

7

Closing the Trust Gap: Preventing Fraud in Agricultural Finance with IoT and Blockchain

Yashodeepto Narayan Ghosh^{1*} & Abhijit Aditya²

^{1,2}Assistant Professor, Dr. B. C. Roy Academy of Professional Courses (BCRAPC), Durgapur, MAKAUT, West Bengal, India.

*Corresponding Author: yashodeepto@gmail.com

Abstract

Agriculture finance is a difficult ballgame. The critical information on which the entire business runs, and which is used by parties like lenders, index insurers, and other agencies is not in front of them and so has to be communicated to them. This covers points like actual existence and location of the field, what was sown and when, how was the growth, was there any infestation or not and if yes, how was the infestation eradicated, how much was the yield, and so on. Due to most of this actually happening away from the lending agencies, there is an asymmetry of information, which leaves a gap which fraudulent parties can exploit, with inflated yield, staged losses, and overstated claims. This is a point in the business, where emerging tools like blockchain and Internet of Things (IoT), remote sensing and different other related technologies need to be used as a combined approach, since neither of them alone can close the gap effectively. Blockchain provides a decentralized ledger of transactions with absolute transparency, where data is immutable and settlements are automated through smart contracts; however, it cannot verify the data itself. This is the “Oracle Problem”. IoT devices can collect and transmit data from the field level, but the devices can be spoofed, and there is no guarantee of the data quality either. Thus, the data captured and transmitted by the IoT devices, through a blockchain-based network needs to be verified thoroughly before any automatic action can be taken on it using the smart contracts. This chapter introduces a multi-layered conceptual framework, handling the tasks of data capture, automatic detection of anomalies and validation of data, ledger-based records using smart contracts and subsequent governance covering data privacy, data ownership and farmer participation. The framework looks at a few possible fraud domains, namely, lending, area-based subsidies, index insurance and finally carbon credits, taking as examples cases on different crops, subsidy monitoring using satellites, crop insurance using blockchain, and tokenized carbon credits. A study of the cases shows that the need for institutional action remains even after technical implementation, and that adoption of the technology depends on different factors including the trust it enjoys from the farmer level, the cost of implementation,

interoperability with other technical and non-technical systems, and the benefits of sharing information and resources. The conclusion is that fraud-prevention is a socio-technical design problem where all three out of verified evidence, transparent rules and accountable governance are equally important, and empirical testing, and development of standards and policies to support systems that are dominated by smallholders need to be prioritized.

Keywords: Agricultural Finance, Fraud Prevention, Blockchain, Internet of Things, Smart Contracts, Index Insurance, Remote Sensing.

Introduction

Financing in the agriculture domain runs on information about activities which the lenders very rarely get to see for themselves. The bank has to believe that the seeds were legitimately purchased and sown by the applicant in a field legally owned by the borrower and the crops were harvested and the yield was actually as claimed in terms of quality and quantity; the index insurer has to believe that the loss actually occurred due to causes as being claimed by the insured; the carbon buyer must believe that the changed methods of farming impacted the carbon emissions and soil carbon in the manner as reported. Thus, the bank, index insurer, carbon buyer, or, the counterparty in general has to believe the evidence supplied by the party who, in some way, will benefit from this “belief”.

There is thus a distance between what has to be trusted and what can be verified. This is the “trust gap”. In cases where the firms are small, scattered and undocumented, site visits become costly, thus, records are less and the trust gap is more. Frauds happen in different ways – like inflated yields, exaggerated losses, multiple pledging of the same collateral, and environmental benefits that are only claimed, not delivered. Studies show the level of seriousness of such instances. Probst, et al. (2024) conducted a systematic assessment of carbon crediting projects and noted that approximately 16% of the issued credits were backed up by actual reduction of emissions. Most of the difference may not point to deliberate frauds; mostly they are just over-crediting. However, this gives an idea about the level of impact of accepting claims that can’t be checked.

