This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNB.2020.2999637, IEEE Transactions on NanoBioscience

An efficient double-layer blockchain method for vaccine production supervision

1st Shaoliang Peng ✉
College of Computer Science and Electronic Engineering
HuNan University
Changsha, China
slpeng@hnu.edu.cn

2nd Xing Hu
College of Computer Science and Electronic Engineering
HuNan University
Changsha, China
hu_xing@hnu.edu.cn

3rd Jinglin Zhang ✉
Key Laboratory of Meteorological Disaster, Ministry of Education
Nanjing University of Information Science and Technology
Nanjing, China
Jinglin.zhang@nuist.edu.cn

4th Xiaolan Xie ✉
College of Information Science and Engineering
Guilin University of Technology
Guilin, China
xie_xiao_lan@foxmail.com

5th Chengnian Long
Departmen of Automation
Shanghai Jiao Tong University
Shanghai, China
longcn@sjtu.edu.cn

6th Zhihui Tian
Smart City Research Institute
Zhengzhou University
Zhengzhou, China
iezhtian@zzu.edu.cn

7th Hongbo Jiang
College of Computer Science and Electronic Engineering
HuNan University
Changsha, China
hongbojiang@hnu.edu.cn

***Abstract*—A vaccine is a biological product which is an important means for human beings to protect themselves. Most of its users are young children with weak immunity. Once a vaccine has a problem, it will pose a serious threat to the lives of many people. At present, the supervision of vaccine production is very simple. The vaccine production record is completely controlled by the enterprises. Enterprises only submit production records to the supervisory agency for review when the vaccine needs to be sold. Production records are easily forged and modified.**

In order to solve the shortcomings of traditional centralized management. We propose a supervision method for vaccine production based on double-level blockchain.

At first, we have designed a double-level blockchain structure. The first level is private data of vaccine prduction enterprise, including production records and corresponding hash. The next level is public data, including production records hash and vaccine information. In this way, we make vaccine enterprise to submit production records in a timely manner without fear of privacy leaks. We avoid enterprise tampering or falsification of production records through the non-tampering features and time stamps of the blockchain.

To improve the time efficiency, we propose a consensus mechanism for multi-node cooperate. The primary supervisory node provides sorting services and verifies the correctness of the blockchain replica. The ordinary supervisory node can replace the primary supervisory node when necessary, and help the primary supervisory node recovers data in case of information loss. The review node is responsible for providing complete and correct blockchain copies for other nodes. So we can avoids the problem of waste of time resources in the traditional blockchain system.

In addition, in order to avoid the waste of space caused by the redundancy of the blockchain, we propose a vaccine data cutting mechanism. We use the timestamp of the blockchain and the vaccine validity period to determine if the block can be cutted. At the same time, it is also possible to judge whether the block can be cutted based on the information exchange with the vaccination institution.

Through these methods, we have realized spatiotemporal efficiency supervision of vaccine production. And for the time being, research work in the field of vaccine production supervision is still very rare. So Our work is ground-breaking.

***Index Terms*—vaccine, producton, supervision, blockchain**

(Corresponding author: Shaoliang Peng, Jinglin Zhang, Xiaolan Xie)

I. Introduction

Vaccine is considered one of the greatest public health achievements in the 20th century. It can prevent diseases and can be said to directly affect people's health. Once the vaccine has a problem, it can cause serious harm to the vaccinator's body. The problem vaccine will also make the vaccinator unable to resist many infectious diseases. These diseases can harm the health of patients and even cause death. In addition, there are many young children and infants among the users of the vaccine. They are weakly resistant and need safer vaccination.

However, in recent years, the vaccine industry, which should be strictly supervised, has experienced many accidents. The vaccination incident of Changchun Changsheng biotechnology company shocked the country. The Shandong problem vaccine case affected in 24 provinces or cities. Shanxi's invalid vaccine has caused nearly 100 children to die, maiming, or serious illness.

These incidents have caused enormous harm. Vaccine production requires deeper supervision.

A typical supervisory method of vaccine production is shown in Fig. 1. First, the FDA is responsible for determining the list of vaccine lot release agency. Second, the local FDA is responsible for assisting the local vaccine lot release agency to carry out the vaccine lot release work. When a vaccine

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNB.2020.2999637, IEEE Transactions on NanoBioscience

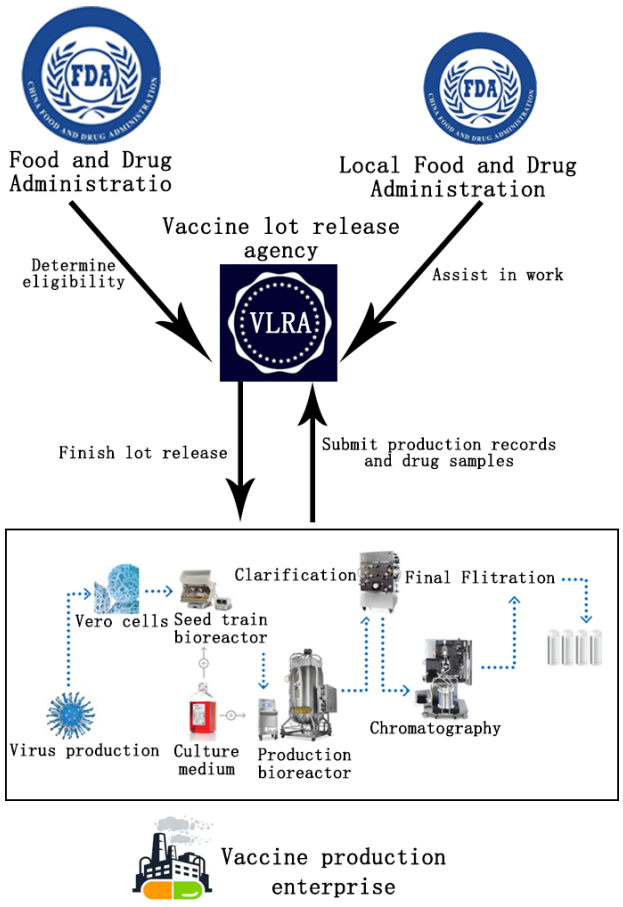

Fig. 1. Vaccine production, review, and marketing process(Part of the production process picture comes from Encyclopaedia of Occupational Health and Safety 4th edition[18]).

