Journal of Innovative Technologies
Vol. 5 (2022)
https://academicpinnacle.com/index.php/JIT

EDI and Blockchain in Supply Chain: A Security Analysis

Sai Kumar Reddy Thumburu

Senior Edi Analyist At Asea Brown Boveri, Sweden

Corresponding Email: saikumarreddythumburu@gmail.com

Abstract:

Integrating Electronic Data Interchange (EDI) and blockchain technology is reshaping supply chain management, especially from a security standpoint. EDI has long been a fundamental tool for streamlining information flow between supply chain partners, enabling rapid data exchanges and reducing manual errors. However, traditional EDI systems have been vulnerable to data breaches and cyberattacks due to centralized data storage and a lack of advanced security protocols. With its decentralized and immutable ledger, blockchain offers a promising solution to address these security challenges. By implementing blockchain with EDI, supply chains can benefit from enhanced data integrity, traceability, and transparency. Blockchain's cryptographic algorithms ensure that data is secure and tamper-proof, fostering trust among participants. Additionally, integrating intelligent contracts within blockchain allows for automated processes, minimizing human intervention and reducing the risk of fraud. Despite these benefits, adopting blockchain technology in EDI-based supply chains presents particular challenges, such as scalability concerns, high energy consumption, and the need for widespread industry adoption. This paper delves into the security benefits and challenges of combining EDI and blockchain in supply chain management. It explores case studies and recent research to highlight real-world applications and assess the effectiveness of this integration. By analyzing both technologies' capabilities and limitations, this paper aims to provide insights into how EDI and blockchain can create a more secure, efficient, and resilient supply chain ecosystem.

Keywords: Supply Chain Security, Electronic Data Interchange (EDI), Blockchain Technology, Data Integrity, Transparency in Supply Chains, Decentralized Ledger, Smart Contracts, Automated Data Exchange, EDI

Standards, Blockchain Integration, Supply Chain Transparency, Secure Data Exchange, Supply Chain Automation, Blockchain Security, Data Tampering Prevention, Supply Chain Efficiency, Cryptographic Security, Digital Transformation, Traceability in Supply Chains, Blockchain Applications in Supply.

1. Introduction

Global supply chains have transformed significantly in recent decades, driven by rapid technological advancements and the growing need for efficiency and transparency. These changes have created a complex web of interconnected suppliers, manufacturers, distributors, and retailers across different geographical locations. As companies increasingly rely on these intricate networks, the flow of information becomes essential to keeping supply chains efficient and responsive. However, this interdependence also introduces substantial challenges in data management and security, with traditional methods like Electronic Data Interchange (EDI) needing improved data integrity, transparency, and resilience against cyber threats.

Since its inception, EDI has been a fundamental tool in supply chain operations, allowing businesses to electronically exchange critical data, such as purchase orders, invoices, and shipping information. The adoption of EDI systems enabled companies to move away from paper-based processes, reducing errors, speeding up transactions, and improving communication between partners. However, EDI operates on centralized networks, which makes it vulnerable to data breaches and system failures. As supply chains expand, these risks become more pronounced, exposing sensitive information to potential cyber-attacks and raising concerns about data accuracy and trustworthiness.

In recent years, blockchain technology has emerged as a promising solution to address some inherent weaknesses of traditional EDI systems. Blockchain, the technology behind cryptocurrencies like Bitcoin, operates as a decentralized digital ledger that records transactions across a network of computers immutable and transparently. Unlike conventional data storage methods, blockchain's distributed structure enhances security by removing single points of failure and enabling all participants in the network to have a synchronized copy of the data. Each transaction, or "block," is cryptographically linked to the previous one, forming a chain resistant to tampering or unauthorized modifications.

Integrating blockchain with EDI in supply chain management is an evolving concept that leverages both technologies' strengths. While EDI provides a

standardized format for data exchange, blockchain adds an extra layer of security and trust through its decentralized nature. This hybrid approach is seen as a way to enhance data integrity, improve transparency, and secure sensitive information against unauthorized access and fraud. As more industries explore the potential of blockchain, the supply chain sector is uniquely positioned to benefit from this technology's capabilities, given its need for secure and reliable data exchange.

