IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12520

BLOCKCHAIN INSPIRED RFID BASED INFORMATION ARCHITECTURE FOR THE FOOD SUPPLY CHAIN

D.R. ANGEL KIRUBA[1], ANGEL PRINCY A[2], JEVITHA R[3], MADIHA ZEHRA K[4]

Assistant Professor, Department of Computer Science, DMI College of Engineering, Chennai, Tamil Nadu, India[1]

Student, Department of Computer Science, DMI College of Engineering, Chennai,Tamil Nadu, India[2-4]

Abstract: This paper proposes a blockchain-inspired Internet-of-Things architecture for creating a transparent food supply chain. The architecture uses a proof-of-object-based authentication protocol, which is analogous to the cryptocurrency's proof-of-work protocol. The complete architecture was realized by integrating a radio frequency identification (RFID)- based sensor at the physical layer and blockchain at the cyber layer. The RFID provides a unique identity of the product and the sensor data, which helps in real-time quality monitoring. For this purpose, a small feature size 900-MHz RFID coupled sensor was fabricated and demonstrated for real-time sensor data acquisition. The blockchain architecture aids in creating a tamper-proof digital database of the food packages at each instance. A detailed security analysis was performed to investigate the vulnerability of the proposed architecture under different types of cyber-attacks.

Keywords: Food Supply Chain, Blockchain, radio frequency identification (RFID), tamper-proof.

I. INTRODUCTION

In this, we propose a blockchain-inspired internet-of-things architecture for creating a transparent food supply chain. The architecture uses a proof-of-object-based authentication protocol, which is analogous to the cryptocurrency's proof-of-work protocol. The complete architecture was realized by integrating an RFID-based sensor at the physical layer and a blockchain at the cyber layer. The RFID provides a unique identity of the product and the sensor data, which helps in real-time quality monitoring. For this purpose, a small feature size 900 MHz RFID coupled sensor was fabricated and demonstrated for real-time sensor data acquisition. Agriculture is a big part of the economy of any country because it helps feed the entire population. It connects and communicates with all of the related industries. If the agriculture base is strong, it is generally regarded as a socially and politically stable society. Many modern farms make use of cutting-edge technology and scientific and technological ideas. The following are some of the reasons for food supply chain problems and processing environment challenges. The maximization of the profits relies on some farmers' vegetables and fruits with chemicals. Chemical fertilizers, insecticides, and other compounds are used in several plants and fruits. As a result, pesticide residues in vegetables and fruits become excessive. It is a significant health risk. Food gets contaminated with heavy metals. The irrigation water source of crops is polluted by the excessive intrusion of heavy metal elements such as lead, tin, mercury, and zinc, which are dangerous to human health. Food additives are used excessively in food processing. Some nefarious enterprises use excessive food additives, antibiotics, hormones, and harmful substances.

II. METHODOLOGY

1. Supplier:

For each product, it contains a barcode number and its number will be passed through food API then ingredients will be taken out by using the barcode number. First registration. The registration form contains supplier details. Then login. The supplier sells the products to all manufacturers what they produce.

2. Manufacturer:

The manufacturer initially creates the account. They will analyze the raw materials and the manufacturer will request the number of raw materials to the supplier. Then suppliers will accept the request from the manufacturer and raw materials will be added to the manufacturer's inventory. The manufacturer will send the product ID, expiry date, number of packets, etc to the blockchain and then the created product will be added to the manufacturer's shipment. From the blockchain, the manufacturer will retrieve the product.

3. Distributers:

In the First registration, the registration part contains distributor details. The distributor will be seeing the product in the manufacturer's cart and then buying the product by the distributor will be added to the blockchain.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12520

4. Consumer:

First Registration. The registration form contains user details. Then consumer login. Consumer buys the product from the distributor. The consumer scans the QR scan by using the mobile app and then views the product on the mobile such as manufacturing date, packing date, etc. The consumer will check the product and they will buy the product by using an online transaction. Finally, the user transaction ID, product name, and cost will be added to the blockchain.

