High-Level Design and Rapid Implementation of a Clinical and Non-clinical Blockchain-Based Data Sharing Platform for COVID-19 Containment

Sohag Saleh[1]* and Farabi Shayor[2]*

[1] Faculty of Medicine, Imperial College London, London, United Kingdom, [2] Research Intelligence Systems (IntelXSys), London, United Kingdom

As the world has moved toward rigorous containment measures due to the spread of a novel coronavirus, it is crucial to push the boundaries of clinical data obtaining methods using real-time capturing facilities. During this time of crisis, data-centric technologies that could provide authenticity and immediate access to patient data are essential. A blockchain-based digital health protocol for access to real-time data with user-centric data protection measures can achieve these aims. Immediate and secure access to biomedical data can provide credible insights and also help in discovering intelligence to expediate the development of effective therapeutics. It also aids in altering policies for restrictions by extracting key insights required for modeling studies. This paper delivers a high-level design of a blockchain-based clinical research data collection and health service intervention platform, where the users can exercise control of data. This application also provides a platform to deliver technology-based interventions which would assist in streamlining aid for vulnerable users to prevent the NHS from being overwhelmed. Further steps are also recommended to achieve a data compliant solution for rapid deployment, based on available resources, allowing a collaborative effort, which is extremely necessary at times of such crisis.

Keywords: COVID-19, pandemic, public health, communication, technology-based intervention, digital health solutions

INTRODUCTION

A cluster of pneumonia cases was first reported in the Wuhan district of China (Shi et al., 2020), where it was revealed that the biological samples were similar to the Severe Acute Respiratory Syndrome (SARs) and Middle East Respiratory Syndrome (MERs). Subsequent whole-genome sequencing identified the novel human virus SARS-CoV-2, which caused the disease named *COVID-19* (Peeri et al., 2020). SARS-CoV-2 is an *RNA betacoronavirus* (Zhu et al., 2020), and although the pathological features are similar to SARS (Xu et al., 2020), it is distinctive in terms of the overall characteristics. At the beginning, in the first epicenter, China had a case fatality rate (CFR) of 18% (Dorigatti et al., 2020), but later, as the epicenter shifted to Italy and then to the United States, the CFR was revised to around 2% (Mahase, 2020).

SARS-CoV-2 is deemed to have a median incubation period of 14 days (Wang et al., 2020), during which a patient may or may not display signs or symptoms of the infection (Day, 2020). These include fever, dry cough (Wu et al., 2020) and lymphocytopenia (Bai et al., 2020; Guan et al., 2020). Patterns of illness include infection in the upper respiratory tract, non-compromising pneumonia and acute pneumonia with fast relapse of the respiratory functions (Heymann and Shindo, 2020). A large constellation of patients presenting with pneumonia required invasive respiratory ventilation and critical care support (Paules et al., 2020). CT imaging revealed that several patients suffered from ground-glass opacities leading to a number of deaths (Chung et al., 2020; Huang et al., 2020; Lei et al., 2020), while some COVID-19 patients have died due to both myocardial and respiratory failure (Ruan et al., 2020). Pre-existing comorbidities that influence outcome include cardiovascular disease, diabetes, chronic respiratory disease and cancer (Chen et al., 2020; Jung et al., 2020; Ong et al., 2020).

The extended incubation period relative to influenza H1N1, and the asymptomatic presentation highlights the importance of contact tracing and case isolation (Hu et al., 2020), as carriers may contribute to the continuity, without realization (Al-Tawfiq, 2020). Moreover, a lack of scientifically grounded information amongst the sheer volume of social media misinformation had led to both public apathy and societal panic, causing difficulties in disease management strategies.

With millions already infected, surveillance testing and contact tracing are critical during this stage. Supervision on a national scale could only be achieved by accumulating crowdsourced data. The same platform could be utilized to operationalise healthcare services to the users in self-isolation. For this analysis, "CO-App DHS" is explored, a platform to deploy blockchain technology to share clinical and non-clinical data for infectious disease control (**Figure 1**).

IMPORTANCE OF A DIGITAL PLATFORM

The impact of COVID-19 was underestimated, which has led to a significant number of casualties and almost complete lockdown across the globe. The pandemic has spread so rapidly that it is becoming harder to contain and many countries have no exit-strategies from the lock-down (Oxford Analytica, 2020). There was lack of similar real-time data during the H1N1 pandemic, ipso facto, the health officials faced numerous barriers.

"The combination of incomplete surveillance data and socially-narrow simulation methods threatens to limit the ability of national public health agencies to provide policy-makers and the general

FIGURE 1 | CO-App Digital Health Solution (DHS), a private-permissioned blockchain application powered by the Ethereum protocol.

public with critical and timely information required during an outbreak of pandemic influenza." (Ekberg et al., 2009)

European countries have struggled due to a lack of surveillance infrastructure and preparation. Besides, controlling the spread of misinformation is a tough challenge during times of crisis (Rajdev and Lee, 2015). The remarkable speed of information scattered on the internet and the propagation of fake news created a challenge for public health officials (Wong et al., 2020). Such propagation of unreliable sources of information poses a considerable challenge for the officials as accurate and clear communication is as crucial now as ever. The multifaceted interconnected web cannot be controlled, and this requires alternative processes to stem the velocity and establish direct connection with the public.

Before this pandemic, minimal effort was made by policymakers toward the development of any digital solutions for outbreak containment. Operating a clinical research programme for the development of therapeutics requires access to user-permitted biomedical data. If provided by the government, users could run home-tests and share the results with the health services to assist in developing vaccines. Therefore, all aspects of combating the virus, including the use of technology must be explored. Emerging technologies can deliver better outputs for infectious disease modeling and prevention (Christaki, 2015).

Abbreviations: ACE2, Angiotensin-Converting Enzyme 2; API, Application Programming Interface; ASIC, Application Specific Integrated Circuit; CCU, Critical Care User; CFR, Case Fatality Rate; CMS, Content Management System; DHS, Digital Health Service; DNN, Deep Neural Network; DPA, Data Protection Act; EVD, Ebola Virus Disease; JSON, JavaScript Object Notion; MERS, Middle East Respiratory Syndrome; MLA, Machine Learning Algorithm; NHS, National Health Service; REST, Representational State Transfer; RPC, Remote Procedure Call; SARS, Severe Acute Respiratory Syndrome.
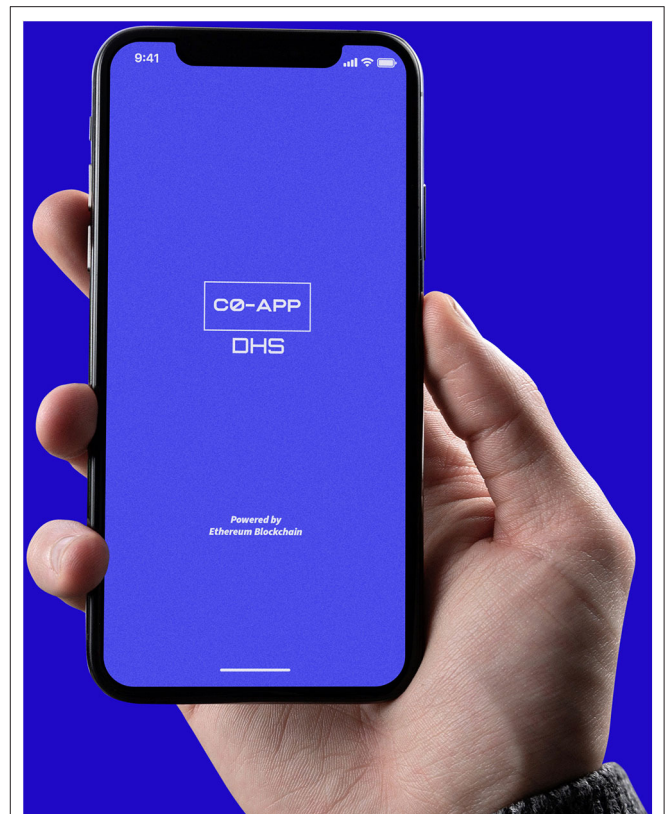
Artificial intelligence (AI) and blockchain could aid in increasing the accuracy of disease modeling, given that access to real-time data sharing processes are established.

By the end of the twentieth century, technological innovation has had a profoundly positive impact on preventing infectious diseases by improving the clinical processes, such as intensive care, and surgical interventions (Breiman, 1996). In the past decade, the emergence of CRISPR technology and its application is aiding in the diagnosis of infectious diseases (Gootenberg et al., 2017; Chiu, 2018). However, no single technology could singlehandedly solve all the problems. Data analytics using blockchain and AI could act as a positive catalyst and help reduce the basic reproduction number (R_0). It could also aid efforts to minimize barriers to communication and increase international collaboration. Rapid data sharing is significant at times of such global crisis for emergency public health action (Gates, 2020; Moorthy et al., 2020). Hence, the aim for this analysis is to focus on three key goals: implement technology-based healthcare intervention by following the *purpose limitation principle*, gain insight into predictive models for appropriate policymaking, and discover potential cases for contact tracing.

Technology for Crisis Management and the Gaps

Disease Preparedness

Several studies have championed the utilization of advanced technology for disaster preparedness. Before the widespread adoption of blockchain, it was demonstrated that wireless network using a peer-to-peer architecture could provide a promising solution for non-clinical disaster prevention response, including tracking of victims, data retrieval and incident management (Arnold et al., 2004). It has also been demonstrated that community-based disaster management by implementing a *community resource-database* can strengthen collaborative efforts among organizations mobilizing during a crisis (Troy et al., 2008). Use of information communication technology (ICT) can improve disaster response (Harrison et al., 2008) and community-based application to cooperate and gather crowdsourced data could aid in preparedness for disaster management (Quinto and Lim, 2016; Ernst et al., 2017).

Previous studies have also exhibited the effectiveness of using ICT for emergency disaster response to share community-related information (Shklovski et al., 2008). During the Ebola Virus Disease (EVD) outbreak, mathematical modeling was used to develop strategies (Pandey et al., 2014), which demanded surveillance data and crowdsourced information. Although there have been repeated calls for better surveillance systems, these have been overlooked. EVD has resulted in a major learning experience with regards to understanding the necessity of an improved real-time surveillance response (Tambo et al., 2014). Substantial focus is needed in technological infrastructure for better surveillance, a major barrier that has been lifted by the presence of faster communications devices, distributing real-time data even in resource-scare countries (Woolhouse et al., 2015).

"There is an urgent need to develop and implement an active early warning alert and surveillance response system for outbreak response and control of emerging infectious diseases." (Tambo et al., 2014)

Nevertheless, the impact of information technology for crisis preparedness during a pandemic has not been comprehensively explored. One of the possible reasons could be the timing of the previous pandemic, H1N1 influenza. At that point in time, the world of ICT was not ready for it to be utilized to counteract the pandemic. Fortunately, technology has swiftly progressed since then. Besides, other outbreaks such as the EVD mostly affected the West-African countries. COVID-19 has led to the disruption on an unprecedented scale, prompting a concerted international response and a requirement to explore new methods.

The World Health Organisation (2020), have repeatedly suggested testing and contact tracing for COVID-19. However, due to the speedily increasing number of cases in countries such as the UK and the US, it is practically impossible to trace the path without access to live data. The reported number of cases all over the world is presently demonstrated using a map-based tracker by John Hopkins University (Dong et al., 2020), which validates the severity and devastation caused by the SARS-CoV-2.

Patient Testing and Tracking

Accurate projections based on mathematical modeling depends on the quality of data. To improve management, administration and communication during a crisis, new technologies can reduce the burden of managing information and facilitate faster data reporting (Garshnek and Burkle, 1999). The United Kingdom's National Health Service (NHS) have health records stored within a secured network. However, crowdsourced data such as consolidated results from the antibody tests, as well as data from potential patients is required to implement contact tracing. Further, having a significant number of users on one platform would allow devising heatmaps, therefore generating explanations faster. Biomedical data is the key to conduct effective research, but typical methods are not adequate to process such vast amounts of data (Jatmiko et al., 2016). With the world under lockdown, big data analytics is only achievable through a digital platform. The application requires connecting hospitals, clinicians, researchers and health service providers to share data. Pirtle and Ehrenfeld (2018) recommend that aggregated health reporting to a Content Management System (CMS) is one of the attainable prospects of blockchain technology.

Purpose Limitation

One of the larger goals of the central governments should be aggregating disruptive technologies to provide control of data to the users and substantiate that the data usage has a clearly defined purpose. Crowdsourced data, a great source of healthcare intelligence, can be made user-centric using blockchain (Yue et al., 2016), and provide an extra layer of security to protect the data (Magyar, 2017). Such system design would influence response-planning and decision-making. It enables a multiplicity of rarely obtainable information, transferring the burden of supervision to the machine learning algorithm (MLA). Blockchain also enables sustainable supply-chain management

(Saberi et al., 2018), which could be utilized to oversee COVID-19 test. Some developments are already in progress, such as the "COVID-19 tracker app," where the users can report their symptoms daily (Spector, 2020). The NHS has also deployed a track and trace application called the "NHS COVID-19."

Scientific Communication

Transparent risk communication is very challenging and essential to ensure that the public instills trust in the information. Trust and widespread misinformation play a vital role in the outbreak of viral disease (Vinck et al., 2019). A mobile application could be a utilized as a platform for scientific communication to the public by distributing information with regards to the understanding of viral pathogenesis in a simple manner. Besides, transparently outlining the prognosis would ensure that the public is reporting to their respective health services when similar symptoms develop.

Health Services Intervention

Another factor limiting the crisis response is the lack of a confidential platform for receiving healthcare services. Previous research from the EVD outbreak extrapolated that response efforts need to address psychological needs (Bortel et al., 2016). Self-isolation is detrimental to the economy; however, it is also damaging to mental health; therefore, assessment and support needs are crucial as a part of the health response (Armitage and Nellums, 2020; Xiang et al., 2020). To minimize public frustration, and safeguard clinical operations support for the self-isolating and elderly, it is essential to launch a unified platform.

A Review of Blockchain and Its Use Cases

Blockchain is a type of *distributed ledger technology* that allows storage and archiving of data across multiple nodes without the need for a third-party (Zheng et al., 2017). There are no central failure points as it is operated using a peer-to-peer network model. Each *node* solves a computational algorithm to verify the integrity of the data and eventually, it is compiled and stored in a block. The core functionality of blockchain is the consensus algorithm, which allows blockchain to securely distribute and verify data stored across multiple nodes. The *Nakamoto Consensus* is a classic algorithm where the log is replicated across the state machine. The *miners* solve a cryptographic puzzle to operate the *mining node*, verify the data integrity and are required to produce a *proof* of work in a computationally intensive manner. Two major functions are performed by the consensus—the process of transaction validation to be included in the new block, and process of validating a Boolean judgement on whether or not a block has structural properties to be added to the chain. In a typical scenario, a node operator of a public blockchain, such as the bitcoin protocol, receives incentives for providing computational power to the network. The node operators of bitcoin can self-authenticate and become "miners" by providing computational capacity to process transactions, provided that they have capital to purchase sufficient Application Specific Integrated Circuit (ASIC) miners.

