Journal of Artificial Intelligence Practice (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/jaip.2023.060609
ISSN 2371-8412 Vol. 6 Num. 6

# *Enhancing Trust in Supply Chain Management with a Blockchain Approach*

**Safiye Turgay[1,a,*], Suat Erdoğan[2,b]**

[1]*Department of Industrial Engineering, Sakarya University, Sakarya, Turkey*
[2]*Maro International Information Technologies Consulting, Development, Support Services Industry and Trade Joint Stock Company, İstanbul, Turkey*
[a]*safiyeturgay2000@yahoo.com*, [b]*suat_er@hotmail.com*
[*]*Corresponding author*

***Keywords:*** Trust Model; Block Chain Management; Supply Chain Management; Mathematical Model

***Abstract:*** Blockchain technology has the potential to significantly enhance trust in supply chain management by providing a secure and transparent system for recording and tracking transactions. A blockchain is essentially a distributed ledger that is maintained by a network of nodes, and each node holds a copy of the same ledger. Transactions validated and recorded by the nodes in the network, and once a transaction is recorded, it cannot be altered or deleted. One of the key benefits of using blockchain technology in supply chain management is the ability to provide end-to-end traceability of products. By using a blockchain-based system, every transaction that occurs within the supply chain can be recorded and tracked, allowing for greater transparency and accountability. This can help to reduce the risk of fraud, counterfeiting, and other illegal activities within the supply chain. By using a decentralized system for recording and tracking transactions, there is less need for intermediaries and intermediaries, which can reduce costs and increase the speed of transactions. Overall, blockchain technology has the potential to significantly enhance trust in supply chain management by providing a secure and transparent system for recording and tracking transactions. However, there are still some challenges that need to be addressed, such as interoperability between different blockchain systems, and the need for standardization of data formats and protocols.

## 1. Introduction

In recent years, supply chain management has become an increasingly important area of focus for many businesses, as companies look to optimize their supply chains for greater efficiency, cost-effectiveness, and sustainability. However, with the increasing complexity of global supply chains, there are also growing concerns around transparency, accountability, and trust. One technology that has emerged as a potential solution to these challenges is blockchain. Blockchain is a decentralized, immutable ledger that enables secure, transparent, and tamper-proof record-keeping. By using blockchain-based models, supply chain participants can create a shared, trust-based ecosystem where data is shared securely, and transactions are verified by multiple parties.

In the context of supply chain management, blockchain can be used to enhance transparency and traceability, reduce fraud and counterfeiting, and increase efficiency and cost-effectiveness. By creating a secure, transparent record of all transactions and activities along the supply chain, blockchain-based models can enable supply chain participants to identify potential issues and inefficiencies, reduce waste and delays, and improve collaboration and communication. However, implementing blockchain-based models in supply chain management requires careful planning and coordination. Key challenges include integrating blockchain with existing supply chain management systems, ensuring interoperability and standardization across different blockchain platforms, and addressing issues around data privacy, security, and governance.

Despite these challenges, the potential benefits of blockchain-based models in supply chain management are significant. By enabling greater transparency, trust, and collaboration across the supply chain, blockchain can help businesses optimize their supply chains for greater efficiency, cost-effectiveness, and sustainability, while also enhancing customer satisfaction and brand reputation.

## 2. Literature Survey

There is a growing body of literature on the use of blockchain-based models in supply chain management, with a focus on enhancing trust, transparency, and traceability. Several studies have highlighted the potential of blockchain to address the challenges of supply chain management, such as the lack of transparency, trust, and coordination [1-6]. For example, a study by Lohmer et al. (2019) showed that blockchain-based models can improve the transparency and traceability of supply chains, enabling supply chain participants to monitor the movement of goods and services and identify potential issues and inefficiencies [7]. Other studies have explored the use of blockchain in specific industries, such as food and beverage, pharmaceuticals, and logistics [8-10]. For instance, a study by Rana et al. (2018) showed that blockchain can enhance the security and traceability of pharmaceutical supply chains, reducing the risk of counterfeit drugs and improving patient safety [11]. In addition to these benefits, researchers have also highlighted the challenges and limitations of implementing blockchain-based models in supply chain management [12-15]. For example, a study by Manzoor et al. (2019) identified several challenges, such as the lack of standardization and interoperability across different blockchain platforms, the need for secure and reliable data sharing, and the potential for data privacy and security breaches [16].

