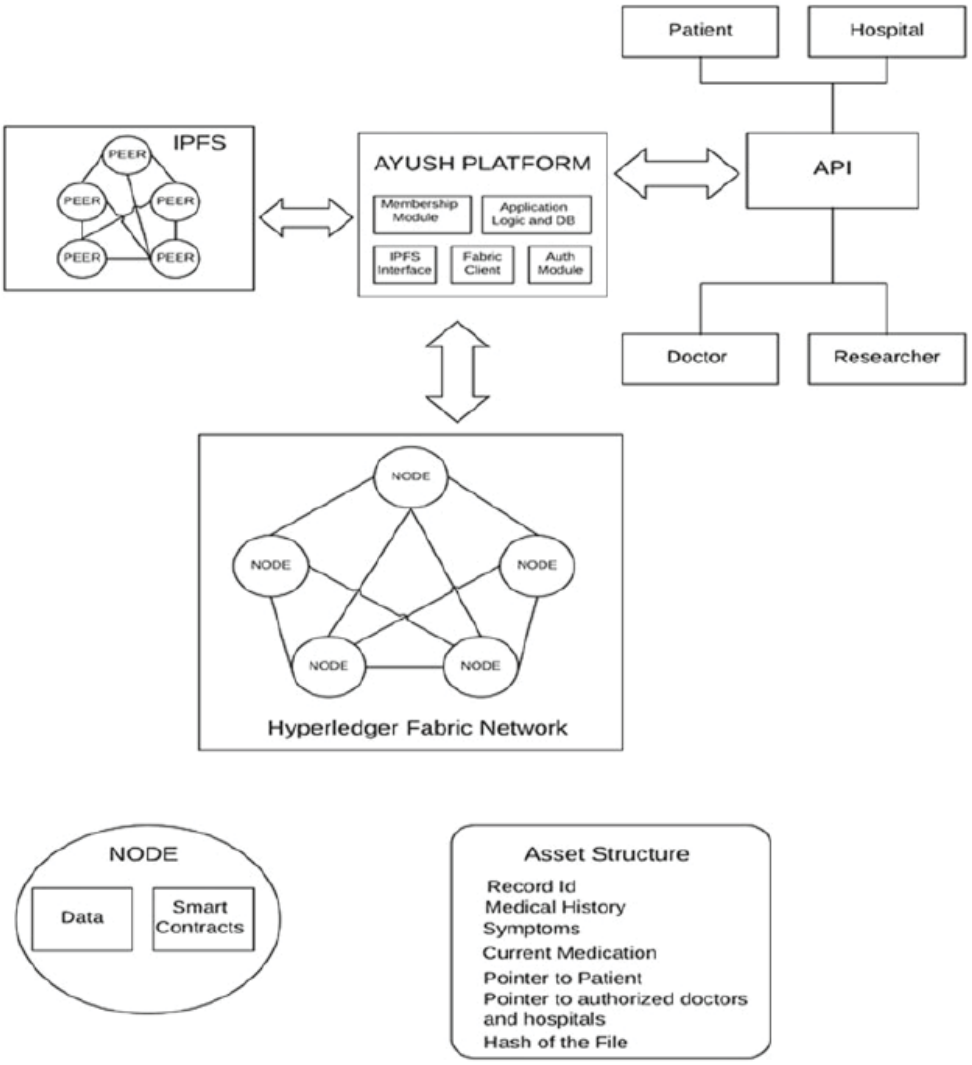

Fig. 6 AYUSH Architecture [26]

assist application development, the blockchain network layer may deliver blockchain-based services to other applications.

- *Improving IoMT system interoperability*. The blockchain network layer uses the built-in overlay peer-to-peer (P2P) network to link several IoMT subnetworks. The fragmented IoMT components are therefore merged to provide seamless services to other applications. Consequently, IoMT interoperability may be enhanced.

1) Analysis: IoMT has security and privacy issues. The followings examine the benefits of blockchain-enabled IoMT from different point of views [28].