5. Data Encryption:

IoT applications collect tons of data. Data retrieval and processing is an integral part of the whole IoT environment. Most of this data is personal and needs to be protected through encryption. Encryption is widely used on the internet to protect user information being sent between a browser and a server, including passwords, payment information, and other personal information that should be considered private. Organizations and individuals use encryption to protect sensitive data stored on computers, servers, and mobile devices like phones or tablets.

6. Data Authentication

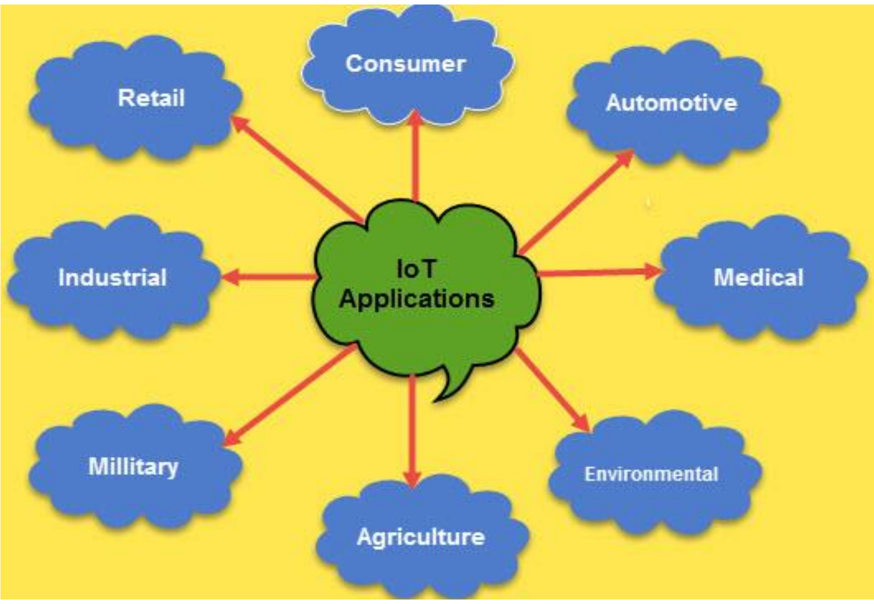
After successful encryption of data chances of the device itself being hacked still exist. If there is no way to establish the authenticity of the data being communicated to and from an IoT device, security is compromised. For instance, say you built a temperature sensor for smart homes. Even though you encrypt the data it transfers there is no way to authenticate the source of data then anyone can make up fake data and send it to your sensor instructing it to cool the room even when it's freezing or vice versa.

Healthcare:

IoT in healthcare aims to empower people to live healthier lives and regular checkups by wearing connected devices. The collected data will help in the personalized analysis of an individual's health and provide tailor-made strategies to combat illness.

Internet of things

The INTERNET of Things (IoT) has huge potential to impact the global food supply chain (FSC) by increasing productivity in terms of supply chain performance. Among many challenges, agri-food safety and its impact on the environment due to food wastage are of major concern. The United States Center for Diseases Control (CDC) estimates that 48 million people get sick from foodborne illness, 128000 are hospitalized, and 3000 die each year in the U.S. alone. Apart from illness, economically and criminally motivated food adulteration is also a growing concern due to globalization and wide-growing supply chain networks. Real-time monitoring of the food quality and visibility of that quality index would prevent outbreaks of food-borne illnesses, economically motivated adulteration, contamination, food wastage due to misconception of the labeled expiry dates, and losses due to spoilage, which have broad impacts on the food security. To improve safety and prevent wastage, modern IoT-based technologies are required to monitor the food quality and increase the visibility level of the monitored data. There are several IoT-based tracking and tracing infrastructures, such as electronic article surveillance (EAS), radio frequency identification (RFID), and QR codes which are primarily targeted for automatic package-level tracking