enterprise applies to the local vaccine lot release agency for vaccine lot release, the vaccine lot release agency verifies the production records and vaccine samples submitted by the vaccine enterprise. If the vaccine is qualified, the vaccine lot release agency will issue a lot release certification to the enterprise.

There are quite a few problems with this type of supervision. The vaccine production record is fully managed by the vaccine enterprise. Only when the vaccine needs to be sold, the vaccine enterprise submits the vaccine production records. In this management mode, the vaccine enterprise can make any modifications to their production records. Vaccine enterprises can also completely destroy their original production records and fabricate new production records. They can even create a batch of vaccines by way of blending and make a fake production records.

In order to address the problem of centralized method,we propose a new method to vaccine production supervision. It enables decentralized management and privacy protection of vaccine production records. Vaccine production records are stored on the blockchain. The vaccine production time can be determined by the timestamp on the blockchain. The main innovations are as follows:

1) Double-level blockchain struct: We divide the blockchain structure into double-level. The first level is the private data of the vaccine enterprise. This part of the data is stored in the vaccine enterprise's local database and no one else has access. It consists mainly of production records in the vaccine production process. In addition, each production record holds the corresponding hash and the hash of previous process record. The next level is public data. This part of the data is stored in a public blockchain. Any node participating in the blockchain can see it. It consists primarily of production records of hash and vaccine informaton(eg vaccine name, expiration date, etc.) and corresponding electronic signatures. In this way, vaccine enterprises can submit production records in a timely manner while ensuring that private data is not leaked. We avoid tampering with production records through the non-tampering feature of the blockchain. Due to the existence of timestamps on the blockchain and the limited production capacity of each enterprise, we can also prevent enterprises from falsifying production data (blockchain data will show that the enterprise's production capacity is not normal).

2) Consensus mechanism for multi-node cooperate: We propose a consensus mechanism for multi-node cooperate. The primary supervisory node provides sort services for other nodes and help them verify the correctness of the blockchain replica. The packaged block is sent to the primary supervisory node, and the primary supervisory node ordering broadcasts the block to the blockchain network. The other nodes only receive the blocks sent by the primary supervisory node and are in the correct order. Other nodes can also connect to the primary supervisor node and verify that the blockchain replica they saved is correct based on the blockchain data it holds. An ordinary supervisory node can replace the primary supervisory node when necessary. In this way, we have realized the consensus of the blockchain and avoided the waste of resources in the traditional blockchain system.

3) Cutting mechanism based on timestamp and information interaction: We propose a vaccine data cutting mechanism. The supervisor node sets a cut flag for each block. It determines whether the vaccine can be cutted based on the timestamp and the validity of the vaccine stored in the block. It periodically checks if the validity period of the vaccine represented by a block expires. If it expires, the cut flag will be set true. When the vaccination agency sends a signal to the supervisory node, it indicates that a certain batch of vaccine has been used. The cut marks for the blocks representing this batch of vaccines will also be set true. Eventually these blocks will be discarded.

The overall structure of this paper is as follows: the section II is the introduction of related work, the section III details our technical details and related design. The section IV describes our system implementation and evaluation of this method. Finally, the section V is conclusion.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNB.2020.2999637, IEEE Transactions on NanoBioscience

II. Related work

A. Blockchain Background

Blockchain is a new application mode of computer technology such as distributed data storage, point-to-point transmission, consensus mechanism, and encryption algorithm. It was first born in the Bitcoin white paper [1] released by Nakamoto in 2008, and is the underlying core technology of the well-known bitcoin system. The blockchain system can be thought of as a distributed system implemented with a group of replicated state machines [3] in a peer-to-peer network. New transactions can be replicated and finally delivered to the blockchain system by executing the corresponding group of replicated state machines, usually including executions of some consensus algorithm and external validity of transactions [2].

Transaction is the most basic unit of the blockchain. In the Bitcoin system, it consists of two parts, input and output. The input consists of an output from one of the previous blocks (ie some bitcoins) and signature from the owner of this output. The output consists of the currency value and an address (the address of the person who got the coins). A transaction usually represents the transfer of certain digital assets. Every time someone initiates a transaction, it will broadcast to the blockchain network. Some nodes within the blockchain network maintain a transaction pool. A transaction pool is a list of transaction information received by other nodes. These nodes will combine the transactions in the transaction pool into a block at the right time. Finaly one block will add in blockchain. A blockchain is a chain consisting of many blocks. Each block of the blockchain holds its own hash and a hash of the previous block. If a destroyer modifies the data of a certain block, this behavior will result in the hash change of this block. This behavior then causes the data of the next block to be changed (because the previous block hash saved in the block has changed). This change will eventually be reflected on the latest block. Therefore, unless the destroyer modifies all the data from one block to the latest block, this modification will be discovered. In addition, nodes on the blockchain hold a replica of the blockchain. Therefore, the destroyer needs to modify the data of most nodes on the entire blockchain network to successfully modify the data of some blocks. This type of storage and data structure is a source of non-tamperable feature of the blockchain [1].