1) *IoMT security upgrade*: It is possible to safeguard IoMT data using the built-in security features of the blockchain, such as asymmetric encryption/decryption techniques and digital signatures. A second way to improve security is to combine blockchain technology with additional security measures, such as authentication and access control. IoT devices may be made more secure by incorporating smart contracts into their firmware, which triggers the auto-upgrading programs to automatically update IoT devices' software. Decentralization of the blockchain may also reduce the likelihood of system failures due to single-point failures or other malicious attacks (e.g., DDoS attack), which improves system security and dependability.
2) *The protection of IoMT data privacy*: Using the blockchain to hide account addresses and encrypt transaction data may provide some level of privacy protection. There are various privacy-preserving strategies, such as homomorphic obfuscation and cryptographic algorithms, that are integrated into blockchain-enabled Internet of Medical Things (IoMT). Edge computing nodes at the edge computing layer may perform data gathering and processing operations in an approximation to consumers, as in Fig. 7. As a result, the sensitive IoMT data may be kept and processed locally before being sent to a distant cloud service.

Open Science Index, Information and Communication Engineering Vol:17, No:2, 2023 publications.waset.org/10012975.pdf

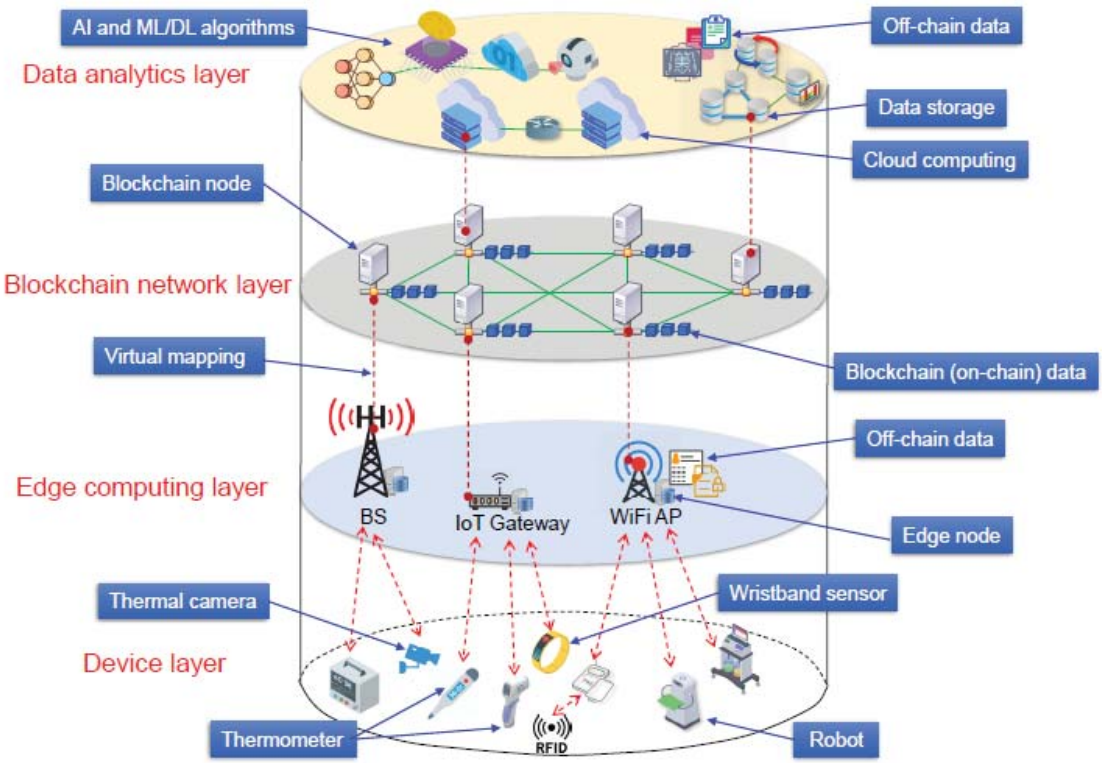

Fig. 7 Architecture of blockchain-enabled IoMT [28]

3) *IoMT dataset's traceability*: Blockchain-enabled IoMT may classify IoMT data into two types: "on-chain" and "off-chain," depending on whether the IoMT data are kept on the blockchain or not. On-chain data at blockchain may be tracked all the way back to its origin. The blockchain's decentralized consensus algorithms and asymmetric cryptographic techniques allow for on-chain data tracing and non-repudiation. IoMT data can be stored on blockchain, however this is impracticable due to the enormous amount of IoMT data, particularly for medical images and videos. The off-chain storage of IoMT data, such as images and videos, is preferable since it is more secure, while blockchain can only store metadata or hash values for the off-chain IoMT data. Off-chain IoMT data can be more easily tracked with the addition of digital signatures and access control methods to the blockchain-enabled IoMT. An off-chain IoMT dataset may be stored on the blockchain to maintain its traceability while reducing storage costs.

