Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.029053
Article

Tech Science Press

Smart Quarantine Environment Privacy through IoT Gadgets Using Blockchain

Nitish Pathak[1], Shams Tabrez Siddiqui[2], Anjani Kumar Singha[3], Heba G Mohamed[4], Shabana Urooj[4,*] and Abhinandan R Patil[5]

[1]Department of Information Technology, Bhagwan Parshuram Institute of Technology (BPIT), GGSIPU, New Delhi, 110078, India
[2]Department of Computer Science, Jazan University, Jazan, 45142, Saudi Arabia
[3]Department of Computer Science, Aligarh Muslim University, Aligarh, 202002, India
[4]Department of Electrical Engineering, College of Engineering, Princess Nourah bint Abdulrahman University, P O Box 84428, Riyadh, 11671, Saudi Arabia
[5]Sanjay Ghodawat University, Kolhapur, Maharashtra, 416118, India
*Corresponding Author: Shabana Urooj. Email: smurooj@pnu.edu.sa

Received: 24 February 2022; Accepted: 05 May 2022

Abstract: The coronavirus, formerly known as COVID-19, has caused massive global disasters. As a precaution, most governments imposed quarantine periods ranging from months to years and postponed significant financial obligations. Furthermore, governments around the world have used cutting-edge technologies to track citizens' activity. Thousands of sensors were connected to IoT (Internet of Things) devices to monitor the catastrophic eruption with billions of connected devices that use these novel tools and apps, privacy and security issues regarding data transmission and memory space abound. In this study, we suggest a blockchain-based methodology for safeguarding data in the billions of devices and sensors connected over the internet. Various trial secrecy and safety qualities are based on cutting-edge cryptography. To evaluate the proposed model, we recommend using an application of the system, a Raspberry Pi single-board computer in an IoT system, a laptop, a computer, cell phones and the Ethereum smart contract platform. The models ability to ensure safety, effectiveness and a suitable budget is proved by the Gowalla dataset results.

Keywords: Ring signature; blockchain; IoT; encryption; smart contract; decryption; authentication; privacy-preserving

1 Introduction

The SARS-2 causes coronavirus disease 2019 (COVID-19) which is an infectious disease caused by SARS-2 coronavirus [1]. The disease is quickly spread across the world. Approximately 211 million cases have been reported on 31st October 2021. Over 4.4 million people have died [2] across all 188 registered countries, the mortality rate is 3.6%. Covid-19 is contagious many people died across the world [3] because of its fast transmission and factiousness, all the countries made tremendous efforts to fight against this COVID-19 pandemic. Xiang et al., believe in anti-infection policies (by imposing the lockdown in the countries) have significantly reduced the infection rate and the measurable health outcomes [4,5] whereas different countries have followed different approaches and practices [6]. The most common measure has been taken i.e, segregation of the apartment (staying at home or hotel) which includes managing family members in a family environment, that can prevent the spreading of the virus infection between people or patients by domestic quarantine method, the patients are physically diagnosed in the physical quarantine. Many people contracted the covid-19 virus without their knowledge and home isolation became a problem for them. A proper set of rules and restrictions for foreign travelers to stop spreading the viruses is required. The governments have deployed the police personnel to fight against the covid-19 with proper anti-infection guidelines which includes home isolation, [7] and also they are using the technologies like GPS and Bluetooth of the Smartphone for monitoring the people and patients. Whereas this monitoring methods have a few disadvantages which cannot guarantee whether the number of the mobile is matched with the owner at the time, there is a possibility of separation of the person from the machine. In general, people cannot get rid of the above situation even though they wear smart devices such as smart bracelets [8,9]. The condition of the house is determined in real-time with the help of the internet of things which is set up in the smart home. If we do not use the smart home equipment, intercom access, control, and security cameras effectively, the position of the house is traceable, and privacy is lost. Today the data is highly concentrated; it is vulnerable to targeted attacks, which causes the risk of a single point of failure [10].To fix this problem, we have a solution i.e., blockchain technology [11–13]. This technology along with the Internet of Things has brought so many changes in the industries and helps to develop business models as well as distributed applications. There are reports that blockchain and the Internet of Things can work together to facilitate resource and service exchanges between devices [14,15]. Christidis et al. [16] pointed out, that the point-point distribution and public ledger functions of blockchain will be a fit for the cloud computing services, and it includes the data sources, auditing, digital asset management, and the distributed consensus. The blockchain facilitates users to create a protected environment from unauthorized access by using encryption techniques, it links all the transaction blocks together, so that the record cannot be altered.

Siddiqui et al. [17] created a more efficient system by combining the smart grid with the blockchain. Microgrids and intermittent power supplies played an essential role in the power supply after the evolution of the power grid. It can be used more wisely, such as logistics, transportation, and sensor data are the most important data of the internet of things [18,19].

In conclusion, this work makes three contributions;

- With the help of a smart home's security system, we can have the daily in and out, record what happens after the present state is recorded, and then generate a report after preprocessing. A digital signature will be issued by the Centre for Disease Control and allocates a virtual number for internet-of-things (IoT) devices, the main idea behind this is to build a secure virtual environment [20,21].
- It is possible to examine the reported segregation using blockchain smart contracts based on specified standards, and we must retain a record of aberrant data, which will not meet the blockchain segregation requirements at a low cost [22] with the assistance of blockchain smart contracts.

We can create security protection methods that are specific to the situation with the help of the public and private key pairs of the blockchain system. To report segregation, the system uses a community as the base unit, which will not have information particular to the household. We can complete this ring signature with the help of the other devices public keys of the same community and maintain the inhabitant's anonymity by ensuring data consistency. In case of an infection, we need to be handled differently, like information relevant to a residence with a virtual house number, which is encrypted with the public key of a police officer for ensuring the data security and authenticity before it is forwarded to the workers in charge of pandemic prevention [23]. The paper comprises of the following sections: Section-1 Introduction, Section-2 Background of the work, and Section-3 deals with Architecture Proposal. Whereas, Section 4 has an in-depth discussion of the experiments and results, while Section 5 contains a comparison of the proposed model with relevant work. Section 6 concludes the study by making allusions to the study's conclusion.

