Research Article

Mechanism for strengthening the integrity of device carrying-in/out record management applying blockchain

Jinsu Kim* and Namje Park**

*Department of Convergence Information Security, Graduate School, Jeju National University
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 690-781, Korea
**Department of Computer Education, Teachers College, Jeju National University,
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 690-781, Korea
*Corresponding author.; Email address: namjepark@jejunu.ac.kr

Article History:Received:11 november 2020; Accepted: 27 December 2020; Published online: 05 April 2021

Abstract : In the case of a general goods carry-in/out management system, each device is registered by assigning a unique number to RFID, and is managed as data from a server. In this method, a single server is used, and integrity corruption behavior may occur due to errors of the single server or external attacks. Blockchain uses a peer-to-peer (P2P) network to strengthen data integrity through consensus between each client. In addition, since it does not rely on a single server, the availability of a single system can be improved in that the error of a single system does not significantly affect the entire network. In order to prevent damage to the integrity of the system, we propose a mechanism to strengthen integrity through blockchain.

Keywords: Blockchain, record management, RFID (Radio-Frequency IDentification), block network.

1. Introduction

The management of equipment import and export records in the industry is used as a system for managing loss and identification of assets held, and by attaching RFID tags to equipment requiring major management. The management of incoming and outgoing records can be quickly identified for the assets held, and the management of the devices can lead to higher production efficiency. It is also easy to manage by using RFID to obtain and manage identification codes for each device from a long distance, eliminating the need to identify each device[1-3].

RFID, in particular, has been applied and utilized in a variety of areas, such as food, health care and industry, in that it can track and monitor targets from a long distance. However, it is generally relatively expensive compared to barcodes used on behalf of RFID, and is difficult to apply when goods are cheap and large in quantity due to problems such as the possibility of information leakage through RFID, but easy to manage in case of an import and exit management system that manages limited resources[4-5].

In the case of a commodity import and exit management system, which is normally used based on RFID, a single server is configured and the unique identification number attached to each item is recognized and managed through the server. In the case of a single server, the structure is simple, easy to manage, and the network does not have to be opened externally, so it has the advantage of being able to construct a closed system. However, they share the problem that they are relatively vulnerable to falsification of data written to the server and that problems with a single server can compromise the availability of the system. In response to these problems, the block chain can verify falsification based on a shared ledger over a distributed network and increase the availability of the system because errors at one point do not significantly affect the network[6-8].

In recent years, studies have been conducted on various areas such as RFID and block chain-applied food supply chain, commodity management, and supply chain management, and several examples are presented[9-11].

Block chain can strengthen trust in a ledger, sharing the director of strong functions to verify the integrity on an open network. Data on an open network reliability required for the typical food management in the livestock industry, are block chain and logistics industry see consumers through rfidReliable represent the areas that can be granted. Wanjun yu (2018) is a block to verify food safety for using a chain and rfid foot ring was designed. The study is applying benefits, such as birds such as prevention of damage in the chain blocks about the life cycle of foot ring by block through the chain by food.Devised a way to improve trust [12]. feng tian (2016) is China's agrifood supply chain about the reliability as a way to strengthen the chain block and rfidBased on supply chain tracking system proposed [13] trust in the supply chain, which is an environment that can not be guaranteed for the information about the agrifood by tracking.With more secure market data for the agrifood and can contribute to shared to enhance data integrity can be. In addition, Petri et al (2016) emphasized the importance of real-time tracking in the global supply chain configured by multiple participants and proposed a system for real-time tracking of supply chains and logistics involving multiple participants. This study conducted a study of reliable systems by receiving information about supply chain and logistics in real time

*Corresponding author: Namje Park
Department of Computer Education, Teachers College, Jeju National University,
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 690-781, Korea
Email address: namjepark@jejunu.ac.kr

through RFID and providing transaction records with enhanced integrity by using the block chain[14-16].

In this paper, on RFID-based commodity import and exit management system for equipment held by the agency, a mechanism is proposed to enhance the integrity of records through the Blockchain's transaction ledger records and distributed networks, and to grasp the overall status of take-out and take-out[17-18].

2. Mechanism Design: Blockchain-based RFID commodity import and exit management mechanism

This section introduces the overall concept of the block chain-based RFID commodity import and exit management mechanism to be proposed. The Blockchain-based RFID commodity import and exit management mechanism proposed in this paper is implemented on an open block network and consists of a block of goods listing information about the goods for the management of the goods, a block of records of the goods taking and leaving records, and a block of user information having information about users authorized by the agency.