With the rapid development of bitcoin and blockchain technology, more and more excellent researchers have joined the field. But the academic research of blockchain are still in a relatively slow development stage. At present, the work on blockchain research mainly focuses on the security, efficiency and scalability of consensus protocols, with emphasis on the application of cryptocurrency or general blockchain, and treated it in a more and more formal way learned established practices in areas of distributed systems and cryptography [4,5,6].

The most outstanding work in this area is Ethereum [7], which is the first attempt to introduce smart contracts into the blockchain system, thus greatly expanded the application of blockchain. Hyperledger Fabric [8] is also an outstanding representative in this field. It has changed the traditional blockchain model to a large extent, and built a blockchain system that is different from the original public chain and replaced it with an alliance chain. This framework is ideal for inter-enterprise applications and provides a blockchain solution for many businesses.

Blockchain is also expected to bring beneficial changes to the safety of vaccines or other drugs. We can prevent production data from being modified through a blockchain-based vaccine production monitoring system. We can also use the transparency of the blockchain to strengthen the audit of vaccine production.

B. Blockchain of vaccine supervisory

At present, there are few studies on vaccine safety using blockchain technology. Most of the research focuses on the safety of general drugs in circulation or discovery of the vaccine problem timely. There is little research on the safety issues that arise from the production of vaccines.

Mettler et al. [9] discussed the possibility of using blockchain technology to combat counterfeit drugs in the field of drug safety. Kurki et al. [11] discussed the benefits and guidance of using blockchain technology to supervisory drug circulation in the drug supply chain. Archa et al. [12] demonstrated their insights into the traceability of the drug distribution supply chain in conjunction with the GDP IoT framework and the Tendermint blockchain [13].

Hinrichsen et al. [14] proposed using electronic medical records to enhance detection and reporting of vaccine adverse events. Botsis et al. [15] proposed a text mining for the Vaccine adverse event reporting system to find the vaccine problem.

It is important to trace the circulation of the vaccine to ensure its safety and timely discovery of vaccine problems. However, consideration should also be given to possible problems with the vaccine during the production process. In particular, some recent fake vaccine incidents have had a major impact. These incidents are all due to the lack of effective supervision in the production of vaccine. Once the vaccine has problems in the production process, no matter how the supervision of vaccine circulation is in place, it can't prevent the fake vaccine from reaching the users.

To this end, we propose a solution based on blockchain technology for the process of vaccine production, and hope to better protect the safety of vaccine at the source.

III. Specific design

A. Double-level blockchain struct

The vaccine production undergoes a number of different steps and potency testing experiments during the producing process. Different vaccines have different production steps and testing experiments. We also consider testing as part of the production process steps. Then, we treat the production record of each production step as a separate piece of data. This piece of data holds the production record or experimental result

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNB.2020.2999637, IEEE Transactions on NanoBioscience

of the current step. In this way, no matter what the specific production process of a certain vaccine is, we can connect it to a series of production data. In this way, we can handle the various vaccines produced by different processes.

The storage of data is divided into two parts, the first part is private data, and the second part is public blockchain data.

Private data is stored in a local database of vaccine enterprises. Other nodes within the blockchain do not have access to it. The specific content of the private data is shown in Table I. Its main content is the production records, the time when the production record is generated and corresponding hash.

TABLE I
PRIVATE DATA STORAGE STRUCTURE.

Production record 1	**Record time 1**	**Hash**	**Start signal**
Production record 2	**Record time 2**	**Hash**	**Previous hash**
.....			

Public blockchain data is mainly divided into two parts. One is the block head data, and the other are a lot of transactions. The specific data structures are shown in Table II.

The header data of the block mainly includes the block number (that is, the block height, indicating how many blocks are currently included in the blockchain), the timestamp, the signature of the enterprise and the vaccine name (used to determine the vaccine production time and the enterprise production capacity), the hash value of the block and the hash value of the previous block (to prevent the block data from being tampered with), the validity period of the vaccine and lot release numbering (for cutting the block), and the signatures of the review and supervisory nodes.

One block represents a batch of vaccines, multiple transactions in each block. Each transaction in the block represents a process for each batch of vaccine in the production process. The hash of the transaction is the encryption of the production record of this production process. Each transaction also has its own timestamp and signature of the production enterprise, as well as the hash value of the previous transaction (previous production process) to prevent production data fraud.

Based on the traditional blockchain structure, we redesign the data structure for the vaccine production process. The current structure is a blockchain structure that is specifically adapted to the supervision of vaccine production. This structure stores the enterprise's privacy data and hash data separately, protecting the process privacy of the enterprise's production of vaccines. In addition, uploading the hash also ensures that the real data will not be tampered with. With this structure, enterprises can safely upload data to the review nodes instantly. This method guarantees the authenticity of the production records of the enterprise while guaranteeing the privacy of the production of the enterprise.

B. Consensus mechanism for multi-node cooperate

We maintain the consistency of the blockchain replica through the sorting service provided by the primary supervisory node. The primary supervisory node receives the blocks

TABLE II
BLOCKCHAIN DATA STORAGE STRUCTURE.

Block head	Block number	Timestamp
	Hash	Previous Block Hash
	Review node signature	Enterprise signature
	Vaccine name	Validity period
	Lot release numbering	Supervisory node signature
Transaction	Hash	Previous transaction Hash
	Enterprise signature	Timestamp

from each of review nodes. It arranges the blocks in the order in which they are received. It then broadcasts the blocks in turn to the blockchain network.Each node will receive the blocks sorted by the primary supervisor node. These nodes again judge whether the received blocks are in the correct order based on the hash value and the previous block hash value saved by the received block. In this way, it can be ensured that the replica of the blockchain held by each node is a sorted blockchain by the primary supervisory nodes. This method ensures the consistency of the blockchain replica saved by each node and avoids the occurrence of forks. At the same time, this method also avoids problems such as low time efficiency and waste of resources caused by traditional blockchain consensus mechanisms such as proof of work.

