electronics

MDPI

Article

Blockchain Use in IoT for Privacy-Preserving Anti-Pandemic Home Quarantine

Jinxin Zhang and Meng Wu *

School of Computer Science & Technology, Nanjing University of Posts and Telecommunications,
Nanjing 210023, China; 2017040237@njupt.edu.cn
* Correspondence: wum@njupt.edu.cn

Received: 3 September 2020; Accepted: 18 October 2020; Published: 21 October 2020

Abstract: The outbreak of the respiratory disease caused by the new coronavirus (COVID-19) has caused the world to face an existential health crisis. To contain the infectious disease, many countries have quarantined their citizens for several weeks to months and even suspended most economic activities. To track the movements of residents, the governments of many states have adopted various novel technologies. Connecting billions of sensors and devices over the Internet, the so-called Internet of Things (IoT), has been used for outbreak control. However, these technologies also pose serious privacy risks and security concerns with regards to data transmission and storage. In this paper, we propose a blockchain-based system to provide the secure management of home quarantine. The privacy and security attributes for various events are based on advanced cryptographic primitives. To demonstrate the application of the system, we provide a case study in an IoT system with a desktop computer, laptop, Raspberry Pi single-board computer, and the Ethereum smart contract platform. The obtained results prove its ability to satisfy security, efficiency, and low-cost requirements.

Keywords: COVID-19; IoT; blockchain; smart contract; authentication; privacy

1. Introduction

Coronavirus disease 2019 (COVID-19) [1] is an infectious disease caused by the coronavirus SARS-2. The infection broke out and spread rapidly in various countries around the world. As of 5 October 2020, more than 35 million cases have been reported across 188 countries and territories, resulting in more than 1 million deaths [2]. The fatality rate of COVID-19 is 2–5%, and the virus has caused many deaths worldwide as it is highly infectious [3]. All countries have made considerable efforts to deal with the pandemic. Hsiang et al. believe that anti-contagion policies (closing schools and restricting people to their homes) have significantly and substantially slowed this growth. The policy packages now deployed are achieving large, beneficial, and measurable health outcomes [4].

Approaches in different countries have been diverse [5]. As the most common measure, home segregation (stay-at-home or shelter-in-place) refers to managing residents in a home environment. The purpose of home segregation is to prevent the spread of infection by the movement of physically diagnosed patients or patients who may be in a latent period through physical quarantine. During the outbreak, many people were infected with the virus unconsciously, and home segregation became an effective way to stop the spread of the virus. However, it was still necessary to put relevant quarantine restrictions in place for multinational travelers. To adopt an anti-infectious policy against the COVID-19 pandemic, including managing family isolation, governments used police patrols, CCTV, drones, geo-fences, and other measures [6]. However, these measures take up a lot of social resources.

Some companies have developed alternative mobile apps, which use GPS to track and locate, and Bluetooth to monitor distance [7]. There are defects in using the mobile phone's GPS and Bluetooth as the monitoring method, as it does not guarantee that the mobile phone corresponds to the owner at all times, and there is a possibility of human–machine separation. Even people use wearable devices such as smart bracelets, it is difficult to eradicate the above situation at all.

With the use of the IoT in the home, the condition of the home can be sensed in real-time. One service supported by the IoT is the smart home system, which is also an option for the supervision and management of home segregation. The most practical and essential home control functions in the smart home system include smart home appliance control, security system, intercom access control, etc.

Notably, the location data of each resident is private information, and protecting personal privacy is a concern that needs attention during this pandemic. Besides, the analysis and processing of private data are highly centralized at present. It has the hidden danger of a single point of failure and is vulnerable to targeted attacks [8]. To address this issue, blockchain technology [9] may be an alternative suggestion.

The combination of blockchain and IoT is promising and leads to notable changes in many industries, paving the way for new business models and novel distributed applications. In their work [10], they describe that the combination of blockchain and IoT can promote resource sharing and make the service market between devices possible.

Tosh et al. [11] pointed out that the public and distributed peer-to-peer ledger capabilities of the blockchain will benefit cloud computing services, which need to include functions such as assured data provenance, auditing, management of digital assets, and distributed consensus. The underlying consensus mechanism of the blockchain allows the construction of a tamper-proof environment. By using encryption methods, transaction blocks are chained together to enable the immutability of records.

Mengelkamp et al. [12] combine blockchain with smart grids to create a more efficient system. As the grid evolves, intermittent energy and micro-grids will become a significant part of the energy supply. By balancing electricity demand and supply through micro-transactions, power resources distributed throughout the network can be utilized more appropriately.

Scenarios such as logistics and transportation and sensor data are an important part of the Internet of Things. Lucena et al. [13] analyze the feasibility of a blockchain-based fresh goods quality tracking system in actual transportation chain application scenarios. The application of blockchain technology to save and transmit data enables suppliers, transportation units, and food companies to grasp the status of fresh goods in transit in real-time. The system also realizes the immutability of sensor data and the traceability of supply chain data, ensuring the security of the food supply.

The blockchain was initially a distributed and immutable ledger of transactions for cryptocurrency systems. Thanks to the contraption of smart contracts [14], the blockchain has now strengthened into a promising platform for developing distributed and trustworthy applications. In this manuscript, we propose a scheme to show the potential of the combination of the Internet of Things and blockchain to provide applications for segregation management and implementation. Our scheme, while realizing the decentralized supervision of home segregation, also ensures the security requirements of personal data integrity and privacy protection.

In summary, the contributions of this work are threefold:

- Use the security system in a Smart Home to record the daily in and out status of quarantined personnel and report it after processing. The Centers for Disease Control (CDC) officer designs and issues virtual house numbers and attaches digital signatures to make a light authentication for IoT devices. The purpose is to create a reliable virtual community easy to manage.
- Apply smart contracts in the blockchain to examine the reported segregation according to definite rules. Write the abnormal data that does not meet the segregation requirements in the low-cost log of the blockchain.
- The public–private key pair of the blockchain system is used to design security protection measures in a targeted manner. The system uses the community as the basic unit to report the segregation and does not involve specific household information. Using the public keys of some other devices in the same community to complete the ring signature can ensure the anonymity of residents and

maintain data integrity. As for infection events that require special handling, household-specific information with a virtual house number is encrypted with an officer's public key to ensure data authenticity and security before it is sent to the pandemic prevention workers.