2 Background

2.1 Internet of Things (IoT)

Internet of Things (IoT) is all about collecting information about any kind of object from various sensors; these objects are monitored, connected, and will interact in a real-time world; and transmitting the information over to actualize the omnipresent connection of items, the network is used, along with other smart things and people. The result is all about intelligent perception recognition and management. In the real world, IoT devices have a huge scope, i.e., mainly included in a few sectors like Smart-personal, private homes, offices, factories, and warehouses [24]. There are three major development attributes of IoT devices i.e., connectivity, perception, and intelligence. We can achieve the overall perception of IoT devices, with the help of the integration and the convergence of network communications, artificial intelligence, deep learning, and blockchain technology, which can aggregate all the links effectively with the help of the normalized management. As well as we can share data and resources, provide one-step objects and all-around services. The Internet of Things (IoT) gadgets in a smart house allow us to do many things, such as turn on or off the lights, open or close the windows, adjust the temperature of the air conditioners, heaters, and security systems and alarms [25]. Fig. 1 shows how a hub connects all of these connected smart devices.

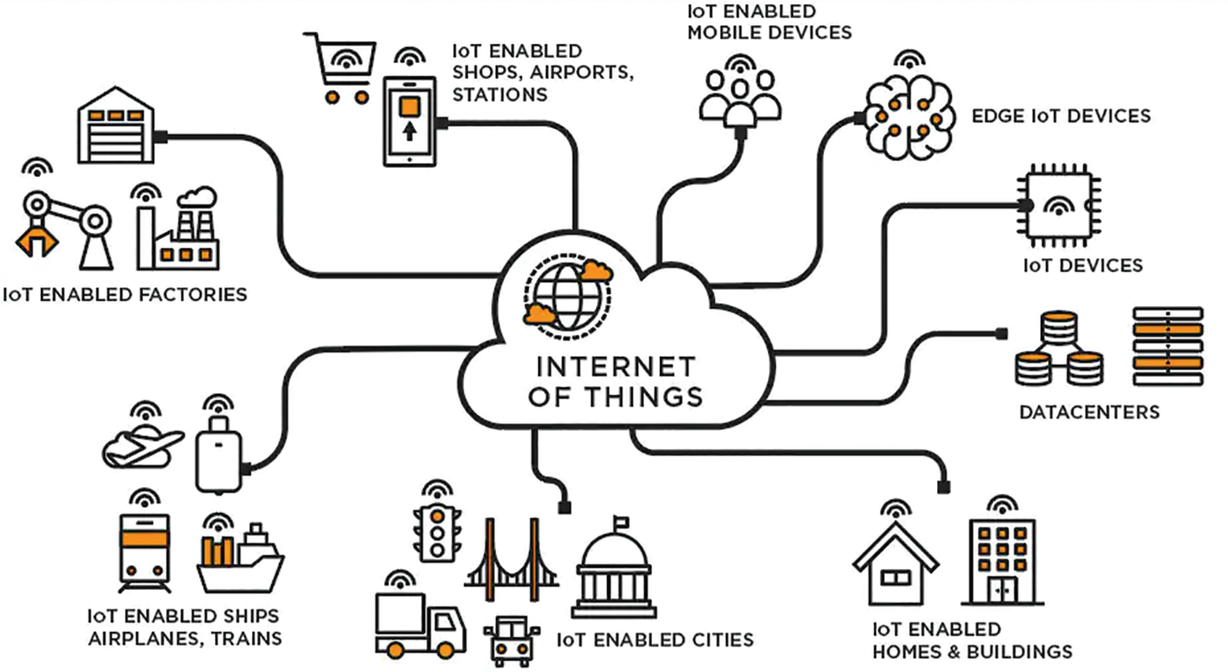

IoT ENABLED SHOPS, AIRPORTS, STATIONS
IoT ENABLED MOBILE DEVICES
EDGE IoT DEVICES
IoT DEVICES
IoT ENABLED FACTORIES
INTERNET OF THINGS
DATACENTERS
IoT ENABLED SHIPS AIRPLANES, TRAINS
IoT ENABLED CITIES
IoT ENABLED HOMES & BUILDINGS

Figure 1: Architecture of IoT

2.2 Blockchain

Satoshi Nakamoto was the first to introduce blockchain technology in 2008, since then, it has attracted because of its decentralization, it got a lot of attention, incapacity to rewrite, and anonymity. Blockchain eliminates the limits of traditional methods underlying technology, so it has a variety of possible applications. As an example, blockchain has the potential to build a decentralized system of cryptocurrencies, thereby revolutionizing the financial sector and other industries. Unlike traditional digital currency systems, people on unreliable networks can directly trade with each other without relying on external institutions. Algorithms for encryption, transaction processing, consensus, and technology are based on distributed ledgers [26]. Encryption, as demonstrated in Fig. 1, the algorithm provides transparency and verifiability of data on the entire network, while retaining the anonymity of personal information. The present state of the blockchain is described by blockchain nodes and then combined to form a new block. Distributed ledgers record participants in the network transactions. This time is saved by using a ledger and the cost involved in bridging the gap between many ledgers. The use of consensus algorithms removes the potential of data tampering and replaces third parties. Blockchain is mainly operated by these components; encryption, immutability, tokenization, distribution, and decentralization. The following information contained in each block: the current block, the previous block hash value, the time when the agreement is achieved and the transaction data.

2.3 Contracts with Intelligence

The origins of smart contracts can be traced back to the 1994s, before the invention of blockchain technology, Szabo turned a connection into a confirmed digital partnership by forcing the concept of a paper contract, because of an environments lack of credibility, these smart contracts were not employed in real applications at first. However, blockchain technology provided the trustworthiness of an environment in which these smart contracts and forms were executed. The most important component of the system for using a smart contract is a piece of algorithmic code, which can digitize complex relationships, humans who are similar to one another, agreements on the law and in addition, computer networks, among other things. It is possible to perform autonomous execution and deployment after checking with a smart contract, which is a protocol running on a computer. This application is not limited to banking; it is also appropriate for distributed computing, the Internet of things, and other areas. The blockchain ecosystem with the help of these smart contracts, can make a reliable transactions and perform the operations without third parties, it is re-laid on the blockchain nodes of communication and consensus. Once the contract is made then it will start the execution according to the terms and conditions of a computer programmer, with the help of the other nodes we can check the execution status automatically but, monitoring the progress and tampering is not possible. Smart contracts are applied in many fields like medical, education, data security, certification, and copyright protection. Peer-to-peer technology is used in these smart contracts for spreading networks in the blockchain environment. The received contract is saved in memory by the verification code and waits for the contract to be triggered by the process. At this point, everyone agrees, that a contract set holds all the contacts of verification node packages and calculates this contract set hash value, all the blocks are assembled, and spread all over the network. After receiving the verification set, the verification nodes will compare and contrast the data they have collected with the contract's specifications. Finally, the verification nodes will establish a consensus based on the stated time frame on the most recent contract, to obtain this agreement, several times checking and comparison will be done. It is known that Ethereum is an electronic payment system and has a smart contract feature [27]. Ethereum is also like a bitcoin; both of them use the ledger that is distributed which is utilizing blockchain technology. This is not restricted to the characteristics of digital currency like Ethereum, Bitcoin provides a platform where we can develop verifiable decentralized applications (Dapps).

