World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:16, No:3, 2022

Integrating Blockchain and Internet of Things Platforms: An Empirical Study on Immunization Cold Chain

F. Abujalala, A. Elmangoush, M. Ashibani

***Abstract*—**The adoption of Blockchain technology introduces the possibility to decentralize cold chain systems. This adaptation enhances them to be more efficient, accessible, verifiable, and data security. Additionally, the Internet of Things (IoT) concept is considered as an added-value to various application domains. Cargo tracking and cold chain are a few to name. However, the security of the IoT transactions and integrated devices remains one of the key challenges to the IoT application's success. Consequently, Blockchain technology and its consensus protocols have been used to solve many information security problems. In this paper, we discuss the advantages of integrating Blockchain technology into IoT platform to improve security and provide an overview of existing literature on integrating Blockchain and IoT platforms. Then, we present the immunization cold chain solution as a use-case that could be applied to any critical goods based on integrating Hyperledger fabric platform and IoT platform.

***Keywords*—** Blockchain, Hyperledger fabric, internet of things, security, traceability.

I. Introduction

SUPPLY chains that distribute heat-sensitive products are known as cold chains. Cold chains define complex distribution processes by analyzing data constantly from the manufacturer to verifying the product at the consumer. This chain involves measuring, controlling, and documenting real-time values with absolutely no room for errors. Accordingly, cold chains should be monitored carefully to control the temperature and prevent broking the chain. The pharmaceutical cold chain is one of the most serious use-cases in this field, as there have been cases where exposure to heat has led to inactivated vaccines being given to patients [1]. In addition, circulating drugs or vaccines from manufacturer to patients is a very critical concern in many developing countries due to the hot climate and poor infrastructure. The World Health Organization (WHO) has identified nine key criteria for vaccine storage and distribution [2], where temperature control is the second criterion. The recommended temperature values were set between 2 to 8 °C. Also, in the current global pandemic of the COVID-19, vaccine exposure to undesirable temperature values could lead to inactive ingredients and serious side effects. Moreover, the reluctance of people to vaccinate their children in Libya is caused by a lack of confidence in the cold chain. According to Mohamed Mleetan [19], director of the national vaccination program in Misurata, a reliable tracking system is highly needed to monitor the state of vaccines and provide real-time values. It is expected that such system will help in minimizing the response time and avoiding discarding affected vaccine doses.

Since the introduction of the IoT technology, supply-chain management had become a very attractive research area. Accordingly, IoT devices such as RFID tags or QR codes, Wireless Sensor Networks (WSN), and gateways; readers were distributed across multiparty to collect and maintain logistics data. These implementations have provided an efficient solution for traceability of goods and reduced costs. However, they lack a strong authenticity and transparency for ledgers across multiparty systems. This is highly required in Smart transport and logistics systems.

This paper proposes a traceable immunization cold chain system based on IoT and Blockchain technologies. The use of IoT technology contributes to monitoring and recording temperature, humidity, and GPS measurements through the whole chain. While Blockchain technology provides a decentralized, secure, and immutable shared ledger, which guarantees data integrity. More important, the Blockchain's digital ledger can define the responsibility of any violation in the cargo in the cold chain.

The remaining of this paper is structured as follows: Section II discusses the need for the Blockchain in IoT applications and Smart Systems. Section III reviews the related work. Section IV introduces the proposed framework. Section V discusses system implementation. Section VI introduces the adopted evaluation method. Finally, Section VII concludes the paper and defines future work.

II. IoT and the Need for Blockchain

The IoT is growing exponentially converting the physical world into a massive information system, also some researchers predict that Machine-to-Machine (M2M) connections will grow dramatically in the next years [3]. However, because of the lack of standardization of IoT modules researchers have not yet been able to define a single reference model [4]. Accordingly, the non-standardization of IoT technologies may cause security incidents in IoT systems such as ransom payment, data theft, and data forgery.