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⪤ Impact Factor 8.102 ⪤ Peer-reviewed / Refereed journal ⪤ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12520

Radio-frequency identification (RFID)

RFID uses electromagnetic fields to automatically identify and track tags attached to objects. An RFID system consists of a tiny radio transponder, a radio receiver, and a transmitter. When triggered by an electromagnetic interrogation pulse from a nearby RFID reader device, the tag transmits digital data, usually an identifying inventory number, back to the reader. This number can be used to track inventory goods. Passive tags are powered by energy from the RFID reader's interrogating radio waves. Active tags are powered by a battery and thus can be read at a greater range from the RFID reader, up to hundreds of meters. Unlike a barcode, the tag does not need to be within the reader's line of sight, so it may be embedded in the tracked object. RFID is one method of automatic identification and data capture (AIDC).

RFID tags are used in many industries. For example, an RFID tag attached to an automobile during production can be used to track its progress through the assembly line, RFID-tagged pharmaceuticals can be tracked through warehouses, and implanting RFID microchips in livestock and pets enables the identification of animals. Tags can also be used in shops to expedite checkout and prevent theft by customers and employees. Since RFID tags can be attached to physical money, clothing, and possessions, or implanted in animals and people, the possibility of reading personally-linked information without consent has raised serious privacy concerns. These concerns resulted in standard specifications development addressing privacy and security issues.

III. MODELING AND ANALYSIS

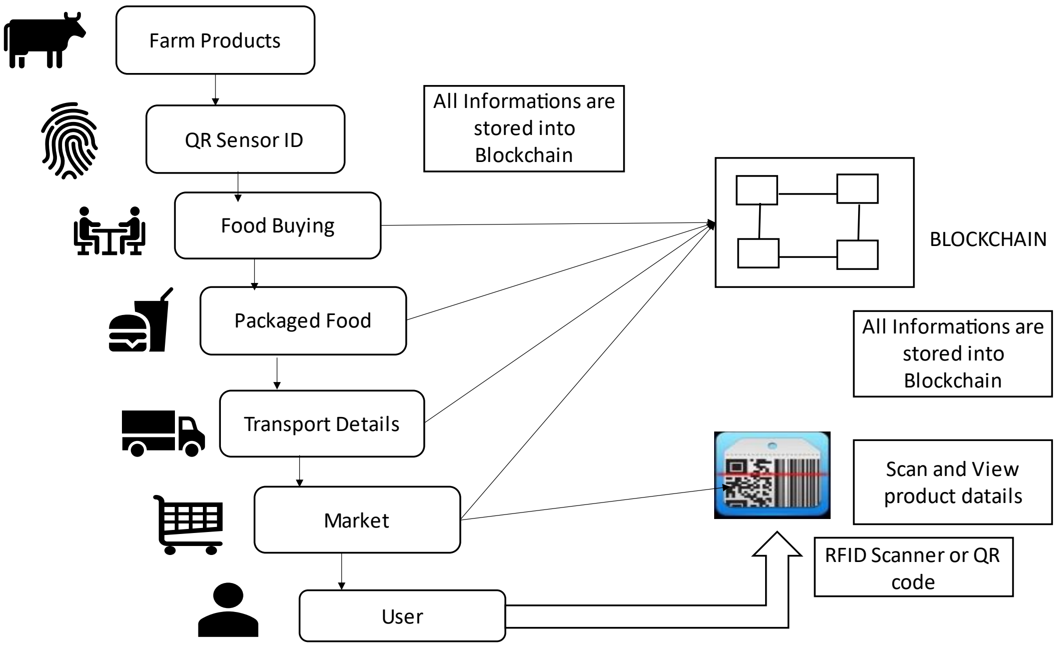


Figure 1:Architecture for Food Supply Chain Using Blockchain

The blockchain layer contains three particular blockchains, and the Agri-product information blockchain is the first. The user information blockchain is the second one. It has all the information about the network participants. The transaction information blockchain is the last one on the list. It holds a wealth of information, including user personal information, intermediate information, transactions, logistics, and agricultural product data.

