Blockchain technology: Comparisons, consensus models, supply chain case study using blockchain

Ahmed Jafar, Khaled Elabbani and Mustafa Mohammed - Collage of Computer Technology Benghazi.
Akram. Gihedan - Derna university

ABSTRACT

In the world of information technology, blockchain technology is a relatively new method. Blockchain-based applications are gaining traction in a variety of industries, including financial services, supply chain management, and the creation of immutable data backups, among others. Many people know blockchain on the scale of cryptocurrency. Blockchain is a decentralized ledger that allows transactions to take place in an unchangeable method. Blockchain is a decentralized ledger system that handles data and transactions using time-stamped blocks and cryptography. It works across a computing network in a decentralized way. Blockchain-free solutions are being developed by IT companies for usage in a variety of areas. These solutions have produced extremely positive results in a variety of disciplines, particularly those that assist the economy. The issues surrounding blockchain technology will be discussed in this paper, as well as a case study supporting Libya's marine resources in the future.

Keywords: Blockchain, Cryptography, Supply chain, Consensus model.

الملخص

التطور المستمر في علوم الحاسوب وتكنولوجيا المعلومات وظهور تقنيات جديدة، حيث تعتبر تقنية سلسلة الكتل التي تعرف بمصطلح (**Blockchain**) من التقنيات الرائدة في العديد من المجالات والتطبيقات المالية وسلاسل التوريد والصانعات، وإنشاء نسخ احتياطية من البيانات غير قابلة للتغيير مما يضيف إليها خاصية الوثوقية والاستدامة، وحيث اشتهرت واستخدمت تقنية سلسلة الكتل على نطاق العملات الرقمية المشفرة كعملة البيتكوين كدفتر أستاذ لامركزي يسمح للمعاملات أن تتم بطريقة غير قابلة للتغيير حيث يعمل بطريقة لامركزية لحفظ البيانات، أسفرت هذه الحلول عن نتائج إيجابية للغاية في الكثير من التخصصات، لا سيما تلك التي تساعد الاقتصاد وتطويره حيث ستتم مناقشة القضايا المحيطة بتكنولوجيا سلسلة الكتل في هذه الورقة، بالإضافة إلى دراسة حالة لدعم الموارد البحرية الليبية في المستقبل.

Introduction

Recently, the rapid development of technology and the volume of data available on the Internet has increased, which has become a mainstay for the use of data processing and analysis applications for companies and governments. The demand for the use of

Internet of Things technology has also increased and with the continuous growth of the network of physical devices connected to the Internet, a moreover, Significant increase in the use of smart devices, however, in **2025** the volume of data will reach to **180** Zettabytes on the Internet [1].

In view of the above, security and privacy have become a challenge and an important element in the transfer of large data and information in cloud systems, especially if they are used over the Internet. In addition to the element of trust that cloud systems lose due to their exposure to many attacks in various applications such as financial system, supply chain management, agriculture and healthcare [2]. Blockchain is a technology that is effective in not relying on the centralization of traditional databases, which do not depend on one place when storing, also considered one of the solutions when using applications that require privacy and trust, and obtaining strong security. Blockchain technology is working on changes in all Fields that include sharing applications and cooperation that lack trust between them, and other advantages in following up on decentralized transactions between multiple parties, enhancing security and privacy and reducing costs [3].

Today, blockchain has a great impact in fields that depend on the exchange of information and decentralization of the database and participates in decision-making and is not limited to digital currencies as many people think and promote it from the media. [4]. Increasing the world's dependence on the use of globalization, with the widespread use of individuals and institutions for electronic services and Internet applications, etc. In the last decade, we have also witnessed the interest of researchers in the fields of artificial intelligence, the Internet of things and cloud computing, with a leap in addressing the topic of blockchain.We have decided to present the proposal of the topic of blockchain in Libya as a future idea and how to benefit from this technology. As we know that the State of Libya has a long coastline, it has not received much interest from the Libyan State and there is no complete control over marine resources. Libya also depends on the supply of frozen meat without following up on the source and supplier. For this, it is possible to take advantage of blockchain technology in the future supply chain in Libya, which gives confidence, guarantee and protection that starts from the supplier to the consumer and contributes to improving the Libyan economy. This paper is organized as follows: Section **2** and **3** definition and background; Section **4** Block Structure; Section **5** comparison between blockchain and database; Section **6** blockchain types; Section **7** Consensus Models ; Section **8** supply chain management; Finally Libyan marine resources supply chain case study.