New technologies like blockchain and IoT are many times promoted as solutions to such problems. This is because of the inherent characteristics of these two technologies. Blockchain provides a transparent and distributed ledger of transactions which is tamper-evident and running on smart contracts, while IoT devices enable automated, continuous and real time capture of observations from the field, like yield details. Reviews conducted by researchers like Alobid et al., (2022), Lin et al., (2020) and Xiong et al., (2020) describe a fairly fast-growing family of

applications in the agriculture sector. However, the focus of most of these works is more on the food and agriculture side of the activities and less on finance. Also, the claims are much stronger than the available evidence. As noted by Bager et al. (2022), blockchain is not the magic which will drive out all problems. In fact, as pointed out by Reyna et al. (2018), combining it with the concept of IoT results in questions regarding security, trust and scalability.

This chapter, instead of becoming an empirical test, through literature reviews takes a look at how the trust gap can be reduced using the technologies of blockchain and IoT. It provides a four-layer framework, focusing on four domains more susceptible to fraud, and checks the credibility of the approach using case studies.

Background and Literature Review

- **Fraud and the Trust Gap**

Frauds in agri-finance can be grouped by the underlying domain.

In lending, this misrepresentation may be about the land, collateral or output. In index insurance, it may be about the behavior of the index, the quantum of loss, or maybe the loss itself. While the process accommodates for this by paying a token amount rather than recovering the entire reported loss, however the basic risk of the actual index behavior being different from the reported farm-level outcomes remains, which can be reduced by close monitoring (Afshar et al., 2021). In case of subsidies, the misrepresentation is about the cultivated area, or it could be about different compliances related to environmental conditions. In carbon markets, the misrepresentation could be about the benefits (Probst et al. 2024). Research on food-fraud shows that the food supply chains show similar patterns, with misrepresentation being around origin and authenticity of and treatment given to the product. Here, again, ledger-based tracking is prompted as a detection tool (Leung et al., 2021).

However, the problems actually worsen if the recordkeeping is fragmented. Thorpe et al. (2022) demonstrates how the origins become hard to trace in the tuna value chain due to patchy and uncoordinated traceability systems.

- **Blockchain in Agriculture**

The distributed ledger technology of blockchain makes altering validated records difficult while the smart contracts help by automated execution of agreements, based on pre-decided rules. Researchers like Alobid et al., (2022), Lin et al., (2020) and Xiong et al., (2020) have documented its application across production, processing, trade and finance, and most significantly, agri-food traceability (Bosona & Gebresenbet, 2023; Ordoñez et al., 2024). Van Wassenaeer et al. (2021) insist that blockchain is not a single process, since the architectures differ, resulting in differences in governance, openness and cost, and therefore, selecting

the one to implement is a huge managerial decision and not just a technical detail. Prominent attempts include the Chinese case of a credible environment for food trade being built using blockchain, as described by Mao et al., (2018), the soyabean traceability system as described by Salah, et al. (2019), the smart contracts and tokens enabling third party certifications as reported by Dos Santos et al. (2021) and the rice supply chain as discussed by Yakub, et al. (2022).

- **IoT, Remote Sensing and Analytics**

The data and observations come from the IoT devices, so it can be said that the observational layer is provided by IoT. Blockchain-IoT integrations have been reviewed by various researchers. Bhat et al. (2022) and Kaur et al. (2022) describe conditions and events being recorded by sensors and then ported into shared ledgers, while Ismail et al. (2023) discuss extending the idea to sectors like the fish supply chain.

From the point of view of finance, two complementary evidence sources become important – satellite remote sensing and machine learning.

The first source, satellite remote sensing observes every individual package or item instead of samples; for example, nation-wide monitoring of area-based subsidies in Hungary was supported by imagery from Sentinel-2 (Henits et al., 2022) while monitoring of crop performance improved the performance of index-insurance (Afshar et al., 2021).

The second source is machine learning, which can screen the data received from sensors in real time to identify anomalies; Cheng et al. (2022) proposed an algorithm to detect anomalies in IoT time series data in smart agriculture.

However, as noted by Gupta et al. (2020), security and privacy threats are there in smart farming as well, so the sensing layer itself is also susceptible to attacks.

