Decentralization of the Internet of Things in Industry 4.0

Dmitrii Korenev[1,*], Alexander Zakharov[2]
Tyumen State University, Tyumen, Russia [1]
Tyumen State University, Tyumen, Russia[2]
stud0000109291@study.utmn.ru

Abstract: *Rapid progress in the field of industrialization and informatization methods has led to huge progress in the development of next-generation production technologies. The Internet of Things (IoT) is a pervasive technology, and now it is used in all areas of everyday life, from healthcare to technological production. The new industrial revolution began with connected technologies supported by the Internet of Things. However, the security of the Internet of Things is still an open question since in case of unauthorized access, data from sensors can be changed, for example, by a user with authorized access rights, which can lead to unforeseen consequences.*

Keywords*: IOT, BLOCKCHAIN, DECENTRALIZATION, INFORMATION SECURITY*

1. Introduction

At the moment, centralized servers are used to collect data from IoT devices, which are an additional attack vector and should also be protected, because if the server is unavailable, data from the devices will not enter the database or in case of unfair hosting on which the servers are deployed. Some of the protection methods may be quite effective, but they do not give much guarantee. At the moment, there is a trend towards decentralization, which is gradually coming to replace the client-server architecture, which is much more widespread at the moment. Unlike the client-server architecture, the decentralized blockchain architecture has several security advantages [1-2]:

- trust is based on a mathematical model and is supported by cryptographic methods
- natural immunity to single point of failure (SPOF)
- immunity to replay attack

However, there are several problems related to the performance and scalability of classical blockchain models, such as Bitcoin, Ethereum etc. The alternatives proposed by other researchers [3] do not consider such features of the field of medicine as:

- connection with other data, since it is necessary to know to which patient data relate to
- more efficient data storage mechanisms

2. Preconditions and means for resolving the problem

The main goal of this work is to create a more efficient blockchain model that can close the above problems. To consider any options, it is necessary to find out how the blockchain works. When each transaction occurs, it is recorded as a “block” of data, these transactions show the movement of an asset, which can be tangible (product) or intangible (intellectual). The data block can record information of your choice: who, what, when, where how much and even the condition — for example, the temperature of food delivery. Each block is connected to the blocks before and after it, these blocks form a chain of data as the asset moves from place to place or changes hands. The blocks confirm the exact time and sequence of transactions, and the blocks are securely linked to each other to prevent any block from being modified or a block inserted between two existing blocks. Each additional block reinforces the verification of the previous block and, consequently, the entire blockchain. This makes blockchain forgery obvious, providing the key strength of immutability. This eliminates the possibility of an attacker interfering and creates a transaction registry that you and other network participants can trust. An example of a blockchain scheme is illustrated in Fig. 1 [4].

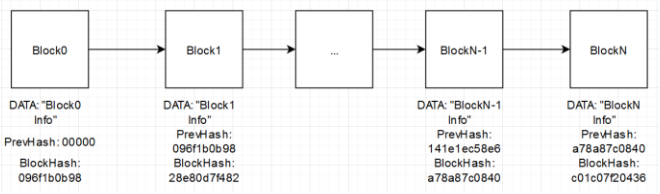

Fig. 1 *Example of blockchain principles*.

In the basic architecture of the blockchain, each transaction needs to be verified which cannot be altered. The blockchain is a Peer-to-Peer network of connected devices, when a transaction is added, it is transmitted to all nodes available in the network. After all nodes received transaction a validation of transaction is started, usually blockchain network uses SHA-256 algorithm for hash generation. After successful validation the block is going to the ledger chain and added existing blockchain, this process illustrated at Fig 2 a-c.