To address these challenges, researchers have proposed various solutions, such as the use of smart contracts to automate supply chain transactions, the development of blockchain standards and protocols, and the establishment of governance frameworks to ensure secure and transparent data sharing. Moreover, the literature suggests that blockchain-based models have the potential to transform supply chain management by enhancing trust, transparency, and traceability. However, successful implementation will require careful planning, coordination, and collaboration among supply chain participants, as well as addressing key technical and governance challenges.

## 3. Model and Method

A blockchain-based model for supply chain management typically involves creating a shared, decentralized ledger of transactions and activities along the supply chain. Each participant in the supply chain has a copy of the ledger, and all transactions are verified and recorded using cryptographic algorithms. To analyze the effectiveness of blockchain-based models in enhancing trust in supply chain management, researchers typically use simulations or case studies to evaluate the performance of the system under different scenarios [17-20]. For example, a simulation study by Kshetri (2018) modeled the impact of blockchain on supply chain trust and found that blockchain-

based models can significantly enhance trust by improving transparency and reducing the risk of fraud and counterfeiting [21]. Another study by Zheng et al. (2019) used a case study approach to analyze the implementation of a blockchain-based supply chain system in the food and beverage industry [22]. The study found that the system improved transparency and traceability, reduced transaction costs, and enhanced trust among supply chain participants. In addition to these studies, researchers have also developed various metrics and frameworks to evaluate the effectiveness of blockchain-based models in enhancing trust in supply chain management [23-26]. Overall, the analysis of blockchain-based models in supply chain management suggests that they can enhance trust by improving transparency, reducing fraud and counterfeiting, and enabling secure and reliable data sharing among supply chain participants (in Fig. 1). However, successful implementation will require addressing key technical and governance challenges, such as interoperability, data privacy, and standardization.

**Agent-Based Modeling (ABM):**

- **Mathematical Representation:**
  - *A* - Set of agents in the simulation.
  - *E* - The environment represented as a space with various factors (e.g., hazards, resources).
  - *t* - Discrete time steps.
- **Cognitive Science:**
  - Mathematical Representation:
    - *P* - Perception module.
    - *A* - Attention module.
    - *M* - Memory module.
    - *R* - Reasoning module.
    - *D* - Decision-making module.
- **Cognitive Architecture**
  - **Definition**: A cognitive architecture is a framework or model that describes the structure and functioning of cognitive processes within an intelligent system, such as the human mind or a virtual agent.
  - **Significance:** The design of a cognitive architecture serves as the basis for endowing virtual agents in emergency response simulations with cognitive capabilities.
- **Perception:**
  - Mathematical Representation:
    - *Pt(ai,ej)* - Perception function for agent *ai* regarding element *ej* at time *t*.
- **Attention:**
  - Mathematical Representation:
    - *At(ai,ej)* - Attention allocation function for agent *ai* regarding element *ej* at time *t*.
- **Memory:**
  - Mathematical Representation:
    - *Mt(ai)* - Memory state for agent *ai* at time *t*.
- **Reasoning:**
  - Mathematical Representation:
    - *Rt(ai)* - Reasoning state for agent *ai* at time *t*.
- **Decision-Making:**
  - Mathematical Representation:
    - *Dt(ai)* - Decision-making function for agent *ai* at time *t*.
- **Interactions:**
  - Mathematical Representation:
    - *It(ai,aj,ek)* - Interaction function between agent *ai*, agent *aj*, and element *ek* at time *t*.
- **Learning and Adaptation:**
  - Mathematical Representation:
    - *Lt(ai,ΔM,ΔR)* - Learning and adaptation function for agent *ai* based on changes in memory *(ΔM)* and reasoning *(ΔR)* at time *t*.

Figure 1: Agent Based Block Chain Model

Blockchain-based models have gained significant attention in the field of supply chain management due to their potential to enhance transparency, security, and trust. These models leverage the decentralized nature of blockchain technology to create a tamper-resistant and immutable record of transactions and events throughout the supply chain.