1.1 EDI: Strengths and Limitations

EDI has been integral to supply chain management for decades, streamlining operations by facilitating quick and accurate information sharing. Traditionally, EDI systems enable data exchange between different business entities, regardless of the software platforms they use. This compatibility is a key advantage, as it allows companies to maintain relationships with various partners without worrying about data format inconsistencies. Furthermore, EDI supports automation, reducing manual data entry and minimizing human error, which helps speed up transactions and enhance productivity.

Despite these benefits, EDI has its drawbacks. One of the most critical issues is the lack of transparency. EDI transactions typically occur between two parties and are processed through centralized systems, often with minimal visibility into the transaction details for other stakeholders in the supply chain. This opacity can lead to discrepancies, misunderstandings, and delays, especially when multiple parties are involved. Additionally, centralized EDI systems are susceptible to cyber threats. A single breach can compromise the entire network, exposing sensitive information to unauthorized users and potentially disrupting business operations. These vulnerabilities underscore the need for a more secure and transparent system, particularly in today's digital landscape, where cyber attacks are increasingly sophisticated and widespread.

1.2 Blockchain: Enhancing Security and Trust

Blockchain technology offers several features that make it a compelling addition to traditional EDI systems. One of the primary advantages of blockchain is its decentralized structure. Unlike centralized databases, which store information on a single server or a cluster of servers controlled by a single entity, blockchain distributes data across a network of nodes. Each node maintains a complete copy of the transaction history, which is constantly updated and verified through a consensus mechanism. This decentralization makes blockchain inherently more resilient to attacks, as no single point of failure could bring down the entire network.Moreover, blockchain's immutability ensures that a transaction cannot be altered or deleted once a transaction is recorded. This feature is precious for

supply chain management, where data integrity is crucial. By recording each step in the supply chain on a blockchain, companies can create a permanent, tamper-proof record of every transaction, from raw material sourcing to final product delivery. This transparency allows all participants in the supply chain to verify the authenticity of the data, fostering trust and reducing the potential for fraud.

In addition, blockchain supports smart contracts—self-executing agreements encoded directly onto the blockchain. Based on predefined conditions, smart contracts can automate various processes in the supply chain, such as payment releases or inventory management. By integrating smart contracts with EDI, companies can further enhance efficiency and security, reducing the reliance on intermediaries and minimizing the risk of human error or deliberate manipulation.

1.3 Toward a Secure and Transparent Supply Chain

Integrating blockchain with EDI represents a significant step forward in the evolution of supply chain management. By combining EDI's standardization with blockchain's security and transparency, companies can create a more robust framework for data exchange. This hybrid approach addresses some of the most pressing challenges in supply chain management, such as data breaches, fraud, and lack of visibility. While implementing blockchain in supply chains is still in its early stages, the technology's potential benefits make it an attractive option for companies looking to enhance their data security and operational efficiency.

As supply chains grow in complexity, adopting innovative solutions like blockchain can provide companies with a competitive edge. By leveraging blockchain's decentralized architecture and EDI's established protocols, supply chain stakeholders can improve collaboration, reduce risks, and ensure their operations remain secure and transparent in an increasingly interconnected world.

2 Overview of EDI in Supply Chain

2.1 History and Development of EDI

Electronic Data Interchange (EDI) has transformed supply chain operations for decades, enabling businesses to exchange critical information quickly and accurately. EDI emerged in the 1960s as a means to automate the transfer of business documents between organizations, eliminating the need for manual processes that were time-consuming and prone to errors. By the 1970s, significant players in industries like retail and automotive had already begun integrating EDI into their operations to share purchase orders, invoices, and

shipping notices. The American National Standards Institute (ANSI) introduced standardized EDI protocols in the early 1980s, which helped EDI gain wider adoption by setting industry-specific standards for data exchange. As a result, businesses could communicate and collaborate efficiently across regions and even internationally because EDI provided a common language for different systems.