The rest of this paper is organized as follows: Section 2 describes the background. Section 3 describes the overall design. We present the system implementation and the performance evaluation results in Section 4. Open issues are discussed in Section 5. Section 6 concludes this paper and presents some future work.

2. Background

2.1. The Internet of Things

The Internet of Things (IoT) refers the ability to use various information sensors to collect information about any object that needs to be monitored, connected, and interact in real time, and to transmit data through the network to realize the ubiquitous connection of things and other things, and things and people. This results in intelligent perception, recognition, and management. The IoT digitizes the real world, and its application scope is immense, mainly including the following sectors: smart environments [15] (homes, offices, and factories), personal and social fields [16], etc.

Connectivity, perception, and intelligence are the three major characteristics of the development of the IoT. The Internet of Things achieves an all-round perception through the integration and convergence of network communications, big data analysis, edge computing, deep learning, artificial intelligence, and blockchain. Normalized management can effectively aggregate all links, share resources and data, and provide objects with one-step and all-round services.

A smart home represents the IoT application that is close to life. It can control lights, windows, temperature, and humidity, etc., and may also include home security, such as access control or alarms [17]. When connected to the internet, the system connects via a hub (or gateway) that can connect smart security devices such as access control, smart locks, and cameras with internet big data and cloud services to achieve home protection. In this paper, we assume that the relevant devices can accurately sense the entry and exit of people.

2.2. Blockchain

Blockchain technology was introduced in 2008 by Takemoto [9] and has since attracted much attention due to its decentralization, anonymity, and the inability to rewrite over it. Blockchain breaks through the limitations of traditional central technology, and thus has many potential applications. For example, blockchain can create decentralized cryptocurrency, representing a revolution in financial and other industries. Unlike traditional digital currency systems, individuals can trade directly with each other on untrusted networks without relying on third-party agencies.

The operation of the blockchain mainly relies on four components: the encryption algorithm, transaction processing, consensus algorithms, and distributed ledger technology [18], as shown in Figure 1. Encryption algorithms ensure the data of the entire network are transparent and verifiable while preserving the anonymity of personal information. Transactions continuously generated from the blockchain nodes describe the current state of the blockchain and are then assembled into new blocks. The distributed ledger records transactions between network participants. This shared ledger reduces the time and expense incurred by mediating different ledgers. Using the consensus algorithm eliminates the possibility of data modification, replacing third-party agents in traditional applications.

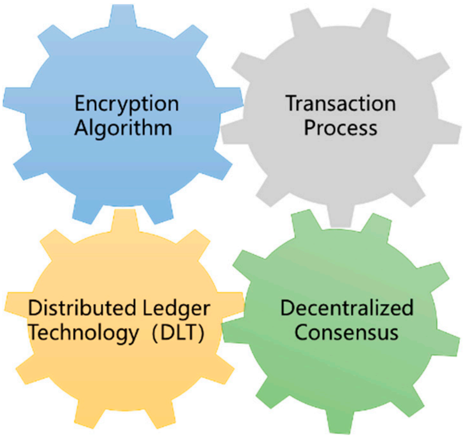


Figure 1. Blockchain is mainly operated by four components.

Each block contains the following information: the hash value of the current block, the hash value of the previous block, the timestamp when the consensus is reached, and the transaction information.

2.3. Smart Contract

The concept of smart contracts can be traced back to the 1990s [14], which is much earlier than the blockchain technology. Szabo pushed the concept of a contract from a paper relationship to a confirmed digital relationship. However, due to the lack of a credible performance environment, the smart contract could not initially be used for practical applications. Blockchain can provide a credible execution environment for smart contracts and forms the most crucial piece of the system for the application of smart contracts. Narrowly, a smart contract is an algorithmic program code that digitizes the complex relationship between people, legal agreements, and computer networks. A smart contract is a computer protocol that can achieve autonomous execution and the result can be checked after deployment. Its application is not only limited to the financial field; it can also be used in distributed computing, the Internet of Things, and other fields.

Smart contracts can perform reliable transactions and operations in the blockchain ecosystem without third parties, relying on the communication and consensus between blockchain nodes. Once the contract starts, it will execute under the terms of the computer code, and the execution status will automatically check the other nodes so that it can track the progress and tampering is impossible.

Smart contracts can be applied in many fields, such as the medical field, knowledge copyright protection, important data certification, and the IoT, and their employment can achieve positive results in all these areas. Smart contracts spread through the peer-to-peer (P2P) network in the blockchain ecosystem. The verification node saves the received contract in the memory and waits for the trigger to process the contract. In the consensus stage, the verification node packages all contracts saved in the most recent period into a contract set, calculates the hash value of this contract set, assembles it into blocks, and spreads it to the entire network. After receiving the verification set, the other verification nodes compare and verify the received information with the contract set saved by them and send a copy of the approved contract set to further verification nodes. Through many rounds of sending and comparison, all the verification nodes finally reach an agreement on the latest contract set within the specified time.

Ethereum is a smart contract and electronic payment system [19]. Like Bitcoin, Ethereum is a distributed ledger based on blockchain. However, as it is not limited to the digital currency attributes of Bitcoin, Ethereum provides a platform for developing secure and verifiable decentralized applications (dapps).

2.4. Ring Signature

A ring signature is a digital signature scheme originally proposed by Rivest et al. [20]. It is a simplified group signature. In the ring signature, there are ring members but no managers.

Ring signatures can meet the following security requirements:

1. Correctness: If the message is signed according to the correct signature steps and no one tampers with the signature during the propagation process, then the ring signature meets the signature verification equation.
2. Anonymity: Even if the adversary illegally obtains the private keys of all signers, they can determine the probability that the true signer does not exceed $\frac{1}{n}$, where n is the number of ring members.
3. Unforgeability: Without knowing the private keys of any members, even if an external attacker can obtain the signature of any message m from a random oracle that generates a ring signature, the probability that they will successfully forge a legal signature is negligible.
4. Spontaneous: A ring signature can realize the primary function of the group signature but does not require trusted third parties or group administrators to participate.

The main process is as follows:

Setup: The message sender selects several members to form a ring member set $R = \{R_1, R_{2,}, \ldots, R_n\}$ and ring members' public keys constitute a ring public key set $K = \{K_1, K_{2,}, \ldots, K_n\}$.

Signature: Using message m, the private key k_M of the M message senders and public key set K are employed to generate digital signature σ.

Verify: The message receiver verifies the validity of (m, σ).