Blockchain can also be private and permissioned, where the responsibility of a node operator can be offered to a consortium (Sanjana et al., 2018). In a private blockchain, node operators are authorized by the consortium, hence they are not able to self-authenticate. Due to tighter control on pseudonymity and data sensitivity, the miners are not able to go through self-verification, as the consortium holds the provision of authorizing the control of information they have access to. Therefore, private-permissioned blockchain adopts variations of the Byzantine Fault-Tolerance consensus to operate protocol with one or more nodes, using a leader-peer hierarchy for proposing new blocks. For instance, Hyperledger Fabric, a modular permissioned blockchain developed by the Linux Foundation uses Practical Byzantine-Fault Tolerance (PBFT). The potential and uses cases of blockchain have been explored in various industries (Chen et al., 2018; Hughes et al., 2019; Mackey et al., 2019). Blockchain is also gaining substantial notice for its characteristics that fit with clinical and non-clinical research-based use cases (Agbo et al., 2019).

Unlike a computationally intensive protocol such as bitcoin, a private-permissioned blockchain can be developed without a large number of operators and heavy electricity usage. Permissioned blockchain has several use cases, including confidential data and rights management (Pănescu and Manta, 2018). Blockchain-based applications are being probed for automated certification and authenticity generation (BouSaba and Anderson, 2019; Gresch et al., 2019), and digital libraries (Hoy, 2017). Studies have also expanded on blockchain to cope with the demand for health care services and manage health care workers (Mackey et al., 2020). Estonia has adopted the blockchain to safeguard patient "electronic health records" (Heston, 2017; Einaste, 2018).

Blockchain-based applications are widely known as *Decentralized Application* or DApp, that uses smart contracts for operational management (Bogner et al., 2016). These applications use a type of smart-contract known as "Application Layer Contract" (ALC) (**Figure 2**). Ethereum is a popular blockchain protocol to develop such smart contracts and DApps (Antonopoulos and Wood, 2019). The significance of blockchain applications for storage, security, backup and efficient management of biomedical data, including ways to expand operational capacity in the supply chain, has been emphasized in wide-ranging studies (Pilkington, 2017; Clauson et al., 2018; Pirtle and Ehrenfeld, 2018; Dimitrov, 2019; Johnson et al., 2019). Blockchain-based management framework has also been presented to establish trust among various service providers in disaster management (Samir et al., 2019).

Addressing Key Requirements
Collection of Large Data Samples

Although not fully decentralized by definition, private-permission blockchain are compatible with private and public sector platforms due to the way authentication and authorization are handled. Research suggests that both commercial and public sector could benefit from the systematic implementation of private, permissioned blockchain (Carson et al., 2018). Blockchain has several use cases for the public sector and
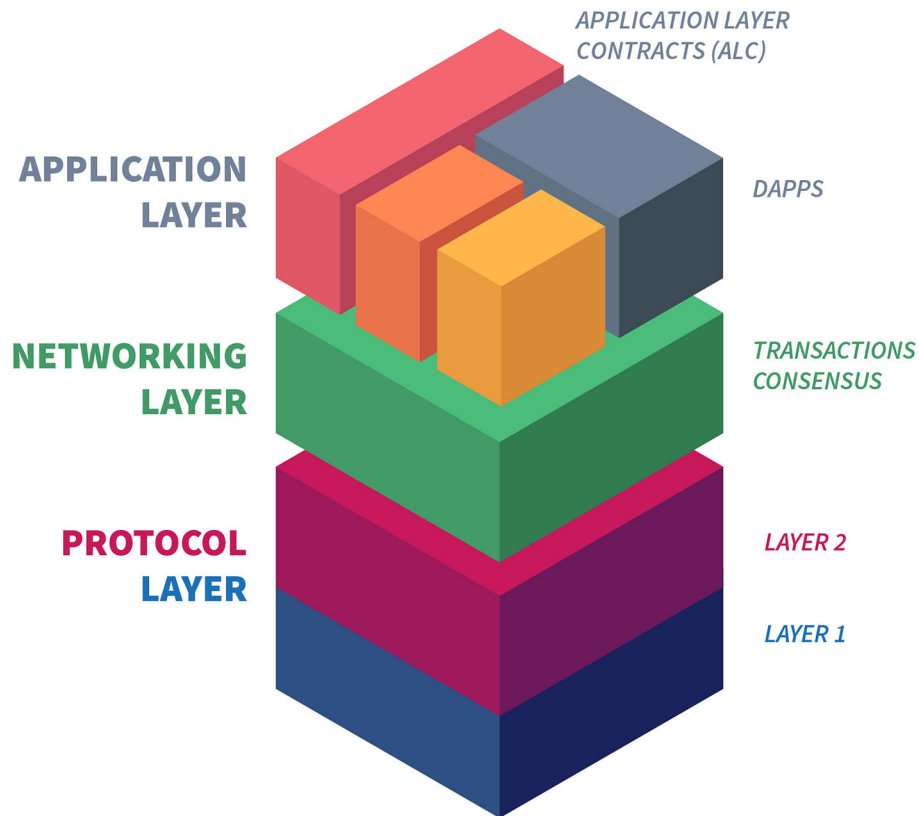
FIGURE 2 | Blockchain technology stack.

that the governments could benefit from the potential of the technology (Ølnes et al., 2017; Alketbi et al., 2018). One such requirement is collection of vast amounts of data—as it is crucial to calibrate national response, more studies by the integration of data types are needed (Lipsitch et al., 2020). To collect such data, users can volunteer so that the scientists can retrieve data on reported symptoms, collect and compare them with underlying conditions to project the probability of a user being affected by the COVID-19. The users are also provided with privacy terms that strictly follows the principles of purpose limitation.

Using AI to Detect COVID-19 Case Accuracy

The existing application use a two-step process and three simple parameters to check symptom and instruct a user to self-isolate. For instance, if users select "fever," they are likely to be asked to self-isolate, rendering the true symptomatic

user data to become inaccurate. However, having a high-temperature does not necessarily mean that the affected user is a COVID-19 suspect. In this aspect, a machine-learning algorithm can automatically synthesize user clusters to distinguish potential COVID-19 cases (see Neural Network for CO-App). Such data is also vital for extrapolating the correct value of R_0.

Robust Audit Trail

Current COVID-19 application collect data in a centralized database; therefore, transactional data can be manipulated. Blockchain can be utilized for a robust data audit trail and solve this problem. Preparedness and response methodologies could be improved using this decentralized data-centered infrastructure. The same methodology could also benefit the underdeveloped countries. Those healthcare systems are encountering substantial risks and could be incapacitated due to outdated models of preparedness (Gilbert et al., 2020).

Encouraging a Collaborative Ecosystem

Blockchain has the potential to reduce the fragmented processes in pharmaceutical industries and overcomes the pitfalls of enterprise resource planning (Saberi et al., 2018). CO-App can track and automate a multitude of processes, which could assist in early detection of COVID-19 by instantaneously sharing data among various class of users, such as companies undertaking vaccine development. It is a viable solution through a collaborative approach among universities, hospitals, and service providers. The aim is to establish the following framework: classify, authorize, collaborate, control, inform, mobilize, contain, and normalize.

Communicating With the Public

Public science communication is also vital during a crisis. The existing infrastructure does not push any NHS updates to the users. It only allows users to "Read Latest Advice," using which they are directed to an external website. The Co-App utilizes its user base and provides vital scientific information to disseminate knowledge.

THE PROPOSED PLATFORM FOR INFECTIOUS DISEASE CONTROL

This analysis explores an interdisciplinary approach toward addressing the gaps in scientific communication, increase crisis management efficiency, infection prevention and allow control procedures to be aggregated. The main purposes of the platform, "CO-App DHS" is bringing the users to one platform to deliver:

- End-to-end data sharing platform
- Empirically grounded research evidence in a straightforward manner
- Conceptual frameworks surrounding therapeutic development
- Expert opinions and critical support to self-isolating users, as well as the millions of elderlies who are in requirement of urgent critical support.

Features of CO-App
The Convergence of Disrupting Technology Paradigms

The aim of CO-App is not replacing the legacy enterprise systems, but to develop an application that would act as a supplementary support system for the national health service. The trust of immutability is handed over to the computational intelligence, which solves cryptographic puzzles to examine the validity. CO-App's private-permissioned protocol is the bridge between the blockchain and external resources to chronologically create a trail of evidence, forming a historical chain of events. Starting from the genesis block, the chain would continue to grow and update information as per issuance.

Extensive User Control of Data

The users can reclaim personal information using blockchain (see Usership Registration). Large corporations may use personal information outside the EU to other companies to monetise their platform. Using blockchain, users can enforce permission-control and own their information, such as COVID-19 tests or previous health records. It ensures auditability and verifiability.

Relatively Rapid Deployment

The analysis pertains to the implementation of an infrastructure within a very short period. Therefore, the enterprise-grade permissioned network does not require complete development from scratch; instead, it is built on the Ethereum mainchain for it to allow importing the standardized procedures. Additionally, it aids in benefitting from the updates and would not require additional maintenance. It also permits interoperability with other DApps as the protocol expands in the near future.

P2P Data

Co-App would be targeted toward a new group of users in need of support. Therefore, only the invited users by the NHS and key workers would be initially allowed for the pilot. They can request case data from specific users using a peer-to-peer connection. Data from test results can be securely acquired via one direct transaction from the user to the researcher. The approval of transfer is anchored to the blockchain network, which delivers a permanent proof of authenticity.

Protocol Design

The basic design of the platform follows the standardized protocols of the Ethereum Foundation (Antonopoulos and Wood, 2019). To demonstrate how blockchain could be utilized to deploy a platform for the NHS rapidly, this analysis proposes the development of a decentralized application on a private-permissioned protocol based on three foundations: security of user data, permissioned nodes and consensus that can support scaling. Compared to traditional blockchain networks, a private-permissioned network with off-chain storage and integration of artificial intelligence allows faster processing of vast amount of data in a relatively short period. The entire project can also be open-sourced.

Privacy

It is noteworthy that the application is not developed on a fully decentralized network. By theory, a fully decentralized solution such as the Bitcoin network is typically "public" and does not have any central control over the operations of the platform. The application is certainly decentralized in nature, and adheres to the control of information, privacy and self-sustaining automation necessitated by the blockchain technology's ethos. However, with regards to a fully public decentralized blockchain, the decisions of hard-fork or upgrades to the network are made by a consortium, therefore it is completely automated and self-sustained. However, such solutions cannot be implemented on a fully decentralized "public" network to tackle privacy concerns. The application collects a considerable amount of health reports and clinical data, which is enormously sensitive in nature, and therefore, required to be stored in an encrypted database with access for only a handful of administrative personnel and researchers requiring those data. Additionally, claims regarding data protection and compliance issues, such as deletion of certain data, and protection of users by monitoring user access cannot be restricted on a fully

decentralized blockchain. Furthermore, permissioned network allows data to be processed faster, and also provides a certain degree of control over data-protection mechanism to the PHE and NHS, which is critical to comply with GDPR and Data Protection Act.

Consensus Mechanism

Each blockchain is designed to follow a consensus using which data integrity is verified. CO-App is built on *Proof-of-Authority* (PoA), a reputation-based algorithm intended to scale private blockchain networks. It reduces time-lag for block execution and uses the "reputation" of a node operator. PoA follows a method where each consensus participant can delegate multiple nodes on their behalf. The network operates without the requirement of the transaction cost. Proof-of-Authority has been in existence for many years, and widely adopted for corporate use cases (Singh et al., 2019).

For the purpose of this paper, there are several benefits to the use of PoA. Firstly, by allowing operations to be distributed on a blockchain, it could reduce the cost of server operations. Secondly, it reduced the consumption of electricity as a node operator does not require expensive equipment to run a node, providing better efficacy. Thirdly, PoA offers increased security by lowering the risks of attack vectors relevant to the public blockchains. Finally, permissioned network allows a certain level of control required for handling biomedical data in a legally compliant manner.

Neural Network

A deep neural network (DNN) is a silicon-based artificial intelligence network consisting of an input layer, 1 or >1 hidden layer and one final output layer that presents the result, with each layer having multiple neurons or nodes (Wang, 2003). The nodes or "neurons," similar to the human brains, are capable of gradually learning from their interactions and deliver computational probability. DNNs have been proven effective in various healthcare-setting. Previous studies have demonstrated efficacy in potential cancer risk detection to identify high-risk population (Hart et al., 2019). Neural networks have been successfully utilized for modeling sentences, image classification), and medical-image categorization (Sharma et al., 2017; Eghbali and Hajihosseini, 2019). DNN constructed using a *multi-class algorithm* successfully detected diseases from images as data input (Litjens et al., 2017). DNN models of multi-label classification have also been proposed for predicting chronic diseases from clinical datasets (Zhang et al., 2019). Co-App uses "K-means clustering model" and a "multi-class neural network," which has been detailed in section Neural Network for CO-App.

Blockchain Protocol Functionalities

The systems architecture of the blockchain protocol includes *Node Operators* (NodeOps), a *Server Load Balancer*, and an *Encrypted Data Vault* using industrial-grade SSD (**Figure 3**). Allowing storage of non-transactional data and secure health data in an Azure DB permit conformity across GDPR compliant regions, high throughput, and low latency in comparison to a fully distributed network. The system is accessible via public IP,

allowing internet users to join the network with permission. The application comprises the following layers:
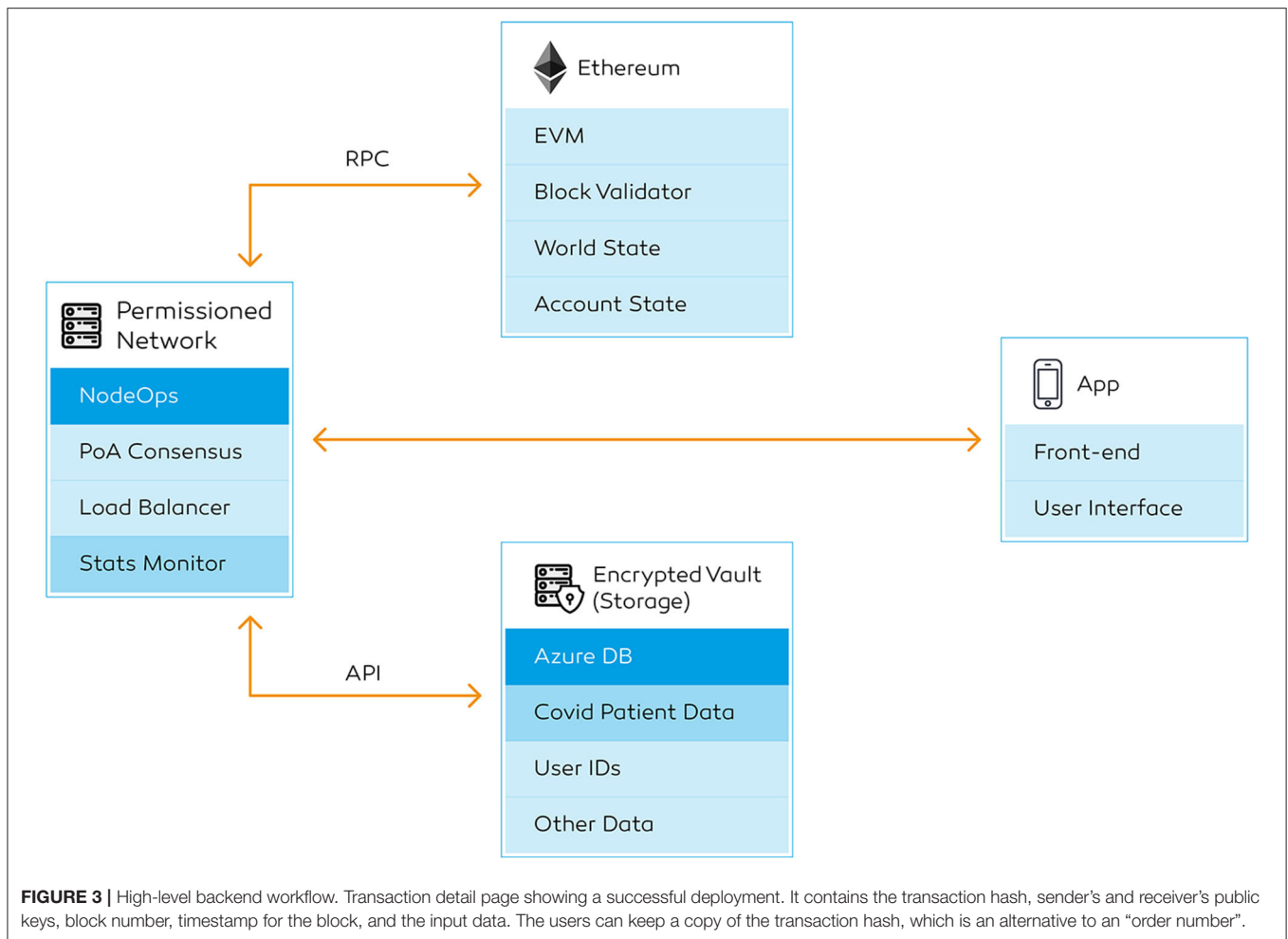
a. Protocol Layer

- Layer 1, the primary protocol, Ethereum Network
- Layer 2, with limited nodes, off-chain storage and computation, and identity store.

b. Networking Layer

- HTTP JSON RPC for connection with the layer 1 protocol
- Transaction manager coordinating and connecting peers within the network.

c. Application layer

- The front-end interface interacting with the contracts
- Smart contract generation interface.

