Ensuring the Security of the Full Logistics Supply Chain Based on the Blockchain Technology

Igor Shostak[1[0000-0002-3051-0488]], Yashar Rahimi[1[0000-0002-5468-9726]], Mariia Danova[1[0000-0002-8116-8598]], Olena Feoktystova[1[0000-0001-8490-3108]] and Olga Melnyk [2[0000-0002-9671-108X]]

[1] National Aerospace University "Kharkiv Aviation Institute", Chkalova Str. 17, 61070 Kharkiv, Ukraine

[2] National University of Civil Defence of Ukraine, Chernyshevska Str. 94, 61023 Kharkiv, Ukraine

iv.shostak@gmail.com, rahimi.yashar@gmail.com, danovamariya@gmail.com, e.i.shostak@gmail.com, melnyk.olja.2014@gmail.com

Abstract. Issues related to ensuring the security of the functioning of the full logistic supply chain of dried fruit (SCDF) in Ukraine are considered. It is shown that the creation and function of the SCDF, compared to other supply chain management (SCM) class systems, raises a number of specific problems caused by the complexity of the interaction of raw material suppliers (fresh fruit), manufacturers of final products (drying, packaging), storage terminals, distributors, 3PL and 4PL providers (retailers). These problems are due to the fact that the interaction of participants in business processes in the SCDF generates a lot of material, financial and information flows, as well as flows of services from sources of raw materials to the final consumer. An important aspect of improving the performance of the SCDF is the development of methods and tools, and on their basis the applied information technology to ensure the reliability and security of the SCDF. To solve this problem, it was proposed to use the Blockchain technology to protect the telecommunication channels connecting the circuit elements from unauthorized access. The method of identification and authentication of digital objects of the SCDF, which guarantee the security of SCDF elements and provide them with the necessary level of confidentiality, is described.

Keywords: Full Logistics Supply Chain, Security of the IoT-Objects, Blockchain, Authentication of IoT-Objects.

1 Introductions

A typical example of a complete logistics chain is the supply chain of dry fruit to Ukraine (SCDF). SCDF is a complex socio-economic system consisting of many suppliers of raw materials (fresh fruit), manufacturers of final products (drying, packaging), storage terminals, distributors, 3PL and 4PL providers who have certain resources [1, 2]. The interaction of the participants of business processes in the SCDF is

reflected by the multitude of material, financial and information flows, as well as the flows of services from sources of raw materials to the final consumer. These features determine the specifics of this subject area, namely, a relatively large number of participants in business processes and, accordingly, the complexity of the telecommunication structure of SCDF. Due to this circumstance, there are increased risks of unauthorized access to the SCDF communication channels by competitors. The variety of world regions from which dried fruit is delivered to Ukraine, a wide range of products supplied, yield, currency fluctuations, seasonality are the causes of a high level of uncertainty in the processes of formation and decision-making by the SCDF participants [3].

These circumstances determine the lack of effectiveness of the existing SCDF and dictate the need to modernize it by expanding the concept of supply chain management (SCM) [4] by supplementing it with Internet of Things (IoT) objects, which will make it possible to achieve a conjunctive consensus between all elements of the SCDF in its functioning [5, 6].

A prerequisite for effective management of SCDFs is coordination of joint activities of SCDF participants and synchronization of their business processes, which ultimately is achieved by increasing efficiency: formulating goals and objectives of SCDFs, developing an action strategy based on in-depth and comprehensive analysis of the supply market (including the requirements of a specific customer) and the current state of the supply chain of dried fruit in Ukraine. The fulfillment of this condition is possible only if the appropriate level of protection of digital objects, which are part of the supply chain, is ensured from unauthorized access [7 - 9].

The purpose of the article is to present an approach to ensuring the security of digital objects in the SCDF, presented in the form of IoT, based on a special procedure involving the integrated use of certain software platforms within Blockchain technologies.

2 Ensuring the Protection of IoT Objects that are Part of the SCDF

Security and confidentiality is part of the measures that guarantee the reliable operation of connected IoT objects and compliance with regulatory requirements for the functioning of SCDF. The proper level of security for the operation of the SCDF is determined, in particular, by the high level of protection from unauthorized access to digital objects of chain represented in the form of IoT. The most important is the protection of such objects in the modes of identification and authentication. Identification of the Internet of Things Objects (IDoT) is a task area for assigning unique identifiers and associated metadata to the Internet of Things objects, which allows them to exchange information with other entities on the Internet [10, 11].