All nodes in the blockchain network can verify whether there is a problem with their own blockchain replica by accessing the primary supervisory node or review nodes. If a node does not receive a complete replica of the blockchain or saves an incorrect replica of the blockchain, it can connect to the primary supervisory node and then download the complete and correct replica of the blockchain.

When there is a problem with the primary supervisory node, the function can be replaced by an ordinary supervisory node. If the primary supervisory node is invalid, it can delegate one ordinary supervisory node to replace it. If the primary supervisory node has problems such as data loss, it can connect to all ordinary supervisory nodes, then selects a consistent blockchain replica saved by most of ordinary supervisory nodes to download and save.

The way to verify the correctness of the blockchain replica and the way to recover the data are shown as Fig. 2. The arrows of the primary supervisory node and ordinary supervisory nodes are mainly used to ensure the reliability of the blockchain. The arrows between ordinary enterprise nodes and review nodes, and the arrows between them and the primary supervisory node are mainly used to verify and download correct and complete data.

C. Cutting mechanism based on timestamp and information interaction

To cut unwanted blocks, first, The supervisor node will set a cut flag for each block.

As shown in Fig. 3, In both cases, the supervisor node sets the cutting flag of the block to require cutting. First, the time when the vaccine represented by the block reached the expiration date was detected. In this case, the node will

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNB.2020.2999637, IEEE Transactions on NanoBioscience

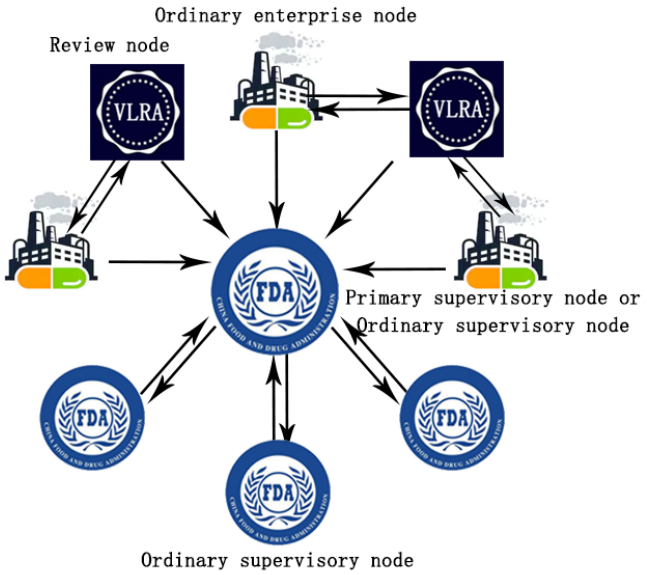

Fig. 2. Verify the correctness and restore.

compares the current time with the validity period of the vaccine stored in the block to determine whether the batch of vaccines has exceeded the validity period. Second, the vaccination agency sends information to a supervisory node through the application software. The supervisory node judges that the vaccine represented by a certain block has been used according to the received information, and then sets the cutting flag of the block should to be cutted.

Audit work is carried out regularly between the various supervisory nodes. At this point, the saved cut marks are integrated between the nodes. After the integration is completed, if the oldest part of the blockchain should be cutted, the primary supervisory node will broadcast to the entire network. The node that receives the broadcast cuts the blockchain replica that it has saved. For auditing purposes, we recommend that the primary supervisory node still maintain the most complete blockchain data.

In this way, we can ensure that the production source of the vaccine that needs to be used can be verified, while removing unnecessary redundant information. This cutting mechanism can effectively control the size of the blockchain and avoid excessive space requirements.

IV. Implementation and Evaluation

A. *Specific process of vGuard*

We first built a blockchain network. As shown in Fig. 4, according to the real vaccine supervision process, we divide the nodes participating in the blockchain into four categories: ordinary enterprise nodes, review nodes, ordinary supervisory nodes, and primary supervisory node. At the same time, our network will interact with consumers and vaccination agencies.

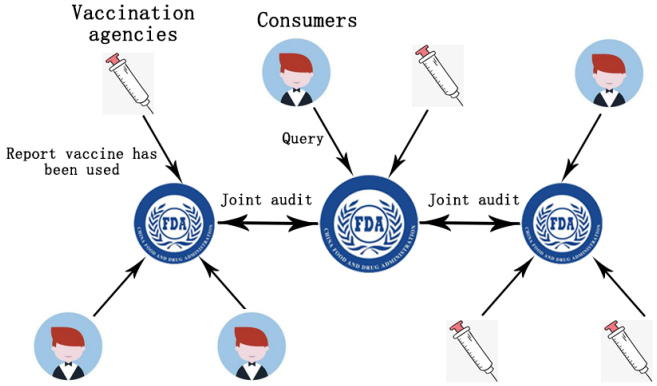

Fig. 3. Cutting mechanism for vaccine data.

