Blockchain-enabled Telehealth Services using Smart Contracts

H. R. Hasan*, K. Salah*, R. Jayaraman†, I. Yaqoob*, M. Omar†, and S. Ellahham‡
*Department of Electrical Engineering and Computer Science,
†Department of Industrial & Systems Engineering,
Khalifa University of Science and Technology, Abu Dhabi, UAE.
‡Heart & Vascular Institute, Cleveland Clinic Abu Dhabi, UAE.

***Abstract*—Telehealth has gained a huge traction during the Coronavirus (COVID-19) pandemic. Telehealth enables physicians and medical care providers to remotely care for patients and monitor their symptoms. Today's telehealth systems fall short in providing transparent, immutable, traceable, auditable, secure, and trustworthy services. In addition, they are centralized and subject to the single point of control and failure. In this paper, we present, study, and evaluate a blockchain-based solution and framework to overcome the aforementioned challenges. We demonstrate how specifically three important telehealth services; namely, teleconsultation, drug administration, and medical testing can be enhanced using blockchain technology. Our proposed solution also ensures integrity, immutability, accountability, and non-repudiation for telehealth transactions initiated by multiple actors. For storing and keeping track of large-size digital content, such as images and audio and video recordings of telehealth service sessions, our proposed solution is integrated with off-chain storage systems including cloud storage or a decentralized storage system as that of the Interplanetary File System (IPFS). The registered participants are provided with access privileges based on their roles to ensure that restrictions are enforced on-chain. Smart contracts are developed to maintain data provenance and generate reliable alerts and notifications. The implementation and testing details of the algorithms are presented. We discuss, compare, and analyze the security features of our solution. The smart contracts code is made publicly available on GitHub.**

***Index Terms*—Telehealth; Telemedicine; COVID-19; Blockchain; Ethereum Smart Contracts; Security; Traceability**

I. Introduction

The Coronavirus (COVID-19) outbreak has begun in late 2019. It is confronting and challenging the existing healthcare systems. Recently, many doctors living in the U.S. felt the urge to step in during the COVID-19 Indian crisis [1]. This was made possible through telehealth services and remote consultations. Although telehealth is not a new technology, the spread of the pandemic urged the healthcare industry to work around the hurdles and expedite its adoption worldwide [2]. Telehealth has proven to be a practical, convenient, and beneficial tool in many healthcare services (e.g., during pregnancy and for aiding diabetic and psychiatric patients) [3], [4], [5]. Shifting from face-to-face to remote and virtual interactions can help to maintain ongoing care and treatment despite travel restrictions and geographic boundaries.

The unprecedented challenges posed by the pandemic have led to redesign the healthcare model to triage and timely deliver services while reducing the risk of contamination and transmission of COVID-19 [6]. Technology and expense are important factors that can play a major role in curbing and limiting the integration and interoperability of telehealth into the healthcare model [7]. Technological limitations include both hardware and software as well as internet access. Personnel healthcare devices must be leveraged to enable healthcare providers to provide telehealth services smoothly without depending on special technological features or devices [8]. The lack of staff trained to provide medical services remotely was another hurdle that COVID-19 proved can be overcome. All medical correspondents should be trained on the telemedicine platforms and devices to ensure that proper consultation is received adequately by the patient [6]. Privacy and medical confidentiality of the patients are also some of the challenges that exist in today's telehealth systems. However, with the advancement in technology and cybersecurity, telehealth privacy and security can be sustained. Consequently, telehealth has proven to be a beneficial technology that has the potential to mitigate the spread of the infectious COVID-19 [9]. Doctors and medical practitioners can reach patients at the convenience of their own homes using telehealth. Furthermore, when resources are scarce and protective personnel equipment (PPEs) are limited in quantities, telehealth can greatly reduce the risk of contamination and the spread of infections [8]. Furthermore, it helps in providing ongoing care and treatment regardless of geographic location.

Blockchain is an immutable and tamper-proof ledger which keeps its records in a shared ledger [10]. It is a peer-to-peer network that has immutable event logs which are an important tool for history tracking and tracing. During the pandemic, blockchain has proven to be an integral part in fighting against COVID-19 [11]. In this paper, we propose a blockchain-based telehealth system. It is a decentralized solution which aims to respect the confidentiality of the healthcare industry and the privacy of its users. To implement trust, accountability, and transparency, we use a private blockchain that respects the confidentiality of the patients and the medical practitioners. Our solution incorporates digital smart contracts that are programmable to register users and achieve three main goals of the telehealth industry such as teleconsultation, drug administration, and medical testing for the patients remotely. Our proposed solution is a generic telehealth system which can be used in different medical use case scenarios and applications with minimal efforts and modifications. In our solution, each actor is held accountable for its actions using his/her own on-chain digital signatures. Each executed function creates an event which is logged and timed for reference and history tracking.

A. Related Works and Contributions

Telehealth equipped with the intrinsic security features of the blockchain technology has been showing promising results during the pandemic as can be seen in [12], [13], [14], [15] [16]. Herein, we review the existing works focused on the integration of telehealth with blockchain technology.

The authors in [17] presented a telehealth architecture that incorporates blockchain technology. The solution involved multi-access edge computing (MEC), elliptic curve cryptography, Internet of things (IoT), and Fifth-generation (5G) communications technology. They mainly focused on the service architecture. Hence, there were no details mentioned on the smart contracts involved, code, testing, or implementation details. However, they have created a scenario to test their service architecture using Raspberry pi devices and the Hyperledger Fabric. They have shown great details on the IoT devices and the MEC nodes.

On the other hand, the authors in [18] highlighted the importance of using blockchain technology to track physicians' burnout and stress level during the COVID-19 pandemic. The research work aims to spot the light on frontline workers and showcases how blockchain can be leveraged to track their health and mental status especially with the additional burden of scarce and limited resources. They showcase the importance of blockchain and telehealth in monitoring chronically ill patients and in maintaining compliance standards in administrative processes. However, this study lacks implementation details. Also, the study emphasizes the importance of a permissioned blockchain network to comply with the Health Insurance Portability and Accountability Act (HIPAA).

Since it is crucial to monitor the early signs and symptoms of COVID-19, the authors of [19] presented a mobile health care system that asynchronously provides patients with the needed medical attention. The patients use their mobile devices for ongoing real-time monitoring. Other patients can use their smartphones for an early diagnosis based on their communicated symptoms. The solution depends on smartphones and blockchain technology. However, there is no detailed implementation information on the use of programmable smart contracts or testing information.

To overcome the efficiency and technical issues faced during the pandemic with regards to convalescent plasma (CP) transfusion, the authors in [20] proposed a specialized framework. The study highlights the importance of telehealth and the needs of critical patients that require a speedy transfusion. Hospitals offering telehealth vary in terms of management policies. Hence, to overcome the interoperability issues and focus only on finding a donor and match pair, the authors present a framework that focuses mainly on telehealth for convalescent plasma (CP) transfusion across centralized and decentralized hospitals.

