ISSN: 2586-7652 | 2635-7607 Vol. 02, No. 02 September 2019

International Journal of Advanced Engineering

Source: http://ictaes.org

Manuscript received: August 17, 2019; Revised : September 15, 2019 ; Accepted : September 20, 2019



Blockchain in Handicraft Supply-chain Management

Janardan Bhatta[1], Shiva Gaire [2], Saurav Pandey[3], Shekhar Koirala[4], Kushal Gajurel[*]

[1 ,3 ,4, *] *Institute of Engineering Thapathali Campus, Tribhuvan University*
[2] *Kathford International College of Engineering and Management*

Janardan.bhatta@ioe.edu.np[1], geeksambhu@gmail.com[2], pysaurav@gmail.com[3], shekharkoirala4@gmail.com[4], gajurelkushal1994@gmail.com[*]

Abstract

Supply-chain Management involves a network of facilities that function through the procurement of materials, transformation of these materials into intermediate and final products, and their distribution to consumers. In this paper, we propose an efficient Supply-chain management system for Handicrafts using Blockchain which addresses the deficiencies pertaining to the traditional system. The proposed Blockchain system involves a distributed, immutable and highly reliable ledger that records information on a Handicraft when it moves through manufacturer to its buyer in a Supply-chain, along with cheap Internet of things devices that provides transparency, flexibility, and tracking.

Keywords: *blockchain; proof of authority; internet of things; supply-chain; transparency.*

1. Introduction

The traditional supply chain is inefficient, there is a lack of transparency regarding the true value of the product. In Nepal, handicrafts worth 52 billion rupees were exported in fiscal year 2016/2017 (Artisans in Nepal: Honoring Tradition, Crafting the Modern), yet we lack proper methodologies to ensure their authenticity. The cultural future of 1.1 million populations, who are involved in handicraft industry that constitutes 20% of the total exports (Artisans in Nepal: Honoring Tradition, Crafting the Modern), is at risk. This is where a Supply-chain Management system empowered by a Blockchain can play an important role.

Corresponding Author: Kushal Gajurel
Author's affiliation: Inistitute of Engineering Thapathali, Tribhuvan University
Email: gajurelkushal1994@gmail.com

A Supply-chain comprises of three phases: the flow of raw materials into a manufacturing plant, it's processing by manufacturers and finally distribution of the final goods to the consumers through a distribution system [1]. The current implementations of Supply-chain management systems have the downside of being inefficient, expensive and vulnerable [2]. Moreover, avoiding counterfeit products, handicrafts in our case, in a Supply-chain is a real problem which creates a trust gap between manufacturers and consumers. Blockchain is a peer-to-peer distributed ledger that records transactions in a cryptographically secure and permanent fashion. It is basically a chain of blocks that use hash pointers to point to the previous block. It uses a decentralized consensus mechanism to provide a means of agreeing to a single version of truth by all peers on the blockchain network [3]. We propose to use Proof of Authority as the consensus mechanism in our systems since the manufacturer needs some sort of control over the system. By sharing ledger between multiple parties, blockchain essentially removes the need for intermediaries who were previously required to act as trusted third parties to verify, record and coordinate transactions [4].

Internet of things (IoT) system architecture comprises three layers, a physical layer consisting of a Radio Frequency Identification (RFID) sensor, a network layer and an application layer. RFID makes use of low power Radio Frequency waves to read and write data providing a unique ID to every item in the supply chain. Similarly, a consumer will be interfacing a Near-Field Communication device (NFC) [5], which operate at the same frequency. The upper layer than physical layer is network layer which is made up of wireless sensor network. This layer provides a real-time data network for the physical layer which is used by the upper industrial application layer. The application layer mainly deals with strategic data analysis using machine learning algorithms, which is out of the scope of this paper.