2.4 Ring Signature

Zhang et al. [28] proposed the ring signature first which is a digital signature scheme and it is a simplified group structure. There are so many ring members in this ring structure. The ring structure has to meet the below-mentioned security requirements.

i) *Correctness*: A message should be signed according to the steps of the correct signature, this helps to prevent the tampering of a message during the process of propagation, and then the ring structure meets the equation of the verification of signatures.

ii) *Anonymity*: The probability that the true sign does not exceed $\frac{1}{N}$ (where ring members are N) even though obtaining the private keys illegally of all the signers.

iii) *Enforceability*: It's really hard to forge the legal signature even if you don't know the secret keys though any message m of a random prophecy that can be obtained by an external attacker in the ring structure, is negligible.

iv) *Spontaneity*: When performing the fundamental functions of a ring signature, it is not necessary to employ group signatures with the participation of a trusted third party or a group administrator; however, this is an option. The basic process is as follows: Configuration: The sender of the message selects a group of people to form a set of S = ring members = (S_1, S_2,. , S_n) and the public keys of ring members from the public key set K = (K_1, K_2,…, K_n)

v) *Signature*: Use message m, message sender's private key K_M of the message M and K are to generate a set of public keys for signing σ.

vi) *Check:* The mail recipient checks the validity of (m, σ).

3 Architecture Proposal

In Fig. 2, the home is outfitted with smart devices for example security system, smart magnetic doors, and infrared sensors which will connect through the outside world internet i.e., smart gateway devices. The system only admits authorized users, which helps to avoid malicious attacks from the outside world. Smart gateways in a cluster will be in the same community as the cluster, which helps to keep the system safe. Fig. 2, illustrates a smart home system. The connected indicator's threshold is a specific manifestation, and each household's smart gate will collect related information and format it along with the aggregate. This regulated information will be sent to the smart contract in question, and this smart contract will be the officer's order with the quarantine regulations. Once, the contract has been deployed, no one is allowed to make any modifications to it. To ensure the safety and privacy of a home, the smart contract will use the ring signature to verify the validity of data reported by other members of a similar community and will notify the management department if the value exceeds the specified threshold. The officer can use this to gain insight into the community's structure. The information provided is neither private nor confidential which will consider the current state of the smart device's limited resources, the information is not encrypted. Expect in the case of enquiring for assistance, any information of households can be kept private, and the overlay network preserves privacy. The system will be deployed for that we might rely on the blockchain public ledger which can put smart contracts into action, for restricted environments, a private blockchain is a good option, once we deploy the system we cannot add new users. A public blockchain's scalability and adaptability are inherent properties, allowing us to grow indefinitely. The system can be deployed in a house which has a smart home architecture based on IoT shown in Fig. 2. The following items can be found in smart homes; all the family members are aware of the ecosystem which is based on the internet of things devices, the devices mainly contain sensors which collect the information about the environmental data, and then the data will be sent to admin or service providers. Every one of us has equal access to the public (users). Emergencies are handled by frontline personnel in the pandemic prevention field. To combat the COVID-19 pandemic, the CDC officer

(Person): offers the basic requirements or guidelines for quarantine and makes them available as smart contracts. Essential conditions in the area are inspected by this smart contract.

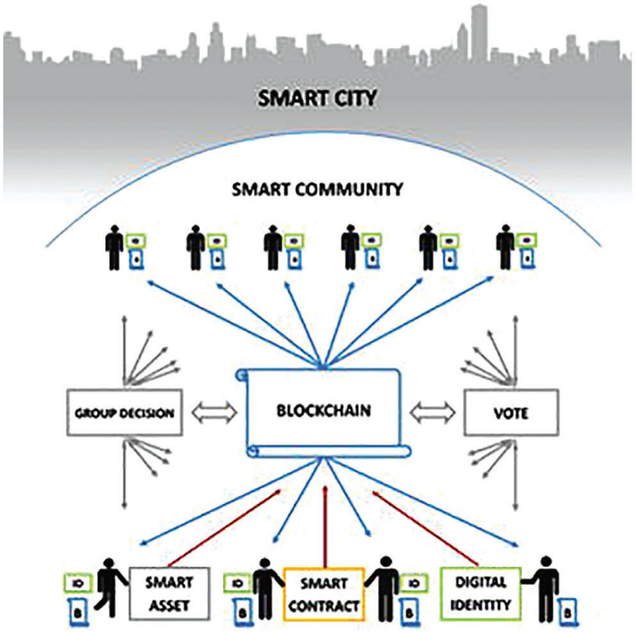


Figure 2: Using Blockchain as a platform for smart city

3.1 Phase of Initialization

Our scheme is suitable to apply for the administration of the community, where it requires a phase of initialization, the smart device includes the internet of things gadgets, smart home storage, actuators, sensors, smart gateways, etc. These gadgets are all enormous, diverse, complex, and use resources are restricted, this is in direct opposition to the basic storage capacity and blockchain technology necessitates a lot of computational power. Computers and smart gateways, two of the most important participants in the blockchain, help us overcome the challenge. The officer delivers a certain charge to the device wallet before developing the system (O). In this the device is integrated into the blockchain system, to get the keys i.e., pair of public/private keys. Blockchain addresses are used in the system. Providing certificates is akin to initialization. An officer(private key)'s key k is used to sign a number allocated to a virtual home on the blockchain, which includes the community phone number and blockchain address. Once the blockchain system has validated the validity of all linked devices, it is feasible to create a virtual community. ID is a virtual house number, X_1X_2 is community ID; Y_1Y_2 is blockchain and signature by $k_{officer}$.

