CTU Journal of Innovation and Sustainable Development
ISSN 2615-9422 | e-ISSN 2815-5602

DOI:10.22144/ctujoisd.2023.043

A practical blockchain-based framework for anti-counterfeiting and traceability

Ho Dac Hung, Vo Van Len, Nguyen The Bao, Nguyen Cao Hoai Phuong, and Tran Van Huu*
Institute of Engineering and Technology, Thu Dau Mot University, Viet Nam
**Corresponding author (huutv@tdmu.edu.vn)*

Article info.

Received 18 Jul 2023
Revised 18 Sep 2023
Accepted 3 Oct 2023

Keywords

Anti-counterfeiting, blockchain-based, traceability

ABSTRACT

Blockchain has features that help systems overcome the inherent limitations of traditional centralized approaches. Integrating blockchain technologies into systems to improve security, privacy, and transparency is a prominent trend. Currently, consumers are very concerned about the origin and the legitimacy of the products, so it is necessary to strengthen anti-counterfeiting and traceability in product management. Many theoretical approaches have been proposed recently. In this study, we propose a practical framework based on blockchain that supports anti-counterfeiting and traceability. Based on the proposed practical framework, we implemented a pattern as a proof-of-concept of the approach. We conduct experiments at Thu Dau Mot University, a pioneer in the production and transfer of biotechnology. The results show feasibility and good results regarding the proposed practical framework. Moreover, we also published our code base to GitHub with an open license.

1. INTRODUCTION

As a key element of the bitcoin cryptocurrency, blockchain technology initially emerged in the recent decade. A distributed network of nodes with specialized storage, communication, and consensus mechanisms to maintain synchronous copies of the ledger is what a blockchain is. Incorporating blockchain into systems to improve security, privacy, and transparency is a prevalent trend. Currently, consumers are increasingly demanding traceability and anti-counterfeiting measures to ensure their food is authentic. Anti-counterfeiting is a problem that is becoming worse and demands the use of solid, trustworthy techniques to confirm the authenticity of products all along the food chain. Blockchains are effective instruments for preventing food fraud by verifying, for instance, the geographic and biological origin of the product. Using blockchain technology to standardize food authentication concerns has given rise to many techniques. With the aid of blockchain technology, all parties may examine a product's complete history and current location, for instance. Technology also makes everything transparent for everyone involved. Blockchain technology generates a certain level of credibility that helps the sector become more sustainable by permanently keeping data. The blockchain network can be broadly divided into two types: public networks and private networks. On a public network, every node can join an open distributed ledger network like that in Nakamoto (2008), and any two peers can conduct transactions there without the need for any kind of authorization from a central authority. On the other hand, in private networks (Androulaki et al., 2018), if there is no rationale for on-chain governance, the consortium administrator or certificate authority decides who may join the network as a validator node or listener node. All nodes are pre-authenticated, and other nodes operating on the same network and in the same consortium are aware of their identities—at the very least, the controller is. As a proof-of-concept for the approach, we implemented a pattern at Thu Dau Mot University that respects the practical framework. The findings show the feasibility of the proposed practical framework.

The study is organized as follows: Section 2 presents related work; Section 3 presents the proposed practical framework; Section 4 presents the compatibility evaluation experiments; Section 5 presents conclusions, and directions for future research.

2. RELATED WORK

Currently, there are many studies showing the application of blockchain in various fields including, but not limited to manufacturing (Islam and Cullen, 2021; Sumathi et al., 2021; Chen et al., 2022; Lee et al., 2023), education (Panagiotidis, 2022), social network (Huynh et al., 2023), Internet of Things (Ma et al., 2020; Chen et al.,2020), finance (Swami and Arage, 2022), food (Islam and Cullen, 2021), and healthcare (Sumathi et al., 2021; Swami and Arage, 2022).

A blockchain-based application system, especially the blockchain can be Bitcoin-based or Ethereum-based (Ma et al., 2020). The main goal of implementing blockchain is to ensure the items are authentic and traceable.

It’s easy to see that the author (Panagiotidis, 2022) analyzed some studies of blockchain applications for education, which show the features and advantages of blockchain technology in the educational sector. The authors (Huynh et al., 2023) share some reviews and analysis methods of blockchain-based in the metaverse which is a popular social network. In addition, this study shows some good reviews of blockchain on key-enabling technologies in the metaverse, and it’s more important than the use of blockchain in the metaverse in the future.