Smart contracts are used in this paradigm. Those automated contracts use the highest level of data encryption currently available in the security industry. As a result, it will confirm the quality of the decision and guarantee clarity and effective communication between entities.

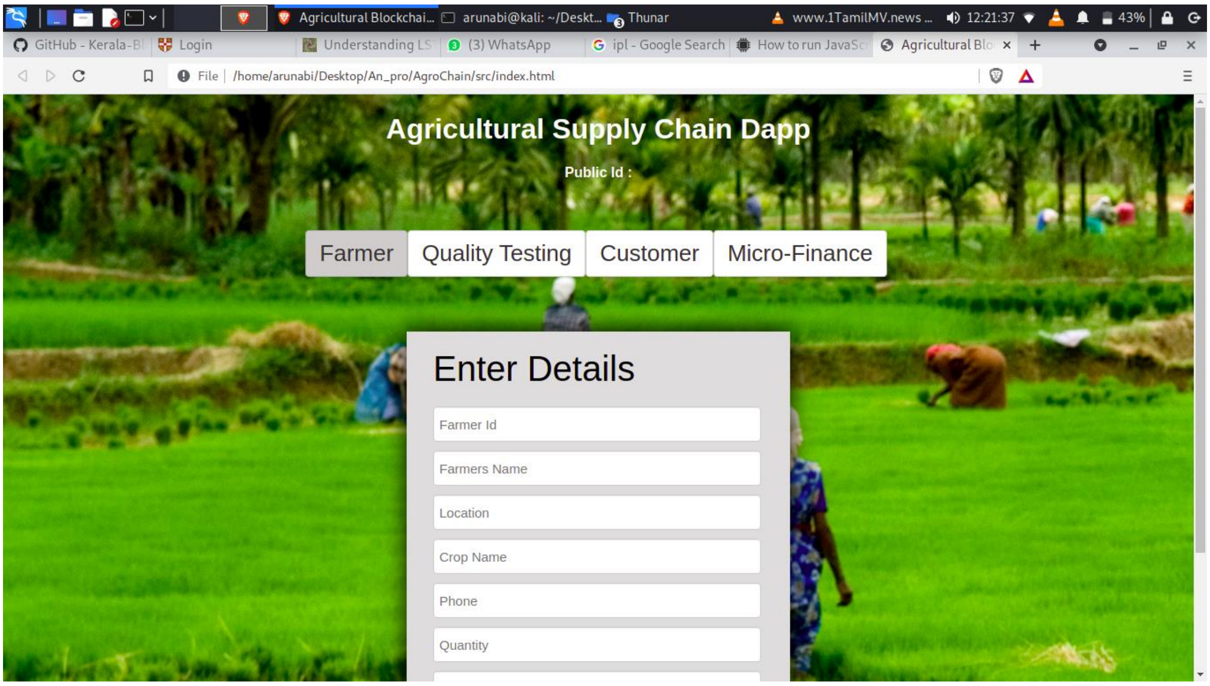
ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