- **The Oracle Problem and Data Governance**

The blockchain platform and its restrictions guarantee that the contents of the data ledger can't be changed without information to and approval of all users; so, the data once entered can't be deleted or even modified later. However, the ledger does not guarantee that the data entered is not wrong at the start. This is the crux of the oracle problem; the entire mechanism runs on external data but there is no way to check the reliability of the data at the point of entry (Caldarelli, 2020). As noted by Caldarelli and Ellul (2021), responses differ in how much trust they place on the data related to decentralized finance data received through the blockchain platform, while Reyna et al. (2018) report a similar situation regarding open challenges like IoT Integration, scalability, storage, security and trust on devices. Durant et al. (2021) added questions of ownership, incentives and governance when looking at this from the domain of agri-food data sharing.

A Four-Layer Framework for Trust-Preserving Agricultural Finance

The above discussions clarify that there is a vital but missing component, which needs to be incorporated in the transactions. Trust. The framework proposed focusses on this component. It works on the premise that in the field of agri-finance, trust should be based on evidence and not declaration and that blockchain should preserve and use that evidence. The framework has four layers, and it looks at four related domains from where frauds can originate.

Table 1: Fraud domains and the corresponding evidence and controls

Domain	Typical misrepresentation	Independent evidence	Ledger-based control
Lending	Non-existent or inflated transaction; double pledging	Data from Geo-tagging, satellite detection; records of input and delivery	Shared registry of collaterals; verification of transactions before release of funds or stock
Index insurance	Manipulated index data, resulting in mismatches	Multiple reports from multiple sources regarding weather and related information; checking of crop models	Automated payout on trigger based on position of index
Subsidies	False statements regarding area and compliance	Time series data from sources like Sentinel-2; field level sensors	Immutable history of claims and inspection; automated flags on eligibility
Carbon credits	Inflated statement of reduction	Measuring practices and outcomes multiple times	Public issuance record; retirement tracking to prevent double counting

(Source: Authors)

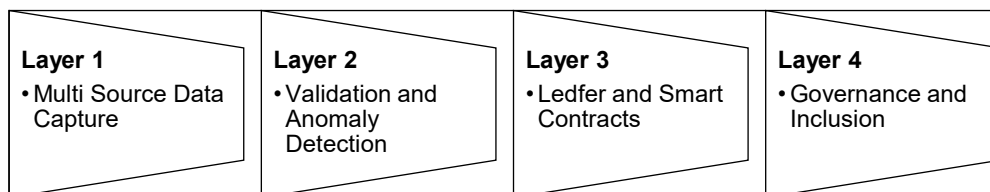


Figure 1: The multi-layer framework

(Source: Authors)

• **Layer 1: Multi-Source Data Capture**

The 1st layer of the framework focuses on data collection from multiple, independent sources, which do not have a common point of failure, thus creating a redundancy.

Information on factors like weather, moisture content of soil, machinery activity, storage conditions are recorded by devices implanted in the field. Observation regarding crop cover and phenology comes from the satellite. Certifiers and other 3rd parties like cooperatives and input suppliers confirm purchases and deliveries, while the certificates themselves can be recorded on a ledger through smart contracts (Dos Santos et al., 2021).

Redundancy is the most important point here. Multiple independent observations take place before a claim can be accepted; so, the fraudulent claim has to pass through multiple checks and the difficulty increases accordingly. In these, sources that can't be controlled by the claimant, like satellite coverage, are especially valuable.

- **Layer 2: Validation and Anomaly Detection**

The 2nd layer cross checks the different pieces of evidence against each other, as a step of due diligence; for example, it checks sensor readings against satellite indicators and regional weather data, or reviews time series data to find patterns; and finally assigns a confidence level to each record. There are various models for detecting anomalies, for example the model by Cheng et al. (2022), which have the ability to flag faults with sensors, and patterns that are suspicious, and send the flagged data for human review instead of being decided upon automatically. However, devices can also be attacked (Gupta et al., 2020), therefore, this layer also authenticates devices, source updates and tamper alerts.

So, the purpose of this layer is to directly address the oracle problem. Considering that the ledger can't improve the trustworthiness of the data, therefore, this layer focuses on making the data as trustworthy as possible before it is sent to the ledger.