The manager who manages the records of incoming and outgoing goods is assumed to be a separate member. In the event that records of goods are managed by managers belonging to different agencies on the open network, the managers of each agency record only the encrypted contents on the block to be disclosed through public key-based encryption, as information about the secrets of the agency or users belonging to the agency may be leaked. At this time, the block can request information according to the identification information of each manager by performing a hash operation of the manager identification information to identify the block header that has information about the structure of the block, the contents of the block that has information about the goods import and exit record or the user, and the structure of the manager identification block that records the results in order to identify the blocks created by each manager. The proposed mechanism manages the status of goods and the records of take-out through three blocks.

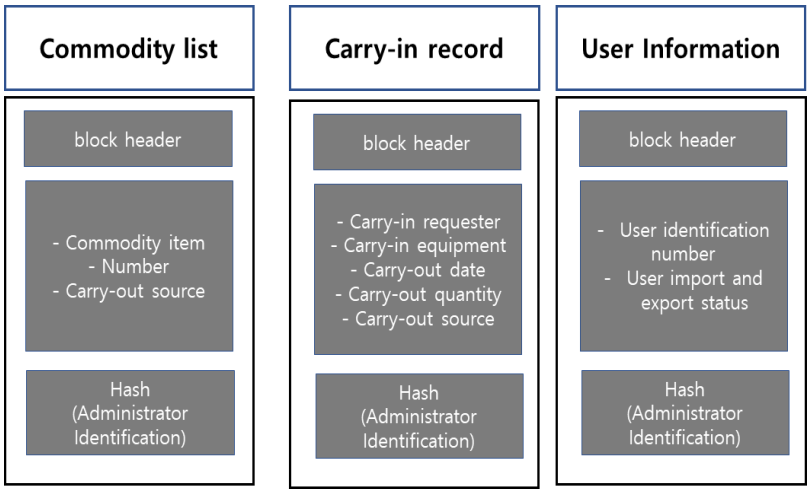

Figure 1 Block configuration of proposed mechanism

[Figure 1] shows the block structure used in the proposed mechanism. The proposed mechanism largely includes an item list block that records the status of currently stored items, a carry-in record block that records information on equipment permitted by a carry-in request, and finally, a user's identification number and a user to prevent indiscriminate carry-in. It is composed of user information blocks to check the status of carrying in/out.

[Figure 2] shows an overall schematic of the proposed mechanism. When a request for goods is made by a user, the management system requests a block of user information from the block network to authenticate the user, while at the same time preventing reckless requests from users. If the authenticated user is a normal user, the user requests a list of incoming and outgoing requests for the required goods from the user, and the user sends the list of necessary items to the management system. The management system requests the items, numbers, and outlets of the items from the block network to check the status of the items, and if it is possible to take them in and out, inform the manager that permission has been requested from the user and wait for the results of the permission. When goods are allowed in and out by the manager, the management system requests the creation of the import and exit record block by encrypting the requestor's identification number, requested item, date and quantity to the block network. The block network communicates the generation of incoming and outgoing blocks to the management system, and the management system finally conveys to the user that they are permitted to carry in and out.

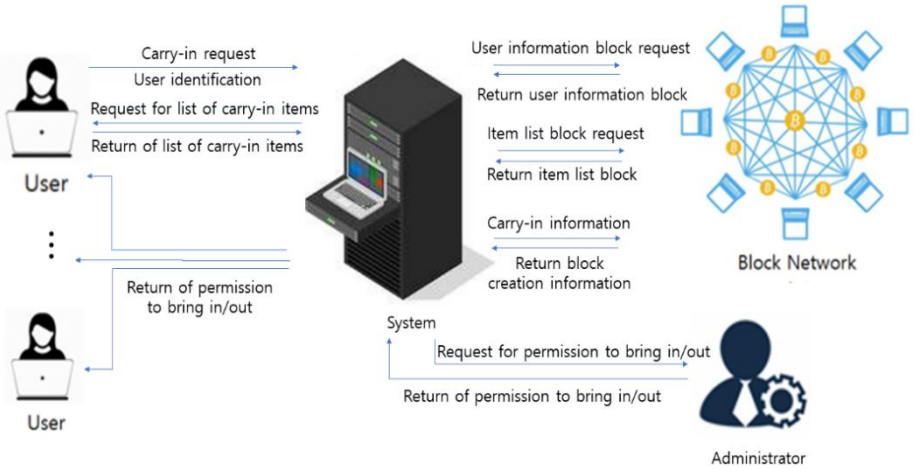

Figure 2 Concept diagram of the proposed mechanism

3. Proposed Algorithm

3.1. Terms

This section proposes and describes the algorithm. Methods adapted. (see table 1)