In summary, the aforementioned works agree on the importance of telehealth and its contributions. For example, the authors in [21], [22], [23], [24] emphasized on the role of telehealth when there was an acute shortage in resources such as PPE, ventilators, medical supplies and devices. The pandemic helped to rapidly overcome hurdles such as expenses, reimbursement, policies and management, and paved the future of telehealth. However, the current literature lacks enough research on blockchain-based telehealth solutions and the opportunities that can be acquired when a complete solution is designed and implemented using programmable smart contracts. High-performance patient data management with preserved data security, privacy, accessibility, availability, and provenance health records are all features that can be achieved using the distributed blockchain ledger. The peer-to-peer network offers no manipulation on the patient and doctor data using its tamper-proof logs and restrictions on function executors [14]. Our solution leverages blockchain features to ensure transparency, privacy, and security.

The main contributions of this paper can be summarized as follows:

- We propose a blockchain-based decentralized solution for telehealth services, which does not depend on third parties or centralized servers.
- We show how to integrate our decentralized on-chain framework with off-chain storage systems such as cloud storage or a decentralized storage system as that of the Interplanetary File System (IPFS). Off-chain storage is used for storing and keeping track of large-size digital content such as video calls of telehealth sessions.
- We develop four smart contracts along with six algorithms to register the participating entities and offer the patients different telehealth services in a manner that is transparent, traceable, auditable, private, secure, and trustworthy.
- We implement and test the developed smart contracts for three different telehealth services: teleconsultation, drug administration, and medical testing. We make the code publicly available on GitHub[1].
- Our proposed blockchain-based telehealth solution is generic enough to be adapted into different use case scenarios with minimal efforts and modifications.

The rest of the paper is organized as follows. Section II presents the design details of the proposed blockchain-based solution followed by the implementation details in section III including the smart contracts and algorithms. Section IV presents the testing details followed by section V which showcases the security analysis and comparison with the existing solutions along with discussing generalization aspects. Section VI concludes the paper.

[1] https://github.com/smartcontract694/telehealth/blob/main/Code

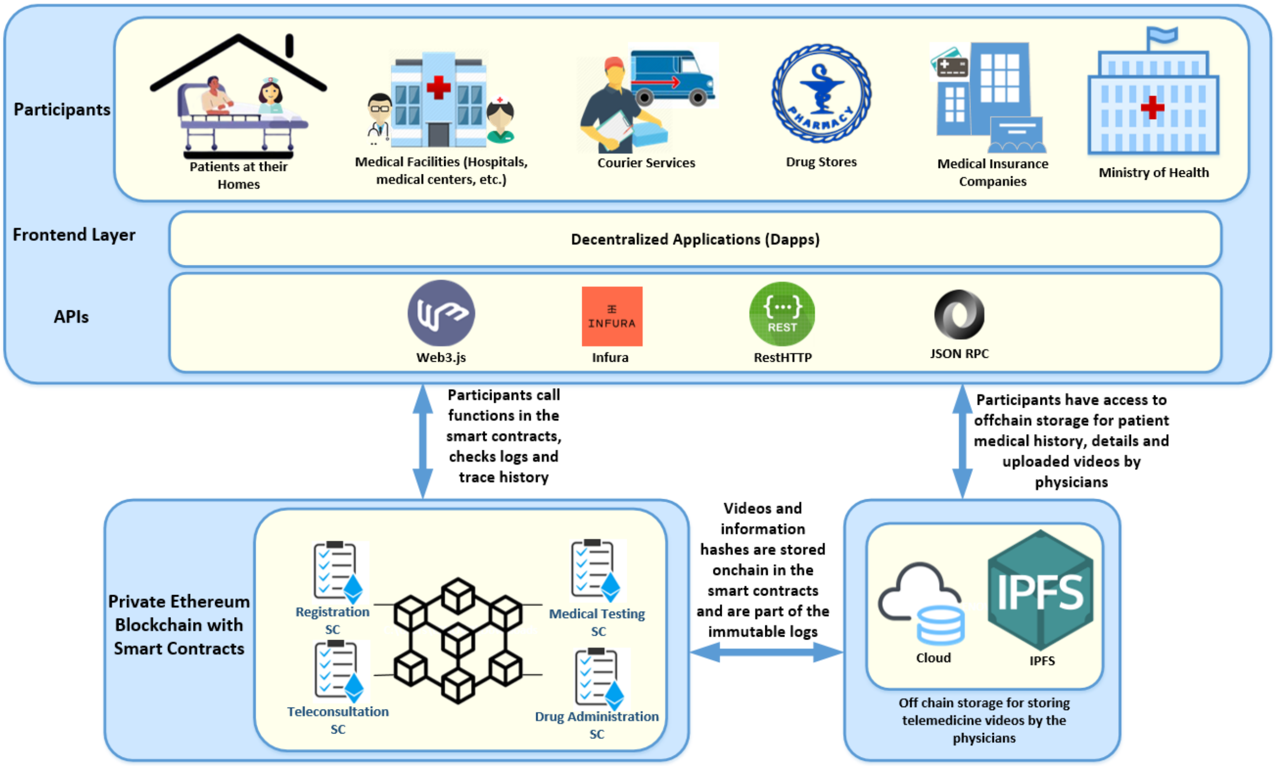

Fig. 1: Blockchain-based system architecture for telehealth

II. System Design

This section describes the details of our system design. It explains the breakdown of our solution and presents the sequence of events in the smart contracts and solidity code. Figure 1 shows the components of the proposed blockchain-based solution. The system depends on the doctors and the medical practitioners who aim to provide in-home treatment services remotely. The doctors rely on teleconferencing calls to see and hear the patients and assess their needs. Medical drugs are administered as needed as well as medical tests are carried out when necessary. Courier services are also used to make treatment and testing possible. The video calls are all recorded and uploaded on a cloud storage or a decentralized storage platform such as IPFS. The system is managed, traced, and tracked through blockchain. The role of each part in the system is also explained below in further detail.

A. Participants

To facilitate the telehealth process on-chain, the participants need to communicate using smart contracts. As can be seen in figure 1, the participants are the patients at their own homes. Also, the figure shows the medical doctors and nurses who connect remotely to the patient. Moreover, other than the medical facilities such as hospitals and medical centers, courier services play a vital role in the process to enhance the telehealth process and facilitate in-home testing and treatments for the patients. In addition, since the practicing practitioners will require medications when needed by the patients registered, affiliated drug stores are also important participants along with the medical insurance companies to cover the cost of the treatments for the insured patients. Also, the Ministry of Health is a higher authority that ensures all the medical practitioners and drugs are authorized and registered. This assures trust and governance.

B. Frontend Layer and APIs

The participant can communicate on the chain through Decentralized Applications (DApps) which use Application Programming Interfaces (APIs) to talk to the decentralized blockchain. There are several APIs that can be used to establish good communication between the participants and the blockchain. These APIs include Web3.js, Infura, RestHTTP, and JSON RPC as can be seen in figure 1. Those APIs help in providing requests and subscriptions based responses. Infura ensures that the participants have accessed information based on the latest network updates [25]. The latest network updates include events such as the courier or the nurse reaching the patient, alerts about the patient's health and vitals, actions including the doctor uploading the recorded virtual call on the decentralized storage.