- **Layer 3: Ledger and Smart Contracts**

The 3rd layer applies pre-set rules on the validated records. Since storing every reading on the platform is impractical considering the scalability and limits of storage as noted by Reyna et al. (2018), therefore, the bulk data is generally kept off the platform while key events and cryptographic fingerprints are kept on it. Smart contracts then get executed automatically when the pre-set conditions are met, like making payments on task completion, triggering insurance on index behavior or blocking collateral that is already pledged (Omar et al. (2023).

As suggested by Van Wassenae et al. (2021), a permissioned ledger governed by a consortium, like the Hyperledger Fabric, may be a better option than a public one when it comes to regulated finance. However, the choice would depend on who may need to read, write and audit the data and also on the level of interoperability that may be required, as, generally, the different stakeholders will have different systems (Bhat et al., 2022).

- **Layer 4: Governance and Inclusion**

The final layer takes care of system governance and decides on inclusion of different partners. It looks at matters like data ownership, data visibility rights, error and dispute resolution process, selection and accountability of data providers and validators, and support mechanism for farmers.

Research regarding data sharing shows that data ownership, incentives for sharing and privacy are important aspects to be handled for a participation to be sustainable (Durrant et al., 2021); Caldarelli and Ellul (2021) show that decentralized designs of data sourcing reduce dependency on a single provider. In this regard, Huang & Fu, (2023) and Singh et al., (2022) show that the perspectives of farmers must also be considered, since if the farmers can't afford or can't trust a system, that system will not generate reliable data.

Case Studies and Applications

- **Traceability-Linked Lending**

A very interesting set of related case studies focus on traceability of the product – providing production histories that are generally not available with the lender. Examples are like the RiceChain framework (Yakubu et al., 2022) and the Soyabean design of Salah et al. (2019), which record production and handling details on the platform, so that the participants can check the origin. Mao et al. (2018) and Ismail et al. (2023) describe comparable scenarios, discussing blockchain-based credibility checking in the food trade in Shandong and IoT-enabled model for fish chains respectively. In case of financial transactions in the agriculture domain, availability of a verified history of inputs, harvests and sales serves as evidence of creditworthiness for farmers in absence of formal collateral.

There are exceptions as well. The Tuna Case (Thorpe et al. 2022) provides an example where due to the systems being fragmented and not linked to each other, the individual records can't be trusted, and if the data ecosystem is not coordinated, even introducing a ledger can't add much value.

- **Index Insurance**

In Index insurance, payouts are dependent on the data and not on the claim assessment. This suits the proposed framework very well.

As per Afshar et al. (2021), a combination of satellite-derived phenology with crop models improves index performance. Considering this, Omar et al. (2021) proposed an approach to crop insurance based on blockchain, with smart contracts automating the insurance.

The catch here is again the input data. If the data feed is either manipulated or wrong, the automatic payout from the contract will also be wrong. This, again, is the oracle problem (Caldarelli & Ellul, 2021), highlighting the importance of the multiple data sources and cross validations as described in layers 1 and 2 respectively.

- **Area-Based Subsidies**

Henits et al. (2022) demonstrated that satellite imagery data from Sentinel-2 can be used to monitor Hungary's Single Area Payment Scheme and greening subsidies on a national level. Going by the suggested framework, the compliance flags derived from the satellite would be validated and then passed on to the platform along with the inspection history, and the audit trail would become reliable.

This proves that scaling the evidence layer up to the national level is possible, and the ledger can be made to provide the record and workflow behind its validation instead of the actual detection.

- **Carbon Crediting**

Carbon markets are both an opportunity and a risk.

Ballesteros-Rodríguez et al. (2024) studied tokenized carbon credits using the case of KlimaDAO and noted that it results in the process of issuance, transfer and retirement becoming transparent and prevents double counting of credits; however, it does not prove that the underlying reduction actually happened. In fact, Probst et al. (2024), found that only a handful of credits reflect real reductions, which is a failure in the measurement and verification process, and can't be rectified by simply maintaining a ledger.