As technology evolved, so did EDI. The rise of the internet in the 1990s opened up new opportunities for EDI to expand, as it could now operate over public networks, reducing the need for expensive Value-Added Networks (VANs) that had initially supported these exchanges. By the early 2000s, EDI had cemented its role as the backbone of data exchange in supply chains, facilitating millions of transactions across industries like healthcare, finance, and manufacturing.

Despite their contributions, traditional EDI systems still rely on older technology. While they have adapted over the years, they are not immune to modern cybersecurity challenges. Legacy EDI systems remain vulnerable to various threats that can compromise the integrity and confidentiality of data shared among trading partners.

2.2 Security Concerns with EDI

While EDI has revolutionized how businesses communicate, its security features have only sometimes kept up with advancements in cyber threats. One of the biggest security concerns is the potential for data breaches due to insufficient data protection mechanisms. Many EDI systems lack comprehensive encryption, leaving transmitted data vulnerable to interception. For example, in an unencrypted EDI system, sensitive information such as pricing details, customer information, and financial data could be intercepted by hackers during transmission. This can lead to unauthorized access to proprietary business information, damaging an organization's reputation and economic stability.

Another issue with traditional EDI systems is that they rely heavily on static IP addresses and fixed communication channels, making them susceptible to spoofing attacks, in which attackers disguise themselves as trusted trading partners to gain access to confidential data. Without robust authentication and verification protocols, malicious actors can infiltrate the system, posing as legitimate partners to intercept or even manipulate data.

Moreover, legacy EDI systems often have limited monitoring capabilities, hindering an organization's real-time ability to detect and respond to potential

security incidents. As a result, EDI-related breaches might go unnoticed until significant damage has already occurred. EDI's limitations pose a severe risk in today's cybersecurity landscape, where real-time monitoring and quick response are crucial.

Another significant security concern involves outdated protocols not designed to address modern cyber threats. Many traditional EDI setups still operate over insecure channels or use outdated encryption algorithms, if any at all. This lack of encryption makes EDI exchanges vulnerable to man-in-the-middle attacks, where attackers intercept and possibly alter the information during transmission. Although EDI standards have been updated over time, many companies are reluctant to upgrade their systems due to the high cost and operational disruption involved. This leaves organizations relying on legacy systems that may not comply with modern security standards.

2.3 Advantages and Disadvantages

- **Advantages of EDI**EDI offers numerous advantages that make it indispensable in the supply chain sector. One of its most significant benefits is the efficiency it brings to business processes. By automating the exchange of documents such as purchase orders, invoices, and shipping notifications, EDI reduces the time and labour needed to manage these tasks manually. In addition, EDI minimizes errors related to data entry, as transactions are processed electronically. The result is faster turnaround times and improved accuracy, which can enhance relationships between trading partners.
  Another advantage is standardization. EDI follows specific standards that dictate how data is formatted and transmitted. This consistency allows companies across different industries and regions to communicate seamlessly, regardless of the software or systems they use internally. Standardization also simplifies compliance, as many regulatory bodies require specific transaction protocols. By using EDI, businesses can ensure they meet industry and government regulations, which reduces the risk of fines and penalties.

  EDI also improves visibility within the supply chain, allowing companies to track real-time transactions. This transparency helps businesses plan more effectively, manage inventory, and make informed decisions based on accurate data. Additionally, EDI can enhance data security through

secure channels and digital signatures, although these features may not be as robust as needed in today's threat landscape.

