A Blockchain Semantic-based Approach for Secure and Traceable Agri-Food Supply Chain

Boubakeur Annane
LRSD, Department of Computer Science, University Ferhat Abbas of Setif-1, Algeria
boubakeur.annane@univ-setif.dz (corresponding author)

Adel Alti
Department of Management Information Systems and Production Management, College of Business and Economics, Qassim University, Saudi Arabia | LRSD, Department of Computer Science, University Ferhat Abbas of Setif-1, Algeria
a.alti@qu.edu.sa

Abderrahim Lakehal
LRSD, Department of Computer Science, University Ferhat Abbas of Setif-1, Algeria
lakehal.adbderrahim@univ-setif.dz

Received: 3 September 2024 | Revised: 4 October 2024 | Accepted: 12 October 2024

ABSTRACT

Ensuring food security is crucial for maintaining food quality and enhancing consumer services by guaranteeing both safety and satisfaction. However, traditional methods to ensure food security are often susceptible to various forms of fraud and require significant processing overhead, making them inefficient for the evolving demands of modern food supply chains. To address these shortcomings, blockchain technology has emerged as a robust and efficient solution to enhance food security. This paper presents a novel lightweight blockchain-based signature mechanism designed for the rapid detection of food fraud. It also includes a domain-specific ontology to serve as a structured knowledge model, allowing systematic analysis and detection of different types of fraud within the food supply chain. This approach uses smart contracts built on lightweight blockchain technology to initiate and manage transactions related to food fraud. Then, semantic rules are applied to detect and identify fraudulent activities. Once fraud is detected, associated transactions are encrypted and tracked, ensuring visibility and traceability among consortium members. Experimental results based on large-scale transaction data demonstrated ~7.5× speed improvement over iterative search algorithms while maintaining high transaction traceability and significantly reducing storage costs.

Keywords-food security; lightweight blockchain; ontology; traceability; food fraud detection

I. INTRODUCTION

The expansion of transportation and digital economies is driving the emergence of many innovations. A sector that is growing rapidly is the agricultural supply chain [1]. Advanced technologies with expanding control capabilities are introduced to ensure the delivery of high-quality food and services to consumers. As e-agricultural supply chains for various food products evolve, the issue of fraud detection has become more prominent. However, these supply chains face numerous challenges, such as new forms of fraud, and inefficiencies, including monopolization, price manipulation, and ingredient tampering [2]. It is crucial to address these obstacles from different angles and actively seek effective solutions to alleviate them. Food fraud involves intentionally misrepresenting food products for financial gain using deceptive strategies to provide inaccurate information on labels and engage in counterfeiting. It can result in financial losses, undermine consumer confidence, and create potential health risks. Recently, blockchain and the Internet of Things [3-5] have emerged as automated solutions to ensure anticounterfeiting in the food supply chain. A blockchain-based ontology and the IoT offer a promising approach to improve traceability, transparency, and security within the food supply chain.

Researchers have begun to explore the integration of IoT with blockchain and ontologies to monitor the origins of products [6-19]. This integration promises to track the location, condition, temperature, and other parameters of agricultural products and to enhance food security by leveraging blockchain's decentralized nature. However, despite these advances, the integration of IoT within blockchain-based ontologies remains an emerging area of research with significant challenges. Previous studies have proposed various frameworks to incorporate IoT into blockchain supply chain systems. For example, in [13] traditional blockchain and IoT technology were combined to secure the pharmaceutical supply chain. However, some frameworks [16-18] often rely on simple static smart contracts without any semantic enrichment or flexibility. Despite the widespread use of ontologies to depict domain-specific rules in various technologies such as the IoT, their incorporation into blockchain is limited. Ontologies offer a formal way to describe domain knowledge, providing structured representations of concepts and relationships. Recent studies have explored the potential of using ontologies in supply chain platforms. For instance, in [19], an ontology model was proposed to identify fraud in halal food products. However, these efforts have primarily focused on the ontology itself, rather than on the blockchain that governs the smart contracts. Combining blockchain technology with ontology offers great advantages in improving food fraud detection. However, the implementation of this approach raises important ethical concerns, particularly regarding privacy. This involves the sensitivity of data related to products, suppliers, and locations, potentially exposing proprietary practices to unauthorized individuals and allowing attackers to identify specific persons or businesses through advanced analytical methods. Additionally, there are security concerns related to supply chain data and food transactions, as attackers can exploit smart contracts, resulting in unintended or fraudulent consequences. This misuse of data collected through IoT and stored on a blockchain could occur in ways that were not originally expected.