C. Smart Contracts

We develop four smart contracts. The smart contracts are written in Solidity using the Remix IDE [26]. The first smart contract (SC) is the Registration SC. The Registration SC is required to ensure that only the authorized participants can communicate on-chain and execute function calls. It has functions that register doctors, nurses, and couriers. It can also disallow a previously registered participant from gaining access privileges and executing function calls. This is done through mappings, boolean variables, and the Ethereum Addresses (EAs) of the participants. Each other smart contract from the remaining three inherits the variables and functions of the Registration SC. This is because before executing any call, the SC would check if the caller's EA is registered and authorized. The other smart contracts are used for telehealth calls (i.e., Teleconsultation SC, Medical Testing SC, and the Drug Administration SC). Their functions as well as events and flow sequence are all detailed in the following section.

D. Blockchain

A private blockchain is the core of this distributed and decentralized design. The digital ledger securely keeps a record of all the transactions and maintains a chronological history keeping reference [27]. A programmable blockchain uses smart contracts to execute logic through function calls and emitted events [28]. To protect the privacy of the patients and medical confidentiality, a private Ethereum blockchain and solidity smart contracts were used in the design and implementation. However, the design is not limited to private Ethereum blockchains such as Quorum [29], Hyperledger Besu [30] but can also be implemented on any other private blockchain including Hyperledger Fabric [31]. Ethereum private blockchains use smart contracts and can use solidity for writing smart contracts. However, they may vary with the applied consensus algorithm. For instance, Besu supports Proof-of-Authority (PoA) and Istanbul BFT (IBFT); whereas, Quorum supports Raft and Istanbul BFT [32], [29]. Besu also offers identity management through a separate component known as 'EthSigner'; whereas, Quorum does not support identity management [29], [33]. On the other hand, Fabric uses chain-codes and has very flexible plug-and-play consensus, components, and membership services [31]. Based on the requirements, needs, and implementation costs, a private blockchain can be chosen.

E. Off-chain Storage: Cloud and IPFS

Off-chain storage is used to store the recorded audio/video calls. The doctor records the virtual video calls where teleconsultation, medical testing, and drug administration take place. The video is then uploaded by the doctor onto the cloud or a decentralized storage system such as IPFS. Cloud can be used if all parties trust the cloud provider. Otherwise, a fully decentralized storage system can be used with an added level of security using proxy re-encryption [34]. This would allow multiple parties, such as the care givers and the patients to access the uploaded encrypted files securely. The hash of the recording is only used on-chain for history tracking, tracing and as a reference for the participants when needed. Another use of off-chain storage is when the courier picks up the medical kit from the patient to deliver it to the doctor. The medical kit received from the patient is first captured by the courier, uploaded on the cloud or the IPFS, then its hash is used on-chain.

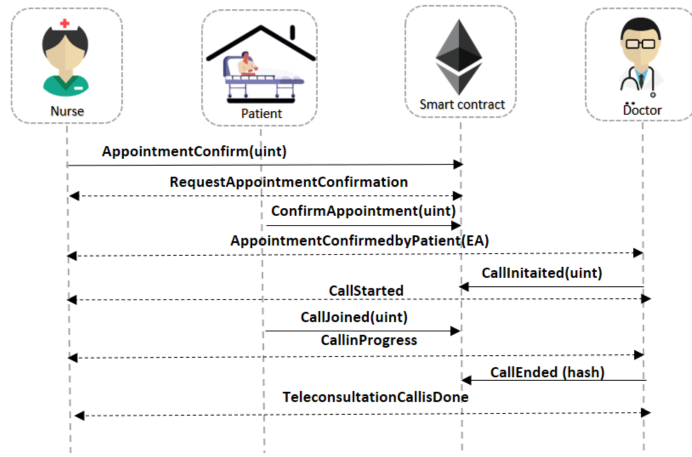

Fig. 2: Teleconsultation sequence diagram with functions calls and events

F. Teleconsultation SC

The Teleconsultation SC is designed to accommodate all requests by patients at the convenience of their homes. The registered patient, nurse, and doctor communicate on-chain and provide the patient with the consultation needed. Figure 2 shows the sequence of the function calls and the emitted events that take place in the smart contract. The sequence diagram illustrates how the nurse first confirms the appointment with the patient on-chain and waits for a response from the patient. Then the doctor starts the video call which is recorded and uploaded on the decentralized storage of the IPFS. The consultation is done through a video call between the doctor and the patient. When the call ends, the doctor then uploads the recording of the video call on the IPFS and stores the hash on-chain. The hash is kept on-chain as a reference for all the participating entities and history tracking and tracing purposes.

G. Drug Administration SC

A patient at home may require the administration of drugs under the doctor's supervision and accompanied by a nurse. Therefore, this telehealth service facilitates for the patient to have a nurse arrive at their home to administer the drugs. The remotely located practitioner must approve that the patient is qualified to take the medication. The nurse first confirms the appointment with the patient. Then the patient would wait for the nurse's arrival at the patient's home. Figure 3 shows the sequence of events in a Drug Administration SC. The nurse announces her arrival on the chain. Then the patient also agrees that the medical assistance (nurse) reached them. The doctor then starts the video call and documents the time on-chain. The nurse measures the patient's vitals which include their blood pressure, temperature, oxygen saturation, and heart rate. The vitals are examined by the doctor and the doctor would then either approve administering the drugs to the patient or refuse