2. Architecture Overview

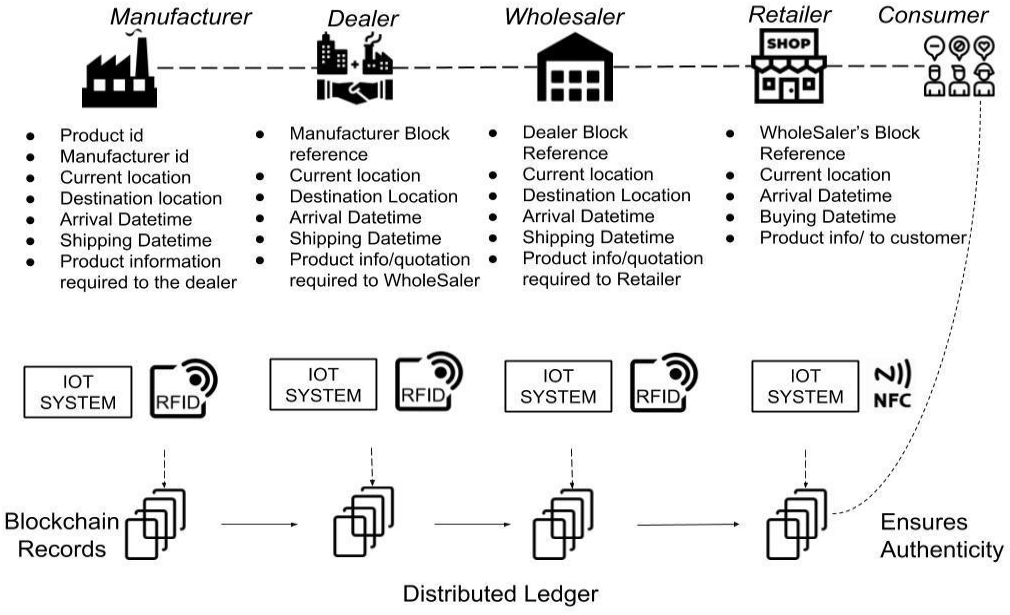


Figure 1. System architecture overview: blockchain powered supply-chain

Proposed Supply-chain system, powered by a Blockchain, encompasses any number of nodes, which may be a manufacturer, a dealer or a retailer, that maintain their own list of parameters (refer Figure 1) of each handicraft in the Supply-chain. A fixed number of such information (record) forms a fixed-sized block. The block is then validated by authorized nodes to authenticate the records. This is a consensus mechanism called Proof of Authority (PoA). Once a block is verified, it is cryptographically written into the ledger of the validator and then synced with all other identical ledgers across the network, forming a valid and immutable chain of blocks. All the nodes in the network have access to this identically distributed ledger from where they can retrieve and accumulate information. This cryptographically secured information is transferred physically, from a node to the other via RFID device where the blockchain provides authenticity to the embedded information.

2.1 Record structure

The manufacturer's record will include product id which uniquely identifies the product, manufacturer id to uniquely identify the manufacturer, current location and destination location for the real-time tracking of product, shipping and arrival date to keep track of outgoing and incoming products, and the manufacturer will also include the product information required by the dealer. Similarly, a dealer's record includes the hash of manufacturer's block for preventing redundant data across the chain of the block for a particular product. This also provides tamper-proof evidence of data being stored by the manufacturer. Furthermore, records of dealer, wholesaler and retailer include current location and destination location for the real-time tracking of the product, arrival date and shipping date to track the product they hold in stores. The records are synced between all the nodes. The dealer, wholesaler and retailer will also keep the previous block reference as a hash such that information is not redundant in a blockchain transaction which minimizes blockchain transaction cost.

2.2 IoT implementation

Each node consists of an IoT system that accumulates records into a block which is appended to the chain of the distributed blockchain. The information in a record is embedded into the RFID device and attached with handicraft and sent to the next node. During transportation between the nodes, an IoT system handles real-time monitoring of transportation sensor data. When the package arrives at the destination node, an IoT system appends the transportation sensor data with the product's data in RFID tags. The combined data is then hashed that forms a record and a chunk of such records (block) is appended to blockchain network and flash written to the same RFID tag of the item. This process continues for every node.