Ethereum protocol and Microsoft delivers a fully-integrated solution to build on the blockchain, therefore these backend functionalities are readily available. A stats explorer is built for monitoring all the data being operated within the transaction layer, which can be observed by a front-end explorer. The nodes performance, as well as contract execution, can be monitored using the explorer. The private transaction manager is available to the service providers who are managing the administrative process. The users, on the other hand, do not require access to transaction manager—they will only have access to information that are relevant to them, for instance, transaction IDs of a particular service they request.

The network consists of the following six key components: secure hypertext transfer protocol (HTTPS) gateway, a public and private subnet, Ethereum JSON-RPC, transaction explorer, command-line interface for Geth and Azure DB (**Figure 3**). It is essential to concentrate on a turn-key solution due to the current velocity of the crisis. Cloud infrastructure providers such as Microsoft Azure with the integration blockchain deployment service deliver a turnkey solution (Wang et al., 2019), hence a faster deployment timeline. This information can be managed off-chain and verified using *secp256k1* (Ethereum, 2019) and *ECDSA* cryptography (**Annex Table 2**). These components are not required to be developed from scratch. Due to the nature of a private blockchain, the administrators can set the block height and difficulty. In contrast with the public networks, this architecture does not require complex ASIC or graphics processing units, as a central processing unit (CPU) can perform the task.

Node Operations

The node operations on the blockchain protocol allow multi-party node operators or *miners* with geographically restricted usage. The NodeOps can be observed using a command-line interface and hypertext transfer protocol secure (HTTPS) connection. The node operators each have their own unique Ethereum identities. To begin with, the prototype only requires a few node operators to run the application with a limited number of end users. In the event of expansion, node operators can be provisioned across various regions. Only a limited number of

FIGURE 3 | High-level backend workflow. Transaction detail page showing a successful deployment. It contains the transaction hash, sender's and receiver's public keys, block number, timestamp for the block, and the input data. The users can keep a copy of the transaction hash, which is an alternative to an "order number".

node operators can be permitted to operate from a particular region to reduce geo-redundancy. The node operators do not need to use the DApp for operational purposes. The end users, on the contrary, will not have direct access to blockchain-related operations. They will only be permitted to see details of the transactions that are relevant to their account.

Furthermore, each of the node operators is restricted to deploy a certain number of nodes. No node operator is permitted to operate more nodes than the first one within the network. Having a geographically distributed node operations benefits from the load balancer of the region in which the person is operating in; therefore, granting a faster performance without having to queue within the network. The node operators require minimal computational capacity and do not need to monitor operations continuously. CO-App also allows external operators to operate a node with a vote from an existing operator, which extends its capability to become bigger and faster. The process allows a combination of low-cost infrastructure and horizontal scaling in a short space of time.

The node operators are to be invited to join the network by the NHS digital team, following similar framework used to recruit volunteers to perform critical tasks at the NHS Nightingale Hospital. All the node operators interested in participating in the process are thoroughly vetted and enhanced through Disclosure and Barring Service (DBS) to mitigate against criminal activities, such as cybercrimes. The application would be governed by a consortium, involving both the NHS digital team, the node operators and a selected number of end-users.

Payload Classification

The data will be divided into three classes—confidential, transactional, and others. Firstly, personal identifiable information (e.g., name or ID) is classed as confidential data. Users are assigned with unidentifiable public keys, which are stored on the blockchain instead of their actual names. Secondly, every time a transaction is sent to the blockchain, it will generate a transactional data. The blockchain network generates a hash for all the transaction on the network, with a timestamp and a block number. While the registry is recorded on-chain, the actual "confidential" data is encrypted and stored off-chain in an encrypted vault. The data can be accessed via the blockchain protocol using application programming interface (API).
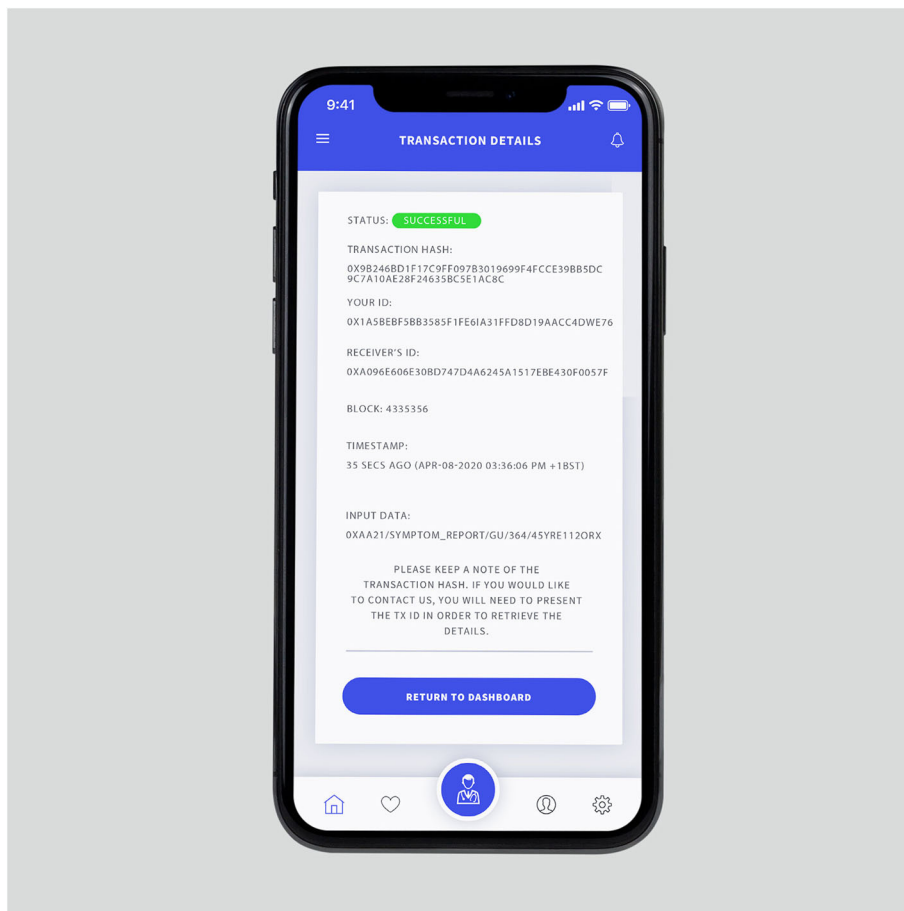
FIGURE 4 | Transaction page showing a successful deployment. It contains the transaction hash, sender's and receiver's public keys, block number, timestamp for the block and the input data. The users can keep a copy of the transaction hash, which is an alternative to an "order number".

When a data is sent to the blockchain, the system generates a transaction hash, each being is a record of the particular event on the chain. Each transaction detail contains a hash, state, block number, block ID, receiver address, sender's address, and input data classifying the category of the transaction (**Figure 4**). If the information is updated at a later date, the new transaction is linked to the previously stored hash on the chain. CO-App ensures that all events for one patient requiring access to services have an immutable record of transactions. The confidential records, such as detailed user reports and clinical images are stored off-chain and can be accessed only through the blockchain gateway using API. Only authorized users can access all the previous transaction details using an "Explorer."

Data Management
It is vital for the researchers to have direct access to the health records across the country to accelerate the process of vaccine development and develop better forecasting studies. It not only applies to this scenario, but also for any future pandemic. In this system, the user is guaranteed with anonymity, especially if the user agrees to exchange it. Therefore, researchers specialized in infectious disease control, such as microbiologists responsible for COVID-19 vaccine research cannot use test data without a user granting full access. The users on CO-App recovering from the virus could become vital personnel in developing future vaccines. As the platform allows static and dynamic asset registration, a certification system can be issued via the blockchain platform to ensure that the recovered users are particularized.

High-Level DApp Functionalities
User Grading
CO-App DHS consists of six primary users—general users, clinicians, service providers (**Table 1**), scientists and researchers, node operators, and network administrators or central operations team. For the users to join the network, a person needs an invitation and follow *usership registration* via the blockchain network's access control scheme (**Figure 5**). The process is automated; therefore, human intervention is not required. In the event of intervention, administrators can manually approve usership. During the initial phase, the users only need to provide email, password and agree to safeguard a *private key* (**Table 1**). During the registration process, the users

TABLE 1 | Definitions.

System parameters	Description
Network	Private—Only users with authorization are allowed within the network Permissioned—Only permitted operators are allowed to join and operate a node
Password	An 8-digit password required for registration, which includes a small cap, large cap, and a combination of numbers
Private key	A 64-byte hash algorithm, downloaded in form of a "JSON"—JavaScript Object Notion file
Public key	A blockchain address, or an Ethereum user address
Service providers	Health service providers that work alongside the NHS, including NHS volunteers
Scientific resource teams	A team of distributed volunteers posting validated news about the updates of the COVID-19 pandemic
Regions	Particularized areas within the country from where the node operators can perform their functions, with each having its regional server. The load balancers can divert traffic to the regions to normalize traffic load.
Clinical operations	Tasks conducted by clinicians, or deemed as "clinical," including interventions

are provided with a backup seed recovery that allows any user to gain access if the private key is compromised.

Each user on CO-App has a wallet for communication. The system replaces a user's name with a blockchain address, or public key in the explorer. Administrators of the blockchain have access to the "Explorer" to track and audit submissions.

During the phase of user-testing, NHS would be in charge of recruiting "test users" by sending out a press release. Once sufficient testing data has been collected, the application is made available for wider release to the public within the country. The DApp follows the characteristics stated below:

a. Independent Existence: General users have full right to withdraw and delete all the personal "confidential" information (see Payload Classification) from their user dashboard
b. Control of Information: Users have full access to control of information, and that the users are able to choose whether the data is disclosed with a second party within the DApp
c. Transparency of Data Usage: Although the data operators and machine learning algorithm manage the data, the process is transparently outlined so that it is not abused by any third-party, including law enforcement agency
d. Data Confidentiality: Identities are not transferred outside the scope of use defined by the CO-App DHS
e. Limit Purpose: All users are provided with a detailed explanation that the data would only be used for lawful, appropriate and specified purposes, and not administered in a manner that unsuited with the original mission

f. Protection: Sufficient protocols in place to ensure that the safety of user data is systemically reviewed and improved.

It is noteworthy that only personally identifiable information which is stored off-chain (see Payload Classification) can be deleted from the application. Any transactional data generated by the users are immutable as it is stored on the blockchain; therefore, their "names" will be permanently replaced by their public keys. It is ensured to carry out a robust-audit trail in the future.

Usership Registration

Usership registration allows the collection of certain information to comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations. Unlike the smart contracts that operate within the *Transaction Layer*, these contracts are primarily operational on the application layer. Deemed as the Application Layer-specific Contracts (ALCs), the functionalities and development are more intricate than the transactional smart contracts. These smart contracts also allow the applications to create interoperability (i.e., the function to communicate with other decentralized applications within the protocol). Allowing a combination of ALCs and Application Programming Interfaces (APIs) to be operational on this layer, the DApp can also connect with social media networks, as well as other DApps within the Layer 1 protocol ecosystem for faster and efficient usership registration process in the future. Each user has full and user-controlled access and can exercise their data protection rights. The process functions as follows:

1. The users request access to be registered on CO-App to generate a usership ID (**Supplementary Material**)
2. CO-App sends the users an encrypted form with a set of parameters, including NHS ID (**Figure 6A**)
3. The verifier requests access to previous *electronic health record* (EHR) from the NHS database, which can be declined by the user (**Figure 6A**)
4. The users complete the form and undertake *key exchange protocol*, during which the user signs the document digitally
5. The verifier generates unique *public key* (0xabc34…) and transfers confidential *payload* to the encrypted vault
6. The verifier issues *private key*: using *ECDSA* (**Annex Table 2**), an algorithm to generate a *64-byte integer,* essentially two *32-byte integer* along X and Y of the elliptic curve
7. The users confirm the download of the private key and secure storage of the seed phrase
8. The verifier generates a CCU ID based on the cluster of 1.5 million people already identified to have underlying health conditions (National Health Service, 2020). The CCU users receive their IDs immediately via email after their registration data has been verified.