3. Proposed Overall Architecture

As shown in Figure 2, the households' homes are equipped with a security system, such as cameras, infrared sensors, and smart magnetic door suction devices, which are connected to the outside world through smart gateway devices. The system does not allow unauthorized device access to prevent malicious behavior from consuming social resources. Smart gateways in the same community form a cluster and have the same cluster name.

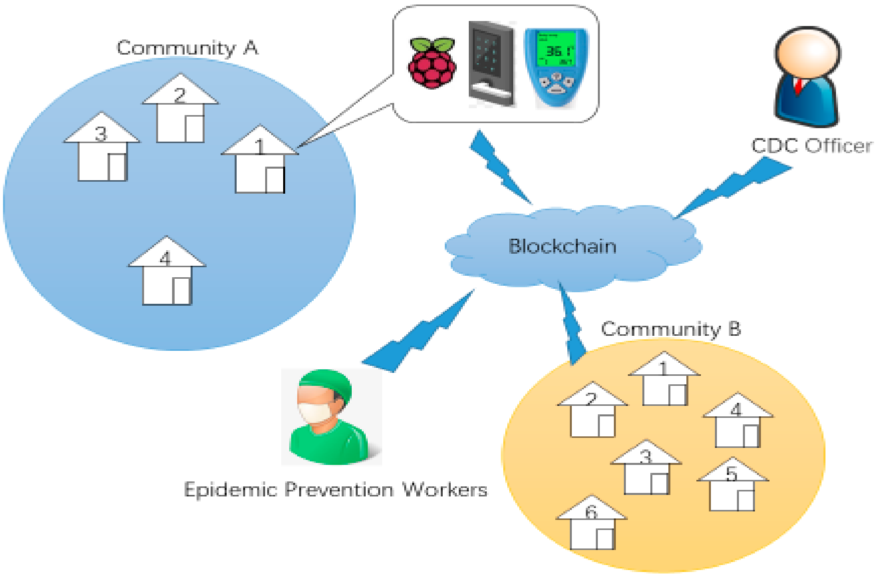


Figure 2. Illustration of the considered smart home system.

Each household's smart gateway collects related information and completes formatting and aggregation. It regularly sends the complete information to the relevant smart contract. This smart contract is issued by the officer and is related to the quarantine regulations. The specific manifestation is the threshold of the associated indicator. No one can edit contracts after deployment.

To protect the privacy of households, the ring signature can be created using the public keys of other users in the same community. The smart contract analyzes the reported data. If the value exceeds the specified threshold (such as multiple entries and exits or going outside for a lengthy period), the smart contract notifies the management department of the related data, along with the digital signature in the form of an event. The officer verifies the authenticity of the data through the signature. In this way, the officer can learn about an abnormal situation in the community and take relevant countermeasures. In the case of an emergency, the smart gateway directly sends a rescue request to the pandemic prevention personnel.

Because the reported data are not confidential information and considering the actual situation of the limited resources of smart devices, the data are not encrypted. Except for the request for assistance, all data in the household should be anonymous, and privacy is preserved for the entire overlay network.

To deploy this system, we rely on a public blockchain that can implement smart contracts. Relatively, private blockchains are suitable for mostly restricted environments. Once the system is deployed, it is hard to add new users. However, public blockchains have considerable scalability and flexibility in the system.

We can deploy our system under the IoT smart home architecture. As shown in Figure 2, the smart home system includes the following components:

Smart Home: A family-aware ecosystem based on IoT devices. The IoT devices in the system mainly include sensors that can sense environmental data and send these data to service providers or users. The public blockchain is open to any user.

Pandemic prevention workers (W): Frontline staff who handle emergencies accordingly.

CDC officer (O): Managers of the fight against the pandemic who set the basic requirements for quarantine and publish them in the form of smart contracts. They check the essential local conditions.

Next, we describe the entire life cycle of the system.

3.1. Initialization Phase

Our scheme can be applied to management of the community, which requires an initialization phase. The IoT devices considered in the smart home include storage devices, smart gateways, actuators, sensors, etc. These devices are massive, heterogeneous, and have limited resources, which contradicts the basic storage capacity and computing power requirements needed by blockchain technology. To solve this contradiction, our design uses computers and smart gateways as the major participants of the blockchain. The officer (O) transfers a certain fee to the wallet of the device in advance for the system construction.

In the system, the device is introduced into the blockchain to obtain a unique public/private key pair and blockchain address in the blockchain. The initialization process is similar to issuing certificates (virtual house numbers). The virtual house number of each set of equipment includes the community number, blockchain address, and issues after being signed by the officer (O)'s private key $k_{officer}$. Once the blockchain verifies the authenticity of all devices, it has completed the establishment of a virtual community.

Virtual house number (Vhm)
Community ID: AA
Blockchain Add: BB
Signature by $k_{officer}$

3.2. Operation Phase

In the system, only devices with virtual house numbers issued by officers are legal. The smart contract sets the threshold of data involved in quarantine management (access times, the maximum time to go out from the home, etc.). The sensors in the smart home (A1, A2) send perceived information to the smart gateway. The smart gateway can select the public keys of some devices in the same community to sign the information and send it to the corresponding smart contract for analysis. The threshold determines the standard of the quarantine policy. If the data exceed the threshold, the smart contract creates an event and sends the abnormal data with a ring signature to the officer. We assume that the perceived data are final and there is no need to use cloud devices to store data, as shown in Figure 3.

