Blockchain

Subjects: Agriculture, Dairy & Animal Science
Contributor: Konstantinos Demestichas

This entry provides an overview of the application of blockchain technologies for enabling traceability in the agri-food domain. It presents relevant definitions and the various types of blockchain solutions used in "farm to fork" traceability, including public vs private blockchain networks, consensus protocols and smart contracts.

Keywords: traceability ; from farm to fork ; distributed ledger ; blockchain ; supply chain

Nowadays, traceability systems address a range of issues, including food fraud, food security and withdrawal, compliance with regulations, societal issues and consumer awareness [1]. In addition to societal and consumer benefits, tracing and tracking products can lead to increased value of business assets and to increased profit through costs reduction in the long term.

1. Overview and Definitions

Some groundwork for what we nowadays refer to as “blockchain” was performed by Stuart Haber and W. Scott Stornetta in 1991, in their article entitled “How to Time-Stamp a Digital Document” [2], while the popular paper by Satoshi Nakamoto in 2008 [3] established bitcoin as a cryptocurrency and devised the first blockchain database. According to Mayank Raikwar et al., a very general definition of blockchain is: “Blockchain is a distributed ledger maintaining a continuously growing list of data records that are confirmed by all of the participating nodes” [4].

A block is a record that includes data inside it, as well as a value with the previous block’s hash and, finally, a value that represents its own hash. The hash stands for the digital fingerprint of an amount of data of the block. The link between the hash of the current block and the hash of the previous block explains the meaning of the cryptographically linked chain of blocks through these hashes. If anyone tampers with the data, this digital fingerprint will be changed and finally the chain will be invalid. There are many more concepts around blockchain, such as mining, distributed peer-to-peer network protocols, consensus ledgers, cryptographic hashes, etc.

The “fingerprint” attribute represents the unique identifier of every block and is one of the core principles in the blockchain architecture. A commonly used algorithm for cryptography implementation on any digital data source is the well-known SHA256 hash, which was developed by the National Security Agency (NSA). SHA stands for secure hash algorithm and ‘256’ is the number of bits it takes up in memory. There are five basic requirements that SHA256 satisfies:

- One-Way decryption algorithm;
- Deterministic (meaning that it will produce the same result each time the same input is used);
- Fast computation;
- Avalanche Effect;
- Withstanding collisions [5].

The reason for using a hashing algorithm is because reverse engineering techniques are not practical. Thus, the importance of the use of the SHA256 algorithm lies on the fact that any attempt or effort to crack it is not realistically possible, due to its inherent characteristics (hashing is a one-way function).

Blockchain is also an immutable digital ledger, meaning that if anyone tries to tamper or corrupt the data of a specific block, thus changing the hash of this block, this results in a cryptographic link disruption, due to the usage of different hash(es) between the linked blocks of the chain. Because of the change in a chain’s block, all the blocks after that will no longer be valid, which means that it will no longer be connected to the chain. Therefore, from the moment data have entered into the blockchain, they cannot be altered, as all the entries following the tampered block of the chain need to be

altered as well. Because of this fundamental structure, it is practically impossible to change a single block in the chain, especially as more and more components are added. It has to be noted that any digital ledger (blockchain on this occasion) is as reliable as the organization that maintains it [6].

In case one or many blocks of the chain are maliciously changed, or a system error occurs in the process of data input, the cryptographic link will be broken and this will cause a data re-storage problem. This problem is solved through the deployment of distributed peer to peer (P2P) networks, which are one of the key components of blockchain technology and offer a significant enhancement of data storage technology compared to traditional centralized models. A P2P distributed network consists of a great number of computers (nodes) where every device is interconnected (locally, wirelessly or by a cable); ideally the more the nodes connect the better it is. The actual approach of how this type of distributed network is used can affect the whole blockchain scenario.