Table1 Terms

Content	Abbreviation
RSA encryption	RSA_E
RSA decryption	RSA_{DE}
Item list	L_I
User identification	U_{ID}
Hash operation	H_a
Administrator public key	RSA_{PKadm}

3.2. RFID Equipment Registration Process (Administrator)

The administrator can largely determine the authority to register RFID equipment with the system and whether to grant permission for incoming and outgoing requests received from the user. The manager sends RFID identification information and information about items in the goods to request registration to the system, and the management system requests the goods list block containing the hash computed manager public key of the block network. The item, number and source of the item encrypted by the RSA public key are recorded in the returned item list. The management system decrypts the contents of the returned commodity list blocks and matches the identification information based on the items of the management system requested for registration to the items of the management system, adding the identification number to the list of new identification numbers and requesting the creation of the item list blocks with additional numbers. The Block Network generates a commodity list block with a new identification number added and returns the generated results to the management system, and the Management System sends the results to the administrator [19].

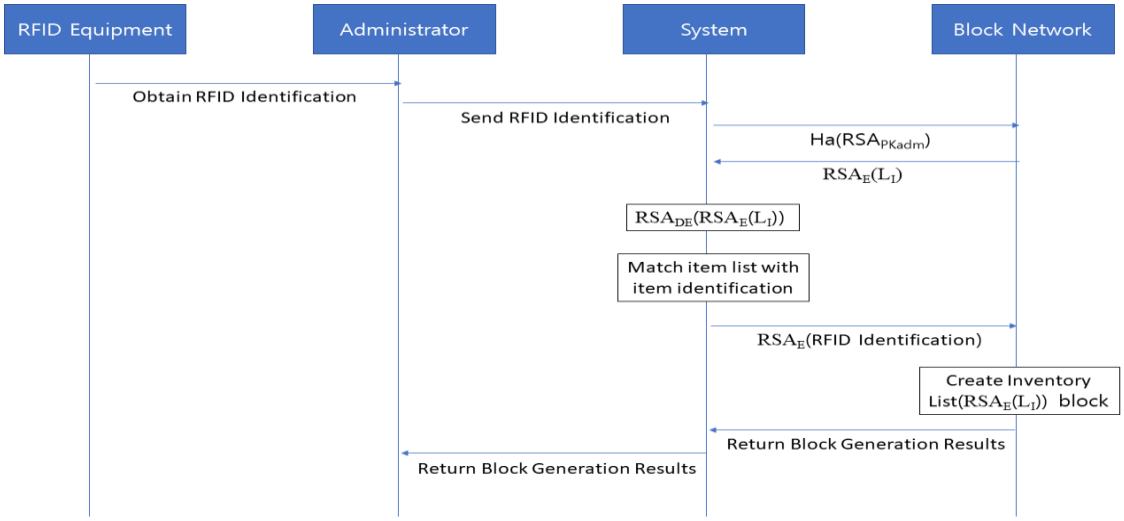

Figure 3 Process for RFID equipment registration

[Figure 3] shows the registration process of the RFID equipment described earlier and is carried out along the following steps.

Step 1: When registering a new item, the manager receives the identification information of the RFID and requests the registration of the new item in the management system.

Step 2: The management system performs a hash operation on the manager's public key and sends the generated result value to the block network to request a commodity list block with the result value of the hash operation.

$$Block\ Identification = Ha(RSA_{PKadm}) \quad (1)$$

Step 3: The inventory returned from the block network is encrypted based on the public key of the management system, and the management system decrypts the information of the transmitted commodity list block using the private key. The public key encryption method used in this section assumes the RSA public key encryption method.

$$Commodity\ List\ Block\ Information = RSA_E(L_i) \quad (2)$$
$$RSA_{DE}\left(RSA_E(L_i)\right) = L_i \quad (3)$$

Step 4: The management system matches the list of goods recorded in the block information with the identification information of the transmitted goods, and, in the case of a new identification number, requests the creation of a registered commodity list block, with the identification number of the requested item encrypted by the public key.

$$Commodity\ List\ Block\ Information = RSA_E(RFID\ Identification) \quad (4)$$

Step 5: Block Network generates commodity list blocks and returns the results to the management system, and the management system sends the block generation results to the manager.

