

Architecture of a Smart Container Using Blockchain Technology

Oleg Iakushkin(✉), Dmitry Selivanov, Ekaterina Pavlova, and Vladimir Korkhov

Saint-Petersburg State University, St. Petersburg, Russia
o.yakishkin@spbu.ru

Abstract. The use of blockchain technology introduces the possibility to decentralize logistic systems. These are more efficient and the information inside is easy accessible and verifiable. Additionally, data security is preserved at this time. This paper presents the architecture of a smart container that uses blockchain technology. It stores its location and status data in a distributed ledger. In addition, users and suppliers can use the mobile application to access this data. As the information about the container movements is available in realtime, the relevant parties will be able to take action quickly when a problem occurs in the supply chain. Sensitive and private documents will require a permissioned blockchain infrastructure such as Hyperledger Iroha. Blockchain technologies allow users to abandon the idea of a central server or a regulatory authority that support the operation of the system and be responsible for safety and storage of data. Such a decentralized network does not have a central point of failure and is better able to withstand malicious attacks.

Keywords: Smart container · Distributed ledger · Blockchain · Iroha · Raspberry Pi

1 Introduction

For the management of logistic chain organizing the delivery of goods by unrelated intermediaries it is necessary to form an ecosystem of trust. To realize the possibility of secure information exchange during shipments based on blockchain [1] technology, there are several main components:

- a “smart container” hardware-software - a system being implemented in the field to monitor the current situation
- a software logistic system that allows carriers to exchange orders and optimize costs
- an API for building end-user applications

This article describes a smart container that can be transferred between owners and that will be able to use blockchain technology to store data about its location, membership status, and other information. Such a container makes

© Springer Nature Switzerland AG 2019
S. Misra et al. (Eds.): ICCSA 2019, LNCS 11620, pp. 537–545, 2019.
https://doi.org/10.1007/978-3-030-24296-1_42

logistic processes more convenient and transparent not only for the end user, but also for suppliers.

Blockchain technologies allow users to abandon the idea of a central server or a regulatory authority that support the operation of the system and be responsible for safety and storage of data. Such a decentralized network does not have a central point of failure and is better able to withstand malicious attacks. In addition, changes in public blocks of the chain are publicly accessible to all parties, which creates transparency of information. It is important to ensure that all information on movements and the final destination point is visible only to the supplier, which is the last destination in the sequence of movements of the container. This distinction is designed to preserve anonymity and prevents the intentional disruption of deliveries. To accomplish this, distribution of access rights in the blockchain framework is used, which will be described in more detail below.

This paper presents two software platforms. The first is for suppliers, providing access to the location and status of all containers that currently belong to them. At the same time it is possible to view information about the previous owner and the next destination. The second platform is for users, providing access to the status and movement history of the container enclosing their order. These platforms are implemented in the form of two mobile clients.