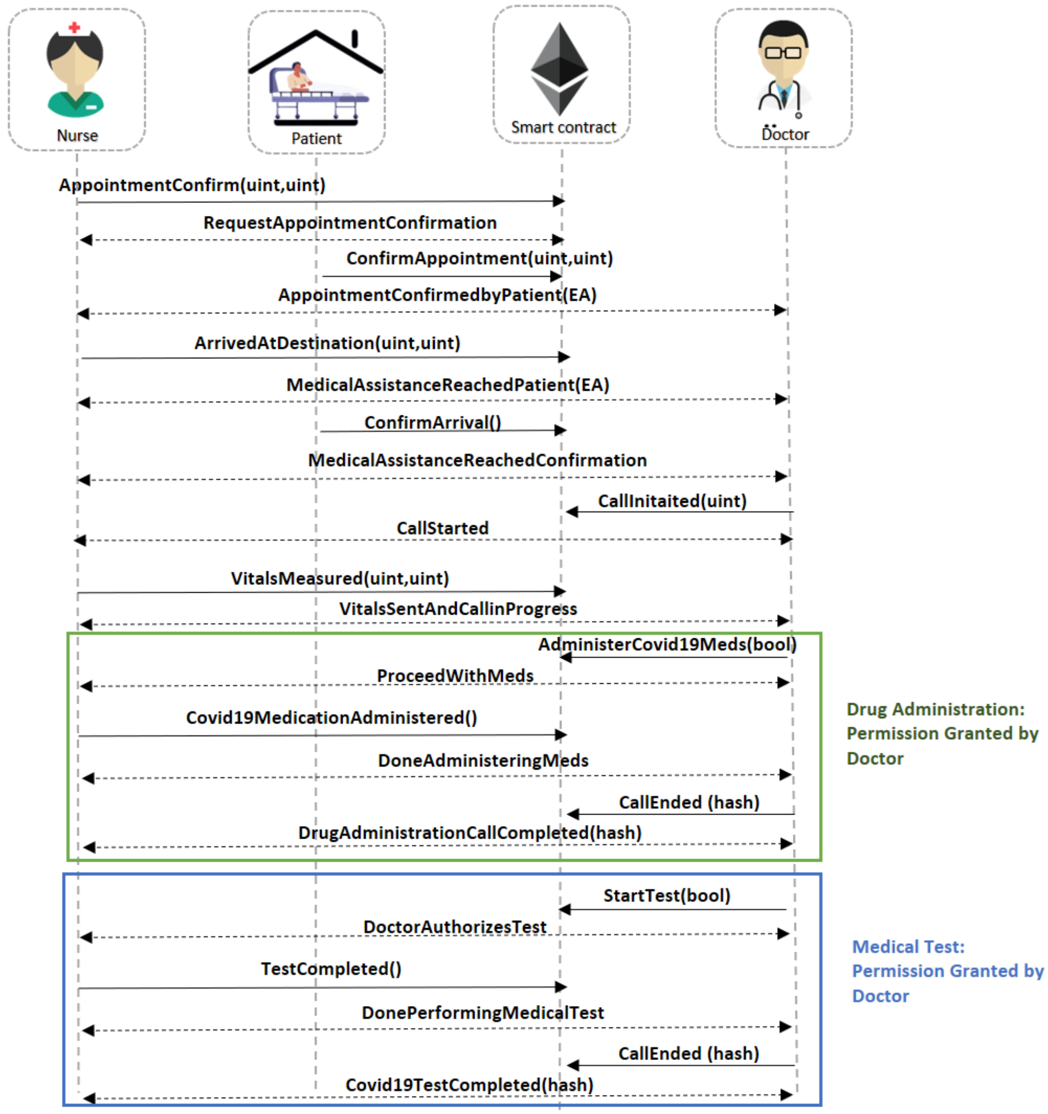

Fig. 3: Drug administration and Medical Testing SCs sequence diagram

it. The green section in figure 3 shows the sequence of events after the doctor grants the permission to administer the drugs. The nurse confirms administering the drugs to the patient which allows the doctor to end the video call. The recorded video call is then uploaded by the doctor on IPFS. The hash of the call is used on-chain to enhance tracking, tracing, and history recording. The sequence of calls and events can also be customized depending on the case and the disease cured. Furthermore, this telehealth case is not restricted to Covid-19 or infectious diseases as it can be used to administer drugs for other diseases as required by the physician.

Another possible option that the patients can opt for is having the drugs administered by themselves. To make that possible, a trusted registered courier has to transfer the medical kit to the patient for drug administration. The process at the beginning follows the same procedure as previously mentioned where the appointment is confirmed by both the nurse and the patient. Then instead of the nurse arriving at the patient's home, a medical kit arrives with a registered courier. Figure 4 shows the details and sequence of events as the courier arrives at the destination and the patient confirms on the chain the arrival of the medical kit with the courier. The role of the nurse here is just to confirm the patient's appointment. The doctor initiates the video call then requests the patient to measure the vitals. Based on the vitals measurements the doctor advises the patient to take the drugs or not. If the patient is medically fit, the doctor requests the patient to take the drugs. Then the call is ended by the registered doctor. The recording of the call is also uploaded on IPFS and its hash is added on-chain.

H. Medical Testing SC

A doctor might require a patient at home to perform a medical test to better study the perceived symptoms or to check on the body's improvement status with the prescribed

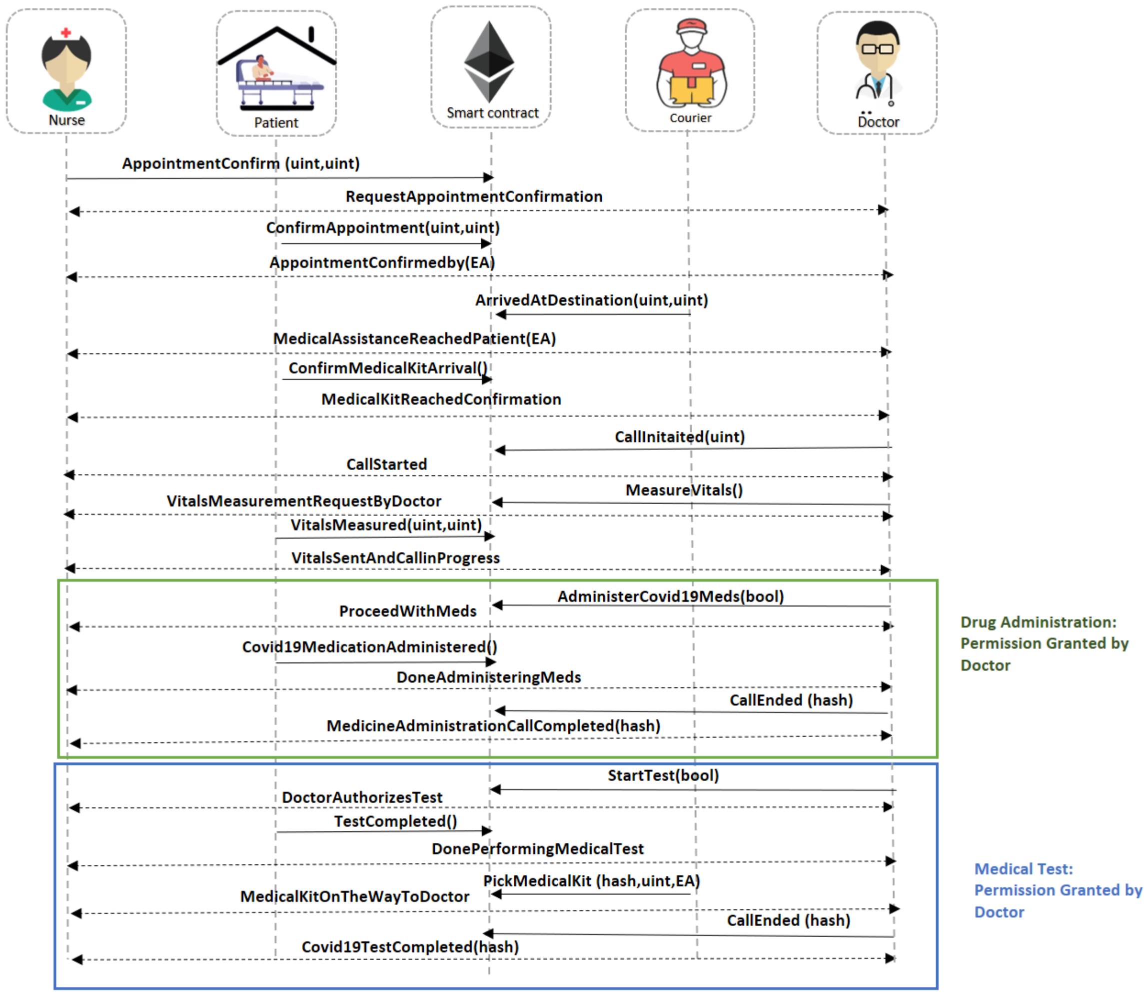

Fig. 4: Drug administration and Medical Testing SCs sequence diagram with a registered courier

medications. In all cases, the doctor needs the medical test to be performed correctly and accurately just the way it would be in the medical center or hospital. Therefore, the nurse first requests for an appointment confirmation from the patient. Then after the appointment is confirmed as can be seen in figure 3, the patient waits for the arrival of the registered nurse. When the patient confirms that the nurse has arrived, the doctor initiates the video call. The vitals are measured by the nurse to ensure that the patient is medically fit to take the test. These steps are similar to the steps taken before the drug is administered. Hence, they are common for both the medical testing SC and the drug administration SC as seen in figure 3. Based on the vitals readings measured by the attending nurse, the doctor decides if the patient can have the medical test done. If the patient is allowed by the doctor, the doctor on-chain executes a function called $StartTest(bool)$ which shows that the doctor authorized the patient to take the test. The nurse then performs the test and announces it on-chain. At the end, the recorded video call is uploaded on a decentralized storage such as IPFS and the hash is used on-chain for history recording, tracking and tracing. The sequence of function calls and events are highlighted in figure 3.