IoT is defined by International Telecommunication Union – Telecommunication sector [ITU-T] as "A global infrastructure

F. Abujalala is with Misurata University, Misurata, Libya; (e-mail: f.abujalala@it.misuratau.edu.ly).

A. Elmangoush and M. Ashibani are with Collage of Industrial Technology, Misurata, Libya; (e-mail: asma_elmangoush@cit.edu.ly, mashibani@yahoo.com).

for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies." [5]. As the definition states, IoT is an infrastructure open to new innovative information technologies. Developing reliable IoT applications is still considered a challenging job. Many crucial issues have to be solved in order to ensure the security and transparency of shared data between multi-stakeholders. Also, centralization is vulnerable to a single point of failure and data privacy breach. In order to overcome these challenges, future IoT systems need to be designed and developed according to security requirements that guarantee data and device security.

A. Blockchain Overview

Principally, Blockchain is a distributed database where assets can be stored and exchanged through a decentralized peer-to-peer network of computers. What distinguishes Blockchain from other databases is that the Blockchain ledger is an append-only database. Information in the Blockchain ledger cannot be changed or altered, i.e., every entry is a permanent entry. Furthermore, every entry is combined with the digital signatures of issuers. Thus, Blockchain technology provides good security for the user's data and also the transaction data.

The Blockchain ledger is a growing list of records, called blocks, which are linked using cryptography algorithms. As shown in Fig. 1, each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (Tx). Any attempt to change the data inside a block necessitates rehashing, not only the block relevant to the transaction but all subsequent blocks. This is possible theoretically, but it is impractical since the blocks grow continuously as other nodes add blocks to the Blockchain [6]. Transactions that are written to Blockchain ledger determines the type of Blockchain application. For instance, a Bitcoin transaction shows information about the sender, the receiver, and the number of Bitcoins to be transferred. The first block in the ledger is called the Genesis block.

Each node in the Blockchain network is assigned two keys (Public key and Private key). The assets are distributed through the network, but only the owner who has the private key can make transactions on this asset. The other computers' nodes in the network act as validators for the transaction (miners) [7]. Each transaction is verified for validity by the nodes in the Blockchain network, before recording it as a new Block into the Blockchain ledger. The nodes reach an agreement on which transactions must be kept in the Blockchain to guarantee that there will be no corrupt branches and divergences.

Depending on the Blockchain type, different consensus mechanisms exist. The most well-known is the Proof-of-work (PoW). PoW requires solving a complicated computational process, like finding hashes with specific patterns.

Many security researchers consider Blockchain as a promising solution to achieve a trusted IoT system, due to its capabilities such as immutability, transparency, auditability, data encryption, and operational resilience [8], [9]. However, Blockchain technology was originally developed for crypto-currency, and adapting it to IoT platforms and applications is still an open issue [10], [11].

B. Challenges for Adopting Blockchain with IoT

Generally, IoT applications are designed according to the traditional cloud-based architecture, where all the data collected at the node level are forwarded to the cloud for further processing. However, this architecture is not suitable for Blockchain IoT applications due to the amount of traffic that is generated by the application, and Blockchain-based systems do not rely on a unique central server or a cloud. Accordingly, researchers have presented Edge and fog computing architectures to decrease the network traffic and the computational load of traditional cloud computing systems. Fog computing is based on a set of local gateways (single-board computers such as Raspberry Pi or BeagleBone), which can respond to IoT node requests, perform local processing, interact with each other, and with the cloud. Edge computing architecture is fog gateways in addition to cloudlet to provide high-speed responses to compute-intensive requests from the node layer [7].

III. Related Work

Although Blockchain technology was originally developed for crypto-currency, it could be applied in many fields. For example, Han et al. have presented a Smart Door Lock System based on Blockchain, in order to improve IoT security issues and provide data integrity and non-repudiation [12]. Also, Lei et al. [20] have proposed a framework for providing secure key management within Vehicular Communication Systems (VCS), to improve road safety and traffic efficiency.

The framework is based on Security Managers (SM) to capture the vehicle departure information, encapsulate block to transport keys and then execute rekeying to vehicles within the same security domain.

The implementation of Blockchain technology for distributed key management has led to better key transfer time than the structure with a central manager, while the dynamic scheme allows SMs to flexibly fit various traffic levels [13]. In addition, [14] proposed a food traceability system based on Blockchain and IoT technologies to track and monitor the whole lifespan of food production. They have used IoT devices to replace human intervention for recording and verification, and Blockchain technology is used as the core of the whole system to establish a trusted, self-organized and open peer-to-peer system. Furthermore, [15] presented a start-up that uses IoT devices and Blockchain technology for the pharmaceutical supply chain. The system uses sensor devices to monitor the temperature of each parcel, and then these data are transferred manually to the Blockchain where a smart contract assesses against the product attributes.