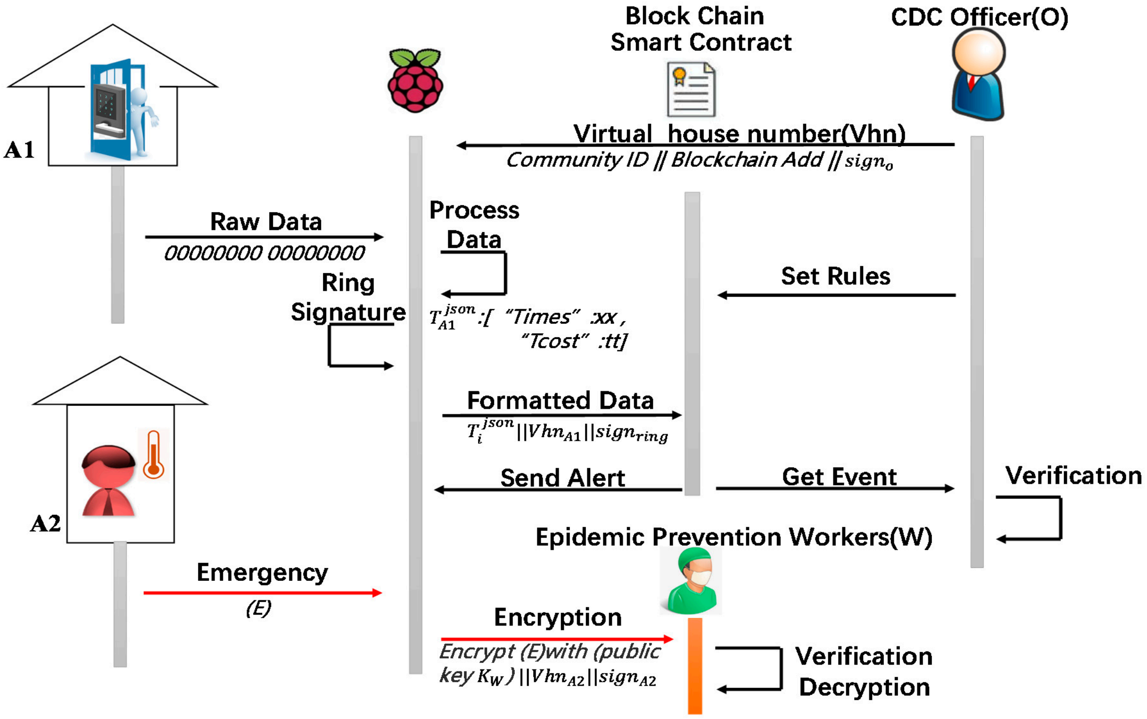

Block Chain
Smart Contract
CDC Officer(O)
A1
Virtual house number(Vhn)
Community ID || Blockchain Add || $sign_o$
Raw Data
00000000 00000000
Process
Data
Ring
Signature
Set Rules
T_{A1}^{json}:["Times" :xx , "Tcost" :tt]
Formatted Data
$T_i^{json}||Vhn_{A1}||sign_{ring}$
Send Alert
Get Event
Verification
A2
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 the system execution.

The public data only include basic personnel access information and do not require encryption. However, from the perspective of protecting privacy, data protection must be considered, so the ring signature method is used. On the blockchain, the public keys of other devices in the same community can be easily captured and combined with the device's key to create ring signatures as shown in Algorithm 1. The ring signature's features are suitable for this application scenario. It can ensure that information has not been tampered with and allow signers to sign messages anonymously. After mixing with the public keys of other devices, it is impossible to recognize which member signed the message.

Algorithm 1 Ring Signature

```
function SIGNATURE (data)
    if smart gateway chose anonymity on blockchain then
        hash_d ← calculate hash of the data
        Create the digital Signature using hash_d and signers private key sks
        Mix the signature with another smart gateway group to form a ring
    end if
end function
```

Considering the different quarantine policies in different regions, the thresholds of the related parameters (frequency and duration of going out) in the smart contract are set by the officer following the requirements. The smart gateway gathers the relevant information within an interval (for example, per day) and sends it to the smart contract created using Algorithm 2 by the officer. The officer's equipment monitors events and verifies the ring signature to determine the authenticity of the data. After the verification is complete, the officer can learn about the violation of a quarantine order in the community and promptly develop an appropriate response (increasing the number of patrols, increasing public awareness, etc.).

Algorithm 2 The smart contract home quarantine rules

```
Input: quarantine state h_state, ring signature ring_s
Output: result
Require: policyCheck ← false,
         policyThreshold list   policies
if this request is from the smart gateway then
    p ← policies
    if p.policy = "meet" then
        policyCheck ← true.
    else
        policyCheck ← false.
    end if
    result ← policyCheck
end if
Trigger event reportResult (h_state, ring_s).
```

We can also consider the occurrence of public health events. In response to the occurrence of infection symptoms in A2 and the necessity for targeted treatment (sample collection, the concentration of quarantine, etc.), the home gateway will use the public key K_w of the pandemic prevention worker (W) to encrypt personal information and the virtual house number. Only the private key of the pandemic prevention worker (W) can decrypt the information.

3.3. Summary

After the smart contract is created, the officer sends it to the blockchain in the form of transactions, where it is verified by the miners. If the verification is successful, the contract is deployed, and the officer will receive an address. This smart contract address is public, and any user can use it without restrictions.

The public blockchain is a flexible and decentralized system that has enough scalability. It has powerful resistance to forging and tampering. Similarly, no one can change it after the smart contract is deployed in the blockchain. Using ring signatures for information prevents tampering while ensuring the privacy of the users. The important information encrypted with the relevant party's public key can protect the data security and the virtual house number ensures the authenticity of the identity.

4. Experiments and Results

As mentioned above, the proposed system uses an Internet of Things device to perceive the state of home quarantine of the households, and then uses smart contracts for analysis and processing. In this section, we evaluate the safety, time, and operating costs of our method.

4.1. Use Case Scenarios

The use cases considered in the home quarantine case study are as follows:

(1) Strong home quarantine: In the initial stage of the infection outbreak, the state of the spread of the virus is undiscovered, so strict quarantine measures are introduced in areas with severe outbreaks. The policy prohibits visits to avoid cross-infection. It also prohibits all family members from leaving the home. The pandemic prevention staff provide for the necessities of the family.

(2) Moderate home quarantine: In the general period at the beginning of the pandemic, a brief amount of time outside of one's household is allowed, such as for dumping garbage and picking up takeout food, but this is restricted.
(3) General home quarantine: Many regions have issued more reasonable quarantine policies. Residents are not allowed to leave their residence unless they are engaged in necessary work or must go out to purchase required items.

In these application cases, the CDC worker needs to grasp the relevant information of each family. If malicious forgery or modification of this information occurs, it will have serious consequences for pandemic prevention work. This information is private. Therefore, the authentication, integrity, and privacy of these messages are critical.

4.2. Evaluation Framework

To evaluate the time and energy consumption of our method, we used three types of end nodes: a desktop computer, laptop, and Raspberry Pi single-board computer. As the officer's device, the laptop was mainly used to issue virtual house numbers, create smart contracts, and monitor the logs in the blockchain. As a smart gateway, the Raspberry Pi was responsible for collecting and aggregating information, completing ring signatures, connecting to the blockchain, and encrypting emergencies. The desktop computer was used for decryption as the worker's device.