Blockchain definition

Blockchain is the largest open and distributed digital record regardless of the type of data. In other words, it is not just limited to financial data. It allows the transfer of ownership from one party to another at the same time without an intermediary between them, while achieving a high degree of security and privacy for the transfer process against fraud or manipulation attempts [5]. Data cannot be changed without the permission of the legal quorum of the parties. If someone tries to change the data, all participants will be notified and they will know who is attempting. Involved in this record of all individuals around the world. Blockchain can currently be considered the largest decentralized ledger distributed globally among individuals [6].

Blockchain background

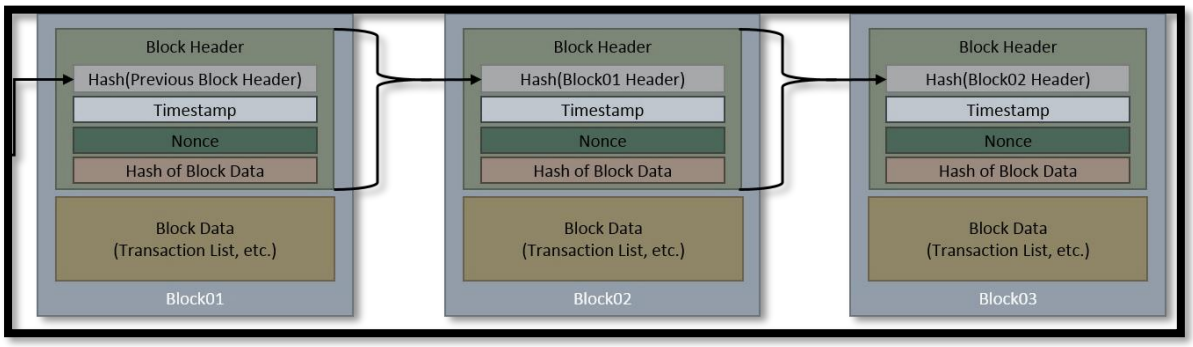
The name Satoshi Nakamoto appears in the majority of articles on blockchain technology, as basic ideas related to blockchain technology first surfaced in the early 1990s. In **1989**, Leslie Lamport created the Paxos protocol. The protocol was first published in **1998** [7]. It presents a consensus approach for obtaining a decision in a network of computers if the computers or network are unreliable. A signed chain of information was utilized as an electronic ledger for digitally signing papers in **1991**, with the ability to quickly prove that none of the signed documents in the collection had been modified [8].

In **1991**, a way to safeguard electronic records was presented. Haber and Stornetta's method is based on time stamping and connecting hashes of documents to prevent manipulation with the system [9]. Blockchain was first used in **2008** by Nakamoto. Blockchain became very popular with its first appearance, as the main platform for the virtual currency of Bitcoin, which derives its strength and the trust of the dealers in it thanks to this system. It has also been used in many other applications, such as property registration and transaction documentation [10].

Block Structure

A block is made up of two parts: a block header and block data. Metadata block is contained in the block header. A list of authenticated and validated transactions that have been committed to the blockchain network is contained in the block data [11]. Block Header contained the block number, the previous block header hash value. A hash representation of the block data, the timestamp, and the size of the block [12]. The data block consists of ledger events included within the block as shown in **Fig (1)**.

Fig (1) Block Structure



Compare between Blockchain and Database

The key point difference between a blockchain and a database is the degree of centralization which is presented in fig **(2)**. While all records are protected in a central database, each participant in the blockchain has a secure copy of all records, as shown in table **(1)**, which was gathered from different sources[3,13].