The use of IoT and Smart Contract leads to full process automation in terms of physical, financial, and information flows. The proposed framework in this paper aims to ensure M2M communication between IoT nodes and the Blockchain

network, unlike [15] as their start-up depends on the driver to send the data to the Blockchain through a mobile application. Also, the responsibility for the cargo will be defined.

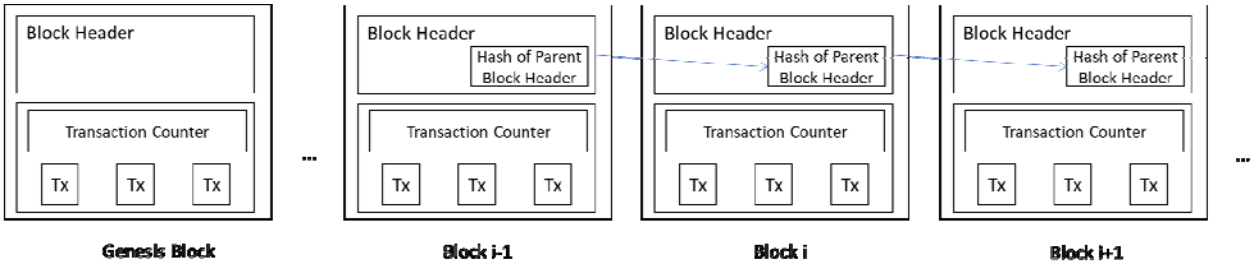

Fig. 1 Simplified Block's Structure in Blockchain

IV. The Proposed Framework

Blockchain technology is considered an efficient way to overcome security issues in IoT systems, which connect physical world data with the digital world [16]. This can be achieved by using different kinds of sensors and actuates and connecting them to the global Internet. In our use case, where vaccine packages are transported through a long road in different climatic conditions to consumers, the packaged vaccine shall be equipped with temperature and humidity sensors. The temperature and humidity data shall be aggregated at regular time intervals along the cold chain. To avoid any manipulation with the data, the Blockchain network will be in charge. A Smart Contract will be defined to control the operation of the whole system with reflection to the agreements between counterparties.

According to [17], the details of the contract should always be publicly visible to all participants. During the transportation process, the current counterparty (CP) holding the cargo specifies the next CP responsible. The handover information along with the temperature and humidity data gets written inside a block and added to the Blockchain. This enables the cold chain owner (OW); usually the vaccine's manufacturer; and any cold chain observer (OB); the buyer and transporting companies; to figure out which CP is liable at any time. The project workflow in Fig. 2 indicates all possible states of the Smart contract, as well as the transition functions for each state. It also indicates when telemetry data are collected, and how the smart contract specifics are enforced, should there be any humidity or temperature issues during the transportation process.

The Smart Contract is initiated in the Created state by the manufacturer (owner). From this point, the sensors are started to aggregate data to track the containers. Whenever the responsibility of the cargo is transferred, the state changed to In transit state. This state indicates which CP is responsible for the transferred goods (vaccines in our use-case) as well as ingesting telemetry. If the cargo reached its destination and contract rules have been verified, this will change the state to completed indicating that the smart contract ended successfully. However, if any of the contract rules have been broken during Created or In transit states, then the state will be changed to Out of compliance state indicating that the smart contract ended because of failure.

