Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Blockchain for secure Data Sharing: Enhancing Security and Trust in Inter-organizational Exchange

Yandapalli Nagendra[1], Dr. Suryakanth V Gangashetty [2]
[1] *Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, 522502,AP, India.*
yandapallinagendra9@gmail.com
[2] *Associate Professor, Department of CSE, Koneru Lakshmaiah Educationn Foundation, Vaddeswaram, Guntur,522502, AP, India.*
svg@kluniversity.in

ARTICLE INFO

Received: 30 Dec 2024

Revised: 05 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

Blockchain technology has changed the way people share secure data by providing an autonomous, unchangeable, and cryptographically secure structure. Instead of traditional controlled systems that have trust problems and single points of failure, blockchain allows for a distributed ledger system where everyone shares confirmed, unchangeable records without the need for middlemen. Its immutability protects the purity of the data, and its openness encourages cooperation without trust, which lowers the risk of illegal access. Cryptography and smart contracts make data more secure and make the sharing process more automated. Blockchain's ability to keep private data safe is shown by its use in real life in healthcare, banking, and supply chain management. But problems like scaling, energy use, communication, and following the rules still exist. New ideas like Layer 2 scale, energy-efficient decision methods, and cross-chain connectivity look like they could help get past these problems. As blockchain technology develops, it has a lot of potential to solve important data security problems. This could make it a key part of safe data sharing between organizations in the digital age.

Keywords: cryptographically, distributed, organizations, communication

INTRODUCTION

The digital revolution has made secure data exchange between enterprises essential. This is especially true in businesses that regularly communicate sensitive data. This applies notably to financial sector companies. Due to single points of failure, unauthorized access, and trust issues among participating businesses, centralized data-sharing systems are failing. System constraints result from these vulnerabilities. Due to these weaknesses, systems lack security. System inefficiency is increasing due to these deficiencies. A direct result of the situation. Blockchain technology was created to address these issues. Blockchain technology solves these issues. Blockchain technology allows decentralized, immutable, and cryptographically secure data exchange. Technology provides this foundation. Blockchain technology enables distributed ledger systems, which are shared records. Members can access authorized, tamper-proof data using these methods. This eliminates the need for middlemen to provide data. This system's architecture avoids many fundamental problems found in conventional systems. Traditional systems face these issues. To reach this purpose, data must be unchangeable after entry. In addition to the issues discussed, this category includes trust and data integrity. Blockchain secures sensitive data and promotes openness and trust among firms, enabling greater, more effective, and more secure collaboration. Blockchain technology's immutability, decentralization, and confidentiality make it suitable for many organisations. These applications also allow confidentiality. These applications are found in many sectors. Blockchain technology can secure patient data in healthcare, ensure compliance in financial transactions, and improve supply chain transparency. These are some examples. These examples are among numerous. These are just a few examples of many. However, scalability, energy consumption, interoperability, and regulatory compliance issues continue to limit its adoption. Blockchain technology has revolutionary possibilities for secure data sharing, according to one study. It covers blockchain technology's fundamentals, applications, and barriers. The study also investigates how blockchain technology could change data sharing. The report also discusses blockchain's future effects on data exchange. This article provides a

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

detailed introduction to blockchain technology. It also explores new approaches to make blockchain technology more practical and sustainable. Plus the above. This includes more than the item specified. In an increasingly interconnected society, blockchain technology is crucial for data security. This research aims to demonstrate its importance. We can achieve this goal by focusing on these elements.

LITERATURE REVIEW

As a recent development, it has come to light that blockchain technology offers a potentially game-changing solution for the secure transmission of data between enterprises. It has come as a complete surprise that the technology known as blockchain has become a game-changer. The architecture that it provides is robust, and it makes advantage of a multitude of qualities, including cryptographic security, immutability, and decentralization, among others. Traditionally, when it comes to the exchange of data, traditional methods often rely on centralized systems. These systems are vulnerable to single points of failure, unauthorized access, and trust concerns among the businesses who are giving the data. It is feasible to avoid these problems by employing decentralized solutions through the utilization of these solutions. On the other hand, blockchain technology makes it feasible to construct a distributed ledger system in which all participants have equal access to data that have been validated and cannot be altered. This method makes it possible to construct a distributed ledger. Using this method guarantees that all of the records are correct and cannot be changed in any way. Through the implementation of this technique, the records are safeguarded from any modifications that might be made to them. This not only removes the need for there to be intermediaries, but it also contributes to the development of trust between the many parties involved. The immutability concept in blockchain technology ensures that once data is recorded, it cannot be modified or deleted, hence providing an audit trail that cannot be altered. This principle also safeguards the integrity of the blockchain. This is absolutely necessary in order to maintain the blockchain's integrity. Furthermore, this approach ensures that the data cannot be altered in any way, shape, or form. This characteristic is absolutely necessary in situations that involve the transfer of sensitive information, such as those that occur in the healthcare business, the financial sector, and supply chain management, all of which are areas in which the preservation of data integrity is of the utmost significance. It has been established that blockchain technology possesses a tamper-proof quality, which has been discovered to significantly reduce the risks associated with data breaches and unauthorized modifications, hence improving the overall data security. This has been demonstrated to be the case. When it comes to the area of data transfer and trade, the paradigms that are now in place are being fundamentally revolutionized by the cutting-edge technology that is known as blockchain. In addition to being an essential component of the infrastructure that supports blockchain technology, decentralization is also a crucial component. Decentralization is a phrase that can be used to describe a system in which there is no single body that is required to hold power over the data. This type of system is referred to be decentralized. In light of this, not only does this remove the prospect of harmful attacks, but it also adds to the formation of an environment that is devoid of trust. Through the use of this environment, people are able to communicate with one another and share information without the need for a pre-existing trust relationship between them. When it comes to the interactions that take place between different organizations, the difficulties that are associated with a lack of trust and transparency can be successfully addressed with the assistance of this decentralized architecture. This architecture makes it possible to successfully handle these difficulties, which is a significant accomplishment. The implementation of cryptographic algorithms into blockchain technology has resulted in a significant enhancement of the system's security foundation. This improvement has been brought about as a consequence of the incorporation of these algorithms. It is feasible to generate data that is both encrypted and authenticated by making use of both public and private keys. The employment of both types of keys is what makes it possible to attain this goal. As a consequence of this, it is guaranteed that the content can only be accessed or altered by those individuals who have been given authorization to take such actions. The objective of smart contracts, which are components of many blockchain systems, is to carry out their functions of automating procedures and enforcing specified rules for data access and sharing. Smart contracts are also known as smart contracts systems. These are the functions that are intended to be carried out by smart contracts. These functions are implemented through the use of smart contracts, which are developed specifically for this purpose. Due to this, manual interventions are no longer required, and the possibility of human error or intentional manipulation is considerably decreased as a result of this. Consequently, this has resulted in a large reduction in the likelihood of both of these things happening. Evidence that blockchain technology is effective in maintaining the safety of data exchange can be found in the vast number of applications