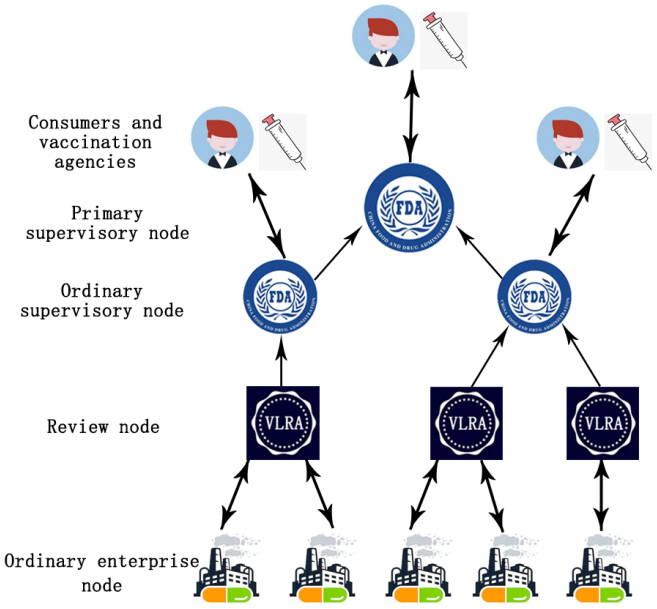

Fig. 4. Composition of vGuard.

The primary supervisory node issues certificates for each node in turn, so that these node can join the blockchain system.

All nodes are connected to the primary supervisor node. The ordinary enterprise node finds each review node by asking the primary supervisory node, and then selects some review nodes to establish a connection.

To further ensure that the production of each batch of vaccine is real, we add embedded equipment to the first equipment (such as bioreactors) that should be used in the production of vaccines. The device sends a hash to the review nodes and the enterprise node when the machine is booted.

Then, vaccine enterprises begin to produce a batch of vaccine. When a production process is completed, the staff needs to save the production record. Production records are saved to the vaccine enterprise's local database. they will also save the timestamp when each production record is generated. Next, the worker hashes the production record. The production record hash and time stamp, the hash of the previous process

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNB.2020.2999637, IEEE Transactions on NanoBioscience

record, etc. constitute a transaction, and broadcast to the review nodes. The previous process hash of the first transaction is the hash send by the embedded device.

To further protect the privacy of the vaccine enterprise's producing process, we allow vaccine enterprises to send some extra-transactions.

The purpose of these transactions is to keep the number of transactions in each block consistent. In this way, we hide the number of process steps a enterprise produces for a vaccine.

These transactions, just like normal transactions, have their own hash, timestamps, and hash of previous production record. The difference is that the hash of these transactions is not generated by a specific production record but by a random string chosen by the vaccine enterprise. The order in which these transactions are generated is random. They may be sandwiched between any two production process transactions.

In addition, the content of these transactions used for hashing will also be submitted to the review agency for review.

When a batch of vaccine production is completed, the vaccine enterprise sends a lot release application to the review node. The application contains the final transaction, ie a lot release transaction.

You can see the specific operation of this process in Algorithm 1.You can also see the visual representation of this process in Fig. 5.

Algorithm 1 Production

1: $equipment.get(hash)$
2: $hash \rightarrow$ Review node
3: $hash \rightarrow$ Current node
4: // Send start signal
5: $equipment.get(data)$
6: $equipment.get(time)$
7: // After finished production step 1
8: // Get production data and time
9: $data \rightarrow$ Local database
10: $time \rightarrow$ Local database
11: // Save the first data
12: $transaction.hash \leftarrow SHA256(data)$
13: $transaction.prehash \leftarrow hash$
14: $transaction.time \leftarrow time1$
15: $transaction.signature \leftarrow enterprise.signature()$
16: $transaction \rightarrow$ Review node
17: // Form a transaction
18: // And send to review node
19: $\vdots$
20: $creatapply(vaccine\ name, period, last\ transaction)$
21: $apply \rightarrow$ Review node
22: $local\ database \rightarrow$Review node
23: // Enterprise submit application

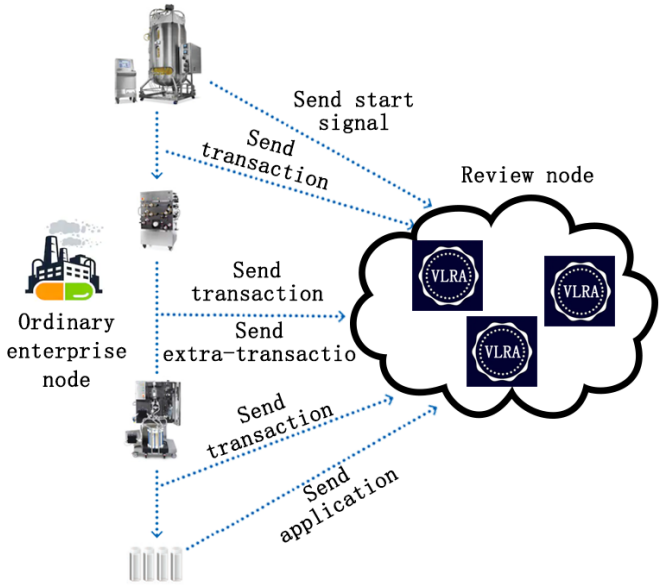

Fig. 5. Production process and consistent transaction quantity principle.

The vaccine enterprise issue a lot release application and submit production records and vaccine samples. The review node finds all relevant transactions from the transaction pool based on the hash of previous transaction saved in the transaction. Then it packages all transactions and related information(Such as vaccine name, expiration date, etc.) into one block.

The review node begins to check the production records and vaccine samples provided by the vaccine enterprise. They also need to check whether the hash of the submitted production records is consistent with the hash of the intra-block transaction.

If this batch of vaccine passes the review, the review node needs to write the corresponding lot release number to the block. In addition, the review node also needs to sign the block with its own private key.

The review node sends the block to the primary supervisor node. The primary supervisory node checks the block. If the check is successful, the primary supervisory node signs the block. Finally, it broadcasts block sequentially to the entire network.