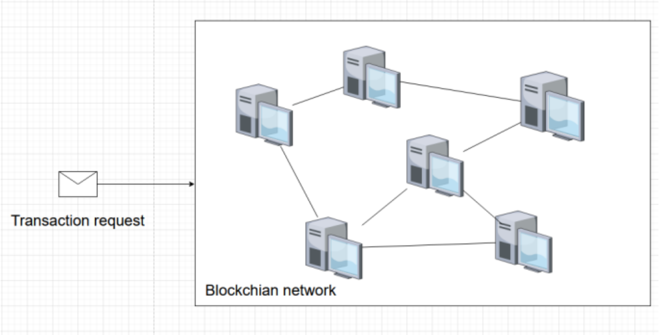

Fig. 2a *Transaction request in blockchain network*

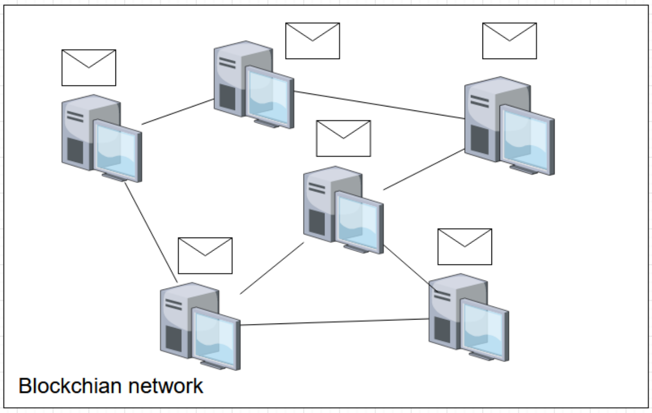

Fig. 2b *Transmission of transaction in blockchain network*

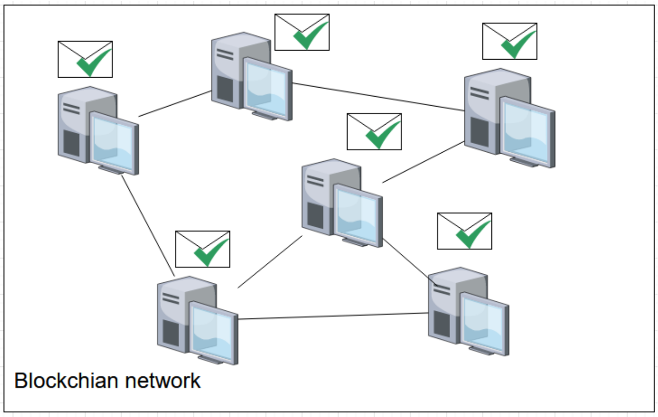

***Fig. 2c** Validation of transaction*

There also several types of blockchain:

- public
- private
- permissioned

In public blockchain anyone can join and contribute to the network. Anyone can read, write, and audit the ongoing activities on the public blockchain network, which helps a public blockchain maintain its self-governed nature. But there is also a downside of that approach because this type of blockchain becomes more and more power consuming the more participants join it.

Private blockchain allows only verified participants by authentication or verified invitation. It also allows execute the consensus protocol that decides the mining rights and rewards and maintenance of the shared ledger.

Permissioned blockchain is a combination of public and private blockchain with customization options.

3. Solution of the examined problem

An important factor is the data for which interaction is planned, at the moment data are considered as: blood pressure. cholesterol level, glucose level. AST, ALT. The data in the blockchain will be generated based on the device identifier and the data read by the sensor.

In the case of applying a conventional model to IoT devices, several problems arise:

- IoT devices don't have as much storage space for the entire blockchain
- the computing power of the devices does not allow for more complex computing processes

In this regard, it is proposed to transfer the entire formation of the blockchain to decentralized servers according to the model described below in Fig 3. This will solve the problem that it is necessary to perform calculations, as well as store data on an IoT device.