Translated into the case of agricultural carbon, this indicates that the steps of evidence gathering through sensors and satellites and subsequent verification thereof as outlined in the 1st and 2nd layers of the proposed framework are important, and tokens can be issued only after these layers validate the measurements.

- **Coffee Value Chains: A Cautionary Case**

The Curious Case of Coffee is a caution.

Bager et al. (2022) noted that the existence of a blockchain platform in a coffee supply chain does not automatically make the system sustainable. This is because of factors like data quality at origin and human control on the system. Singh et al. (2022) documented and studied views of the coffee producers themselves on the technology. The conclusion was that priorities might differ between the data sources and the system designers.

Translated to financial transactions in the agriculture domain, there is a very direct lesson. If the farmers perceive the system as a surveillance tool instead of a support, both participation and data will be weak.

Discussion

- **What the Evidence Supports**

Three conclusions come out of the reviewed literature

- It is technically possible to have shared records where any tampering would become evident. This has been achieved for various commodities.

- Sensing at a large scale is also feasible, as was seen from the cases of satellite monitoring in Hungary, and also from index insurance.
- The weakest link is the credibility and quality of the data when it moves from the physical domain to that of the platform.

Therefore, the safest way is to put the ledger as the last step of verification, and execute the verification by combining blockchain, IoT and satellite evidence.

- **Adoption, Inclusion and Cost**

The technology used to close a gap for the lender can open one for the farmer, as already noted above through the curious case of coffee. Huang and Fu (2023) found that automatic participation of farmers in traceability systems can't be assumed. As noted by Zheng et al. (2023), it is rather like an evolution of supply chain actors, where the outcome depends on factors like incentives, cost and coordination that can be influenced by policy. This is because essentials like devices, connectivity and digital skills come at a cost, which the smallholder farmers may not be able to bear. Without cost sharing, an interface that is easy to understand and use, and transparent distribution of benefits, the system may end up being unable to include the very farmers who it was supposed to serve.

- **Security, Privacy and Interoperability**

Attackers can enter through every added device, as noted by Gupta et al. (2020); also, financial and location data are quite sensitive. Again, there would be conflicts between the data-protection rules on correction and deletion and the concept of immutability. Therefore, the systems should be designed so as to keep personal data out of the platform and record only the cryptographic fingerprints.

Interoperability is another concern, as enterprise blockchains are often not in a position to handshake with each other (Bhat et al., 2022), and data sharing protocols are still immature (Durrant et al., 2021).

To reduce lock-ins and lower costs, open standards are required for devices, data formats and ledger interfaces.

- **Challenges and Research Agenda**

A notable challenge here is that the study is conceptual and the literature reviewed is about prototypes, reviews and traceability applications. A few studies referred to focus on fraud reduction in lending or insurance scenarios, and the reported benefits may have publication bias.

Future research in this context may focus on approaches like field trials measuring the accuracy of fraud detection and the cost of false positives on the smallholder farmer, overall cost-benefit analyses for different farm sizes, test of data resilience against manipulation - even deliberate, process of certification of devices

and data providers, and regulatory process for acceptance of digital evidence in contracts relating to lending and insurance.

Conclusion

Frauds in agricultural finance increase when the reports of the farmers can't be verified by other stakeholders like lenders, insurers, agencies and buyers. Blockchain and IoT can handle this, but only when used along with each other and in a wider system environment. Tamper evident records and automated rules are provided by the blockchain platform, IoT and satellite data provide evidence, protection is taken care of by the analytics and governance ensures participation of farmers by providing fair terms.

The oracle problem is a major constraint since there is no authenticity proof of the data that comes to the ledgers. The cases studied show that traceability, scalability, insurance, monitoring – are all feasible and that acceptance and inclusion are equally important.

The approach, therefore, should be to treat the data ledger as the final verification step; first level investment should be towards capturing trustworthy data and involving farmers in the system design.

Researchers need to test these ideas in real business scenarios so that technology is able to support closing the trust gap through evidences instead of assumptions.