3.3. Product carry-in request process (user)

The user can request the management system to bring the goods in and out. First, the user sends a request to the management system for carrying in/out of goods, and the management system requests the user's identification information. The user encrypts the identification information using the RSA public key and transmits it to the management system. Verify whether is a legitimate user. When it is verified that the authenticated user is a legitimate user, the user requests a list of items desired to be carried in and out, and the user transmits a list of items desired to be carried in and out. The management system requests an item list block based on the public key of the administrator who performed the hash operation to the block network. Thereafter, the management system decrypts the received item list block and, if it is possible to carry in/out, requests a carry-in/out permission from the manager, and the manager transmits the permission status to the management

system. When carrying in/out is permitted, the management system requests the block network to create a carry-in/out record block, and the block network returns a result. Finally, the management system transmits the result of carrying in/out to the user. [Figure 4] shows the user item import request process described earlier and is carried out following the following steps.

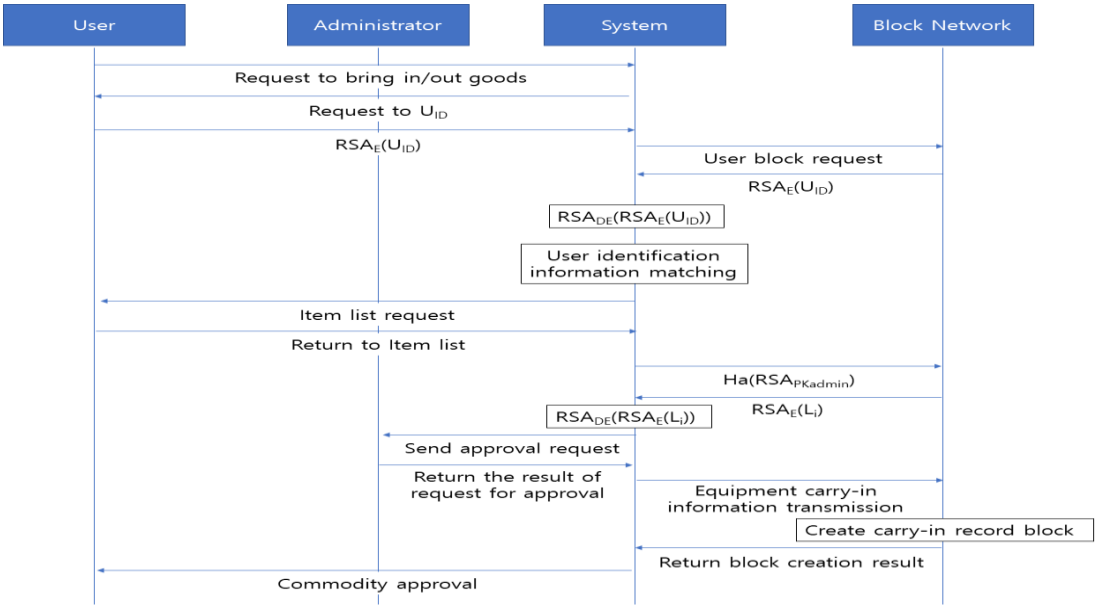

Figure 4 User item import request procedure

Step 1: Users request permission to take goods into and out of the management system, and the management system requests user identification information from the user to receive encrypted user identification information based on the public key.

$$Transferred\ user\ identification\ number = RSA_E(U_{ID}) \quad (5)$$

Step 2: The management system requests user blocks to the block network for user authentication through user identification numbers, and the block network authenticates the user by deciphering encrypted user identification information and matching the user identification information sent to the user and the user identification of the block user block.

$$RSA_{DE}\big(RSA_E(U_{ID})\big) = U_{ID} \quad (6)$$

Step 3: Once certified as an authorized user, the management system requests the user a list of incoming and outgoing equipment they wish to request and the user returns the list of incoming and outgoing equipment to the management system.

Step 4: The management system requests the commodity list block based on the administrator public key in which hash operations have been performed on the block network, and the block network returns the encrypted commodity list block.

$$Block\ Identification = Ha(RSA_{PKadm}) \quad (7)$$
$$RSA_{DE}\big(RSA_E(L_i)\big) = L_i \quad (8)$$

Step 5: The management system requests the manager to take the requested goods in and out, if possible, and waits for results.

Step 6: The management system requests the creation of blocks for the incoming and outgoing records added to the block network, the block network returns the results for the generated blocks to the management system, and the management system sends the final results for the requested take-out to the user.