3.2 Operation Phase

Only official-issued digital gadgets with digital numbers can be stored in the device. Quarantine management information can soon be gleaned from the intelligent settlement units (such as entry and exit times, and the longest period of time spent away from the residence, among other things). A smart home's (A1, A2) sensors provide the statistical data they detect to an intelligent gateway, which can then pick and designate the network's shared public key for certain devices and transfer the data to the most intelligent location for analysis possible. Isolation techniques are used in most cases when this barrier is crossed. As soon as the settlement realizes that the information has gotten out of hand, they seize on an opening and transmit it along with the officer's signature, replete with a hoop. As depicted in Fig. 2, we believe that the perceived data will be the last to be stored, eliminating the need for cloud gadgets. A logical collection of device execution is depicted in Fig. 3. Public information provides the easiest fundamental worker access to statistics and, therefore, does not require encryption from the standpoint of information security; however, information security must still be considered, that is why the hoop signature approach is employed. The network may be recorded and blended with the tool to create ring signatures with no difficulty; to accomplish the key shown in Algorithm 1 is needed. The homes of the hoop signature are adequate for the particular software scenario. To ensure that the statistics have not been manipulated in any manner, you can allow signers to signal messages anonymously. In the case of mixing with the public keys of various devices, it is not possible to determine which member signed the message.

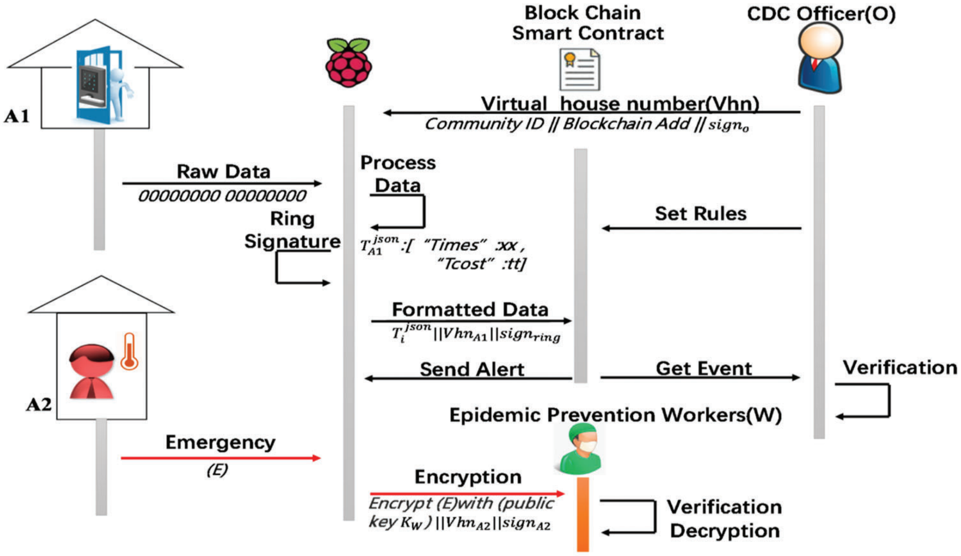

Block Chain
Smart Contract
CDC Officer(O)
A1
Virtual house number(Vhn)
Community ID || Blockchain Add || $sign_o$
Raw Data
00000000 00000000
Process
Data
Ring
Signature
T_{A1}^{json}:["Times" :xx ,
"Tcost" :tt]
Set Rules
Formatted Data
$T_i^{json}||Vhn_{A1}||sign_{ring}$
A2
Send Alert
Get Event
Verification
Epidemic Prevention Workers(W)
Emergency
(E)
Encryption
Encrypt (E)with (public key K_W) $||Vhn_{A2}||sign_{A2}$
Verification
Decryption

Figure 3: Logical flow of execution system

Algorithm 1: Algorithm of Ring Signature

```
Fun Ring _Signature (data),
If anonymity in the blockchain, the Smart Gateway has chosen,
hash_key ←Text Message or hash data to be calculated,
Digital Signature created with the help of hash_key and Private Key Signers (PKS),
The signature mixed with other smart gateway groups to form Ring Signature,
end if
end Fun
```

The officer adjusts the threshold values of the associated parameters in the smart contract in accordance with the needs of the situation, taking into consideration the varying quarantine regulations in different places. According to algorithm 2, the smart gateway collects relevant data at regular intervals (i.e., once a day) and passes it to the officer's smart contract.

Algorithm 2: Rule of smart contract in-home quarantine

```
Input: quarantine homesitehome_state, ring signature ring_s,
Output: result,
Required: homeCheck false,
home list home policy,
Grand comes from the smart gateway then
h← home policy,
if h.homelist = “meet” then
home policy ←Ture
else
home policy ←False
end if
result←homepolicy
end if
TriggerResults (home_state, ring_s)
```

We can even take into consideration the prevalence of public health events. With the appearance of A2 infection symptoms and the need for a more precise therapy (sampling, isolation, quarantine, etc.), the public key of the Kw pandemic was used at the gateway. The prevention expert (W) encrypts personal information of virtual house numbers. The old data can only be overwritten by the personal key (W) of a pandemic interference worker.

4 Experiments and Results

It is employed in the above-mentioned proposed system as an Internet of Things device to detect and process home quarantine, and it makes use of smart contracts to analyze and process the data from the homes. We intend to address the evaluation of operations in terms of their safety, timeliness, and financial costs.

4.1 User Case Summary

In the home quarantine case study, the following use cases were considered:

- *Strong quarantine at home:* Initial stages of the COVID outbreak, we could not be able to find the spreading reason of the virus, so we must follow strict quarantine measures in the affected areas. We can reduce the cross-infection. It does not allow family members to leave the house; health workers or pandemic prevention officers provide the necessities of households [29].
- *Moderate Home quarantine:* One person in the household is not allowed to go outside that too for a small amount of time, like bringing the necessary things or dumping the garbage.
- *General Home quarantine:* Different regions follow different types of quarantine policies, residents are not allowed to go out, and they are allowed to go out if it is necessary to work like buying food items or medicines. In these situations, the CDC worker must gather pertinent information from each family, if any change in the information then it will have a huge impact on pandemic prevention work, that’s why these messages must be authenticated, have integrity, and be private.