B. Contact Tracing & IoMT

COVID-19 has an average incubation time of 5.5 days from infection to symptoms, and many patients are asymptomatic. To stop the spread of COVID-19, it is critical to quickly identify all social contacts that occurred during the incubation phase. Contact tracing is used to track close connections. When someone is diagnosed with COVID-19, their close contacts should be notified and given guidelines. Several mobile contact tracking apps use Bluetooth Low Energy (BLE). Using BLE, one may record nearby calls between phones, wearables, and IoT devices. The main worry with this strategy is user data security and privacy. In a centralized cloud, people lose control of their data as it is kept and processed. Here, we annotate ideas from [29].

Blockchain can handle data security and privacy issues. With blockchain, users may keep complete control of their data instead of relying on a centralized database. Patients and users may create smart contracts to limit access to patient data. Pseudo-anonymity may also preserve patients' privacy. Instead of disclosing a patient's genuine identity, the blockchain-based system might assign them a unique digital fingerprint (public key or hash).

Sharing data across healthcare partners is critical in the COVID-19 pandemic. Global data sharing among foreign researchers may assist generate strong data sets that can benefit COVID-19 research. These data-sharing systems must comply with all national and international data-sharing laws. The most critical problem is patient privacy, which is preventing the widespread use of medical data exchange systems. National and international entities enforce Health Insurance Portability and Accountability Act (HIPAA) and create data access control regulations. Moreover, Internet of Medical Things (IoMT) devices may collect specific patient data such as blood oxygen

Open Science Index, Information and Communication Engineering Vol:17, No:2, 2023 publications.waset.org/10012975.pdf

levels, heart rates, and prescription dosages.

Blockchain's decentralized storage might substantially enhance healthcare data security and privacy. The absence of expensive middlemen in the form of centralized databases also gives patients and hospitals more control over their data. Also, blockchain may help break down conventional medical record barriers, allowing hospitals and doctors throughout the nation and perhaps globally to share data more easily. Real-time data exchange is possible with blockchain. Directly uploading IoMT data to a blockchain-based system eliminates data forgery and mutation. Transparency in data collection, storage, and sharing helps stakeholders trust one another while protecting patients' privacy.

1) Challenges & Solutions: Blockchain technology may greatly assist in the present epidemic. Nevertheless, several obstacles must be overcome to fully profit from blockchain technology. This section will outline the issues and potential remedies.

