Food Traceability and Prevention of Location Fraud using Blockchain

1st Kar Seng Loke
Research Section
Grassroots Lab
Kuala Lumpur, Malaysia
https://orcid.org/0000-0001-7871-6322

2nd Ong Chin Ann
School of Engineering & Technology
PSB Academy
Singapore, Singapore
https://orcid.org/0000-0003-0335-9011

Abstract—**Food traceability has gained widespread prominence in recent years due to the widely reported food fraud and safety issues and there is a need for a simple low-cost solution. Adopting the design science research methodology, we proposed a design-based set of practical criteria for food tracking system that includes the prevention of location data input fraud. The design was successfully implemented on a blockchain as food tracking system. Based on our evaluation, the design and prototype demonstrate a viable approach to food tracking and limiting food fraud.**

Keywords—blockchain, food traceability, food provenance, food safety, food fraud

I. Introduction

Food mobility and global trade has brought different varieties of food products to different ends of the world providing unprecedented choice to consumers. However, this leads to longer and complex production chains that is less responsive to food safety issues including food contamination, disease propagation, food fraud and food authenticity related problems. This list of food safety related incidents include E. coli outbreak in Germany [1], horsemeat incident in Europe [2], egg contamination [3] and so on. The Grocery Manufacturers Association (US) reported 18% of food companies lost between $30 million and $99 million due to recall and lost sales [4]. 47% of recall are due to microbiological contamination and 26% are for labelling issues. They also report that food fraud cost the global food industry $10-15 billion a year, affecting about 10% of food sold [5].

Long supply chains face challenges in keeping the integrity and authenticity of the product because of the possibility of switching or substitution to occur in the long supply line. However, if there are better guarantees of authenticity, then the question of long or short supply chain is irrelevant. Many consumers nowadays are seeking traceable products that are safe and authentic from ethically responsible food producers and businesses. Traceability addresses some of the issues related to food authenticity. The idea is that if the food products can be traced to its source and every transfer point is reasonably secure, then the food authenticity on the supply chain can be reliably assured than without traceability. We wish to address some of these issues with a proof of concept implementation of traceability on the blockchain.

The contribution of this work is the development and instantiation of a blockchain tracking system with fraud prevention, i.e. we do not assume that any data that is incorporated into the block chain is necessarily trustworthy. In particular:

1. We created the design for traceability based on the requirements from literature review and our experience on blockchain implementation
2. We created an artifact implementation proof for analysis. The implementation incorporated the Android mobile system, authentication system and blockchain.
3. We have developed an implementation proof of a location fraud system build on top of the blockchain. Our system incorporated a cryptographic system to prevent fraudulent location input to the blockchain. A working description is also provided for further analysis and reference.
4. We have evaluated our system based on our design goals.

II. Blockchain Systems in Supply Chain

A. Brief Review

Blockchain is a public technological system that can be used for mediating trust through peer to peer distribution of cryptographically secured electronic records named as “blocks”. It provides a consensus mechanism by through public history of transactions that is impractical to undo. Once the transaction is recorded into the system, it is not possible to reverse out the record without undoing all the previous records because all records are cryptographically linked or “chained” [6].

Blockchain applications have the potential for breakthrough in supply chains especially in terms of visibility and optimization by being able to identify counterfeit products, provenance and reducing paper processing [7]. In a review [8], fraud prevention, integrity verification has been identified for use in provenance. However, most of the reviewed applications are proposals and few are working implementations. Hackius et al [9] found in their survey that despite many proposed use cases, middle managers are wary about data security on the blockchain. They feel that is its overhyped and lack technical maturity. Tribis et al [10] in their review identified trust and decentralization as key blockchain technology characteristics. They also list real-time traceability as one of the benefits of blockchain technology. Kshetri [11] reviewed eleven supply chain applications include some of those discussed below. Details of implementation of those applications are hard to come by as most are referenced from blog posts and press releases. It was indicated that businesses that face counterfeiting risks are more likely to adopt blockchain in the supply chain. They also believed that

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

blockchain has the potential to end unethical practices and can help in food authenticity.