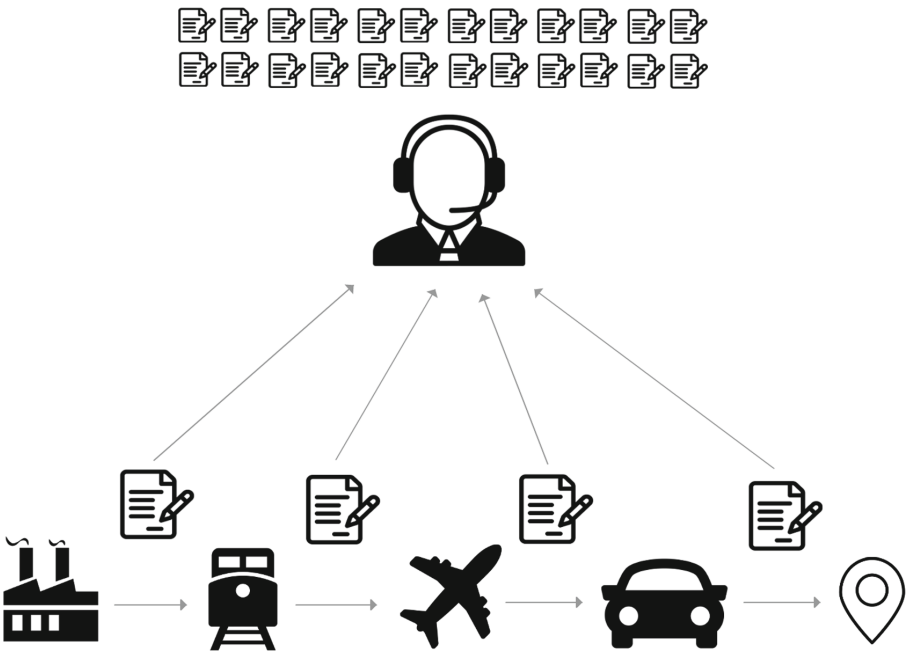


Fig. 1. Centralized logistic system.

Figure 1 is a schematic representation of a centralized logistic process. In this process, some goods were manufactured at the factory, and then sent to the destination using three consecutive movements: by train, by plane and by car. At the same time, a document was generated for each movement. Verification and creating of documents, as well as the administration of movements is performed using some central node. However, to organize the effective work of each of the units, time and money is required.

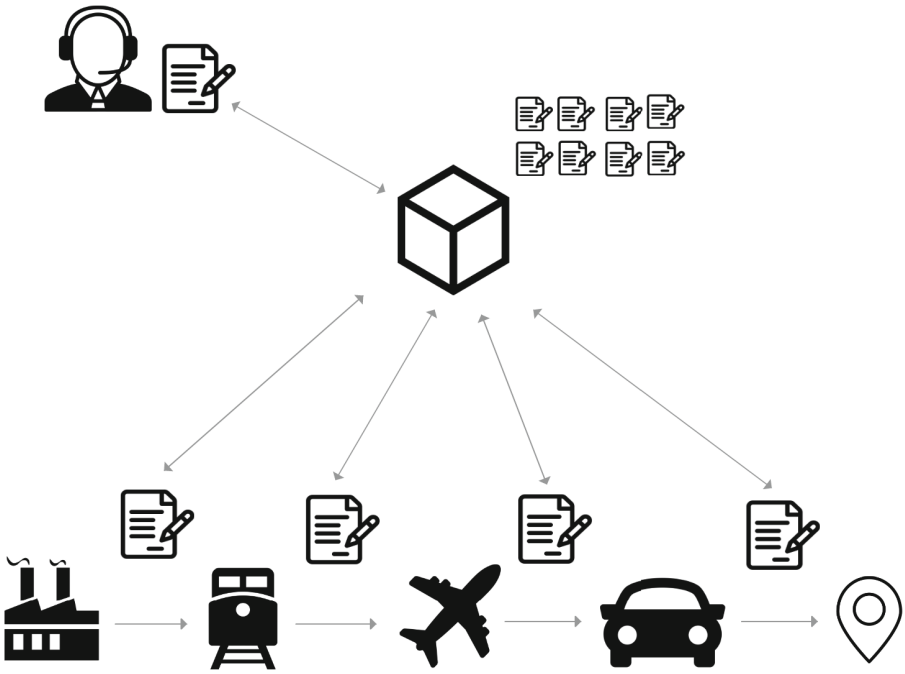


Fig. 2. Decentralized logistic system.

Figure 2 shows a schematic representation of a decentralized logistic process using blockchain technology. In such a system, the organization of the delivery of goods occurs in presence of unrelated intermediaries in a certain ecosystem of trust. The ability to safely exchange information during the course is carried out using the blockchain technology. The number of paper documents or emails will be significantly lower in these ecosystems than in the case of a centralized one. Documents about movements will be stored electronically in a distributed ledger.

2 Current Situation

The existing solution in the market of logistic systems is the "Smart Containers" company [5] and their products SkyCell or FoodGuardian. They provide smart containers for delivering medicine and food.

Until today, their containers are tracked using data that goes to a centralized database. In addition, the administration is done manually. This means that one of the operators checks the location of the containers by contacting the client in specific cases. This creates financial and time costs.