The major limitation of RFID for the system is, any intruder can easily copy or read every bit of data written in an RFID tag. That intruder can sell any other item using the valid, possibly encrypted copy of RFID tag. We proposed a location-based RFID system where we write an item details along with GPS location address of next distribution center to every RFID tag of a distribution IoT [6]. The encrypted key will only be validated when the key is used around from the specified GPS location. So, to get the item's data for showing a fake item is real, the intruder must be in the GPS location which adds a new layer of security in the system. Similarly, only the admin of a distribution system can write next GPS location to a block in the blockchain.

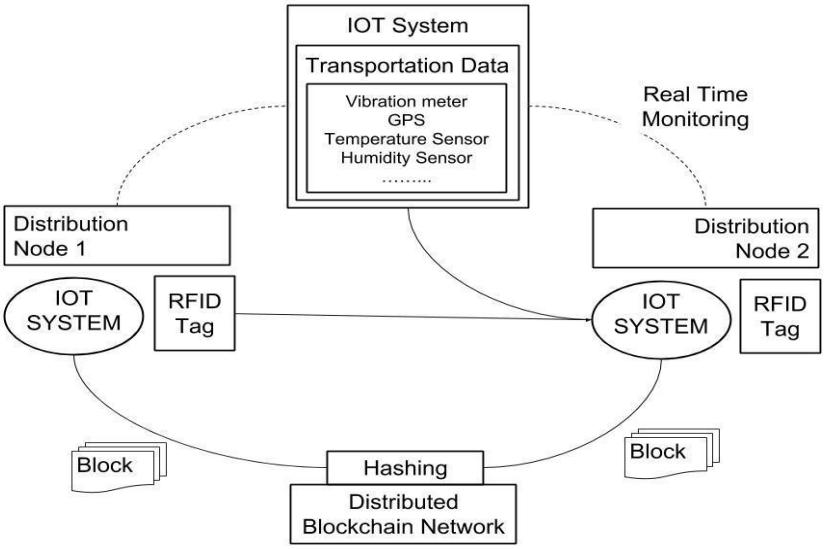


Figure 2. IoT System Implementation

5. Conclusion

The proposed Handicraft Supply-chain Management system utilizes Blockchain technology which is relatively new in the realm of Supply-chain but has tremendous possibilities for making a Supply-chain better. Therefore, we can conclude that incorporation of Blockchain technology along with IoT devices into the existing Supply-chain Management substantially maximize efficiency, minimize expenses and create a transparent system, along with providing authenticity to a Handicraft product.

Among the various challenges in the implementation of blockchain in a supply chain, if any intruder exchanges a handicraft during transportation, we are unable to detect the counterfeit one. The problem can be solved by using fingerprint-based RFID [7]. The present research only deals with handicrafts and its tracking. The monetary prospect of Supply-chain is yet to be revolutionized by blockchain technology called smart contracts.

Acknowledgment

The research is supported by IOE, Thapathali campus, for technical as well as financial support for all phases of the research.

References

[1] Hofmann, E., Strewe, U., & Bosia, N. (2018). Supply Chain Finance and Blockchain Technology. Cham: Springer.

[2] Verhoeven, P., Sinn, F., & Herden, T. (2018). Examples from Blockchain Implementations in Logistics and Supply Chain Management: Exploring the Mindful Use of a New Technology. *Logistics, 2*(3), 12.

[3] Bashir, I. (2018). Mastering Blockchain. Birmingham, UK: Packt Publishing, p.88.

[4] M., Heutger, & D., Kückelhaus. (2018). BLOCKCHAIN IN LOGISTICS (p. 3, Publication). Troisdorf: DHL Customer Solutions & Innovation.

[5] Kaur, M., Sandhu, M., Mohan, N., & Sandhu, P. (2011). RFID Technology Principles, Advantages,Limitations & Its Applications. International Journal Of Computer And Electrical Engineering, 151-157.
[6] Li, Z., Wu, H., King, B., & Ben, Z. (2017). On the integration of event-based and transaction-based architectures for supply chain. International Conference on Distributed Computing Systems Workshops, 376-382.
[7] Periaswamy, S., Thompson, D., & Jia Di. (2011). Fingerprinting RFID Tags. IEEE Transactions On Dependable And Secure Computing, *8*(6), 938-943.