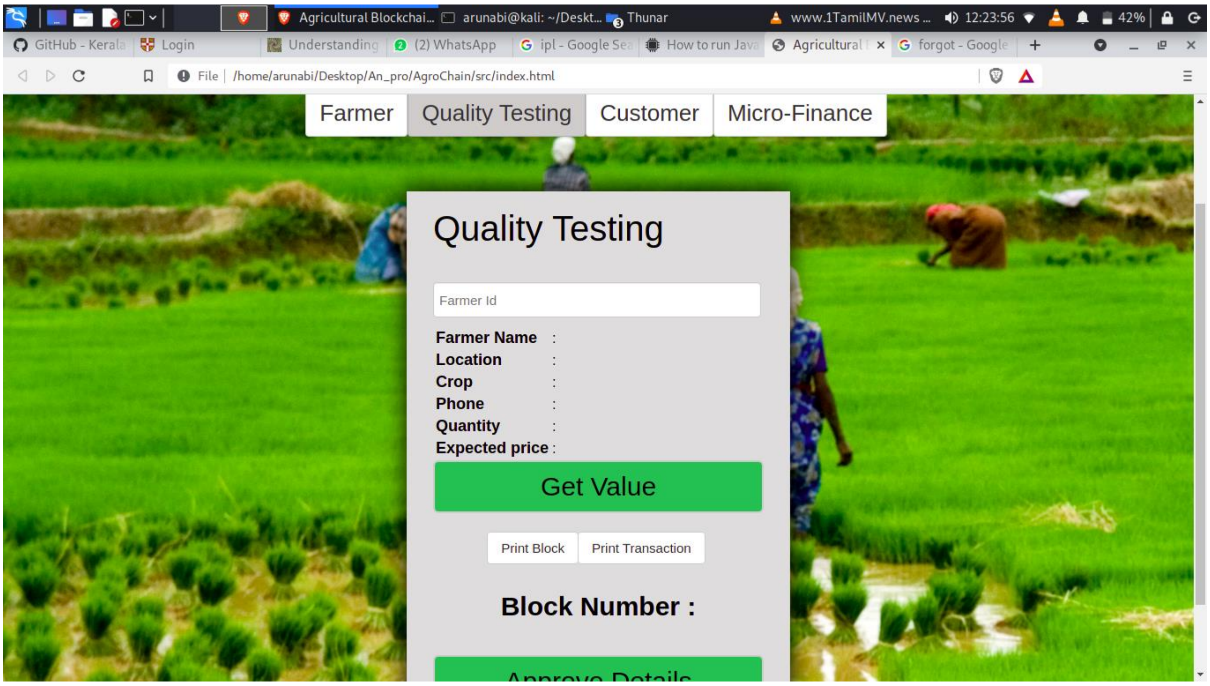
ISO 3297:2007 Certified ⁙ Impact Factor 8.102 ⁙ Peer-reviewed / Refereed journal ⁙ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12520

IV. RESULT AND DISCUSSION



The above figure shows the registration form for the farmer in the supply chain application. The entered details are stored directly onto the blockchain. The underlying technology uses Truffle for the deployment and go-Ethereum (geth) as the backend blockchain. We use the Web3 Java script provider API to interact with the blockchain.