References

1. Afshar, M. H., Foster, T., Higginbottom, T. P., Parkes, B., Hufkens, K., Mansabdar, S., Ceballos, F., & Kramer, B. (2021). Improving the performance of index insurance using crop models and phenological monitoring. *Remote Sensing*, 13(5), Article 924. <https://doi.org/10.3390/rs13050924>
2. Alobid, M., Abujudeh, S., & Szűcs, I. (2022). The role of blockchain in revolutionizing the agricultural sector. *Sustainability*, 14(7), 4313. <https://doi.org/10.3390/su14074313>
3. Bager, S. L., Singh, C., & Persson, U. M. (2022). Blockchain is not a silver bullet for agro-food supply chain sustainability: Insights from a coffee case study. *Current Research in Environmental Sustainability*, 4, 100163. <https://doi.org/10.1016/j.crsust.2022.100163>
4. Ballesteros-Rodríguez, A., De-Lucio, J., & Sicilia, M. Á. (2024). Tokenized carbon credits in voluntary carbon markets: The case of KlimaDAO. *Frontiers in Blockchain*, 7, 1474540. <https://doi.org/10.3389/fbloc.2024.1474540>

5. Bhat, S. A., Huang, N. F., Sofi, I. B., & Sultan, M. (2022). Agriculture-food supply chain management based on blockchain and IoT: A narrative on enterprise blockchain interoperability. *Agriculture*, 12(1), 40.
<https://doi.org/10.3390/agriculture12010040>
6. Bosona, T., & Gebresenbet, G. (2023). The role of blockchain technology in promoting traceability systems in agri-food production and supply chains. *Sensors*, 23(11), 5342. <https://doi.org/10.3390/s23115342>
7. Caldarelli, G. (2020). Understanding the blockchain oracle problem: A call for action. *Information*, 11(11), 509. <https://doi.org/10.3390/info11110509>
8. Caldarelli, G., & Ellul, J. (2021). The blockchain oracle problem in decentralized finance—A multivocal approach. *Applied Sciences*, 11(16), 7572. <https://doi.org/10.3390/app11167572>
9. Cheng, W., Ma, T., Wang, X., & Wang, G. (2022). Anomaly detection for Internet of Things time series data using generative adversarial networks with attention mechanism in smart agriculture. *Frontiers in Plant Science*, 13, 890563. <https://doi.org/10.3389/fpls.2022.890563>
10. Dos Santos, R. B., Torrisi, N. M., & Pantoni, R. P. (2021). Third party certification of agri-food supply chain using smart contracts and blockchain tokens. *Sensors*, 21(16), 5307. <https://doi.org/10.3390/s21165307>
11. Durrant, A., Markovic, M., Matthews, D., May, D., Leontidis, G., & Enright, J. (2021). How might technology rise to the challenge of data sharing in agri-food? *Global Food Security*, 28, Article 100493.
<https://doi.org/10.1016/j.gfs.2021.100493>
12. Gupta, M., Abdelsalam, M., Khorsandroo, S., & Mittal, S. (2020). Security and privacy in smart farming: Challenges and opportunities. *IEEE Access*, 8, 34564–34584. <https://doi.org/10.1109/ACCESS.2020.2975142>
13. Henits, L., Szerletics, Á., Szokol, D., Szlovák, G., Gojdár, E., & Zlinszky, A. (2022). Sentinel-2 enables nationwide monitoring of Single Area Payment Scheme and greening agricultural subsidies in Hungary. *Remote Sensing*, 14(16), 3917. <https://doi.org/10.3390/rs14163917>
14. Huang, Y., & Fu, S. (2023). Understanding farmers' intentions to participate in traceability systems: Evidence from SEM-ANN-NCA. *Frontiers in Sustainable Food Systems*, 7, 1246122.
<https://doi.org/10.3389/fsufs.2023.1246122>
15. Ismail, S., Reza, H., Salameh, K., Kashani Zadeh, H., & Vasefi, F. (2023). Toward an intelligent blockchain IoT-enabled fish supply chain: A review and conceptual framework. *Sensors*, 23(11), 5136.
<https://doi.org/10.3390/s23115136>