We used Ethereum as a blockchain to develop a smart contract that meets our approach function using Solidity language. For writing and compiling the smart contract, we used Remix, which is a browser-based integrated development environment (IDE) for Solidity (i.e., the programming language for writing smart contracts) [21]. We chose web3.js to communicate with the corresponding geth client through HTTP connections for deploying and monitoring the states of the smart contract. The frame is illustrated in Figure 4.

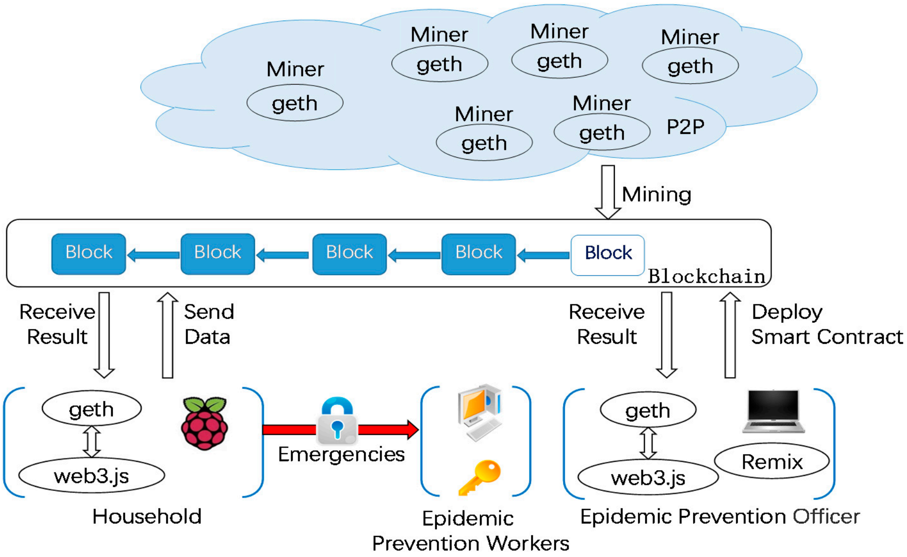


Figure 4. Software used in the case study.

4.3. Evaluation Results

The adversary may be a sensing device in a smart home, a smart gateway, or other nodes in the P2P network. It can tamper with or delete stored information, create false events, etc. Considering the above situation, our purpose is to respond to such security threats. Our attention is placed on the overall macro security situation. For an independent node, we assume that after issuing a virtual house number, it will be regarded as an honest one that can truly reflect the actual isolation status in the house. Table 1 summarizes the solution that allows our method to meet the safety requirements.

Table 1. Safety requirements solution.

Requirement	Solution	State
Integrity	Hashing of data blocks	Each new block contains the hash of the previous block, which guarantees that the information has not been modified
Confidentiality	Public-private key pair	Encrypt the data with the other party's public key in the blockchain, and only the corresponding private key can decrypt the data
Availability	Smart contracts	Automated continuous verification ensures that the data quality is more reliable and trustworthy so that decisions can be more transparent, efficient, and refined
Anonymity	Ring signature	When mixed with other public keys, the receiver cannot tell which member signed the message
Scalability	P2P network	P2P networks are one of the best solutions for meeting scalability at a large scale

4.3.1. Security Requirements Evaluation

Designers need to consider three major security requirements: confidentiality, integrity, and availability. Confidentiality guarantees that only authorized users can participate in the system. Integrity is responsible for messages sent to the destination with no changes, and availability means that users can always handle the data when needed. We evaluated the security margin of our proposed method under various threats.

Some potential attack scenarios are as follows:

- Sybil attack: A Sybil attack is a means of attacking data redundancy mechanisms. Malicious nodes pretend to be multiple nodes by creating multiple identifiers in the P2P network. The data that needs to be backed up by various nodes are fraudulently backed up by the same malicious node. In our design, each smart gateway can only have one virtual house number. Each time the information is reported, a virtual house number should be attached to it to identify the community to which it belongs. The officer approves all virtual house numbers with the private key, so attackers cannot use fake virtual house numbers.
- Denial of Service (DoS)/Distributed DoS (DDoS): Attackers try to block the authentic users from accessing services in the network. Here, the attackers increase the traffic in the network by initiating an enormous amount of useless information to cause network congestion. The decentralized architecture of the blockchain can be resistant to DoS/DDoS attacks. Even if the attackers block some nodes successfully, they cannot block all nodes of the network. Furthermore, transactions in the blockchain require payments. For example, in Ethereum, the cost of a transaction is related to the size of the packet transmitted. For this reason, the attackers are prevented from transmitting transactions endlessly.
- Spoofing attack: A spoofing attack, in cybersecurity, refers to an object pretending to be the identity of another object in an attempt to gain one's trust, enter the system, and steal data or funds or spread malware. In our design, an attacker cannot spoof another object's identity since they cannot spoof its private key.
- Linking attack: A linking attack occurs when the opponent collects auxiliary information of an object from multiple data sources and then combines these data to determine the overall picture of the target. In the blockchain, the attacker establishes a link between multiple transactions or data ledgers with the same public key to find the target. Since the virtual house number only contains general community information and does not contain the actual residential address, all relevant information only exists in the blockchain log and cannot connect to other information. Even for public health incidents, the personal information of households needed in the design is encrypted

using the public key of the worker. Under the premise that the worker's private key does not leak, the encrypted data cannot contact an object.