- **Disadvantages of EDID Despite** its benefits, EDI has some notable drawbacks, particularly regarding security. Traditional EDI systems are often built on older technology that may not incorporate the latest security protocols. Many EDI setups lack modern encryption standards, which can leave sensitive data exposed. While EDI providers offer secure options, upgrading costs are high, and some businesses are reluctant to invest in overhauling legacy systems. This exposes them to risks like data breaches, man-in-the-middle attacks, and unauthorized access.
  Another disadvantage is the cost of implementation and maintenance. Setting up an EDI system requires an initial investment in hardware, software, and employee training, which can be a barrier for small and medium-sized businesses. Maintenance is costly, as EDI systems need regular updates to comply with evolving standards and security requirements. Additionally, since EDI systems are highly specialized, organizations often need to invest in dedicated IT support to manage and troubleshoot these systems.

  Moreover, while EDI provides standardization, it lacks flexibility. Traditional EDI is based on rigid standards that can be challenging to customize for unique business needs. Companies with non-standard data requirements may need help to adapt EDI to fit their processes, limiting its usefulness. Finally, EDI must integrate more easily with newer technologies like cloud-based solutions and blockchain. As businesses increasingly rely on advanced technology to streamline operations, EDI's limited compatibility can be a disadvantage.

3. Introduction to Blockchain Technology

3.1 Blockchain Basics

Blockchain technology, often described as a distributed ledger, is a decentralized digital record of transactions that is securely shared across a network. Its origins can be traced back to 2008 when it was first conceptualized by an anonymous entity known as Satoshi Nakamoto. Nakamoto introduced blockchain as the underlying technology for Bitcoin, a cryptocurrency that operates without a central authority. However, blockchain's applications have grown far beyond Bitcoin, now spanning various sectors, from finance and healthcare to supply chain management.

At its core, blockchain operates by recording information in "blocks" linked together in a chain. Each block contains a list of transactions, and once a block is added to the chain, it cannot be altered without altering every subsequent block. This structure makes blockchain uniquely secure and resistant to tampering. In a blockchain network, every participant has a copy of the ledger, which is continually synchronized and updated as new blocks are added. This decentralized nature eliminates the need for a central authority, enabling trust between parties even when they don't know each other.

3.2 Security Features

Blockchain technology offers several security features that appeal to applications where data integrity and security are crucial. These features include decentralization, cryptographic hashing, consensus algorithms, and immutability.

- **Decentralization**: One of blockchain's most prominent security features is its decentralized structure. Instead of relying on a single central server or authority, blockchain operates on a network of nodes. Each node stores a copy of the entire blockchain, ensuring that no single point of failure can compromise the network. This decentralization also enhances the blockchain's transparency since all transactions are visible to every participant on the network.
- **Cryptographic Hashing**: Blockchain uses cryptographic hashing to secure data within each block. A hash is a unique string of characters generated by a mathematical algorithm based on the contents of the block. Any change in the block's data would alter its hash, making it immediately noticeable. Hashes also link blocks together; each block contains the previous block's hash, creating a secure chain that would require vast computational power to tamper with.
- **Consensus Algorithms**: To ensure the validity of transactions and to add new blocks to the chain, blockchain networks use consensus algorithms. The most well-known consensus mechanism is Proof of Work (PoW), which requires participants to solve complex mathematical puzzles to add a new block. This process is energy-intensive and time-consuming, which discourages malicious actors from attempting to alter the blockchain. Other consensus mechanisms include Proof of Stake (PoS) and Delegated Proof of Stake (DPoS), which provide alternative ways of achieving consensus without the high energy costs of PoW.
- **Immutability**: Once a block is added to the blockchain, it cannot be altered or deleted. This immutability is one of the most powerful security features of blockchain technology. It ensures that the history of

transactions is preserved and cannot be changed, which is critical in industries where data integrity and traceability are essential. Any attempt to alter a block would be immediately noticeable, as it would require modifying every subsequent block in the chain.

These security features work together to make blockchain a highly secure and reliable technology, particularly well-suited for applications where data security and trust are paramount. The combination of decentralization, cryptographic hashing, consensus algorithms, and immutability provides a strong defence against tampering, fraud, and cyberattacks.