A P2P network stores and transfers data between the clients (or nodes) of the network without the need for a central point of storage (central server), so the data are less vulnerable to being hacked or lost. In a blockchain P2P network, the blocks of the chain can actually be copied across all the existing computers of the network (thousands or millions of computers) through the usage of the appropriate cryptographic key across all the peers. As time passes, the blockchain grows and the system becomes more and more complex. If someone attempts any malicious alteration on one or more blocks of the chain, they have to control, attack or manipulate at least 50% of the network's peers or more in order to break the blockchain, otherwise the other peers of the network will immediately realize the difference and will alert the whole network by sending a signal to replace the broken one. In this way, distributed P2P networks add an extra level of security on the existing cryptographic hash, which is a one-level security schema. In a consensus protocol, the more layers of security used, the stronger and safer the blockchain is made [7].

Every block that composes the blockchain contains at least four fields, namely:

- The number of the block;
- The stored data (or stored transactions);
- The hash of the previous block;
- The hash of the current block.

Another field in the block is called nonce (number used only once) and relates to the meaning of "mining". The hash of every block is dictated by four components, i.e., block number, the previous hash, the stored data, and the nonce, and is generated by providing these as input to the SHA256 hashing algorithm. The block number, the previous hash, which is linked directly to contents of the previous block, as well as the stored data, cannot be changed because this would essentially mean that data tampering is attempted. Nonce provides additional control and flexibility that makes defining the correct hash value (one that meets certain requirements) possible, without the need to change any of the other components. In Proof of Work systems like blockchains, miners must find (by using brute force and significant computational power) a nonce value that, when plugged into the hashing algorithm, generates an output that meets specific requirements (e.g., a certain number of leading zeros).

Hence, mining can be perceived as the process of creating a new block for the blockchain and enriching it with a number of transactions. The mining difficulty indicator is the number that suggests the work intensity that a node's computer has to perform in order to create a new block. In the bitcoin blockchain, this is not a constant number but is automatically adjusted every 2016 blocks. Normally, the creation of this number of blocks should take exactly two weeks. In this period, if more blocks need to be created, the mining difficulty is increased, otherwise it is reduced. For the blockchain, this means that if more miners try to solve the cryptographic puzzle in a shorter timeframe, the system should increase the difficulty in order to maintain it. In an opposite situation (a lot of users may stop mining), the difficulty has to be reduced. In other words, the difficulty adjustment ensures that the mining process is performed for a specific amount of time, no matter how many users are mining or how fast the hardware is. One important disadvantage of this is that it tends to lead to centralization.

Decentralized applications (Dapps) on the blockchain are interfaces enabling people to connect and interact with many components of it. They are applications that can exist as decentralized programs that can run and can be stored on the peers' computers in the blockchain network rather than in a centralized server. The core visionary idea is to build a global

super-computer in a distributed manner, which will be facilitated through a blockchain where everything (programs, transactions) will be recorded, tracked and stored in an immutable manner. Simultaneously, a copy of that blockchain application will reside with the clients.

2. Ethereum and Smart Contracts

Ethereum is a project platform that was created in 2013 by Vitalik Buterin. Essentially, the idea behind the Ethereum protocol is that all peers of a network are interconnected. Blockchain technology not only allows one to store transactional data but also to store and facilitate programs, as well as execute them, enabling any application to be decentralized [8]. The article of Vitalik Buterin, the founder of Ethereum, referred to the meaning of decentralization and presented the three different levels of the (de)centralization:

- Logical (de)centralization;
- Political (de)centralization;
- Architectural (de)centralization [7].

Even today, many applications use the certification access mechanism which does not provide full visibility to the peers of the network. In order to address the aforementioned problem, in applications such as product supply chains, an environment that facilitates “smart contracts” is a promising approach. The term “smart contract” was firstly used by Nick Szabo in 1997. His main vision for smart contracts was the creation of a distributed ledger to store contracts. A contract is a set of rules or clauses that parties have agreed upon the governing relationship between them. Smart contracts are just like contracts in the real world, with the difference that they are completely digital. They are small script programs that are used and stored in blockchains, featuring a tamper-proof logic code into them. Smart contracts inherit some important blockchain attributes; they are immutable and distributed because of their storage inside the blockchain. Being immutable ensures that no one can tamper with the code of the contract, while being distributed secures the validation of smart contracts’ output from everyone on the network. Smart contracts are used in many types of blockchain applications such as in supply chains and in the health sector.