To our knowledge, no previous research has explored the use of blockchain and ontologies to ensure accurate and context-aware fraud detection that can adapt to new fraudulent behaviors. This gap in the literature motivated this research to leverage the benefits of ontologies and blockchain in developing a semantic secure framework for a traceable supply chain. The goal is to offer an innovative and secure framework to address the growing issue of food fraud in new ways by integrating food fraud ontology with blockchain technology. This study contributes to the field of food security by introducing several crucial advances: (i) Leverages ontology to enrich the semantics of data, which aids in identifying food frauds, (ii) ensures that only authorized users are permitted to enter data into the system, thereby preventing unauthorized access and enhancing food safety and fraud prevention measures, (iii) defines individuals' rights to view and utilize these data, thereby preserving privacy, and (iv) evaluates the proposed approach using real food and agricultural transactions in Algeria, in terms of traceability and execution time, demonstrating its effectiveness in detecting fraud within the agricultural supply chain.

II. FOOD FRAUD ONTOLOGY MODEL

The food fraud ontology, FraudOnto, conceptualizes knowledge within the agricultural supply chain domain, focusing primarily on food fraud detection modeling. The ontology was designed to facilitate reasoning, unify existing fraud detection models, and share previous consumption experiences to enhance the overall understanding of fraud prevention in the supply chain. FraudOnto is a knowledge model for analyzing frauds.

A. Ontology Description Model

FraudOnto defines key concepts and their interrelationships to support all food fraud detection and traceability preservation activities. Figure 1 provides an overview of the ontology structure, highlighting the following concepts:

- The *Product* represents a product tracked in the supply chain. It defines various categories of products.
- The *Acrigole-actor* defines all entities involved in the supply chain, including customers, suppliers, retailers, and farmers.
- The *Consumer* purchases products.
- The *Supplier* is a business supplying a product. Two types of suppliers are distinguished: wholesale suppliers and agricultural suppliers.
- The *Retailer* is a business selling products to consumers.
- The *Farmer* is a business producing food products.
- The *Farm Location* represents the location of a farm.
- The *Farm Supplier* is a supplier providing products to a farm.
- The *Transaction* denotes purchase and sale transactions.
- The *Fraud* represents products involved in fraudulent activities. Two types of fraud exist in the supply chain: *Storage-distribution-production* including falsification of invoices, alteration of labels, etc., and *Manufacturing-packaging-products* including alteration of certificates, violation of contracts, etc.

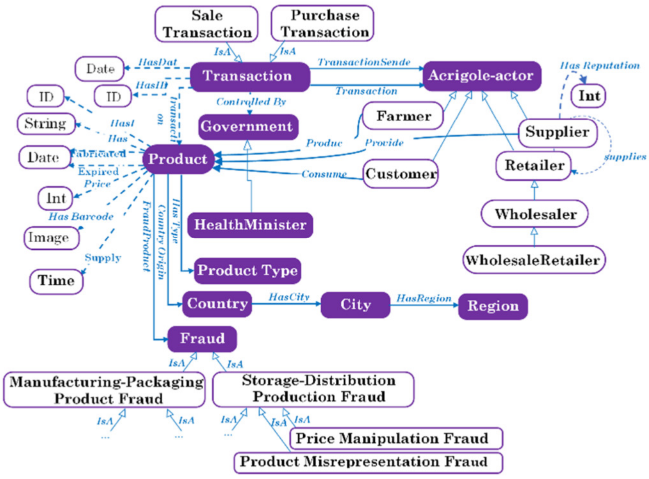


Fig. 1. An overview of the ontology model.

B. Ontology Fraud Detection Rules

The fraud food ontology defines a set of rules to ensure food safety and provide a food-checking service for consumers.

