Blockchain-Based Certificate Authentication for International Food Trade

Subjects: Automation & Control Systems

Contributor: William George , Tareq Al-Ansari

Maritime transportation plays a critical role for many Arab countries and their food security and has evolved into a complex system that involves a plethora of supply chain stakeholders spread around the globe. This inherent complexity brings huge security challenges, including cargo loss and high burdens in cargo document inspection. The emerging blockchain technology provides a promising tool to build a unified maritime cargo tracking system critical for cargo security. This is because blockchains are a tamper-proof distributed ledger technology that can store and track data in a secure and transparent manner.

blockchain technology food certifications digitized food logistics distributed ledger technology food security food supply chain food certificate authentication

1. Introduction

Food certifications are an important part of the international food trade and are necessary to guarantee the quality, safety and sustainability of food products as they move through the supply chain. These certifications, which give customers and businesses assurance in the goods they purchase, help the global food trade function smoothly. The role of the national government in food security is indispensable to the healthy living and prosperity of a nation. This role is understated and often considered irrelevant to investing in technology infrastructure. Every neoteric food policy presupposes a robust and versatile technology infrastructure. This facility is then utilized in unveiling, surveilling and evaluating the efficiency and sufficiency of the policy. The Nordic countries (Denmark, Finland, Norway and Sweden) [1] and some European nations (Luxembourg, Germany and Estonia) have governments that are recognized for their extensive adoption of technology in national food security governance. For example, as part of its strategic relationship with the World Food Program, the Luxembourg Government seeks to bolster progress toward Zero Hunger by adopting a common UN blockchain system, which will steer programs that engage the effectiveness of cash-based interventions (CBIs) and leverage food traceability [2]. Another illustrative instance is the visionary roadmap of the Ministry of Rural Affairs and the Ministry of Enterprise and Innovation in Sweden that aims to invest in technology to foster food system collaboration, empowering farmers and ameliorating knowledge management within different stakeholders of the food system [3][4].

As shown in **Figure 1**, the digitization of the global food trade is playing a bigger role in the development of world economies and comes with many advantages. The process can be made more productive, swifter and transparent while also improving the traceability and security of food products by utilizing digital platforms and technologies, like the blockchain. From farmers and producers to traders and consumers, this will be advantageous to all parties involved in the food trade process. A more sustainable and dependable food trade system will be possible for everyone if blockchain technology is used to increase the transparency, security and efficiency of the food trade.

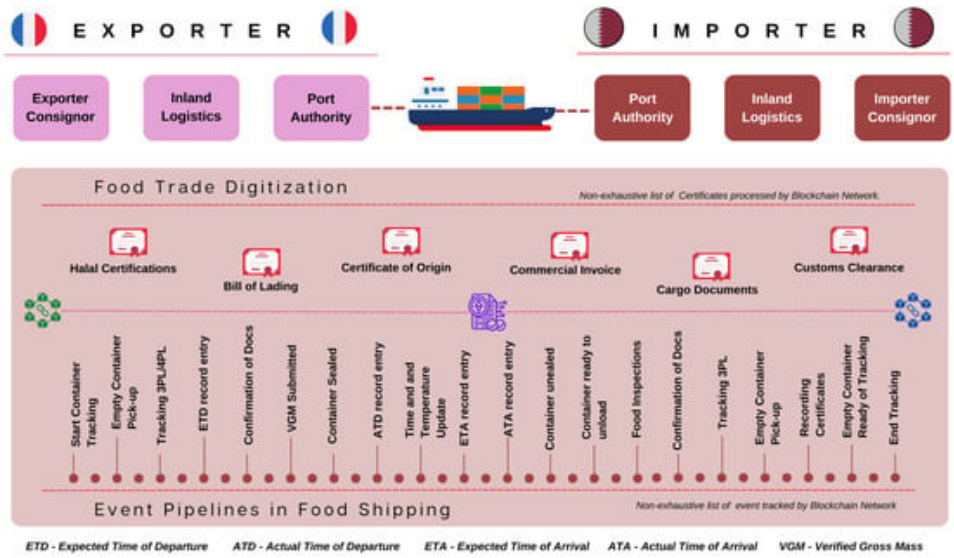

Figure 1. Digitization of trade certificates in the food system.