Fig (2) Centralized Database and Blockchain

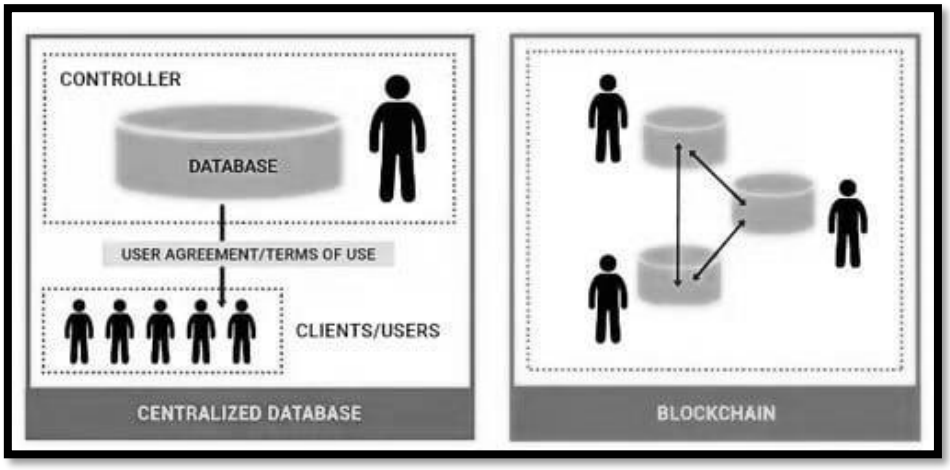


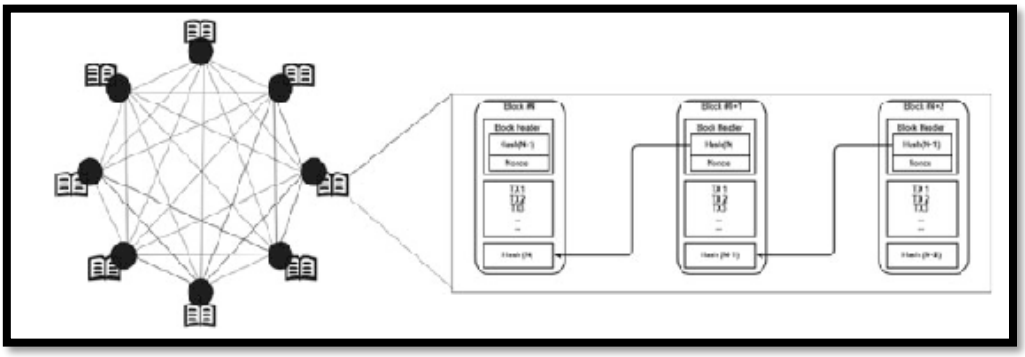
Table (1) Comparison: Blockchain and Database

Feature	Blockchain	Database
Requires administrator	No administration, Blockchain is decentralized, distributed among nodes.	Has administration and centralized.
Operations data	Read and append-only by the users.	Support operation: Create, Read, Update, and Delete **(CRUD)**.
Performance speed	Slow to reach consensus.	Fast execution.
Protection	Use cryptographic.	Use access control.

Data access control	No permissions, anyone can reach.	Accessed after permission has been granted.
Records History	There is a history of records with identification of the owner of the property.	No history records.
Transfer of ownership	No intermediation between parties.	Intermediation is allowed.

Blockchain is a data-storage and-transmission system. It uses a peer-to-peer network **(P2P)** to enable safe and transparent communication between nodes without the requirement for a central control authority. Every node has its copy of the database, which is referred to as the ledger. Data is organized into blocks, with each block having a hash code that links it to the one before it [7]. Blockchain architecture shown in Fig. **3**. Blockchain consists of a set of the following elements: **P2P** network, a distributed ledger, consensus mechanisms and cryptography.