The medical testing can also be performed by the patient without the nurse and under the supervision of the doctor. To do so, the registered courier delivers a medical kit to the patient. The medical kit will have the needed medical equipment for the patient to perform the test. The procedure is followed like before except that now the patient waits for the arrival of the medical kit by the courier after the appointment is confirmed. Figure 4 shows how the courier announces the arrival at the destination followed by a confirmation by the patient. The doctor then initiates the call. The doctor also requests the patient to measure the vitals. If the patient is medically fit, the doctor authorizes the patient to perform the medical test under the doctor's supervision. The test is performed while the doctor is talking and viewing exactly how the patient is following the doctor's instructions. When the test is done, the medical kit is returned by the patient to the courier and the courier takes it back to the doctor. The courier takes a photo of the medical kit package, uploads it on the IPFS storage, and then includes the IPFS hash of the uploaded image on the chain. The uploaded hash of the image ensures that the courier has taken the package from the patient and is also used for reference and history tracking purposes. The doctor then ends the call and adds the hash of the recorded video call on the chain as well.

III. Implementation Details

In this section, we present the implementation details of the three main smart contracts; namely, Teleconsultation Smart Contract (SC), Drug Administration SC, and Medical Testing SC. The code of all the telehealth SCs along with Registration SC is written in Solidity using the Remix IDE [26]. It is compiled and tested using Remix. Below are given the details of the functions, algorithms, and sequence of events that take place in the SCs. Each algorithm is accompanied by an explanation that describes how this algorithm is applied in each SC and the key differences if any exist. The algorithms are ordered based on the events. Hence, they start with the appointment confirmation and end with the virtual call terminated by the doctor. In our proof of concept implementation, we decide on going with a fully decentralized storage option. Hence, we use the IPFS hash in our code and algorithms. However, if the leading participating entities decide on cloud storage, the hash of the file stored on the cloud can be used in the place of the IPFS hash in our implementation.

A. Nurse Appointment Confirmation Request

The three main smart contracts implemented for telehealth start with the nurse requesting an appointment confirmation from the patient. Algorithm 1 shows the details of the $AppointmentConfirm$ function. This function can only be executed by the registered nurse. It takes the time and the patient Ethereum Address (EA) as parameters. Furthermore, in the Drug Administration SC and the Medical Testing SC, the function also takes the appointment type. This additional parameter helps identify if the medical assistance home service would include a nurse or only a courier. In this algorithm, the state of the contract is checked at first to ensure it is the first state as expected which is $waitingforanewappointment$. Additionally, the EA of the patient passed as a parameter is checked to ensure it is a registered patient. This function updates the contract state and emits an event to alert the patient to confirm the appointment on-chain.

B. Medical Kit or Nurse Arrival at the Destination

The Medical Testing SC and the Drug Administration SC require the arrival of the nurse to the patient's home or the arrival of the courier with a medical kit. Hence, algorithm 2 in function $ArrivedAtDestination$ is used to confirm the arrival of the medical assistance to the patient's home. This algorithm is not needed in the Teleconsultation SC as no medical nurse or courier is required to be available at the patient's home. Therefore, this function checks if the caller is a registered nurse or if it's the registered courier. Furthermore, the appointment type is checked also along with the caller's Ethereum address to ensure that the patient appointment type matches the home service they are receiving. An appointment type of '1' means that the nurse arrived and an appointment type of '2' means the patient is only expecting a medical kit with a courier. This algorithm is executed after algorithm 2 is completed and the appointment is confirmed by the patient. At the end of this algorithm, based on the appointment type, the state is updated to either $NurseArrived$ or $KitArrived$ respectively. Additionally, an event is emitted to announce that the medical assistance reached the registered patient.

Algorithm 1: Nurse Appointment Confirmation Request

Input : patient, caller, nurse, time, state

$patient$ holds the Ethereum Address of the patient.
$caller$ holds the Ethereum Address of the function caller.
$nurse$ holds the Ethereum Address of the registered nurse.
$state$ is a variable that has the contract state.
$RegisteredPatientList$ is a list that has all the registered patients.
if $caller == nurse \wedge state == waitingForNewApp \wedge patient \in RegisteredPatientList$ **then**
    $currentPatient = patient$
    Emit a Request Appointment Confirmation alert using the patient EA and time.
    $state = appConfirmedbyNurse$
end
else
    Show an error and return the contract to the previous state.
end

The execution of this function notifies the patient that he/she needs to confirm the arrival of the medical assistance to the home before the doctor can initiate a video call. Therefore, the function $ConfirmArrival$ or $ConfirmMedicalKitArrival$ can only be executed by the registered patient after algorithm 4 is completed. The state would then be updated to $NurseArrivalConfirmation$ or $KitArrivalConfirmation$ respectively. Also, an event is emitted that announces the medical assistance arrival is confirmed by the patient.

C. Vitals Measurement

After the video call is joined by the patient, depending on the purpose of the call, the patient's vitals might be needed. The Drug Administration SC and the Medical Testing SC require that the patient's vitals are measured and sent on-chain to proceed. If a nurse is available with the patient at home, then the nurse automatically executes algorithm 3 and sends the vitals. However, if the patient is alone at home without a nurse and received the medication or medical kit with the courier, the patient would be guided by the doctor and told on-chain to measure the vitals. The patient would then execute

Algorithm 2: Medical Kit or Nurse Arrival at the Destination

Input : caller, time, nurse, state, courier, appType

$nurse$ holds the Ethereum Address of the registered nurse
$courier$ holds the Ethereum Address of the registered courier
$currentPatient$ holds the Ethereum Address of the regsitered patient
$caller$ holds the Ethereum Address of the function caller
$state$ is a variable that has the contract state
$appType$ is a variable that holds the appoinmtment type of 1 (nurse arrives) or 2 (only courier with the kit)
if $(caller == nurse \lor caller == courier) \land state == appConfirmedbyPatient$ **then**
    Emit an event stating that the medical assistance reached patient $currentPatient$
    if $appType == 1$ **then**
        $state = NurseArrived$
    end
    else
        $state = KitArrived$
    end
end
else
    Preview an error and return the contract to the previous state.
end

algorithm 3 and send their vitals. The vitals measured include blood pressure, heart rate, temperature, and oxygen saturation. Hence, algorithm 3 shows how the vitals are sent on-chain by either the nurse or the patient. Furthermore, the state is updated to $VitalsMeasured$ and an event is emitted to notify all the listening parties about the new update. Following the vitals measurement, the doctor would then authorize proceeding with the medical test or drug administration if the patient is fit. If the vitals are not within the normal range, the doctor will not authorize the patient to proceed and the call would end as would be explained in algorithm 6.