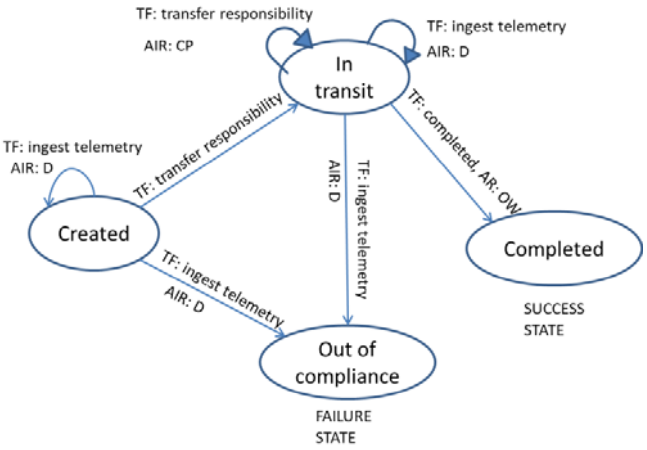

Fig. 2 Smart Contract Statues Diagram

The system architecture adopted in the project is shown in Fig. 3. Each shipment consists of one container that contains a number of boxes. So, a smart sensor will be assigned to each box that communicates with a gateway in the container through Wi-Fi or Bluetooth. The gateway communicates with the IoT Hup to record telemetry data and device ID in a database. If the readings are out of the desired range, then it will be sent to the Blockchain network and the smart contract will be updated. An intelligent IoT gateway has been chosen to be implemented on a Raspberry-pi board to ensure M2M communication, as well as processing the data locally because it is not connected to the internet all the time.

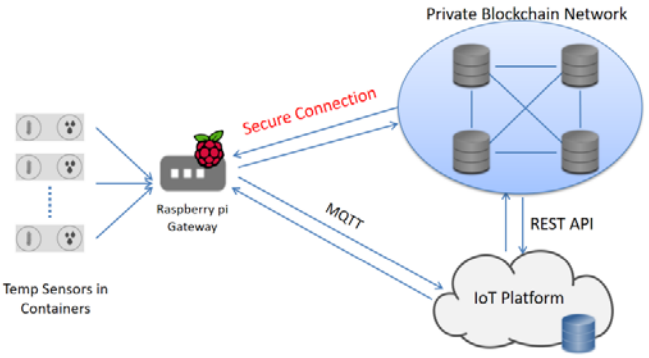

Fig. 3 System Architecture

The mechanism that is implemented to build this project is described as:

- First, the gateway will be in the Created state and define the initiating counterparty (ICP); usually, this will be the manufacturer. Then, it will configure all sensors within its WiFi or Bluetooth range using their MAC addresses, and start receiving temperature and humidity values to store them locally.
- After that, current readings and smart contract setup will be sent to the IoT database to be used for referencing data later in the chain, and the Blockchain ledger. The latter will return the smart contract ID to the gateway.
- Due to the mobility of the sensors inside the containers, the Internet connectivity is assumed to be lost most of the time. Therefore, storing and processing the data will be done locally on the gateway and it will update the IoT cloud and Blockchain ledger once the Internet connection is available. The smart contract will verify compliance with the rules and decide whether to stay in the current state or move to Out of compliance state.
- In addition, the ledger will be updated every time a new event occurs, for example starting the shipment and moving to the In transit state will change the CP to a shipment company (X).
- Lastly, arriving the cargo at its destination will change the CP to the observer (buyer) and update the ledger. The smart contract will then request measurements from the IoT database and verify compliance (Completed state) and send a complete report to the gateway.

V. System Implementation

The proposed framework consists of three major implementation stages:

- Building distributed Blockchain network using Hyperledger Fabric version 2.1 on Almadar Aljadid cloud.
- Building IoT framework based on IBM Watson IoT platform to track and store all sensor readings.
- Designing a user interface using React framework to provide API for interacting with Blockchain.

A. Blockchain Network

There are many possible scenarios that can be adopted to design the Blockchain network. Because the main concerns in this project are Internet availability and container mobility across borders, we considered two network implementations that guarantee data integrity and authentication. This shall prevent any attacker or dishonest trader from changing data from sensor devices. The first possible implementation is to have four organizations (owner – Org1, carrier – Org2, observer – Org3, and monitor – Org4) building up the network and two channels, as in Fig. 4. The main channel connects all parties and shares the same ledger recording all transactions from telemetry logging to carrier handover. The second channel connects the monitor organization within the shipment connecting all containers in that shipment building up a Local Area Network traveling with the cargo. The monitor organization consists of IoT full Blockchain gateways; each gateway is responsible for one container. This channel is responsible for sharing and mining telemetry data blocks while the shipment is disconnected from the main channel and synchronize the ledger with other organizations when the shipment reaches a port or harbor. This mechanism is suitable for large applications when the shipment consists of more than one container.