When a block (or transaction) is scanned and sourced through a completely digitized way, then the specific transaction is confirmed and the block is appended at the chain. After the execution of the contract, a certificate is issued, where a variety of information related to the blockchain transactions can be retrieved. Finally, every client in the network retains a copy of the smart contract and, as a result, each node has the following:

- History of all smart contracts;
- History of all transactions;
- Current state of all smart contracts [9][10].

Ethereum was specifically created and designed for smart contracts support. There are many examples of programming languages that allow software coding within the blockchain. A widely used tool for this purpose is Ethereum’s Solidity programming language, a Turing-complete language. Solidity defines and determines a sequence of specific rules that dictate how a program operates and executes [8].

Table 1 provides an overview of the utilization of smart contracts in different agriculture traceability systems where blockchain technology is applied. As may be observed, the majority of current research results adopts the smart contract technology on the Ethereum blockchain in order to implement various types of transactions (such as transactions between farmers, suppliers and distributors).

Table 1. Survey or research works in the agriculture traceability systems—classification depending on the usage (or not) of smart contracts.

Use of Smart Contracts	Literature Works
Literature involving smart contracts in agriculture traceability systems	[11][12][13][14][15][16][17][18][19][20][21][22][23][24][25][26][27][28][29][30][31][32][33][34][35][36][37][38][39][40][41][42][43][44][45][46][47]
Literature involving blockchain technology but without the use of smart contracts in agriculture traceability systems	[48][49][50][51][52][53][54][55][56][57][58][59][60][61][62][63]

3. Consensus Methodologies

A very important characteristic, not only for the blockchain technology, but also for any type of decentralized system, is byzantine fault tolerance. The byzantine generals' problem was conceived in 1982 as a logical dilemma that illustrates how a group of generals, who may have communication problems, will try to agree on the next move. If we apply the above definitions to the operation of blockchains, each general represents a network node, and all nodes need to reach a consensus on the current state of the system. This means that the majority of the participants within a distributed network have to agree and execute the same action in order to avoid failures. The byzantine generals' problem gave birth to the concept of byzantine fault tolerance. Byzantine fault tolerance is the property of a system to resist all the possible costs of failures derived from the byzantine generals' problem. In other words, a byzantine fault tolerant system is able to continue operating, even if some of the nodes fail to communicate or act in a malicious way. There are multiple ways of developing or building a byzantine fault tolerant blockchain system, and these are related to the different types of consensus algorithms/protocols [64][65].

A consensus algorithm can be defined as a mechanism through which a blockchain network reaches consensus. The consensus protocol for a blockchain has to solve two major challenges: the first one is to protect the network from attackers, and the second one is to tackle competing chains. The most celebrated consensus protocols are the Proof of Work (PoW) and the Proof of Stake (PoS) . In addition to these, there are some other consensus algorithms, such as Proof of Authority (PoA), Proof of Burn (PoB), Proof of Elapsed Time (PoET), Proof of Capacity (PoC), and others.

More specifically, PoW gives more rewards to people that own more and better equipment. As a result, the higher the hash rate of a user is, the higher the chance of creating the next block and receiving the mining award. In the end, the hash that every block has is the proof of work, which occurs by solving a cryptographic challenge puzzle. The term "mining pools" refers to the combination of hashing power and the distribution of the reward across every node in the winning pool. The use of mining pools renders the blockchain more centralized, as opposed to decentralized schemas.

In order to solve the above issue, an idea for a new blockchain consensus protocol, as an alternative to the proof of work protocol, was born. In 2011, a Bitcointalk forum user called QuantumMechanic proposed a new technique called Proof of Stake (PoS). The differences between PoW and PoS are quite significant. PoS is more decentralized than PoW, it does not let every user to mine for new blocks, it is a lot less expensive compared to the PoW mining equipment requirements, and finally, encourages more people to set up a node, making the network more decentralized as well as more secure.