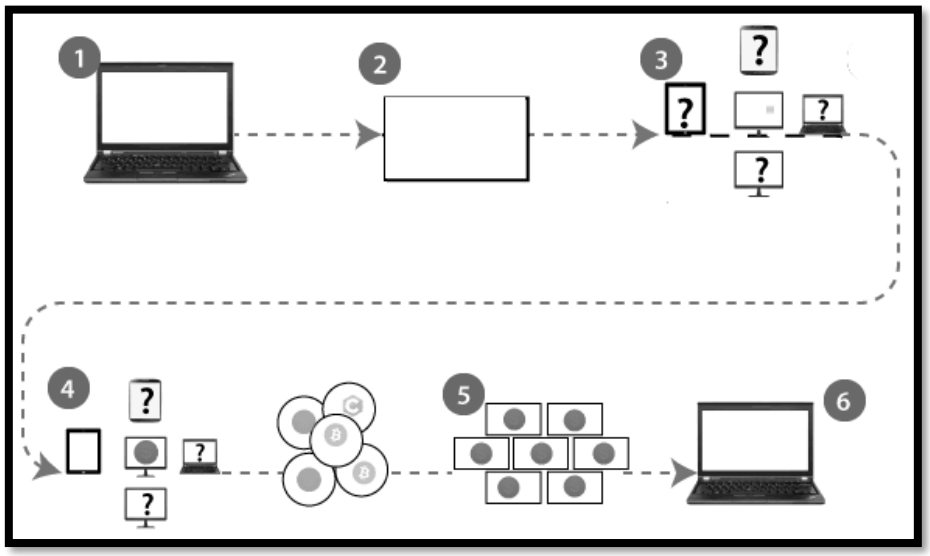
Fig (3) Blockchain architecture



In **[3]** the following stages illustrate how the blockchain works as shown in Fig.**4**:

1. In the network, users a request transaction. Contracts, cryptocurrencies, or information records could be involved in the transaction.
2. A block in the network has to be used to represent the transaction request.
3. The block is distributed to every node in the network.
4. Each participant analyzes and validates the received block from the network.
5. The consensus algorithm is used to validate the blocks, then the new block is added to the network.
6. Complete the transaction.

Fig (4) Working mechanism of Blockchain



Blockchain Types

Blockchain is characterized by consensus, distributed computation, immutability, and authentication. It is applied in a variety of applications and different methods. Blockchain techniques are categorized into three types: public, private and consortium.

Public Blockchain

Public chain is a permissionless ledger, which is considered an open-source technology. Joining the network does not necessitate any permissions. Due to the immutable nature of the records, public blockchain functions in trustless networks. In this blockchain system, whole records are broadcast, and everyone is participating in the process of confirming and authenticating transactions. Bitcoin and Ethereum are examples of public blockchain [14].

Private Blockchain

A centralized network is referred to as a private blockchain. Blocks are encrypted with a private key, and no one can read them. Only authorized users have access to them. One group has complete authority, and only members of that organization are involved in the process of reaching a consensus. Fabric, Quorum, and Hyperledger are examples of private blockchain [15].

Consortium Blockchain

Consortium blockchain is a semi-decentralized and semi-private structure. Several entities control and govern this blockchain system, which is partially decentralized because only a few pre-selected groups of nodes are chosen to participate in the decision-making process [3].

The consortium chain works with a limited number of parties with the same permissions and does not depend on the open system, in which everyone has permission to verify the blocks or one party as a closed system. The consortium chain works with a limited

number of parties with the same permissions and does not depend on the open system, in which everyone has permission to verify the blocks or one party as a closed system, across different organizations [16]. In following Table 2 illustrates the differences between blockchain Types.

TABLE (2) blockchain Types comparison

.Attributes	Public	Private	Consortium
Consensus determination	All nodes	Single organization	Some identified nodes
Access	Allowed read and write to all	High access limit	Relatively lower access limit.
Stability and Immutability	Unchangeable	Could be changeable	Could be changeable
Efficiency	Low	High	High
Consensus process	Permissionless	Permissioned	Permissioned

Consensus Models

It's a method for adding blocks to a structure. To add a new block to the blockchain network, all nodes reach an agreement. Consensus models are used in blockchain technology to allow a group of users that are distrustful of each other to collaborate. In the following, several of the most consensus models will be illustrated.