All IoT objects in the SCDF must be registered under unique and, very importantly, constant identifiers that are assigned at the level of the control center (focal company), and each identifier must correspond to a set of metadata - detailed information about the IoT object determined depending on context of the functioning

of the object in the composition of the SCDF. At the same time, the set of metadata itself is essentially a digital object with a clear structure. Thus, the identification and authentication of digital objects that exist in the SCDF, require the development of special algorithms, since such objects must be identified and managed. When sending confidential information, sureness in the protection of information from unauthorized use or disclosure by competitors is required [12, 13].

When building a SCDF with IoT elements, there are two key security components: the integrity and authenticity of the software of IoT objects, that is, only the software that was allowed to work on this device is loaded; authentication of IoT objects before they can transmit or receive information on material, financial and information flows within the SCDF.

3 Ensuring the Security of IoT Objects as Part of the SCDF Using Blockchain Technologies

In recent years, the Blockchain technology is at the zenith of the Gartner Hype Cycle, and now there are a large number of projects in which this technology is used to organize trusted calculations, identify and authenticate objects [14]. Using Blockchain technology to store data that has been protected with cryptographic keys gives confidence that data will not be to forged with [15, 16]. By nature, Blockchain is a distributed database in which storage devices are not connected to a common server. This database stores an ever-growing list of ordered records, so-called blocks. Each block contains a timestamp and links to the previous block. Blockchain makes intervention almost impossible, because it requires simultaneous access to database copies at all information processing centers in the SCDF. IoT data, Blockchain distributed architecture and the ability to verify ownership form the methodological basis for ensuring the appropriate level of confidentiality of business processes that occur during the functioning of SCDFs [16].

A distributed account, or the registry, which is used in Blockchain technologies, enables the ownership, transparency and general decentralization of the functioning of digital devices in the form of IoTs that are part of the SCDF.

The decentralized registries underlying Blockchain technologies are based on a circuit where the centers of trust and control are transferred to the virtual control network of the SCDF, whose nodes constantly record transactions in a specific order, into publicly available blocks, thereby creating a chain (Blockchain). Each block is a container with data that can be accessed only by the owner of the container, but any node of the SCDF can conduct the owner authentication procedure.

To build a SCDF, it is advisable to apply the so-called smart contracts: small programs that are recorded along with the data block. These programs contain rules by which data will be used. The main idea of reasonable contracts is that the parties can independently verify operations, agreeing on the conditions. Thus, metadata, including information about the owner of the object, can be recorded inside blocks, and Blockchain, among other things, is responsible for the resolution system [17].

The concept of using Blockchain to ensure the security of SCDF operation is based on three software platforms - TeleHash, BitTorrent and Ethereum. TeleHash is a decentralized and secure peering (P2P) protocol for exchanging data and transmitting messages over the network [18]. Under this security concept, data and messages transmitted using the TeleHash protocol are verified and certified by a third party; herewith the communication model is temporary, the client-server model is not used. BitTorrent is a peering (P2P) network protocol for cooperative file sharing, it implements the concept of file sharing through the interaction of source clients (seeders and leeches) [19]. The third component is Ethereum - based on the Blockchain virtual machine and a set of Web 3.0 services, which gives users the opportunity to work with the software environment of reasonable contracts, developing and filling it with content at their discretion, by supporting contract programming [20].

Based on the described software platforms, an environment of protected digital objects in the form of IoT is created, ensuring the stable functioning of the SCDF. At the same time, IoT objects within the SCDF can exchange data with each other through a hypermedia environment and form a single global continuous chain of transaction records, similar to Blockchain for bitcoins. The principal difference of this concept from the bitcoin technology is that the content and types of network entries will be determined by the contracts that will be concluded between the SCDF nodes.

A rational circuit for using Blockchain to increase the level of security for SCDF functioning will be its incorporation into the existing IoT object identification circuit as an alternative system for resolving objects or using it as an additional center of trust. For example, with a resolution in the system, the returned metadata may contain a link to the corresponding block in the decentralized registry.

New standards for IPv6-based protocols, such as 6LoWPAN, show that it is possible to create an efficient circuit for assigning unique identifiers for IoT objects in the SCDF.

4 The Identification Algorithm for Iot-Objects in the SCDF Based on the BLE/Blockchain Stack

Encryption of blocks ensures that only those parts of the chain of blocks are accessible to users for which they have private keys, without which reading or changing the record is impossible. Encryption ensures synchronization of copies of a distributed chain of blocks for all users.