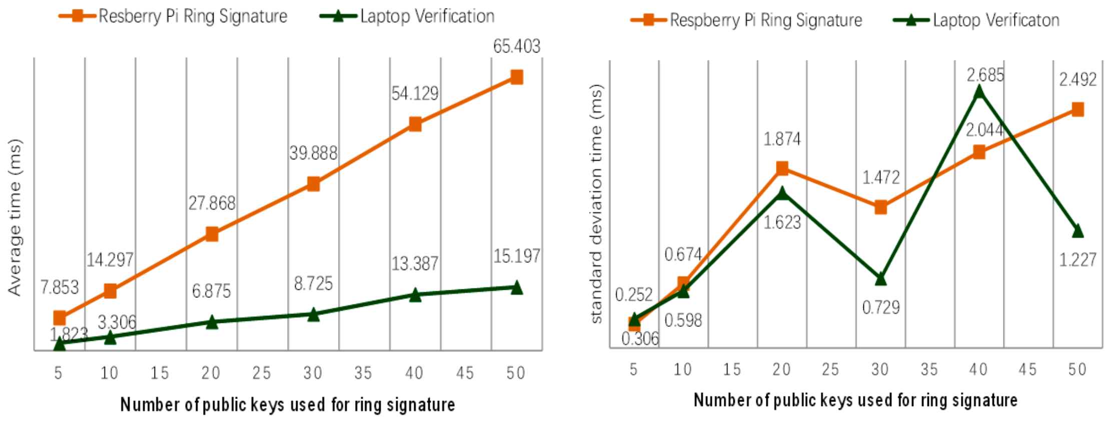
4.3.2. Time Consumption

The specifications of these devices are listed in Table 2. The computer corresponds to the user devices in the system and the single-board computers correspond to the local gateways. In the system, Raspberry Pi uses the public keys of other devices to execute ring signatures and the laptop verifies the signatures. From the experiment, we observed that for the Raspberry Pi, the time required to verify the signature is directly proportional to the number of public keys used. In comparison, when using a laptop with a better performance to verify the signature, the slope of the time-consuming curve is relatively low. In both cases, the standard deviation is low, which proves the stability of the calculation.

Table 2. Specifications of devices.

Device	CPU	Operating System	Memory	Hard Disk
Dell OptiPlex 7050	Intel Core i7, 3.4 GHz	Windows 7 Home (64 bit)	8 GB	128 GB SSD + 2 TB
Lenovo k4450	Intel Core i5, 1.9 GHz	Windows 10 Home (64 bit)	12 GB	1 TB
Raspberry Pi 4 Model B	quad-core ARM Cortex A72, 1.5 GHz	Raspbian (buster-full)	2 GB SD RAM	32 GB (micro SD card)

Figure 5 presents the average and standard deviation of the ring signature using different numbers of public keys employed in the 50 conducted experiments. We use Rivest-Shamir-Adleman (RSA) algorithm to construct a one-way trapdoor function. The abscissa represents the number of other devices (X_i) in the same community that uses the public key to ring signatures. In (a), the average time of ring signature increases approximately linearly as the number of public keys used by other devices increases. In (b), the standard deviation of the ring signature fluctuates slightly, but it also shows a trend of rising with the number of public keys used. For encrypted transmission for emergencies, we verified the time consumption of the encryption with Raspberry Pi and decryption with the computer. The encryption and decryption algorithm are written by Python 3.7. And the encryption required about 380 ms and decryption about 50 ms.



(**a**) (**b**)

Figure 5. Time-consuming mean and standard deviation of ring signatures. (**a**) Average time of ring signature. (**b**) Standard deviation of ring signature.

We did not consider the time the event consumes in communication because this relies on network technology and protocols. Notably, the event execution time in the blockchain also needs to consider the different block generation times of the different consensus algorithms. For example, Bitcoin takes about 10 min to generate blocks, whereas Ethereum takes about 15 s. Taking Ethereum as an example, according to the Ethereum protocol, it charges fees for each calculation step performed in a contract or transaction. A smart contract is executed when triggered by a message or transaction, and the operation of each instruction has a specified cost, expressed in "gas" as the unit. Each process of a smart contract consumes a certain amount of gas according to its complexity. The execution of smart contracts also needs to consider the order of event execution. The more gas prices bid, the higher the execution priority, and the shorter the execution time.

4.3.3. Financial Cost

We employed the Ethereum verification platform, which uses "gas" to measure the amount of work required to complete certain tasks. Gas has a price, so the amount of gas consumed represents the cost of executing tasks. When using remix to draft smart contracts, we estimated the gas consumption of the smart contract in the various cases mentioned above. As shown in Table 3, the essential consumption is only a calculated value. The specific cost is affected by the number of reports, the bytes of reports, and other factors. For various numbers of public keys participating in the signature, we conducted the comparison shown in Figure 6. The results revealed that following the same premise, the gas consumption positively correlates with the number of public keys used. The essential reason for this is that the storage of ring signature public key information requires gas. The Ethereum Yellow Book [22] states that events generate logs and the logs are stored on the blockchain. The gas charge stored in the log is much cheaper than in the contract (the log costs 8 Gas per byte, and the contract storage is 20,000 Gas per 32 bytes).

Table 3. Estimated financial cost of a smart contract.

	Sign with Five Public Keys			Cost Estimate [1]
Case	**Code Deposit Cost**	**Execution Cost**	**Total Cost (Gas)**	**Price (USD)**
General home quarantine (report times)	51,600	20,111	71,711	4.35618509
Moderate home quarantine (report times, duration)	70,800	40,135	110,935	6.738901884
Strong home quarantine (hair-trigger)	51,400	105	51,505	3.128743332

[1] Eth: USA$368.16, Proposed Gas Price: 165 gwei, https://etherscan.io/gastracker (accessed on 16 September 2020).

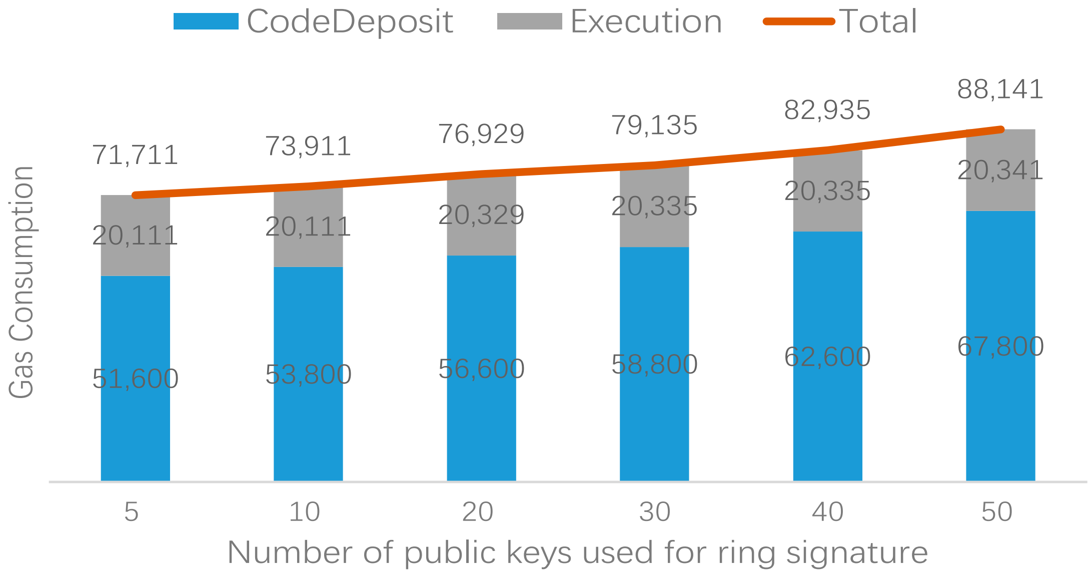


Figure 6. The smart contract gas consumption in a general home quarantine case.