These mathematical representations provide a high-level view of how the basic building blocks of a cognitive architecture interact within an agent-based emergency response simulation. In practice, the actual mathematical models for each cognitive module would be more detailed and may involve differential equations, probabilistic models, or computational algorithms to capture the

intricacies of perception, attention, memory, reasoning, and decision-making. The interactions and learning processes would also involve more complex equations and rules tailored to the specific requirements of the simulation.

A simplified algorithmic representation of a trust-based supply chain management system using blockchain:

**1) Identity Verification**: Each participant in the supply chain, such as manufacturers, suppliers, distributors, and retailers, is assigned a unique digital identity or public key. These identities are verified through a consensus mechanism, such as proof-of-work or proof-of-stake, to ensure authenticity.

**2) Smart Contracts**: Smart contracts are self-executing agreements that reside on the blockchain. They encode the terms and conditions of transactions between different parties. Smart contracts automate processes and enforce compliance, reducing the potential for errors and disputes.

**3) Recording Transactions**: Whenever a transaction occurs, such as the transfer of goods or funds, it is recorded as a new block on the blockchain. This block contains the details of the transaction, including the parties involved, time-stamps, and relevant information such as product descriptions, quantities, and prices.

**4) Consensus Mechanism**: Blockchain networks rely on a consensus mechanism to validate and agree on the order of transactions (in Fig.2). A consensus algorithm is a fundamental concept in distributed computing and blockchain technology (in Fig. 3). It ensures that a network of nodes or participants can agree on a single value or state even when some nodes may be faulty or unreliable. There are various consensus algorithms, and they can be mathematically modeled in different ways.

1. **Nodes and Messages:**
   a. N: Total number of nodes in the network.
   b. $f$: Maximum number of Byzantine faulty nodes.
   c. 2f+1: Minimum number of honest nodes required for consensus.
   d. Nodes communicate with each other by exchanging messages.
2. **Message Types:**
   a. Nodes send messages to other nodes containing their proposed values.
   b. Nodes receive messages from other nodes and use them to determine the agreed-upon value.
3. **Message Flow:**
   a. Specify the types of messages that nodes can send and receive.
   b. Define the conditions under which a node sends or responds to specific messages.
   c. Establish message ordering and delivery guarantees.
4. **Protocol Rules:**
   a. Nodes follow a set of protocol rules to decide how to send, receive, and process messages in each round.
5. **Consensus Rules:**
   a. Define the criteria for a decision to be considered "reached" or "committed.
   b. Specify how nodes reach an agreement (e.g., majority vote, leader election, etc.).
   c. Formalize the conditions under which consensus is guaranteed.
6. **Termination:**
   a. The protocol must eventually terminate, meaning that nodes agree on a value or detect that they cannot reach consensus.
7. **Performance Metrics:**
   a. Define metrics for evaluating the algorithm's performance, such as throughput, latency, and scalability.
   b. Provide mathematical expressions or models for these performance metrics.

Figure 2: A General Consensus algorithm

**5) Immutable Record**: Once a block is added to the blockchain, it becomes a permanent and unalterable record. This immutability helps to prevent fraud, tampering, or unauthorized modifications of transaction data. Participants can have confidence in the integrity and accuracy of the recorded information. Each transaction or data entry in the blockchain is stored as a block, and once added, it cannot be altered or deleted. This immutability ensures data integrity and enables stakeholders to verify and trace every step in the supply chain, enhancing transparency.

**6) Enhanced security**: Blockchain utilizes cryptographic algorithms to secure data and transactions. This cryptographic layer ensures that information is encrypted, protecting it from unauthorized access and maintaining data confidentiality.

**Simplified POW Mathematical Model:**

1. **Block Mining Probability:**
   a. Let $P$ represent the probability that a miner successfully mines a new block within a given time frame.
   b. $P$ is a function of the miner's computational power (hash rate) denoted as $H$, and the network's total computational power, denoted as $N$.
   c. The PoW mining probability can be described as: $P(H,N) = \frac{H}{N}$
2. **Block Confirmation Probability:**
   a. Let $Q$ represent the probability that a transaction or block is confirmed after a certain number of confirmations (blocks added on top of it).
   b. $Q$ is a function of the mining probability $P$ and the number of confirmations