Rule 1: Looking for the country of origin indicated on the product label is different from the country where the product is generally manufactured, flag the product for further investigation, as this could indicate a potential attempt of food fraud. This rule is formalized in First-Order Logic (FOL) as follows:

$$\texttt{Product(p)}\wedge\texttt{Country\_Origin\_Product(p, }c_1\texttt{)}\ \wedge\texttt{Country\_Manufactured\_Product (p, }c_2\texttt{)}\ \wedge\texttt{(c1} \neq \texttt{c2)} \rightarrow \texttt{Food\_Fraud (F)}$$

Rule 2: When the price of the product is significantly lower than the average market price for similar products, perform additional checks to verify its authenticity and quality, as this could suggest a possible substitution or adulteration. This rule is described as follows:

```
Product(p)^Price_Product(p, price)
^Avg_Market_Price_Product(p, avg_p)
^(price < avg_p) →
Authenticity_Quality(p)
```

Rule 3: When a product is labeled as "organic" but contains prohibited or synthetic substances, then classify the product as non-compliant and investigate possible fraud in the organic certification process. This rule can be described as follows:

```
Product(p)^Type_Product(p,"organic")
^Product_Ingredients(p, "proh")
→ Organic_Certification_Fraud(F)
```

III. BLOCKCHAIN SEMANTIC-BASED SECURE AGRI-FOOD SUPPLY CHAIN SYSTEM

A secure and robust platform for tracking food and agricultural products throughout the supply chain is essential to promote high-quality food and ensure complete food traceability. This study integrates lightweight blockchain technology with domain ontology to create a secure and traceable supply chain management system aimed at improving transparency and building trust in the supply chain.

A. General Architecture

The secure and traceable supply chain management system, shown in Figure 2, consists of the following components: (1) Sender, (2) Blockchain, (3) Food Fraud Detection Agent, (4) Indexer Ontology Agent, (5) Indexer Ontology Agent, and (6) Recipient.

The *Sender* defines the *prover* (i.e., farmers, manufacturers, importers, wholesalers, delivery companies, retailers, sellers) and the *Issuer* (i.e., ministry of commerce, ministry of agriculture, and ministry of health) that must prove that they have the right to carry out a transaction. A transaction involves adding a product, supplied by the prover, and selecting the receiver for the transfer. Alternatively, it may be an operation of issuing a signature that represents a digital certificate for the product by the *Issuer*. *Blockchain* is a technology for storing and transmitting information in a secure, transparent, and decentralized manner. It operates as a distributed ledger that records transactions chronologically and immutably. The *Food Fraud Detection Agent* is an intelligent agent that uses ontology-based reasoning to detect and prevent food fraud. The *Indexer Ontology Agent* operates on a block containing a set of validated transactions. Each block is linked to the previous one using a cryptographic hash function, thus forming a chain of blocks. This ensures data integrity and creates an immutable structure where any modification of a block requires the modification of all subsequent blocks. The *Recipient* refers to a verifier user (i.e., agents of the fraud control and repression inspection, customs officials, police, etc.) who must demonstrate its authorization to determine whether the blockchain conforms to the fraud ontology class.

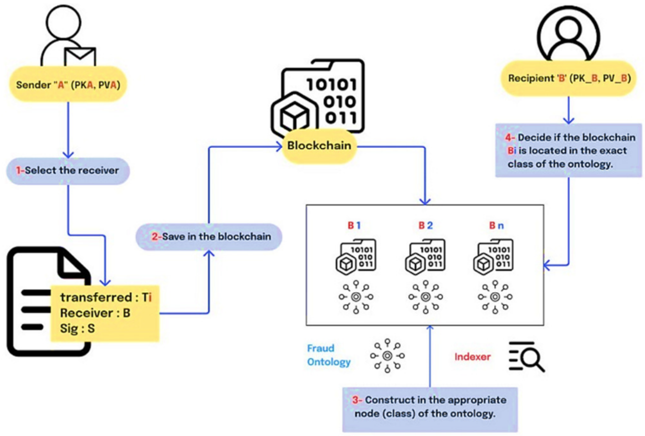

Sender "A" (PKA, PVA)
Blockchain
10101
010
011
Recipient 'B' (PK_B, PV_B)
1-Select the receiver
2-Save in the blockchain
4- Decide if the blockchain Bi is located in the exact class of the ontology.
transferred : Ti
Receiver : B
Sig : S
B 1
B 2
B n
Fraud Ontology
Indexer
3- Construct in the appropriate node (class) of the ontology.