We describe this process in Algorithm 2. You can see the visual representation of the process in Fig. 6.

When consumers need to verify the reliability of the vaccine, they can connect to the supervisory node responsible for the area by scanning the barcode on the vaccine bottle. The supervisory node sends back the query result through the saved blockchain replica(Return true if the batch of vaccine information is saved in the blockchain). If the search result is true, the vaccine is a validated vaccine, otherwise the vaccine may be problematic.

Using the transparency of the blockchain, we encourage ordinary enterprise nodes to check the data stored on the blockchain. They can query the timestamps on each block and the timestamps of transactions within the block, vaccine enterprises in various blocks and vaccines represented by each

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNB.2020.2999637, IEEE Transactions on NanoBioscience

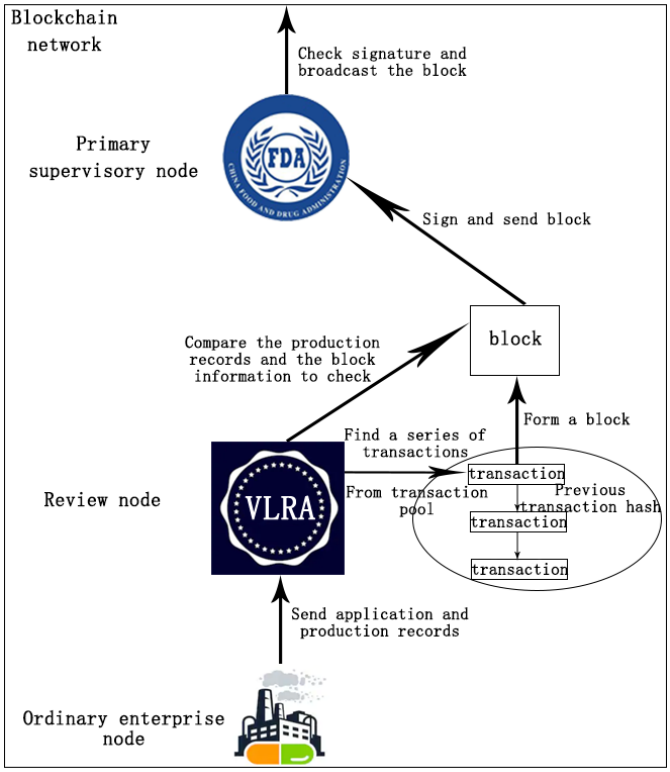

Fig. 6. Review process.

Algorithm 2 Review

1: $review\ node.get(transaction)$
2: // The review node finds all transactions from the transaction pool
3: // By previous transaction hash saved per transaction
4: $review\ node.get(data)$
5: // The review node get production data from enterprise
6: $review\ node.creatblock(transactions, blockhead)$
7: $if\ SHA256(data)! = transaction.hash$
8: $then$ Return false
9: // Review node audit block data
10: $review\ node.signature(block)$
11: $block \rightarrow$ Primary supervisory node
12: // Send block
13: $if(block.enterprise-signature.error()||block.review-signature.error())$
14: $then$ Return false
15: $primary\ node.signature(block)$
16: $block \rightarrow$ Blockchain network
17: // Check the block and sign it.Then broadcast the block to the Blockchain network
18: Return true

block. Based on these, they judge whether the production capacity of a certain vaccine enterprise is in an abnormal state. If there is a problem, they can report to the supervisory node. Once the report is verified, the supervisory agency will give the reported enterprise a certain reward. At the same time, the supervisory agency will also impose penalties on the illegal enterprises, including invalidating their certificates, and other realistic penalties.

B. System implementation

We implemented vGuard based on Fabric framework which provided by IBM. Our operating environment is Ubuntu 18.04. The Docker container was also used for the development of our system prototype. We use nodejs for backend development and writing business logic (such as writing smart contracts). As shown in Fig. 7, we provide different programs for different nodes. These include management pages for primary supervisory node, WeChat application for users and vaccination agencies, and management pages for review nodes. In addition, it also includes some management applications and related server programs. We also use these programs to systematically test the method we design. These tests are used to evaluate the performance of our completed systems and to demonstrate that our design method is fully applicable to current vaccine production.

C. Evaluation

1) Spatiotemporal efficiency: The number of general vaccine production processes is between 10 and 30 [20]. According to our test, the size of one transaction is about 1kb. The annual vaccine produced in China is around 4000-6000 batches. We took the maximum value(6000 batches) to test the size of the blockchain. The test results are shown in Fig. 8.

It can be seen that even in the largest case, the data generated by the entire blockchain in a year will not exceed 200MB. Since the shelf life of the vaccine is generally one to three years, the data stored in the blockchain will not exceed the data volume of three years, which is about 600MB. For modern computers, this is an acceptable size.

In addition, we also tested the throughput and latency of the system through scripts. The results are shown in Fig.9 and Fig.10.

In China, there are currently about 33 large vaccine enterprises. Even if these enterprises send transactions and submit lot release application within one second, our system has enough throughput to handle, and this situation is almost impossible in reality.

In the actual production process, generally every transaction is sent a few days apart. Checking production records and vaccine samples is also a lengthy process that can last for months. The latency of the system is negligible.

