Design and research of a smart monitoring system for 2019-nCoV infection-contact isolated people based on blockchain and Internet of things technology

Ling Zheng
North China Electric Power University
Chunjian Xiao (2276068980@qq.com)
North China Electric Power University https://orcid.org/0000-0002-8523-9891
Fei Chen
North China Electric Power University
Yonghong Xiao
Zhejiang University

Research article

Keywords: Internet of Things, Blockchain, 2019 nCoV, mentoring, isolators

Posted Date: March 23rd, 2020

DOI: https://doi.org/10.21203/rs.3.rs-18678/v1

Design and research of a smart monitoring system for 2019-nCoV infection-contact isolated people based on blockchain and Internet of things technology

ZHENG Ling[1], XIAO Chunjian*[1], CHEN Fei[1], XIAO Yonghong[2]
zhengling@ncepu.edu.cn[1]
*correspondence to: 2276068980@qq.com[1]
chenfei@ncepu.edu.cn[1]
xiao-yonghong@163.com[2]

Abstract

Objective: In order to cope with a sudden outbreak of new coronavirus infection, a large number of potential infected persons need to be isolated. A new smart monitoring system which integrates Internet of things and blockchain technology to monitor isolated people in real time was design and studied.

Methods: A internet of things devices will collects the location and physical data of isolated people, the data will be sent to master devices which will integrate and format those data and transfer to a smart contract. A smart contract compares and analyses the data with the threshold which is predefined. When the data exceed the threshold, the smart contract will alert the master device, which will notify the isolated person and center for disease control and prevention, the event will be stored in the consortium blockchain. The blockchain does not store the isolated people's details, which are stored in electronic health records linked to the blockchain to guarantee the data safety.

Results: This system realizes the effective real-time monitoring of isolators including their physical condition and geographical position on the premise of protecting their privacy and security.

Conclusion: By the system, the center for disease control and prevention can respond quickly according to their alerts. It has the advantages of good integrity, tamper-proof, and transparency to isolators.

Keywords: Internet of Things, Blockchain, 2019-nCoV, mentoring, isolators

Backgroud

The new coronavirus infection (COVID-19) that broke out in Wuhan, China in December 2019 has become a severe public health crisis. As of February 27, 2020, 82294 people have been infected [1]. Disease prevention and control has become the most urgent task in China, and the government has invested a lot of manpower and material resources to control the epidemic. According to the basic theory of infectious disease control, eliminating the source of infection, cutting off the transmission route, and protecting the susceptible people are the most effective measures. At the current stage, due to the lack of effective vaccines and preventive drugs, eliminating the source of infection and cutting the transmission route has become a very urgent task. As far as the source of infection is concerned, people who are in close contact with patients may become new patients or new sources of infection. For this reason, it is very important for these people to take quarantine and medical observation. According to the current practice, most of the close contact people use the home isolation method. In order to ensure the isolation effect, the community needs to strictly control the isolated people, and it is also necessary to timely understand the dynamics of them and whether an infection occurs; according to the latest data of the National Health and Health Commission, the number of people are receiving home isolation and medical observations has reached 523,183 [1]. Observing these people requires a lot of manpower and material resources, putting a huge burden on the prevention and control of

this quick spreading disease, and it is difficult to achieve scientific management. If modern information network technology is applied, the isolation process will be greatly simplified and the isolation effect will be significantly improved, besides, the secondary damage to the isolated persons will be reduced [2]. This article designed a smart monitoring system which uses sensors to record the physical condition and geographic location of the isolated people to monitor them in real time. For example, when a rapid rise in body temperature occurs, medical personnel are notified in a timely manner. In addition, an alarm is triggered when they leave the quarantine area, and the Track personnel locations to prevent further infection.

The rapid development of the Internet of Things (IoT) and wearable devices has provided new possibilities for smart medicine, especially remote monitoring of isolated people. Using the Wireless Body Area Network (WBAN), the isolator is equipped with a wearable monitoring device, which can measure heart rate, breathing and temperature and other vital indicators in real time [3]. A-geofence is a virtual perimeter of a real-world geographic area [4]. Geofences could be dynamically generated—as in a radius around a point location, or a geo-fence can be a predefined set of boundaries (such as school zones or neighborhood boundaries). Through the wearable monitoring device, the position and physiological information of the isolated people is sent to the center of disease control and prevention (CDCP) staff in real time, so as to ensure that the isolated people is within the proper range and grasp the incidence of the quarantine in real time.

However, because IoT devices are prone to information leakage during data transmission, medical data is very vulnerable to hackers. Therefore, in a real-time monitoring, the privacy of the isolated people must be protected, at the same time, the data recorded by it must be easy to manage and transmit. Anonymity and tamper-proof are important features of blockchain technology [5], which ensure the integrity and safety of personal information. Therefore, blockchain can be used as a distributed ledger to store data in this system.

Objectives and methods

Objective

For better monitoring the isolated people during the epidemic under the premise of efficiency and privacy, we combined IoT and blockchain technology to collect and analyze their real time data. First of all, IoT devices collect isolated people's physiological & geographic data. Due to the probable leak out of confidential data, the data will be transmitted to smart contracts in the blockchain for further analyze. Smart contracts will decide whether to issue an alert and write alerts as a new transaction in the blockchain. The self-execution would greatly improve respond to abnormality and ensure the data authenticity and privacy.

Methods

1.1.1 Body area network equipment remotely monitoring isolated people Body area network (BAN), also known as wireless body area network (WBAN) or body sensor network (BSN) or medical body area network (MBAN), is a network consist of wearable computing devices [6-9]. A WBAN system can use Wireless Personal Area Network (WPAN) wireless technology as a gateway to reach longer distances. Gateway devices make it possible to connect wearable devices on the human body to the Internet. This way, medical professionals can access patient data online using the internet independent of the patient location [10].