Besides these advantages, the PoS protocol entails additional risks when compared to PoW. Specifically, if a single or a group of miners can obtain 51% of the hashing power, they can effectively control and manipulate the blockchain. This attack is known as the 51% Attack. PoS makes this type of attack very impractical on specific cryptocurrency values, so it is actually less likely to occur with this type of consensus protocol, yet still remains an important risk. Another important risk issue is the way that PoS algorithms select the next validator. The process is random, and validators can typically be selected based on a combination of the lowest hash value and highest stakes, or based on how long their tokens have been staked for. Another problem of PoS is due to the possibility of selecting a user as the next validator, a role that may not come along its duties. An approach to solving this is by choosing a large number of backup validators [66].

4. Public vs. Private Blockchain

Adhering to the view for open access to everyone, many widely used blockchains (Bitcoin, Ethereum and Dash) are public networks. Public blockchain networks are characterized as permissionless, where anyone can join, read and/or write data, create smart contracts or even run a node within them, ensuring one hundred percent transparency as well as a high level of anonymity. Public networks are recommended for entities involved mainly in crypto-economics. In contrast to public blockchain networks, private networks restrict either participant or validator access as a classic closed ecosystem where all peers are well defined and only pre-approved entities can run nodes. Following a business-to-business approach, many companies use private blockchain networks in order to benefit from this technology without sacrificing their autonomy. Private blockchains, in contrast to public ones, typically use a type of consensus other than PoW, and might aim at keeping certain information private from the public. In summary, public blockchain networks enjoy freedom in decentralization, whereas private blockchain networks enjoy freedom in configurational flexibility [67]. Hybrid approaches also exist—these are called permissioned blockchain systems. Different types and configurations of permissioned blockchain systems exist, but typically the consensus process is controlled by a predefined list of participants, and users cannot participate without permission. Access to the full information of transactions on the blockchain might be restricted, depending on the user role.

Table 2 provides an overview of the types of blockchain used in different agriculture traceability systems. The majority of research works have used public blockchain types, in association with either Ethereum or Hyperledger, whereas a smaller percentage prefer the adoption of permissioned or fully private blockchains. Nonetheless, it is notable that many research studies attempt to make a more theoretic contribution and do not explicitly make reference to a specific blockchain implementation.

Table 2. Literature survey—use of different blockchain types and implementations in agriculture traceability systems.

Public vs. Private Blockchain	Blockchain Implementation	Research Works
Public	Ethereum	[17][18][19][20][22][27][40][41][45][51][52]
	Hyperledger Sawtooth	[43]
	Hyperledger (other than Sawtooth)	[23][38]
	Ethereum or Hyperledger Sawtooth	[32]
	Ethereum or Hyperledger (other than Sawtooth)	[12]
	Not specified	[48][11][13][15][25][28][30][31][33][35][39][44][48][49][53][54][56][58][59][61][62][68][69]
Private	Ethereum	[40]
	Ethereum or Hyperledger Sawtooth	[12]
	Not specified	[15][21][36][39][55]
Permissioned (Hybrid)	Ethereum	[16][29][37]
	Hyperledger Sawtooth	[26][34][46][47]
	Hyperledger Fabric	[24][42][57]
	Not specified	[14][50][60]

5. Traceability from Farm to Fork Using Blockchain

Blockchain technology provides the ability to create a smarter and more secure supply chain, offering a clear and solid audit trail of the tracked products in real-time. Traceability information regarding product origin and possible allergens or added substances, which has to be stored in a secure and immutable manner, can be established and shared through a collaborative blockchain network between farmers, manufacturers and distributors. Such blockchain networks can exist at global scale (as done today in the case of many crypto-currencies), spanning across multiple countries and organizations, establishing a trustworthy information flow among stakeholders with specific agreements when it comes to data exchange. According to Robert Sinfield, Vice President of Product for Sage Business Cloud X3 [70]: “On the visibility side, blockchain

ERP systems could enable everyone involved to track the product's journey from the manufacturing floor to the retailer's shelf, without having to worry about records being lost or tampered with… Nowhere is this more prevalent than in the food and drink space, where blockchain will provide transparency and product provenance that is validated from farm to fork".