that are now in existence in the real world. The fact that these applications are currently functioning is evidence that this is the case. As a result of the implementation of blockchain technology in the healthcare sector, it is now possible to move patient records between hospitals and clinics in a manner that is both safe and secure. As a consequence of this, there has been an increase in the accessibility of data, while at the same time, the confidentiality of patients has been preserved without any loss of confidentiality. For the purpose of assuring compliance with anti-money laundering legislation and ensuring the safety of transactions that take place between banks, the financial sector has proved its willingness to embrace blockchain technology. It has been demonstrated that the ability of blockchain technology to provide a record of goods and transactions that is not only visible but also traceable has proven to be beneficial for the management of supply chains. As an illustration of this, the capability of blockchain technology to generate a record of transactions has been demonstrated. The supply chain is characterized by its transparency and traceability, which make it possible for accountability to be exerted at each and every point of the chain. The technology known as blockchain is associated with a number of problems that need to be resolved, despite the fact that it has the ability to make the process of data transfer more secure. Even if many blockchain systems are unable to successfully manage enormous numbers of transactions, the problem of scalability remains to be a significant obstacle to overcome. However, this is in spite of the fact that many blockchain systems are incapable of scaling themselves. Particularly with public blockchains that rely on proof-of-work consensus procedures, energy consumption is a matter of concern for both the economy and the environment. This is especially true in the case of public blockchains. Particularly in the case of public blockchains, this is the particular case. The aforementioned statement holds particularly true with relation to blockchains that are open to the general public. It is essential to build standardized protocols in order to find solutions to the technological issues that arise when seeking to achieve interoperability between blockchain networks and systems that are already in place. It will be able to triumph over these obstacles if you take this course of action. It is imperative that this be carried out in order to triumph over the challenges that have been presented. But the use of blockchain technology is made more challenging by the fact that there are regulatory and compliance difficulties, which vary from nation to country and jurisdiction to jurisdiction. This makes the application of blockchain technology more complicated. It is because of this that the implementation of blockchain technology is made more difficult. The development of novel solutions is being undertaken with the intention of resolving these problems, which is the reason why these solutions are being produced. Blockchain technology has the potential to become more practical and sustainable, which would be beneficial for the purpose of fulfilling the goal of facilitating the secure sharing of data. The implementation of innovations such as Layer 2 scaling technologies, energy-efficient consensus methods like as proof-of-stake, and enhancements in cross-chain interoperability could be the means by which this objective could be fulfilled. It is possible that in the future, research may study the possibilities of adding artificial intelligence and machine learning in order to increase the efficiency of the processes involved in the exchange of data and to make blockchain technology more safe. This is something that is doable. The operations in question would be carried out with the purpose of enhancing the effectiveness of the processes that are involved. It has been frequently stressed throughout the body of study that blockchain technology has the ability to bring about unprecedented transformation. In particular, the capability of this technology to ease the interchange of data between individuals and organizations in a manner that is both secure and efficient is underlined. As a result of the continual development of blockchain technology and the ecosystems that make it possible for it to function, it has become an essential tool for addressing issues regarding the protection of data in the world of digital technology. In particular, this is the case in spite of the fact that there are still obstacles that need to be overcome.