- Compliance to Privacy Laws: Each organization's core position or entity is accountable for general smooth operation and legal difficulties. However, given blockchain provides for decentralization, anonymity, and automation, the problem is defining: Who owns what in terms of legal responsibility [30]? Which jurisdiction will apply in the event of a legal dispute, notably touching public blockchain infrastructure? Who is responsible if a smart contract is revealed to be incorrect? For blockchain-based creative services and use cases to flourish, courts and legal systems must create a new legal framework and administrative procedures. Efforts like this would facilitate the adoption of blockchain technology by governments. Blockchain technology augments and improves current public services, not replaces them.
- Throughput, Scalability, and Voluminous Data Management: Latency is the time it takes for the blockchain infrastructure to confirm a transaction. Much of blockchain lag is due to block mining time. The delay observed varies depending on the blockchain and platform utilized. Currently, delay ranges from seconds to minutes. High latency reduces transaction throughput, causing scalability concerns. The difficult problems are: Can current methods do hundreds of transactions per second on blockchain? Will scalability compromise security? Researchers are working on revolutionary blockchain solutions like sharding [31] and layer-2 scalability [32]. Sharding allows a rapidly expanding blockchain network to be logically separated into units called shards. Each node may then be mapped to one or more shards, processing and storing transactions. Recently, a DAG technique was developed to boost transaction throughput [33]. In order to optimize latency, throughput, and scalability, designing application-specific consensus algorithms and hierarchical blockchain systems may improve the situation.
- Privacy: Blockchain stores data in a distributed manner, such that all nodes (miners) have access to the same database. This raises difficulties of confidentiality, control, and management of data [34], which may be personal data of users or trade secrets of a company. Depending on the blockchain (and the cryptography or encryption algorithms used), the methods for data processing, storage, and viewing may vary, resulting in varying degrees of security risks and non-compliance with privacy regulations. So, which blockchain should be utilized for whatever application domain? Then, which privacy rules apply if the mining nodes are global? Is it determined by the miner who mined the new block? So, should privacy rules be part of blockchain operations to govern where mining occurs? Private data should be held off-chain to make blockchain technology viable for organizations/companies who are wary of its adoption. While centralized off-chain storage is possible, distributed off-chain storage ensures data availability and privacy. Another level/layer of security may be used based on the application context to ensure off-chain storage privacy. These include Privacy Enhancing Technologies (PETs) including homomorphic encryption, attribute-based encryption, zero-knowledge proof, non-interactive zero-knowledge proof, format-preserving encryption, secure multi-party computing and obfuscation.
- Security: Blockchain is a secure mix of P2P networking, distributed ledger, consensus mechanism, and cryptographic algorithms. However, blockchain applications may be attacked through wallet hijacking, crypto-stealing malware, and transaction likability. These attacks seek to change transaction data at the entry point such that rogue transactions are immutably verified on the blockchain [30]. So, is blockchain technology safe and fit for the future? How can current data be moved if blockchain design concepts need to be reinvented? Better encryption mechanisms will be developed. For example, homomorphic signatures outperform public-key certificates [35]. A hybrid blockchain system may justify varying levels of security, although caution is advised at intersections. Using a Trusted Execution Environment (TEE) with game-based smart contracts may increase the security of smart contracts.
- Resource Utilization: The fundamental transaction validation method incentivizes mining and distributed storage, making blockchain technology (hyper) resource-intensive. The reward for mining a new block has led to a worldwide network of mining farms using high-end application-specific computers. These mining farms use a lot of electricity, which has negative environmental implications. In this environment, how might a lighter, more energy-efficient blockchain be built? Lightweight cryptographic methods will be necessary to encourage and facilitate the adoption of blockchain technology. These algorithms must be safe, immune to quantum computing threats, and computationally cheap. With the advent of 5G enabled IoT applications, a new application-specific consensus technique is necessary.

Open Science Index, Information and Communication Engineering Vol:17, No:2, 2023 publications.waset.org/10012975.pdf

VI. Discussion & Future Work

Transparency and confidentiality are the first two challenges. Due to the fact that "everyone can see everything" on a blockchain network, increased openness and decreased secrecy, such as open disclosure of information during transfer, are commonly seen as blockchain limitations. Because patient-related data are very sensitive, this problem is essential for biomedical/health-care applications [9].

Speed and scalability are the next two problems. Depending on the protocol, blockchain transaction times might be long, and this speed limitation may limit the scalability of blockchain-based systems. When developing real-time and scalable blockchain-based health care/biomedical apps, this problem is critical [9].

In order to meet the scalability, accessibility and security in healthcare data sharing, [8] proposed a blockchain-based solution alongside the cryptographic algorithms to provide integrity, security, privacy, and portability of user-owned data. They also claimed that their system is unique because of its fully containerized architecture, making it deployable across multiple hospital IT infrastructures. Their proposed system is built as a platform with a distributed microservice architecture that can scale up or down depending on deployment needs.

Many nations' primary aim is to stop COVID-19 transmission from spreading in the future. As a result, contact tracing is receiving a lot of attention these days. In the battle against infectious illnesses, contact tracking is a critical pillar. COVID-19 tracking also comprises monitoring or surveillance to identify early outbreaks, safeguard the public, and effectively manage testing resources [23]. Other challenges may include:

- Test resources must be improved
- Scalability issues in terms of the total number of active cases
- Challenging manual contact tracing since its effectiveness is dependent on an individual's capacity to remember encounters when infectious, even before feeling unwell.
- Contact tracking and quarantine regulations are not 100 percent effective, which disadvantages people in low-resource areas.

A. Polkadot - Next Blockchain Generation

Currently, available Blockchains are still insufficient to satisfy extensibility and scalability. Dr. Wood and his partners introduce an architecture, which basically separates the canonical and validity aspects of the consensus architecture. They claim that this heterogeneous network enables different kind of consensus systems to cooperate in a fully decentralized environment, allowing open and closed networks to have access to each other without trust issues. In this section, we entirely discuss works from [36].