$$Q(P,C) = 1 - (1-P)^C$$

3. **Difficulty Adjustment:**
   a. The network aims to maintain a constant block generation rate, typically every $T$ minutes.
   b. The network adjusts the difficulty parameter $D$ such that $P(H,N) = \frac{1}{T}$.
   c. The relationship between $D$, $H$, and $N$ can be described as: $D = \frac{H}{N}.T$
4. **Security and 51% Attack:**
   a. PoW's security relies on the assumption that honest nodes control the majority of the network's hash power, i.e., $H > \frac{N}{2}$.
   b. The probability of a successful double-spending attack by a malicious miner with $m$ hash power is calculated as:
   c. $P_{attack}(m,N) = \sum_{k=m+1}^{N} \binom{N}{k} \left(\frac{m}{N}\right)^k \left(1 - \frac{m}{N}\right)^{N-k}$
5. **Block Time Analysis:**
   a. PoW aims to maintain a consistent block time, which can be analyzed using Poisson distribution if miners behave independently. The probability of finding $k$ blocks in a time interval $\Delta t$ follows a Poisson distribution with mean $\lambda = \frac{\Delta t}{T}$

Figure 3: POW Mathematical Model

**7) Supply chain visibility**: By integrating IoT devices and sensors with the blockchain, real-time tracking and monitoring of goods become possible. This increased visibility allows stakeholders to track the movement, condition, and authenticity of products throughout the supply chain.

**8) Traceability and Transparency**: With a blockchain-based supply chain management system, each participant can trace the origin and journey of a product throughout the supply chain. This transparency helps to identify bottlenecks, inefficiencies, or potential issues in the process. It also enables consumers to verify the authenticity and quality of products, fostering trust between producers and consumers.

**9) Auditable and trusted records**: Blockchain's transparent nature enables stakeholders to audit and verify transactions independently. This auditability builds trust among participants and ensures compliance with regulations and industry standards.

**10) Trust Scores and Reputation:** To further enhance trust, participants' actions and behavior within the supply chain can be tracked and evaluated. Trust scores or reputation systems can be implemented based on predefined criteria, such as on-time deliveries, quality compliance, or fair pricing. These scores recorded on the blockchain and made accessible to other participants, facilitating informed decision-making and fostering accountability.

By leveraging these features, a blockchain-based model algorithm can provide a trusted and secure environment for supply chain management. It enhances transparency, reduces fraud, streamlines processes, and strengthens trust among participants, ultimately leading to more efficient and reliable supply chain operations. Cyber threat in their supply chain strengthens their cybersecurity supply chain management practices, build resilience, and regain the trust of their customers. Cybersecurity risks in supply chain management encompass a wide range of potential threats and vulnerabilities that can impact an organization's products, services, and data. Here are some common cybersecurity risk types in supply chain management, Third-Party Vendor Risks (Compromised Suppliers; Insufficient Security Practices; Inadequate Access Control), Supply Chain Disruptions (Physical Disruptions, Cyber-Physical Attacks), Counterfeit or Tampered Components (Counterfeit Products, Tampering), Data Breaches and Data Loss (Data Exposure, Data Loss), Malware and Cyberattacks (Malware Distribution, Advanced Persistent Threats

(APTs)), Inadequate Security Patching (Delayed Patching, Unverified Updates), Data Interception and Eavesdropping (Data in Transit), Insider Threats (Malicious Insiders, Negligence), Regulatory and Compliance Risks (Non-Compliance), Lack of Transparency and Accountability (Unclear Responsibility, Inadequate Reporting), Dependency Risks( Single-Source Dependencies), Geopolitical and National Security Risks (Trade Restrictions, National Security Concerns).

To mitigate these cybersecurity risks in supply chain management, organizations should implement a comprehensive risk management strategy that includes due diligence, regular monitoring, threat intelligence, and collaboration with suppliers and vendors to ensure security throughout the supply chain lifecycle.