1.1.2 Geo-fence limits the range of quarantine activity Geo-fence is a virtual perimeter for a

real-world geographic area [4]. A geo-fence could be dynamically generated—as in a radius around a point location, or a geo-fence can be a predefined set of boundaries (such as school zones or neighborhood boundaries). One usage example involves users who use a location-based service (LBS) location-aware device to get in and out of a geo-fence. This event may alert users of the device and send a message to the geo-fence operator. This info, which could contain the location of the device, could be sent to a mobile telephone or an email account. [11,12].

1.1.3 Blockchain stores data Satoshi Nakamoto [5] originally proposed the blockchain technology in 2008. The blockchain adds blocks through a consensus mechanism, and uses hash values to connect each block to form a distributed ledger to record transactions, which is immutable and authentic. In 2013, Vitalik Buterin proposed Ethereum [13], which is also known as blockchain 2.0. The biggest feature of Ethereum is the use of smart contracts. A smart contract is a piece of code that can be executed. In Ethereum, smart contracts have their own addresses on the blockchain and will be automatically executed when conditions are met.

1.2 System design

1.2.1 Overall design The remotely monitored isolated people is equipped with wearable IoT devices, including WBAN and geo-fence devices. These devices collect metadata and send it to the master "smart device", usually a smartphone or tablet. Then, metadata is integrated and formatted by the decentralized application (Dapp). After that, the formatted information is sent to the relevant smart contract for comprehensive analysis along with the customized threshold. The smart contract will evaluate the provided data, and determine whether to issue an alert to the master device based on the evaluation results. If the master device receives the alert, it will display the alert to the isolated people and the CDCP. At the same time, the alert will be treated as a transaction and the nodes on the blockchain will verify and write it on the blockchain, and the detail information of the isolated people will be stored in the electronic health record (EHR) connected to the blockchain (Figure 1).

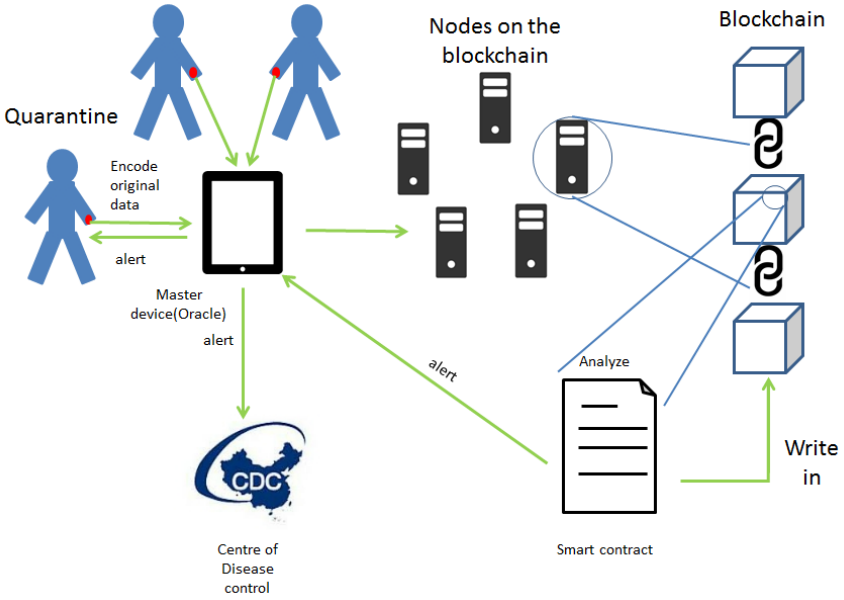

Figure 1 Smart monitoring system structure

1.2.2 Data collection, sorting and transmission The IoT devices collect data of the isolated people and the transmit it to the smart device for integration and formatting. The CDCP staff and

people being isolated can see real time data in real time on their smart devices. After processing the data, the smart device will send the previously set thresholds of different isolated people and to the smart contract for analysis. The providers of these data that communicate directly with smart contracts are called Oracle [13]. In this study, Oracle is the master device, and its transmission process is shown in Figure 2.

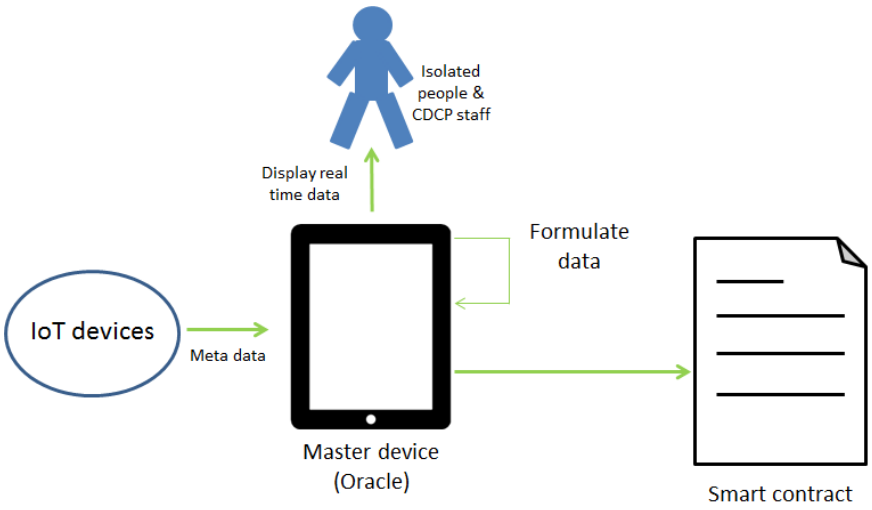

Figure 2 master device collecting & processing & transmitting data

1.2.3 Alert generation process

1.2.3.1 Deployment of smart contract The structure of the smart contract is modular and customized for each patient and their devices. First, all master devices call the same initial smart contract. Then, the initial smart contract will call the sub-contract relevant to the specific isolated person and device in turn. Each individual sub-contract will analyze the data according to the threshold, and then issue any necessary alarm. Contracts cannot be edited after deployment, it must be "terminated" and deploying new contracts, so this modular structure can easily replace the contract of one device without affecting the operation of other devices. The process of smart contracts analyzing data is shown in Figure 3.