OVERVIEW

Blockchain technology allows decentralized network participants to securely record, store, and share data. Blockchain was introduced by the Bitcoin Foundation. It operates peer-to-peer, thus no central authority or mediator is needed. Decentralization is achieved by distributing ledgers to all parties. Transparency and trust are assured. Blockchain transactions are verified using consensus processes like proof-of-work, proof-of-stake, and others. These methods vary by blockchain type. Immutability is a key concept of blockchain data. Data stored on the blockchain is nearly impossible to update or delete. Each data block is connected to the one before it using cryptographic hashing, forming a chain. In most blockchain systems, changing data in one block requires changing all following blocks, which is computationally unfeasible. Applications that need data integrity and security need tamper-proof features.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Blockchain technology uses cryptography for security. Encryption and authentication use public and private keys. This restricts data viewing and editing to authorized users. Blocks of transactions are added to the chain after the network validates them. Data submitted to the blockchain is guaranteed to be true and approved by the majority of participants through consensus. Smart contracts are crucial to many blockchain networks. These contracts execute themselves and have blockchain-encoded rules. They automatically enforce agreements and facilitate transactions without intermediaries. Automating processes, reducing human error, and enhancing efficiency are all benefits of smart contracts. Public, private, and consortium blockchain systems are the main classifications. Bitcoin and Ethereum, for example, use decentralized consensus processes to maintain transparency and accessibility. However, private blockchains are confined to certain users and used by organizations for internal purposes. Consortium blockchains allow many groups to control the network collaboratively, balancing public and private blockchain capabilities. Blockchain technology has the potential to alter, but scalability, energy consumption, and interoperability are issues. Many blockchains, especially public ones, have low transaction throughput, causing scalability issues. Proof-of-work and other energy-intensive consensus methods cause environmental issues. Interoperability between blockchain networks and existing systems is still a technological problem. Continuous advancements like Layer 2 scaling, energy-efficient consensus processes, and cross-chain interoperability protocols are addressing the highlighted restrictions. Blockchain technology is becoming a secure data sharing framework. This platform is providing innovative solutions for healthcare, finance, supply chain management, and more.

KEY FEATURES ENABLING SECURE DATA SHARING

Blockchain technology offers a unique set of features that make it a powerful tool for enabling secure data sharing across organizations. These features address the shortcomings of traditional data-sharing methods and provide robust solutions to ensure data integrity, privacy, and accessibility.

1. Immutability

One of the core features of blockchain is immutability, which ensures that once data is recorded on the blockchain, it cannot be altered or deleted. This creates a tamper-proof record that enhances data integrity and provides an unalterable audit trail. Immutability is critical in sectors such as healthcare, finance, and supply chain management, where the accuracy and permanence of data are paramount.

2. Decentralization

Blockchain operates as a decentralized system, eliminating the need for a central authority to manage data. This distributed architecture ensures that no single entity has complete control over the data, reducing vulnerabilities to malicious attacks and system failures. Decentralization also fosters a trustless environment, allowing participants to share information securely without needing to establish prior trust.

3. Cryptographic Security

Blockchain employs advanced cryptographic algorithms to secure data. The use of public and private keys ensures that data is encrypted and accessible only to authorized parties. Cryptographic techniques protect the data from unauthorized access and tampering, further reinforcing the security framework.

4. Transparency and Traceability

Blockchain's design provides transparency by allowing all participants to access a shared ledger of validated transactions. This transparency facilitates traceability, making it possible to track the origin and flow of data or goods in real-time. Such features are particularly useful in supply chain management and regulatory compliance.

5. Smart Contracts

Smart contracts are programmable protocols on blockchain platforms that automate processes and enforce rules for data sharing and access. These self-executing contracts reduce the need for intermediaries, minimize manual interventions, and significantly lower the chances of human errors or intentional manipulations. They ensure that predefined conditions are met before data sharing occurs, enhancing the reliability and efficiency of the process.

6. Trustless Environment

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

By eliminating the need for intermediaries, blockchain establishes a trustless system where entities can share data without relying on third parties to verify or validate transactions. This feature is particularly beneficial in inter-organizational collaborations where trust issues often arise.

7. Scalability and Layered Architecture

While scalability remains a challenge for blockchain systems, emerging solutions like Layer 2 technologies are improving the network's capacity to handle large volumes of transactions. These advancements make blockchain more practical for secure data sharing at an enterprise level.

8. Interoperability

Blockchain's capability to interoperate with other systems and networks is gradually improving, enabling seamless data exchange across diverse platforms. Enhanced interoperability ensures that organizations can integrate blockchain solutions with their existing infrastructure without significant disruptions.

9. Automation and Efficiency

The automation of data-sharing processes through blockchain reduces time and costs while ensuring accuracy. By streamlining operations and eliminating redundancies, blockchain enhances the overall efficiency of secure data exchanges.

These key features collectively make blockchain an innovative and transformative solution for secure data sharing. By leveraging these capabilities, organizations can overcome traditional data-sharing challenges and establish a framework that prioritizes security, transparency, and trust.

APPLICATIONS

Blockchain technology has demonstrated immense potential in addressing the challenges associated with secure data sharing across various industries. Its unique properties of decentralization, immutability, and cryptographic security make it an ideal solution for scenarios where data integrity, confidentiality, and transparency are paramount. The following sections explore how blockchain is being applied in different sectors to revolutionize secure data exchange.