4. Conclusion

This paper records user information, import/export records, product list, etc. by blocks in an RFID-based

export management system and records them in a block network, so that only encrypted information in each block can be stored and used in an open format. By classifying blocks using the administrator's public key, the integrity of the contents recorded in the blocks can be guaranteed through one common block network of different organizations, and the availability of the system can be increased through a distributed network environment. In the future, research is required on mechanisms that can ensure the integrity of logistics records on closed networks.

5. Acknowledgements

This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2019S1A5C2A04083374).

7. References

1. Jie Xu, Shuang Guo, David Xie, Yaxuan Yan, Blockchain: A new safeguard for agri-foods, Artificial Intelligence in Agriculture; 2020, p. 1-21.
2. Robert Garrard, Simon Fielke, Blockchain for trustworthy provenances: A case study in the Australian aquaculture industry, Technology in Society; 2020.
3. Bin Shen, Xiaoyan Xu, Quan Yuan, Selling secondhand products through an online platform with blockchain, Transportation Research Part E: Logistics and Transportation Review; 2020.
4. Jinsu Kim, Namje Park. Lightweight knowledge-based authentication model for intelligent closed circuit television in mobile personal computing. Personal and Ubiquitous Computing; 2019, p. 1-9.
5. Siye Wang, Shaoyi Zhu, Yanfang Zhang, Blockchain-based Mutual Authentication Security Protocol for Distributed RFID Systems, 2018 IEEE Symposium on Computers and Communications (ISCC); 2018
6. Peter Verhoeven, Florian Sinn, Tino T. Herden, Examples from Blockchain Implementations in Logistics and Supply Chain Management: Exploring the Mindful Use of a New Technology, logistics; 2018.
7. Gallay Olivier, Korpela Kari, Tapio Niemi, Nurminen Jukka K, A peer-to-peer platform for decentralized logistics, Digitalization in Supply Chain Management and Logistics; 2017.
8. Jinsu Kim, Namje Park, Blockchain-Based Data-Preserving AI Learning Environment Model for AI Cybersecurity Systems in IoT Service Environments, Applied Sciences; 2020.
9. Hackius Niels, Petersen Moritz, Blockchain in logistics and supply chain: Trick or treat?, Technische Universität Hamburg (TUHH); 2017.
10. Edvard Tijan, Saša Aksentijević, Katarina Ivanić, Mladen Jardas, Blockchain Technology Implementation in Logistics, Sustainability; 2019.
11. Mario Dobrovnik, David M. Herold, Elmar Fürst, Sebastian Kummer, Blockchain for and in Logistics: What to Adopt and Where to Start, logistics; 2018.
12. Wanjun Yu, Shiyuan Huang; Traceability of Food Safety Based on Block Chain and RFID Technology. 2018 11th International Symposium on Computational Intelligence and Design (ISCID); 2018 Apr. DOI: 10.1109/ISCID.2018.00083
13. Feng Tian; An agri-food supply chain traceability system for China based on RFID & blockchain technology. 2016 13th International Conference on Service Systems and Service Management (ICSSSM); 2016 Jun; DOI: 10.1109/ICSSSM.2016.7538424
14. Petri Helo, A.H.M. Shamsuzzoha; Real-time supply chain—A blockchain architecture for project deliveries. Robotics and Computer-Integrated Manufacturing; 2020 Jun; 63; DOI: 10.1016/j.rcim.2019.101909
15. Saikat Mondal, Kanishka P. Wijewardena, Saranraj Karuppuswami, Nitya Kriti, Deepak Kumar, Premjeet Chahal; Blockchain Inspired RFID-Based Information Architecture for Food Supply Chain. IEEE Internet of Things Journal. 2019 Mar; 6; 3; 5803-5813; DOI: 10.1109/JIOT.2019.2907658
16. Namje Park, Younghoon Sung, Youngsik Jeong, Soo-Bum Shin, Chul Kim. The Analysis of the Appropriateness of Information Education Curriculum Standard Model for Elementary School in Korea. Journal of Studies in Computational Intelligence; 2018 791, p.1-15.
17. Namje Park, Byung-Gyu Kim and Jinsu Kim. A Mechanism of Masking Identification Information regarding Moving Objects Recorded on Visual Surveillance Systems by Differentially Implementing Access Permission. ELECTRONICS; 2019 8(7), 735.
18. D. Lee, N. Park. Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree. Multimedia Tools and Applications; 2020; p. 1-18
19. Kumar, N. M., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 132, 1815-1823.