Shipping giant Maersk and IBM [12] have announced a joint venture to explore the use of blockchain for conducting global trade. An initial proof of concept was conducted in September 2016 [13] tracking a container of flowers from Kenya to Netherlands. Provenance [14] , a UK startup, together with non-governmental organizations International Pole and Line Foundation and Humanity United, conducted a 6-month pilot using the Ethereum blockchain [15] and RFID (radio frequency ID) tagging to track Tuna fish in Indonesia In October 2016, Walmart, together with IBM and Tsinghua University conducted tests with blockchain technology to develop food safety and traceability protocols [16]. Chinese pork and US mangoes were tracked by digital scanning from the farms to Walmart shelves. They reported that tracing food origins took 2.2 seconds on the blockchain. It is not apparent how the systems would function if deliberate fraud was induced in the system, for example, entering false or misleading information into the system. Hang et al [17] discussed the use of IOT and agricultural insurance in addition to provenance. The lack of integration with supply chain systems is mentioned as one of the limitations. Motta et al [17], in their review mentioned that Blockchain is still not matured yet.

B. *Benefits*

One of the advantages of using the blockchain is the cost savings [11]. Since the open source blockchain is open to public use, there is no infrastructure cost. And since the blockchain network is self-maintaining, management overheads are shared [7]. The blockchain has the potential to benefit the supply chain with cost savings, efficiency gains and reduced data reconciliation [17]. Chang et al [18] listed out some of the desirable features of blockchain for traceability. They include open data where the public can search for information on the blockchain. The blockchain system is also decentralized in the sense that there is no one party controlling the data entry. The data is tamper-resistant once recorded on the blockchain. This makes the traceability data once recorded to be accurate. However, this is only the case if the data can be checked for validity. In our design we will consider some techniques to make it more difficult for falsify data entry.

III. Design Criteria

The proposed system has following design criteria:

1. Low cost – The cost is kept low by using existing technology and software. There is no need to reinvent the wheel. This criterion is provided by the open source blockchain technology.

2. Publicly accessible – The traceability information should be open to public. This benefit is accorded by the public blockchain technology

3. Loose coupling – there is no tie up with any existing logistics or supply chain systems. There is also no requirement for any system to be in place. It should exists independently of any supply chain systems.

4. Simple light weight system to spur initial adoption. One of the mentioned gaps for adoption is the high degree of computerization requirement [10].

5. Simple to use – It should not be complicated to use. There should be minimal data entry so that operation time is not increased. All functions should be automated as much as possible; a simple demonstration should suffice for any user to start using the system.

6. Location fraud prevention – There must be mechanism in place to prevent or minimize data entry fraud. This will be elaborated in the next section. We elaborate on how traceability can be incorporated into the system.

7. Cryptographic key management system that aids fraud prevention. This will be discussed in the following section.

IV. System Design and Implementation

The blockchain was first discussed by Nakamoto [6] in 2008, even though it was not called such then. In the paper, it was described as a distributed timestamp server on a peer to peer basis through the use of proof-of-work. The blockchain is meant as a way to prevent double spending by keeping track of all spending in verifiable and transparent manner. The design of the blocks is such that it cannot be changed without undoing all the work on all previous blocks. The blockchain as a distributed ledger provides a system in which all participants can agree on a single history of the events in the order they occurred. The blockchain then is a trustless distributed system for tracking spending events. This functionality also makes it a good fit for use in tracking distribution of goods and products.

Our implementation uses the Nxt blockchain[1]. Nxt is an open source blockchain platform written on the Java platform. It has many advanced decentralized core features such creating digital assets, creating a decentralized marketplace or conducting a poll, and so on. The Nxt platform has a powerful and simple to use API system that allows new applications to be built on top of it. Queries and requests on the Nxt are done by REST based http microservices.

For prevention of location fraud, at each of the supply chain location, we place on location a physically secure computer (SC); by which we mean that the physical access to the machine is secure. The machine is also immobilized so that it can't be moved. This machine is not internet connected but will have a local area wireless connection. This machine serves multiple purposes. This machine holds a cryptographic private key that is not accessible to the produce owners or supply chain operators. This private key together with the public key is generated randomly during the installation process. This public key for each location will be uploaded to a separated internet-connected server. Secondly this machine also generates scannable QR codes.

At the source of the produce, i.e. farms, this secure computer SC generates two types of QR codes. The first QR code, the product QR code, is the code (QR-Prod) that is for attaching to the produce packaging. This code contains the produce identification and the produce NXT blockchain account number. The second QR code (QR-Trans) stores the transaction NXT account number. These QR codes are

[1] https://nxtplatform.org/what-is-nxt/

scanned by android apps. There two different apps one for supply chain operators and the other for consumers. The consumer app (App-C) is used by consumers for tracking produce by scanning the QR-Prod code. The supply chain operators' app (App-S) are used to update the blockchain on the movement of the produce. In additional, there is another publicly accessible server PS that stores all the public key certificates for all SC local servers.

