Proof of Authenticity of Logistics Information with Passive RFID Tags and Blockchain
(Extended Abstract)

Kenji Saito
Graduate School of Business and Finance, Waseda University, Japan
E-mail: ks91@aoni.waseda.jp

I. INTRODUCTION

Today, the logistics of physically moving resources and materials has become increasingly important, as behaviors of people change, and society is restructured through the penetration of digital communication technologies, the spread of infectious diseases and other factors, and as remote presence and remote work become more common.

In tracing the (robotically automated) logistics of large quantities of goods, inexpensive passive RFID (Radio Frequency IDentification[1]) tags are easy to use from a cost perspective. Accordingly, security between such tags and readers have primarily been studied in the literature[2] among many issues surrounding RFID in the past. However, the authenticity of the identified information cannot be guaranteed by measures between tags and readers alone if the communication between clients and services is considered, because services may give false information, deliberately or by accident. Although the use of blockchain[3] is often discussed, it is simply a recording system, so there is a risk that false records may be written to it at the beginning, in which case the tamper-evidentness of blockchain becomes meaningless.

We feel a strong need to overcome these challenges, and ensure the authenticity of information obtained through RFID in a logistics network. This paper is an extended abstract version of [4], an effort to answer such needs.

II. PROBLEM

We would like to design an information infrastructure to ensure that information written to or read from tags at specified locations by controlled RFID readers is correctly shared in the logistics network. In particular, we have to solve the problem of whether the data in the tag read and written by the reader is treated with integrity, and communicated with the client as it is, even through the service provider that can be seen as an opaque box. Security between the reader and the tag is out of scope of this work, although unclonability of tags is assumed.

III. DESIGN

To solve the problem, we introduce an additional entity to provide digital evidences. Our design is outlined as Fig. 1.

In our proposal, an RFID reader, identified by digital signatures, functionally constrained to work only at a specific physical location through a positioning system, and is tamper-evident, writes the digital evidence to blockchain as it reads from and writes to the RFID tag in an atomic (non-separable) operation. To be tamper-evident, a reader is assumed to be equipped with an unclonable chip, and needs to be occasionally replaced by its vendor as the public key certificate expires.

RFID data readout and its evidence are formulated as shown in Fig. 1. A public key digest is used as the identifier of a reader. A ⟨random number, tag ID⟩ pair is used as a key for searching readouts or evidences. The random number (presumably generated by the service) is used for hiding the tag ID from blockchain operators, and is shared among clients, the service and readers. Timestamp and location are assumed to be obtained by the reader’s internal positioning system.

IV. FEASIBILITY

We are building an experimental prototype to implement our design for evaluation and demonstration purposes. A bluetooth RFID reader is coupled with a smart phone (can be replaced by a microcomputer) to simulate a more intelligent reader. In the real setting, the reader is to be equipped with physical identification as described in [5] and [6] for tamper-evidentness. We use BBc-1[7], a toolkit to make applications of blockchain, in our prototype. If the evidence is written to Ethereum[8] (blockchain of our choice for the prototype) each time when a large number of tags are read or written, the cost will be enormous. Therefore, we construct a Merkle tree[9] off-chain using the toolkit, and periodically write only the Merkle root to Ethereum to realize a blockchain service as a whole.

An example run of the prototype, assuming logistics services 1 and 2, is as follows:

1) An RFID reader generates a key pair.
2) The vendor of the reader issues a certificate for the relevant public key.
   • Typically this is followed by shipment of the reader.
3) Reader reads the tag’s ID and writes data (that can identify service 1 and the final destination, for example) to the tag by the order from service 1.
   • At the same time, the corresponding evidence is sent to the digital evidence service by the reader, and a Merkle tree is grown, and the Merkle root is periodically written to Ethereum.
4) The package with the tag is transported to a distant relay point.

5) The tag in question is read by another reader at the relay point by the order from service 2, yielding ID and data.
   • At the same time, the corresponding evidence is sent to the digital evidence service by the reader, and eventually stored in Ethereum in the form of a Merkle root.

6) Service 2 identifies service 1 from the data, and gets the past readout from service 1.

7) Service 2 gets the Merkle proof (a subtree from which the Merkle root can be obtained through simple calculations) of the evidence regarding the past readout from the digital evidence service.

8) Service 2 recalculates the Merkle tree from it and finds that the readout obtained from service 1 is authentic as it matches the Merkle root stored in an Ethereum block, and from the block number representing the block creation time for the Merkle root, service 2 can confirm approximately by what time the readout was recorded. Then service 2 can forward the package to the verified final destination.

We estimated the cost of operating the smart contract in our prototype on Ethereum, and found that that would impose just a moderate cost onto the digital evidence service, which would be more than offset by the increased benefits this infrastructure will bring.

V. CONCLUSIONS

Although we will continue to work on the prototype for evaluation, and refine our proposal, we believe that our proposal makes it possible to trace authentic logistics information using inexpensive passive RFID tags. Furthermore, by abstracting the reader/writer as a sensor/actuator, the method can be extended to the Internet of Things (IoT) in general.

REFERENCES

[1] A. Razaq, W. T. Luk, K. M. Shum, L. M. Cheng, and K. N. Yung, “Second-Generation RFID,” IEEE Security & Privacy, vol. 6, no. 4, pp. 21–27, 2008.

[2] J. Juels, “RFID Security and Privacy: A Research Survey,” IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 381–394, 2006.

[3] K. Saito, “Asia Internet History Projects - Fourth Decade (2010s) Section 2.3 Blockchain,” InternetHistory.Asia, Sep. 2020, https://sites.google.com/site/internethistoryasia/book-4-2011-2020.

[4] H. Watanabe, K. Saito, S. Miyazaki, T. Okada, H. Fukuyama, T. Kato, and K. Taniguchi, “Proof of Authenticity of Logistics Information with Passive RFID Tags and Blockchain,” Nov. 2020, https://arxiv.org/abs/2011.05442.

[5] H. Watanabe, “Can Blockchain Protect Internet-of-Things?” in Proceedings of the 2017 Future Technologies Conference (FTC). The Science and Information (SAI) Organization, 2017, pp. 104–112.

[6] H. Watanabe and H. Fan, “A Novel Chip-Level Blockchain Security Solution for the Internet of Things Networks,” Technologies, vol. 7, no. 1, p. 28, Mar 2019.

[7] K. Saito and T. Kubo, “BBc-1: Beyond Blockchain One – An Architecture for Promise-Fixation Device in the Air –,” beyond-blockchain.org, Oct. 2017, https://github.com/beyond-blockchain/bbc1/blob/develop/docs/BBc-1_design_paper.pdf.

[8] V. Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” ethereum.org, 2013, https://github.com/ethereum/wiki/wiki/White-Paper.

[9] R. C. Merkle, “A Digital Signature Based on a Conventional Encryption Function,” in Advances in Cryptology — CRYPTO ’87. Berlin, Heidelberg: Springer, 1988, pp. 369–378.