Proof of work (PoW)

This algorithm is commonly utilized in the mining process. Miners are working to solve the problem that will allow them to add a block. The hash of the minor is agreed upon by the network nodes, and the block is added to the network. This methodology is used to validate transactions and produce new blocks for the blockchain [7]. To solve the problem, you'll need a lot of processing power. PoW is a consensus approach employed on Ethereum, and Hashcash is an element of the bitcoin mining process [15].

Proof-of-stake (PoS)

This algorithm validates the block based on the amount of money invested by the participants. PoS algorithms were established largely to address the drawbacks of PoW algorithms, such as high energy consumption during mining operations. As a result, PoS is a more energy-efficient alternative than PoW [14]. To replace the usual mining operation of PoW algorithms, an alternate technique utilizing users' shares in the virtual money is adopted. Simply explained, instead than investing a particular amount in, say, mining equipment, the user might use that money to acquire similar block generation

possibilities by rising as a validator by investing in the coin share. PoS saves more energy and is more efficient than PoW. Unfortunately, because the cost of mining is so low, assaults may occur as a result [9].

Practical byzantine fault tolerance (PBFT)

PBFT is a replication technique that can survive Byzantine faults. It works by reaching an agreement even when nodes in the network fail. This method focuses on node failure, taking into account both broken and functioning nodes [7]. This method is based on the Byzantine Generals' Problem. By taking the proper values of working nodes and applying the default vote value to the problematic nodes, fault tolerance may be accomplished. As a result, the network agrees on the proper values. The main distinction between PoS and Delegated proof of stake (DPoS) is that PoS is a direct democratic system, whereas DPoS is a representative democratic system. Stakeholders choose who will produce and validate blocks [14].

Delegated PoS (DPoS)

Larimer developed DPoS, a decentralized consensus algorithm. To counteract the negative impacts of centralization, it adds a layer of technical democracy [9]. To achieve decentralized voting, it employs a reputation system and is based on an election procedure. The fundamental concept is to designate a group of delegates (also known as witnesses) to protect the network on behalf of the other shareholders. Delegates take turns randomly constructing blocks [7]. The block might be verified rapidly, allowing transactions to be completed rapidly. A delegate's reputation is lost if he or she fails to correctly build a block. As a result, shareholders might withdraw their votes in favor of that delegate and replace him or her with another. Furthermore, consumers need not be concerned about dishonest delegates because they may quickly be voted out. DPOS is Bitshares' foundation. The primary distinction between PoS and DPOS is that PoS is a direct democratic system, whereas DPOS is a representative democratic system [14].

Proof of Elapsed Time Consensus Model (PoET)

The PoET model, which was developed open-sourced by Intel, utilizes both permissionless and permissioned blockchains in a probabilistic transaction finality. It has no entry fee and is extremely scalable. Each publishing node receives requests under this model. This assists in handling the consensus algorithm's open-ended involvement of nodes and untrusted nodes. The publishing node software will get a random wait time generated by the secure hardware time source [7]. The publishing nodes take the random time allotted to them and become idle for that amount of time. When a publishing node awakens from an idle state, it generates and publishes a block to the blockchain network, notifying other nodes of the new block. Any publishing nodes that are still waiting will stop waiting, and the process will begin again. This approach necessitates the use of a random time since if the time to wait was not chosen

at random, a malicious publishing node would simply wait the shortest time possible to gain control of the system. This paradigm also necessitates ensuring that the publishing node waits the appropriate amount of time before starting. This assists in dealing with the consensus algorithm's open-ended involvement of nodes and untrusted nodes [15]. Table 3 provides a comparison of different consensus algorithms using some common Attributes.