2) Privacy: In our design, we divide the saved data into two parts. The first part is private data, and the second part is blockchain data.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNB.2020.2999637, IEEE Transactions on NanoBioscience

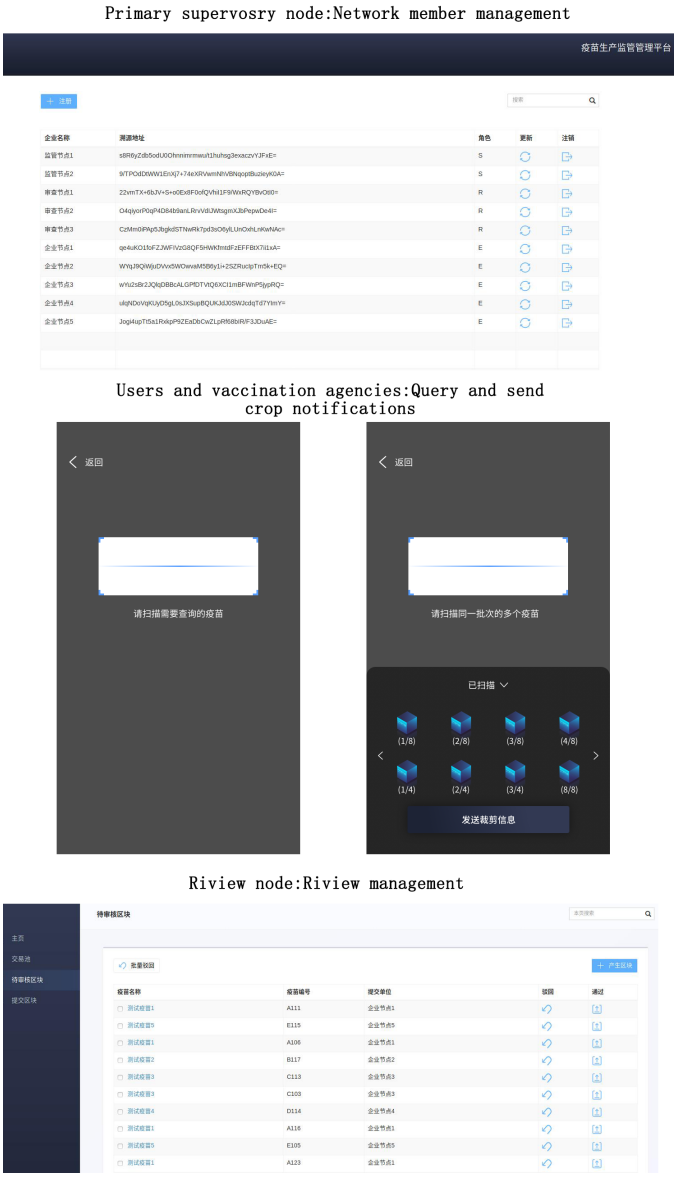

Fig. 7. A system we have developed specifically for the vGuard.

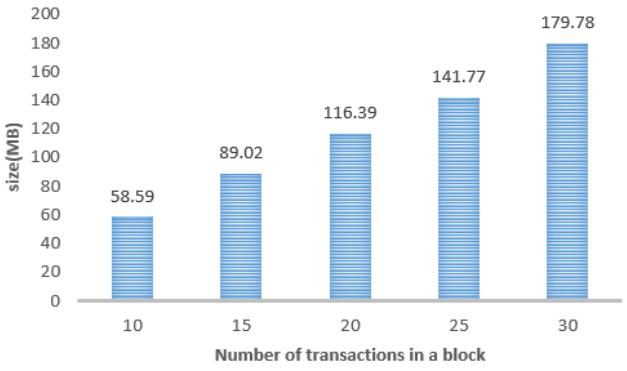

Fig. 8. Impact of transaction number on blockchain size.

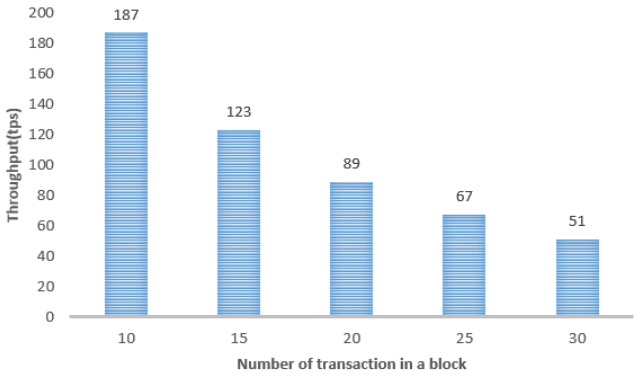

Fig. 9. Impact of transaction number on throughput.

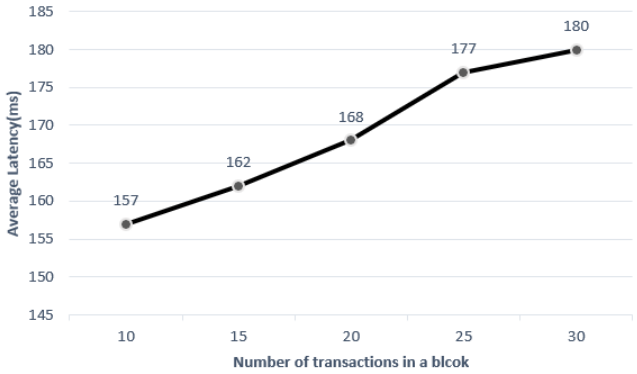

Fig. 10. Impact of transaction number on latency.

Private data is stored in the vaccine enterprise's local database and no other nodes have access. This part of the data is protected by the enterprise itself for its privacy content.

The blockchain data is shown in the table III:

TABLE III
INFORMATION PUBLISHED ON THE BLOCKCHAIN.

Vaccine name	**public**
Production enterprise	**public**
Lot release number	**public**
Vaccine production time	**public**
Vaccine validity period	**public**
Review agency	
Production record(hash)	**encryption**
Number of production steps	**consistent**

The information exposed on the blockchain is listed in the table. Among them, the production record is protected by hash encryption, and the number of production processes is protected by the principle of consistent transaction quantity. The name of the vaccine, the enterprise, the lot release number, the date of production, and the vaccine validity period are all public data. We can make inquiries on the web[19].