4.3.4. Comparison with Related Work

The amount of data generated by smart devices has experienced explosive growth, and due to the requirements of the Internet of Things for availability, scalability, security, and flexibility, cloud-based storage and computing solutions cannot handle such large-scale data. With the help of P2P network architecture and consensus algorithm, blockchain can be used as an alternative to centralized cloud storage and computing [23].

Before the large-scale explosion of COVID-19, some papers presented research on the medical Internet of Things (MIoT) and related fields. The outbreak of the pandemic has prompted scientists, researchers, and organizations from all over the world to conduct many studies on vaccine development and pandemic prevention. However, we found that research articles are lacking in the use of blockchain technology and other scientific and technological methods as pandemic prevention methods.

A paper [24] proposed a blockchain-based security and privacy protection Personal health information (PHI) sharing (BSPP) scheme to improve the diagnosis of electronic medical systems. By designing the data structure and consensus mechanism of the blockchain, two types of blockchains, a private blockchain and consortium blockchain, are constructed. The private blockchain is responsible for storing PHI, whereas the consortium blockchain stores the safe index records of PHI to achieve data security, access control, privacy protection, and safe searches.

The author proposed a secure and lightweight mutual RFID authentication (SecLAP) protocol [25], which realizes secure communication and privacy protection in the MIoT system. Security analysis showed that the SecLAP protocol is robust in anti-synchronization, replay, reader/marker simulations, and traceability attacks. It ensures the security of forward and backward data communications. By comparing and verifying its performance, the study showed that it is lightweight and consumes fewer resources.

In [6], Chamola et al. explore the feasibility of using technologies such as the Internet of Things, drones, blockchain, artificial intelligence, and 5G to help alleviate and control the COVID-19 pandemic. The article believes that before a vaccine for this disease comes out, managing and restricting the development of the pandemic depends on the use of these technologies.

Others [26] analyzed the role of blockchain in pandemic prevention and control and summarized it in terms of four aspects. First, the infection report data are stored in the blockchain without going through any intermediary parties. This increases the efficiency of data transmission regarding infectious disease outbreaks. Second, the use of donations in kind and money becomes transparent. The entire donation process, including logistics, warehousing, and distribution, can be stored on the blockchain. Third, the information in the blockchain is open and transparent, which can prevent the spread of infectious diseases and wrong information. Fourth, the use of the blockchain to transfer diagnostic information can reduce the risk of infection through face-to-face contact.

Torky and Hassanien [27] proposed a blockchain-based framework that uses the advantages of blockchain point-to-point, timestamps, and decentralized storage to build an alternative system to verify and detect cases of unknown COVID-19 virus infection. The system includes four components: an infection verification program subsystem, a blockchain platform, a P2P mobile application, and a large-scale surveillance system. It can help governments and health authorities to detect suspected cases of coronavirus (COVID-19) and obtain the location of patients, as well as autonomously estimate and predict the risk of infection.

The authors introduced the concept of digital health passports (DHP) to verify that individuals are free from disease risks and how to use them to restore international tourism [28]. The article presents the DHP Framework, which uses a private blockchain and proof of authority for issuing digital health passports. A distributed infrastructure is employed to support the issuance of the DHP by foreign health systems and used by relevant stakeholders (such as airlines and border control authorities) for verification.

To summarize Table 4 describes the studied works. From the table, we can find that their functions are mainly focused on personnel management and data traceability. It can be found that avoiding the interference of human factors (trick systems, identity forgery, and data manipulation) is contradictory to privacy protection.

Table 4. Summary of the related works.

Approach	Equipment	Technology	Authentication	Privacy	Human Factors	Decentralization
BSPP [24]	Patient Management System	Blockchain	√	√	×	√
Contact Tracing [7]	Phone + App	Bluetooth + GPS	×	√	×	×
Health code [29]	Phone + App	QR code	√	×	√	×
SecLAP [25]	Internet of Medical Things (IoMT)	RFID	√	√	×	×
COVID-19 blockchain framework [27]	P2P-Mobile Application	Blockchain	×	×	√	√
Our Proposed	Smart home Security System	Blockchain	√	√	√	√

5. Open Issue

Our approach suffers from two main issues:

Not suitable for real-time corresponding quarantine scenarios: our method uses public blockchain. According to the consensus protocol in the blockchain, each transaction (block) is verified in each determined period. Therefore, the transaction (message) sent by the device will be performed after this period. This limits the application of this scheme in real-time scenarios.

The evolution of the cryptocurrency exchange rate: Our method relies on the public blockchain, and its cost depends on the cryptocurrency used by the blockchain system. Security services require a cost, as long as it is less than the potential loss, it is feasible. However, at the time we wrote this paper, the exchange rate of Ethereum's cryptocurrency Eth continued to fluctuate enormously. We judge that this phenomenon is affected by the pandemic and is not normal.

Private blockchain may solve these issues but at the expense of scalability.

6. Conclusions

The pandemic is still expanding rapidly. To cope with its spread, person-to-person contact must be diminished, and social distance maintained. Therefore, we proposed a home quarantine management system based on the blockchain's security and privacy protection. First, the officer uses the blockchain public and private keys system to issue virtual house numbers to households in the community. Then, the household access information is perceived by sensors of the smart home. After the information is signed by a ring signature, the smart gateway transmits it to a smart contract created according to quarantine policy. The smart contract records the process results in the blockchain log and the officer listens to the log to grasp the quarantine state. However, for an emergency, the smart gateway in the smart home encrypts the events and sends them to the pandemic prevention workers with the virtual house number. Pandemic prevention workers respond to the emergency after decryption and verification. The evaluation of the system shows that it meets the security and application requirements.

In future work, besides using ring signature technology on the data generation side, we will consider using aggregation technology to process the data and facilitate its use and transmission. On the data usage side, we will implement data access control, incorporating authentication and authorization to provide secure access to the data. For the blockchain that acts as a bridge between the two sides, we will consider blockchain sharing technology and double-blockchain [30] for reducing the resources consumed and the transaction processing time of the blockchain.