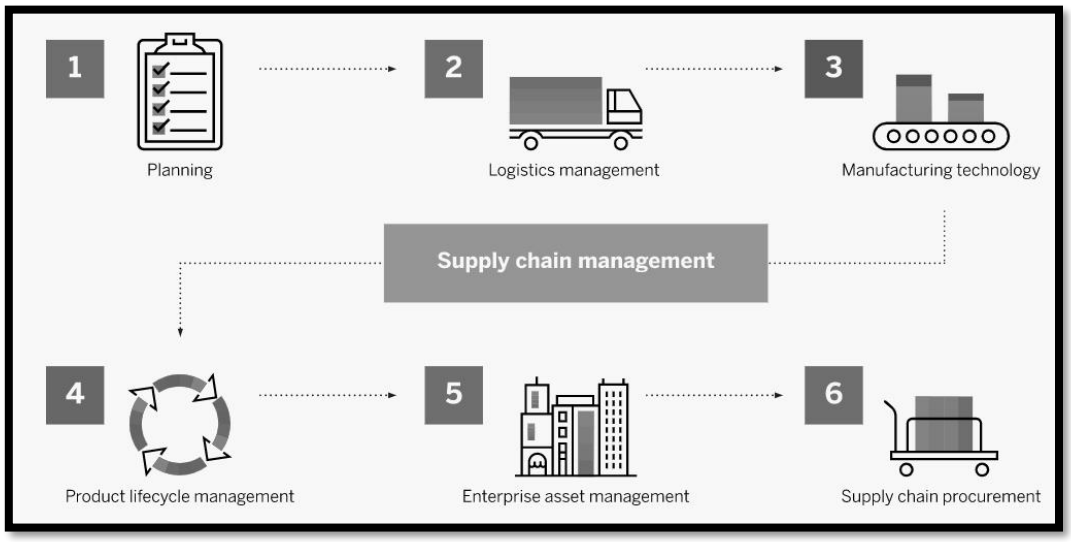
Table 3 illustrates the differences between Consensus Models

Attributes	PoW	PoS	PBFT	DPoS	PoET
Categories	Permissionless	Both	Both	Both	Both
Trusted Module	Untrusted	Untrusty	Semi-trusty	Untrusty	Untrusty
Transaction rate	Low	High	High	Medium	Medium
Transaction finality	Probabilistic	Probabilistic	Immediate	Probabilistic	Probabilistic
Cost of participation	Yes	Yes	No	Yes	No
Network scalability	High	High	Medium	Medium	High
Implementations	Bitcoin	Peercoin	Hyperledger Fabric	Bitshares	Hyperledger Sawtooth

Improving supply chain management using blockchain

Blockchain is still generating several areas, especially in financial transactions. It's a technology that has the potential to transform everything, and one of the first areas where it appears to be making a substantial difference is supply chain management **(SCM)**. The supply chain is a network of people, businesses, resources, activities, and technology that are involved in creating and selling a product. The supply of raw materials or inputs from a supplier to a manufacturer, and subsequently to the end-user is included. The process of supervising supplies, information, and financial resources as they flow from supplier to manufacturing, wholesaler, and retailer to the customer is known as supply chain management **(SCM)**. Every product will be able to be traced back to its origin or provenance, as well as the raw materials required to make that good, using a blockchain platform. The ledger's decentralized design makes it difficult for anybody to claim control of or change the data in it. Transactions are crypto-based, which makes them more secure. In Fig **5** shows supply chain processing.