The decentralized peer-to-peer Blockchain network prevents individual participants from controlling the core infrastructure of the SCDF or destabilizing its operation. All SCDF participants are considered equal and are connected to the network using the same protocols. The circuit of using the described technology for identifying the user's rights to manage the IoT-object of the SCDF shows Fig. 1.

The participant's public key (1, 2, 3) is the address itself, for managing the IoT object.

The transaction hash is a unique identifier (checksum of the entire transaction from start to finish).

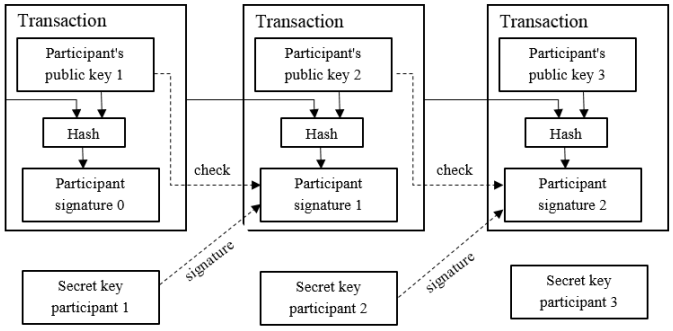

Fig. 1. The transaction process to identify the user rights of the IoT object as part of the SCDF

The signature of the participant (1, 2, 3) - with the help of the secret key confirms his authority as the owner of the object.

The generated transaction enters the block, and, like all new transactions, is launched into the network, where within a certain time, it will be attached to the chain. The network, in turn, contains a large number of nodes that form the new unit and verify the reliability of the transaction.

Nodes, by computation, select a hash for the block through a direct search of various values. When a value is found and it meets all requirements, the block is considered formed.

The application of the described algorithm ensures that all data in the SCDF is protected. Through the information in any block you can see the entire number of objects, but it is not possible to find out who owns them. In order to view the data, you need to confirm ownership of this transaction.

A special key is used to identify the user. In this case, the user has only one key, which has two different properties: having the key in hand, it will not be possible to find out the primary (source) information; it is impossible to select another data packet that would give the opportunity to create the same key.

IoT objects in the SCDF must be equipped with passive radio frequency identifications (RFID) and bluetooth low engineering (BLE) modules to ensure object identification and data transfer capabilities. BLE consists of two main parts: the controller and the host. The controller includes a physical and data link layer. The functions of the SCDF node include: the level of logical link control (LLC), the adaptation protocol (L2CAP), the attribute protocol (ATT), the generic attribute profile protocol (GATT), the security manager protocol (SMP); generic access profile (GAP). Additional application layer functionality can be implemented above the host level.

Using distributed registers to manage IoT objects is considered as the basic component of the SCDF architecture to ensure confidentiality, that is, in the proposed architecture, the Bluetooth-enabled gateway uses Blockchain technology to protect the user from unauthorized access (Fig.2).

Consider the algorithm of functioning of the gateway. This algorithm is illustrated in Fig. 3. We divide network participants into three main types: owners or administrators of IoT objects; gateway administrators; end users.