There are five key questions against present technology:

1) Scalability: Under peak conditions, how many transactions can be performed based on resources, bandwidth, and storage usage? How scalable the system is?
2) Isolability: Is it possible to address the various needs of multiple parties as optimal as possible under the same framework?
3) Developability: Do everything work fine? Can the APIs address the developers' needs properly? Are there any educational materials provided?
4) Governance: In order to bring an effective leadership of such a decentralized system, can the network be flexible over time? Is the decision-making process going to be legitimate and transparent?
5) Applicability: Do we require another middleware to cover the gap to real applications? Does the technology able to address essential needs itself?

The number of transactions processed per second is very low in the current real-world blockchain networks. This limitation is due to existence of a synchronous consensus mechanisms. The underlying consensus mechanism should both determine which transaction to be executed and which of the chains are valid among the numerous possible valid ones. These two mechanisms are called "state transaction mechanism" and "canonicalization" [36].

Polkadot itself is not designed for providing application functionality. It provides a so-called *"relay-chain"* through which numerous valid dynamic data structures can be hosted simultaneously. These data structures are called *"parachains"* without any special need to be blockchain in nature. Polkadot provides a simple infrastructure, letting middlewares to address much of the complexity [36].

As we have understood so far, the two major obstacles facing blockchain implementation across many healthcare systems are scalability and privacy. We propose that Polkadot platform seems to be very efficient and suitable to be employed in addressing those challenges. By using Polkadot as the backbone of a healthcare data sharing system, we may achieve a lot more scalable system and much more privacy-preserving possibilities thanks to its consensus process.

Polkadot can also assist us manage global vaccine distribution, which is unquestionably vital to restrict the spread of a virus and prevent further mutation, which may lead to fewer deaths. It is obvious that a rapid and equitable vaccination rollout over the world improves both the economy and people's mental health. Future Polkadot-based data-sharing services will be able to trace emotional well-being as well. As each pandemic fades, the psychological effects may last longer in a wider range of individuals.

Additionally, combination of the Community Detection algorithms with Polkadot enables the tracking and tracing of cases without minding the privacy and scalability. Positive cases, together with their associated data on the blockchain, may provide a data set for community detection algorithms to use to identify and inform people who may have been exposed to the virus.

VII. Conclusion

Although the use of blockchain in medical applications is not without challenges, we are sure of significant benefits from this technology. The current challenges, such as scalability,

Open Science Index, Information and Communication Engineering Vol:17, No:2, 2023 publications.waset.org/10012975.pdf

privacy, security, and speed, will be resolved and blockchain technology will serve as the cornerstone and platform for future medical advancements. According to the frameworks described earlier, several COVID-19 issues may be addressed with the use of blockchain functionality [37].

In this paper, we have reviewed primary studies prior to the COVID-19 pandemic, aiming for secure data sharing between different parties. Those scholarly works tended to answer whether it is feasible to deploy a blockchain-based system for recording health data on a large scale with proper privacy. Also, the role of blockchain in managing pandemics has been described in seven categories, particularly the COVID-19. Within a year after COVID-19 has been diagnosed and announced as a pandemic, different prototypes and architectures have been proposed. They tried to address the most critical challenges every community faced to control the spread of the virus, namely social distancing and contact tracing. At the final stages of our review, we elaborated the relation between Blockchain and Internet of Medical Things (IoMT). We also discussed some possible solutions for the current blockchain systems in healthcare, mainly based on Polkadot.

REFERENCES

[1] "Coronavirus disease (COVID-19) EURO." [Online]. Available: https://www.who.int/europe/health-topics/coronavirus

[2] WHO. (2021) "Coronavirus Disease (COVID-19) – World Health Organization". [Online]. Available: https://www.who.int/emergencies/diseases/novel-coronavirus-2019

[3] ——. (2021) WHO Coronavirus (COVID-19) Dashboard. [Online]. Available: https://covid19.who.int

[4] M. Swan, *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[6] 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*, 2020.

[7] A. Khatoon, "Use of blockchain technology to curb Novel Coronavirus Disease (COVID-19) transmission," *Available at SSRN 3584226*, 2020.

[8] M. A. Cyran, "Blockchain as a Foundation for Sharing Healthcare Data," *Blockchain in Healthcare Today*, Mar. 2018.

[9] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017.

[10] Y. Alabdulkarim, A. Alameer, M. Almukaynizi, and A. Almaslukh, "Spin: A blockchain-based framework for sharing covid-19 pandemic information across nations," *Applied Sciences*, vol. 11, no. 18, p. 8767, 2021.