We now describe the sequence of operations (Fig. 1 and Fig. 2). From the source farm where the produce originates, we need to generate the QR-Prod that tags the produce. This is generated by the SC at the farm after keying the produce information including description, type, weight (volume, etc.) and batch identification. The QR code is then attached to the produce packaging. When the produce is ready to be shipped out to another location (such as warehouse, distribution center, wholesaler, etc.), the operator generates a QR-Trans code. This code also contains the produce identification code. The operator scans the QR-Prod and QR-Trans with the App-S, which then updates the Nxt blockchain with the location, date, time and identification. However, this information needs to be secured so only the operator at the location can perform the update so that the information can't be spoofed. We will discuss this separately in the Blockchain Update section.

When the produce reaches the new destination, the next operator in the chain, will similarly obtain a QR-Trans code from the SC at the location. Upon arrival, the operator scans the QR-Prod on the produce, then the QR-Trans to affect the transaction to the blockchain. When the produce is ready to ship out, a new QR-Trans is generated and scanned with the produce QR-Prod. This step is repeated until it reaches the end of the supply chain, i.e. the retail shop or supermarket. At the retail end or supermarket, the consumer can use the App-C to obtain the supply chain trace of the produce by scanning the QR-Prod on the packaging.

A. Updating the Blockchain

Each of the supply chain nodes (or location) has a secure computer SC that holds the public key certificate that is unique to each location. The SC generates a new Nxt-Prod account at the origin of the produce which is embedded in all produce tags. The SC also obtains the Nxt-Trans account that is unique for each location. This Nxt-Trans account is required for blockchain update and a small fee is charged for each update. The first half of the payload for the Nxt-Trans includes the produce identification, description, type, etc. coupled with location and date-time information. The message digest is first generated from the data payload. This message digest is then encrypted with the private key of the SC. This encrypted message digest forms the second half of the payload to be uploaded to the blockchain. This blockchain message is sent from Nxt-Trans local account to the Nxt-Prod account using the SendMessage application programming interface (API) call using the App-S Android app (Figure 2).

The corresponding Android app App-C will scan the QR-Prod code that contains the Nxt-Prod account (Figure 1). The app will query the Nxt-Prod account and retrieve the message stored in the blockchain. The first half of the message is the clear text information and the second half the encrypted message digest. Based on the information from the clear text the app will query the FoodChain public information server to retrieve the public key of the supply chain location mentioned in the clear text. The app will decrypt the message digest using the public key and verify that the message digest is corresponding to the clear text. The app will then display the list of supply chain routes for the produce.

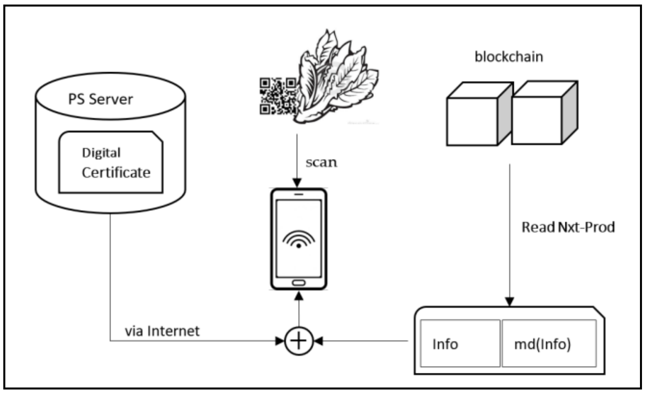

Fig. 1. Consumer scanning app for supply chain routes on the blockchain..

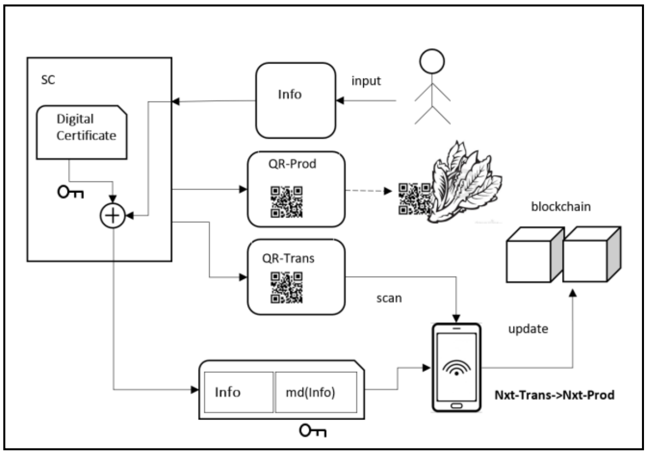

Fig. 2. Updating the Nxt Blockchain with product information at the supply chain locations.