A problem that many studies mention is the use of blockchain technology to develop a system where customers can undertake product traceability to anti-counterfeiting. Anthonya et al. (Lee et al., 2023) proposed a model that can trace every item’s creation and transactions, ensuring every product exists as an authentic one, but this model only showed the relationship between the manufacturer, seller, and consumer. This system was built by the Ethereum blockchain at an acceptable cost. Similarly, (Chen et al., 2022) undertook the analysis of specific processes in the supply chain such as Brand Party, Product Manufacturer, Material Supplier, Product Distributor, and Logistics Provider will form a consortium blockchain, together with the Third-Party Verify Organization, Blockchain Center, Consumers, and Deliveryman. Then blockchain technology applies to the complete production and distribution history of luxury products, allowing third parties to verify this. However, the cost of this proposed scheme is quite high because it includes computational cost and communication costs. In another sector, Swami and Arage (2022) propose a management system for pharmaceutical distribution using blockchain-based in real-time, and here, Ethereum is employed for the medicine supply chain management system. This has a distribution chain including manufacturers, suppliers, wholesalers, distributors, and pharmacists.

To save the cost, we would like to propose a practical framework that builds upon open-source projects. A proof-of-concept respecting the proposed practical framework has been built and evaluated at Thu Dau Mot University. Moreover, we also publish our proof-of-concept to GitHub with an open license.

3. PROPOSED APPROACH

3.1. Architecture

Based on multi-tier architecture, we propose a design with basic layers, including applications, web services, product identity flow services, Hyperledger, and data layers (Figure 1). This design will serve the user groups related to the product identity management system. The components are described as follows:

– User groups related to the system include but are not limited to organizations, certifying agencies, suppliers, retailers, shipping units, service providers, and customers. Each user can take the role of a node in the blockchain network.

– The applications pool includes applications related to supply chain management systems. Users can use private keys and web services provided by the web service layer to build applications that perform queries or invoke the ledger. The applications pool may contain some queuing applications to proactively receive data (Apache Kafka).

– Web services provide APIs that allow users to use private keys to make calls to smart contacts to query or invoke the ledger.

– Product identity flow services are smart contracts that implement the actual product identity flows of the institutions.

– Certifying agencies issue accounts and private keys for users to join the network, and provide certification of new technologies and products that the organization wants for business.

– Hyperledger stores data for product traceability. We propose IBM Hyperledger fabric (Androulaki et al., 2018).

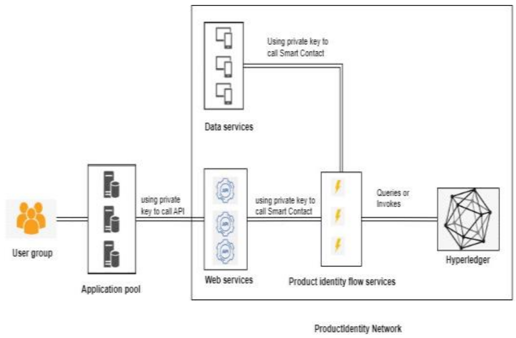


Figure 1. Proposed overall architecture

In design, blockchain acts as both a place to store data as NoSQL and as a place to execute operations as smart contracts. This is because modern blockchains are all enterprise blockchains and have evolved, not merely transaction storage, like the first version. Node spread and consensus mechanism between nodes are key to ensuring privacy, security, and transparency. Smart contracts can include multiple parties to confirm the constraints, which will clearly improve fraud resistance.

3.2. Product identity flow

The proposed blockchain network stores 3 types of data structures, such as user, technology, and product, described as follows:

User{userName, hashPassword, fullName, address, phone, logo, type}

Technology{key, name, register, registrationDate, certifyingAgency, status}

Product{key, name, image, description, price, techKey, producer, owner, transfer, status}

In this study, we build an anti-counterfeiting and original product traceability system based on blockchain technology (Hyperledger Fabric) and use a cryptographic hashing algorithm (bcrypt)[15] to secure the user's account during authentication. The product identity flow is shown in Figure 2.

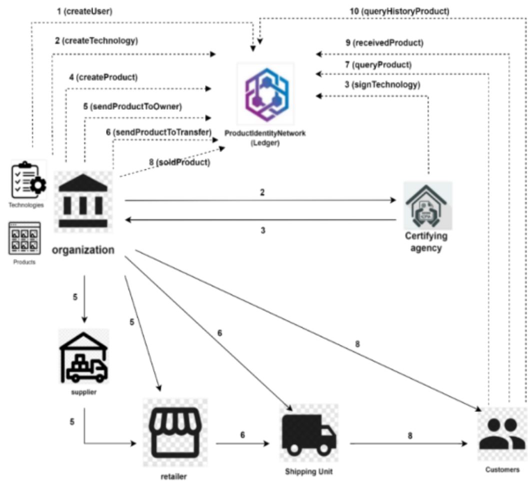


Figure 2. System flow diagram

Product Identity Network is a blockchain network that allows organizations participating in the network to register user accounts with username and password. The system will return proof of identity and a public/private key pair to each party.