4.2 The Framework Evaluation

We must concentrate on the evaluation of time and energy consumption in the method; there are three various types of end nodes, including desktop, laptop, and single-board computers such as the Raspberry Pi. The laptop is primarily used by the officer, and it assists the officer in issuing virtual house numbers, creating smart contracts, and monitoring logs in the blockchain system. The responsible party is a smart gateway to collect information through the Raspberry Pi, and it also completes the ring structures, by connecting the blockchain, and it encrypts emergencies, with a desktop device being used to decrypt these at the worker side. It is necessary to write and compile smart contracts to use the Ethereum blockchain, which is primarily focused on the Solidity computer language. The smart contract writing and compiling is accomplished using remix, which is based on an integrated development environment (IDE) for solidity that runs in the browser [29]; in this case, web3. When using Js for communication, HTTP connections are required for deployment and for tracking the current status of a smart contract in order to get the client's consent, as illustrated in Fig. 4, which shows how the frame is constructed.

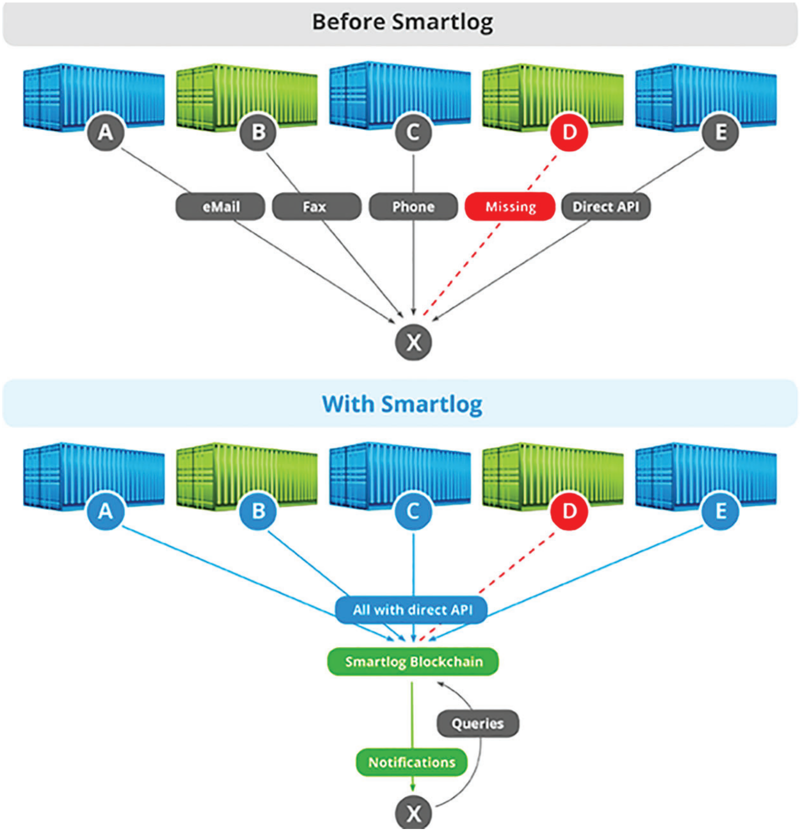


Figure 4: Blockchain and IoT case study

4.3 Results Evaluation

Detecting a smart device in a home with intelligence and a smart gateway or other p2p network nodes is the most difficult part. To protect ourselves, we must be prepared to respond to security threats, such as the deletion of stored data or the creation of a bogus event, among others. An independent node is assigned a virtual number which will reflect the house's genuine isolation status; the solution for the required safety measures is described as shown in Tab. 1.

Table 1: Requirements for a safety solution

Requirement	Solution	State
Scalability	Peer-to-peer network	Scalability of best solution at large scale in one of (SC) the peer-to-peer network.
Anonymity	Signature of ring	The receiver cannot sign the message when combined with another public key.
Availability	Contracts of smart	More data is reliable and trustworthy which ensures continuous verification.
Confidentiality	Key pair of private-public	Data is encrypted is a different party as the public key in the form of a blockchain and is comparable to a private key.
Integrity		Block of data using the Previous block of using hash function contains new blocks, that (IN) hashing guarantees the information is not modified.

4.4 Evaluation of Security Requirements

Developers are required to adhere to certain security criteria. The three most significant security measures that must be taken into consideration are availability, confidentiality, and integrity, and they are listed below. Confidentiality ensures that only authorized users have access to the system, while Integrity ensures that the message is delivered to its intended destination without any data being lost in transit. The availability of data allows us to access it whenever we need it, and we will examine security margin approaches under different types of risks in the following sections.

- *Sybil Attack:* Attacks on data redundancy techniques are carried out by malignant nodes, which multiply the number of nodes in the P2P network, and these nodes generate data in the P2P network that contains several IDs that are also backed up by the malicious nodes in the P2P network. As previously stated, each smart gateway is identified by a unique virtual number. The information has been submitted each time; it should be associated with a virtual house number and the community to which it belongs, among other things. Not all virtual home numbers are approved by an officer with the assistance of attackers who do not have access to a secret key and are therefore able to use fictitious virtual numbers in order to commit fraud.
- *Denial of service:* A common tactic used by attackers to prevent authenticated users from gaining access to the network is to send unnecessary data over the already congested network. An attacker may be able to shut down part of the network nodes, but they will not be able to shut down the entire network due to the decentralized nature of the blockchain.
- *Spoofing attack*. Attackers masquerade as trusted entities to acquire the trust of other entities so that they can steal data or money or spread malicious software. The private key cannot be spoofed in the design paradigm. Identity spoofing is impossible for them.

4.5 Total Time Spent

The specifications of the devices can be found in Tab. 2 of such documents. Single-board computers are used as local gateways in this scenario, where computers are the user devices. Ring topologies of various devices and laptops are verified by the Raspberry Pi using their public keys. The experiment showed that the number of public keys is exactly proportional to the number of secret keys used in the network while verifying a signature on the Raspberry Pi. To verify the signature, a laptop is used since it has superior performance, the curve that takes so long slope is relatively low, and in the above two instances, the standard deviation is minor, which assists to confirm Tab. 2 computation stability. The averages and standard deviations of a ring structure are shown in Fig. 4 after conducting 51 experiments with a variety of public keys.