B. Implementation

The SC computer is a standard computer with local wi-fi access for local area network connected. It is not connected to the Internet. The SC computer must be physically fixed to the location and should be secure from unauthorized physical access (Figure 2). The software on it is XAMPP distribution software for the Apache HTTP server with mariaDB, PhP and Perl with Javascript on the front end. There is a data entry front end for keying the produce information from which the QR-Prod code is generated. The SC front end also generates QR-Trans for scanning which is scanned when the produce changes location to be updated to the blockchain.

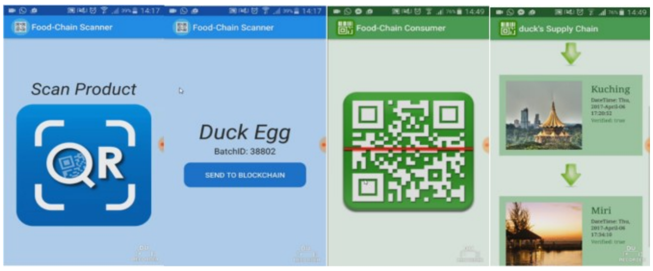

Fig. 3. The supply chain scanner app on Android with sample screen shot (left). The consumer scanner app with sample display of the tracking (right)

Separately there is a custom coded Java server for calculating the message digest and encrypting the message digest before sending it to the Android App-S for upload (Fig. 1). The Android app App-S and App-C are shown in fig. 3. The complete demo is available on YouTube. The design was successfully implemented and demonstrated that singular products can be tracked on the blockchain.

V. Evaluation

We consider some of the common usage scenario of the system, including deliberate abuse of the system. In normal usage, a tag or QR code would be generated at the origin or farm (Fig. 4). This is the QR-Prod that stores the details of the product and is affixed to the packaging. At other locations the QR-Trans is generated for uploading to the blockchain. This code need not be fixed to the product and can be scanned of the screen. If any of the QR-Trans is missing, then the blockchain would have an incomplete record and the supply chain trace would be broken. The QR labels also can't be forged easily because they are generated by a physically secure computer SC with a locked in private keys. We could have a case whereby a merchant trying to claim the origin of a product by affixing a QR-Prod in the middle of the supply chain (Fig. 5, Case 1 and Case 2). However, it needs to have the QR-Trans to upload the location but since the vendor can't alter the location in the QR, he can't claim a different origin. The QR-Prod also can't be re-used because it has a timestamp in it. Suppose now the produce originator duplicates the product QR-Prod and affixed it multiple products using the same code (Fig. 5, Case 3). This will cause confusion because the same batch-id would be used in the blockchain. This would not be advantageous to the primary or original producer. We assume that the primary producer is sincere and trustworthy because making fraudulent claims would not help the sales of the produce.

In another scenario, the middleman duplicates a QR-Prod and affix it to a produce from a different source of origin (Fig. 5, Case 4). A double transaction would have been created for the product where the QR-Prod was duplicated. This could be detected by the blockchain tracking software easily.

Instead of duplicating the QR-Prod, the label could be transferred and fraudulently affixed on another product (Fig. 6, Case 5). Now we a batch of genuine produce and a batch of fraudulently labelled produce. The re-seller (or distributor) would have more quantity (including the dubious items) to sell than he had received from the genuine source. He would have to convince buyers why some are tracked, and some are not, and may get away with it in isolated markets. In the long run this may not be sustainable maintaining the deception.

This implementation is a loosely coupled system. It is a separate traceability system that can be built without the need of an existing supply chain system, and it can be operate separately or jointly without interference or integration to any existing system. It is also simple to use. The tracking abilities are based on mobile QR code scanning. Its operation should be easy to learn without further training apart from an initial demonstration of use. The use of Android mobile system is familiar to many non-technical users. It is publicly accessible as the tracking information are updated and secured in a public blockchain. We have shown that the blockchain based traceability can be successfully accessible to consumers using only an app on their mobile phones.