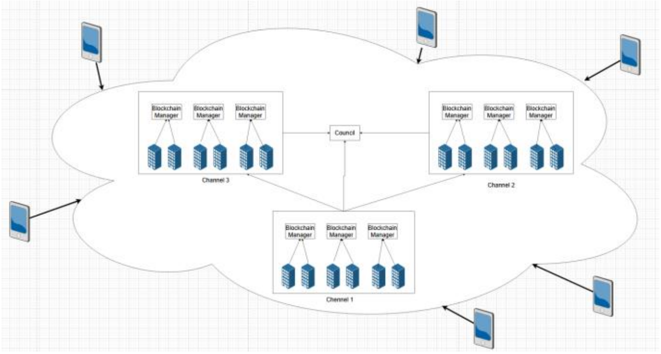

***Fig. 3** Proposed blockchain model*

The network permissioned and almost private, that is, for each new device, its registration in the network is required. IoT devices will be in the “external” layer from which requests will be submitted to the cloud, the server is selected depending on its availability, thus decentralization can still be ensured and protection from SPOF is provided. the only drawback of this approach is the fact that you may have to do additional configurations that may not be supported by some devices. The channels are the points where IoT devices will transfer data, also they are representing connections between hospitals which can be located on a different cloud.

Blockchain managers are used to generate and compress data to blockchain, they also act as sources for smart contracts, since it stores a replicated copy of the blockchain network.

The validation of the network blocks is handled by the “council”, it contains N devices performing validation, thereby providing SPOF protection in case one of the nodes is unavailable for validation by the “council”. The “Council” has mutual access with “blockchain managers” this is shown in Fig 4.

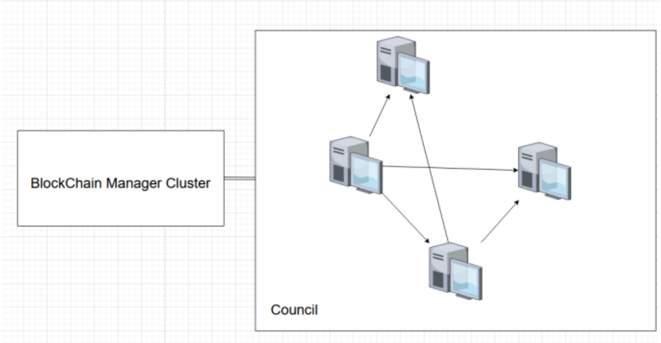

***Fig. 4** Council scheme.*

Based on the diagram in Fig 3 and Fig 4, the following interaction is planned:

- The IoT device sends a request to add to one of the channels
- One of the blockchain managers forms a request and sends it for validation to the "council"
- After validation, the blockchain is updated for everyone
- If another medical professional needs to apply for some data from sensors, for example for research, he can do it using smart contracts

4. Results and discussion

The result of this work was an alternative model for decentralized and more secure storage of medical data. The model covers the entire cycle of data circulation, from sending from IoT devices and ending with the secure receipt of data by a third party using smart contracts.

However, there are points that require additional consideration. For example, how many blockchain managers and members of the "council" are needed for the best performance and how to calculate amount of them? What configuration should these devices have?

5. Conclusion

This work suggests an alternative blockchain model that has the potential to be more efficient than other models. The proposed model was reviewed, its main modules were described. The source code and data can be viewed here: https://github.com/DemonEach/med-blockchain-iot.

The study was supported by a grant from the Russian Foundation for Basic Research and the Tyumen Region within the framework of the scientific project No. 20-47-720005 and the RFBR grant 22/2020.

6. References

1. A, Liu, S, Khatun, H. Liu, M. Miraz, IEEE, *Lightweight Blockchain of Things (BCoT) Architecture for Enhanced Security: A Literature Review* (2020)
2. A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, FGCS, *On blockchain and its integration with IoT. Challenges and opportunities,* **88**, 173-190 (2018)
3. L. Ismail, H. Materwala, S.Zeadally, IEEE, *Lightweight Blockchain for Healthcare* (2019)
4. U. Bodkhe, S.Tanwar, K.Parekh, P.Khanpara, S.Tyagi, N.Kumar, M.Alazab, IEEE, *Blockchain for Industry 4.0: A Comprehensive Review* (2020)