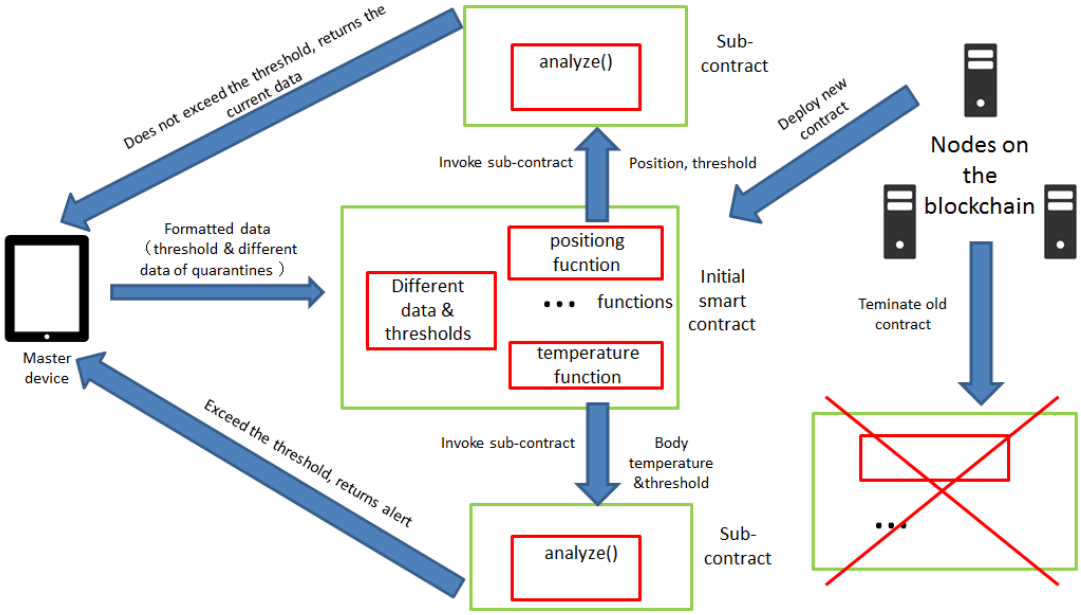

Figure 3 Smart contract analysis data flow chart

1.2.3.2 Analysis process of smart contracts After the smart contract receives the formatted data, it will compare it with the preset threshold to determine whether an alarm is needed. When the threshold is exceeded, the smart contract will send an alarm to the master device and form a new transaction. After receiving the alarm, the master device will notify the epidemic CDCP and the specific isolated person.

1.2.4 Validation of new block In this system, a consortium blockchain is used. Only authorized users can read the blockchain and designated users can call smart contracts and validate new blocks. Through identity verification, restricting system users to isolated people and CDCP staff, which can reduce the excessive exposure of private information. In addition, in the consortium blockchain, verifying a valid block must contain signatures from the smallest number of member (such as 20 of 30 members). In addition, since the members are determined in advance, this ensures that there is no external nodes can insert false events in the blockchain, ensuring the authenticity of the data. The consensus mechanism for verifying the blockchain utilizes a protocol such as Practical Byzantine Fault Tolerance (PBFT) to reach consensus [15].

1.2.5 Storage of private information In order to protect the private information of the isolated people, the system will not store confidential medical information in the blockchain or smart contracts. It only records what happened and uses the blockchain as a ledger. The specific measurement results will be forwarded to the designated EHR storage database, and a new event will be added to the blockchain. The system will integrate with the EHR Application Programming Interface (API) and send data directly to the EHR for storage. Similarly, all orders from smart contracts and CDCP will be recorded on the blockchain as complete transactions. Events on the blockchain are connected to the EHR to provide authentication of the data in the isolated people's medical records as a comprehensive care and regulatory record. This certification will help validate and prevent tampering of EHR.

2 Results

2.1 System Deployment As a proof of concept, we wrote an smart contract using Ethereum programming language Solidity. This system uses Remix to write smart contracts. Remix is a website with a compiler to test contract functionality. This system does not operate and deploy smart contracts on the Ethereum public chain, but runs on an independent private chain using the Ethereum protocol. Figure 4 shows the logical execution flow of the system.