Fig (5) supply chain stages

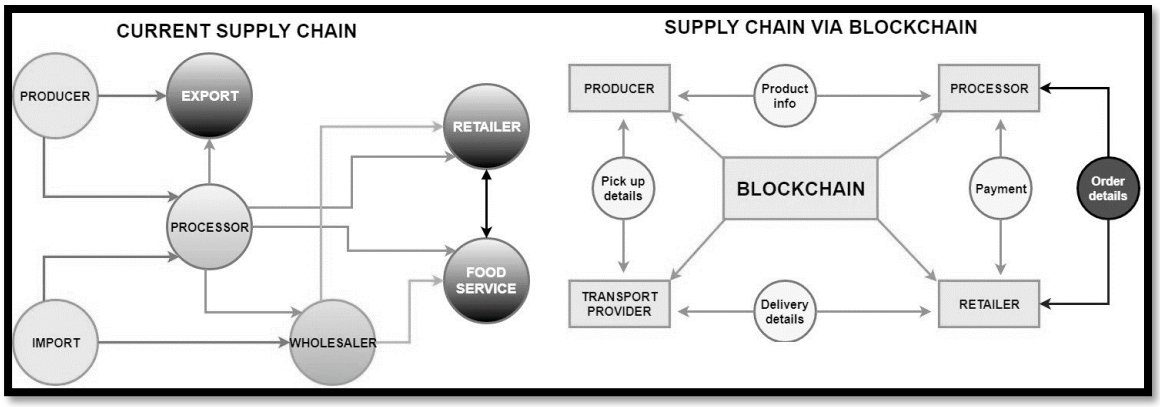


Libyan marine resources supply chain case study

In this study, which was discussed in **[17]** and we used for the future development of Libyan marine resources **(LMS)**. This model proposes a method for tracking maritime resources in order to improve Libyan exports. The multi-agent system is limited to blockchain and employs smart contracts to track all types of fish exports in the Libyan marine supply chain. The supply chain will benefit from the addition of blockchain in order to implement the proposed model for support LMS. In Fig.6 shows the difference between supply chain and supply chain architectures by blockchain. Both approaches are discussed in detail below, as well as the benefits of the new supply chain model.

- **The present supply chain:** starts with the producer and ends with the import. The products and data of these two supply chain members are sent to the next layer of the supply chain. The export, processor, and wholesaler are the next layers. This is the layer in the supply chain that processes the fundamental products received. Finally, the merchant and the foodservice sell the products at the final level. That data is centralized in every element of the supply chain and the remaining parts cannot see transactions is the main disadvantage of this model. Therefore, the consumer has no way of authenticating the origins of the food being purchased. Furthermore, there is no method to ensure that consumer data is trustworthy.
- **Supply Chain Using Blockchain:** With the inclusion of blockchain in the marine resource supply chain, the model changes to all supply chain members keeping all of their transactions on the blockchain, allowing for high security and trust. In addition, this new model addresses well-known supply-chain issues. The data in the blockchain is decentralized because each member can read the data that is pertinent to their operations. A producer, for example, can show product information to a processor and pick-up information to a transportation provider.

Fig (6) Food stages in supply chain and supply chain by blockchain

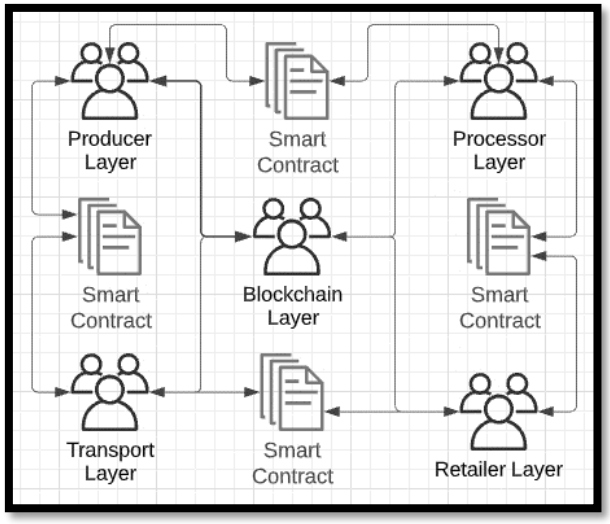


A 5-layer MAS is created to coordinate all supply chain participants in this model made presented via the blockchain as shown in Fig 7.

1. **Producer Layer**: Coordination is made through the product agent all specific operations such as purchasing materials and selling products.
2. **Processor layer:** In this layer, products are sold and contracted with transport providers.
3. **Transport Layer:** Transfers are coordinated between other participants in the supply chain.
4. **Retailer layer:** In this layer, the agent coordinates the purchase of materials from the processor and then selling to the consumer.
5. **Blockchain layer:** All transaction data is stored properly in the blockchain by synchronizing with other layers.

Through the use of this proposed model which supported LMS in future, it will encourage countries that have concerns about dealing with Libya in giving confidence and security in tracking marine resources products, in addition to the financial returns that support the Libyan economy through the transition to a digital economy.