3 Hardware

The compact single board computer Raspberry Pi 3b is used as the main module of the smart container. A GPS module with an external antenna is used to determine the location. In addition, a 3g modem is connected to the Raspberry Pi 3b. Connection devices which are based on 3g technology are preferred because modems using LTE technology have increased power consumption. The RC522 module is used to read RFID [3] tags.

In addition, a Real Time Clock module is connected to the Raspberry PI 3b, since this single board computer does not have a built-in module and resets the local time after a reboot. Several ultrasonic distance sensors are installed to detect the opening and breaking status of the container. They connect to the GPIO connections of the Raspberry PI 3b. Also, the servo drive is used to control the mechanical lock, and the LED RGB module acts for debugging purposes. Further additional components are a microSD memory card module and a battery.

For convenience of connecting modules and sensors, a GPIO expansion board is used. A full description of the hardware architecture of the smart container is presented in Fig. 3.

4 Software

The software consists of the following main parts:

- container software
- c platform for suppliers that provides information on the location of all containers owned by the supplier, delivery dates, and the status of all containers (burglary signals, open/closed state signal, etc.)
- A user platform that provides location and order status information

4.1 Container Software

The operating system for the Raspberry PI is Raspbian. The software for the interactions with the sensors and modules is written in Python 3. Most sensors

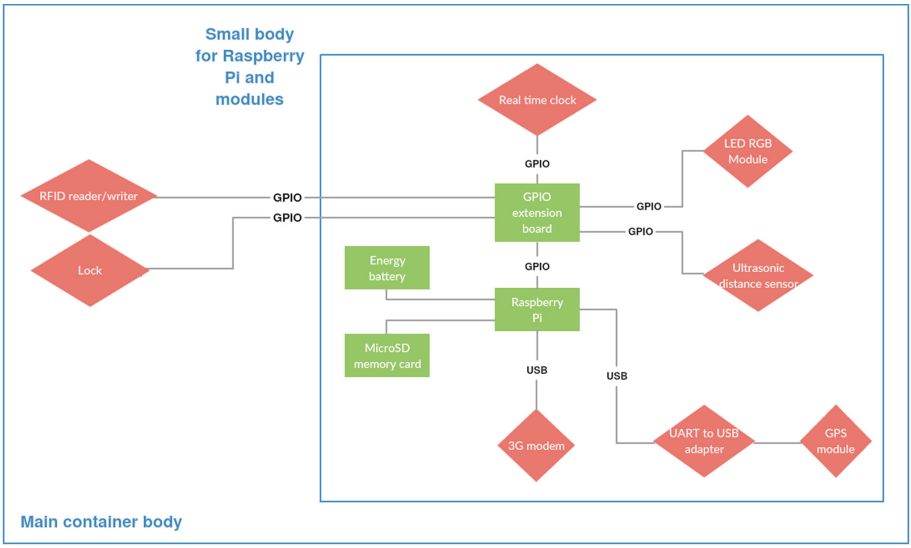


Fig. 3. Hardware architecture of a smart container.