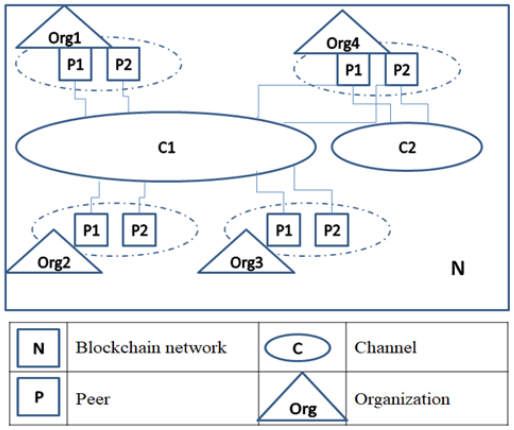

Fig. 4 Implementation of Scenario 1

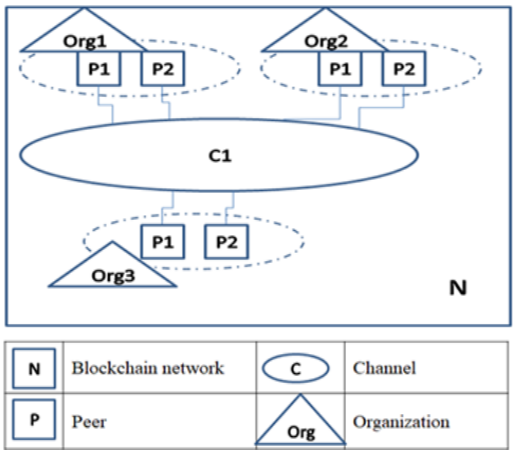

Fig. 5 Implementation of Scenario 2

The second scenario is to build the network with three organizations (owner – Org1, carrier – Org2, and observer – Org3) and one channel, as shown in Fig. 5. This implementation considers one IoT gateway working as a full Blockchain node and belongs to the observer organization. When the cargo is disconnected from the Internet, the gateway uses a digital signature and hashing algorithm to sign transactions enforcing data integrity and authentication in a block. Then, this block is mined in the ledger once the gateway is connected to the Internet. This mechanism is suitable for small shipments that are disconnected for short time in a period of hours. In this project, we adopted the second scenario, because it suits the proposed use case that is one box of vaccine transferred by airplane. The size of the block can be adopted depending on the trip period. Currently,

the Blockchain network is built on one machine and the smart contract is functioning properly. In addition, APIs are designed using the spring boot framework to invoke and query transactions from outside the Blockchain. Next, we built the Blockchain network on four machines using docker swarm.

Blockchain consensus mechanism is chosen to be Raft algorithm, as it is well adopted for private Blockchain and IoT devices. Raft mechanism features high throughput and low latency [18].

B. IoT Framework

Smart containers or intelligent boxes are required to record all sensor readings changes to the system. The gateway consists of the following components:

- Raspberry pi 4, model B running Ubuntu server arm 64 image.
- Temperature sensors used for measuring temperature and humidity.
- GPS module used for determining the location.

In order to avoid Blockchain scalability issue, all the measured data will be recorded on IBM Watson IoT platform and only undesirable values will be stored on the Blockchain. When the cargo reaches its final destination the Blockchain will synchronize the data with IBM Watson IoT platform to generate a final report.

Fig. 6 illustrates system implementation using sequence diagrams. First, the proposed application will be in the Created state and the CP is set to ICP, usually this is the manufacturer. Then, the gateway will define and connect to sensors within its container to start receiving the measured data. Once the gateway starts receiving telemetry data it sends it with CP configuration to IoT and Blockchain platforms, and the latter replays with the smart contract ID. The gateway continues to receive the measured data in an endless loop until the program is terminated. Then, at a certain time the cargo will be shipped and its responsibility moves to the carrier, as defined in *In transit* state. This will raise an event in the program to change the CP and log all the data to the Blockchain network to verify smart contract compliance, as in Fig. 7. After that, at some time in *In transit* state, Internet connectivity might be lost, so program behavior is modeled in Fig. 8. The gateway will sign and store all transactions locally and upload them to the network once it is connected and verify compliance with smart contract rules.