References

1. Burke, T. Blockchain in food traceability. Food Traceability 2019, 133–143.
2. Stuart Haber; W. Scott Stornetta; How to time-stamp a digital document. *Journal of Cryptology* **1991**, *3*, 99-111, 10.1007/bf00196791.
3. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing List. 2008. Available online: https://metzdowd.com (accessed on 20 May 2020).
4. Raikwar, M.; Gligoroski, D.; Kralevska, K. SoK of used cryptography in blockchain. IEEE Access 2019, 7, 148550–148575.
5. Penard, W.; van Werkhoven, T. On the secure hash algorithm family. In Cryptography in Context; Wiley: Hoboken, NJ, USA, 2008; pp. 1–18.
6. Berg, C.; Davidson, S.; Potts, J. The Blockchain Economy: A Beginner's Guide to Institutional Cryptoeconomics. Available online: https://medium.com/cryptoeconomics-australia/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4 (accessed on 21 October 2019).
7. Buterin, V. The Meaning of Decentralization. Available online: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 (accessed on 18 October 2019).
8. What is Ethereum? The Ultimate Beginners' Guide. Available online: https://coincentral.com/what-is-ethereum-the-ultimate-beginners-guide/ (accessed on 21 October 2019).
9. Project Provenance Ltd Blockchain: The Solution for Transparency in Product Supply Chains. Available online: https://www.provenance.org/whitepaper (accessed on 22 October 2019).
10. Jabbari, A.; Kaminsky, P. Blockchain and Supply Chain Management. In Proceedings of the College Industry Council on Material Handling Education, Phoenix, AZ, USA, 27 September 2018.
11. Leng, K.; Bi, Y.; Jing, L.; Fu, H.-C.; Van Nieuwenhuyse, I. Research on agricultural supply chain system with double chain architecture based on blockchain technology. Future Gener. Comput. Syst. 2018, 86, 641–649.
12. Caro, M.P.; Ali, M.S.; Vecchio, M.; Giaffreda, R. Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. In Proceedings of the 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), Tuscany, Italy, 8–9 May 2018; pp. 1–4.
13. Casado-Vara, R.; Prieto, J.; De La Prieta, F.; Rodríguez, J.M.C. How blockchain improves the supply chain: Case study alimentary supply chain. Procedia Comput. Sci. 2018, 134, 393–398.
14. Hong, W.; Cai, Y.; Yu, Z.; Yu, X. An agri-product traceability system based on IoT and blockchain technology. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 17–19 August 2018; pp. 254–255.
15. Schmidhuber, J.T.M. Emerging Opportunities for the Application of Blockchain in the Agri-food Industry; Food and Agriculture Organization of the United Nations and International Centre for Trade and Sustainable Development (ICTSD): Geneva, Switzerland, 2018.
16. Mao, D.; Hao, Z.; Wang, F.; Li, H. Novel automatic food trading system using consortium blockchain. Arab. J. Sci. Eng. 2018, 44, 3439–3455.
17. Kim, M.; Hilton, B.; Burks, Z.; Reyes, J. Integrating blockchain, smart contract-tokens, and IoT to design a food traceability solution. In Proceedings of the 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 1–3 November 2018; pp. 335–340.
18. Baralla, G.; Ibba, S.; Marchesi, M.; Tonelli, R.; Missineo, S. A blockchain based system to ensure transparency and reliability in food supply chain. In Proceedings of the Euro-Par 2018: Parallel Processing Workshops, Turin, Italy, 27–28 August 2018; Mencagli, G., Heras, D., Cardellini, V., Casalicchio, E., Jeannot, E., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 379–391.
19. Lin, Q.; Wang, H.; Pei, X.; Wang, J. Food safety traceability system based on blockchain and EPCIS. IEEE Access 2019, 7, 20698–20707.
20. Salah, K.; Nizamuddin, N.; Jayaraman, R.; Omar, M. Blockchain-based soybean traceability in agricultural supply chain. IEEE Access 2019, 7, 73295–73305.

21. Kamble, S.S.; Gunasekaran, A.; Sharma, R. Modeling the blockchain enabled traceability in agriculture supply chain. In t. J. Inf. Manag. 2020, 52, 101967.

22. Figorilli, S.; Antonucci, F.; Costa, C.; Pallottino, F.; Raso, L.; Castiglione, M.; Pinci, E.; Del Vecchio, D.; Colle, G.; Proto, A.R.; et al. A blockchain implementation prototype for the electronic open source traceability of wood along the whole s upply chain. Sensors 2018, 18, 3133.