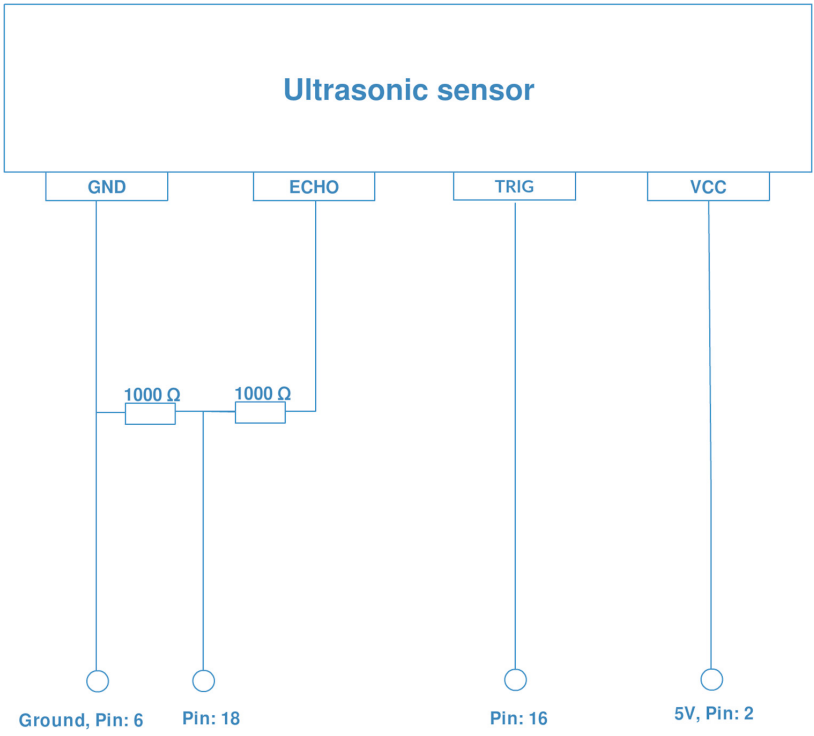


Fig. 4. Schematic representation of the distance sensor connection.

connect to a general purpose input/output (GPIO) interface. The RPi.GPIO library [6] is used to work with this interface.

Interaction with distance sensors occurs through interrupts. As soon as an electrical signal is sent to a certain pin, an interruption is called for data processing. In our case, this data is recorded and compared with previous records. This is done in order to understand whether the container is open at the moment and whether authorized access to its content has been accomplished.

Figure 3 shows the hardware architecture of a smart container. There are two metal bodies. The first body contains Raspberry Pi and main modules/sensors connected to it. The second (main) body contains the RFID reader/writer, the lock and the first body. The ratio of the sizes of metal cases in the figure does not correspond to the real. In reality, a small metal case takes up little space, while the main space remains for storing the contents of orders. The more detailed image of the connection of the distance sensor is presented in Fig. 4

Interaction with the GPS module occurs through reading data from the corresponding tty port on the Raspberry PI. As shown in Fig. 3, The GPS module is connected to a single board computer using a USB connection. However, data is exchanged using the UART interface, which, in the Raspbian operating system, is provided by default with the /dev/ttyAMA0 device. After the module establishes a connection with the satellites, it begins to send data on the latitude, longitude and height to the corresponding tty port at some intervals.

Figure 4 shows a schematic representation of the ultrasonic distance sensor connection. This sensor has 4 connection pins. First pin is called "GND" which means the ground connection that completes electrical pathway of the power. Second pin is called "ECHO". The echo sends a signal back if an object has been detected or not. If a signal is returned, an object has been detected. If not, no object has been detected. Third pin is called "TRIG". A pulse is sent here for the sensor to go into ranging mode for object detection. And last pin is called "VCC". It connects to 5 V of positive voltage for power. Pins 6,8,16 and 18 at the bottom of the figure mean corresponding GPIO pins on the Raspberry Pi. We put two 1000 Ω resistors because the GPIO pins only tolerate maximal 3.3 V.

For reading and writing RFID [3] tags, the RC522 module and the MFRC522 software library [7] in Python is used, which is distributed under the GNU Lesser General Public License.

4.2 Iroha Network

The blockchain framework Hyperledger Iroha [8–10] was chosen for this project. It is designed to be easily embedded in infrastructure projects. In addition, the framework is written in C++ and has a high performance. To join the network, read data and execute commands specific privileges are needed. In Hyperledger Iroha there is a permission distribution system. In addition, targeting mobile platforms and portability of this framework is a strong advantage.