Table 2: Devices specification

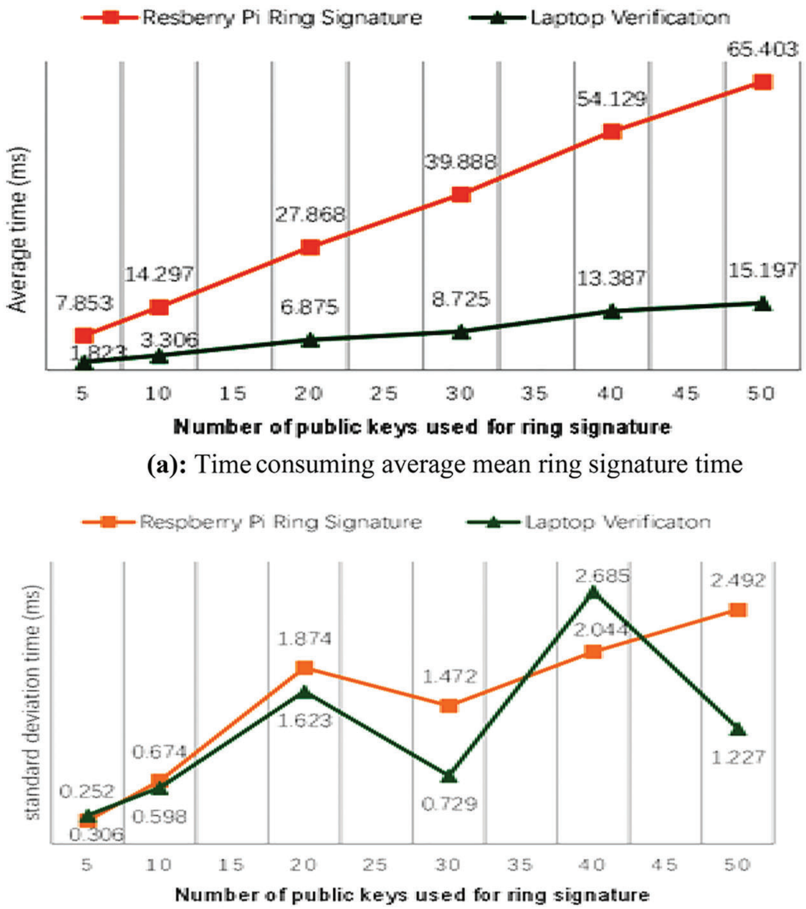
Hard disc	Operating system	CPU	Devices memory
250 GB 128 GB7050	Window 7	Core i7	3.9 GHzDell OptiPlex
4TB Lenovo 80e5 1 TB	Windows 10	intel core i7	8650u 1.9 GHz
SanDisk Ultra 128GB 8 GB SD	Raspberry Pi OS	Arm Cortex	A72ZX Spectrum

The Rivest-Adelman (RSA) technique was utilized to build a trapdoor with a one-way function in the case. The Abscissa represents the variety of extra devices (Xi), which are used within the same gated community and make use of the public key to ring constructions. Ring constructions in Fig. 5a indicate a linear increase in the average time to the public numbers used by other gadgets, whereas Fig. 5b shows a minor fluctuation in the ring structure standard deviation. The time it takes to encrypt data on a Raspberry Pi and the computer-assisted decryption, this written encryption or decryption algorithm in the Python 3.8, 380 ms for encryption and 50 ms for decryption must be verified in the event of an encrypted transmission emergency. Here we did not take into consideration of event time consumption in the communication process because this depends on the network protocols and technology.

The blockchain event execution time also takes into account many consensus methods, each of which has a unique block generation timescale, i.e., Bitcoin. Bitcoin requires a minimum of 10 min to build a block, but Ethereum takes 15 s, and Ethereum charges a fee for each calculation step completed during a transaction. When smart contracts are executed, each command of an operation has a specified cost, which is expressed in the form of "Gas." When we execute a smart contract, a particular amount of gas is spent. We also need to consider the execution order; when gas costs are greater, such transactions are completed first and have a shorter execution time.

4.6 Financial Cost

"Gas" is used to calculate the amount of work needed to execute a task, and gas has a cost. The price of gas is based on the amount of gas consumed by the tasks being executed. Smart contracts also require gas, and the amount of gas consumed is estimated based on a variety of factors, as indicated in Tab. 3. An Essential consumption has a monetary value that can be determined. How many reports, how many bytes of reports, and other aspects affect costs. Fig. 6 shows the results of some comparisons depending on the different numbers of participating public keys in the signature. Gas consumption is directly related to the number of public keys being used; this is because gas is needed to store the ring structure. The Ethereum Yellow Book [30] states that these events generate logs, which are then kept in the blockchain along with other information like the cost of the gas used (8 gas per byte costs to store the gas log and contact storage require 32 bytes to store the 20000 gas).



(a): Time consuming average mean ring signature time

(b): Time consuming standard ring signature deviation

Figure 5: (a) Time consuming average mean ring signature time (b) Time consuming standard ring signature deviation

Table 3: Smart contract financial costs

Five public keys, each with a signature Estimated cost			
Cases	**Cost of code**	**Deposit execution of cost**	**Total price (Gas) Price (USD)**
Quarantine at home in general 5.435,8605 (Report time)	52,700	21,122	69,811
Moderate home quarantine 7.743980,775 (Report Time)	69,788	41,143	120,1000
Strong home quarantine 4.345765,132 (Report Time)	52,499	125	52,605