D. Covid19 Drugs Administration

For the drugs to be administered or the medical test to be done, the patient must be fit and their vitals should be normal. Therefore, algorithm 4 allows only the doctor to make this call and to provide an authorization on-chain for the patient to receive the drugs in the Drug Administration SC. The same logic is also applied in the Medical Testing SC. This would change the state to $AuthorizedToTakeMeds$ accordingly. If the patient is not authorized, then the state is updated to $NotAuthorizedToTakeMeds$. In both cases mentioned, events are emitted to update the listening par-

Algorithm 3: Vitals Measurement

Input : caller, time, patient, state,BpHR, TOx

$currentPatient$ holds the Ethereum Address of the registered patient
$caller$ holds the Ethereum Address of the function caller
$state$ is a variable that has the contract state
$BpHR$ is a variable that holds the blood pressure and the heart rate.
TOx is a variable that stores the temperature and the oxygen saturation.
if $(caller == nurse \land state == CallJoinedbyPatient) \lor (caller == currentPatient \land state == VitalsMeasurementRequest)$ **then**
    Emit an event stating that the vitals have been sent and the call is in progress
    $state = VitalsMeasured$
end
else
    Preview an error and return the contract to the previous state.
end

Algorithm 4: Administer Covid19 Drugs

Input : caller, result, doctor, state

$doctor$ holds the Ethereum Address of the registered doctor
$result$ holds a boolean
$caller$ holds the Ethereum Address of the function caller
$state$ is a variable that has the contract state
if $caller == doctor \land state == VitalsMeasured$ **then**
    if $result == true$ **then**
        Emit an event stating that the patient is authorized to take the drugs
        $state = AuthorizedToTakeMeds$
    end
    else
        Emit an event showing that the authorization is not given
        $state = NotAuthorizedToTakeMeds$
    end
end
else
    Preview an error and return the contract to the previous state.
end

ties about the authorization. If the patient is authorized to take the medication or take the medical test, the function $Covid19MedicationAdministered$ or $TestCompleted$ is executed by the patient or the nurse depending on whether the patient requested a nurse along or only a courier service. This would update the state to $MedsAdminitered$ or $TestCompleted$ accordingly.

Algorithm 5: Medical Kit Pickup

Input : caller, time, courier, state, photoHash, currentPatient

$courier$ holds the Ethereum Address of the registered courier
$caller$ holds the Ethereum Address of the function caller
$state$ is a variable that has the contract state
$photoHash$ is a variable that holds the hash of the uploaded package photo by the courier
$currentPatient$ holds the Ethereum Address of the registered patient
if $caller == courier \land state == TestCompleted$ **then**
    Emit an event stating that the medical kit is on the way using the $photoHash, time, currentPatient$
    $state = MedicalKitOnTheWayToDoctor$
end
else
    Preview an error and return the contract to the previous state.
end

E. Medical Kit Pickup

The function $PickMedicalKit$ is only available in the Medical Testing SC and it follows the logic described in algorithm 5. This algorithm can only be executed by the registered courier, only when the medical test has been completed. Therefore, the EA of the caller is checked to match the EA of the courier, and the state is checked to ensure that the test has finished. The courier would take photos of the medical test packaged for delivery and would hash the photos that are uploaded on the IPFS servers. The hash of those photos is passed as an attribute in the function call along with the patient's EA and the time. An event is then emitted to update everyone on-chain that the medical kit is on its way to the doctor and the state is also updated.

F. Call Termination by the Doctor

In our smart contracts; namely, Teleconsultation, Medical Testing, and Drug Administration SCs, the video call is ended by the doctor after the purpose is achieved. Algorithm 6 shows the details of the call termination by the registered doctor. The function takes the EA of the doctor, the state, and a hash. This hash is the hash of the video call that is uploaded by the doctor to the decentralized IPFS servers. The doctor first uploads a video of the recorded virtual call, then

---

Algorithm 6: Call Ended by the Doctor

Input : caller, time, doctor, state, vidHash

$doctor$ holds the Ethereum Address of the registered doctor
$caller$ holds the Ethereum Address of the function caller
$state$ is a variable that has the contract state
$vidHash$ is a variable that holds the IPFS hash of the uploaded video call
if $caller == doctor \land state == CallJoinedbyPatient$ **then**
    Emit an event stating that the video call has ended and provide the $vidHash$
    $state = waitingForNewApp$
end
else
    Preview an error and return the contract to the previous state.
end

---

executes the algorithm and uses the hash of the uploaded video as an attribute. In this algorithm, the caller's EA is first checked to ensure that only the doctor can execute this function. Also, the state must be checked and this varies depending on the type of smart contract. In the Teleconsultation, Medical Testing, and Drug Administration SCs, the smart contract state must be either $CallJoinedbyPatient$ or $MedicalKitOnTheWayToDoctor$ or $MedsAdministered$ accordingly. Furthermore, if the patient was not allowed to take the test or the drugs, then the call would end and hence the state can also be $NotAuthorizedToTakeTest$ or $NotAuthorizedToTakeMeds$, respectively. After verifying the state, an event is emitted to announce that the video call with the hash '$vidHash$' has ended. In the end, the state of all contracts would be updated to $waitingForNewApp$ which states that the contract is ready to accept new appointments.

IV. Testing and Validation

Our blockchain-based telehealth solution consists of four smart contracts such as Registration, Teleconsultation, Drug Administration, and Medical Testing Sc. These smart contracts were tested for correct execution, expected results, and the right restrictions. The testing is done using the Remix [26] IDE. The functions can only be executed in a particular order. This is done based on the smart contract state. Each function checks for the contract state before its execution and updates it to the next one as needed. Only registered users can execute the functions based on their roles. Before testing any of the medical smart contracts, the users are first registered in the Registration SC. The following subsections show results from the testing of the smart contracts.

A. Nurse Appointment Confirmation

For any of the telehealth services such as Teleconsultation, Drug Administration or Medical Testing, a patient must first confirm their requested appointment. Hence, in the function $AppointmentConfirm$, the nurse requests the registered patient to confirm their availability on the requested appointment. Figure 5 shows the registered nurse executing the function and successfully emitting an event $RequestAppointmentConfirmation$ with the appointment time.

Fig. 5: Logs showing a successful appointment confirmation request by the nurse

B. Medical Assistance Arrival

Both the Drug Administration and Medical Testing SCs require either the nurse or the courier to arrive at the patient's home. Hence, this function in both smart contracts is tested successfully. The function $ArrivedAtDestination$ was successfully executed in the Medical Testing SC. The event $MedicalAssistanceReachedPatient$ is emitted and the patient appointment is of type '2' in the decoded input which indicates that the courier has arrived at the patient's home and not the nurse.

C. Vitals Measurement

The $VitalsMeasured$ function can be executed by the nurse or the patient depending on the appointment type. This function helps the doctor better assess if the patient can be administered the drugs or take the medical test. The function is successfully tested where the patient vitals are available in the decoded input and the event $VitalsSentandCallInProgress$ is emitted to let the doctor and all participating entities be aware of the patient vitals.

D. Drugs Administration

In the Drug Administration SC, the drugs are administered based on the vitals results and the authorization from the doctor. The function $AdministerCovid19Meds$ is executed by the doctor only and an event $ProceedWithMeds$ is emitted based on the doctor's authorization decision. In our testing, the event was emitted successfully which indicates that the patient is ready to receive the drugs.