Accounts on the Iroha network are grouped into domains. Here, the "customers" domain for user accounts, the "containers" domain for containers and

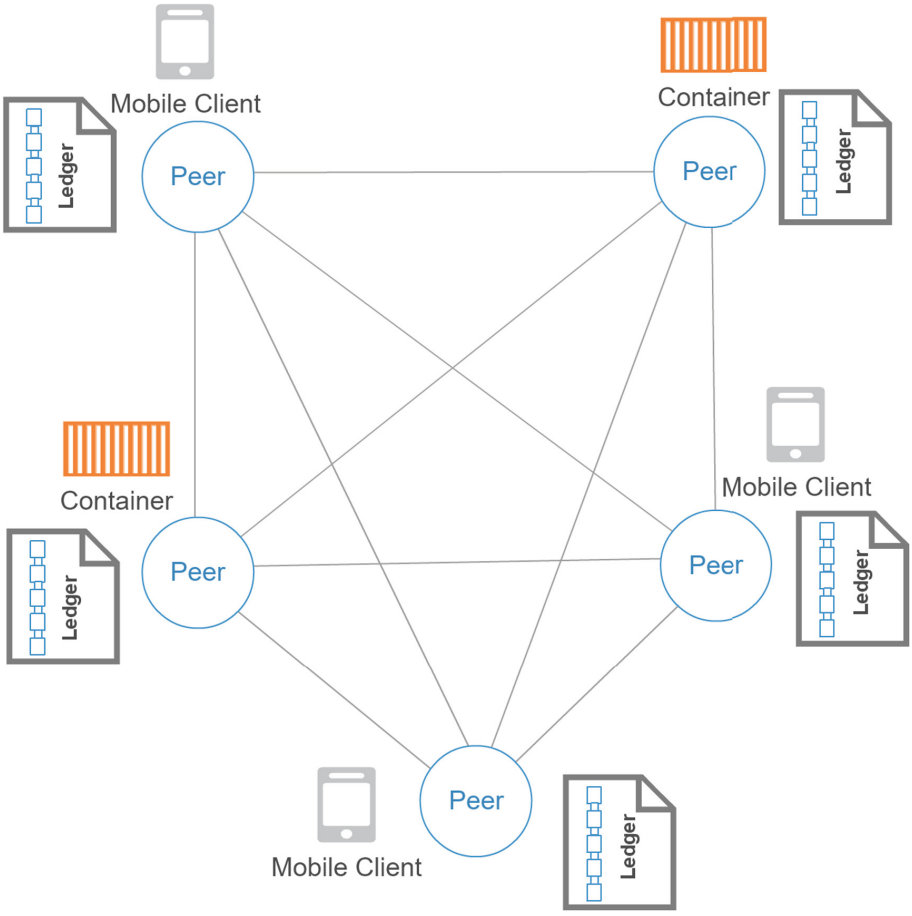


Fig. 5. Schematic representation of a blockchain infrastructure.

the names of the other domains coincide with the names of the supplier companies registered in the network are used. Each physical smart container has a registered account in the "containers" domain with a full history of movements and owners. Each record, for example data about the current location, is safely and securely stored in the account as JSON format. Additional, information also stored there:

- data about the current status: values open/closed;
- order status: values waiting to be sent/in transit/delivered/error/ unauthorized access

Rules in the user domain are adjusted in a way so only the user who is the author of the order can read the data from the account of the corresponding container. In this case, the system of distribution of privileges in the supplier's