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

[12] L. Fang, G. Karakiulakis, and M. Roth, "Are patients with hypertension and diabetes mellitus at increased risk for covid-19 infection?" *The lancet respiratory medicine*, vol. 8, no. 4, 2020.

[13] S. H. Wong, R. N. Lui, and J. J. Sung, "Covid-19 and the digestive system," *Journal of gastroenterology and hepatology*, vol. 35, no. 5, pp. 744–748, 2020.

[14] R. Baldwin and E. Tomiura, "Thinking ahead about the trade impact of covid-19," *Economics in the Time of COVID-19*, vol. 59, 2020.

[15] E. Team, "The epidemiological characteristics of an outbreak of 2019 novel coronavirus diseases (covid-19)—china, 2020," *China CDC weekly*, vol. 2, no. 8, p. 113, 2020.

[16] H. Chen, J. Guo, C. Wang, F. Luo, X. Yu, W. Zhang, J. Li, D. Zhao, D. Xu, Q. Gong *et al.*, "Clinical characteristics and intrauterine vertical transmission potential of covid-19 infection in nine pregnant women: a retrospective review of medical records," *The lancet*, vol. 395, no. 10226, pp. 809–815, 2020.

[17] D. Wang, B. Hu, C. Hu, F. Zhu, X. Liu, J. Zhang, B. Wang, H. Xiang, Z. Cheng, Y. Xiong *et al.*, "Clinical characteristics of 138 hospitalized patients with 2019 novel coronavirus–infected pneumonia in wuhan, china," *Jama*, vol. 323, no. 11, pp. 1061–1069, 2020.

[18] 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. 90 253–90 256, 2020.

[19] 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.

[20] Apple, "Privacy-preserving contact tracing - apple and google," 2020. [Online]. Available: https://www.apple.com/covid19/contacttracing

[21] I. Levy, "The security behind the nhs contact tracing app," *National Cyber Security Centre*, 2020.

[22] P. Mozur, R. Zhong, and A. Krolik, "In coronavirus fight, china gives citizens a color code, with red flags," *The New York Times*, vol. 1, 2020.

[23] S. M. Idrees, M. Nowostawski, and R. Jameel, "Blockchain-based digital contact tracing apps for COVID-19 pandemic management: Issues, challenges, solutions, and future directions," *JMIR Medical Informatics*, vol. 9, no. 2, p. e25245, 2021.

[24] P. Durneva, K. Cousins, and M. Chen, "The current state of research, challenges, and future research directions of blockchain technology in patient care: Systematic review," *Journal of medical Internet research*, vol. 22, no. 7, 2020.

[25] 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.

[26] A. V. Aswin, K. Y. Basil, V. P. Viswan, B. Reji, and B. Kuriakose, "Design of AYUSH: A Blockchain-Based Health Record Management System," in *Inventive Communication and Computational Technologies*, G. Ranganathan, J. Chen, and A. Rocha, Eds. Springer Singapore, Jan. 2020, pp. 665–672.

[27] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the thirteenth EuroSys conference*, 2018, pp. 1–15.

[28] H.-N. Dai, M. Imran, and N. Haider, "Blockchain-enabled Internet of Medical Things to Combat COVID-19," *IEEE Internet of Things Magazine*, vol. 3, no. 3, pp. 52–57, 2020.

[29] 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.

[30] J. Salmon and G. Myers, "Blockchain and associated legal issues for emerging markets," 2019.

[31] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu, "Survey: Sharding in blockchains," *IEEE Access*, vol. 8, pp. 14 155–14 181, 2020.

[32] M. Jourenko, K. Kurazumi, M. Larangeira, and K. Tanaka, "Sok: A taxonomy for layer-2 scalability related protocols for cryptocurrencies." *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 352, 2019.

[33] I. Kotilevets, I. Ivanova, I. Romanov, S. Magomedov, V. Nikonov, and S. Pavelev, "Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions," *IFAC-PapersOnLine*, vol. 51, no. 30, pp. 693–696, 2018.

[34] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164 908–164 940, 2019.

[35] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An id-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, pp. 20 632–20 640, 2018.

[36] G. Wood, "Polkadot: Vision For A Heterogeneous Multi-Chain Framework," *White Paper*, vol. 21, 2016.

[37] M. R. Hasan, S. Deng, N. Sultana, and Z. H. Muhammed, "The applicability of blockchain technology in healthcare contexts to contain covid-19 challenges," *Library Hi Tech*, vol. 39, no. 3, pp. 814–833, 2021.