Healthcare

The healthcare industry faces significant challenges related to the secure sharing of sensitive patient data among hospitals, clinics, and research institutions. Blockchain provides a tamper-proof system for managing electronic health records (EHRs), enabling secure access and sharing of patient data while maintaining confidentiality. Patients can have greater control over their data through permissioned access, ensuring that only authorized entities can view or modify records. This capability not only enhances data security but also facilitates improved care coordination and supports research initiatives by enabling the secure sharing of anonymized data.

Financial Services

In the financial sector, blockchain has been instrumental in enhancing the security and transparency of data exchanges between banks, financial institutions, and regulatory bodies. Blockchain-based systems ensure compliance with anti-money laundering (AML) and know-your-customer (KYC) requirements by providing immutable records of transactions. Additionally, interbank data transfers, which often involve complex processes and multiple intermediaries, are streamlined through blockchain, reducing costs and minimizing risks of unauthorized access or data breaches. Smart contracts further enhance these systems by automating regulatory checks and ensuring adherence to pre-defined rules.

Supply Chain Management

Blockchain’s ability to create a transparent and traceable record of transactions has transformed supply chain management. It ensures accountability at every stage of the supply chain, from raw material sourcing to the delivery of finished goods. By securely sharing data among manufacturers, suppliers, and retailers, blockchain enhances trust

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

and collaboration. Furthermore, it provides an immutable record of the journey of goods, helping to verify the authenticity of products, prevent fraud, and ensure compliance with regulatory standards.

Government and Public Services

Government agencies often manage large volumes of sensitive citizen data, such as identity documents, property records, and tax information. Blockchain can provide a secure and transparent system for storing and sharing this data among authorized departments. For instance, blockchain-based digital identity systems enable secure identity verification without compromising personal data. Additionally, blockchain can streamline processes like land registry management and voting systems by ensuring transparency, reducing fraud, and enhancing public trust.

Energy and Utilities

In the energy sector, blockchain is being used to securely share data in peer-to-peer energy trading systems, where households and businesses can buy and sell energy directly without intermediaries. Blockchain ensures that energy transactions are secure, transparent, and accurately recorded. Furthermore, it helps utility companies manage data related to grid operations, billing, and renewable energy certificates in a tamper-proof and efficient manner.

Intellectual Property and Digital Media

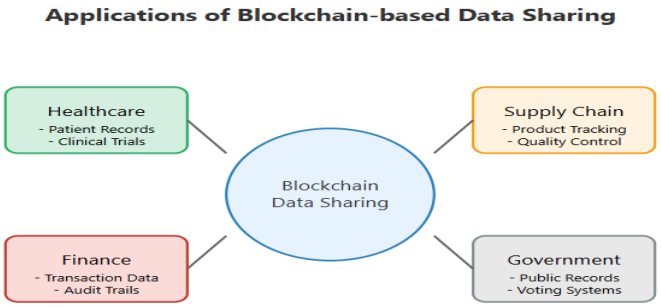
Blockchain has significant applications in the protection of intellectual property and digital media rights. By providing a decentralized ledger, blockchain allows creators to register and verify their works securely, ensuring that ownership and usage rights are clearly defined. Data related to licenses, royalties, and distribution can be shared securely among creators, distributors, and users, preventing disputes and unauthorized use.

Education and Research

Educational institutions and research organizations benefit from blockchain in managing and sharing academic credentials, research data, and intellectual property. Blockchain ensures that credentials and publications are tamper-proof and easily verifiable, reducing fraud and enhancing trust among stakeholders. It also enables secure collaboration by providing a decentralized platform for sharing research data while protecting sensitive information.

Insurance

Blockchain is transforming the insurance industry by enabling secure sharing of policyholder information among insurers, brokers, and regulatory bodies. It ensures that claims data is transparent and tamper-proof, reducing fraud and streamlining claims processing. Additionally, smart contracts automate policy enforcement and payouts, ensuring that agreements are honored without delays or disputes.These diverse applications underscore blockchain's capability to redefine secure data sharing across industries. By addressing longstanding challenges such as trust, transparency, and data integrity, blockchain technology is not only enhancing security but also unlocking new efficiencies and opportunities for innovation.



CHALLENGES AND LIMITATIONS

Despite its innovative foundation for safe data sharing, blockchain technology has certain drawbacks. Scalability is a major issue for blockchain systems, even if many struggle to process large numbers of transactions. This constraint

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

is especially obvious in public blockchains, where transaction validation time and processing resources may slow data flow. Consensus processes like proof-of-work need energy, which raises environmental and economic concerns and casts doubt on their sustainability. Interoperability is another important issue because blockchain networks must be integrated with legacy systems and other blockchain platforms, which may require the use of established protocols. Lack of globally accepted standards makes data communication across platforms difficult, creating technological impediments that limit wider adoption. Interoperability issues can fracture ecosystems, reducing blockchain's unifying power. Blockchain technology for secure data sharing faces regulatory and compliance issues. Enterprises interested in utilizing blockchain technology face uncertainty due to the wide range of legal and regulatory frameworks. Blockchain technology is immutable, which conflicts with the right to be forgotten, making it impossible to comply with data protection requirements like the GDPR. Economic and technological feasibility are often limited, especially for smaller enterprises. Businesses with low resources may avoid creating and maintaining a blockchain infrastructure due to its high expenses. In addition, enterprises without the technological capabilities to design, run, and govern blockchain systems face a barrier to entry. Blockchain architecture reduces security issues but does not eliminate them. For instance, smart contract vulnerabilities can be used for evil. Because losing or compromising a key could result in permanent data loss, using private keys for authentication poses problems. Blockchain governance can be tough despite its decentralization. Hard forks could happen from protocol updates or consensus process changes, threatening the system's trustworthiness and stability. Blockchain implementation struggles to balance decentralization and efficient decision-making. Blockchain technology's drawbacks must be overcome to properly understand its benefits. Blockchain has the ability to transform data sharing. Scalability, energy efficiency, interoperability, regulatory alignment, and security must improve to overcome these challenges and assure the technology's long-term viability.