Key Exchange Protocol

The smart contract function, an end-to-end encrypted connection, as demonstrated below, tasks as follows:

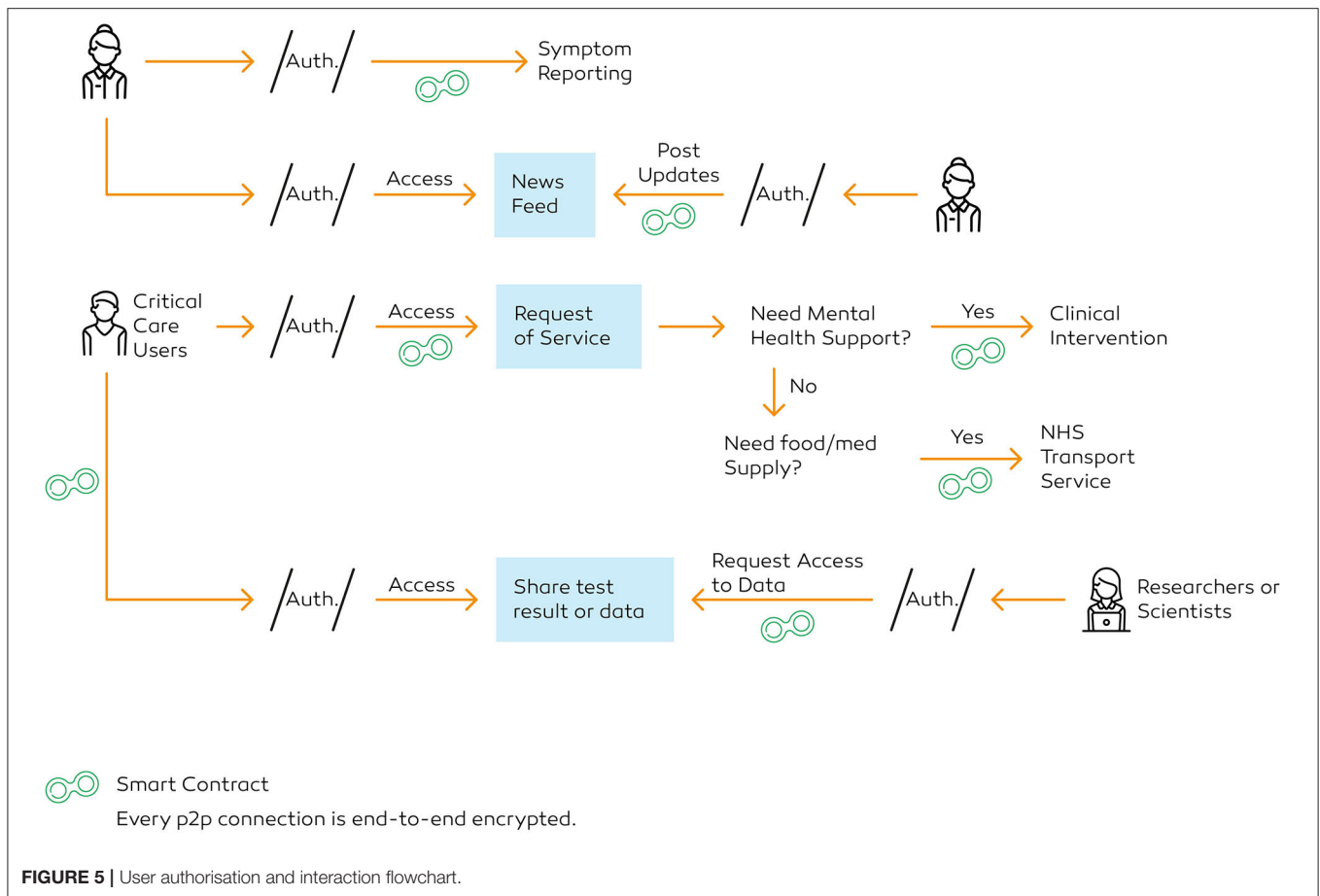1. Sender generates a request for a service (e.g., medicine delivery)

FIGURE 5 | User authorisation and interaction flowchart.

2. The verifier provides sender an encrypted form with a set of parameters
3. Once completed, sender signs the document digitally, using *secp256k1* curve and *ECDSA* cryptography to generate a *hash* and *nonce*
4. The system transfers the *payload* to the recipient
5. Recipient receives a notification to gain access. The verifier presents a challenge. To decrypt, the recipient uses the *public key* of the sender to verify the *hash* and its three components: *bytes32 R; bytes32 S; uint8 V*.
6. Recipient validates the integrity of *payload*, *nonce* and source using *keccak256* hashing function
7. Once decrypted, API enables the verifier to forward the encrypted data to user B
8. After the task is completed, the system deploys the results
9. The verifier validates the contract, generates a transaction *hash* against the task
10. Central operations can use the shared key to request access, in the event of an intervention.

User Experience
Registration and news feed
For registered users to gain access to the platform, they need an email address, password, and private key (**Figure 6B**). The users are then introduced to the application with an onboarding presentation. In order to comply with data protection law, users must accept the terms and conditions before signing up for the DApp. With regards to the principles set by the Information Commissioner's Office, the users of the application are provided with a very simple and easily read-able privacy statement to explain the four core issues of privacy—transparency and pseudonymisation, data minimization, data exercise rights, and strength of data security.

Once the users are presented with the privacy terms, they are required to scroll to the bottom of the page in order to activate the "Accept" button. The users are prompted with a warning if they scroll instantly to fasten the process. This step allows time to think and read through so that they are aware of the process in which their data is utilized. The users are visibly instructed that any personal data collected via the application are only used for specific reasons, such as calculate the number of COVID-19 infections reported, use machine learning to differentiate false positives and comprehend the value of R_0. It is also made transparent that the data will be not be passed on to law-enforcement agencies that might put a user in jeopardy. The end-users on the platform can visit the "Settings" tab to request deletion of any non-transactional and clinical data that are not stored on the blockchain.
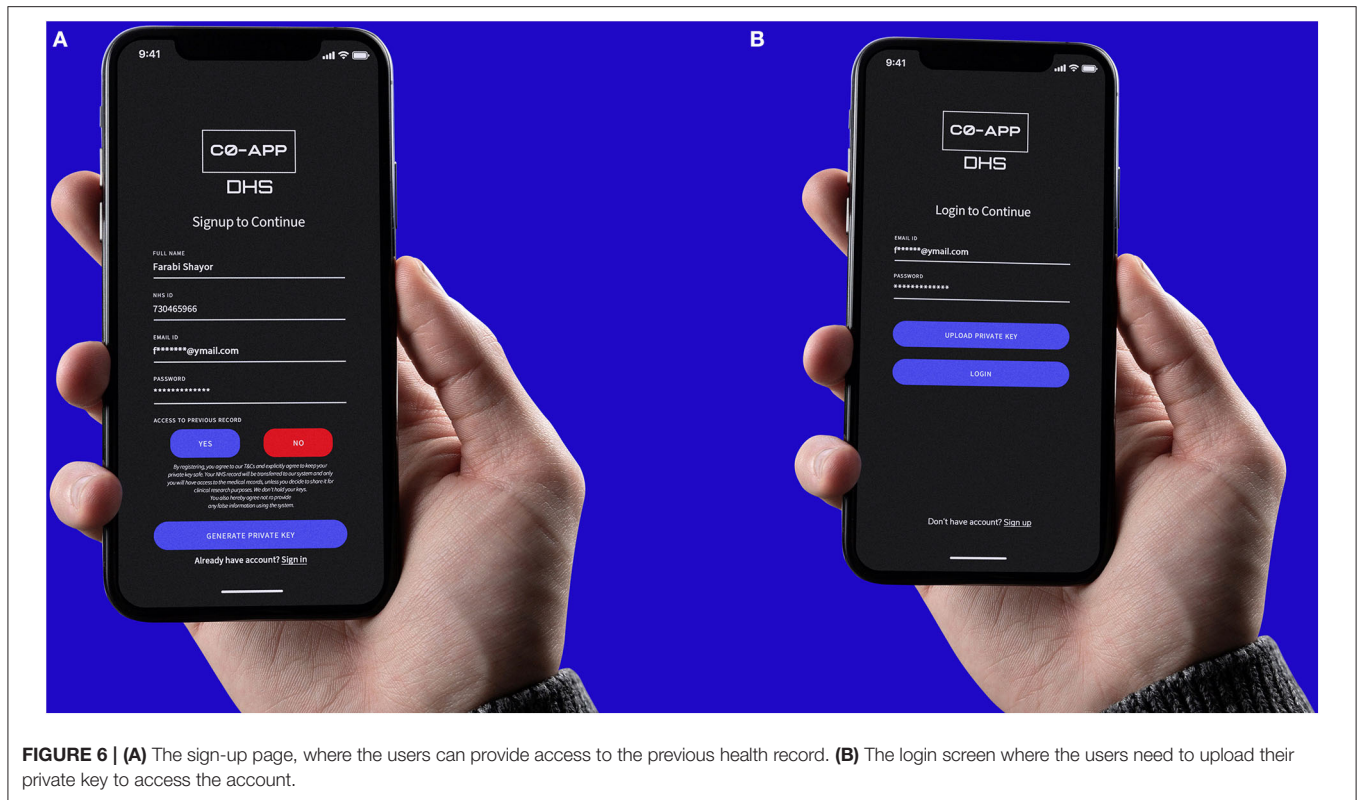
FIGURE 6 | **(A)** The sign-up page, where the users can provide access to the previous health record. **(B)** The login screen where the users need to upload their private key to access the account.

After the users gain access, they are taken to the news feed, comprising of the news posted by verified *scientific resource teams* (**Table 1**), volunteered to produce COVID-19 updates in a way that is comprehensible to the public. It could reduce barriers to scientifically-grounded information, instead of relying on social media. In order to retain the scientific viability of the information, a *reputation mechanism* allows the submitted articles to be reviewed internally before they are posted on the application. Using Key Exchange Protocol, the article writer generates a review request to internal reviewers. The reviewer, once submitted, makes necessary corrections, and signs the document digitally (Key Exchange Protocol). The system transfers the payload to be made publicly available, and a hash is generated against every article. For every revision made, the article is reviewed, and an updated hash is generated to track the document history by internal reviewers and authors. The users on the platform writing these articles for the application receive badges once every task is completed. The badges distinguish a general user from a "CO-App DHS Author." For every article published, the authors move to a higher tier, and receive a badge for every 10, 20, 50, and 100th paper published. Once an author completes submitting 100 articles, they are awarded and invited to become "Editors." All the badges are displayed publicly within the profile page of the application.

Symptom reporting and contact tracing

From the news feed, the users can navigate to the menu (**Figure 7**), where they can visit services, find test-centers, report symptoms, access settings and log out of the account. Next, by

clicking the "Services" tab, the users can access a list of healthcare services, such as reporting symptoms, share COVID-19 tests with researchers and book health services (**Figure 8**).

Using the "Report Symptom" function, a user can report their conditions directly. While symptom reporting is critical for contact tracing, it is also a key to understand the estimated serial interval. The users within the application will be prompted to add their contacts as friends to perform contact tracing, as described in **Figure 9**. For instance, if user A reports a symptom, every person on user A's friend-list is notified immediately. The verifier prompts the user B, a friend of the user A, to complete a self-assessment once user B accesses the notification. If confirmed, user B would be requested to self-isolate for at least 14 days.

It is noteworthy that not all users will provide full access to their previous electronic health record or agree to share contacts. Therefore, when users intend to report a symptom, they will be requested to provide essential data, a list of parameters to describe all the possible symptoms that the user is experiencing, such as fever, or cough (**Figure 10**). Then, an encrypted form with a set of pre-regulated parameters is presented (**Figure 11**). These parameters are then relayed as *tagged-dataset* to be administered by the MLA. Upon completion, the users sign the documents digitally. During this process, the verifier differentiates the critical care users (CCUs) from regular users to be classified as a separate subset (**Figure 12A**). If the users are classified as CCU, the verifier generates a contract on a priority basis and pushes the transaction to be underscored as an emergency. The verifier, using the shared key, allow the administrators to input the parameters
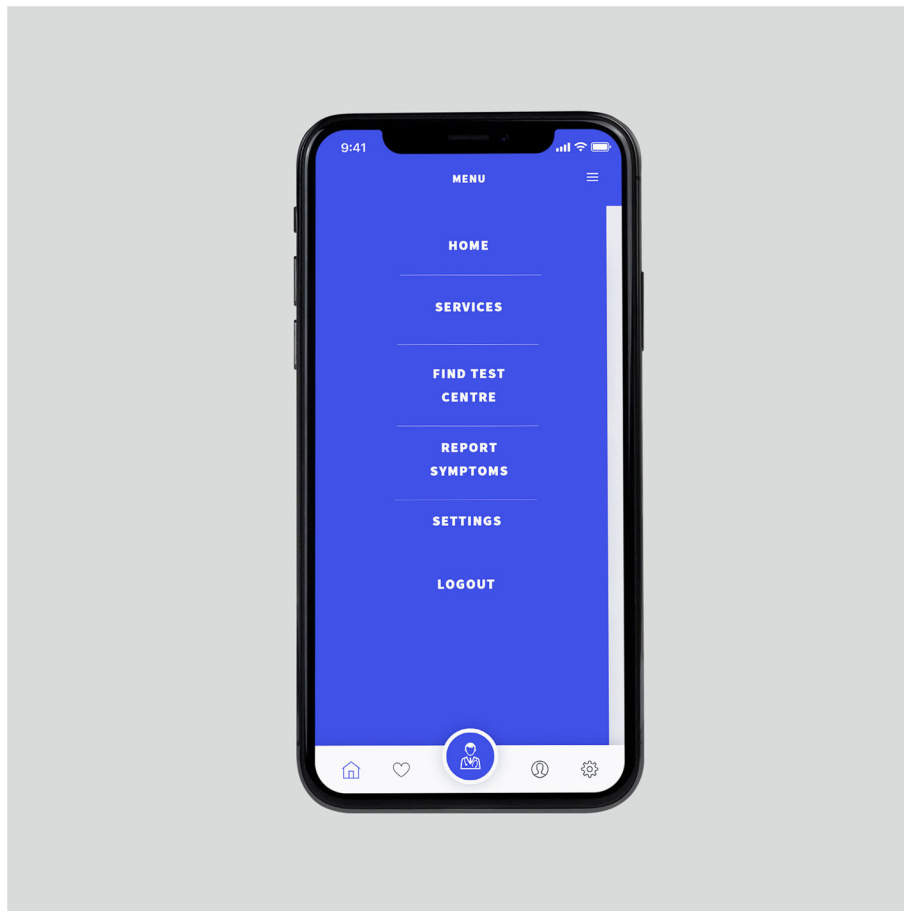
FIGURE 7 | The navigation panel. (From Left) Using the icons at the bottom of the screen, users can also navigate to the home page, access their favorite news articles, visit the services page, access their profile, and application settings.

into the MLA to evaluate the information and find the best possible answer.

Test result exchange

The CO-App users can request for a COVID-19 kit from the NHS, via the retailers. Using reference links, users complete the transaction of purchase on their devices (e.g., phone or computer, and return to the screen once the kit has been received). The users need to upload their data once the tests have been conducted. After the users generate a request, the verifier provides the users with an encrypted form. The verifier is designed to extract specific parameters required to determine the results. The clinicians can use the *key exchange protocol* to request access to the information stored in the encrypted database. The transaction stored on the blockchain replaces critical user information shared among the administrators with a public key. Unless permitted, the administrators and other users having access to patient data can only view the blockchain public key, instead of all the sensitive information at once.

Due to the nature of blockchain, it would be challenging for a user to create a duplicate record, as every single transaction is checked and verified against the previously recorded data. Therefore, every time a user requests a function, the verifier substantiates the contract to ensure one user cannot create multiple copies of the user data. Users can change their profile data within the "Settings"; however, they cannot modify their clinical records. Similarly, administrators or clinicians cannot alter the results of the test due to limited view-only access and backlog.

Health services intervention

CO-App users can request for health services using "Book A Service" tab from the "Services" page. The system is designed to geo-target service providers within a 30-mile region. When a user generates a request, providers immediately receive information from a cluster of CCU users requesting services in a nearby location, such as deliveries of medicine. All the job requests for transport and service delivery are held in an escrow until the task is completed. When the service provider accepts the job, they can access basic confidential data such as name and delivery address.