Fig. 2. System general architecture.

B. Lightweight Blockchain

Blockchain is a remarkable innovation technology that has significantly enhanced integrity and security across various sectors [14]. With the help of blockchain technology, food safety and traceability can be ensured, ensuring consumer health and maintaining trust in the supply chain. In this technology, advanced cryptographic principles are used to ensure data integrity and confidentiality [15]. This can allow stakeholders to track products from the farm to the table, ensuring that all parties have access to accurate and up-to-date information.

To achieve fast encryption and decryption, it is essential to use simple, robust, and lightweight functions. Time-based One-Time Passwords (TOTP) have recently gained prominence in secure online transactions due to their excellent performance in various segmentation tasks. By employing TOTP as a key on both the sender's and the receiver's side, security can be significantly enhanced. To protect the transaction details from attackers for a limited duration, it is crucial to ensure that the code is highly secure. The following mathematical function can be used to generate 16-byte random different numbers in the range $[0,\ 2^m - 1]$:

$$X_{n+1} = (a\,X_n + b)\,mod\ 2^m \qquad (1)$$

where a, b, and m are integer values. It is simple to provide an initial odd number X_0, $n = 31$, $a = 65539$, and $b = 0$. Equation (1) provides an integer between 0 and 2^{31}-1, which can then be normalized to fall within the range (0, 1).

When the sender wants to add a new transaction using his device, he authenticates using his email and password. Then he specifies the product details, the receiver, and his current location. If the credentials are valid, the system prompts the user to add transactions with one-time passwords (OTPs). The system creates a secret key of 6 digits for the user and displays it in a QR code format in the mobile device or the computer web browser. The user scans the QR code or manually enters the security key. The security key is used to sign transaction details and insert them into a blockchain, adding fraud checking (i.e., origin, quality, product size, product type, storage and packaging conditions, and conformity).

The indexer records block identifiers in the appropriate leaf nodes according to the transaction's address or location. This signature is then verified against the secret key generated to confirm the integrity of the transaction. Additionally, a certificate is generated using a smart contract. The system generates a six-digit code to access the transaction from the blockchain. When the system runs, it generates a new six-digit code every 30 seconds. This code, known as an OTP, is used by the user for authentication and transaction certification. This method is used to retrieve, update, and sign the transaction.

C. Protocol Used for Securing Agricultural Supply Chain

The proposed protocol must ensure anonymity between different interacted components, including the sender, receiver, the government, and the indexer. Additionally, the system needs to ensure complete transparency, allowing all connected parties to access transaction hashes. Figure 3 describes the sequence diagram of the tasks performed in the following steps:

1. The process starts with the sender's login page to enter the user identifier and password. It also provides specific information about the transaction T_i.
2. The OTP system generates a secret code and sends it to the sender's mobile device (SK_i).
3. The system takes as input the sender's secret key SK_i, adds transaction T_i belonging to sender i to the blockchain, and calls the fraud detection function to automatically check the fraud food detection rules based on FraudOnto.
4. The food fraud detection agent verifies food fraud detection, and depending on its result, the transaction T_i will have an index in the ontology or not. This function broadcasts a message to the other nodes and returns both the transaction hash and ID.
5. The system generates a certificate to document the findings. This certificate is then indexed and stored in the ontology model for future reference.
6. The system starts the search of the transaction from the top of the ontology and then proceeds to the i^{th} region of the ontology by applying a reasoning search condition. The retrieved address is transmitted to the *Indexer*.