Fig (7) Multi agent system supply chain via Blockchain



Conclusion

In this paper insights focused on blockchain technology and its impact in the future. Moreover, the architecture and main types of blockchain. The databases and the blockchain are also compared. Also illustrated a comparison of the typical consensus algorithms used in the blockchain. The focus of this paper was on the blockchain's significance in current supply chain development. In addition, it demonstrates how the blockchain may be used to record all transaction data in the supply chain for the suggested case study. Furthermore, the multi-agent system use smart contracts to control the entire supply chain process more effectively and without the usage of middlemen. Because the suggested model is automated by the agent system by connecting the blockchain with the chain supply, it is projected to improve the level of security and efficiency in the LMS sector. Shipments can be monitored, the origin and destination can be verified, and all transactions can be validated.

* * * * * * * * * * * * * * *

Reference

[1] Aggarwal, S. and Kumar, N., 2021. Basics of blockchain. **In Advances in Computers** (Vol. 121, pp. 129-146). Elsevier.

[2] Prokofieva, M. and Miah, S.J., 2019. Blockchain in healthcare. **Australasian Journal of Information Systems**, *23*.

[3] Komalavalli, C., Saxena, D. and Laroiya, C., 2020. Overview of Blockchain Technology Concepts. **In Handbook of Research on Blockchain Technology** (pp. 349-371). Academic Press.

[4] Gadde, R. and Vijay, N., 2017. A SURVEY ON EVOLUTION OF BIG DATA WITH HADOOP. **International Journal of Research in Science and Engineering**, *3*, pp.92-99.

[5] Gamage, H.T.M., Weerasinghe, H.D. and Dias, **N.G.J**., 2020. A survey on blockchain technology concepts, **applications, and issues**. **SN Computer Science**, *1*(2), pp.1-15.

[6] Zhang, Y., 2020. Blockchain. In Encyclopedia of Wireless Networks (pp. 115-118). Cham: **Springer International Publishing**.

[7] Yaga, D., Mell, P., Roby, N. and Scarfone, **K**., 2019. Blockchain technology overview. **arXiv preprint arXiv***:1906.11078*.

[8] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfede, S., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, **Princeton University Press**, 2016.

[9] Azbeg, K., Ouchetto, O., Andaloussi, S.J. and Fetjah, L., 2021. An Overview of Blockchain Consensus Algorithms: Comparison, **Challenges and Future Directions**. *Advances on Smart and Soft Computing*, pp.357-369.

[10] Pilkington, M., 2016. Blockchain technology: principles and applications. **In Research handbook on digital transformations**. **Edward Elgar Publishing**.

[11] Baygin, N., Baygin, M. and Karakose, M., 2019, November. Blockchain technology: applications, benefits and challenges. In *2019 1st* **International Informatics and Software Engineering Conference** *(UBMYK)* (pp. 1-5). IEEE.

[12] Vujičić, D., Jagodić, D. and Ranđić, S., 2018, March. Blockchain technology, bitcoin, and Ethereum: A brief overview. In *2018 17th* **international symposium infoteh-jahorina (infoteh)** (pp. 1-6). IEEE.

[13] Chowdhury, M.J.M., Colman, A., Kabir, M.A., Han, J. and Sarda, P., 2018, August. Blockchain versus database: a critical analysis. In *2018 17th* **IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)** (pp. 1348-1353). IEEE.

[14] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H., 2017, June. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017* **IEEE international congress on big data (BigData congress)** (pp. 557-564). IEEE.

[15] Sharma, D.K., Pant, S., Sharma, M. and Brahmachari, S., 2020. Cryptocurrency mechanisms for blockchains: models, characteristics, challenges, and applications. **In Handbook of research on blockchain technology** (pp. 323-348). Academic Press.

[16] Subburaj, J., Ragavi, V., Keerthana, P. and Soundarya Veni, C., 2020. Block Chain Technology: An Outline. In ICDSMLA *2019* (pp. 474-481). **Springer, Singapore**.

[17] Casado-Vara, R., Prieto, J., De la Prieta, F. and Corchado, J.M., 2018. How blockchain improves the supply chain: **Case study alimentary supply chain. Procedia computer science**, *134*, pp.393-398.

* * * * * * * * * * * * * * * *