Use of technology could improve mental health by providing access to such services (Cortelyou-Ward et al., 2018). Once a user requests clinical intervention, the system sends batch requests to the professionals. Once the task is completed, the registered professional can mark the task as "complete" from
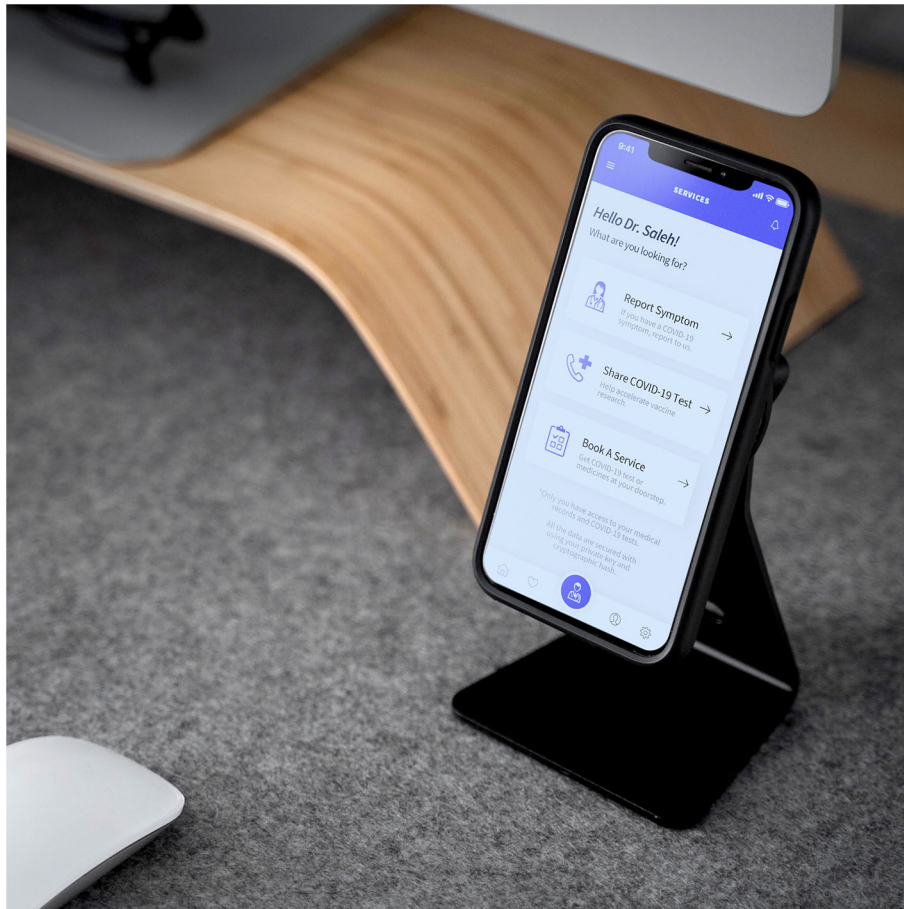
FIGURE 8 | The "Services" screen.

their dashboard, upon which the verifier registers the task on the blockchain.

The critical care users can also receive COVID-19 test kit using "Book A Service" tab. If requested, a CCU is presented with an encrypted form, demonstrated in **Figure 12B**. Upon clicking "Book Your Delivery," the verifier authenticates the data and generates a request to the service providers on an urgent basis. The verifier issues a transaction hash once the task is signed-off as complete (**Figure 3**). The central operations team can use the shared key to intervene in the event of multiple service providers dropping the job request.

Clinical record exchange protocol

The scientists can use the peer-to-peer connection to retrieve data from patients. The scientists can request a cluster of users on the database to gain access to their results stored on the system. Both users need to undertake the *key exchange protocol*. When the verification is completed, the scientists are presented with a challenge, which allows decryption and deliver download procedure of payload. Scientists can also request access to historical clinical information and results of the test directly from the users. They can send a batch request to the users who

have permitted retrieval of medical history during registration. The process of finding blockchain data, aggregation of statistical information and sorting process to develop data-centric articles can be conducted using the REST API (Pratama and Mutijarsa, 2018).

Neural Network for CO-App

There is a substantial risk of a user incorrectly self-diagnosing, causing unnecessary isolation. Therefore, the machine-learning aspect is utilized as a key component to ensure that the users aren't misdiagnosed. Unlike traditional algorithms, deep neural networks (DNN) use *machine-learning algorithms* to perform functions by simulating the design of a human brain. The input layers are independent variables that have associated *weight*, a numeric value which is fed into a transfer or *activate function*. The purpose of the *function* is ensuring non-linearity and that the neurons can function adequately in presences of other neurons. An activation function can typically be a *logistic regression*, which returns the probability of a value using *sigmoid logistic function*. The nodes in the hidden layers receive the data from the previous layer as input and deliver the output to the next layer. Each hidden layer has a separate
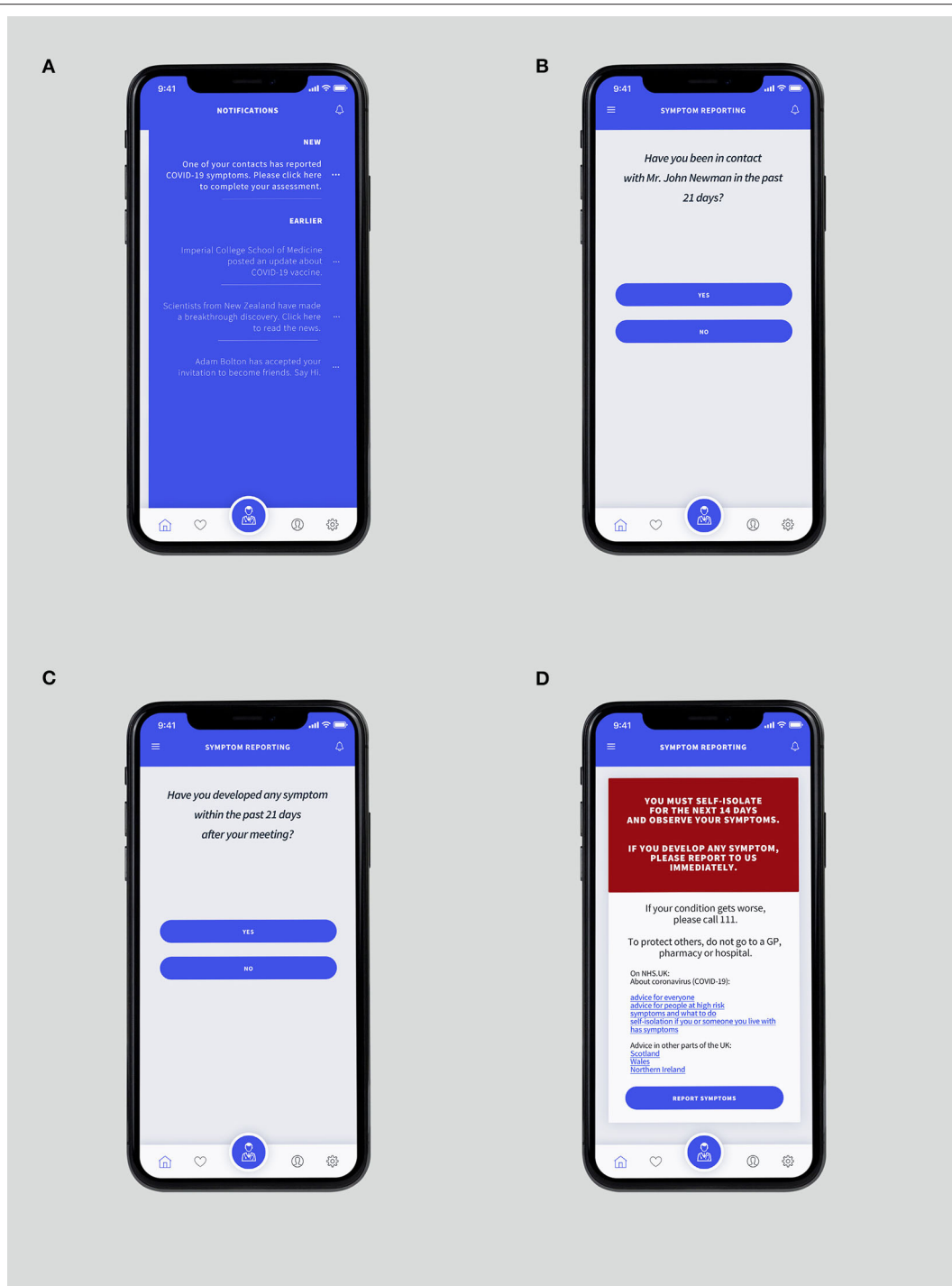
FIGURE 9 | (A) The "Notification Panel" which can be accessed by swiping the screen from the right-hand side. **(B)** "Suspected" recipient is requested whether the user has been in contact with Mr. John Newman, who recently reported COVID-19 symptoms. **(C)** The verifier ensures whether the "suspected" developed any symptom after the meeting. **(D)** The confirmation page is showing details of instructions if suspicion is confirmed.

bias. If there are two layers within the network, then the first hidden layer receives parameters directly from the input layer and delivers the results as an input to the second layer (**Figure 13**). A steep learning curve for the DNN can be ensured

if only specific criteria are fulfilled using its operations, such as determination of the positive or negative, probability of confirmed symptoms and also differentiating a confirmed case with a false-positive.
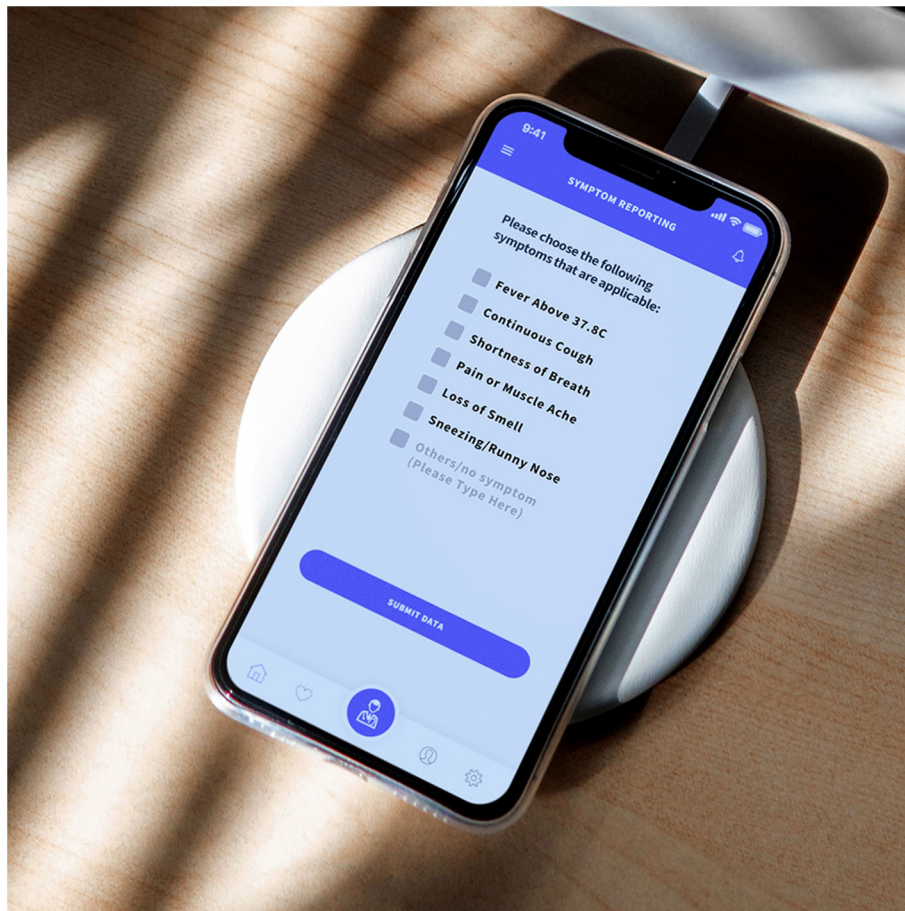
FIGURE 10 | Symptom reporting page, with the most common options for COVID-19. The entries eventually form tagged-dataset for the MLA.

The neural network ought to develop over time; the accuracy of results increase as more information is fed into its data cluster. The neural network designed for CO-App COVID-19 user classification has primary two purposes. First, create clusters of users based on the input parameters, and second, use all possible independent variables to find the probability of a positive user from the reported symptoms. Two different machine-learning algorithms are chosen for these two objectives.

K-Means clustering

In order to develop a precise cluster, *K-Means clustering model* is chosen (Kanungo et al., 2002). The aim of this process is creating clusters possessing similar attributes, such as reported *asymptomatic patients.* It is a non-parametric method assuming that the data does not have a normal distribution. The algorithm creates data clusters of patients based on underlying symptoms, and therefore deduct results based on the parameters. All the data fed into the MLA is labeled to optimize the model. Four *centroids* are chosen to develop four cluster—positive symptomatic, positive asymptomatic, negative symptomatic, and negative asymptomatic. The MLA develops tagged-dataset results based on the distance between the data point and the cluster

center. The data points are assigned to each cluster, meaning that underlying conditions such as diabetes or cardiovascular disease are assigned to the clusters. The algorithm continues to run until the optimal mean positions of K are defined for the four centroids, and the data are partitioned into four groups. An additional cluster can also be introduced to create a different cluster with all the possible outliers (Gan and Ng, 2017).

Multi-class neural network

Once the cluster data is obtained, all other available variables from the encrypted form along with the dataset is fed into another algorithm to find the probability of a user being positive or negative as a binary output. A supervised machine learning method is used to classify a user as a confirmed COVID-19 case. A *multi-class DNN* is utilized to find patterns among the data parameters, including but not limited to the variables from the encrypted form (**Figure 9**), geolocation and patient history. There would be numerous inputs variables; therefore, *hyperparameter optimisation* is necessary. It is a *tuning* process to find an optimal set of parameters required to deduct an automated conclusion. A *grid search* is conducted among all the input parameters. Although it is time-consuming, the method
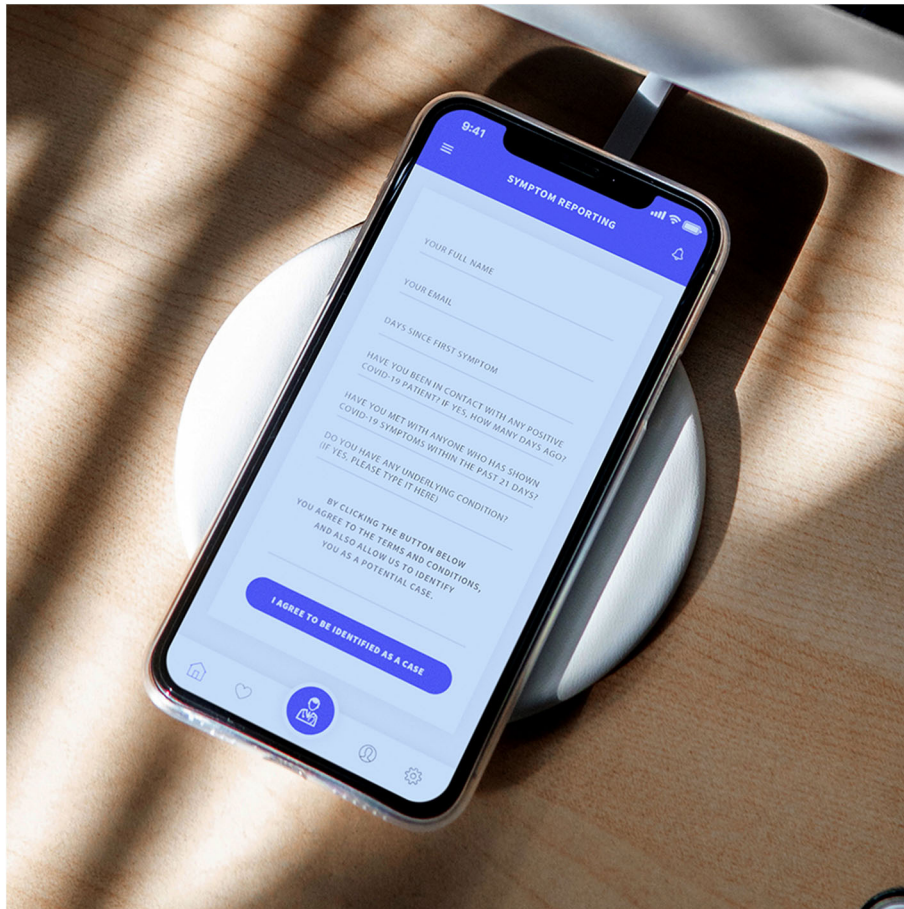
FIGURE 11 | The encrypted form with details to analyze, including the questions required to define a probability.

ensures inferring the optimal set of parameters needed to label a patient. Multiple training models can be created in the *pipeline* to test, increase *accuracy* and *precision*. The output layer delivers a binary result, confirming the probability of being a positive COVID-19 patient.