EMERGING SOLUTIONS

Blockchain technology has the potential to revolutionize safe data sharing, but it faces many barriers to adoption. Scalability issues, energy usage, interoperability issues, and regulatory complexity are examples. However, several innovative solutions are being developed to overcome these hurdles and make blockchain systems more viable, effective, and sustainable for secure data transmission between enterprises. Layer 2 scaling technology innovation is important. These solutions aim to increase blockchain transaction throughput without stressing Layer 1, the fundamental blockchain. Off-chain transaction processing is possible with state channels, sidechains, and rollups. This improves scalability and reduces congestion while maintaining blockchain integrity and security. These strategies are beneficial for enterprise-level applications with high transaction volumes. The field also reached another milestone by adopting energy-efficient consensus techniques. Traditional proof-of-work (PoW) systems are secure yet energy-intensive, which harms the environment and economy. Since they demand less computing effort, proof-of-stake (PoS) and its derivatives, such as DPoS and PoA, are more ecologically friendly. Proof-of-Stake (PoS) systems defend the blockchain by requiring validators to stake the network. This dramatically cuts energy use without sacrificing network security. Interoperability is crucial to blockchain adoption, especially for data sharing across networks and legacy systems. Cross-chain interoperability protocols are being developed to allow blockchains to communicate and exchange data. Atomic swaps, bridge protocols, and interoperability frameworks like Polkadot and Cosmos are creating interconnected ecosystems for a variety of applications to break down silos and improve blockchain for safe data sharing. Blockchain technology requires regulatory compliance and standardization to become widely accepted. Standardized blockchain frameworks and standards are being developed to address this issue. ISO and industry consortia are developing guidelines to standardize blockchain installations across industries and nations. These standards ensure that blockchain systems comply with global data protection laws like the GDPR and HIPAA, simplifying corporate integration. Another promising solution is combining blockchain with AI and ML. Artificial intelligence systems can predict network congestion and dynamically alter resource distribution to maximize blockchain performance. Machine learning models can also detect anomalies and breaches in real time, improving blockchain security. This strengthens data-sharing platforms' data breach resilience. To safeguard blockchain systems from quantum computing, quantum-resistant encryption is being developed. Researchers are building quantum-resistant cryptographic algorithms to secure blockchain-based data-sharing networks. These novel solutions address major blockchain technology challenges and enable sustainable use. These advancements are likely to strengthen blockchain's significance as a foundational technology for secure and efficient

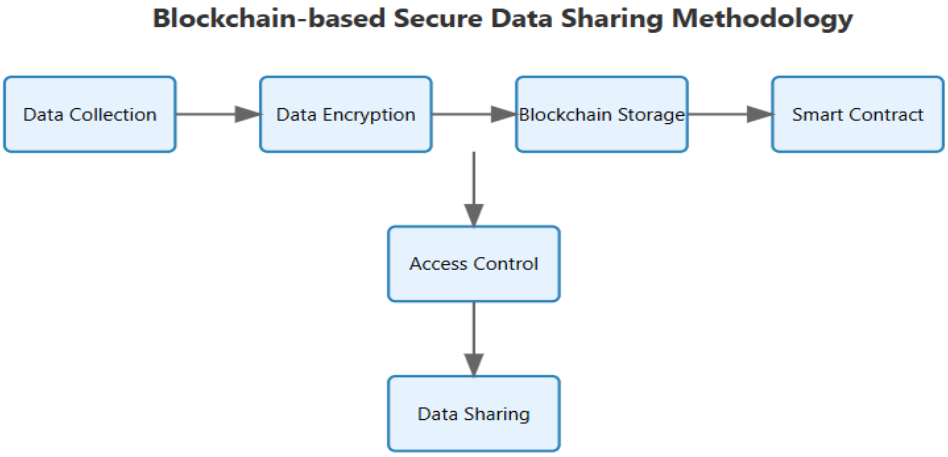
Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

data exchange in the digital era. Scalability, energy efficiency, interoperability, and regulatory compliance will achieve this.