Finally, when the cargo reaches its final destination, the program will raise an event to change the CP to the observer and request all the measurements from the IoT platform to verify the smart contract rules and generate the final report, as in Fig. 9. If the rules comply, then the application reaches the *Completed* state. However, if at any check the rules do not comply, the application goes to *Out of Compliance* state.

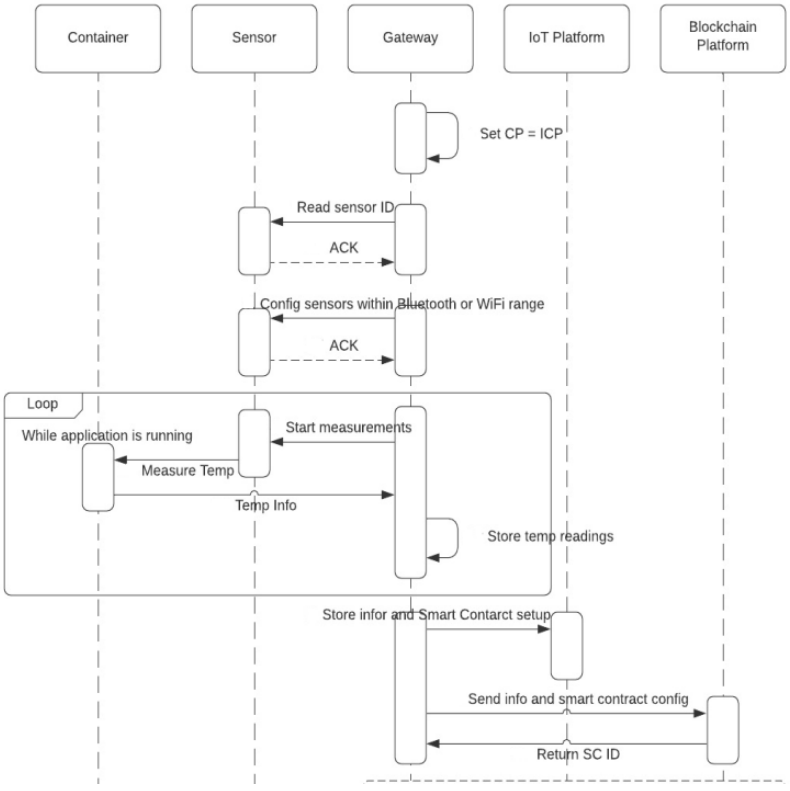

Fig. 6 Sequence Diagram for Application Startup

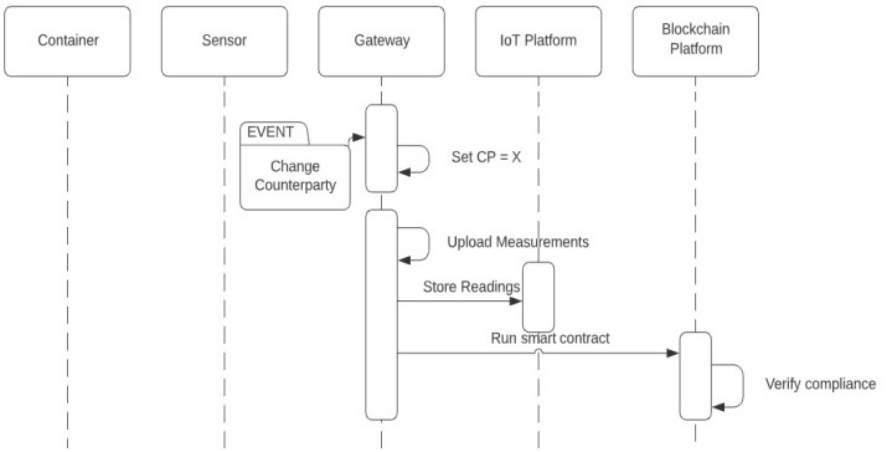

Fig. 7 Sequence Diagram for Changing CP Event

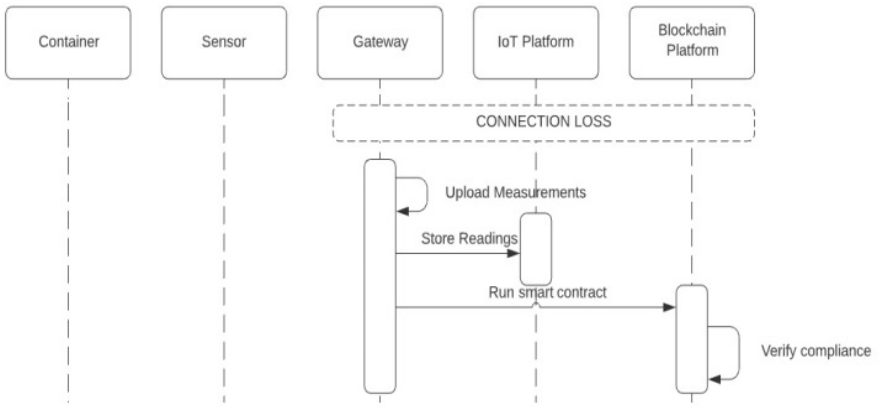

Fig. 8 Sequence Diagram for Modelling Connection-loss

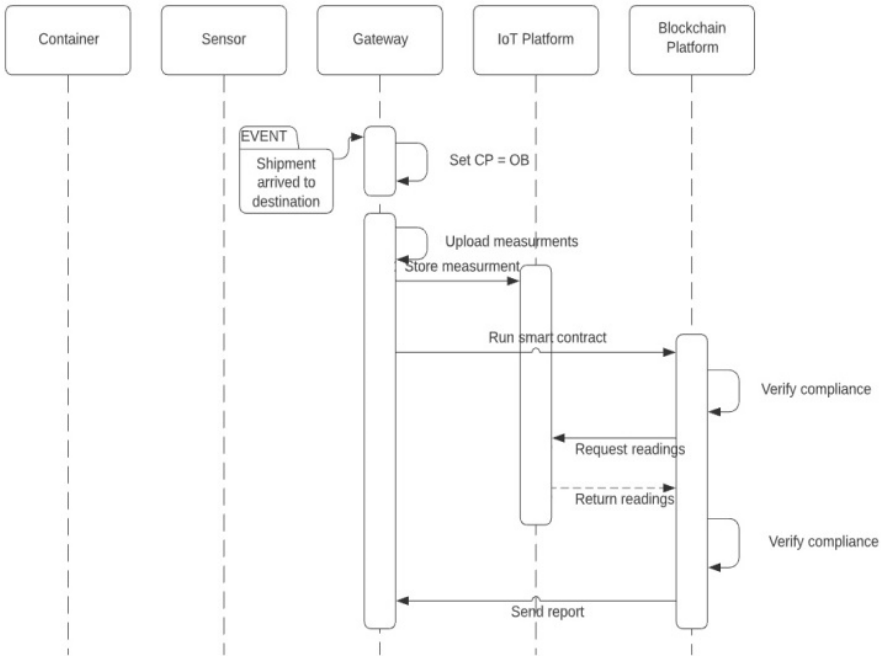

Fig. 9 Sequence Diagram when Shipment Reaches its Final Destination

C. User Interface

User interface will be developed using react framework to enable users to interact with the smart contract to invoke and query transactions which are defined in the smart contract.

VI. System Evaluation

Finding design principles and forming a design framework for implementing Blockchain-powered smart contracts is a complicated process. A suitable approach to form these deliverables is the Design Science Research (DSR) approach. This approach is specifically applicable for information systems (IS) that solve real-life problems, where only little theory has been developed, while people, organizations, and technology are important. Due to the innovative nature of the Blockchain-based artifact, a flexible selection of methods to gather diverse results is selected. This selection includes functional evaluation and technical evaluation.

First, functional evaluation includes expert interviews with demonstrations of the application and its consistency with its environment. At an early stage of this project, we met the director of the national vaccination program in Misurata. In this meeting we introduced the proposed design, and discussed the need for such a system in order to secure the national vaccination program. The interviewee found the proposed system to be appropriate to their needs.

Second, technical evaluation involves quantitative system measurements and a qualitative evaluation. Quantitative system measurements for Key Performance Indicators (KPIs) such as the number of transactions and system latency. While qualitative evaluation includes limitations of the prototype, limitations of IoT integration, limitations of Blockchain, and limitations with user interactions.