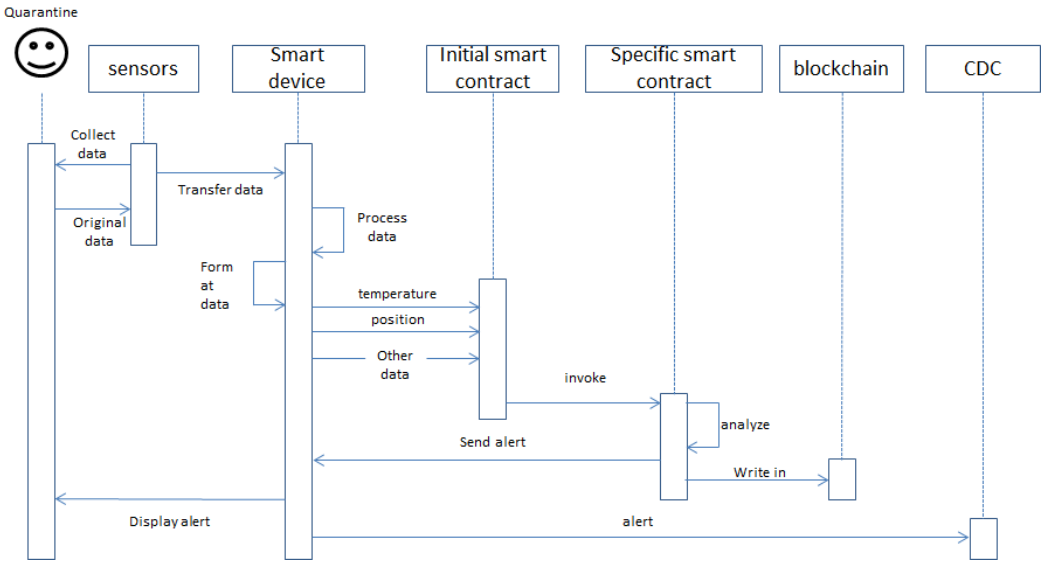

Figure 4 The logical execution flow of the system

2.2 Decentralize application control the transmission of data The User Interface(UI) on the smart device is managed by the Decentralized Application(DApp) on the smart device. The DApp is responsible for communicating with smart contracts on the blockchain and managing user configuration profiles. The configuration file adjusts its settings based on the user's current health status and geographic location. The CDCP personnel have administrator access to the isolated people's account, such as changing thresholds. The input information from the sensors is integrated and formatted in the back end of the DApp and forwarded to the smart contract connected using the web3.js object.

2.3 Calling smart contract In this system, the structure of smart contract is modular, there is a main smart contract *COVIDCaller*, which is called by the smart devices to process all kinds of data, and the *COVIDCaller* creates an appropriate contract for the specific device it's receiving the data from. For example, when the smart device receives the isolated people's body temperature data, the smart device calls the function *COVIDCaller.BodyTemperatrue()*, passing the data and minimum / maximum threshold values as parameters to an object of the COVIDCaller and the function *bodyTemperatureMonitor()*. At this point, the *bodyTemperatureMonitor()* function in the *COVIDCaller* will create a new *BodyTemperatureMonitor* object and pass the same parameters to the object's *analyze()* function. Instead of returning control to the main contract, these specific sub-contracts will analyze the incoming data and perform the necessary response operations themselves. The main contract is more like a "catalog", linking all devices to its related sub-contracts for modularity and easier maintenance. If the *analyze()* function returns any code other than "OK" (0), the subcontract will write this transaction in the blockchain. The same alert will be sent to the smart device to remind the user and CDCP staff can perform the operations (such as sending the person with a high temperature to the hospital, or returning the isolated person to the quarantine area). In order to briefly explain the above process, Figure 5 shows a contract demonstration. In order to be modular and easy to replace, different contracts should be divided into different files, deployed on the blockchain, and called each other through addresses.

```
pragma solidity ^0.4.24;

contract COVIDCaller{

    function bodyTemperatureMonitor(uint temperature, uint min, uint max)public constant returns (uint code){

        BodyTemperatureMonitor bt = new BodyTemperatureMonitor();

        return bt.analyze(temperature, min, max);
    }

}

contract BodyTemperatureMonitor {

    function analyze(uint temperature, uint min, uint max) public constant returns (uint){
        uint x=5;
        if(temperature < min||temperature > max){
            if(temperature < min-1||temperature > max+1){
                x=2;
                return (x);
            }
            x=1;
            return (x);
        }
        else{
            x=0;
            return (x);
        }
    }
}
```

Figure 5 contract demonstration

3 Discussion

3.1 Real-time monitoring using IoT devices Remote Patient Monitoring (RPM) research currently focuses on improving patient efficacy [16] and wireless network sensors [17, 18], as well as out-of-band authentication schemes using IoT devices [19]. A paper introduced an example of using smart contract to define geo-fence[20], another paper demonstrated how to monitoring prisoners by geo-fence[21]. In this system, the use of Internet of Things equipment, including WBAN and geo-fence, can greatly reduce the number of monitoring personnel, CDCP and the isolated people can see their own data in real time, and the system can issue alerts in time once the threshold is exceeded. For example, when abnormal physical characteristics appear in the isolated people, they can be transferred and treated in time to save their lives. In addition, the geo-fence technology will draw a quarantine area in advance. When the isolated people is detected to leave the quarantine area, the CDCP staff will get notified immediately, greatly reducing the time it takes to send the exposed people back to the quarantine area and prevent the further spread of the epidemic. In addition, the use of the system avoids the dispatch of a large number of on-site personnel to investigate the isolated people, reduces the consumption of manpower, and effectively avoids cross-infection.

3.2 Blockchain is very safe Several papers have provided rational applications of the blockchain in the healthcare field [22-25]. Larger companies, such as IBM and its project Hyperledger, which is a consortium blockchain and have marketed a capability to apply blockchain to healthcare and IoT [24]. In a 2018 paper, a proof of concept was proposed to combine the Internet of Things and blockchain in the medical field [26]. The consortium blockchain is used in this system. As a type of blockchain, it integrates many advantages, such as a distributed architecture, which makes the overall stability of the system have obvious advantages compared to traditional centralized databases. It will not cause the entire system to collapse due to the failure of the central node, causing a large amount of data and resource loss. In addition, another advantage of the blockchain is that it cannot be tampered with. All nodes in the system keep a complete record, and it is not realistic for anyone to tamper with the data. Compared with the public chain, the consortium chain has high privacy, and only authorized

users within the alliance can access the blockchain or verify new blocks. Each quarantine has its own anonymous account, which can only be viewed by themselves, while protecting privacy and increasing transparency to the quarantine. In addition, the consortium chain will pre-select trusted nodes to verify newly transactions and pack them into new blocks, so the process of generating new blocks will be more efficient and secure. Furthermore, smart contracts on the blockchain are automatically executed based on predefined conditions. This system uses these contracts to define custom thresholds based on different quarantines (automated analysis of health data and location information collected by IoT devices). When the threshold is exceeded, an alarm will be triggered, which is a great help for real time monitoring.