16. Kaur, A., Singh, G., Kukreja, V., Sharma, S., Singh, S., & Yoon, B. (2022). Adaptation of IoT with blockchain in food supply chain management: An analysis-based review in development, benefits and potential applications. *Sensors*, 22(21), 8174. <https://doi.org/10.3390/s22218174>
17. Leung, H. W., Chapman, A., & Fadhel, N. F. (2021). Identifying food fraud using blockchain. In *Proceedings of the 6th International Conference on Internet of Things, Big Data and Security* (pp. 185–192). SciTePress. <https://doi.org/10.5220/0010423801850192>
18. Lin, W., Huang, X., Fang, H., Wang, V., Hua, Y., Wang, J., Yin, H., Yi, D., & Yau, L. (2020). Blockchain technology in current agricultural systems: From techniques to applications. *IEEE Access*, 8, 143920–143937. <https://doi.org/10.1109/ACCESS.2020.3014522>
19. Mao, D., Hao, Z., Wang, F., & Li, H. (2018). Innovative blockchain-based approach for sustainable and credible environment in food trade: A case study in Shandong Province, China. *Sustainability*, 10(9), 3149. <https://doi.org/10.3390/su10093149>
20. Omar, I. A., Jayaraman, R., Salah, K., Hasan, H. R., Antony, J., & Omar, M. (2023). Blockchain-based approach for crop index insurance in agricultural supply chain. *IEEE Access*, 11, 118660–118675. <https://doi.org/10.1109/ACCESS.2023.3327286>
21. Ordoñez, C. C., Gonzales, G. R., & Corrales, J. C. (2024). Blockchain and agricultural sustainability in South America: A systematic review. *Frontiers in Sustainable Food Systems*, 8, 1347116. <https://doi.org/10.3389/fsufs.2024.1347116>
22. Probst, B. S., Toetzke, M., Kontoleon, A., Díaz Anadón, L., Minx, J. C., Haya, B. K., Schneider, L., Trotter, P. A., West, T. A., Gill-Wiehl, A., & Hoffmann, V. H. (2024). Systematic assessment of the achieved emission reductions of carbon crediting projects. *Nature Communications*, 15(1), 9562. <https://doi.org/10.1038/s41467-024-53645-z>
23. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. *Future Generation Computer Systems*, 88, 173–190.
24. Salah, K., Nizamuddin, N., Jayaraman, R., & Omar, M. (2019). Blockchain-based soybean traceability in agricultural supply chain. *IEEE Access*, 7, 73295–73305. <https://doi.org/10.1109/ACCESS.2019.2918000>

25. Singh, C., Wojewska, A. N., Persson, U. M., & Bager, S. L. (2022). Coffee producers' perspectives of blockchain technology in the context of sustainable global value chains. *Frontiers in Blockchain*, 5, 955463. <https://doi.org/10.3389/fbloc.2022.955463>
26. Thorpe, A., Hermansen, O., Pollard, I., Isaksen, J., Failler, P., & Touron-Gardic, G. (2022). Unpacking the tuna traceability mosaic – EU SFPAs and the tuna value chain. *Marine Policy*, 139, Article 105037. <https://doi.org/10.1016/j.marpol.2022.105037>
27. Van Wassenae, L., Verdouw, C., & Wolfert, S. (2021). What blockchain are we talking about? An analytical framework for understanding blockchain applications in agriculture and food. *Frontiers in Blockchain*, 4, 653128. <https://doi.org/10.3389/fbloc.2021.653128>
28. Xiong, H., Dalhaus, T., Wang, P., & Huang, J. (2020). Blockchain technology for agriculture: Applications and rationale. *Frontiers in Blockchain*, 3, 462928. <https://doi.org/10.3389/fbloc.2020.00007>
29. Yakubu, B. M., Latif, R., Yakubu, A., Khan, M. I., & Magashi, A. I. (2022). RiceChain: Secure and traceable rice supply chain framework using blockchain technology. *PeerJ Computer Science*, 8, Article e801. <https://doi.org/10.7717/peerj-cs.801>
30. Zheng, Y., Xu, Y., & Qiu, Z. (2023). Blockchain traceability adoption in agricultural supply chain coordination: An evolutionary game analysis. *Agriculture*, 13(1), 184. <https://doi.org/10.3390/agriculture13010184>.