## 4. Case Study

Organizations rightfully have increasing concerns about the collection, storage and processing of sensitive personal information. If such data falls into the hands of malicious persons or organizations or confidentiality is disclosed, it may lead to serious consequences. There are various solutions and best practices to avoid such problems and ensure data security. Encrypting sensitive data is a fundamental step in protecting data from unauthorized access. Strong encryption algorithms should be used on databases, storage devices and communication channels. Access to data should be authorized against threats that may come from personnel at work or from outside. Measures such as policy-based access control and multi-factor authentication can be used. Regular backup and recovery of data helps prevent data loss and loss of business continuity. Firewalls and security software should be used to monitor network traffic and block malicious activity. In the event of a data breach, it must be detected quickly and notified to the relevant regulators and affected parties. It is important to comply with relevant regulations and compliance requirements. For example, it may be necessary to comply with regulations such as GDPR, HIPAA. Blockchain technology can be used to securely store and track sensitive data. This can ensure immutability and traceability of data. Data sharing and data protection issues are critical for financial institutions and other organizations. Thanks to data sharing, collaboration and information exchange, it becomes possible to make better decisions, increase operational efficiency and be more effective in the fight against crimes. Mid-sized financial services company (Fig. 4 and Fig.5). They conducted a cybersecurity risk analysis to assess their current security posture and identify vulnerabilities.