Certifying agency (IP VIETNAM) is the state agency that grants certification of new production technology to the organization.

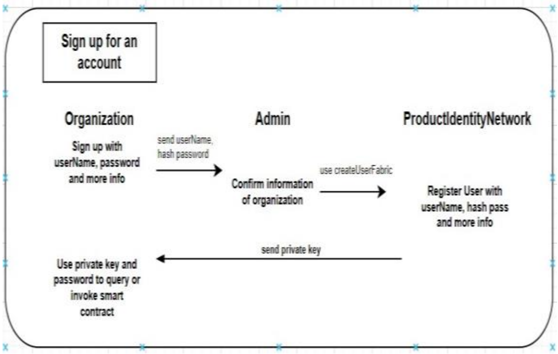
Supplier receives products from manufacturers and distributes products to retailers.

Retailer receives products from suppliers and sells products to customers.

Customers can query the origin of products via a barcode from Blockchain Network, identifying fake goods. Customers can place orders, query the shipping process, as well as confirm receipt of goods on the Blockchain Network.

The product identity flow is realized through the following steps:

Step 1. Organizations taking part in the network must register a user account with a username and password and the organization's credentials. The system administrator (Admin) verifies the information is correct and registers the account with a password after using the cryptographic hashing algorithm bcrypt (Provos and Mazieres, 1999) to the Blockchain network. The system will send the private key to the organization. The types of organizations participating: universities, companies, retailers, suppliers, carriers, certification bodies, and customers, amongst others.



Organizations that query or invoke data into the ledger must call the smart contract we defined in Table 1 with their private key. Moreover, to increase the security of the account, we propose an authentication mechanism that combines the private key and hash password in the smart contract according to the following principles:

```
async SmartContact(ctx, hashPassLogin,....)
{
    let hashPass =ctx.clientIdentity.getAttributeValue("hashPass");
    if(hashPassLogin != hashPass)
        throw new Error("Authentication failed!!!");
    //Execute  query or invoke to the ledger
}
```

Role 1. Authentication mechanism

Step 2. Organizations can register a new technology called smart contract createTechnology according to the following algorithm.

```
async createTechnology(ctx,hashPassLogin,nameTech,userNameCA,registrationDate)
{
    //Authentication by role 1
    //Check userNameCA exist
    let userName =ctx.clientIdentity.getAttributeValue("userName");
    const newTechnology = {
        key: ctx.stub.getTxTimestamp(),
        nameTech,
        register: userName,
        registrationDate,
        userNameCA,
        owner: userName,
        status:'waitingforgranted',
        docType: 'technology',
    };
    //Invoke newTechNology in legder
    ...
}
```

An organization calls a smart contract sendTechnology to transfer technology to another unit and can only transfer technologies that the organization has registered and licensed by the Certifying agency.

Step 3. Organizations can create products based on their licensed proprietary technology and write the product information to the ledger by invoking the createProduct flow described:

```
async createProduct(ctx, hashPassLogin, productID, techKey, name, image, description, price)
{
    //Authenticate by role 1
    const technology = await queryTechnologyByOwner(ctx, techKey);
    const user = ctx.clientIdentity.getAttributeValue("userName");
    const product = {
        key: 'p'+ctx.stub.getTxTimestamp(),
        productID, techKey, name, image, description, price,
        producer: user,
        owner: user,
        transfer: '',
        status: 'available',
        docType: 'product',
        history:user,
    };
    //Invoke newProduct in ledger
    ...
}
```

The organization uses its private key and licensed technology to create a new product. From the private key, the smart contract will validate the organization's username and update the producer, owner, and history fields. The manufacturer can provide products available to distributors and retailers by invoking the sendProductToOwner flow which will then update the owner and history for the product. The history field stores information about all the organizations that manufacture and distribute the product. And the seller will call the soldProduct flow to update the sold status of the product. The customer can check the origin of the product by invoking the queryProduct flow. If the owner does not match the seller or the product is sold out, it is fake. If the product quality is poor, customers can trace the production and distribution of the product through the history field.