The following are some of the major advantages of blockchain technology-based certification traceability in the blockchain:

- Risk mitigation. By offering a safe and impenetrable method to track and confirm the authenticity of food products as they move through the supply chain, blockchain technology can help reduce the risk associated with file signing and document traceability in the food system. A blockchain-based system can verify that documents and files related to a food product that have not been tampered with by using digital signatures. Additionally, by recording all transactions and changes to a product's status on the blockchain, it is possible to trace the product's path from farm to consumer. Additionally, the blockchain can offer a secure, decentralized method for various actors in the food supply chain to share and access information about a product. This can help to increase transparency and trust between supply chain participants.

- Dramatically reduces transaction costs and time. Instead of relying on a centralized authority or middleman, a blockchain-based system enables a decentralized network of participants to access and share information about a food product. This can lower the price of using intermediaries and lessen the need for coordination and communication among various supply chain participants.

- Improved asset authenticity verification. Blockchain technology can offer a transparent and unchangeable record of a food product's entire supply chain journey. This may lessen the requirement for costly and time-consuming inspections and audits. Blockchains are an amalgamation of four security features: hash functions, public–private key encryption, consensus algorithms and smart contracts.

- Decreased fraud and compliance costs. A blockchain-based system can use digital signatures to guarantee that documents and files related to a food product have not been tampered with, which can help identify and stop fraudulent activities. A tamper-proof record of all transactions and modifications to a food product's status is produced by blockchain technology. This can aid in the detection and prevention of dishonest practices like the falsification of documents or the mislabeling of goods.

- New financing opportunities. Through the use of various techniques like smart contracts, tokenization, supply chain finance, trade finance, crowdfunding and automation, blockchain technology can provide new financing opportunities in the contemporary supply chain. By automating the payment process, these methods can increase supply chain efficiency and

financing opportunities while reducing intermediaries and financing costs. They can also improve access to capital for SMEs and provide new ways to raise capital and create liquidity.

- Decreased risk and increased document trade facilities. Systems for tracking food products as they move through the supply chain that are based on blockchain technology may offer a more precise and effective method. As a result, product recall costs can be decreased and problem detection and resolution times can be sped up. Blockchain-based systems can offer an unambiguous and auditable record of every transaction, which can help to ensure compliance with legal requirements and cut down on the expense of compliance audits.

- Simple, secure data sharing between institutions. The supply chain can be made more efficient overall if blockchain technology is used to enable real-time access to the same information by multiple parties. This can help with coordination and cut down on errors. A key component of blockchain technology is consensus algorithms. They are used to make sure that new transactions are valid and that everyone in a blockchain network agrees on the ledger's current state.

Role of Certifications in the Food System

Many of the manual procedures involved in the global food trade, like tracking and documentation, can be automated by using digital platforms and technologies [5]. International public and private players could have access to a wide variety of food product certifications, which helps to ensure food security for populations around the world; blockchain integration into international food trade is an essential sector for world economies. However, the conventional method of conducting international food trade is frequently slow, laborious and prone to mistakes, which can cause delays and increased costs. The need for the digitization of the global food trade is expanding in order to address these problems. The increased efficiency and speed of the process are some of the main advantages of digitizing international food trade. The time and expenses involved in the global food trade may be reduced as a result, making it more convenient and affordable for all parties involved.

The increased transparency and traceability of food products are other significant advantages of digitizing international food trade. A tamper-proof and immutable record of food products' movement through the supply chain can be made using blockchain technology. As well as assisting in locating any potential issues or problems, this can help build trust and confidence in the food products being traded. One of the main technologies being used to digitize the global food trade is blockchain technology. A tamper-proof and immutable record can be created using the decentralized and distributed ledger technology known as the blockchain, as shown in **Figure 2**. This makes it ideal for use in supply chain management since it enables the creation of a transparent and auditable record of food products as they move through the supply chain.