The system is low cost and cheap to install and use. The system that was implemented are all based on open-source system and not commercial tool set. Therefore, the cost is free in terms of software systems. The hardware system is standard issue therefore the cost is also minimal. However, a full commercial system will need more robust hardware especially for the SC computer that needs to be physically secured.

We have implemented also fraud prevention system by cryptographically encrypting data on the blockchain so that false data can be detected. The implemented system prevents false location information from being updated to the blockchain.

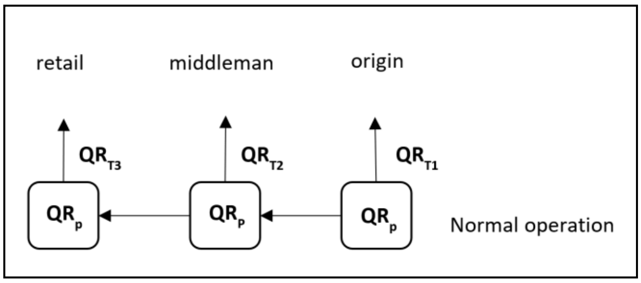

Fig. 4. Normal operation of FoodChain

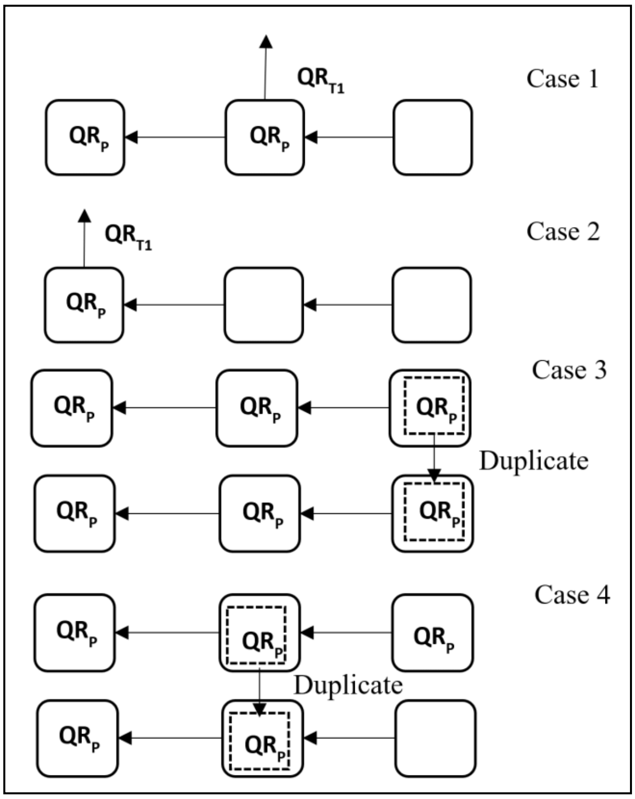

Fig. 5. Improper usage case1-4

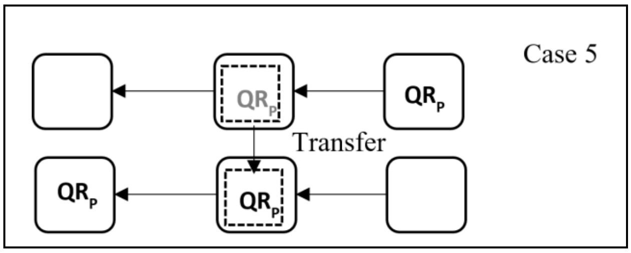

Fig. 6. Improper usage case 5

VI. CONCLUSION

We have successfully demonstrated a blockchain based food traceability system with location fraud prevention. Many systems seem to accept data input integrity as a given. We think this is the weak point of any blockchain system. The blockchain data may be immutable but if the data input is fraud driven and inconsistent, it will only serve to demolish any trust on it.

Our other motivation was to investigate the implementation of a loosely coupled system on the blockchain with the view for future commercialization. As a proof of concept this prototype was implemented successfully. Since this is a prototype, further issues need to be considered before the system can be commercially viable.