3.3 Use in Supply Chain Management

Blockchain technology has made significant inroads in the supply chain. Supply chain management involves tracking and coordinating products as they move from suppliers to manufacturers, distributors, and ultimately to consumers. Traditional supply chains can be complex, with multiple stakeholders and a reliance on manual record-keeping, which can lead to inefficiencies, delays, and opportunities for fraud. Blockchain has the potential to streamline and secure these processes.

- **Tracking Goods**: Blockchain can enhance traceability in the supply chain by providing a transparent and immutable record of every transaction. As goods move through the supply chain, each transaction is recorded on the blockchain, creating a permanent history that authorized parties can access. This traceability is especially valuable in industries where provenance is essential, such as food, pharmaceuticals, and luxury goods. By knowing exactly where a product has been at each step, businesses can ensure quality, verify authenticity, and quickly identify and address any issues, such as contamination or counterfeiting.
- **Enhancing Transparency**: Transparency is another key benefit of using blockchain in supply chain management. Because blockchain is a shared, decentralized ledger, all parties in the supply chain can view and verify transactions in real time. This visibility fosters trust between parties, as everyone can access the same information. Additionally, consumers are increasingly interested in knowing where their products come from and whether they are sourced ethically. Blockchain can provide consumers with detailed information about a product's journey from the source to the store shelf, enhancing brand loyalty and consumer trust.
- **Reducing Fraud and Errors**: Data manipulation and fraud can be challenging to detect in traditional supply chains. Paper records and isolated databases are susceptible to tampering and human error, which can lead to significant financial losses. Blockchain's immutability makes

it nearly impossible to alter records once they are added to the chain, reducing the risk of fraud and enhancing the reliability of the supply chain. Moreover, because blockchain is automated, it reduces the need for manual record-keeping and minimizes the likelihood of errors.

Blockchain technology has shown great promise in transforming supply chains by increasing efficiency, reducing costs, and enhancing security. With its decentralized structure, secure data handling, and transparent record-keeping capabilities, blockchain offers a viable solution to many of traditional supply chains' challenges. As more businesses explore the potential of blockchain, we can expect to see even greater innovation and transformation in how goods are produced, tracked, and delivered worldwide.

4. How Blockchain Enhances EDI Security?

4.1 Immutable Record-Keeping

In traditional EDI systems, the data exchange relies on a centralized network or trusted third parties, which leaves a window open for potential data tampering or unauthorized alterations. With its foundational structure of an immutable ledger, blockchain brings a new layer of security to this process. Once data is recorded on the blockchain, it’s secured through cryptographic hashing, meaning each transaction is effectively sealed and tamper-evident.

In a blockchain, each transaction is grouped into a block linked with the previous one, forming a chain of chronological, interdependent blocks. This structure ensures that if someone tries to alter even a tiny detail in an earlier block, it will disrupt the entire chain, immediately signalling that tampering has occurred. As a result, EDI data shared across this chain remains unalterable, providing a robust record-keeping mechanism.

Companies in a supply chain could benefit from this immutable ledger when sharing sensitive data such as purchase orders, invoices, or shipment records. For instance, an EDI transaction involving a purchase order would be securely recorded on the blockchain, and any changes to that order—such as adjustments in quantity or delivery details—would need to be documented in subsequent blocks. This maintains a complete audit trail that can be verified by all parties, fostering trust and accountability within the supply chain.

4.2 Decentralized Networks

Traditional EDI relies on centralized servers, which can present a single point of failure—a significant vulnerability in today’s interconnected business landscape. If these servers experience downtime or, worse, fall victim to a cyberattack, the

flow of information is disrupted, impacting the entire supply chain. Blockchain technology, by contrast, operates on a decentralized network, distributing data across multiple nodes (computers) that continuously synchronize with one another. This decentralized approach provides redundancy and improves resilience, as the blockchain remains accessible even if individual nodes fail.

This decentralized network plays a pivotal role in EDI security by ensuring data availability. In a blockchain-based EDI system, each participant maintains a copy of the shared ledger, which means the supply chain can continue to operate smoothly even if one participant's systems are down. Additionally, the decentralized nature of blockchain reduces the risk of a single point of failure being exploited. For example, even if a hacker manages to breach one node, they cannot alter the data across the entire network without control over the majority of nodes. This task would require enormous resources.