Product identity flows heavily rely on the smart contracts. In this study, we propose corresponding flows as shown in Table 1.

4. RESULTS AND DISCUSSION

We deployed the system on a PC with a 7th generation core i5 CPU with 16GB RAM and 200GB SSD. The experiment, we established was based on the design with a Hyperledger Fabric blockchain including 20 nodes to run the following product identity flow in Ubuntu 20.04.

The user logs in to the system using the username, password, and private key provided according to Figure 3. The system administrator will verify the information and provide an account with the private key for the organization taking part in the network according to Figure 4. Organizations can register new technologies and products for VIETNAM IP according to Figure 5. IP VIETNAM licenses new technologies and products to the organization according to Figure 6. Customers can check product information by scanning barcodes via phone as shown in Figure 7.

Table 1. Corresponding flows in the proposed framework

#	Flow	Type
1	createUserFabric	invoke
2	createTechnology	invoke
3	queryTechnology	query
4	queryTechnologiesByOwner	query
5	queryTechnologiesSign	query
6	signTechnology	invoke
7	sendTechnology	invoke
8	createProduct	invoke
9	queryProduct	query
10	queryProductsByOwner	query
11	sendProductToOwner	invoke
12	sendProductToTransfer	invoke
13	bookedProduct	invoke
14	soldProduct	invoke
15	receivedProduct	invoke
16	queryHistoryProduct	query

Organizations can register We check the system's performance including 20 nodes to run the following flows "*createTechnology, createProduct, signTechnology, sendProductToOwner, soldProduct, and queryProduct*". We conduct experiments with the network configuration parameter "*{BatchTimeout: 0.1s, MaxMessageCount: 10, AbsoluteMaxBytes: 99 MB, PreferredMaxBytes: 512 KB }*" in the file configtx.yaml (Androulaki et al., 2018). The latency is seen in Table 2.

The flow queryProduct basically reads the data from Hyperledger at nodes without performing any update operation so it takes the smallest average latency. The flow createTechnology and signTechnology perfume write new technology information with few data fields on the ledger so it takes a higher average latency. The flow createProduct and sendProductToOwner write new product information with multiple data fields on the ledger and performs multistakeholder verification including external systems so it takes the highest average latency. About the flow soldProduct perform find and update the status product to sell, so the latency is as low as the flow queryProduct. The average latency is less than or equal to 1 second so this result is acceptable in practice.

We run the flows in the particular order: createTechnology, signTechnology, createProduct, sendProductToOwner, soldProduct. Corresponding to each type write 200 blocks to the ledger according to interface 6. And the sellProduct flow that writes the most blocks is 88 blocks/minute. And the flow createProduct and sendProductToOwner writes the least blocks is 63 blocks/minute.