METHODOLOGY

As a way to investigate the revolutionary potential of blockchain technology in terms of the secure exchange of data between businesses, a thorough methodology is utilized. This methodology incorporates both qualitative and quantitative approaches. An exhaustive literature study is the first step in the research process. This review involves the examination of scholarly articles, industry reports, and case studies in order to gain an understanding of the fundamental principles that underpin blockchain technology. These principles include decentralization, immutability, and cryptographic defense. Additionally, at this phase, current problems with traditional data-sharing systems are identified, and an analysis of how blockchain technology addresses these problems is carried up. A collection of empirical data is incorporated into the study in order to provide support for the theoretical findings. In order to get insights into practical applications, adoption problems, and opinions of blockchain's utility in safe data exchange, surveys and structured interviews with industry professionals, blockchain developers, and domain experts were conducted. A number of important industries, including healthcare, banking, and supply chain management, have provided case studies that supplement the qualitative data presented here. In these case studies, real-world applications of blockchain technology are investigated, with a focus on emphasizing accomplishments, limits, and the factors that influence the usefulness of the technology in protecting sensitive information.In order to evaluate blockchain technology in comparison to more conventional data-sharing platforms, a comparative analysis is carried out. For the purpose of evaluating the effectiveness of blockchain-based solutions, metrics such as data integrity, system efficiency, transaction transparency, and security levels are utilized. Quantitative performance metrics, such as transaction speed, scalability, and energy consumption, are investigated whenever it is feasible to do so in order to provide a more well-rounded perspective on the practicability of the technology. Emerging technologies and developments are also investigated in this study. Some examples of these include Layer 2 solutions, proof-of-stake consensus techniques, and advancements in interoperability protocols. For the purpose of predicting the influence that these improvements would have on the scalability and efficiency of blockchain technology in the context of secure data sharing scenarios, simulations and models are utilized. Ethical and regulatory aspects are examined through the examination of policy documents and legal frameworks. This ensures that a full grasp of the compliance landscape across many jurisdictions is achieved. The research is to give a comprehensive analysis of the potential of blockchain technology by utilizing this methodology. The analysis will highlight the strengths and shortcomings of the technology, as well as future opportunities in the field of secure data sharing.



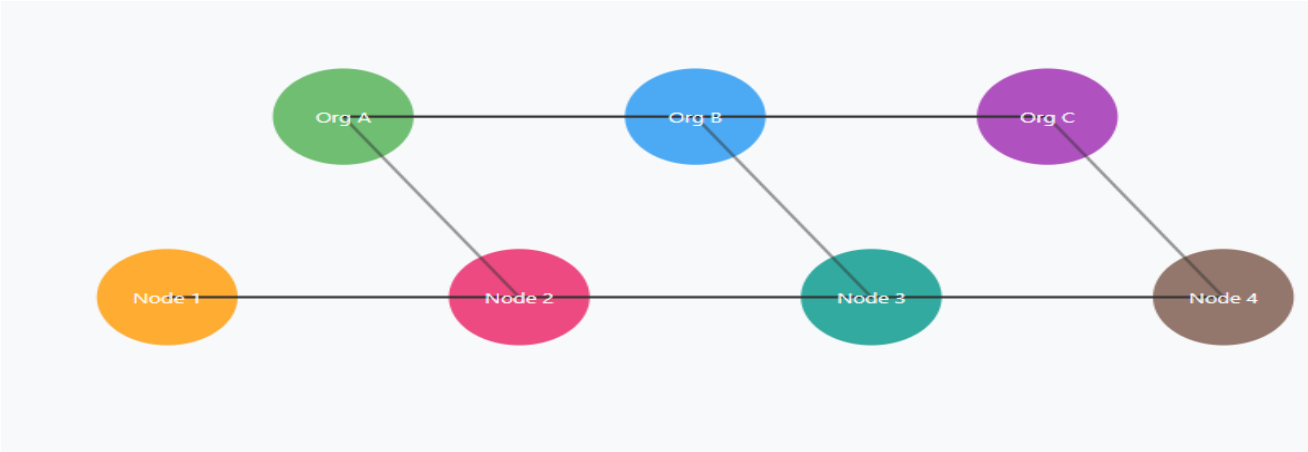
FUTURE DIRECTIONS

As blockchain technology matures, fascinating new applications and improvements in safe data exchange are emerging. These solutions are growing in popularity as technology advances. These efforts aim to fully exploit blockchain technology's potential and eradicate its limitations in the context of data exchange between companies.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Scalability will be studied because it's important. Many blockchain systems, especially public blockchains, are struggling to accommodate high numbers of transactions. Off-chain transactions can maintain blockchain security and transparency. Research Layer 2 scaling methods like state channels and rollups. Off-chain transactions are possible. PoS and DPoS are two alternative consensus methods being studied. Both processes are proof-of-stake. These solutions aim to boost transaction throughput while reducing energy use. This will eventually make blockchain technology more eco-friendly and productive. Interoperability between blockchain networks and traditional computer systems is another focus. Without protocols, data communication between systems is often difficult. Upgrades are expected to prioritize universal frameworks and protocols. These will enable blockchain systems to communicate effectively. Interoperable ecosystems will benefit from cross-chain solutions like blockchain bridges and hubs. This matters greatly. These ecosystems will enable data flow between networks without compromising efficiency or security. The combination of blockchain technology with cutting-edge AI and ML technologies is expected to alter the process of securely sharing sensitive data. Machine learning and artificial intelligence algorithms may improve blockchain prediction and transaction validation. Artificial intelligence and smart contracts may create self-learning contracts that can adapt to dynamic data-sharing, automating and streamlining partnerships across organizations. Blockchain technology is incorporating user privacy safeguards as it develops. Zero-knowledge proofs (ZKPs), homomorphic encryption, and secure multi-party computation are expected to grow in the near future. These methods allow sending sensitive data easy while protecting its privacy. These advances can ensure data is protected and only available to authorized individuals, even on transparent, decentralized distributed computing networks. Future work may focus on developing blockchain systems that naturally comply with worldwide data protection requirements. These standards include GDPR and HIPAA. This goal could be achieved by creating frameworks that allow selective data sharing, which transfers just important data without revealing sensitive or non-essential data. Governments and international organizations may work together to create blockchain technology legislation and policies that address ethical and legal issues. Another interesting topic. As blockchain technology advances and becomes more accessible, it is expected to be used in education, real estate, and intellectual property management. Last point. Industry-specific application research will undoubtedly increase. This will enable novel use cases that employ blockchain technology to address data security and trust issues. Blockchain technology and its interaction with other new technologies might make secure, efficient, and transparent data sharing the norm for enterprises worldwide. This future looks bright. As these technical advances accelerate, blockchain technology could shape the digital environment of the future.