23. Lucena, P.; Binotto, A.P.D.; Momo, F.D.S.; Kim, H. A Case Study for Grain Quality Assurance Tracking based on a Bloc kchain Business Network 2018. In Proceedings of the Symposium on Foundations and Applications of Blockchain (FAB 18), Los Angeles, CA, USA, 9 March 2018.

24. Lei, H.; Israr, U.; Do-Hyeun, K. A Secure Fish Farm Platform Based on Blockchain for Agriculture Data Integrity, Compu ters and Electronics in Agriculture; arXiv: Ithaca, NY, USA, 2020; p. 170. ISSN 0168-1699.

25. Tian, F. A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In Proceedi ngs of the 2017 International Conference on Service Systems and Service Management, Dalian, China, 16–18 June 20 17; pp. 1–6.

26. Bumblauskas, D.; Mann, A.; Dugan, B.; Rittmer, J. A blockchain use case in food distribution: Do you know where your f ood has been? Int. J. Inf. Manag. 2020, 52, 102008.

27. Fishcoin a Blockchain Based Data Ecosystem for the Global Seafood Industry, Fishcoin, White Paper. 2018. Available online: https://fishcoin.co/files/fishcoin.pdf (accessed on 24 May 2020).

28. Rejeb, A. Halal meat supply chain traceability based on HACCP, blockchain and internet of things. Acta Tech. Jaurinens is 2018, 11, 218–247.

29. Kim, H.; Laskowski, M. Agriculture on the blockchain: Sustainable solutions for food, farmers, and financing. SSRN Ele ctron. J. 2017, 10, 2139.

30. Kumar, M.V.; Iyengar, N.C.S.N. A framework for blockchain technology in rice supply chain management plantation. Fut ure Gener. Commun. Netw. 2017, 125–130.

31. Zhang, Q.; Han, Y.-Y.; Su, Z.-B.; Fang, J.-L.; Liu, Z.-Q.; Wang, K.-Y. A storage architecture for high-throughput crop bre eding data based on improved blockchain technology. Comput. Electron. Agric. 2020, 173, 105395.

32. Umamaheswari, S.; Sreeram, S.; Kritika, N.; Prasanth, D.R.J. BIoT: Blockchain based IoT for Agriculture. In Proceeding s of the 2019 11th International Conference on Advanced Computing (ICoAC), Chennai, India, 18–20 December 2019; pp. 324–327.

33. Awan, S.H.; Ahmed, S.; Nawaz, A.; Sulaiman, S.; Zaman, K.; Ali, M.; Najam, Z.; Imran, S. BlockChain with IoT, an emer gent routing scheme for smart agriculture. Int. J. Adv. Comput. Sci. Appl. 2020, 11.

34. Baralla, G.; Pinna, A.; Corrias, G. Ensure traceability in european food supply chain by using a blockchain system. In Pr oceedings of the 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockc hain (WETSEB), Montreal, QC, Canada; 2019; pp. 40–47.

35. Dobbins, A.; Sprinkle, A.; Hadley, B.; Cazier, J.; Wilkes, J. Blocks for bees: Solving bee business problems with blockch ain technology. In Proceedings of the ARBS 2018 5th Annual Conference, Johnson City, TN, USA, 22–23 March 2018; pp. 11–16.

36. Casino, F.; Kanakaris, V.; Dasaklis, T.K.; Moschuris, S.; Rachaniotis, N.P. Modeling Food Supply Chain Traceability Bas ed on Blockchain Technology. IFAC-PapersOnLine 2019, 52, 2728–2733.

37. Shahid, A.; Almogren, A.; Javaid, N.; Al-Zahrani, F.A.; Zuair, M.; Alam, M. Blockchain-based agri-food supply chain: A co mplete solution. IEEE Access 2020, 8, 69230–69243.

38. Wang, Z.; Liu, P. Application of blockchain technology in agricultural product traceability system. In Intelligent Tutoring S ystems; Springer Science and Business Media LLC: Cham, Switzerland, 2019; pp. 81–90.