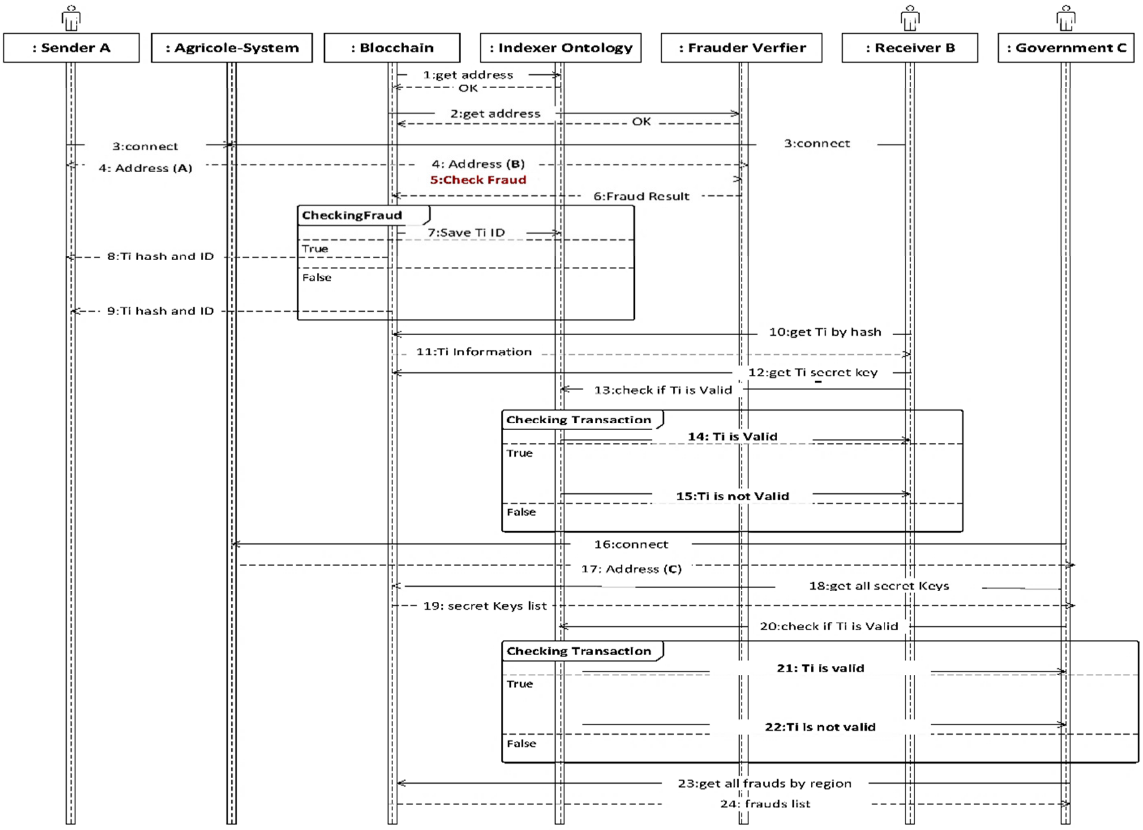
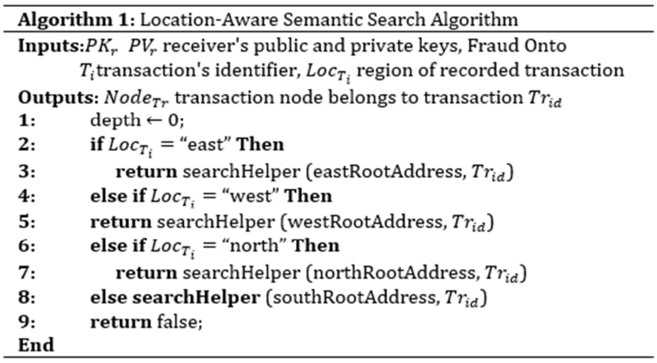


Fig. 3. Sequence diagram of the proposed protocol.

7. When the indexer ontology agent requests the certificate linked to the transaction, the system sends a query to the blockchain. This process is automated using a smart contract, ensuring secure retrieval of the certificate. After the certificate is obtained, it is sent back to the *Indexer*.
8. The system then decrypts the hash and searches for transactions that belong to a receiver in the ontology, following the procedure in Figure 4, and returns the transaction information. If the indexer does not find any transaction, it notifies the receiver to change the transaction identifier.