VII. Conclusion and Future Work

This paper presents a review of the existing problems and vulnerabilities associated with IoT systems, in particular authenticity, integrity, and responsiveness. Accordingly, the proposed framework integrates the permissioned Hyperledger fabric platform with the IoT platform. This integration aims to improve security in IoT applications and provide transparency and traceability through the data flow between trustless counterparties. In our work, we address the use-case of vaccine shipping and the need to trace the cargo to ensure its safety and quality. Besides, Blockchain can drive customer value, improve responsiveness, and contribute to financial success.

As a future improvement of the system, the proposed system can be extended to be applied to any goods that need to be monitored from the manufacturer to their destination. Also, it could be integrated with banking and financial systems, to prevent forgery by linking between bank credits and the content of the cargo. Moreover, a detailed investigation of the relationship between contract's parties and their defined rules is required to implement them in a smart contract. Accordingly, contractual obligations and logistics of medical goods will be studied.

Acknowledgment

This research is supported by Almadar Aljadid company.

References

[1] SupplyChainBrain, “Heat-Proofing Cold Chains with Blockchain.” (Online). Available: https://www.supplychainbrain.com/blogs/1-think-tank/post/28629-heat-proofing-cold-chains-with-blockchain.
[2] WHO, “Immunization Supply Chain,” no. March, 2014.
[3] P. Fraga-Lamas, T. M. Fernández-Caramés, Ó. Blanco-Novoa, and M. A. Vilar-Montesinos, “A Review on Industrial Augmented Reality Systems for the Industry 4.0 Shipyard,” *IEEE Access*, vol. 6. Institute of Electrical and Electronics Engineers Inc., pp. 13358–13375, Feb-2018.
[4] J. Guth *et al.*, “A Detailed Analysis of IoT Platform Architectures: Concepts, Similarities, and Differences,” in *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives*, Springer, 2018, pp. 81–101.
[5] ITU-T, “Recommendation ITU-T Y.2060, Overview of the Internet of Things.” 2012.
[6] R. Beck, “Beyond Bitcoin: The Rise of Blockchain World,” *IEEE Comput.*, vol. 51, no. April, pp. 26–30, 2018.
[7] T. M. Fernández-Caramés and P. Fraga-Lamas, “A Review on the Use of Blockchain for the Internet of Things,” *IEEE Access*, vol. 6, pp. 32979–33001, 2018.
[8] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, “Blockchain’s adoption in IoT: The challenges, and a way forward,” *J. Netw. Comput. Appl.*, vol. 125, no. September 2018, pp. 251–279, 2019.
[9] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, *Blockchain and iot integration: A systematic survey*, vol. 18, no. 8. 2018.
[10] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi, and A. Rindos, “Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric),” in *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, 2017, vol. 2017-Septe, pp. 253–255.
[11] Marko Vukolić, “The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication,” in *International Workshop on Open Problems in Network Security*, 2016, pp. 112–125.
[12] D. Han, H. Kim, and J. Jang, “Blockchain based smart door lock system,” in *International Conference on Information and Communication Technology Convergence: ICT Convergence Technologies Leading the Fourth Industrial Revolution, ICTC 2017*, 2017, vol. 2017-Decem, pp. 1165–1167.
[13] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, “Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems,” *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.
[14] J. Lin, A. Zhang, Z. Shen, and Y. Chai, “Blockchain and IoT based food traceability for smart agriculture,” *ACM Int. Conf. Proceeding Ser.*, pp. 1–6, 2018.
[15] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, “Blockchains everywhere - A use-case of blockchains in the pharma supply-chain,” *Proc. IM 2017 - 2017 IFIP/IEEE Int. Symp. Integr. Netw. Serv. Manag.*, pp. 772–777, 2017.
[16] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018.
[17] C. Gutierrez and A. Khizhniak, “IoT Meets Blockchain: Building a Supply Chain App on Microsoft Azure | Altoros.”
[18] M. Salimitari and M. Chatterjee, “A survey on consensus protocols in blockchain for IoT networks,” *arXiv*, pp. 1–15, 2018.
[19] M. Mleetan, “Interview.” Abujalala, Fawzia
[20] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, “Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems,” IEEE Internet Things J., vol. 4, no. 6, pp. 1832–1843, Dec. 2017.