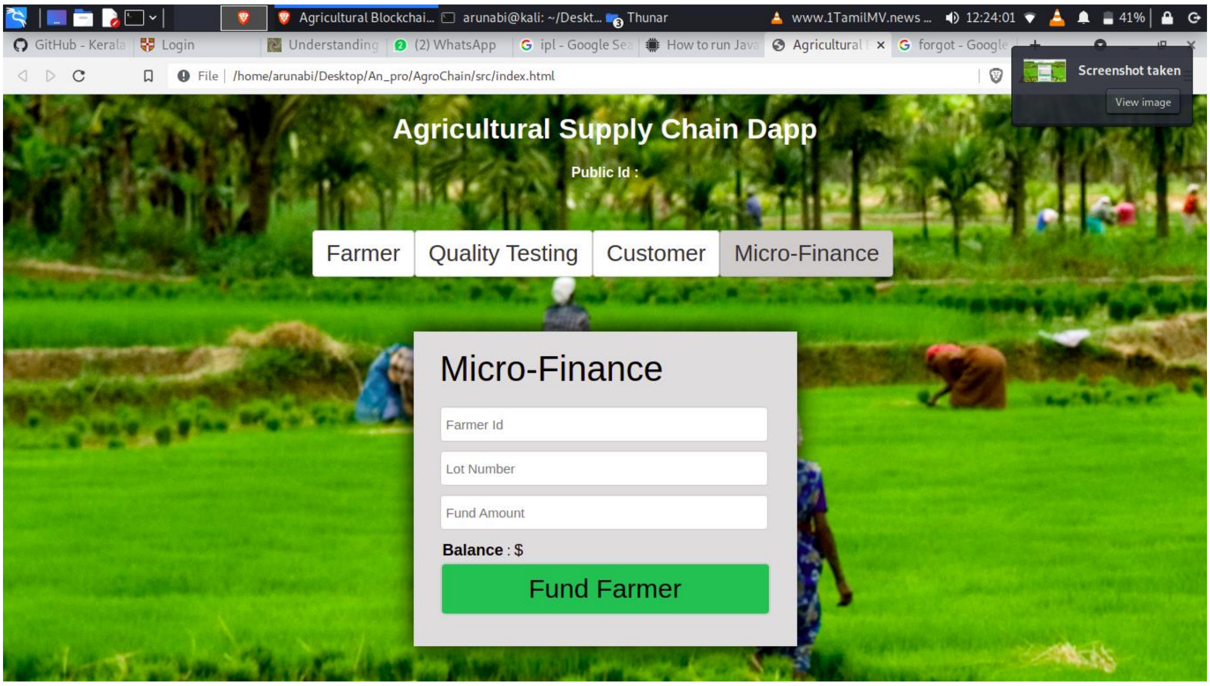
This is the Quality Testing page. Here we can see the block details where the farmer's details are stored on the ocblockchainThe 'Approve Details' will approve the details of the farmer.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12520



The micro-finance form enables any user to fund a farmer. The funding is done by providing the farmer's public id, the lot number of the product, and the amount.

V. CONCLUSION

The proposed blockchain reasonably increases, efficiency, transparency, and low cost for handling. In addition, blockchain adds the features like immutability and transparency, which disallows any fraudulent modifications to the data. The decentralized and permissionless blockchain system can deliver real-time information to all the parties such as the producer and consumer ecosystem on the safety status of food products at all times. In the future, this project will be used to avoid food and create a transparent food supply chain more successfully and efficiently.

REFERENCES

[1] D. I. Ellis *et al.*, "Fingerprinting food: Current technologies for the detection of food adulteration and contamination," *Chem. Soc. Rev.*, vol. 41, no. 17, pp. 5706–5727, 2012.
[2] S. Herschdoerfer, *Quality Control in the Food Industry*, vol. 2. Cambridge, MA, USA: Elsevier, 2012.
[3] J. Landt, "The history of RFID," *IEEE Potentials*, vol. 24, no. 4, pp. 8–11, Oct./Nov. 2005.
[4] R. Saltini and R. Akkerman, "Testing improvements in the chocolate traceability system: Impact on product recalls and production efficiency," *Food Control*, vol. 23, no. 1, pp. 221–226, 2012.
[5] W.-D. Huang *et al.*, "A passive radio-frequency pH-sensing tag for wireless food-quality monitoring," *IEEE Sensors J.*, vol. 12, no. 3, pp. 487–495, Mar. 2012.
[6] E. Smits *et al.*, "Development of printed RFID sensor tags for smart food packaging," in *Proc. 14th Int. Meeting Chem. Sensors*, Nuremberg, Germany, 2012, pp. 20–23.
[7] R. A. Potyrailo *et al.*, "Battery-free radio frequency identification (RFID) sensors for food quality and safety," *J. Agricult. Food Chem.*, vol. 60, no. 35, pp. 8535–8543, 2012.
[8] C. Amador, J.-P. Emond, and M. C. D. N. Nunes, "Application of RFID technologies in the temperature mapping of the pineapple supply chain," *Sens. Instrum. Food Qual. Safety*, vol. 3, no. 1, pp. 26–33, 2009.
[9] J. Virtanen, L. Ukkonen, T. Björninen, and L. Sydänheimo, "Printed humidity sensor for UHF RFID systems," in *Proc. IEEE Sens. Appl. Symp. (SAS)*, 2010, pp. 269–272.
[10] K.-H. Eom, K.-H. Hyun, S. Lin, and J.-W. Kim, "The meat freshness monitoring system using the smart RFID tag," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 7, 2014, Art. no. 591812.
[11] K. H. Eom, M. C. Kim, S. Lee, and C. W. Lee, "The vegetable freshness monitoring system using RFID with oxygen and carbon dioxide sensor," *Int. J. Distrib. Sensor Netw.*, vol. 8, no. 6, 2012, Art. no. 472986.
[12] S. Apte and N. Petrovsky, "Will blockchain technology revolutionize excipient supply chain management?" *J. Excipients Food Chem.*, vol. 7, no. 3, pp. 76–78, 2016.
[13] S. Underwood, "Blockchain beyond Bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⪤ Impact Factor 8.102 ⪤ Peer-reviewed / Refereed journal ⪤ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12520