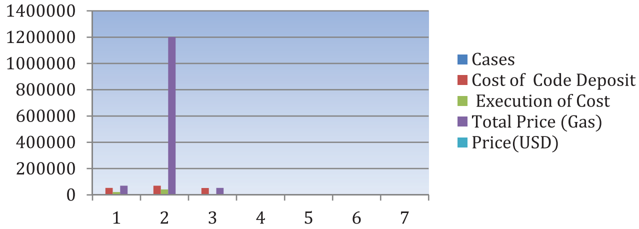


Figure 6: The smart contract in-home quarantine

5 Comparison of Proposed Model and Related Work

IoT, scalability, availability, flexibility, security, cloud-based storage, and computing solutions cannot hold the large amounts of data generated by smart devices, but blockchain may help decentralize cloud storage and computing by using a peer-to-peer network algorithm for reaching a consensus [31]. Research papers on the medical internet of things (IoT) and its related topics will be presented prior to COVID-19. Researchers and scientists from all around the world came together at this COVID-19 to conduct research on vaccine development and prevention. Data security and privacy protection based on blockchain, the study [31,32] suggests a personal health information (PHI) sharing strategy to improve electronic medical records diagnosis, they established the blockchain structure of data and technique for attaining consensus, two distinct blockchain types are there; (i) Private blockchain and (ii) Consortium blockchain. When it comes to storing personal health information (PHI), a private blockchain is used, and the safe index records of PHI are stored by a consortium blockchain. With the help of these technologies, we can make an effort to achieve data security, secure searches, access control, and privacy protection. The author introduced SecLap [33], and maker simulations that are shown in the security analysis lighted consume less energy. In [8], Hale et al. speculate that examining technology, such as 5G, IoT, drones, blockchain, and artificial intelligence, will aid in the containment of the COVID-19 outbreak's spread solely based on the technologies. In the paper [34], the author discussed the critical role played by the blockchain in the prevention and containment of the COVID-19 pandemic, and they summarized the scenario in four main areas.

1. Without the assistance of external parties, infection data will be maintained in the blockchain.
2. Donations (Money) become transparent.
3. The information is transparent in the blockchain.
4. Information diagnostics reduces the risk of infection through face-to-face contact.

Using the benefits of blockchain point-to-point communication, Torky et al. [35] have proposed a new blockchain framework that makes use of timestamps and decentralized storage to construct an alternate method of validating and storing data, as well as to find cases of infection with the unknown covid-19 virus. There are four parts to this system: a verification program subsystem; an infection; a p2p mobile application; a large scale surveillance system; and a blockchain framework. In this publication (DHP), the author suggested the notion of digital health passports (DHP), which may be used to verify that persons are disease-free; this record can be used to revitalize international tourism [36–38]. While the DHP framework makes use of a private blockchain and proof of authority, the DHP is issued by a distributed infrastructure, not a private blockchain. We will pay particular attention to Tab. 4, where personal data management and data traceability are the two most important areas of focus. By avoiding human interference, we will be able to ensure that privacy protection is not compromised.

Table 4: Briefcase of related work

Strategy	Device	Technology	Authenticity	Security	Human
BSPP [32]	System for managing patients	Blockchain	✗	√	√
Tracing contacts [10]	App + Phone	GPS + Bluetooth	✗	√	√
Code of ethics in medicine [38]	App + Phone	QR Code	√	✗	✗
SecLAP [26]	The medical of things	RFID	✗	√	√
Blockchain for P2P	Mobile application	Blockchain	✗	✗	√
Framework COVID-19 [35]			✗	√	√
Our proposed	Home security system	Blockchain	√	√	√

6 Conclusion

Increasingly, the coronavirus is becoming well-known throughout the world. When dealing with a problem that is spreading so quickly, we need to be extremely cautious. Therefore, in all aspects of life and across borders, a proper distance must be maintained and physical contact discontinued. Because of this, we proposed an approach to home-based isolation monitoring based on the blockchain's robustness and trustworthiness. Before moving on to the next phase, the use of the public and private keys of the Blockchain to construct a computer-generated household number for each household in the society. As a second example, the sensors in each smart home keep track of the number of persons who enter. Afterward, the smart gateway sends the data to a smart contract that has been made private. In order to obtain the network's isolation state, the attacker snoops about in the blockchain log. Emergency situations can be avoided by employing computer-generated household numbers to open the smart home's innovative doorway, which encrypts and hides events from virus-infected personnel. An investigation is underway to determine whether or not the suggested model is safe and appropriate for use. As we move forward, we'll look into ways to streamline the use of data broadcasting by using specific procedures and approaches to process records. We want to employ monitoring methods to authenticate data in a safe way when it comes to data usage. For this reason, we intend to leverage blockchain distribution tools and twin blockchains in order to reduce the amount of resources and processing time required. Several countries will look towards implementing liberating measures once the pandemic has been stopped. We're also thinking of awarding prizes and penalties via the blockchain's current monetary system. Strategy grades and grounding influence the synchronization of citizens.

Acknowledgement: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022TR140), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Funding Statement: This research is funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022TR140), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. Wang, W. H. Peter, G. H. Frederick and F. G. George, "A novel coronavirus outbreak of global health concern," *The Lancet*, vol. 395, no. 10223, pp. 470–473, 2020.

[2] A. J. Kucharski, T. W. Russell, C. Diamond, Y. Liu, J. Edmunds *et al.,* "Early dynamics of transmission and control of COVID-19: A mathematical modelling study," *The Lancet Infectious Diseases*, vol. 20, no. 5, pp. 553–558, 2020.

[3] A. K. Singha, N. Pathak, N. Sharma, A. Gandhar, S. Urooj *et al.,* "An experimental approach to diagnose COVID-19 using optimized CNN," *Intelligent Automation & Soft Computing*, vol. 34, no. 2, pp. 1065–1080, 2022.

[4] I. Ashraf, W. S. Alnumay, R. Ali, S. Hur, A. K. Bashir *et al.,* "Prediction models for COVID-19 integrating age groups, gender, and underlying conditions," *Computers, Materials & Continua*, vol. 67, no. 3, pp. 3009–3044, 2021.

[5] J. Sultana, A. K. Singha, S. T. Siddiqui, G. Nagalaxmi, A. K. Sriram *et al.,* "COVID-19 pandemic prediction and forecasting using machine learning classifiers," *Intelligent Automation & Soft Computing*, vol. 32, no. 2, pp. 1007–1024, 2022.

[6] S. Hsiang, D. Allen, S. A. -Phan, K. Bell, I. Bolliger *et al.,* "The effect of large-scale anti-contagion policies on the COVID-19 pandemic," *Nature*, vol. 584, no. 7820, pp. 262–267, 2020.

[7] M. Yamin, A. Ahmed, Z. M. AlKubaisy and R. Almarzouki, "A novel technique for early detection of COVID-19," *Computers, Materials & Continua*, vol. 68, no. 2, pp. 2283–2298, 2021.

[8] T. Hale, A. Petherick, T. Phillips and S. Webster, "Variation in government responses to COVID-19, *Blavatnik school of government working paper*, University of Oxford, vol. 31, no. 2020-11, pp.1–51, 2020.