39. Orsato, R.J.; Cohen, A. The Impact of Blockchain Technology on Eco-labelling Schemes: A Study in the Fishing Industr y, Sao Paulo. 2020. Available online: http://bibliotecadigital.fgv.br/dspace/handle/10438/29033 (accessed on 28 May 20 20).

40. Unurjargal, E.; Comuzzi, M. Blockchain-Supported Food Supply Chain Reference Architecture. Graduate School of UNI ST, 2019. Available online: https://scholarworks.unist.ac.kr/handle/201301/25889 (accessed on 28 May 2020).

41. Mao, D.; Hao, Z.; Wang, F.; Li, H. Innovative blockchain-based approach for sustainable and credible environment in fo od trade: A case study in Shandong province, China. Sustainability 2018, 10, 3149.

42. Ge, L.; Brewster, C.; Spek, J.; Smeenk, A.; Top, J.; Van Diepen, F.; Klaase, B.; Graumans, C.; Wildt, M.D.R.D. Blockch ain for Agriculture and Food: Findings from the Pilot Study; Report 2017-112; Wageningen University and Research: W ageningen, The Netherlands, 2017.

43. Hayati, H.; Nugraha, I.G.B.B. Blockchain based traceability system in food supply chain. In Proceedings of the 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 21 November 2018; pp. 120–125.
44. Gunasekera, D.; Valenzuela, E. Adoption of blockchain technology in the australian grains trade: An assessment of potential economic effects. Econ. Pap. A J. Appl. Econ. Policy 2020, 39, 152–161.
45. de Ruyter de Wildt, M.; van Ginkel, M.; Coppoolse, K.; van Maarseveen, B.; Walton, J.; Kruseman, G. Blockchain for Food: Making Sense of Technology and the Impact on Biofortified Seeds. Community of Practice on Socio-economic Data Report 2019. CGIAR Platform for Big Data in Agriculture. 2019. Available online: https://hdl.handle.net/10568/106615 (accessed on 29 May 2020).
46. Chan, K.Y.; Abdullah, J.; Shahid, A. A framework for traceable and transparent supply chain management for agri-food sector in malaysia using blockchain technology. Int. J. Adv. Comput. Sci. Appl. 2019, 10.
47. Mohan, T. Improve Food Supply Chain Traceability using Blockchain, 2018, The Pennsylvania State University, The Graduate School College of Engineering. Available online: https://etda.libraries.psu.edu/catalog/14913txm91 (accessed on 29 May 2020).
48. Feng, T. An agri-food supply chain traceability system for china based on RFID & Blockchain Technology. In Proceedings of the 2016 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, China, 24–26 June 2016; pp. 1–6.
49. Marinello, F.; Atzori, M.; Lisi, L.; Boscaro, D.; Pezzuolo, A. Development of a traceability system for the animal product supply chain based on blockchain technology. Nantes 2017, 1, 258–268.
50. Lin, J.; Shen, Z.; Zhang, A.; Chai, Y. Blockchain and IoT based food traceability for smart agriculture. In Proceedings of the 3rd International Conference on Crowd Science and Engineering-ICCSE'18, Singapore, 28–31 July 2018; Volume 3, p. 3.
51. Mondal, S.; Wijewardena, K.; Karuppuswami, S.; Kriti, F.N.; Kumar, D.; Chahal, P. Blockchain inspired RFID-based information architecture for food supply chain. IEEE Internet Things J. 2019, 6, 5803–5813.
52. Liao, Y.; Xu, K. Traceability system of agricultural product based on block-chain and application in tea quality safety management. J. Physics Conf. Ser. 2019, 1288.
53. Cook, Blockchain: Transforming the Seafood Supply Chain, WWF. 2018. Available online: http://awsassets.wwfnz.panda.org/downloads/draft_blockchain_report_1_4_1.pdf (accessed on 27 May 2020).
54. Honeysuckle White expands Thanksgiving Traceable Turkey Program, Continuing its Commitment to Food Transparency, Honeysuckle White. 2018. Available online: https://www.cargill.com/2018/honeysuckle-white-expands-thanksgiving-traceable-turkey-program (accessed on 23 May 2020).
55. Hua, J.; Wang, X.; Kang, M.; Wang, H.; Wang, F.-Y. Blockchain based provenance for agricultural products: A distributed platform with duplicated and shared bookkeeping. 2018 IEEE Intell. Veh. Symp. (IV) 2018, 97–101.
56. Biswas, K.; Muthukkumarasamy, V.; Lum, W. Blockchain Based Wine Supply Chain Traceability System. In Proceedings of the Future Technologies Conference (FTC), Vancouver, BC, Canada, 29–30 November 2017; pp. 56–62.
57. Visser, C.; Hanich, Q. How Blockchain is Strengthening Tuna Traceability to Combat Illegal Fishing. 2017. Available online: https://theconversation.com/how-blockchain-is-strengthening-tuna-traceability-to-combat-illegal-fishing-89965 (accessed on 14 May 2020).
58. Saji, A.C.; Vijayan, A.; Sundar, A.J.; Baby Syla, L. Permissioned blockchain-based agriculture network in rootnet protocol. In Proceedings of the International Conference on Innovative Computing and Communications. Advances in Intelligent Systems and Computing, Ostrava, Czech Republic, 21–22 March 2019; Khanna, A., Gupta, D., Bhattacharyya, S., Snasel, V., Platos, J., Hassanien, A., Eds.; Springer: Singapore, 2020; p. 1059.
59. Huynh, T.S.; Nguyen, L.A.T. Developing blockchain-based system for tracking the origin of chicken products. Int. J. Innov. Technol. Explor. Eng. 2019, 8, 10.
60. Scuderi, A.; Foti, V.T.; Timpanaro, G. The Supply Chain Value of POD and PGI Food Products through the Application of Blockchain. Calit. Acces Success 2019, 20, 580–587. Available online: http://hdl.handle.net/20.500.11769/363300 (accessed on 28 May 2020).
61. Malik, S.; Kanhere, S.S.; Jurdak, R. ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains. In Proceedings of the 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 26–28 November 2018; pp. 1–10.
62. Arsyad, A.A.; Dadkhah, S.; Köppen, M.; Dhadkah, S. Two-factor blockchain. In Lecture Notes on Data Engineering and Communications Technologies; Springer Science and Business Media LLC: Cham, Switzerland, 2018; pp. 332–339.