End-to-End Architecture

As a supplementary service, Co-App can sustain co-dependently along with the NHS digital database. For instance, scientists can request historical clinical data, which is required to be pulled from the central NHS database using NHS ID. The architecture is designed to be peer-to-peer; therefore, when a user makes a request, it creates a single read-only data transfer session using API between the application and the NHS database. Furthermore, all the processes and data sharing methods are designed to be end-to-end. For example, if critical care users (CCUs) request for a service provider (see Health services intervention), the data is directly sent to the provider, instead of a central command. The application automatically assigns a service provider to a user. Therefore, when they receive access to personal data such as the address, it does not pass through any other user in between. Similarly, if generic users decide to
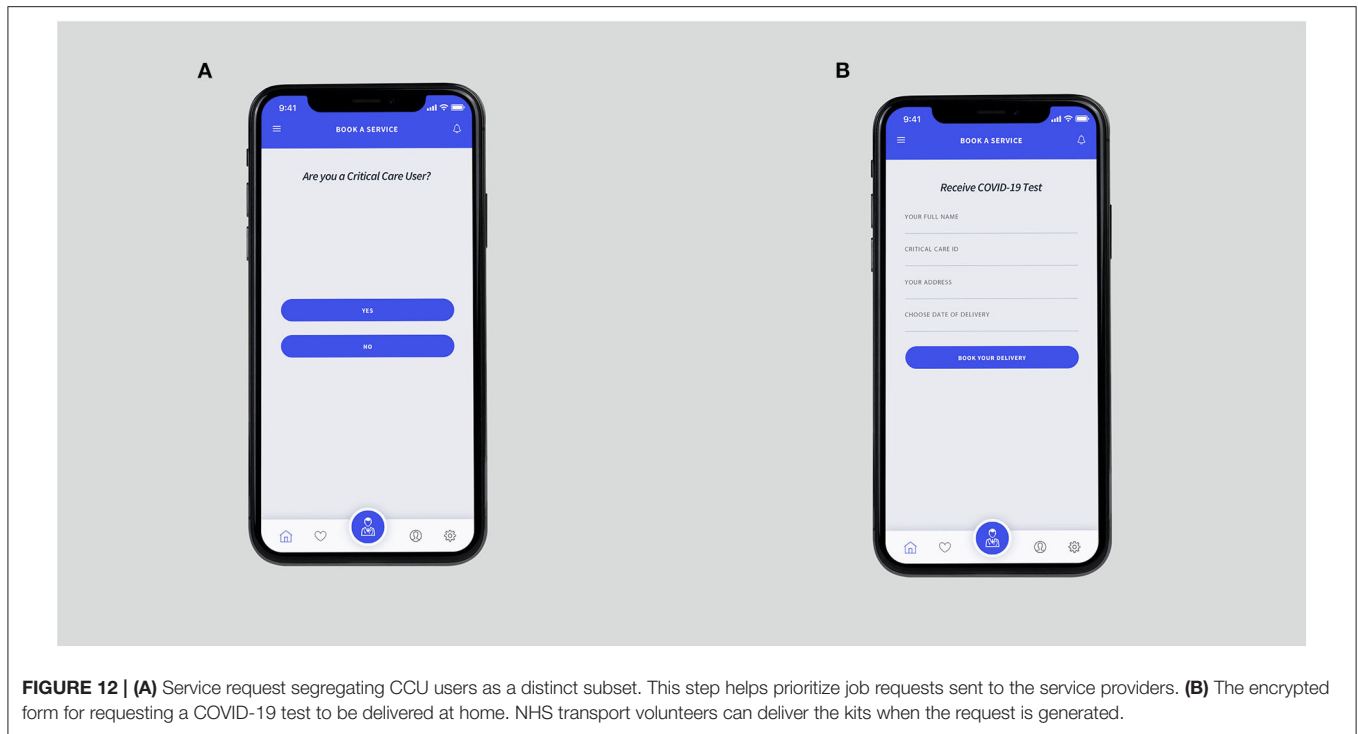
share the clinical record with scientists developing vaccines (see Clinical record exchange protocol), the application generates an end-to-end session between the user and the scientist, which is illustrated in **Figure 4**.

TECHNICAL AND OTHER LIMITATIONS

There are several limitations, including the requirement of new organizational policy for decentralized operations:

Processing Large Data Samples

Due to the limitations of the number of Transactions Per Second (TPS), and overall scalability, decentralized networks still lack the capacity to administer a significant amount of data in contrast to a centralized network. Having centralized servers with distributed node operations may solve the issue, however, in that scenario, it is a complete inverse of the characteristics of blockchain technology. The scalability issues are currently being mitigated by the Ethereum foundation to increment the performance by data partitioning, introduction of ZKSnarks and parallelisation (Bez et al., 2019). As a popular DApp development protocol, study illustrates that probability of triumph of a DApp

FIGURE 12 | (A) Service request segregating CCU users as a distinct subset. This step helps prioritize job requests sent to the service providers. **(B)** The encrypted form for requesting a COVID-19 test to be delivered at home. NHS transport volunteers can deliver the kits when the request is generated.

favors an Ethereum-based model (Worley and Skjellum, 2018). With regards to the development cost, short-term expenses might be higher until a fully-operational model is developed, however, the necessity of adopting the benefits of such a versatile network eclipses the discussion on short-term costs. Hence public and private corporations are adopting private-permissioned blockchain for wide variety of use cases as it provides faster processing capacity.

Barriers to a Collaborative System

It would be expensive and challenging to bring stakeholders such as scientists from different organizations, NHS employees, and other service providers into one single platform. Traditional companies are using legacy enterprise systems, varying from manual operations to using age-old software for data processing. Once a company and its stakeholders are trained to use a specific type of setting, it becomes rather expensive for them to replace it with a new version, which requires further training. With an employee count of over one million, introducing a new system would require most or all the employees at the NHS to be trained. This increases cost, time for adoption, as well as adopting extended plans for implementation. Nevertheless, it is noteworthy that CO-App DHS is introduced as a supplementary system for the purpose of data integrity and transaction management, therefore it would not require a comprehensive overhaul of the backend systems.

Security of User Data

Another major barrier is the user-centric mechanism of blockchain—in order to process and maintain the highest level of security, the private key must be secured locally at all times. Unlike a password which can be maliciously decrypted, a private key cannot be decrypted due to its level of security. However, since the private key is an actual file, not a memorable set of numbers, unauthorized access to this file by cybercriminals could mean that the account has been compromised. The physical separation of the file is a necessity.

In this scenario, the users are encouraged to store the private key file in cold storage, such as a USB drive which cannot be accessed via an internet connection. It may seem discouraging to end users who are more vulnerable. If the private key file is stored in an online storage, such as the Google Drive, it may be accessible to cyber criminals using storage paths created locally in a computer. Furthermore, sharing critical information occurs using the shared key generated by the verifier, which is peer-to-peer in nature. Further adoption of the platform by a large number of users will provide a better understanding if any the features are needed to be improved or any specific attribute of the verification method must be prioritized for improving.

Consensus Mechanism

Although horizontally scalable, the consensus mechanism (Consensus Mechanism), proof-of-authority is less decentralized in comparison to PoW due to the restricted number of operational nodes. The consensus permits node operators to be active based on the "reputation," and in the event of the reputation being damaged, rights for operations might be revoked. However, due to the sensitive nature of the data, the gain from conducting malicious activities within the network can be higher than the reputation in the
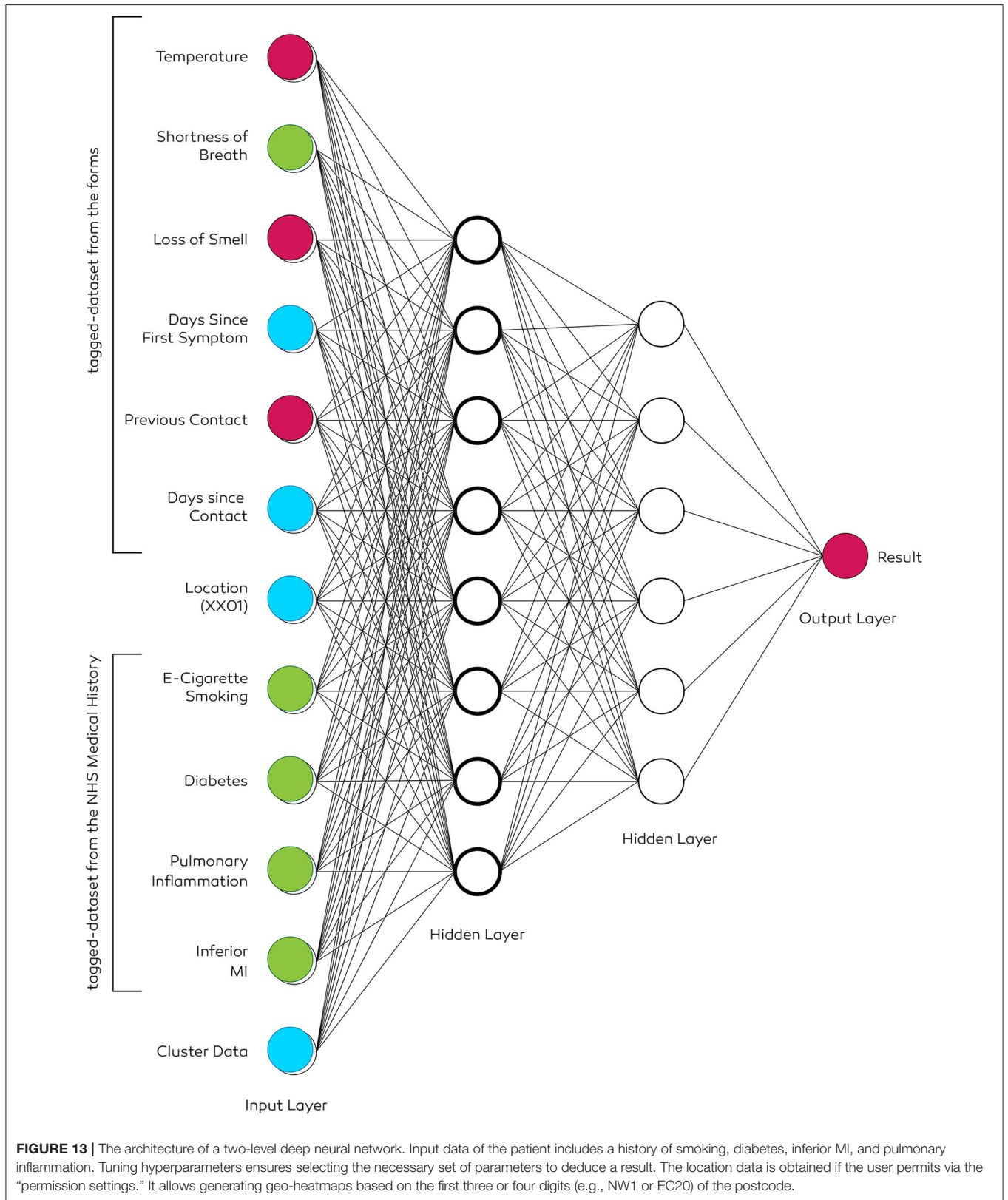
FIGURE 13 | The architecture of a two-level deep neural network. Input data of the patient includes a history of smoking, diabetes, inferior MI, and pulmonary inflammation. Tuning hyperparameters ensures selecting the necessary set of parameters to deduce a result. The location data is obtained if the user permits via the "permission settings." It allows generating geo-heatmaps based on the first three or four digits (e.g., NW1 or EC20) of the postcode.

community. Therefore, in this scenario, the right to gain the status of a node operator must be hard enough so that it eventually becomes damaging to lose. Hence, node operators are required to be authorized by the central administrators to ensure that their anonymity does not damage the activity of the network.

Technical Limitation of AI

With regards to the neural network (Neural Network), although DNNs can process data swiftly, training, on the contrary, can be time-consuming. Therefore, an open-sourced dataset from previous studies or existing NHS data can be used to pre-train the DNN. Accuracy and precision of data modeling will increase over time. Supplementary algorithms can be developed for anomaly detection in large datasets to identify patients with a unique set of characteristics. The paper is also subject to limitations such as lack of proper user testing, user-behavior research, negative or positive externalities and potential conflict of interest. Further, previous studies also emphasized on the lack of user testing in healthcare setting, which is, therefore, vital before the development of such novel platform that could be deployed on such a large scale (Agbo et al., 2019). More time is needed to conduct such large-scale user research.

Purpose Limitation and Public Apprehension

"Track and trace" is a sensitive and highly controversial issue; therefore, it is prudent to acknowledge that the users may be apprehensive with regards to the adoption of the platform. The fear of the users in this scenario are two fold—firstly there is a suspicion that the data might be illicitly used by the government to track and forward to law enforcement or such, and secondly, the data might be stolen. Therefore, the users are assured using the "Terms of Privacy" that their data will only be investigated for clinical purposes and follows article 5(1)(b), *purpose limitation principle* of the Data Protection Act 2018. Additionally, the users can also be persuaded to embrace by showcasing the benefits of a blockchain-based application, as it is much more secure in contrast with the typical centralized application. Such characteristics could be clearly exemplified using high-definition animation and design-focused infographics.

Other Challenges

More innovative approaches with regards to the development of blockchain-based digital health solutions are emerging. However, the public and private sector would prefer the development of traditional application using a centralized server due to the established standards. Shared governance sounds idealistic, although, it may not be perceived as wholly positive to many. Therefore, it is likely that blockchain applications would face rigorous scrutiny and challenges. These challenges will not be specific to policymakers, but also general users, doctors, scientists, and other key workers who would provide their services on the platform.

RECOMMENDATIONS AND PROPOSALS

There remains a scarcity of literature focusing on the quantifiable data that exemplifies the impact of technology-based intervention specific to a pandemic, due to the lack of infrastructure. It is essential to corroborate the potential of these new technologies as the world move toward the fourth industrial revolution (Lu, 2017; Schwab and Davis, 2017). Utilizing blockchain could improve critical decision making (Cerf et al., 2020), which is crucial at times of a crisis in government organizations (Hale et al., 2006). Additionally, users may not comprehend the significance of a new technology which could act as a barrier to adoption (Juma, 2016). Such bottlenecks of technological illiteracy can be surmounted by creating appropriate documentation and awareness programs that could help facilitate the adoption, more notably, among the elderly. Nevertheless, this platform would necessitate a multitude of service providers to collaborate on one unified area; hence it is unclear whether or not the existing corporations proficient in using legacy enterprise systems would be inclusive to such an advanced approach. Information-sharing standardization practices need to be developed so that multiple service providers can work together without conflicts of interest. Additionally, more research into how the private node operators can be compensated needs to be explored in qualitative studies.

It is vital to convey scientifically-grounded content more easily. Therefore, a team of experienced volunteers is necessary to ensure that the scientific data is communicated thoroughly to the public. Besides, during the times of crisis, an open-sourced community can be created from across the nation for the development of a sandbox. Rapid deployment of the platform requires *ad-hoc* crowdsourced development. It will be the most effective way to achieve goals in a shorter period. Li and Ulaganathan (2017) have explored crowdsourced application development for disaster management, real-time data collection and bi-directional communication. CO-App development team would collaborate with the NHS, Public Health England, UK Government, and its team of scientists to deploy research pilots faster. To start with, only a small group of cases and suspected patients can be subjected to the clinical trial. Their input and data collected via the platform would accelerate the adoption, find the key performance indicators and foster cross-country research.