[14] Z. Pang, Q. Chen, W. Han, and L. Zheng, "Value-centric design of the Internet-of-Things solution for food supply chain: Value creation, sensor portfolio, and information fusion," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 289–319, 2015.

[15] S. Piramuthu and W. Zhou, *RFID and Sensor Network Automation in the Food Industry: Ensuring Quality and Safety Through Supply Chain Visibility*. Chichester, U.K.: Wiley, 2016.

[16] C. Costa *et al.*, "A review on agri-food supply chain traceability using RFID technology," *Food Bioprocess Technol.*, vol. 6, no. 2, pp. 353–366, 2013.

[17] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.

[18] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst Appl. (AICCSA)*, 2016, pp. 1–6.

[19] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proc. IEEE 13th Int. Conf. Service Syst. Service Manag. (ICSSSM)*, 2016, pp. 1–6.

[20] F. Tian, "A supply chain traceability system for food safety based on HACCP, Blockchain & Internet of Things," in *Proc. Int. Conf. Service Syst. Service Manag. (ICSSSM)*, 2017, pp. 1–6.

[21] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," in *Proc. ISSC/CIICT*, 2014, pp. 280–285.

[22] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Proc. Annu. Int. Cryptol. Conf.*, 1992, pp. 139–147.

[23] V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer, "KARMA: A secure economic framework for peer-to-peer resource sharing," in *Proc. Workshop Econ. Peer-to-Peer Syst.*, vol. 35, no. 6, 2003, pp. 1–6.

[24] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Working Paper, 2008.

[25] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," White Paper, 2014.

[26] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proc. Annu. Int. Cryptol. Conf.*, 2017, pp. 357–388.

[27] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Cham, Switzerland: Springer, 2017, pp. 297–315.

[28] J. F. Salmerón *et al.*, "Design and development of sensing RFID Tags on flexible foil compatible with EPC Gen 2," *IEEE Sensors J.*, vol. 14, no. 12, pp. 4361–4371, Dec. 2014.

[29] K. Mizuno and M. Shimizu, "Transportation quality monitor using sensor active RFID," in *Proc. IEEE Int. Symp. Appl. Internet Workshops*, 2007, p. 19.

[30] M. S. Khan, M. S. Islam, and H. Deng, "Design of a reconfigurable RFID sensing tag as a generic sensing platform toward the future Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 300–310, Aug. 2014.

[31] S. Gueron, S. Johnson, and J. Walker, "Sha-512/256," in *Proc. IEEE 8th Int. Conf. Inf. Technol. New Gener. (ITNG)*, 2011, pp. 354–358.

[32] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Security Appl.*, vol. 38, pp. 8–27, Feb. 2018.

[33] X. Lu, Q. Li, Z. Qu, and P. Hui, "Privacy information security classification study in the Internet of Things," in *Proc. IEEE Int. Conf. Identification Inf. Knowl. Internet Things (IIKI)*, 2014, pp. 162–165.SS