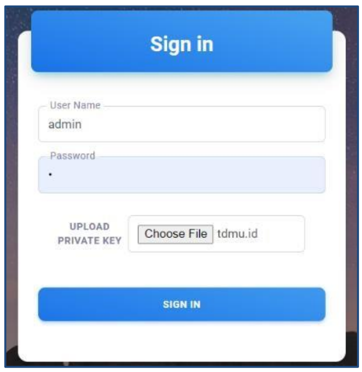


Figure 3. Log in UI

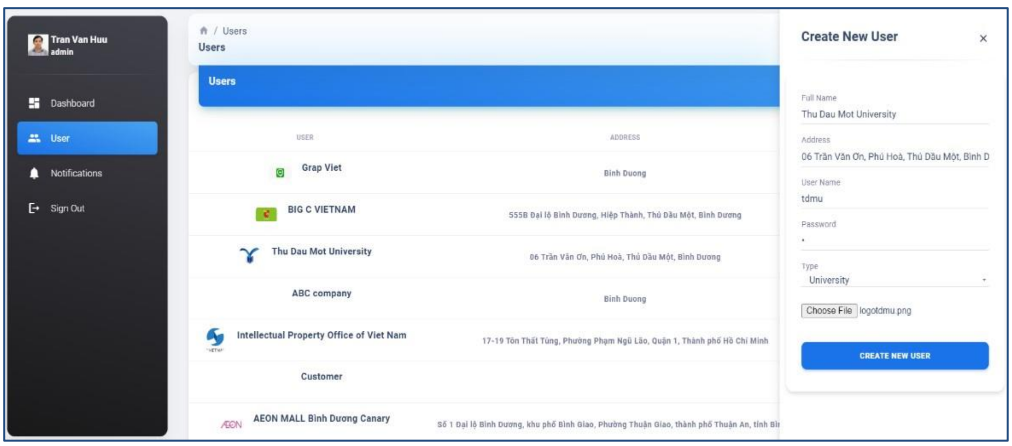


Figure 4. User management UI

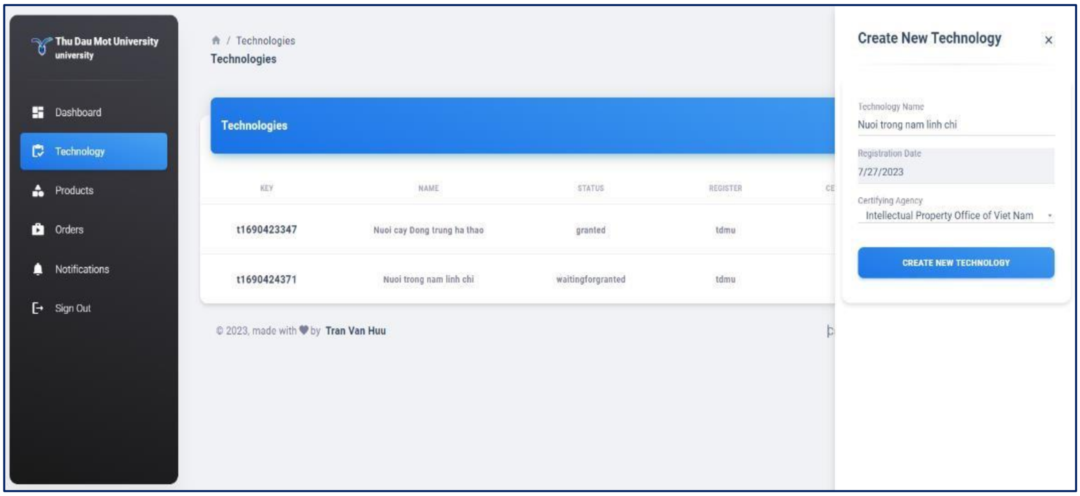


Figure 5. Technology management UI

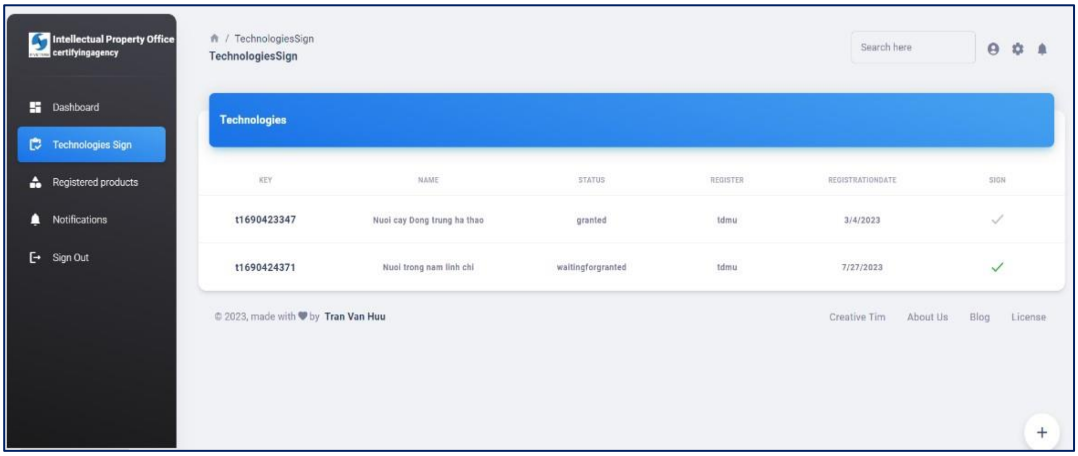


Figure 6. Technology signature UI

Figure 7. Check product UI

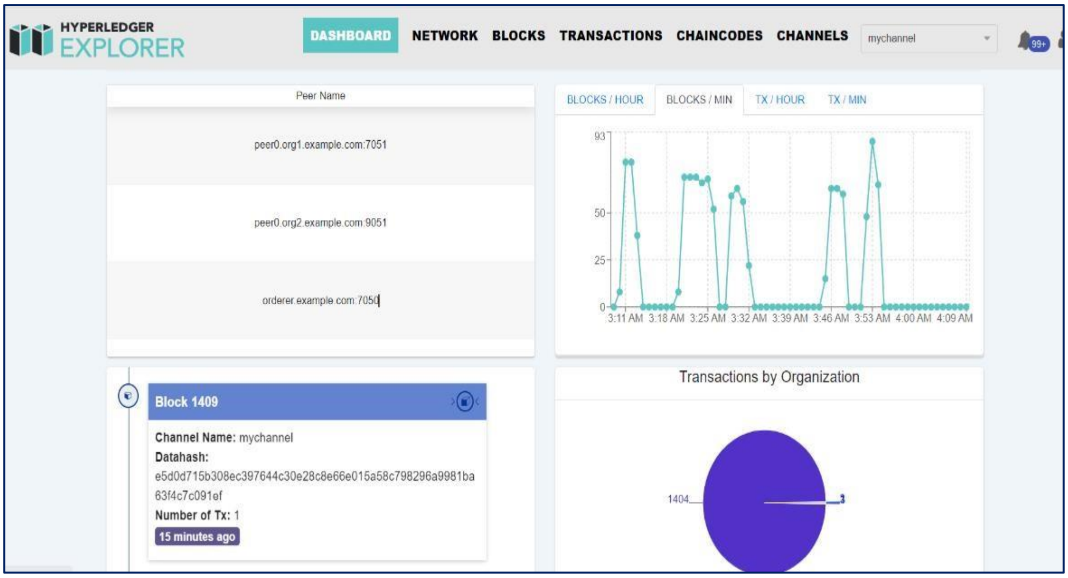


Figure 8. Hyperledger Fabric portal

Table 2. Latency of typical flows in the proposed framework

#	Flow	Type	Min Latency (s)	Max Latency (s)	Average Latency (s)
1	createTechnology	invoke	0.65	1.02	0.78
2	signTechnology	invoke	0.73	1.21	0.88
3	createProduct	invoke	0.83	1.65	1.02
4	queryProduct	query	0.46	0.70	0.53
5	sendProductToOwner	invoke	0.81	1.38	0.94
6	soldProduct	invoke	0.36	0.90	0.68

5. CONCLUSION

Applying blockchain to the product identity management system is an approach that improves privacy, security, and transparency. Users who join the network require both a private key and a password. User security is ensured by specific roles. Moreover, the system provides a web service layer that allows organizations to build their own applications that can read and write the ledger. Deployment does not require too many devices. Experimental results show the feasibility of the approach with an acceptable latency. In the future, we aim to present the scale mechanism to make the framework more sustainable in terms of performance.

REFERENCES

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. *In Proceedings of the thirteenth EuroSys conference* (pp. 1-15).

Chen, C. L., Deng, Y. Y., Li, C. T., Zhu, S., Chiu, Y. J., & Chen, P. Z. (2020). An IoT-based traceable drug anti-counterfeiting management system. *IEEE Access*, *8*, 224532-224548.