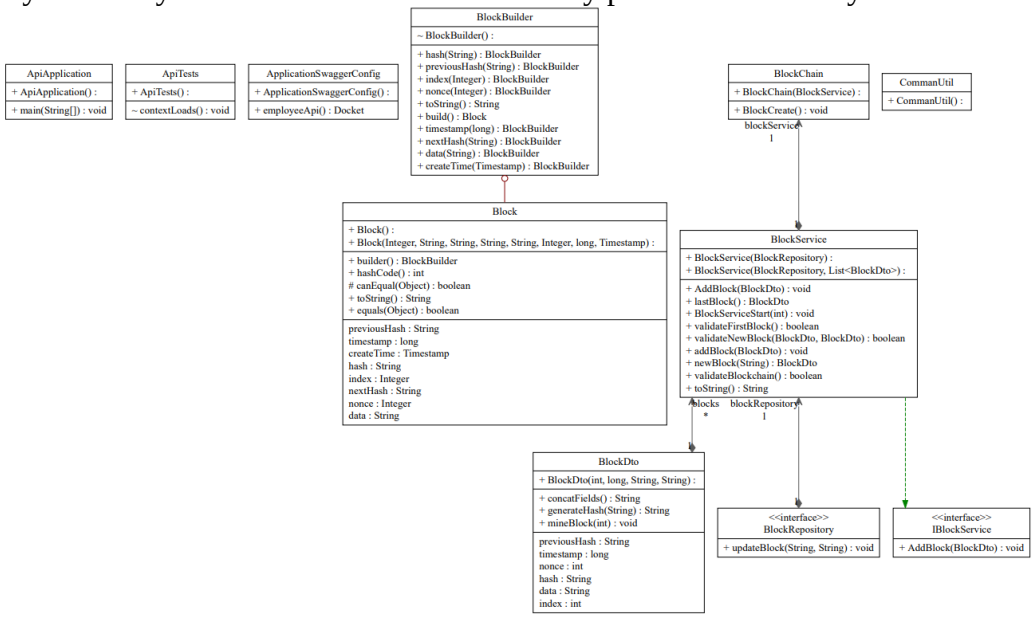


Figure 4: Suggested block chain model relation diagram

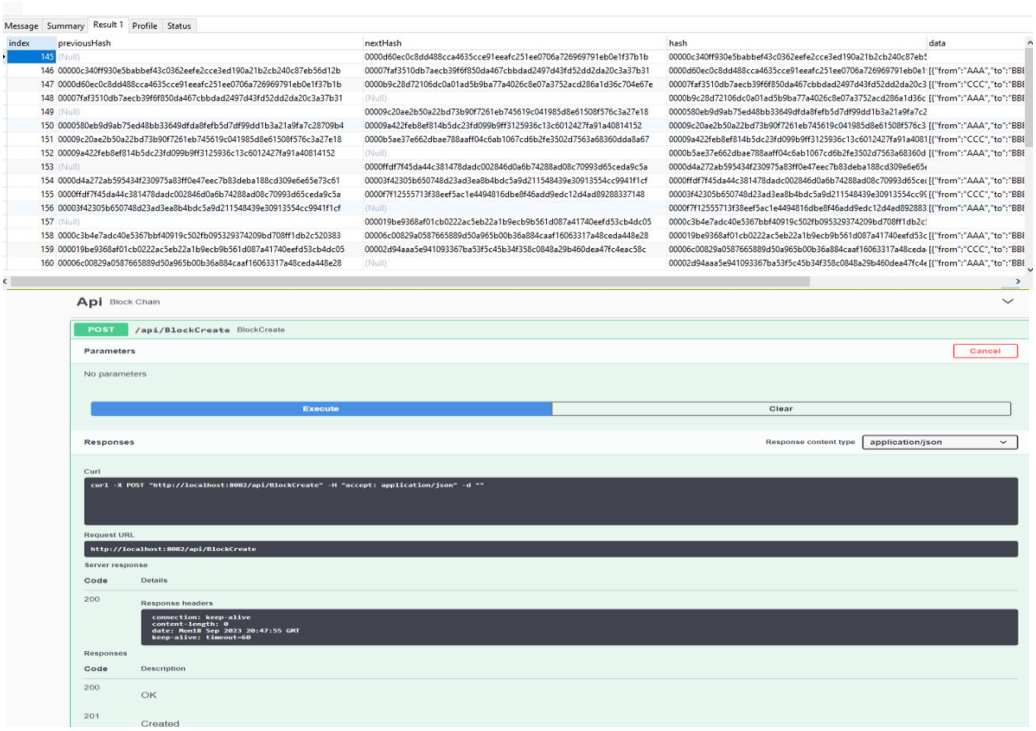


Figure 5: Suggested model message screen out.

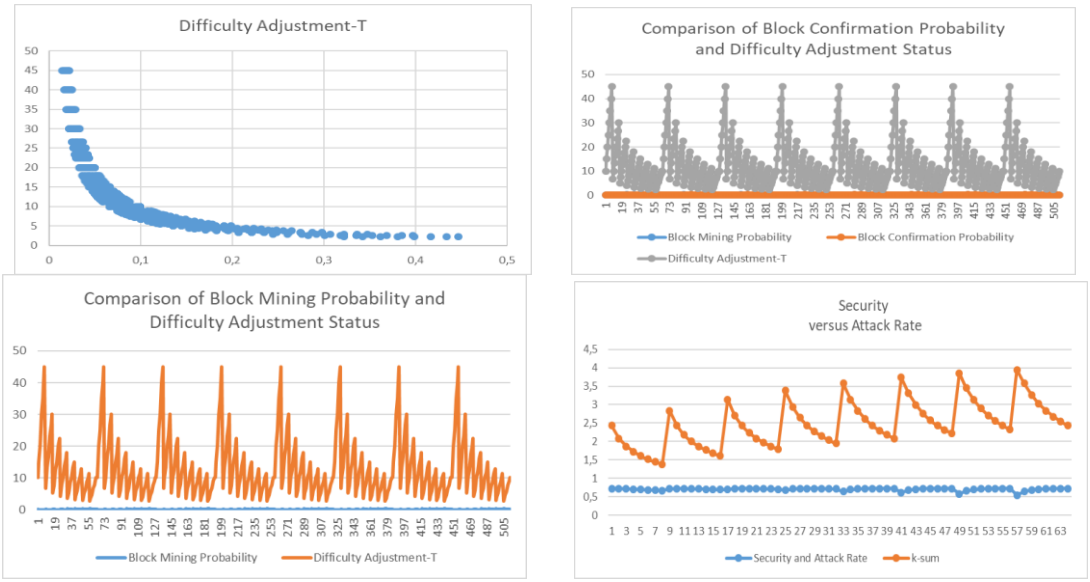


Figure 6: Suggested model performance parameter results

Difficulty adjustment maintains the security and stability of blockchain networks. It also controls how often new blocks need to be added, so that the speed of the network remains consistent. If the difficulty increases, it requires more mining power and this requires more effort to earn mining rewards. Conversely, if the difficulty decreases, mining becomes easier.