E. Medical Kit Pickup

The medical kit is picked up from the patient by the courier once the medical test has ended. The Medical Testing SC allows the courier to execute the $PickMedicalKit$ function to indicate that the kit is picked up from the patient. The function takes the photo hash of the medical kit as well as the time of pick up and the patient's EA. The function is executed successfully and the decoded input included the photo hash as $bytes32$, 0x3fd54831f488a22b28398de0c567a3b064b937f54f81739ae9bd545967f3abab . Also, the event $MedicalKitOnTheWayToDoctor$ is emitted successfully.

F. Call Termination by the Doctor

At the end of the telehealth call, the video call is terminated by the doctor. The doctor uploads the video on IPFS and the hash is then used on-chain for tracing and tracking. The video call hash 0xe0f89ca8eae95281590977802df657506a151304234d15570c12cc26263a8b7a is part of the decoded input. The event $Covid19TestCompleted$ is emitted successfully in the logs which indicates the end of the medical test in the Medical Testing SC.

V. Discussion

In this section, we evaluate our solution using different security parameters. We also showcase how our solution is generic and can be adapted as per the need of emerging medical applications.

A. Security Analysis

Blockchain is a disruptive technology that provides intrinsic security features. It is the highlight of our solution where its characteristics are utilized to best fit the needs of our framework. It eradicates vulnerabilities and exploits that threaten trust, integrity, accountability, authorization, confidentiality, non-repudiation, and transparency. Its immutable records are tamper-proof and its logs provide provenance and help in tracing and tracking.

Integrity is a security feature that enforces trust. In our solution, the participating entities whether the medical practitioners or the patient or delivery couriers should be trusted. Hence, trust is enforced through the tamper-proof logs. The actions taken by the participating entities on-chain such as confirming appointments or administering drugs are all tamper-proof. Hence, on-chain decisions cannot be exploited.

Accountability is a vital characteristic that could clear disputes and ensure that participating entities are held responsible for their actions. Each action on-chain is signed digitally using the Ethereum Address (EA) of the caller. This imposes non-repudiation. Each participating entity has a unique EA and all transactions are signed by the caller's address.

Moreover, authorization is mandatory in our solution as the system is to be used in the medical field where the patient's information must be treated with confidentiality. Only the authorized parties can execute the function calls. This is ensured in our solution by associating every EA with an

TABLE I: Comparison with other telehealth frameworks

Solution	Features	Storage	Description	Blockchain Role	Smart Contracts	Blockchain Type
[17]	Uses multi-access edge computing (MEC), elliptic curve cryptography, internet of things (IoT) and 5G.	Uses IPFS and blockchain	Connecting multiple medical devices and ensuring access control to patients information	Hyperledger Fabric used for registration and monitoring MEC nodes	Uses smart contracts but their implementation is not mentioned	Permissioned
[18]	A proposal to use blockchain and smart contracts to monitor the healthof physicians	Blockchain	Track the physicians burnout and stressors during the COVID-19 pandemic	Trace and notification	Only a proposal, no implementation	Permissioned
[19]	Use IoT, smart phones and blockchain to monitor Covid-19 patients	Cloud and blockchain	Asynchronous telehealth system for monitoring early COVID-19 symptoms	Monitoring	-	-
[20]	Finding a way to match donors with patients across telehealth hospitals	Blockchain, servers	Telehealth for convalescent plasma (CP) transfusion across centralized and decentralized hospitals	Updated ledger of patient details	-	-
Our Proposed Solution	Providing three types of telehealth services: 1) Teleconsultaion 2) Drug Administration 3) Medical Testing	IPFS, Cloud, Blockchain	A fully decentralized telehealth system using permissioned Ethereum network	Tracing, tracking, alerting with notifications, and provenance	Yes, made publicly available	Permissioned Ethereum

identity during registration in the registration SC. Hence, in the execution, only a doctor for instance can authorize a medical test for a registered patient. Also, only a courier can upload the hash of the delivered package on-chain.

Furthermore, confidentiality is crucial in ensuring the solution protects the patient's privacy and medical rights. Therefore, our solution is implemented using a private blockchain. Based on the EA of the user, their rights are provided as well as authority levels and access rights. Furthermore, during registration off the chain, the biometrics data of the individuals are associated with their EAs or on-chain addresses on the chain [35]. Moreover, depending on the chosen private network, the information is encrypted when communicated. Other networks depend on channels and divide the participating entities into groups [36]. Roles and access rights can be administered by a higher authority such as Membership Service Providers (MSP). Hyperledger Fabric uses channels for confidentiality and the MSP for identity management [37].

B. Comparison with Existing Solutions

Table I compares the existing blockchain-based telehealth solutions with our solution. The solution proposed in [17] was implemented using a permissioned blockchain network. The solution depends on IoT devices and focuses on secure communication between the multi-access edge computing nodes and the IoT devices. Furthermore, the solution uses smart contracts and implies that the testing was done using a raspberry pie and the Hyperledger Fabric. One of the limitations of that work is it does not show the testing and coding details of the smart contracts. Unlike the other solutions proposed in [18]–[20], our proposed solution deals with three main telehealth services for patients which are teleconsultation, drug administration, and medical testing. Also, it is fully decentralized using the decentralized storage of IPFS or can be integrated with the cloud. Moreover, our study shows the full implementation and testing details along with the smart contracts' code which is made publicly available on GitHub.

C. Generalization

Our proposed blockchain-based telehealth solution helps to ease the burden of the medical professionals besides facilitating patients. It is fully applicable to the COVID-19 pandemic and other infectious diseases. The proposed solution is versatile and can be fully adapted for other purposes, diseases, and benefits. Our smart contracts' functions can be edited and new functions can be added as required. Furthermore, new roles can also be applied as well as modifiers. This solution is designed to eradicate the spread of disease and to spread the knowledge of the medical practitioners as well as care and treatment. Patients seeking treatment and ongoing care can be handled regardless of their physical geographical location. Consequently, our solution is not restricted to infectious viruses, but it can be used for several other telehealth scenarios (e.g., diabetes, mental health, maternity checkups, etc.).

VI. Conclusion

In this paper, we have presented a fully decentralized blockchain-based telehealth solution. The solution ensures the traceability, integrity, and availability of telehealth transactions and records related to medical care, diagnostics, and monitoring for remote and at-home patients. Our solution leveraged blockchain intrinsic features to ensure trust, accountability, integrity, and transparency. Using the permissioned blockchain network, we were able to maintain the patient's privacy and medical information securely. We showed how our system can integrate with cloud and IPFS storage systems to facilitate the secure accessibility and traceability of immutable large-size digital content and video calls associated with telehealth service sessions. Our proposed system, framework, solution, implementation, as well smart contracts and their algorithms are given and studied in this paper specifically for COVID-19 patients; however, all can be tailored and extended in general for remote patients. As a future work, we plan to deploy the full system in a real Ethereum blockchain main network (Mainet) and build the relevant end-user Decentralized Applications (DApps).

VII. Acknowledgement

This publication is based on work supported by the Khalifa University of Science and Technology under Awards No. CIRA-2019-001 and RCII-2019-002, Center for Digital Supply Chain and Operations Management.