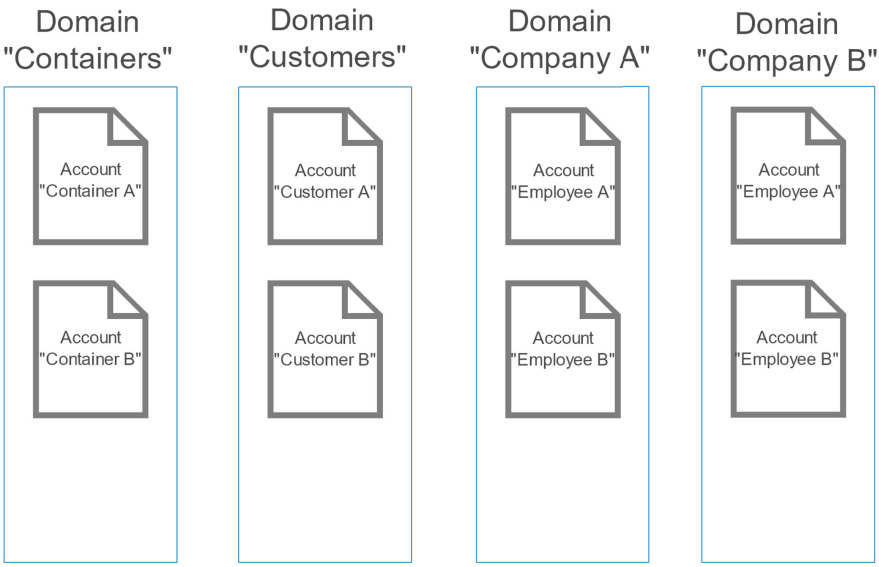


Fig. 6. Domains and accounts structure.

domain is designed that only the supplier who currently owns the container can transfer the ownership status to the next supplier or user. At the same time, information about the previous owner, next destination, as well as the history of movements and container statuses (only during the period of ownership) is available to him.

Figure 5 shows a schematic representation of a blockchain infrastructure. Containers and mobile applications are peers in Iroha network. As it is described above, each smart container has an account in the "containers" domain. Mobile applications also use accounts in the respective domains, depending on whether the account belongs to the customer or employee of the transport campaign. As it is shown in the Fig. 5, every peer keeps a copy of a ledger.

A user with an appropriate level of access can go to the container and open it through a mobile application using NFC [2]. This is made possible by using a set of predefined smart contracts, called teams, that are used to perform key transactions or to obtain information in the blockchain. In addition, mobile clients for users and suppliers use the MapD [4] tool and provide visual information about the history of container movements.

Containers, mobile apps providers and users act as peers on the Iroha Network (Fig. 6).

5 Conclusion

Blockchain technology is an innovation with capability to transform many existing traditional systems into more secure, distributed, transparent, collaborative systems. The described architecture of the smart container allows blockchain

technologies to be used in logistic systems to improve safety and efficiency. In this paper, the hardware and software components of the proposed solution are described in detail, as well as their interaction with the Iroha network.

The possibilities of using the system by users and suppliers are also described. At the same time, components such as the container body and mechanical lock can be changed depending on the wishes of customers, which allows to change the level of safety of the contents of the container for individual requirements. As the information about the container movemenents is available in realtime, the relevant parties will be able to take action quickly when a problem occurs in the supply chain [11].

References

1. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V.: Blockchain technology: beyond bitcoin. Appl. Innov. **2**(6–10), 71 (2016)
2. Patel, J., Kothari, B.: Near field communication-the future technology for an interactive world. Int. J. Eng. Res. Sci. Technol. **2**(2), 55–59 (2013)
3. Want, R.: An introduction to RFID technology. IEEE Pervasive Comput. **1**, 25–33 (2006)
4. Root, C., Mostak, T.: MapD: a GPU-powered big data analytics and visualization platform. In: ACM SIGGRAPH 2016 Talks, p. 73. ACM. July 2016
5. SmartContainers, whitepaper. https://smartcontainers.ch/en/assets/20180502_smartcontainers_whitepaper_v2.pdf. Accessed 20 Mar 2019
6. A python 3 module to control Raspberry Pi GPIO channels. https://pypi.org/project/RPi.GPIO/. Accessed 20 Mar 2019
7. A python 3 library to interact with RC522 module. https://github.com/mxgxw/MFRC522-python/. Accessed 20 Mar 2019
8. An introduction to Hyperledger, whitepaper. https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf. Accessed 20 Mar 2019
9. Hyperledger Blockchain Performance Metrics, whitepaper. https://www.hyperledger.org/wp-content/uploads/2018/10/HL_Whitepaper_Metrics_PDF_V1.01.pdf. Accessed 20 Mar 2019
10. Cachin, C., Vukolić, M.: Blockchain consensus protocols in the wild. arXiv preprint arXiv:1707.01873 (2017)
11. Dolinskaya, I.S., Shi, Z.E., Smilowitz, K.R., Ross, M.: Decentralized approaches to logistics coordination in humanitarian relief. In: IIE Annual Conference. Proceedings, p. 1. Institute of Industrial and Systems Engineers (IISE), January 2011