We believe that displaying the review agency can enhance the user's confidence and further avoid the collusion between

the review agency and the business. It is necessary for vaccine production supervision.

Therefore, our design can be said to have achieved the privacy requirements of vaccine production without revealing more information.

V. Conclusion

In this paper, we propose a new vaccine production supervision method. We use blockchain technology and improve the traditional vaccine production supervision process to further improve the safety of vaccine production. It combines embedded technology with timely data transmission to ensure the safety and reliability of production data. It implements the blockchain consistency through the sorting service provided by the main supervisory node. It protects the privacy of vaccine production by hash and consistent number of transactions. Finally, we propose a cropping mechanism to avoid data redundancy and ultimately achieve stable and acceptable storage.

Of course, in practical applications, our method still has certain problems. This method of production supervision requires the cooperation of multiple parties, and requires the leadership of the FDA and the cooperation of vaccine manufacturers. This method of production supervision also increases the complexity of vaccine production supervision and may reduce the interests of relevant agencies.

Therefore, how to further simplify the application of this method and put it into practical use is a difficult problem to solve. This is also the direction we will try next.

In addition, we still hope to continue research in this direction. We hope to further supervisory the circulation of vaccines. Ultimately, we are able to achieve effective regulation from the production of the vaccine to the circulation of the user to the final process of the user. Through the blockchain method, we can save every process of vaccine from production to circulation on the blockchain to ensure the safety of each bottle of vaccine.

Acknowledgments

This work was supported by National Key R and D Program of China 2017YFB0202602, 2018YFC0910405, 2017YFC1311003, 2016YFC1302500, 2016YFB0200400, 2017YFB0202104; NSFC Grants U19A2067, 61772543, U1435222, 61625202, 61272056, 61762031; The Funds of Peng Cheng Lab, State Key Laboratory of Chemo/Biosensing and Chemometrics; the Fundamental Research Funds for the Central Universities Grant No. 2016B090918122.

References

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”, http://bitcoin.org/bitcoin.pdf, 2008.
[2] C. Cachin and M. Vukoli´ c, “Blockchains consensus protocols in the wild”,arXiv preprint, Jul. 2017, arXiv:1707.01873.
[3] F. B. Schneider, “Implementing fault-tolerant services using the state machine approach: A tutorial”, ACM Computing Surveys (CSUR), vol. 22, no. 4, pp. 299-319, Dec. 1990.
[4] J. A. Garay, A. Kiayias, and N. Leonardos, “The bitcoin backbone protocol: analysis and applications”, in Springer Annual International Conference on the Theory and Applications of Cryptographic Techniques, Apr. 2015, pp. 281-310.
[5] J. A. Garay, A. Kiayias, and N. Leonardos, “The bitcoin backbone protocol: analysis and applications”, in Springer Annual International Conference on the Theory and Applications of Cryptographic Techniques, Apr. 2015, pp. 281-310.
[6] R. Pass, L. Seeman, and A. Shelat, “Analysis of the blockchain protocol in asynchronous networks”, in Springer Annual International Conference on the Theory and Applications of Cryptographic Techniques, Apr. 2017, pp. 643-673.
[7] Ethereum. Available: https://www.ethereum.org
[8] E Androulaki, A Barger, V Bortnikov, et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains[J]. 2018.
[9] M. Mettler, “Blockchain technology in healthcare: The revolution starts here”, in IEEE 18th International Conference one-Health Networking, Applications and Services (Healthcom), Sep. 2016, pp. 1-3.
[10] Min Gyu Kim, Ah Ra Lee, Hwi Jun Kwon, et al. Sharing Medical Questionnaries based on Blockchain[C]// 2018 IEEE International Conference on Bioinformatics and Biomedicine (BIBM). IEEE, 2018.
[11] J. Kurki, “Benefits and guidelines for utilizing blockchain technology in pharmaceutical supply chains: case Bayer Pharmaceuticals”, Bachelor thesis, Aalto University, 2016.
[12] Archa, B. Alangot, and K. Achuthan, “Trace and track: enhanced pharma supply chain infrastructure to prevent fraud”, in Springer International Conference on Ubiquitous Communications and Network Computing, Aug. 2017, pp. 189-195.
[13] Tendermint. Available: https://tendermint.com
[14] Hinrichsen V L , Kruskal B , O’Brien M A , et al. Using Electronic Medical Records to Enhance Detection and Reporting of Vaccine Adverse Events[J]. Journal of the American Medical Informatics Association, 2007, 14(6):731-735.
[15] Botsis T , Nguyen M D , Woo E J , et al. Text mining for the Vaccine Adverse Event Reporting System: medical text classification using informative feature selection[J]. Journal of the American Medical Informatics Association, 2011, 18(5):631-638.
[16] Jen-Hung T , Yen-Chih L , Bin C , et al. Governance on the Drug Supply Chain via Gcoin Blockchain[J]. International Journal of Environmental Research and Public Health, 2018, 15(6):1055-.
[17] Angraal S , Krumholz H M , Schulz W L . Blockchain Technology: Applications in Health Care[J]. Circ Cardiovasc Qual Outcomes, 2017, 10(9):e003800.
[18] James S . Encyclopaedia of Occupational Health and Safety 4th edition[J]. Reference Reviews, 1999, 13(2):31-32.
[19] China Food and Drug Administration. Available: http://samr.cfda.gov.cn
[20] Chinese Pharmacopoeia Commission. Chinese Pharmacopoeia[M]. Bei-Jing: China Medical Science Press, 2015.