This decentralization means enhanced uptime and consistent data availability for supply chain managers. If a warehouse manager needs to access a transaction record, it's readily available through the blockchain, bypassing the need to rely on potentially vulnerable centralized servers. This boost in data availability and reliability leads to smoother operations and fewer disruptions in the supply chain.

4.3 Smart Contracts for Automated Transactions

Intelligent contracts bring an added dimension of automation and security to blockchain-based EDI. A smart contract is a self-executing program that enforces agreed-upon terms when certain conditions are met. In supply chain management, smart contracts can automate various processes, such as payment terms, delivery schedules, and quality checks. This automation reduces administrative overhead and minimizes the risk of human error and fraud.

Take, for example, a situation where a supplier and a retailer have agreed upon a specific delivery schedule. A smart contract can be set up to automatically verify when the delivery is made and release payment to the supplier as soon as the goods are confirmed to be in transit. By eliminating manual intervention, smart contracts streamline transactions, accelerate payment cycles, and provide a consistent and transparent way to enforce contractual obligations.

Moreover, smart contracts can play a crucial role in fraud prevention. Since the terms of the agreement are pre-coded into the contract, there is little room for manipulation or unauthorized changes. In EDI systems, intelligent contracts can validate data transfers, authenticate transactions, and provide real-time visibility into the status of various supply chain activities.

4.4 Case Study

One real-world example of blockchain and EDI integration can be found in the pharmaceutical industry, where security and traceability are paramount. Counterfeit drugs and regulatory non-compliance can lead to severe consequences, so maintaining a reliable and secure supply chain is essential.

A pharmaceutical company facing these challenges decided to integrate blockchain with its EDI system to ensure full traceability of its products from manufacturer to distributor to pharmacy. With blockchain, the company could track each drug batch, documenting each transaction on an immutable ledger accessible by all authorized participants. By adding this level of transparency, the company significantly reduced the chances of counterfeit drugs entering the supply chain.

Furthermore, smart contracts were employed to verify compliance with regulatory standards automatically. For instance, before a batch could proceed to the next step in the supply chain, a smart contract would confirm that it had passed specific quality checks. Only then would the EDI transaction be recorded on the blockchain, allowing the shipment to move forward.

The results were compelling. The company achieved improved visibility and accountability within its supply chain and streamlined its compliance process, reducing the time and costs associated with regulatory audits. This case study demonstrates the tangible security benefits of combining blockchain with traditional EDI systems, particularly in industries where traceability and compliance are critical.

5. Potential Security Risks and Challenges

As supply chain systems evolve, integrating Electronic Data Interchange (EDI) with blockchain technology presents exciting possibilities. However, this integration also introduces new security risks and challenges. Here, we'll explore some of the most significant issues, including scalability, data privacy, implementation, and regulatory compliance.

5.1 Scalability Issues

One of blockchain's core limitations is its scalability. While EDI traditionally processes large volumes of transactions quickly, blockchain technology operates with certain constraints that can impact speed and data storage.

Blockchain is often slower than centralized systems because of its decentralized nature. Each transaction must be verified and validated by nodes within the network, which can lead to bottlenecks. For example, public blockchains like Bitcoin or Ethereum are known to handle only a limited number of transactions per second compared to traditional centralized systems. In a supply chain context, where thousands of transactions could occur in mere seconds, this limitation can slow down EDI processes, potentially impacting the overall efficiency of the supply chain.

Additionally, the amount of data stored on a blockchain is limited. Public blockchains often have storage constraints due to their design, making them unsuitable for systems like EDI, where significant data is exchanged. Although solutions such as off-chain storage can help, they introduce additional complexities and security concerns. Ensuring that the blockchain can handle the speed and volume of EDI transactions is a challenge that requires creative solutions, such as leveraging layer-2 solutions or using private blockchains with increased processing power.