[9] 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. 90225–90265, 2020.

[10] N. Jha, D. Prashar, M. Rashid, M. Shafiq, R. Khan *et al.,* "Deep learning approach for discovery of in silico drugs for combating COVID-19," *Journal of Healthcare Engineering*, vol. 2021, pp. 1–13, 2021.

[11] M. Anwar, F. Masud, R. A. Butt, S. M. Idrus, M. N. Ahmad *et al.,* "Traffic priority-aware medical data dissemination scheme for IoT based WBASN healthcare applications," *Computers, Materials & Continua*, vol. 71, no. 3, pp. 4443–4456, 2022.

[12] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo *et al.,* "A comprehensive survey of blockchain: From theory to IoT applications and beyond," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8114–8154, 2019.

[13] S. Kably, M. Arioua and N. Alaoui, "Lightweight direct acyclic graph blockchain for enhancing resource-constrained IoT environment," *Computers, Materials & Continua*, vol. 71, no. 3, pp. 5271–5291, 2022.

[14] S. Zubair and A. K. Singha, "Network in sequential form: Combine tree structure components into recurrent neural network," *IOP Conference Series: Materials Science and Engineering*, vol. 1017, no. 1, pp. 12004, 2021.

[15] D. Prashar, M. Rashid, S. T. Siddiqui, D. Kumar, A. Nagpal *et al.,* "SDSWSN—A secure approach for a hop-based localization algorithm using a digital signature in the wireless sensor network," *Electronics, MDPI*, vol. 10, no. 24, 3074, pp. 1–25, 2021.

[16] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[17] S. T. Siddiqui, M. Shuaib, A. K. Gupta and S. Alam, "Implementing blockchain technology: Way to avoid evasive threats to information security on cloud," in *2020 Int. Conf. on Computing and Information Technology (ICCIT-1441), IEEE*, Dhaka, Bangladesh, pp. 1–5, 2020.

[18] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer and C. Weinhardt, "A blockchain-based smart grid: Towards sustainable local energy markets," *Computer Science-Research and Development*, vol. 33, no. 1, pp. 207–214, 2018.

[19] Y. Li, J. Qi, L. Min, H. Yang, C. Zhou *et al.,* "CWoT-share: Context-based web of things resource sharing in blockchain environment," *Computers, Materials & Continua*, vol. 72, no. 3, pp. 5079–5098, 2022.

[20] N. Szabo, “Formalizing and securing relationships on public networks,” *First Monday*, vol. 2, no. 9, 1997. https://goi.org/10.5210/fm.v2i9.548.

[21] H. S. A. Hamatta and M. U. Bokhari, “Protocols in mobile ad-hoc networks: A review,” *International Journal of Applied Information Systems (IJAIS)*, vol. 7, no. 10, pp. 11–14, 2014.

[22] M. A. Duhayyim, F. N. Al-Wesabi, R. Marzouk, A. Ibrahim, N. Negm *et al.,* “Integration of fog computing for health record management using blockchain technology,” *Computers, Materials & Continua*, vol. 71, no. 2, pp. 4135–4149, 2022.

[23] S. T. Siddiqui, R. Ahmad, M. Shuaib and S. Alam, “Blockchain security threats, attacks and countermeasures,” *Advances in Intelligent Systems and Computing*, vol. 1097, pp. 51–62, 2020.

[24] S. F. Aghili, H. Mala, M. Shojafar and P. Peris-Lopez, “LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT,” *Future Generation Computer Systems*, vol. 96, no. 1, pp. 410–424, 2019.

[25] B. Stojkoska, L. Risteska and K. V. Trivodaliev, “A review of internet of things for smart home: Challenges and solutions,” *Journal of Cleaner Production*, vol. 140, pp. 1454–1464, 2017.

[26] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and G. Das, “Everything you wanted to know about the blockchain: Its promise, components, processes, and problems,” *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6–14, 2018.

[27] V. Buterin, “A next-generation smart contract and decentralized application platform,” *Ethereum White Paper*, vol. 3, no. 37, pp. 36, 2014.

[28] X. R. Zhang, W. F. Zhang, W. Sun, X. M. Sun and S. K. Jha, “A robust 3-D medical watermarking based on wavelet transform for data protection,” *Computer Systems Science & Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.

[29] C. Dannen, *Introducing ethereum and solidity*, vol. 1, Berkeley: Apress, pp. 159–160, 2017.

[30] A. Gupta, S. T. Siddiqui, S. Alam and M. Shuaib, “Cloud computing security using blockchain,” *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 6, no. 6, pp. 791–794, 2019.

[31] A. K. Singha, A. Kumar and P. K. Kushwaha, “Speed predication of wind using artificial neural network,” *EPH-International Journal of Science and Engineering*, vol. 1.1, pp. 463–469, 2018.

[32] A. Zhang and X. Lin, “Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain,” *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–18, 2018.

[33] S. F. Aghili, H. Mala, P. Kaliyar and M. Conti, “SecLAP: Secure and lightweight RFID authentication protocol for medical IoT,” *Future Generation Computer Systems*, vol. 101, no. 4, pp. 621–634, 2019.

[34] M. C. Chang and D. Park, “How can blockchain help people in the event of pandemics such as the COVID-19?,” *Journal of Medical Systems*, vol. 44, no. 5, pp. 1–2, 2020.

[35] M. Torky and A. E. Hassanien, “COVID-19 blockchain framework: Innovative approach,” arXiv preprint arXiv:2004.06081, vol. abs/2004.06081, 2020.

[36] C. M. Angelopoulos, A. Damianou and V. Katos, “DHP framework: Digital health passports using blockchain–use case on international tourism during the COVID-19 pandemic,” arXiv preprint arXiv:2005.08922, vol. abs/2005.08922, 2020.

[37] S. Chen, L. Yang, C. Zhao, V. K. Varadarajan and K. Wang, “Double-blockchain assisted secure and anonymous data aggregation for fog-enabled smart grid,” *Engineering*, vol. 8, no. 3, pp. 159–169, 2022.

[38] F. Liang, “COVID-19 and health code: How digital platforms tackle the pandemic in China,” *Social Media Society*, vol. 6, no. 3, pp. 1–4, 2020.