3.3 Good data integrity In addition to supporting smart contracts, the blockchain used by this system will also maintain a permanent log of the transmission sequence into and out of the device node in order to track the sequence of events. And, because the blockchain is connected to the EHR, you can find complete physical conditions and treatment records in chronological order.

3.4 Disadvantages There are some areas that need to be improved in the future. First of all, although the consortium chain has great verification speed compared to public chain, there is still some delay in the verification process. Second, the Internet of Things technology is very complicated, which brings about compatibility issues. In addition, the current wireless network technology is not very stable, which may cause a period of network disconnection.

Conclusion

In order to effectively monitor a large number of quarantines during the epidemic, this article proposes a smart monitoring system based on a blockchain architecture and using smart contracts to perform real-time analysis of metadata collected by medical sensors and geo-fences. This system uses a consortium blockchain to execute smart contracts, which will evaluate the information collected by the IoT device of the based on a customized threshold. The smart contract will determine whether to trigger an alarm based on the status of the quarantine, and record the alarm as a transaction on the blockchain to verify the authenticity of the EHR. After analysis, this system has the advantages of timely response, authentic and reliable information, and good privacy protection. It effectively implements real-time monitoring of quarantines under the premise of protecting data integrity and personal privacy. It provides strong support for the integration of IoT and blockchain technology and would be a great example for the development of smart monitoring system.

Abbreviations

IoT: internet of things; CDCP: center of disease control and prevention; BAN: body area network; WBAN: wireless body area network; BSN: body sensor network; MBAN:medical body area network; WPAN: wireless personal area network; LBS: location-based service; Dapp:decentralize application; EHR: electronic health record; PBFT: Practical Byzantine Fault Tolerance; API:Application Programming Interface

Ethics approval and consent to participate

Not applicable

Consent for publication

Not applicable

Availability of data and materials

Not applicable

Competing interests

The authors declare that they have no competing interests

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors

Authors' contributions

XCJ, XYH conceived and contributed to the design of the system. ZL, XCJ wrote this article. XCJ wrote the code. ZL, XCJ, CF, XYH did the review of the article. The authors read and approved the final manuscript.

Acknowledgement

Not applicable

Author's information

1. School of Control and Computer Engineering, North China Electric University
2. State Kay Laboratory of Infectious Diseases, the First Affiliated Hospital, Zhejiang University.

Reference

1. Novel Coronavirus(2019-nCoV) Situation Report – 38. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200227-sitrep-38-covid-19.pdf?sfvrsn=9f98940c_2
2. 浙江出台依法防控新冠肺炎疫情 12 条意见 切实保障人民群众生命健康安全和经济社会稳定发展, http://www.zj.gov.cn/art/2020/2/14/art_1228996602_41917990.html.
3. Mike Bolduc. The future of medical wearables. https://www.mpo-mag.com/issues/2017-06-01/view_columns/the-future-of-medical-wearables/, 2017.
4. Margaret Rouse. "What is geo-fencing (geofencing)?". https://whatis.techtarget.com/definition/geofencing, 26 Jan 2020.
5. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://git.dhimmel.com/bitcoin-whitepaper/, 2019.
6. Effatparvar, M., Dehghan, M. & Rahmani, A.M. A comprehensive survey of energy-aware routing protocols in wireless body area sensor networks. J Med Syst 40, 201 (2016). https://doi.org/10.1007/s10916-016-0556-8
7. Chen, M., Gonzalez, S., Vasilakos, A. et al. Body Area Networks: A Survey. Mobile Netw Appl 16, 171–193 (2011). https://doi.org/10.1007/s11036-010-0260-8
8. S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith and A. Jamalipour, "Wireless Body Area

Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1658-1686, Third Quarter 2014.
9. T. Geller et al., "Learning Health State Transition Probabilities via Wireless Body Area Networks," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6.
10. Yuce, M. (Ed.), Khan, J. (Ed.). (2012). Wireless Body Area Networks. New York: Jenny Stanford Publishing, https://doi.org/10.1201/b11522
11. Cynthia J, Priya C B. IoT based Prisoner Escape Alert and Prevention system[J]. International Journal of Pure and Applied Mathematics, 2018, 120(6): 11543-11554.
12. Victor F, Zickau S. Geofences on the Blockchain: Enabling Decentralized Location-based Services[C]//2018 IEEE International Conference on Data Mining Workshops (ICDMW). IEEE, 2018: 97-104.
13. Wood G. Ethereum: A secure decentralised generalised transaction ledger[J]. Ethereum project yellow paper, 2014, 151(2014): 1-32.
14. Consensys, A visit to the oracle. https://media.consensys.net/a-visit-to-the-oracle-de9097d38b2f, 2016.
15. Castro, M., and Liskov, B., Practical byzantine fault tolerance and proactive recovery. ACM Trans. Comput. Syst. (TOCS) 20(4):398–461, 2002.
16. Noah B, Keller M S, Mosadeghi S, et al. Impact of remote patient monitoring on clinical outcomes: an updated meta-analysis of randomized controlled trials[J]. NPJ digital medicine, 2018, 1(1): 1-12.
17. Hayajneh T, Mohd B J, Imran M, et al. Secure authentication for remote patient monitoring with wireless medical sensor networks[J]. Sensors, 2016, 16(4): 424.
18. Almashaqbeh, G., Hayajneh, T., Vasilakos, A. V., and Mohd, B. J., Qos-aware health monitoring system using cloud-based wbans. J. Med. Syst. 38(10):121, 2014
19. Wu L, Du X, Wang W, et al. An out-of-band authentication scheme for internet of things using blockchain technology[C]//2018 International Conference on Computing, Networking and Communications (ICNC). IEEE, 2018: 769-773.
20. Victor F, Zickau S. Geofences on the Blockchain: Enabling Decentralized Location-based Services[C]//2018 IEEE International Conference on Data Mining Workshops (ICDMW). IEEE, 2018: 97-104
21. Cynthia J, Priya C B. IoT based Prisoner Escape Alert and Prevention system[J]. International Journal of Pure and Applied Mathematics, 2018, 120(6): 11543-11554.
22. Dubovitskaya A, Xu Z, Ryu S, et al. Secure and trustable electronic medical records sharing using blockchain[C]//AMIA annual symposium proceedings. American Medical Informatics Association, 2017, 2017: 650.
23. Ekblaw A, Azaria A, Halamka J D, et al. A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data[C]//Proceedings of IEEE open & big data conference. 2016, 13: 13.
24. Unleashed, I. B., Blockchain is good for your health, and your business. https://www.ibm.com/blogs/blockchain/2017/12/blockchain-good-health-business/, 2017.
25. Yue X, Wang H, Jin D, et al. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control[J]. Journal of medical systems, 2016, 40(10): 218.
26. Griggs K N, Ossipova O, Kohlios C P, et al. Healthcare blockchain system using smart

contracts for secure automated remote patient monitoring[J]. Journal of medical systems, 2018, 42(7): 130.