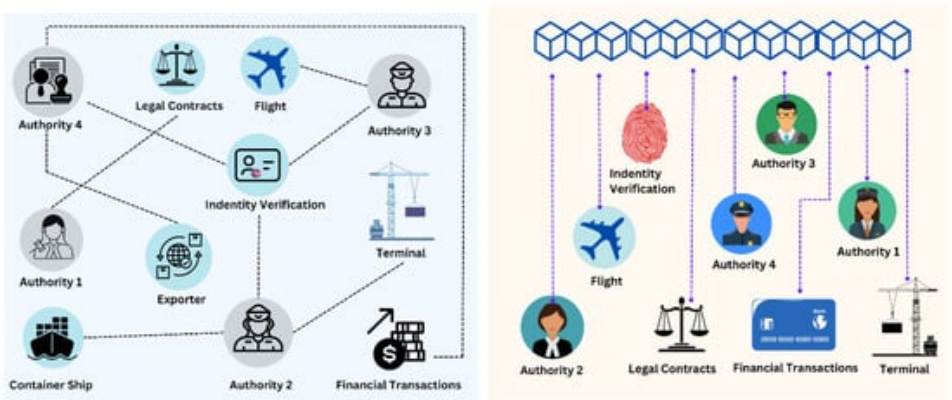

Figure 2. Present system versus proposed system: (**Left**) Present information sharing system without blockchain technology (**Right**) Proposed system with the adoption of blockchain technology.

2. Blockchain-Based Certificate Authentication for International Food Trade

A glance at both the scientific and general literature available on blockchain-based digital record-keeping will provide weighty insights into how BCT will revolutionize different industries.

“The blockchain innovation really allows us to take everything where there’s record keeping, everything where there’s trust around record keeping, and it allows us to make that digital, immutable, permanent, and global.” [6]

- Jeremy Allaire

The notion of storing data in a read-only format in a distributed chain of blocks (nodes) has been around for quite some time. However, it was not until Nakamoto [7] that an actual application for recording decentralized financial transactions was made possible. Blockchains were initially seen as an alternative to financial transactions and were quickly associated with protocols such as Bitcoins, Ethereum [8] and Ripple [9]. Generally speaking, a blockchain is an electronic database that stores data digitally and is mainly used to securely record transactions using established protocols.

2.1. Types of Blockchain Networks

Depending on how data are stored and distributed, and who is given access to the network, blockchain networks can be classified generally into permissionless and permissioned blockchains.

As shown in **Figure 3**, one can further classify distributed ledger networks into the following:

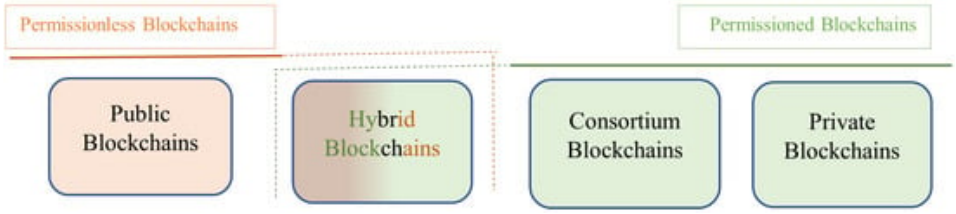

Figure 3. Types of blockchain networks.

2.1.1. Permissionless Blockchains

A permissionless blockchain is a decentralized ledger that is open to the public. The vast majority of cryptocurrencies, including Bitcoin, are powered by permissionless blockchain networks. Here are the key characteristics of permissionless blockchains.

2.1.2. Public Blockchains

The most common type of permissionless blockchain is a public blockchain. The read and write privileges are entirely unconstrained on a public blockchain [10]. The same rules that govern permissioned blockchains apply to writers. The network’s users are all anonymous. Nonetheless, some form of identity management is required when authors are given the option to remain anonymous. If not, it would be conceivable for a tiny business to impersonate a large one, giving it the ability to contribute blocks more frequently than others and, as a result, significant control over which chain of transactions is recognized as legitimate [11]. “Sybil attacks” are this kind of assault. In order to write on the ledger, writers are typically required to first demonstrate that they have completed a computationally challenging assignment. The majority of the most important cryptocurrency blockchains, including those for Bitcoin, Ethereum and Litecoin, employ this technique.