Data security requirements are crucial during crisis management (Seba et al., 2019); therefore, security research for increased data protection is required before national-scale implementation (Halim et al., 2017). With regards to the law, Co-App "Terms of Privacy" would strictly comply with the article 5(1)(b) *Purpose Limitation Principle*, under which personal data is only collected and archived to contain the pandemic. The rules of data processing are made clear from the beginning as to why the personal data are being collected and how the application is meeting obligations with the Data Protection Act. It is also made sufficiently clear that the application administrators comply with transparency rules and ensure that the data would not be disclosed for any other irrelevant purposes.

The data storage solution of CO-App complies with the GDPR of "Regulation (EU) 2016/679" (The Publication Office of the European Union, 2016), as most of the data are stored in an industry-standard storage facility. Therefore, users could reclaim their *rights to be forgotten*. Moreover, some of the activities are to be manually authorized by the administrators to safeguard user rights. Nevertheless, the UK Data Protection Act should be evaluated against the backdrop of the blockchain platform. Legal advice is required to conform with section 14 of the "Part 2, Chapter 2," and the section 19, which describes the rule to safeguard and archive data, as defined by the UK Government (2018). A Data Protection Impact Assessment (DPIA) must be carried out to outline the benefits and disadvantages of the collection of personal data. A small sample of users may be selected for initial user-testing phase, from whom the administrators could collect data to ensure that the data usage, its purposes and limitation enforcement are made sufficiently clear.

Furthermore, infrastructure research is one of the keys for the success of such a platform. Although favored by many, Ethereum, as mentioned earlier, has its current limitations due to the ongoing scalability issues. Therefore, similar applications can be alpha-tested using alternatively available protocols. Hyperledger, developed by Linux Foundation, is a viable alternative to the Ethereum protocol, as it features multiple implementations of the application-specific characteristics that support CO-App DHS. However, due to the availability of open-sourced codes, and acceptance as a widely adopted platform, Ethereum is favorable for developing such decentralized solutions. Nevertheless, these platforms open a wide-array of research prospects as protocols such the Hyperledger and Quorum would eventually become alternative solutions for the development of such private, permissioned blockchain.

Timeframe and cost are also other concerns—although it is possible to develop Co-App very fast, the costs of developing such a platform might be higher than initial expectations. However, the costs are unimportant when compared to the magnitude of trouble the public health officials will be confronting over the coming weeks. CO-App aims to provide support to the public—obtain their concerns, collateralise COVID-19 tests, share scientific discovery and deliver healthcare services. The broader issue of crowdsourced intelligence and user-centricity trumps the point of costs to ensure public instill trust in the platform.

Several forms of treatment for COVID-19 are currently being explored (Lu, 2020), however, to develop a vaccine fast, scientists desperately need access to a manifold of data, and it can be collected using CO-App. The application is one of the reinforcements to reduce person-to-person transmission and promote healthier social distancing approaches. It provides the extra attention mandated by both the CCUs and the vulnerable people. The fatalities in countries with sophisticated medicare facilities such as the US, Italy and Spain could have been prevented if alternative non-clinical routes of containment were explored earlier. Further, human contact tracers are also required to establish a protocol that allows collection of qualitative data that might be needed to portray a complete picture (Public Health England, 2020). Data is at the heart of this pandemic. Therefore, such a data-centric solution would push the development of more frameworks across the globe.

CONCLUSION

It is essential for public health services to improvise and unearth approaches into developing a next-generation technology-based intervention for advancement in the field of clinical research. The proposed platform not only provides a meticulous idea for consolidating all COVID-19 user data but also permit users to participate at their will. This process follows a need-driven approach for the public sector to derive benefits from the technology, instead of a technology-driven approach to ensure the needs of a sound governance. It would be less expensive to authenticate the data integrity as the process of audit is performed by the algorithms. The success of CO-App DHS would be highly circumstantial; however, it stimulates collaboration on an international scale to bridge the gap between the public and the scientific community. The management of biomedical assets would rely on the users themselves, so as the dissemination of personal data. The challenges scrutinized here above should not exacerbate the adoption and discourage the development, as overcoming them are incumbent steps to flatten the curve. CO-App DHS is one of the use-case of applied computational intelligence for infectious disease control—a theme that necessitates further exploration. Policymakers need to recognize the importance of the analysis, which could benefit virus containment, as it is a future-proof resolution to such a challenge. Consequently, a platform built on the notions of democratization, disintermediation, decentralization, and interdisciplinary research can bestow the humanity with the appropriate practices and strengthen the society to be better equipped for the next wave or any imminent forthcoming pandemic.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/**Supplementary Material**, further inquiries can be directed to the corresponding author/s.

AUTHOR CONTRIBUTIONS

All authors involved contributed equally to the development and design of the protocol.

FUNDING

SUPPLEMENTARY MATERIAL

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fbloc.2020.553257/full#supplementary-material

REFERENCES

Agbo, C. C., Mahmoud, Q. H., and Eklund, J. M. (2019). Blockchain technology in healthcare: a systematic review. *Healthcare* 7:56. doi: 10.3390/healthcare7020056

Alketbi, A., Nasir, Q., and Talib, M. A. (2018). "Blockchain for government services — use cases, security benefits and challenges," in *2018 15th Learning and Technology Conference* (L&T) (Jeddah: IEEE), 112–119. doi: 10.1109/LT.2018.8368494

Al-Tawfiq, J. A. (2020). Asymptomatic coronavirus infection: MERS-CoV and SARS-CoV-2 (COVID-19). *Travel Med. Infect. Dis.* 35:101608. doi: 10.1016/j.tmaid.2020.101608

Antonopoulos, A., and Wood, G. (2019). *Mastering Ethereum. 2nd Edn.* California, CA: O'Reilly Media.

Armitage, R., and Nellums, L. B. (2020). COVID-19 and the consequences of isolating the elderly. *Lancet Public Health.* 5:E256. doi: 10.1016/S2468-2667(20)30061-X

Arnold, J. L., Levine, B. N., Manmatha, R., Lee, F., Shenoy, P., Ming-Che, T., et al. (2004). Information-sharing in out-of-hospital disaster response: the future role of information technology. *Prehos. Disaster Med.* 19, 201–207. doi: 10.1017/S1049023X00001783

Bai, Y., Yao, L., Wei, T., Tian, F., Jin, D., Chen, L., et al. (2020). Presumed asymptomatic carrier transmission of COVID-19. *JAMA* 323, 1406–1407. doi: 10.1001/jama.2020.2565

Bez, M., Fornari, G., and Vardanega, T. (2019). "The scalability challenge of ethereum: an initial quantitative analysis," in *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)* (San Francisco East Bay, CA), 167–176. doi: 10.1109/SOSE.2019.00031

Bogner, A., Chanson, M., and Meeuw, A. (2016). "A Decentralised Sharing App running a Smart Contract on the Ethereum Blockchain," in *Proceedings of The 6Th International Conference On The Internet Of Things - Iot'16* (New York, NY), 177–178. doi: 10.1145/2991561.2998465

Bortel, T. V., Basnayake, A., Wurie, F., Jambai, M., Koroma, A. S., and Muana, A. T. (2016). Psychosocial effects of an Ebola outbreak at individual, community and international levels. *Bull World Health Organ.* 94, 210–214. doi: 10.2471/BLT.15.158543

BouSaba, C., and Anderson, E. (2019). *Degree Validation Application Using Solidity and Ethereum Blockchain. 2019 Southeastcon.* Hunsville, AL: IEEE. 1–5. doi: 10.1109/SoutheastCon42311.2019.9020503

Breiman, R. F. (1996). Impact of technology on the emergence of infectious diseases. *Epidemiol. Rev. 18,* 4–9. doi: 10.1093/oxfordjournals.epirev.a017915

Carson, A., Romanelli, G., Walsh, P., and Zhumaev, A. (2018). *Blockchain beyond the hype: What is the strategic value?* Available online at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value (accessed June 15, 2020).

Cerf, M., Matz, S., and Berg, A. (2020). Using blockchain to improve decision making that benefits the public good. *Front. Genet.* 3:13. doi: 10.3389/fbloc.2020.00013

Chen, G., Xu, B., Lu, M., and Chen, N. S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learn. Environ.* 5:1. doi: 10.1186/s40561-017-0050-x

Chen, N., Zhou, M., Dong, X., Qu, J., Gong, F., Han, Y., et al. (2020). Epidemiological and clinical characteristics of 99 cases of 2019 novel coronavirus pneumonia in Wuhan, China: a descriptive study. *Lancet* 395, 507–513. doi: 10.1016/S0140-6736(20)30211-7

Chiu, C. (2018). Cutting-edge infectious disease diagnostics with CRISPR. *Cell Host Microbe* 23, 702–704. doi: 10.1016/j.chom.2018.05.016

Christaki, E. (2015). New technologies in predicting, preventing and controlling emerging infectious diseases, *Virulence* 6, 558–565. doi: 10.1080/21505594.2015.1040975

Chung, M., Bernheim, A., Mei, X., Zhang, N., Huang, M., Zeng, X., et al. (2020). CT imaging of the 2019 novel coronavirus (2019-nCoV) pneumonia. *Radiology* 295, 202–207. doi: 10.1148/radiol.2020200230

Clauson, K. A., Breeden, E. A., Davidson, C., and Mackey, T. K. (2018). Leveraging blockchain technology to enhance supply chain management in healthcare. *Blockchain Healthcare Today* 1, 1–12. doi: 10.30953/bhty.v1.20

Cortelyou-Ward, K., Rotarius, T., and Honrado, J. C. (2018). Using technology to improve access to mental health services. *Health Care Manag.* 37, 101–108. doi: 10.1097/HCM.0000000000000211

Day, M. (2020). Covid-19: four fifths of cases are asymptomatic, China figures indicate. *BMJ* 369:m1375. doi: 10.1136/bmj.m1375

Dimitrov, D. V. (2019). Blockchain applications for healthcare data management. *Healthc. Inform Res.* 25, 51–56. doi: 10.4258/hir.2019.25.1.51

Dong, E., Du, H., and Gardner, L. (2020). An interactive web-based dashboard to track COVID-19 in real-time. *Lancet Infect. Dis.* 20, 533–534. doi: 10.1016/S1473-3099(20)30120-1

Dorigatti, I., Okell, L., Cori, A., Imai, N., Baguelin, M., Sangeeta, B., et al. (2020). *Report 4: Severity of 2019-novel coronavirus (nCoV). WHO collaborating centre for infectious disease modelling MRC centre for global infectious disease analysis.* London: Imperial College London COVID-19 Response Team.

Eghbali, H., and Hajihosseini, N. (2019). *Deep Convolutional Neural Network (CNN) for Large-Scale Images Classification.* Available online at: https://ssrn.com/abstract=3476258 (accessed March 10, 2020).

Einaste, E. (2018). *Blockchain and healthcare: the Estonian experience.* Available online at: https://e-estonia.com/blockchain-healthcare-estonian-experience/ (accessed March 20, 2020).

Ekberg, J., Eriksson, H., Morin, M., Holm, E., Strömgren, M., and Timpka, T. (2009). "Impact of precautionary behaviors during outbreaks of pandemic influenza: modeling of regional differences," in *Annual Symposium proceedings. AMIA Symposium* (San Francisco, CA), 163–167.

Ernst, C., Mladenow, A., and Strauss, C. (2017). "Collaboration and crowdsourcing in emergency management," in *Int. J. Pervasive Comput. Commun.* 13, 176–193. doi: 10.1108/IJPCC-03-2017-0026

Ethereum (2019). *libsecp256k1.* Available online at: https://github.com/ethereum/go-ethereum/tree/master/crypto/secp256k1/libsecp256k1 (accessed March 30, 2020).

Gan, G., and Ng, M. K. (2017). k -means clustering with outlier removal. *Pattern Recogn. Lett.* 90, 8–14. doi: 10.1016/j.patrec.2017.03.008

Garshnek, V., and Burkle, F. M. (1999). Telecommunications systems in support of disaster medicine: applications of basic information pathways. *Ann. Emerg. Med.* 34, 213–218. doi: 10.1016/S0196-0644(99)70231-3

Gates, B. (2020). Responding to COVID-19 — a once-in-a-century pandemic? *N. Engl. J. Med.* 382, 1677–1679. doi: 10.1056/NEJMp2003762

Gilbert, M., Pullano, G., Pinotti, F., Valdano, E., Poletto, C., Boëlle, P., et al. (2020). Preparedness and vulnerability of African countries against importations of COVID-19: a modelling study. *Lancet* 395, 871–877. doi: 10.1016/S0140-6736(20)30411-6

Gootenberg, J. S., Abudayyeh, O. O., Lee, J. W., Essletzbichler, P., Dy, A. J., Joung, J., et al. (2017). Nucleic acid detection with CRISPR-Cas13a/C2c2. *Science* 356, 438–442. doi: 10.1126/science.aam9321

Gresch, J., Rodrigues, B., Scheid, E., Kanhere, S. S., and Stiller, B. (2019). "The Proposal of a Blockchain-based architecture for transparent certificate handling," in *Business Information Systems Workshops. BIS 2018. Lecture Notes in Business Information Processing* 5. eds W. Abramowicz, and A. Paschke (Cham: Springer), 339. doi: 10.1007/978-3-030-048 49-5_16

Guan, W., Ni, Z., Hu, Y., Liang, W., Ou, C., He, J., et al. (2020). Clinical characteristics of coronavirus disease 2019 in China. *N. Engl. J. Med.* 382, 1708–1720. doi: 10.1056/NEJMoa2002032

Hale, J. E., Hale, P., and Dulek, E. (2006). Decision processes during crisis response: an exploratory investigation. *J. Manag. Issues* 18, 301–320. Available online at: https://www.semanticscholar.org/paper/Decision-Processes-during-Crisis-Response%3A-An-Hale-Hale/361c9c1ec210ef3b4ec761f8f056f52d25022af1

Halim, N. S. A., Rahman, M. A., Azad, S., and Kabir, M. N. (2017). "Recent Trends in Information and Communication Technology," in IRICT 2017. *Lecture Notes on Data Engineering and Communications Technologies 5,* eds F. Saeed, N. Gazem, S. Patnaik, A. Saed, F. Mohammed (Cham: Springer), 739–746.

Harrison, J. P., Harrison, R. A., and Smith, M. (2008). Role of information technology in disaster medical response. *Health Care Manager* 27, 307–313. doi: 10.1097/HCM.0b013e31818b95c7

Hart, G. R., Nartowt, B. J., Muhammad, W., Liang, Y., Huang, G. S., and Deng, J. (2019). Stratifying ovarian cancer risk using personal health data. *Front. Big Data* 2:24. doi: 10.3389/fdata.2019.00024

Heston, T. (2017). *A Case Study in Blockchain Healthcare Innovation. Authorea Working Paper No AUTHOREA_213011_3643634*. Available online at: https://ssrn.com/abstract=3077455 (accessed March 29, 2020).