To summarize, block mining probability refers to the probability that a miner will create a new block, while block confirmation probability refers to the probability that a transaction will be confirmed by being included in a block. The two are different concepts and have a significant impact on the reliability and functioning of blockchain networks. Block mining probability determines the ability of miners to add transactions to blocks, while difficulty adjustment status

determines how often blocks are mined and the stability of the network. Block mining probability allows those with more mining power to mine new blocks more frequently, while difficulty adjustment status adjusts the difficulty of the network in line with targeted block times. The concept of "security versus attack rate" refers to a process of analyzing and balancing the security of a system or network against the ratio of potential attacks on that system or network. Ideally, a system should be sufficiently secure so that attackers fail or are discouraged from attempting an attack. This is accomplished by taking measures to improve security and reduce the attack rate. A higher level of security can contribute to a lower attack rate. That is, as a system becomes more secure, it becomes less attractive for potential attackers to target it. However, it should be noted that inadequate security measures or a weak system can increase the attack rate and make attacks more likely to succeed. Security measures and attack rate are important factors to consider during the design and operation of a system or network. A good security strategy is essential to protect against attacks. As a result, managing the balance between security and attack rate well ensures that a system is more resilient and secure against cyber threats and potential attacks. This is achieved by using a variety of security measures and strategies and is continuously monitored and improved in this paper(in Fig.6).

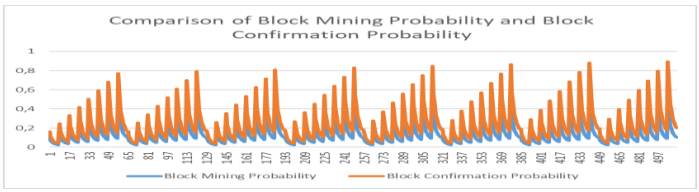


Figure 7: Comparison of block mining probability and block confirmation probability

To summarize, block mining probability refers to the probability that a miner will create a new block, while block confirmation probability refers to the probability that a transaction will be confirmed by being included in a block in this study. The two are different concepts and have a significant impact on the reliability and functioning of blockchain networks(in Fig.7).

## 5. Conclusion

In conclusion, blockchain-based models have the potential to transform supply chain management by enhancing trust, transparency, and traceability. By creating a shared, decentralized ledger of transactions and activities along the supply chain, blockchain-based models can enable secure and reliable data sharing among supply chain participants, reducing the risk of fraud and counterfeiting and improving the efficiency and cost-effectiveness of the supply chain. However, successful implementation of blockchain-based models in supply chain management will require addressing key technical and governance challenges, such as interoperability, data privacy, and standardization. It will also require careful planning, coordination, and collaboration among supply chain participants to ensure the effective integration of blockchain with existing supply chain management systems.

Overall, the literature suggests that blockchain-based models have the potential to enhance trust in supply chain management, and that further research and experimentation is needed to fully realize their potential. With continued innovation and collaboration, blockchain-based models could help businesses optimize their supply chains for greater efficiency, cost-effectiveness, and sustainability, while also enhancing customer satisfaction and brand reputation.

## References

*[1] Yontar, E. (2023). The role of blockchain technology in the sustainability of supply chain management: Grey based dematel implementation, Cleaner Logistics and Supply Chain, Volume 8, September, 100113*