5.2 Data Privacy Concerns

One of blockchain's core strengths is transparency; however, this feature can be problematic regarding data privacy in the supply chain. EDI systems often involve sensitive information, such as pricing details, transaction records, and customer information. Blockchain, particularly public blockchain, is designed to allow any user to verify transactions. This openness may conflict with confidentiality requirements, making it less suitable for organizations that handle sensitive or proprietary data.

To address these privacy concerns, companies may consider private or permissioned blockchains. These blockchains restrict access to authorized users, allowing businesses to control who can view the data. Hybrid blockchain models can also be employed, combining elements of both public and private blockchains. For instance, a public blockchain can verify transaction authenticity, while sensitive data is kept on a private blockchain or an off-chain database.

Advanced cryptographic methods, such as zero-knowledge proofs or homomorphic encryption, also offer ways to enhance privacy on the blockchain. These solutions allow data to be shared across a blockchain network without revealing the content, addressing privacy concerns. However, these technologies are complex and may require significant computational resources, adding another layer of challenge to the integration process.

5.3 Implementation Challenges

Integrating EDI with blockchain technology presents various practical challenges, primarily related to cost, technology compatibility, and the expertise required for implementation. Blockchain is still relatively new in the supply chain industry, and organizations may need to invest heavily in resources to facilitate this transition.

One of the most significant barriers is cost. Implementing blockchain technology is not cheap. Organizations may need to upgrade existing infrastructure, invest in new hardware, or adopt software that can interface with blockchain systems. Additionally, due to blockchain's decentralized nature, transaction fees are often involved in processing and validating transactions, which could add up when applied at scale.

Technology compatibility is another challenge. EDI systems are often based on older technologies that may not seamlessly integrate with blockchain platforms. This lack of compatibility can increase costs and development time as companies work to bridge the gap between legacy systems and new blockchain-based solutions. In some cases, entirely new systems may need to be developed to support blockchain, further complicating the integration process.

Finally, blockchain technology requires specialized knowledge that may not be readily available within an organization. Finding personnel with the necessary expertise to manage and maintain a blockchain-EDI system can be challenging, especially in an industry where blockchain expertise is still emerging. Organizations must consider training existing staff or hiring new personnel, which can be costly and time-consuming. Companies may also have to work with external blockchain consultants or vendors, which can introduce additional security and data privacy complexities.

5.4 Regulatory Compliance

Another significant challenge is navigating the regulatory landscape for blockchain and EDI. Regulatory compliance varies from region to region, and organizations must ensure they adhere to applicable laws and standards, particularly those related to data protection.

Blockchain's distributed nature can complicate compliance with regulations like the General Data Protection Regulation (GDPR) in the European Union, which gives individuals the right to have their data erased. Since blockchain transactions are immutable, deleting data is practically impossible once recorded, raising concerns about compliance with these "right to be forgotten"

requirements. Organizations may need to consider hybrid models where sensitive data is stored off-chain to address this, allowing them to comply with data erasure requests.

Additionally, supply chains that operate internationally must navigate a range of legal requirements in different jurisdictions. For instance, data transfer laws may limit where and how data can be stored and shared across borders, creating compliance challenges for blockchain systems designed to operate globally. Companies may need to work closely with legal teams to understand how these regulations apply to their specific use cases and develop solutions that ensure compliance.

Finally, there are no standardized guidelines for using blockchain in industries where EDI is prevalent. Until greater regulatory clarity is achieved, organizations must tread carefully and stay updated on any new developments in this area. In some cases, this may mean delaying blockchain integration with EDI until regulations mature and standardized frameworks are established.

6. Conclusion

Integrating Electronic Data Interchange (EDI) and blockchain technology marks a promising advancement in supply chain security. As EDI continues to serve as the backbone for standardized data exchange between businesses, blockchain offers a decentralized and immutable ledger system that enhances security and transparency. By combining these technologies, organizations can create a supply chain that minimises vulnerabilities and significantly improves data integrity and traceability.