63. Kakkar, A.; Ruchi., A. Blockchain technology solution to enhance operational efficiency of rice supply chain for food corporation of India. In Sustainable Communication Networks and Application Lecture Notes on Data Engineering and Communications Technologies; Karrupusamy, P., Chen, J., Shi, Y., Eds.; Springer: Cham, Switzerland, 2020; p. 39.
64. Lamport, L.; Shostak, R.; Pease, M. The byzantine generals problem. ACM Trans. Program. Lang. Syst. 1982, 4, 382–401.
65. Konstantopoulos, G. Understanding Blockchain Fundamentals, Part 1: Byzantine Fault Tolerance. Available online: https://medium.com/loom-network/understanding-blockchain-fundamentals-part-1-byzantine-fault-tolerance-245f46fe8419 (accessed on 22 October 2019).
66. Castor, A. A (Short) Guide to Blockchain Consensus Protocols. Available online: https://www.coindesk.com/short-guide-blockchain-consensus-protocols (accessed on 22 October 2019).
67. Massessi, D. Public vs Private Blockchain in a Nutshell. Available online: https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f (accessed on 23 October 2019).
68. Smart Supply Chain: Farm-to-Fork Traceability for Large Scale Farming, Bühler. Available online: https://digital.buhlergroup.com/fileadmin/uploads/buhler/Digital/Images/Smartsupply/Brochure_Final_Light.pdf (accessed on 26 May 2020).
69. George, R.V.; Harsh, H.O.; Ray, P.; Babu, A.K. Food quality traceability prototype for restaurants using blockchain and food quality data index. J. Clean. Prod. 2019, 240, 118021.
70. Wattanajantra, A. How Blockchain Traceability Can Improve Supply Chain Management. Available online: https://www.sage.com/en-gb/blog/blockchain-traceability-supply-chain/#%20gate-2bbb8114-16b1-4518-9f6e-3a7dfb785d23 (accessed on 17 September 2019).