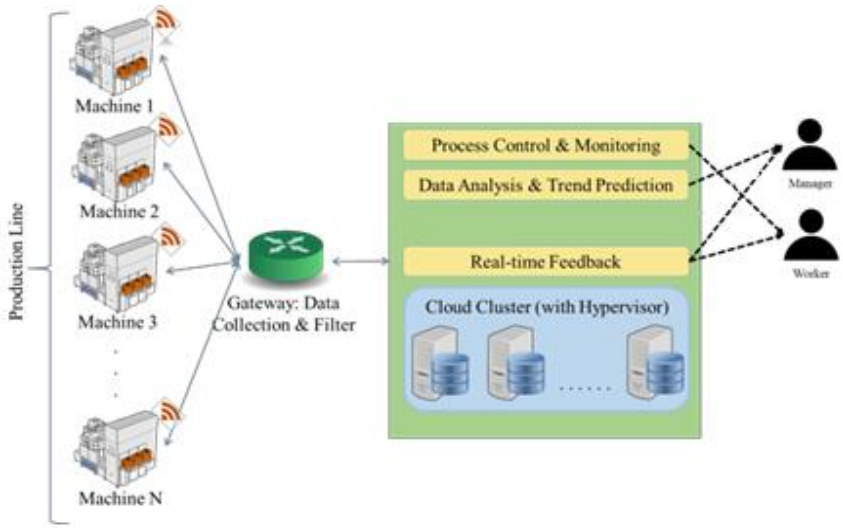

Fig. 2. Interaction of IoT objects during functioning of SCDF

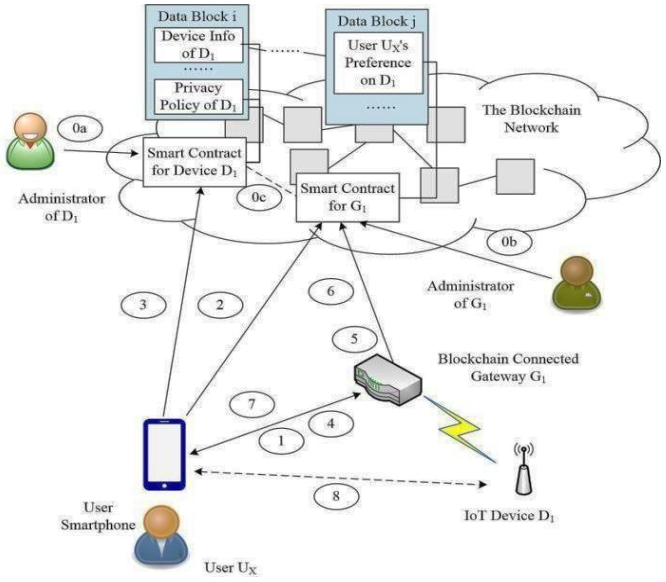

Fig. 3. Schematic representation of the algorithm for identifying IoT objects in the SCDF using Blockchain technology

Before the user can access the IoT device, the device administrator saves device information and device privacy policy in the Blockchain network. In general, the device information includes a list consisting of: a unique device name; processing relevant information; device features, such as device type, device model name and number,

serial number, etc.; other attributes for management purposes, such as a list of device images, a privacy policy, and services provided.

Using the Ethereum platform, the IoT device administrator creates a smart contract for the device and uses the contract to manage the information and privacy policy of the device (step 0a).

The gateway administrator creates a smart contract for the gateway (Step 0b). After physically connecting the gateway to the IoT device, the gateway administrator will associate the smart device contract with the smart gateway contract (step 0c). When a user uses his smartphone to connect to the gateway (Step 1), he gets the address of the smart gateway contract. Information on devices connected to the gateway becomes available to the user (Step 2). Further, the user receives the address of the smart contract of the IoT device, and controls the confidentiality through the smart contract of the device (step 3).

After receiving guarantees of confidentiality of the IoT object, the user connects to the appropriate gateway and informs the gateway that it accepts or rejects its policy (Step 4). After accepting the conditions, the parameters are saved in the gateway (Step 5), the gateway also synchronizes the storage of data in the network (Step 6). When a user accesses an IoT device through a gateway (Step 7 and Step 8), the gateway will process user requests based on the saved user settings.

5 Conclusions

1. The possibilities of using IoT objects as part of the SCDF are considered, which will ensure a reduction in overhead costs for supporting the functioning of such a chain.
2. It is shown that one of the main problems of applying IoT objects in the SCDF is to ensure their level of protection from unauthorized access.
3. It is proposed to use Blockchain technology in the form of a set of software platforms (TeleHash, BitTorrent and Ethereum) for enhancing the identification and authentication of IoT objects as part of the SCDF.
4. The central result of the research is the developed algorithm for identifying IoT objects within the SCDF and their authentication procedures, followed by authorization of the user to provide him with access rights to resources. The scientific novelty of the result lies in the complex using radio frequency identification technologies, BLE and Blockchain, as the basic processing and maintenance architecture for data to resolve conflicts in the field of confidentiality, that may occur during the operation of the SCDF.
5. In the future, the intellectualization of objects of the Internet of things is supposed by presenting them in the form of intelligent agents as part of the SCDF.

References

1. Bauersoks, D., Kloss, D.: Logistika: integrirovannaya tsep' postavok [Logistics: integrated supply chain]. 2nd edn. Olymp-Business, Moscow, 2008.