2.1.3. Permissioned Blockchains

A blockchain that has been given “permission” only allows a specific entity or group of entities to write to it [12]. These organizations are the only ones allowed to propagate and validate transactions, and they also control the blockchain’s rules. The read privilege may be made available to the general public or could be partially kept secret. Here again, expensive identity management is not required because the permitted writers alternately add blocks to the chain in accordance with a predetermined algorithm. As in a private blockchain, writers on a permissioned blockchain are chastised by readers, but they are also disciplined by other writers.

2.1.4. Private Blockchains

On a private blockchain, the contents of the ledger are entirely under the control of one central authority. In other words, there is just one author. The general public, the entity’s clients or a regulator might be the readers in this case. Also, different groups may have various read access on the ledger. A private blockchain does not require identity management because only one entity is allowed to write to the ledger. The system operates similarly to a privately maintained database that grants outsiders read privileges because there are no computational costs. Private blockchains are ideal for sandbox environments; however, they are not viable for enterprise or business solutions.

2.1.5. Consortium Blockchains

A consortium blockchain’s main goal is to increase cooperation in order to tackle an industry’s ongoing difficulties. Consortia blockchains can be used by groups with shared objectives to restructure workflow, transparency and responsibility [13]. The consortium blockchain has a known and verified number of participants. They undertake authentication, which lowers the possibility of data threats. Nodes that go against the established protocols are promptly detected and punished. The consortium blockchain makes additional vulnerabilities like SQL injection, DDoS and “man in the middle” unimportant. The governance model states that a contract is frequently made by a relatively small number of nodes. Because it is less difficult to reach, this kind of consensus is more common. These factors have an immediate impact on transactional outputs, resulting in quick processes and enhanced scalability. Thus, mutual consensus is easier to obtain and, therefore, the blockchain does not consume much power.

2.1.6. Hybrid Blockchains

A hybrid blockchain is a special kind of blockchain technology that combines elements of both private and public blockchains or aims to use the best features of both types of blockchains. As highlighted by [14], with a hybrid blockchain, businesses may create both a private, permission-based system and a public, permission-less system, giving them control over which data will be made public and who has access to them. A hybrid blockchain generates more scalability than a public blockchain network and allows for quick and inexpensive transactions.

2.2. Major Features of Blockchain Technology

Blockchain technology has four highlight features that set it apart from other ledger systems (centralized). These are provenance, finality, immutability and algorithmic consensus. Provenance refers to a full record of every transaction involving the assets that were made and stored on the blockchain. Finality, on the other hand, this means that once a transaction is committed to the blockchain, it is considered "final” and can no longer be “rolled back” or undone. Thirdly, a transaction cannot be altered, deleted or have transactions added before it after it has been recorded on the blockchain. This property is referred to as the immutability of blockchains. This feature allows the user to audit records without fear of human errors. Lastly, consensus refers to the procedure of selecting new transactions, distributing them to network users and creating a common agreement on the history of transactions.

2.3. Blockchain and Food Supply Chains

The food supply chain is a complex system with many nuances and intricate processes. On the whole, the food system is one of the most technologically redundant systems in the world. The major difficulties in an agri-food supply chain include a lack of mechanization, inadequate management, inaccurate information and ineffective supply chains. There is a wide body of research that suggests blockchains ought to be integrated with the food supply chains to make them more transparent, traceable and trustworthy [15][16].

Ref. [17] dives into the different pillars of food security and how blockchains can play a valuable role in the technology infrastructure of food security in a holistic sense. They also discussed the organizational, economic and management aspects of blockchain technology adoption.

As of April 2019, more than 80 brands were participating in the IBM Food Trust network, including Walmart, Kroger, Driscoll's, Nestlé and others [18]. Other examples include the food-tracing system introduced by Chinese retail giant Alibaba in April 2018 to provide end-to-end supply chain traceability for imported goods. This consortium, called the Food Trust Framework, includes Fonterra, New Zealand Post, Blackmores and Australia Post and aims to fight food fraud and win consumer trust in the process [19]. Some of the major decentralized protocols that have use cases in the food sector are the Ethereum, IOTA and Ambrosus networks. IOTA (2016) [20] is a distributed ledger technology (DLT) that uses a unique consensus mechanism called the Tangle. The Tangle is a directed acyclic graph (DAG) that allows for transactions to be confirmed without the need for miners or fees. This makes IOTA ideal for use in applications where high throughput and low cost are essential, such as the food supply chain. Provenance, Connecting Food, FreshFarm, InFoodChain and Farm2Kitchen are some of the companies that use IOTA in their food supply chains. Bext350 uses a permission blockchain protocol called Stellar [21] that can aid in higher transactions per second. The Ambrosus protocol (2017) [22] works by creating a shared ledger of food provenance data using IoT sensor (hardware-in-place technique) data sharing. These data include information such as the origin of the food, the date and time of production, the location of each step in the supply chain and the temperature and humidity conditions at each step.