Some of the issues include the scalability and robustness that the that the blockchain system can support and the transaction rate when processing high volume updates. We also need to benchmark and study the additional time added to their normal processing time when using this system. Currently the system can only be used for single products. The system can’t track products that are a combination or amalgamation of other items from separate supply lines, nor can it track items that products that can be split up or dissociated or pull apart. In the future we can incorporate other fraud prevention approach such as using machine learning to signal any out of the ordinary supply flow such as deviation in the normal routes, abnormal time delay between routes, or mismatch in volume or weight in the supply chain.

VII. REFERENCES

[1] European Food Safety Authority, "E.coli: Rapid response in a crisis," 11 July 2012. [Online]. Available: http://www.efsa.europa.eu/en/press/news/120711. [Accessed 10 January 2018].

[2] Department of Agriculture, Food and the Marine, "Equine DNA & Mislabelling of Processed Beef Investigation Report (Mar 2013)," March 2013. [Online]. Available: http://www.agriculture.gov.ie/media/migration/publications/2013/EquineDNAreportMarch2013190313.pdf. [Accessed 10 January 2018].

[3] Vytenis Andriukaitis, ""FIPRONIL SCANDAL: HOW TO IMPROVE THE EU RAPID ALERT SYSTEM FOR FOOD AND FEED" - STRASBOURG - TUESDAY 12 SEPTEMBER 2017," 12 September 2017. [Online]. Available: https://ec.europa.eu/commission/commissioners/2014-2019/andriukaitis/announcements/fipronil-scandal-how-improve-eu-rapid-alert-system-food-and-feed-strasbourg-tuesday-12-september_en. [Accessed 10 January 2018].

[4] B. Kowitt, "Food Contamination Costs the Food Industry $55.5 Billion," Fortune, 2016.

[5] R. Johnson, "Food Fraud and "Economically Motivated Adulteration" of Food and Food Ingredients," Congressional Research Service , 2014.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system.," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[7] F. Casino, T. K. Dasaklis and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics,* vol. 36, pp. 55-81, 2019.

[8] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda and V. Santamaria, "To Blockchain or Not to Blockchain: That Is the Question," *IT Professional,* pp. 62-74, 2018.

[9] N. Hackius and P. Moritz, "Blockchain in Logistics and Supply Chain: Trick or Treat?," in *Proceedings of the Hamburg International Conference of Logistics* , Hamburg, 2017.

[10] Y. Tribis, A. El Bouchti and H. Bouayad, "Supply Chain Management based on Blockchain: A Systematic Mapping Study," in *International Workshop on Transportation and Supply Chain Engineering*, Rabat, Morocco, 2018.

[11] N. Kshetri, "Blockchain's roles in meeting key supply chain management objectives," *International Journal of Information Management,* vol. 39, pp. 80-89, 2018.

[12] Maersk, "Maersk and IBM to form joint venture applying blockchain to improve global trade and digitise supply chains," 15 January 2018. [Online]. Available: https://www.maersk.com/press/press-release-archive/maersk-and-ibm-to-form-joint-venture. [Accessed 15 May 2018].

[13] T. Groenfeldt, "IBM and maersk apply blockchain to container shipping.," *Forbes,* 2017.

[14] Provenance, "From shore to plate: Tracking tuna on the blockchain," 15 July 2016. [Online]. Available: https://www.provenance.org/tracking-tuna-on-the-blockchain. [Accessed 16 May 2018].

[15] D. Cummings, "Blockchains are Changing the Food Industry," 26 November 2016. [Online]. Available: https://www.ethnews.com/blockchains-are-changing-the-food-industry. [Accessed 17 May 2018].

[16] J. Nation, "Walmart Tests Food Safety With Blockchain Traceability," 2 June 2017. [Online]. Available: https://www.ethnews.com/walmart-tests-food-safety-with-blockchain-traceability. [Accessed 17 May 2018].

[17] X. Hang, D. Tobias, W. Puqing and H. Jiajin, "Blockchain Technology for Agriculture: Applications and Rationale," *Frontiers in Blockchain,* vol. 3, 2020.

[18] G. A. Motta, B. Tekinerdogan and I. Athanasiadis, "Blockchain Applications in the Agri-Food Domain: The First Wave," *Frontiers in Blockchain,* vol. 3, 2020.

[19] Accenture, "Tracing the Supply Chain: How blockchain can enable traceability in the food industry," Accenture, 2018.

[20] P.-Y. Chang, M.-S. Hwang and C.-C. Yang, "A Blockchain-Based Traceable Certification System," in *International Conference on Security with Intelligent Computing and Big-data Services (SICBS’17)*, Taiwan, 2018.