Figures

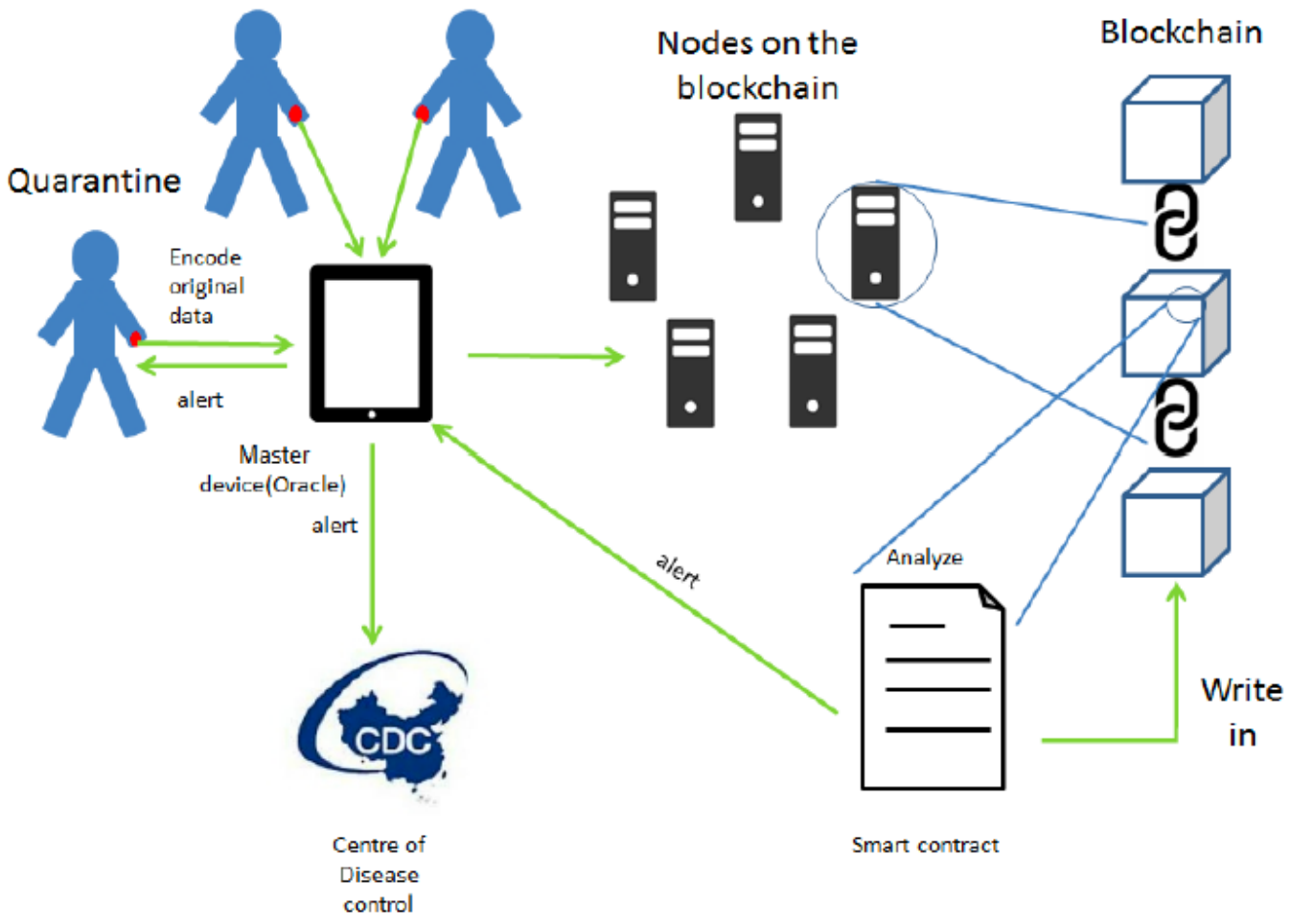

Figure 1

Smart monitoring system structure

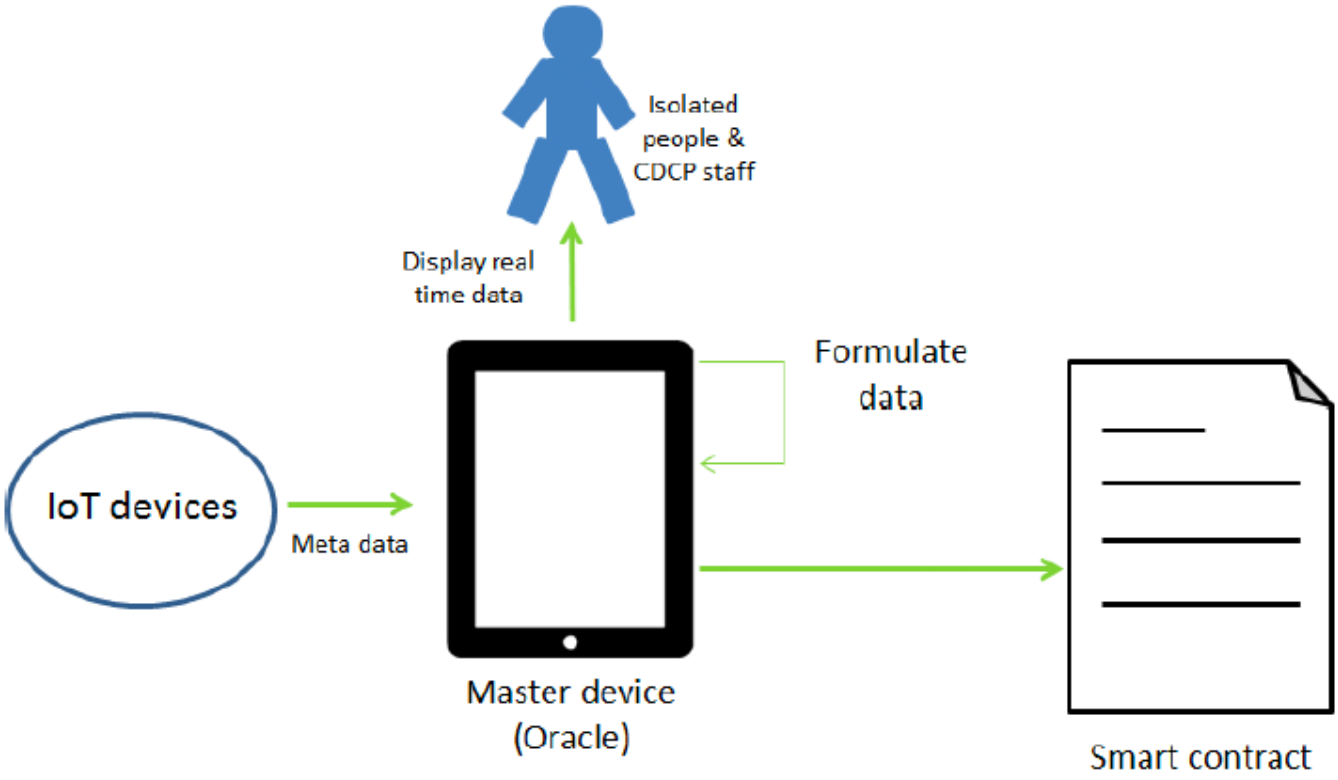

Figure 2

master device collecting & processing & transmitting data

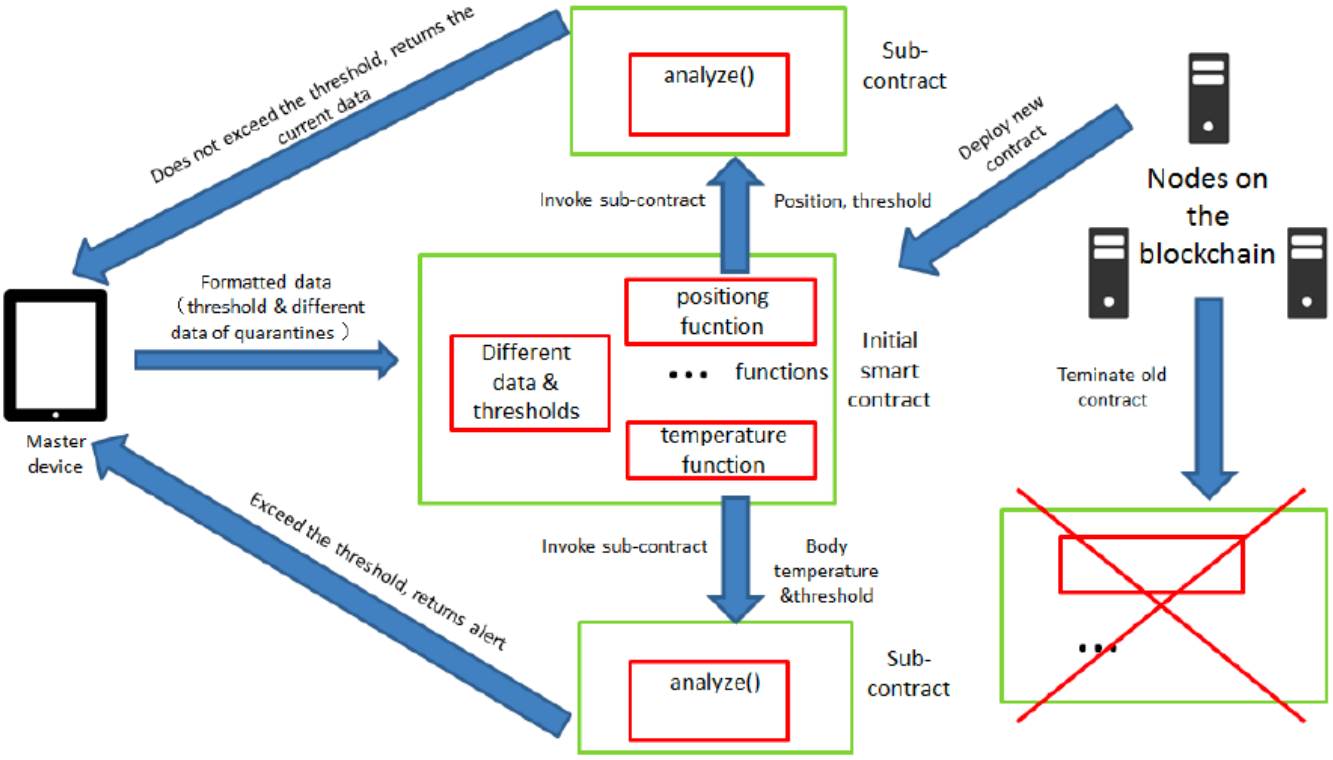

Figure 3

Smart contract analysis data flow chart

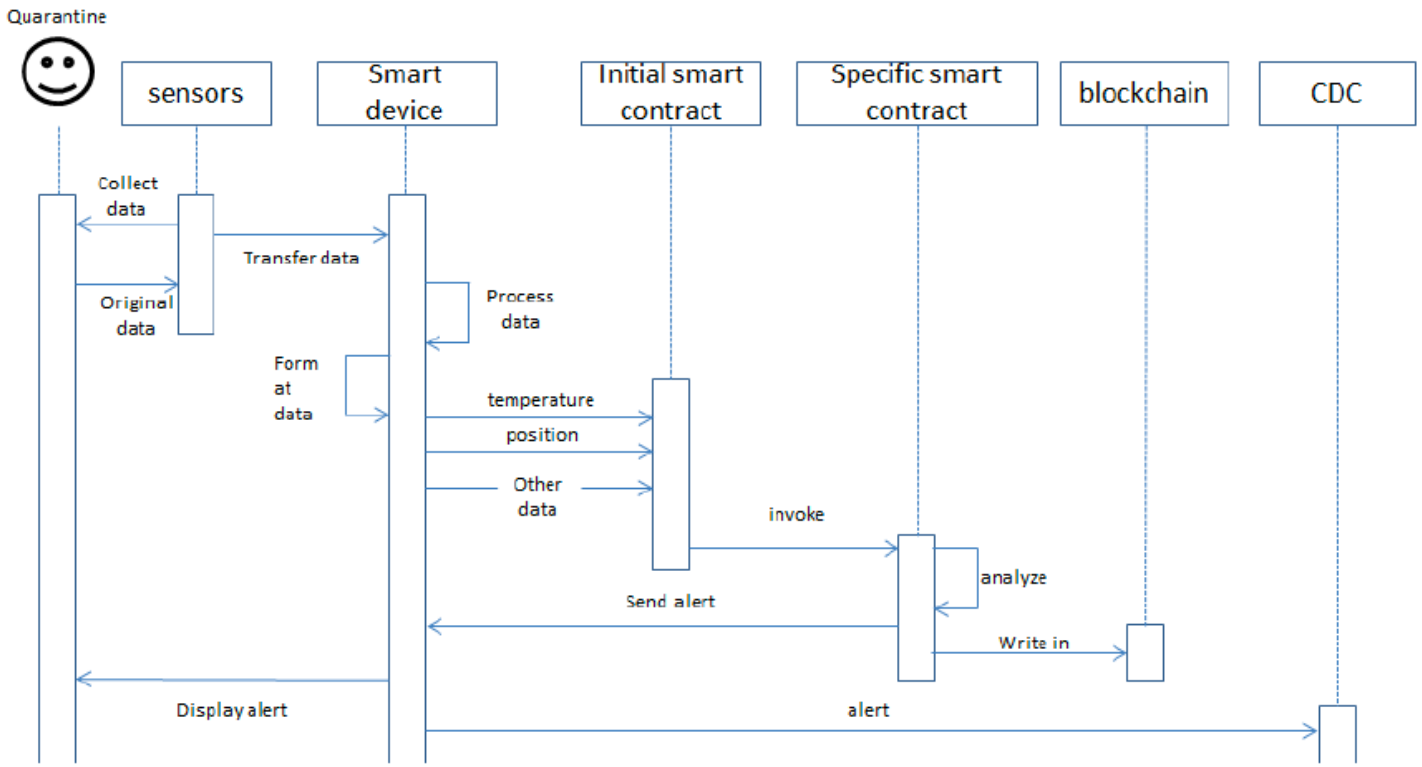

Figure 4

The logical execution flow of the system

```
pragma solidity ^0.4.24;

contract COVIDCaller{

    function bodyTemperatureMonitor(uint temperature, uint min, uint max)public constant returns (uint code){

        BodyTemperatureMonitor bt = new BodyTemperatureMonitor();

        return bt.analyze(temperature, min, max);
    }

}

contract BodyTemperatureMonitor {

    function analyze(uint temperature, uint min, uint max) public constant returns (uint){
        uint x=5;
        if(temperature < min||temperature > max){
            if(temperature < min-1||temperature > max+1){
                x=2;
                return (x);
            }
            x=1;
            return (x);
        }
        else{
            x=0;
            return (x);
        }
    }
}
```

Figure 5

contract demonstration