*[2] Zhang, G., Yang, Z., Liu, (2023). Blockchain-based decentralized supply chain system with secure information sharing, W., Computers & Industrial Engineering, Volume 182, August, 109392*
*[3] Shukla, S., Shyam, K. C. (2023). Leveraging Blockchain for sustainability and supply chain resilience in e-commerce channels for additive manufacturing: A cognitive analytics management framework-based assessment, Computers & Industrial Engineering, Volume 176, February, 108995*
*[4] Wu, A. (2023). A Comprehensive Approach for the Evaluation of the Impact of Blockchain on Photovoltaic Supply Chain Using Hybrid Data Analytic Method, Optik, Available online 9 September, 171361*
*[5] Centobelli, P., Cerchione, R., Del Vecchio, P., Oropallo, E., Secundo, G. (2022). Blockchain technology for bridging trust, traceability and transparency in circular supply chain, Information & Management, Volume 59, Issue 7, November, 103508*
*[6] Ullah, A., Ayat, M., He, Y., Lev, B. (2023). An analysis of strategies for adopting blockchain technology in the after-sales service supply chain, Computers & Industrial Engineering, Volume 179, May, 109194*
*[7] Lohmer, J., Ribeiro da Silva, E., Lasch, R. (2022). Blockchain Technology in Operations & Supply Chain Management: A Content Analysis. Sustainability, 14, 6192. https://doi. org/10.3390/su14106192*
*[8] Guan, W., Ding, W., Zhang, B., Verny, J., Hao, R. (2023). Do supply chain related factors enhance the prediction accuracy of blockchain adoption? A machine learning approach, Technological Forecasting and Social Change, Volume 192, July, 122552*
*[9] Wu, C., Xu, C., Zhao, Q., Zhu, J. (2023). Research on financing strategy under the integration of green supply chain and blockchain technology, Computers & Industrial Engineering, Available online 9 September, 109598*
*[10] Cozzio, C., Viglia, G., Lemarie, L., Cerutti, S. (2023). Toward an integration of blockchain technology in the food supply chain, Journal of Business Research, Volume 162, July, 113909*
*[11] Rana, S. K., Rana, S. K., Nisar, K., Ag Ibrahim, A. A., Rana, A. K., Goyal, N., Chawla, P. (2022). Blockchain Technology and Artificial Intelligence Based Decentralized Access Control Model to Enable Secure Interoperability for Healthcare. Sustainability, 14, 9471. https://doi. org/10. 3390/su14159471*
*[12] Ruihuan Liu, R., Tan, C., Wu, D. D., Zhao, C. (2023). Strategies choice for blockchain construction and coordination in vaccine supply chain, Computers & Industrial Engineering, Volume 182, August, 109346*
*[13] Ramkumar, G., Kasat, K., Khader, R. A., Muhammed, N., Raghu, T., Chhabra, S. (2022). Quality enhanced framework through integration of blockchain with supply chain management, Measurement: Sensors, Volume 24, December, 100462*
*[14] Jiang, R., Kang, Y., Liu, Y., Liang, Z., Duan, Y., Sun, Y., Liu, J. (2022). A trust transitivity model of small and medium-sized manufacturing enterprises under blockchain-based supply chain finance, International Journal of Production Economics, Volume 247, May, 108469*
*[15] Hu, H., Xu, J., Liu, M., Lim, M. K. (2023). Vaccine supply chain management: An intelligent system utilizing blockchain, IoT and machine learning, Journal of Business Research, Volume 156, February, 113480*
*[16] Zhang, X., Feng, X., Jiang, Z., Gong, Q., Wang, Y. (2023) A blockchain-enabled framework for reverse supply chain management of power batteries, Journal of Cleaner Production, Volume 415, 20 August, 137823*
*[17] Bistarelli, S., Faloci, F., Mori, P. (2023). *-chain: A framework for automating the modeling of blockchain based supply chain tracing systems, Future Generation Computer Systems, Volume 149, December, Pages 679-700*
*[18] Risso, L. A, Ganga, G. M. D., Filho, M. G., Santa-Eulalia, L. A., Chikhi, T., Mosconi, E. (2023). Present and future perspectives of blockchain in supply chain management: a review of reviews and research agenda, Computers & Industrial Engineering, Volume 179, May, 109195*
*[19] Meier, O., Gruchmann, T., Ivanov, D. (2023). Circular supply chain management with blockchain technology: A dynamic capabilities view, Transportation Research Part E: Logistics and Transportation Review Volume 176, August, 103177*
*[20] Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.*
*[21] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017) An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, 25-30 June, 557-564.*
*[22] Wu, Y., Zhang, Y. (2022). An integrated framework for blockchain-enabled supply chain trust management towards smart manufacturing, Advanced Engineering Informatics, Volume 51, January, 101522*
*[23] Alkhudary, R., Pierre Fáni ès, P. (2022). Blockchain and Trust in Supply Chain Management: A Conceptual Framework, IFAC-PapersOnLine, Volume 55, Issue 10, Pages 2402-2406*
*[24] Izadi, E., Nikbakht, M., Feylizadeh, M. R., Shahin, A. (2023). A system dynamics model in the humanitarian supply chain based on blockchain technology, International Journal of Disaster Risk Reduction, Available online 9 September, 103977*
*[25] Sunmola, F., Burgess, P. (2023). Transparency by Design for Blockchain-Based Supply Chains, Procedia Computer Science, Volume 217, Pages 1256-1265.*
*[26] Turgay, S. (2022). Blockchain Management and Federated Learning Adaptation on Healthcare Management System", International Journal of Intelligent Systems and Applications (IJISA), Vol. 14, No. 5, pp. 1-13, DOI:10. 5815/ijisa. 2022. 05. 01*