Many countries have proposed rescue plans for after the pandemic has stabilized. We consider using the properties of the digital currency of the blockchain to distribute rewards and punishments based on the degree of policy coordination of residents during the pandemic. Linking with the rescue plan will expand the scope of application of the system.

Author Contributions: J.Z. conceived the system model, performed simulations and data analyses; J.Z. and M.W. wrote the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: We would like to thank the anonymous reviewers for their comments and suggestions that help us improve the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wang, C.; Horby, P.W.; Hayden, F.G.; Gao, G.F. A novel coronavirus outbreak of global health concern. *Lancet* **2020**, *395*, 470–473. [CrossRef]
2. Johns Hopkins University. Coronavirus COVID-19 Global Cases by Johns Hopkins CSSE. Ph.D. Thesis, Johns Hopkins University, Baltimore, MD, USA, 2020.
3. Kucharski, A.J.; Russell, T.W.; Diamond, C.; Liu, Y.; Edmunds, J.; Funk, S.; Eggo, R.M.; Sun, F.; Jit, M.; Munday, J.D.; et al. Early dynamics of transmission and control of COVID-19: A mathematical modelling study. *Lancet Infect. Dis.* **2020**, *20*, 553–558. [CrossRef]
4. Hsiang, S.; Allen, D.; Annan-Phan, S.; Bell, K.; Bolliger, I.; Chong, T.; Druckenmiller, H.; Huang, L.Y.; Hultgren, A.; Krasovich, E.; et al. The effect of large-scale anti-contagion policies on the COVID-19 pandemic. *Nature* **2020**, *584*, 262–267. [CrossRef]
5. Hale, T.; Petherick, A.; Phillips, T.; Webster, S. Variation in government responses to COVID-19. In *Blavatnik School of Government Working Paper*; University of Oxford: Oxford, UK, 2020; Volume 31.
6. Chamola, V.; Hassija, V.; Gupta, V.; Guizani, M. A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact. *IEEE Access* **2020**, *8*, 90225–90265. [CrossRef]
7. Li, J.; Guo, X. COVID-19 Contact-tracing Apps: A Survey on the Global Deployment and Challenges. *arXiv* **2020**, arXiv:2005.03599.
8. Wu, M.; Wang, K.; Cai, X.; Guo, S.; Guo, M.; Rong, C. A Comprehensive Survey of Blockchain: From Theory to IoT Applications and Beyond. *IEEE Internet Things J.* **2019**, *6*, 8114–8154. [CrossRef]
9. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System; Manubot. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 20 October 2020).
10. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
11. Tosh, D.K.; Shetty, S.; Liang, X.; Kamhoua, C.A.; Kwiat, K.A.; Njilla, L. Security implications of blockchain cloud with analysis of block withholding attack. In Proceedings of the 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Madrid, Spain, 14–17 May 2017.
12. Mengelkamp, E.; Notheisen, B.; Beer, C.; Dauer, D.; Weinhardt, C. A blockchain-based smart grid: Towards sustainable local energy markets. *Comput. Sci. Res. Dev.* **2018**, *33*, 207–214. [CrossRef]
13. Lucena, P.; Binotto, A.P.; Momo, F.D.S.; Kim, H. A case study for grain quality assurance tracking based on a Blockchain business network. *arXiv* **2018**, arXiv:1803.07877.
14. Szabo, N. Formalizing and Securing Relationships on Public Networks. *First Monday* **1997**, *2*. Available online: https://firstmonday.org/ojs/index.php/fm/article/view/548/469 (accessed on 20 October 2020). [CrossRef]
15. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
16. Aghili, S.F.; Mala, H.; Shojafar, M.; Peris-Lopez, P. LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. *Future Gener. Comput. Syst.* **2019**, *96*, 410–424. [CrossRef]
17. Stojkoska, B.L.R.; Trivodaliev, K.V. A review of Internet of Things for smart home: Challenges and solutions. *J. Clean. Prod.* **2017**, *140*, 1454–1464. [CrossRef]
18. Puthal, D.; Malik, N.; Mohanty, S.P.; Kougianos, E.; Das, G. Everything You Wanted to know About the Blockchain. *IEEE Consum. Electron. Mag.* **2018**, *7*, 6–14. [CrossRef]
19. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform. White Paper 2014, 3. Available online: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf (accessed on 20 October 2020).

20. Rivest, R.L.; Shamir, A.; Tauman, Y. How to leak a secret. In *International Conference on the Theory and Application of Cryptology and Information Security*; Springer: Berlin/Heidelberg, Germany, 2001.
21. Dannen, C. *Introducing Ethereum and Solidity*; Springer: Berlin/Heidelberg, Germany, 2017; Volume 1.
22. Wood, G. Ethereum Yellow Paper. 2014. Available online: https://github.com/ethereum/yellowpaper (accessed on 20 October 2020).
23. Sharma, P.K.; Chen, M.-Y.; Park, J.H. A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access* **2017**, *6*, 115–124. [CrossRef]
24. Zhang, A.; Lin, X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. *J. Med. Syst.* **2018**, *42*, 140. [CrossRef]
25. Aghili, S.F.; Mala, H.; Kaliyar, P.; Conti, M. Seclap: Secure and lightweight rfid authentication protocol for medical iot. *Future Gener. Comput. Syst.* **2019**, *101*, 621–634. [CrossRef]
26. Chang, M.C.; Park, D. How Can Blockchain Help People in the Event of Pandemics Such as the COVID-19? *J. Med. Syst.* **2020**, *44*, 1–2. [CrossRef]
27. Torky, M.; Hassanien, A.E. COVID-19 blockchain framework: Innovative approach. *arXiv* **2020**, arXiv:2004.06081.
28. Angelopoulos, C.M.; Damianou, A.; Katos, V. DHP Framework: Digital Health Passports Using Blockchain. *arXiv* **2020**, arXiv:2005.08922.
29. Liang, F. COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China. *Soc. Media Soc.* **2020**, *6*, 2056305120947657. [CrossRef]
30. Chen, S.; Yang, L.; Zhao, C.; Varadarajan, V.; Wang, K. Double-blockchain Assisted Secure and Anonymous Data Aggregation for Fog-enabled Smart Grid. *Engineering* **2020**, in press. [CrossRef]

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.