Blockchain’s decentralized nature ensures that no single party controls the entire system, reducing the risk of data tampering or unauthorized access. When paired with EDI, this feature bolsters fraud prevention measures by creating an unalterable record of transactions that can be easily audited. Furthermore, the real-time capabilities of blockchain can complement EDI's batch processing, enabling quicker responses to issues as they arise. This combination can lead to faster, more efficient, and highly secure data exchanges, providing companies and consumers peace of mind.

Despite these advantages, adopting blockchain and EDI in supply chains is challenging. Scalability remains a significant hurdle, as blockchain networks' energy demands and processing power can be prohibitive. Additionally, data privacy is a critical concern, as supply chains often involve sensitive information that must be shared with multiple parties. Regulatory compliance also adds

complexity, especially as blockchain technology is still evolving, and legal frameworks must be fully established in many regions.

Looking ahead, the strategic adoption of EDI and blockchain can offer organizations a robust framework for enhancing supply chain security. The future will likely bring further technological advancements, including integrating IoT and artificial intelligence with blockchain, which will continue to drive improvements in supply chain efficiency, transparency, and security. For organizations aiming to secure their supply chains against emerging threats, investing in these technologies today could offer a considerable advantage in the increasingly interconnected global marketplace.

7. References

1. Merghani, H., & Salmela, S. H. (2019). INTEGRATING BLOCKCHAIN TECHNOLOGY IN SUPPLY CHAIN MANAGEMENT SOFTWARE.

2.Longo, F., Nicoletti, L., & Padovano, A. (2020). Estimating the impact of blockchain adoption in the food processing industry and supply chain. International Journal of Food Engineering, 16(5-6), 20190109.

3.Hofmann, E., Strewe, U. M., & Bosia, N. (2017). Supply chain finance and blockchain technology: the case of reverse securitisation. Springer.

4.Banerjee, A., & Venkatesh, M. (2018). Product tracking and tracing with iot and blockchain.

5.Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology: applications in health care. Circulation: Cardiovascular quality and outcomes, 10(9), e003800.

6.Swaminathan, J. M., & Tayur, S. R. (2003). Models for supply chains in e-business. Management science, 49(10), 1387-1406.

7.Seth, M., Goyal, D. P., & Kiran, R. (2015). Development of a model for successful implementation of supply chain management information system in Indian automotive industry. Vision, 19(3), 248-262.

8.Lee, H. L., So, K. C., & Tang, C. S. (2000). The value of information sharing in a two-level supply chain. Management science, 46(5), 626-643.

9.Detro, J. (2016). Examining the Impact of Supply Chain Technology Implementations on Supply Chain Effectiveness and Firm Value. Global

journal of Business and Integral Security.

10.Srinivasan, K., Kekre, S., & Mukhopadhyay, T. (1994). Impact of electronic data interchange technology on JIT shipments. Management Science, 40(10),

1291-1304.

11.Chwelos, P., Benbasat, I., & Dexter, A. S. (2001). Empirical test of an EDI adoption model. Information systems research, 12(3), 304-321.

12.Erik, F., & Johan, Y. (2019). Utilization of Blockchain technologies for enhanced transparency and traceability in the Supply Chain.

13.Lahjouji, M., el Alami, J., & Hlyal, M. (2020, December). Blockchain Applications for Improving Track and Trace Process on Pharmaceutical Supply Chain. In International Conference on Advanced Intelligent Systems for Sustainable Development (pp. 471-493). Cham: Springer International

Publishing.

14.Lee, H. L., Padmanabhan, V., & Whang, S. (1997). Information distortion in a supply chain: The bullwhip effect. Management science, 43(4), 546-558.

15.Yoon, J. H., Kim, J. S., & Park, H. G. (2020). A study on the priorities of blockchain adoption for port logistics in Korea using AHP: focused on Busan and Incheon ports. Journal of International Trade & Commerce, 16(1), 1-24.