2. Rahimi, Y., Shostak, I., Feoktystova, O.: Nechetkoe modelyrovanye transportnoy sostavlyayushchey polnoy lohystycheskoy tsepy postavok sukhofruktov v Ukraynu [Fuzzy modeling of the transport component of the complete logistics chain of dried fruit deliveries to Ukraine]. Control systems, navigation and communication 3(49), 83-87 (2018).
3. Shostak, I., Rahimi, Y.: Modelirovaniye polnoy logisticheskoy tsepi postavok sukhofruktov v Ukrainu s primeneniyem vlozhennykh setey Petri [Modeling of the complete logistics supply chain of dry fruits to Ukraine using embedded Petri nets]. Modern Information Systems 2(4), 45-48 (2018).
4. Algazinov, E. K.: Analiz i komp'yuternoye modelirovaniye informatsionnykh protsessov i system [Analysis and Computer Modeling of Information Processes and Systems]. Dialog-MIFI, Moscow, 2009.
5. Kharchenko, V., Illiashenko, O., Boyarchuk, A., Sklyar, V., Phillips, C.: Emerging curriculum for industry and human applications in Internet of Things. In: 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), pp. 918-922. IEEE, Bucharest (2017).
6. Arshad, R., Zahoor, S., Shah, M. A., Wahid, A., Yu, H.: Green IoT: An Investigation on Energy Saving Practices for 2020 and Beyond. IEEE Access 5, 15667-15681 (2017).
7. Lord, N. Supply chain cybersecurity: experts on how to mitigate third party risk, https://digitalguardian.com/blog/supply-chain-cybersecurity, last accessed 2018/03/21.
8. Ukraintsev, V.B., Akhokhov, A.M.: Tekhnologiya blokcheyn v logistike: tsifrovizatsiya i pe-rspektivy ispol'zovaniya [Blockchain technology in logistics: digitalization and use prospects]. Logistics and supply chain management 6, 42-48 (2017).
9. Gulyagina, O.S.: Blokcheyn v logistike i upravlenii tsepyami postavok: opyt i perspek-tivy primeneniya [Blockchain in Logistics and Supply Chain Management: Experience and Perspectives of Application]. In: 5 International Correspondence Scientific and Practical Conference on Logistics Systems and Processes in the Conditions of Economic Instability, pp. 48-52. BGATU, Minsk, 2017.
10. The Identity of Things (IDoT): Access Management (IAM) Reference Architecture for the Internet Of Things (IoT), https://pdfs.semanticscholar.org/08c3/4cfe944aee53d004904607f0109326a42990.pdf, last accessed 2018/06/09
11. Chaudhuri, Abhik.: Identity and Access Management for the Internet of Things, https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identity-and-access-management-for-the-iot.pdf, last accessed 2018/06/11
12. Ndibanje, B. Lee, H.-J., Lee, S.-G.: Security Analysis and Improvements of Authentication and Access Control in the Internet of Things. Sensors 14, 14786-14805 (2014).
13. Chatterje, S.: A Survey of Internet of Things (IoT) over Information Centric Network (ICN). P.1-18, https://www.researchgate.net/publication/326987774_A_Survey_of_Internet_of_Things_IoT_over_Information_Centric_Network_ICN, last accessed 2018/08/19
14. Blockchain in logistics: perspectives on the upcoming impact of blockchain technology and use cases for the logistics industry, https://www.logistics.dhl/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf, last accessed 2018/09/12
15. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., Wang, H.: An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In 6th IEEE International Congress on Big Data, pp. 557 -564. IEEE, 2017.
16. Blockchain Technologies for the Internet of Things: Research Issues and Challenges, https://arxiv.org/pdf/1806.09099.pdf, last accessed 2018/10/19

17. Medrish, M. A., Belyavskiy, D.M., Darbinyan, S.S., Zasurskiy, I.I., Kazar'yan, K. R., Levova, I.Yu., Kharitonov, V.V.: Tsifrovaya identifikatsiya ob"yektov [Digital identification of objects]. Nauchnoye obozreniye, Moscow, 2016.
18. Telehash Secure Mesh Protocol, http://telehash.org/v3/spec/v3.0.0-stable.pdf, last accessed 2018/06/10
19. Protocols, Cooperation and Competition, http://medianetlab.ee.ucla.edu/papers/chapter_P2P_hpark.pdf, last accessed 2018/07/23
20. Vujicic, D., Jagodic, D., Sinisa, R.: Blockchain technology, bitcoin, and Ethereum: A brief overview. In: 17th International Symposium on INFOTEH-JAHORINA, pp. 1-6. IEEE, Bosnia and Herzegovina, 2018.