Heymann, D., and Shindo, N. (2020). COVID-19: what is next for public health? *Lancet* 395, 542–545. doi: 10.1016/S0140-6736(20)30374-3

Hoy, M. B. (2017). An introduction to the blockchain and its implications for libraries and medicine. *Med. Ref. Serv. Quart.* 36, 273–279. doi: 10.1080/02763869.2017.1332261

Hu, Z., Song, C., Xu, C., Jin, G., Chen, Y., Xu, X., et al. (2020). Clinical characteristics of 24 asymptomatic infections with COVID-19 screened among close contacts in Nanjing, China. *Sci. China Life Sci.* 63, 706–711. doi: 10.2139/ssrn.3543598

Huang, C., Wang, Y., Li, X., Ren, L., Zhao, J., Hu, Y., et al. (2020). Clinical features of patients infected with 2019 novel coronavirus in Wuhan, China. *Lancet* 395, 497–506. doi: 10.1016/S0140-6736(20)30183-5

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., and Akella, V. (2019). Blockchain research, practice and policy: applications, benefits, limitations, emerging research themes and research agenda. *Int. J. Inform. Manag.* 49, 114–129. doi: 10.1016/j.ijinfomgt.2019.02.005

Jatmiko, W., Arsa, D. M. S., Wisesa, H., Jati, G., and Ma'sum, M. A. (2016). A Review of Big Data Analytics in the Biomedical Field. in: *International Workshop on Big Data and Information Security (IWBIS)*. (Jakarta), 31–41. doi: 10.1109/IWBIS.2016.7872846

Johnson, M., Jones, M., Shervey, M., Dudley, J. T., and Zimmerman, N. (2019). Building a secure biomedical data sharing decentralized app (DApp): tutorial. *J. Med. Int. Res.* 21:e13601. doi: 10.2196/13601

Juma, C. (2016). *Innovation and Its Enemies: Why People Resist New Technologies. New York, NY: Oxford University Press.* doi: 10.1093/acprof:oso/9780190467036.001.0001

Jung, S., Akhmetzhanov, A. R., Hayashi, K., Linton, N. M., Yang, Y., Yuan, B., et al. (2020). Real-time estimation of the risk of death from novel coronavirus (COVID-19) infection: inference using exported cases. *J. Clin. Med.* 9:523. doi: 10.3390/jcm9020523

Kanungo, T., Mount, D. M., Netanyahu, N., Piatko, C. D., Silverman, R., and Wu, A. Y. (2002). An efficient k-means clustering algorithm: analysis and implementation. *IEEE Trans. Pattern Anal. Mach. Intell.* 24, 881–892. doi: 10.1109/TPAMI.2002.1017616

Lei, J., Li, J., Li, X., and Qi, X. (2020). CT imaging of the 2019 novel coronavirus (2019-nCoV) pneumonia. *Radiology* 295, 202–207. doi: 10.1148/radiol.2020200236

Li, L., and Ulaganathan, M. N. (2017). Design and development of a crowdsourcing mobile app for disaster response. *2017 25th International Conference on Geoinformatics* (Buffalo, NY), 1–4. doi: 10.1109/GEOINFORMATICS.2017.8090943

Lipsitch, M., Swerdlow, D. L., and Finelli, L. (2020). Defining the epidemiology of COVID-19 — studies needed. *N. Engl. J. Med.* 382, 1194–1196. doi: 10.1056/NEJMp2002125

Litjens, G., Kooi, T., Bejnordi, B., Setio, A., Ciompi, F., Ghafoorian, M., et al. (2017). A survey on deep learning in medical image analysis. *Med. Image Anal* 42, 60–88. doi: 10.1016/j.media.2017.07.005

Lu, H. (2020). Drug treatment options for the 2019-new coronavirus (2019-nCoV). *Biosci. Trends* 14, 69–71. doi: 10.5582/bst.2020.01020

Lu, Y. (2017). Industry 4.0: a survey on technologies, applications and open research issues. *J. Indus. Inform. Integr.* 6, 1–10. doi: 10.1016/j.jiii.2017.04.005

Mackey, T., Bekki, H., Matsuzaki, T., and Mizushima, H. (2020). Examining the potential of blockchain technology to meet the needs of 21st-century japanese health care: viewpoint on use cases and policy. *J. Med. Internet Res.* 22:e13649. doi: 10.2196/13649

Mackey, T. K., Kuo, T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., et al. (2019). 'Fit-for-purpose?' – challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC Med.* 17:68. doi: 10.1186/s12916-019-1296-7

Magyar, G. (2017). "Blockchain: Solving the privacy and research availability tradeoff for EHR data: a new disruptive technology in health data management," *2017 IEEE 30th Neumann Colloquium (NC).* (IEEE: Budapest), 135–140. doi: 10.1109/NC.2017.8263269

Mahase, E. (2020). Coronavirus: covid-19 has killed more people than SARS and MERS combined, despite lower case fatality rate. *BMJ* 368:m641. doi: 10.1136/bmj.m641

Moorthy, V., Henao Restrepo, A. N., Preziosi, M., and Swaminathan, S. (2020). Data sharing for novel coronavirus (COVID-19). *Bull. World Health Organ.* 98:150. doi: 10.2471/BLT.20.251561

National Health Service (2020). *'Your NHS Needs You' – NHS call for volunteer army*. Available online at: https://www.england.nhs.uk/2020/03/your-nhs-needs-you-nhs-call-for-volunteer-army/ (accessed April 7, 2020).

Ølnes, S., Ubacht, J., and Janssen, M. (2017). Blockchain in government: benefits and implications of distributed ledger technology for information sharing. *Gov. Inf. Q.* 34, 355–364. doi: 10.1016/j.giq.2017.09.007

Ong, S. W. X., Tan, Y. K., Chia, P. Y., Lee, T. H., Ng, O. T., Wong, M. S. Y., et al. (2020). Air, Surface Environmental, and Personal protective equipment contamination by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) from a symptomatic patient. *JAMA* 323, 1610–1612. doi: 10.1001/jama.2020.3227

Oxford Analytica (2020). *Virus testing will be key to lockdown exit strategies.* Available online at: https://www.emerald.com/insight/content/doi/10.1108/OXAN-DB251630/full/html (accessed April 7, 2020).

Pandey, A., Atkins, K. E., Medlock, J., Wenzel, N., Townsend, J. P., Childs, J. E., et al. (2014). Strategies for containing Ebola in West Africa. *Science* 346, 991–995. doi: 10.1126/science.1260612

Pānescu, A., and Manta, V. (2018). Smart contracts for research data rights management over the ethereum blockchain network. *Sci. Technol. Libr.* 37, 235–245. doi: 10.1080/0194262X.2018.1474838

Paules, C. I., Marston, H. D., and Fauci, A. S. (2020). Coronavirus infections—more than just the common cold. *JAMA* 323, 707–708. doi: 10.1001/jama.2020.0757

Peeri, N. C., Shrestha, N., Rahman, M. S., Zaki, R., Tan, Z., Bibi, S., et al. (2020). The SARS, MERS and novel coronavirus (COVID-19) epidemics, the newest and biggest global health threats: what lessons have we learned? *Int. J. Epidemiol.* 49, 717–726. doi: 10.1093/ije/dyaa033

Pilkington, M. (2017). Can blockchain improve healthcare management? *Consumer Medical Electronics and the IoMT. SSRN Electr. J.* doi: 10.2139/ssrn.3025393

Pirtle, C., and Ehrenfeld, J. (2018). Blockchain for healthcare: the next generation of medical records? *J. Med. Syst.* 42:172. doi: 10.1007/s10916-018-1025-3

Pratama, F., and Mutijarsa, K. (2018). "Query support for data processing and analysis on ethereum blockchain," in *2018 International Symposium On Electronics And Smart Devices (ISESD)* (Bandung), 1–5. doi: 10.1109/ISESD.2018.8605476

Public Health England (2020). *Coronavirus (COVID-19): What does a contact tracer do? - Public health matters.* Available online at: https://publichealthmatters.blog.gov.uk/2020/06/04/coronavirus-covid-19-what-does-a-contact-tracer-do/ (accessed June 18, 2020).

Quinto, J., and Lim, A. (2016). Toward developing a humanitarian crowdsourcing model: enabling medical and disaster response through digital collaboration. *Clim. Disaster Dev. J.* 2, 1–10. doi: 10.18783/cddj.v002.i01.a01

Rajdev, M., and Lee, K. (2015). "Fake and Spam Messages: Detecting Misinformation During Natural Disasters on Social Media," in *2015 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT)* (Singapore), 17–20. doi: 10.1109/WI-IAT.2015.102

Ruan, Q., Yang, K., Wang, W., Jiang, L., and Song, J. (2020). Clinical predictors of mortality due to COVID-19 based on an analysis of data of 150 patients from Wuhan, China. *Inten. Care Med.* 46, 846–848. doi: 10.1007/s00134-020-06028-z

Saberi, S., Kouhizadeh, M., Sarkis, J., and Shen, L. (2018). Blockchain technology and its relationships to sustainable supply chain management. *Int. J. Prod. Res.* 57, 2117–2135. doi: 10.1080/00207543.2018.1533261

Samir, E., Azab, M., and Jung, Y. (2019). "Blockchain Guided Trustworthy Interactions for Distributed Disaster Management," in *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON).* (Vancouver, BC), 0241–0245. doi: 10.1109/IEMCON.2019.8936147

Sanjana, P., Sindhu, M., and Sethumadhavan, M. (2018). On blockchain applications: hyperledger fabric and ethereum. *Int. J. Pure Appl. Math.* 118, 2965–2970.

Schwab, K., and Davis, N. (2017). *Shaping The Fourth Industrial Revolution. 1st Edn.* New York, NY: Penguin Random House.

Seba, A., Nouali-Taboudjemat, N., Badache, N., and Seba, H. (2019). A review on security challenges of wireless communications in disaster emergency response and crisis management situations. *J. Netw. Comput. Appl.* 126, 150–161. doi: 10.1016/j.jnca.2018.11.010

Sharma, A., Liu, X., Yang, X., and Shi, D. (2017). A patch-based convolutional neural network for remote sensing image classification. *Neural Netw.* 95, 19–28. doi: 10.1016/j.neunet.2017.07.017

Shi, H., Han, X., Jiang, N., Cao, Y., Alwalid, O., Gu, J., et al. (2020). Radiological findings from 81 patients with COVID-19 pneumonia in Wuhan, China: a descriptive study. *Lancet Infect. Dis.* 20, 425–434. doi: 10.1016/S1473-3099(20)30086-4

Shklovski, I., Palen, L., and Sutton, J. (2008). "Finding community through information and communication technology in disaster response," in *Proceedings of the 2008 ACM conference on Computer supported cooperative work (CSCW '08). Association for Computing Machinery* (New York, NY: CSCW), 127–136. doi: 10.1145/1460563.1460584

Singh, P. K., Singh, R., Nandi, S. K., and Nandi, S. (2019). "Managing smart home appliances with proof of authority and blockchain," in *Innovations for Community Services. I4CS 2019. Communications in Computer and Information Science*, eds K. H. Lüke, G., Erfurth C., and Fahrnberger G. (Springer, Cham), 1041. doi: 10.1007/978-3-030-22482-0_16

Spector, T. (2020). *New symptom tracking app aims to slow spread of coronavirus.* Available online at: https://www.kcl.ac.uk/news/new-symptom-tracking-app-aims-to-slow-spread-of-coronavirus (accessed April 12, 2020).

Tambo, E., Ugwu, E. C., and Ngogang, J. Y. (2014). Need of surveillance response systems to combat Ebola outbreaks and other emerging infectious diseases in African countries. *Infect. Dis. Poverty* 3:29. doi: 10.1186/2049-9957-3-29

The Publication Office of the European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Off. J. Eur. Union* 119, 1–88.

Troy, D. A., Carson, A., Vanderbeek, J., and Hutton, A. (2008). Enhancing community-based disaster preparedness with information technology. *Disasters* 32, 149–165. doi: 10.1111/j.1467-7717.2007.01032.x,

UK Government (2018). *Data Protection Act 2018*. Available online at: http://www.legislation.gov.uk/ukpga/2018/12/part/2/chapter/2/enacted (accessed March 29, 2020).

Vinck, P., Pham, P. N., Bindu, K. K., Bedford, J., and Nilles, E. J. (2019). Institutional trust and misinformation in response to the 2018–19 Ebola outbreak in North Kivu, DR Congo: a population-based survey. *Lancet Infect. Dis.* 19, 529–536. doi: 10.1016/S1473-3099(19)30063-5

Wang, S. C. (2003). "Artificial Neural Network. In: Interdisciplinary Computing in Java Programming,". *The Springer International Series in Engineering and Computer Science* (Boston, MA: Springer), 743. doi: 10.1007/978-1-4615-0377-4_5

Wang, W., Tang, J., and Wei, F. (2020). Updated understanding of the outbreak of 2019 novel coronavirus (2019-nCoV) in Wuhan, China. *J. Med. Virol.* 92, 441–447. doi: 10.1002/jmv.25689

Wang, Y., Lahiri, S. K., Chen, S., Pan, R., Dillig, I., Born, C., et al. (2019). Formal specification and verification of smart contracts for azure blockchain. *arXiv.org:1812.08829 [cs.PL]*.

Wong, J. E. L., Leo, Y. S., and Tan, C. C. (2020). COVID-19 in Singapore—current experience: critical global issues that require attention and action. *JAMA* 323, 1243–1244. doi: 10.1001/jama.2020.2467

Woolhouse, M. E. J., Rambaut, A., and Kellam, P. (2015). Lessons from Ebola: improving infectious disease surveillance to inform outbreak management. *Sci. Transl. Med.* 307:307rv5. doi: 10.1126/scitranslmed.aab0191

World Health Organisation (2020). *Household transmission investigation protocol for coronavirus disease 2019 (COVID-19)*. Available online at: https://apps.who.int/iris/bitstream/handle/10665/331464/WHO-2019-nCoV-HHtransmission-2020.3-eng.pdf (accessed March 24, 2020).

Worley, C., and Skjellum, A. (2018). "Blockchain tradeoffs and challenges for current and emerging applications: generalization, fragmentation, sidechains, and scalability," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (Halifax, NS), 1582–1587. doi: 10.1109/Cybermatics_2018.2018.00265

Wu, Y., Chen, C., and Chan, Y. (2020). The outbreak of COVID-19. *J. Chin. Med. Assoc.* 83, 217–220. doi: 10.1097/JCMA.0000000000000270

Xiang, Y., Yang, Y., Li, W., Zhang, L., Zhang, Q., Cheung, T., et al. (2020). Timely mental health care for the 2019 novel coronavirus outbreak is urgently needed. *Lancet Psychiatry* 7, 228–229. doi: 10.1016/S2215-0366(20)30046-8

Xu, Z., Shi, L., Wang, Y., Zhang, J., Huang, L., Zhang, C., et al. (2020). Pathological findings of COVID-19 associated with acute respiratory distress syndrome. *Lancet Respir. Med.* 8, 420–422. doi: 10.1016/S2213-2600(20)30076-X

Yue, X., Wang, H., Jin, D., Li, M., and Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* 40:218. doi: 10.1007/s10916-016-0574-6

Zhang, X., Zhao, H., Zhang, S., and Li, R. (2019). A novel deep neural network model for multi-label chronic disease prediction. *Front. Genet* 10:351. doi: 10.3389/fgene.2019.00351

Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2017). "An overview of blockchain technology: architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data. BigData Congress.* (Honolulu, HI). doi: 10.1109/BigDataCongress.2017.85

Zhu, N., Zhang, D., Wang, W., Li, X., Yang, B., Song, J., et al. (2020). A novel coronavirus from patients with pneumonia in China. *N. Engl. J. Med.* 382, 727–733. doi: 10.1056/NEJMoa2001017