The following example illustrates the proposed approach. A shipment of olive oil labeled "organic" is currently in transit within the supply chain having been marketed. The proposed system aims to verify organic classification by utilizing data from ontology and blockchain. Initially, the system collects data on temperature, humidity, and other environmental factors to ensure that the product is being transported in compliance with organic standards. Subsequently, ontology rules and smart contracts are used to compare the recorded data type (e.g., "type: non-organic") with the ontology rules (e.g., organic products should not be linked with non-organic fertilizers). This comparison triggers an automatic alert for potential fraud on the blockchain. All participants in the supply chain, such as producers, retailers, and the government, receive real-time alerts through the decentralized blockchain network.



```
Algorithm 1: Location-Aware Semantic Search Algorithm
Inputs:$PK_r$, $PV_r$ receiver's public and private keys, Fraud Onto
        $T_i$transaction's identifier, $Loc_{T_i}$ region of recorded transaction
Outputs: $Node_{T_r}$ transaction node belongs to transaction $Tr_{id}$
    depth ← 0;
    if $Loc_{T_i}$ = "east" Then
        return searchHelper (eastRootAddress, $Tr_{id}$)
    else if $Loc_{T_i}$ = "west" Then
    return searchHelper (westRootAddress, $Tr_{id}$)
    else if $Loc_{T_i}$ = "north" Then
        return searchHelper (northRootAddress, $Tr_{id}$)
    else searchHelper (southRootAddress, $Tr_{id}$)
    return false;
End
```

Fig. 4. Pseudocode of searching transaction-based location-aware semantic algorithm.

IV. IMPLEMENTATION AND VALIDATION

The proposed approach was implemented using the Docker and Ganache frameworks to perform blockchain operations on an NVIDIA GeForce GPU with an Intel Core i5 CPU. The blockchain parameters are configured with a maximum gas limit of 6721975 per block. To reduce gas fees, events 4.3 were used, which store data in the blockchain network instead of smart contracts.

A. Dataset

The experimental results are based on a large dataset consisting of 1000 transactions related to the food supply chain. This dataset contains transactions and their details including product type, origin country, date of purchase, and quality parameters. Transactions also include data related to the locations of both suppliers and customers, allowing analysis of business agreements. Furthermore, random sampling was performed to detect fraudulent activities in the products.

B. Results and Discussion

The computational complexity and storage cost of the proposed approach were compared with the iterative search, as shown in Table I. The iterative search involves examining each transaction sequentially in a systematic manner until the requested transaction is located. As seen in Table I, the proposed approach achieves the lowest computational complexity of $Log_2(T)$ across different transaction numbers while maintaining a storage space of $2n \times 128$ bytes, where T is the number of transactions compared to the iterative search.

TABLE I. COMPLEXITY AND STORAGE COST COMPARISON

Method	Computational complexity	Storage cost
Iterative search	O(T)	$n \times 128$ bytes
Proposed approach	Log$_2$(T)	$2n \times 128$ bytes

Then, to explore the influence of the number of transactions on search time, the number of transactions was varied. Figure 5 shows the performance of the proposed semantic indexing method and the iterative search method. The stable search time of the proposed method is around 9 ms. On the iterative search method, a high computation time was observed, reaching 150 ms for 100 transactions. The search time increases slowly with the proposed method as the number of transactions increases.

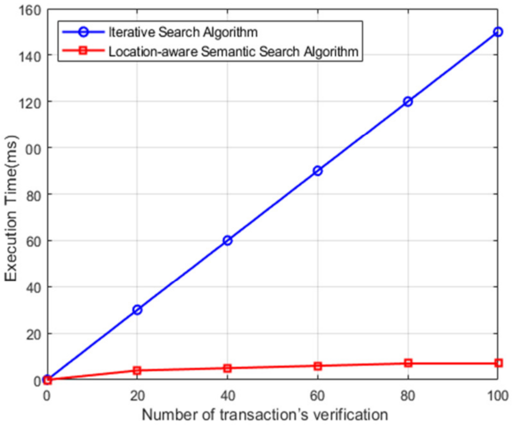


Fig. 5. Searching time between iterative search and the proposed system.

In addition, the proposed method was compared to traditional secure techniques in terms of the number of fraudulent transaction propagation and mitigation. Figure 6 shows a comparison between the proposed and another traditional secure method. From this figure, it is evident that for the proposed system, the number of frauds is limited and low compared to the traditional secure approach. The semantic indexing of different types of fraud allows the reuse of inference effects, leading to higher accuracy due to the limited range of specific frauds and their features. This demonstrates the effectiveness of the proposed system in reducing fraudulent transactions and improving traceability.