One of the many innovations introduced or amalgamated in blockchains is the smart contract. Smart contracts are codes that are executed when a condition is triggered (such as ownership change, location change, timing or crossing a value threshold). Although Bitcoin is a smart contract by definition, the idea of smart contracts for various other applications was popularized by the Ethereum Blockchain framework. These "if-else" conditions are triggered by data or events that are stored in "oracles", which are non-blockchain sources of digital information, converting outside occurrences into information that can be accessed by smart contracts [23].

2.4. Tokenization of Assets

It is vital to discuss the future direction of food supply chains and their corresponding activities, namely asset tokenization. Long before blockchains, digital tokens were increasingly being used to protect sensitive information, such as personal identifiable information (PII), email addresses and account numbers. This is because tokenization significantly reduces the risk of data breaches [24]. When sensitive data are tokenized, they are replaced with a unique identifier or token. This token has no intrinsic value and cannot be used to access the original data. Tokenization has a number of benefits: It can help to protect sensitive data from unauthorized access, use or disclosure. It can make it more difficult for cybercriminals to steal or misuse sensitive data. It can help to comply with data protection regulations. The agri-food business is one area where tokenization has the potential to be used to great effect. Tokens can be used to track the movement of food products throughout the supply chain, ensuring that they are safe and traceable. Tokens can also be used to create more personalized and customized food products, based on the individual needs of consumers. In the healthcare industry, tokens are being used

to protect patient records. In the financial industry, tokens are being used to protect credit card numbers and other financial information. In the retail industry, tokens are being used to protect customer data.

In the government sector, tokens are being used to protect classified information. Tokenization is a promising technology that has the potential to significantly improve the security of sensitive information. As the use of tokens continues to grow, it is expected to see even more innovative ways to use them to protect data. Tokenization is used to safeguard sensitive data while still allowing them to be used for commercial purposes. This differs from encryption, which involves modifying and storing sensitive data in ways that prevent them from being used for business objectives [25]. A properly constructed and executed cloud tokenization platform can avoid the exposure of sensitive data, preventing attackers from obtaining any type of usable information whether financial or personal. The important word here is "useful information." Tokenization is not a security mechanism that prevents hackers from breaking into your networks and systems. Instead, it represents a data-centric security approach based on "zero trust" concepts [26].

References

1. Raheem, D.; Holopainen, A.; Koegst, J.; Tulimaa, M.; Benkherouf, M. Promoting Sustainability within the Nordic-Arctic Region’s Food System: Challenges and Trends. Sustainability 2022, 14, 9716.
2. Luxembourg, G. New Partnership between Luxembourg and World Food Programme’s Innovation Accelerator. 2018. Available online: https://cooperation.gouvernement.lu/en/actualites/articles/2018/PAM.html (accessed on 5 March 2022).
3. Ministry of Enterprise and Innovation. A National Food Security Strategy for Sweden. 2017. Available online: https://www.government.se/contentassets/16ef73aaa6f74faab86ade5ef239b659/livsmedelsstrategin_kortversion_eng (accessed on 5 March 2022).
4. Eriksson, C.; Fischer, K.; Ulfbecker, E. Technovisions for food security as Sweden restores its civil defence. Sci. Technol. Soc. 2020, 25, 106–123.
5. Kim, H.M.; Laskowski, M. Agriculture on the blockchain: Sustainable solutions for food, farmers, and financing. In Supply Chain Revolution, Barrow Books; Blockchain Research Institute: Mountain View, CA, USA, 2018.
6. Zhang, Y. How Does Blockchain Company Circle Improve Transaction Efficiency and Stay Competitive. In Proceedings of the International Conference on Business and Policy Studies, Stanford, CA, USA, 12 March 2022; Springer: Berlin/Heidelberg, Germany, 2022; pp. 412–420.
7. Nakamoto, S. Bitcoin Whitepaper. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 17 July 2019).
8. Dannen, C. Introducing Ethereum and Solidity; Springer: Berlin/Heidelberg, Germany, 2017; Volume 1.
9. Schwartz, D.; Youngs, N.; Britto, A. The ripple protocol consensus algorithm. Ripple Labs Inc White Pap. 2014, 5, 151.
10. Helliar, C.V.; Crawford, L.; Rocca, L.; Teodori, C.; Veneziani, M. Permissionless and permissioned blockchain diffusion. Int. J. Inf. Manag. 2020, 54, 102136.