References

[1] "Indian american doctors pitch in with free telehealth advice during india's Covid-19 crisis," [Accessed on: May 15, 2021]. [Online]. Available: https://edition.cnn.com/2021/05/09/us/india-covid-doctors-us-telehealth-help/index.html

[2] J. R. Maese, D. Seminara, Z. Shah, and A. Szerszen, "Perspective: What a difference a disaster makes: The telehealth revolution in the age of Covid-19 pandemic," *American Journal of Medical Quality*, vol. 35, no. 5, pp. 429–431, 2020.

[3] R. M. Reynolds, "Telehealth in pregnancy," *The Lancet Diabetes & Endocrinology*, vol. 8, no. 6, pp. 459–461, 2020.

[4] T. Kompala and A. B. Neinstein, "Telehealth in type 1 diabetes," *Current Opinion in Endocrinology, Diabetes and Obesity*, vol. 28, no. 1, pp. 21–29, 2021.

[5] K. A. Zoder-Martell, A. M. Markelz, M. T. Floress, H. A. Skriba, and L. E. Sayyah, "Technology to facilitate telehealth in applied behavior analysis," *Behavior analysis in practice*, vol. 13, no. 3, pp. 596–603, 2020.

[6] C. Shachar, J. Engel, and G. Elwyn, "Implications for telehealth in a postpandemic future: regulatory and privacy issues," *Jama*, vol. 323, no. 23, pp. 2375–2376, 2020.

[7] E. E. Thomas, H. M. Haydon, A. Mehrotra, L. J. Caffery, C. L. Snoswell, A. Banbury, and A. C. Smith, "Building on the momentum: Sustaining telehealth beyond Covid-19," *Journal of telemedicine and telecare*, p. 1357633X20960638, 2020.

[8] L. H. Schwamm, A. Erskine, and A. Licurse, "A digital embrace to blunt the curve of covid19 pandemic," *NPJ digital medicine*, vol. 3, no. 1, pp. 1–3, 2020.

[9] E. Monaghesh and A. Hajizadeh, "The role of telehealth during Covid-19 outbreak: a systematic review based on current evidence," *BMC Public Health*, vol. 20, no. 1, pp. 1–9, 2020.

[10] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," *Neural Computing and Applications*, Jan 2021. [Online]. Available: https://doi.org/10.1007/s00521-020-05519-w

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

[12] S. Zawada, "Poster: Blockchain application feasibility in telehealth for dscsa compliance," in *2020 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*. ACM, 2020, pp. 3–4.

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

[14] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, and M. Omar, "The role of blockchain technology in telehealth and telemedicine," *International Journal of Medical Informatics*, p. 104399, 2021.

[15] D. Vervoort, C. R. Guetter, and A. W. Peters, "Blockchain, health disparities and global health," *BMJ Innovations*, vol. 7, no. 2, 2021.

[16] M. MK, G. Srivastava, S. R. K. Somayaji, T. R. Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "An incentive based approach for Covid-19 using blockchain technology," *arXiv preprint arXiv:2011.01468*, 2020.

[17] T. Hewa, A. Braeken, M. Ylianttila, and M. Liyanage, "Multi-access edge computing and blockchain-based secure telehealth system connected with 5G and IoT," in *The 8th IEEE International Conference on Communications and Networking (IEEE ComNet'2020)*, 2020.

[18] V. Dhillon, T. Xu, and C. Parikh, "Blockchain enabled tracking of physician burnout and stressors during the Covid-19 pandemic," *Frontiers in Blockchain*, vol. 3, p. 62, 2021.

[19] T. Alam, "Blockchain-enabled mobile healthcare system architecture for the real-time monitoring of the Covid-19 patients," *Available at SSRN 3772643*, 2021.

[20] T. J. Mohammed, A. Albahri, A. Zaidan, O. Albahri, J. R. Al-Obaidi, B. Zaidan, M. Larbani, R. Mohammed, and S. M. Hadi, "Convalescent-plasma-transfusion intelligent framework for rescuing Covid-19 patients across centralised/decentralised telemedicine hospitals based on ahp-group topsis and matching component," *Applied Intelligence*, pp. 1–32, 2021.

[21] S. Bhaskar, A. Nurtazina, S. Mittoo, M. Banach, and R. Weissert, "Telemedicine during and beyond Covid-19," *Frontiers in public health*, vol. 9, p. 233, 2021.

[22] S. Bhaskar, S. Bradley, V. K. Chattu, A. Adisesh, A. Nurtazina, S. Kyrykbayeva, S. Sakhamuri, S. Moguilner, S. Pandya, S. Schroeder *et al.*, "Telemedicine as the new outpatient clinic gone digital: position paper from the pandemic health system resilience program (reprogram) international consortium (part 2)," *Frontiers in public health*, vol. 8, 2020.

[23] H.-N. Dai, M. Imran, and N. Haider, "Blockchain-enabled internet of medical things to combat Covid-19," *IEEE Internet of Things Magazine*, vol. 3, no. 3, pp. 52–57, 2020.

[24] M. S. Jalali, A. Landman, and W. J. Gordon, "Telemedicine, privacy, and information security in the age of Covid-19," *Journal of the American Medical Informatics Association*, vol. 28, no. 3, pp. 671–672, 2021.

[25] "The foundation for decentralized applications," [Accessed on: May 4, 2021]. [Online]. Available: https://infura.io/product

[26] "Remix," [Accessed on: July 27, 2020]. [Online]. Available: https://remix.ethereum.org/

[27] Y. Chang, E. Iakovou, and W. Shi, "Blockchain in global supply chains and cross border trade: A critical synthesis of the state-of-the-art, challenges and opportunities," *arXiv preprint arXiv:1901.02715*, 2019.

[28] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[29] "Quorum," [Accessed on: May 8, 2021]. [Online]. Available: https://docs.kaleido.io/kaleido-platform/protocol/ethereum/quorum/

[30] "Hyperledger besu," [Accessed on: May 8, 2021]. [Online]. Available: https://docs.kaleido.io/kaleido-platform/protocol/ethereum/besu/

[31] "Hyperledger fabric," [Accessed on: May 8, 2021]. [Online]. Available: https://www.hyperledger.org/projects/fabric

[32] "Announcing hyperledger besu," [Accessed on: May 8, 2021]. [Online]. Available: https://www.hyperledger.org/blog/2019/08/29/announcing-hyperledger-besu

[33] H. R. Hasan, K. Salah, R. Jayaraman, M. Omar, I. Yaqoob, S. Pesic, T. Taylor, and D. Boscovic, "A blockchain-based approach for the creation of digital twins," *IEEE Access*, vol. 8, pp. 34 113–34 126, 2020.

[34] A. A. Battah, M. M. Madine, H. Alzaabi, I. Yaqoob, K. Salah, and R. Jayaraman, "Blockchain-based multi-party authorization for accessing ipfs encrypted data," *IEEE Access*, vol. 8, pp. 196 813–196 825, 2020.

[35] H. R. Hasan, K. Salah, R. Jayaraman, J. Arshad, I. Yaqoob, M. Omar, and S. Ellahham, "Blockchain-based solution for Covid-19 digital medical passports and immunity certificates," *IEEE Access*, 2020.

[36] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, and M. Omar, "Blockchain architectures for physical internet: A vision, features, requirements, and applications," *IEEE Network*, 2020.

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