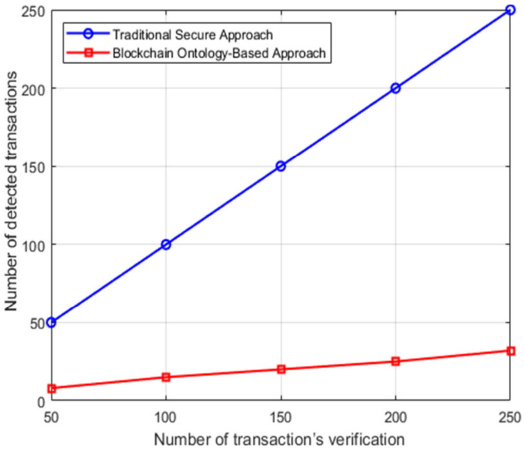


Fig. 6. Traceability between traditional secure techniques and the proposed blockchain ontology system.

From Table I and Figures 5-6, it is evident that the proposed blockchain ontology-driven security approach enables faster search times for specific transactions compared to traditional security methods. Therefore, blockchain ontology promotes interoperability across diverse systems through ontology reasoning, reducing the propagation of fraudulent activities while enhancing accuracy, providing end-to-end traceability, and facilitating the identification of fraud sources to prevent their recurrence. This approach offers a more efficient, secure, and transparent solution for food fraud detection, outperforming existing approaches that utilize blockchain without including semantic data descriptions. In the future, certain issues such as the complexity of maintaining the ontology, limited scalability, and performance imbalances need to be addressed.

V. CONCLUSION

Food fraud is extremely important due to the potential impact of newly emerging fraudulent activities on food supply chains. Previous research on this topic has been limited, failing to effectively address context-aware fraud detection and adapt to evolving fraudulent behaviors. This study presented a blockchain semantic-based approach to efficiently detect food fraud in agricultural supply chains. It introduced a novel method driven by blockchain ontology rules, enabling more accurate and context-sensitive fraud detection that can adapt to emerging fraudulent activities. The experimental results, based on a large number of transactions, demonstrated that the proposed approach improved security, traceability, and fast search time in the food supply chain by combining blockchain with ontology, thus facilitating the detection and prevention of fraud. Future work should exploit the integration of privacy-preserving technologies, such as homomorphic encryption, into the blockchain-ontology framework. Another interesting endeavor would be to develop GAN models to analyze blockchain transaction data and detect unknown attacks.

ACKNOWLEDGMENT

The researchers would like to thank the Deanship of Scientific Research, Qassim University, KSA for funding the publication of this project.

REFERENCES

[1] H. Rana, M. U. Farooq, A. K. Kazi, M. A. Baig, and M. A. Akhtar, "Prediction of Agricultural Commodity Prices using Big Data Framework," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12652–12658, Feb. 2024, https://doi.org/10.48084/etasr.6468.

[2] R. Thirukumaran, V. K. A. Priya, V. Raja, S. Nimbkar, J. A. Moses, and C. Anandharamakrishnan, "Blockchain Technology and Advancements in the Agri-food Industry," *Journal of Biosystems Engineering*, vol. 49, no. 2, pp. 120–134, Jun. 2024, https://doi.org/10.1007/s42853-024-00221-4.

[3] S. Arora, S. Oberoi, T. Nabi, and B. Verma, "How does blockchain impact sustainable food security? Insights from literature review," *International Journal of Information Management Data Insights*, vol. 4, no. 2, Nov. 2024, Art. no. 100276, https://doi.org/10.1016/j.jjimei.2024.100276.

[4] Y. Lu, P. Li, and H. Xu, "A Food anti-counterfeiting traceability system based on Blockchain and Internet of Things," *Procedia Computer Science*, vol. 199, pp. 629–636, Jan. 2022, https://doi.org/10.1016/j.procs.2022.01.077.

[5] S. Balamurugan, A. Ayyasamy, and K. S. Joseph, "IoT-Blockchain driven traceability techniques for improved safety measures in food supply chain," *International Journal of Information Technology*, vol. 14, no. 2, pp. 1087–1098, Mar. 2022, https://doi.org/10.1007/s41870-020-00581-y.