11. Rajab, T.; Manshaei, M.H.; Dakhilalian, M.; Jadliwala, M.; Rahman, M.A. On the feasibility of sybil attacks in shard-based permissionless blockchains. arXiv 2020, arXiv:2002.06531.
12. Polge, J.; Robert, J.; Le Traon, Y. Permissioned blockchain frameworks in the industry: A comparison. ICT Express 2021, 7, 229–233.
13. Dib, O.; Brousmiche, K.L.; Durand, A.; Thea, E.; Hamida, E.B. Consortium blockchains: Overview, applications and challenges. Int. J. Adv. Telecommun. 2018, 11, 51–64.
14. Li, Z.; Wu, H.; King, B.; Miled, Z.B.; Wassick, J.; Tazelaar, J. A hybrid blockchain ledger for supply chain visibility. In Proceedings of the 2018 17th International Symposium on Parallel and Distributed Computing (ISPDC), Geneva, Switzerland, 25–28 June 2018; IEEE: New York, NY, USA, 2018; pp. 118–125.
15. Kumar, K.D.; Kumar, M.; Anandh, R. Blockchain technology in food supply chain security. Int. J. Sci. Technol. Res. 2020, 9, 3446–3450.
16. Ge, L.; Brewster, C.; Spek, J.; Smeenk, A.; Top, J.; Van Diepen, F.; Klaase, B.; Graumans, C.; de Wildt, M.d.R. Blockchain for Agriculture and Food: Findings from the Pilot Study; Number 2017-112; Wageningen Economic Research: Lelystad, The Netherlands, 2017.
17. George, W.; Al-Ansari, T. Review of Blockchain Applications in Food Supply Chains. Blockchains 2023, 1, 34–57.
18. Wieck, M. IBM Blockchain: What Can We Solve Together? IBM THINK Blog. 2017. Available online: https://www.ibm.com/blogs/think/2017/08/blockchain-ibm-food/ (accessed on 10 May 2022).
19. Alizila. Alibaba Ups Food Safety down under via Blockchain. 2018. Available online: https://www.alizila.com/alibaba-ups-food-safety-via-blockchain/ (accessed on 10 May 2022).
20. Guo, F.; Xiao, X.; Hecker, A.; Dustdar, S. A Theoretical Model Characterizing Tangle Evolution in IOTA Blockchain Network. IEEE Internet Things J. 2022, 10, 1259–1273.
21. Kshetri, N. Blockchain and sustainable supply chain management in developing countries. Int. J. Inf. Manag. 2021, 60, 102376.
22. Motta, G.A.; Tekinerdogan, B.; Athanasiadis, I.N. Blockchain applications in the agri-food domain: The first wave. Front. Blockchain 2020, 3, 6.
23. Neuburger, J.D.; Choy, W.; Milewski, K.P. Smart Contracts: Best Practices; Thomson Reuters: Toronto, ON, Canada, 2019.
24. Díaz-Santiago, S.; Rodríguez-Henríquez, L.M.; Chakraborty, D. A cryptographic study of tokenization systems. Int. J. Inf. Secur. 2016, 15, 413–432.
25. Morrow, M.J.; Zarrebini, M. Blockchain and the tokenization of the individual: Societal implications. Future Internet 2019, 11, 220.
26. Syed, N.F.; Shah, S.W.; Shaghaghi, A.; Anwar, A.; Baig, Z.; Doss, R. Zero trust architecture (zta): A comprehensive survey. IEEE Access 2022, 10, 57143–57179.