Chen, C. L., Guo, L. H., Zhou, M., Tsaur, W. J., Sun, H., Zhan, W., ... & Li, C. T. (2022). Blockchain-Based Anti-Counterfeiting Management System for Traceable Luxury Products. *Sustainability*, *14*(19), 12814.

Huynh-The, T., Gadekallu, T. R., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q. V., ... & Liyanage, M. (2023). *Blockchain for the metaverse: A Review. Future Generation Computer Systems*.

Islam, S., & Cullen, J. M. (2021). Food traceability: A generic theoretical framework. *Food Control*, *123*, 107848.

Lee, M. C., Pearl, R. R., Edbert, I. S., & Suhartono, D. (2023). Developing an anti-counterfeit system using blockchain technology. *Procedia Computer Science*, *216*, 86-95.

Ma, J., Lin, S. Y., Chen, X., Sun, H. M., Chen, Y. C., & Wang, H. (2020). A blockchain-based application system for product anti-counterfeiting. *IEEE Access*, *8*, 77642-77652.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system. Decentralized business review*.

Panagiotidis, P. (2022). Blockchain in Education--The Case of Language Learning. *European Journal of Education (EJE)*, *5*(1), 66-83.

Provos, N., & Mazieres, D. (1999). Bcrypt algorithm. *In USENIX*.

Sumathi, D., Poongodi, T., Balusamy, B., Himani, B., & KP, F. K. (Eds.). (2021). *Convergence of blockchain technology and E-business: concepts, applications, and case studies*. CRC Press.

Swami, A. H., & Arage, C. S. (2022). Smart Contract Using Blockchain For Safely Managing The Pharmaceutical Industry Record. *Journal of Pharmaceutical Negative Results*, 10232-10240.