[6] A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," *Journal of Network and Computer Applications*, vol. 68, pp. 90–113, Jun. 2016, https://doi.org/10.1016/j.jnca.2016.04.007.

[7] R. M. A. Latif, M. Farhan, O. Rizwan, M. Hussain, S. Jabbar, and S. Khalid, "Retail level Blockchain transformation for product supply chain using truffle development platform," *Cluster Computing*, vol. 24, no. 1, pp. 1–16, Mar. 2021, https://doi.org/10.1007/s10586-020-03165-4.

[8] V. Maritano *et al.*, "Anticounterfeiting and Fraud Mitigation Solutions for High-value Food Products," *Journal of Food Protection*, vol. 87, no. 4, Apr. 2024, Art. no. 100251, https://doi.org/10.1016/j.jfp.2024.100251.

[9] S. V. S. Kumar, V. S. Avinash, and S. Govri, "Tracking of Food Products from Source to consumption, Enhancing Transparency and Food Safety using Blockchain," in *2024 International Conference on Inventive Computation Technologies (ICICT)*, Lalitpur, Nepal, Apr. 2024, pp. 1573–1578, https://doi.org/10.1109/ICICT60155.2024.10544559.

[10] A. Susanty, N. B. Puspitasari, Z. F. Rosyada, M. A. Pratama, and E. Kurniawan, "Design of blockchain-based halal traceability system applications for halal chicken meat-based food supply chain," *International Journal of Information Technology*, vol. 16, no. 3, pp. 1449–1473, Mar. 2024, https://doi.org/10.1007/s41870-023-01650-8.

[11] N. N. Ahamed and P. Karthikeyan, "FLBlock: A Sustainable Food Supply Chain Approach Through Federated Learning and Blockchain," *Procedia Computer Science*, vol. 235, pp. 3065–3074, Jan. 2024, https://doi.org/10.1016/j.procs.2024.04.290.

[12] S. Datta and S. Namasudra, "Blockchain-based secure and scalable supply chain management system to prevent drug counterfeiting," *Cluster Computing*, vol. 27, no. 7, pp. 9243–9260, Oct. 2024, https://doi.org/10.1007/s10586-024-04417-3.

[13] M. N. *et al.*, "Secure pharmaceutical supply chain using blockchain in IoT cloud systems," *Internet of Things*, vol. 26, Jul. 2024, Art. no. 101215, https://doi.org/10.1016/j.iot.2024.101215.

[14] B. Annane, A. Alti, and A. Lakehal, "Blockchain based context-aware CP-ABE schema for Internet of Medical Things security," *Array*, vol. 14, Jul. 2022, Art. no. 100150, https://doi.org/10.1016/j.array.2022.100150.

[15] S. S. Taher, S. Y. Ameen, and J. A. Ahmed, "Advanced Fraud Detection in Blockchain Transactions: An Ensemble Learning and Explainable AI Approach," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12822–12830, Feb. 2024, https://doi.org/10.48084/etasr.6641.

[16] A. Hassoun *et al.*, "Food traceability 4.0 as part of the fourth industrial revolution: key enabling technologies," *Critical Reviews in Food*

Science and Nutrition, vol. 64, no. 3, pp. 873–889, Jan. 2024, https://doi.org/10.1080/10408398.2022.2110033.

[17] N. Rane, S. Choudhary, and J. Rane, "Blockchain and Artificial Intelligence (AI) Integration for Revolutionizing Security and Transparency in Finance." Social Science Research Network, Nov. 17, 2023, https://doi.org/10.2139/ssrn.4644253.

[18] D. K. Vora, J. H. Patel, D. Shah, and P. Mehta, "Application of Blockchain in Different Segments of Supply Chain Management," in *Sustainable Advanced Computing*, 2022, pp. 537–548, https://doi.org/10.1007/978-981-16-9012-9_43.

[19] S. F. M. Hashim, J. Salim, S. A. M. N. M. Noah, and W. A. W. Mustapha, "Ontology-Based Traceability System for Halal Status of Flavour: A Conceptual Framework," *Malaysian Journal of Information and Communication Technology (MyJICT)*, pp. 65–77, Dec. 2023, https://doi.org/10.53840/myjict8-2-97.