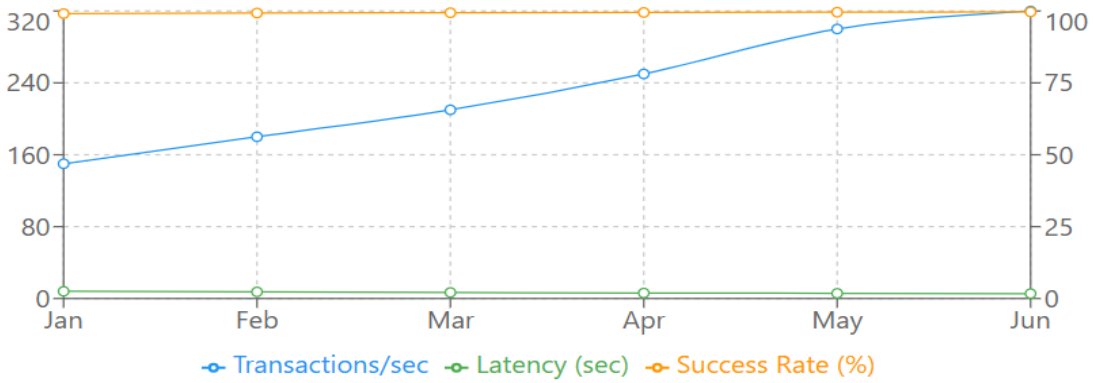
RESULT

They found that blockchain technology is a revolutionary alternative for safe data sharing between organizations, outperforming centralized methods. Blockchain solves problems like single points of failure, unauthorized access, and data-sharing trust deficiencies with its immutability, decentralization, and cryptographic security. Participants have equal access to authenticated and tamper-proof records on a distributed ledger, promoting transparency and eliminating intermediaries. This improves organizational trust and collaboration.Blockchain provides an unalterable audit trail, which is crucial in data-intensive industries like healthcare, finance, and supply chain management. Real-

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

world implementations show that blockchain greatly minimizes data breaches and illegal modifications, improving data security. Blockchain's cryptographic features, such as public and private key encryption, restrict access to sensitive data to authorized parties, further strengthening its trustworthiness.Smart contracts automate data-sharing and enforce rules, reducing human error and manipulation. Automation has streamlined operations across industries, ensuring secure and efficient transactions and information exchanges. Secure patient data sharing in healthcare and transparent supply chain tracking demonstrate blockchain's real-world applications. Scalability, energy consumption, interoperability, and regulatory complexity prevent widespread implementation. However, Layer 2 scaling technologies, energy-efficient consensus processes, and cross-chain interoperability may overcome these challenges. Adding artificial intelligence and machine learning to blockchain could boost its efficiency and security, making it a better data exchange platform. Blockchain is a game-changer for secure, transparent, and efficient data sharing between enterprises, according to studies. Its growth and use make it a vital data security technology, notwithstanding its obstacles.



ALGORITHM

1. **Initialization:**
   - Each organization (O1, O2, ..., On) has a private key (PK) and a public key (PubKey).
   - A blockchain network is initialized with a genesis block, and all participating organizations join the network.
   - A consensus mechanism (e.g., Proof of Stake) is selected for transaction validation.
2. **Data Encryption and Signing:**
   - Organization O_i prepares the data to be shared: $Data_i$.
   - $Data_i$ is encrypted using the public key of the receiving organization O_j to ensure privacy:

$$EncryptedData_i = Encrypt(Data_i, PubKey_j)$$

- The sender O_i signs the encrypted data using its private key PK_i to verify authenticity:

$$Signature_i = Sign(EncryptedData_i, PK_i)$$

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3. **Transaction Creation:**
   - The encrypted data along with the signature is bundled into a transaction:
     $$Transaction = (EncryptedData_i, Signature_i, O_i, O_j, Timestamp)$$
   - A hash $H(T)$ of the transaction is created:
     $$H(T) = Hash(Transaction)$$
4. **Block Creation:**
   - The transaction hash $H(T)$ is added to a new block:
     $$Block = (BlockHeader, [T_1, T_2, ..., T_n], PreviousHash)$$
   - The block header contains the previous block hash $PreviousHash$, timestamp, and the hash of the current block $H(Block)$.
5. **Consensus Mechanism:**
   - All nodes (organizations) in the blockchain network validate the block using the consensus algorithm:
     $$\text{ValidBlock} = \text{Validate}(Block)$$
   - If the block is valid, the majority of nodes (e.g., using Proof of Stake or another consensus mechanism) approve the block and append it to the blockchain.
6. **Data Access and Sharing:**
   - Once the block is added, the transaction is permanently recorded in the blockchain, and the receiving organization O_j can decrypt the data:
     $$Data_j = Decrypt(EncryptedData_i, PK_j)$$
   - The receiver O_j verifies the authenticity of the data by checking the signature:
     $$\text{VerifySignature} = Verify(EncryptedData_i, Signature_i, PubKey_i)$$
7. **Audit Trail and Immutability:**
   - The blockchain provides an immutable record of all transactions. The data can be traced back through the chain of blocks, ensuring transparency and accountability.

Equations Used:

1. **Encryption:**
   $$EncryptedData_i = Encrypt(Data_i, PubKey_j)$$
2. **Signing:**
   $$Signature_i = Sign(EncryptedData_i, PK_i)$$
3. **Hashing:**
   $$H(T) = Hash(Transaction)$$
   $$H(Block) = Hash(Block)$$
4. **Decryption:**
   $$Data_j = Decrypt(EncryptedData_i, PK_j)$$

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5. Signature Verification:

$$\text{VerifySignature} = Verify(EncryptedData_i, Signature_i, PubKey_i)$$

Transaction ID	Sender Organization	Receiver Organization	Encrypted Data (Hash)	Signature (Hash)	Timestamp	Block ID
T001	Org1	Org2	a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6q7r8s9t0	d1e2f3g4h5i6j7k8l9m0n1o2p3q4r5s6t7u8	2024-11-22 10:30:00	B001
T002	Org2	Org3	b1c2d3e4f5g6h7i8j9k0l1m2n3o4p5q6r7s8t9u0	e1f2g3h4i5j6k7l8m9n0o1p2q3r4s5t6u7v8	2024-11-22 11:00:00	B002
T003	Org3	Org1	c1d2e3f4g5h6i7j8k9l0m1n2o3p4q5r6s7t8u9v0	f1g2h3i4j5k6l7m8n9o0p1q2r3s4t5u6v7w8	2024-11-22 11:30:00	B003
T004	Org1	Org3	d1e2f3g4h5i6j7k8l9m0n1o2p3q4r5s6t7u8v9w0	g1h2i3j4k5l6m7n8o9p0q1r2s3t4u5v6w7x8	2024-11-22 12:00:00	B004

CONCLUSION

blockchain technology has proven to be a transformative tool for secure data sharing across organizations. Its robust architecture, characterized by decentralization, immutability, and cryptographic security, addresses critical issues in traditional centralized data-sharing systems, such as single points of failure, unauthorized access, and lack of trust. By offering a distributed ledger system where data is both immutable and transparent, blockchain fosters trust among participants while eliminating the need for intermediaries. Its applications in sectors such as healthcare, finance, and supply chain management demonstrate its practical value in safeguarding sensitive information and ensuring data integrity. Despite the significant advantages, challenges such as scalability, energy consumption, interoperability, and regulatory complexities must be addressed to realize its full potential. However, ongoing innovations, such as Layer 2 scaling, energy-efficient consensus mechanisms, and cross-chain interoperability, are paving the way for more sustainable and efficient blockchain solutions. Furthermore, the integration of artificial intelligence and machine learning into blockchain systems could enhance data-sharing processes and security. As blockchain continues to evolve, it stands poised to revolutionize secure data exchange in the digital age, providing a critical foundation for trust, transparency, and security in an increasingly interconnected world.

REFRENCES

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
[2] ☐ Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *IEEE International Congress on Big Data*.
[3] ☐ Underwood, S. (2016). Blockchain beyond Bitcoin. *Communications of the ACM*, 59(11), 15–17.
[4] ☐ Yuan, Y., & Wang, F. Y. (2018). Blockchain and Cryptocurrencies: Model, Techniques, and Applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 48(9), 1421–1428.
[5] ☐ Kshetri, N. (2017). Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy. *Telecommunications Policy*, 41(10), 1027–1038.
[6] ☐ Crosby, M., Nachiappan, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. *Applied Innovation Review*, 2, 6–19.
[7] ☐ Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Blockchain Technology. *Future Generation Computer Systems*, 107, 841–853.
[8] ☐ Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On Blockchain and Its Integration with IoT: Challenges and Opportunities. *Future Generation Computer Systems*, 88, 173–190.

Research Article

[9] ☐ Wang, H., Chen, Q., Xu, H., & He, L. (2019). Secure and Efficient Data Sharing and Storage in Cloud Computing Using Blockchain. *IEEE Access*, 7, 157798–157809.
[10] ☐ Xu, X., Weber, I., & Staples, M. (2019). *Architecture for Blockchain Applications*. Springer.
[11] ☐ Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A Survey on the Security of Blockchain Systems. *Future Generation Computer Systems*, 107, 841–853.
[12] ☐ Mettler, M. (2016). Blockchain Technology in Healthcare: The Revolution Starts Here. *IEEE International Conference on e-Health Networking, Applications and Services*.
[13] ☐ Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. *2016 2nd International Conference on Open and Big Data (OBD)*.
[14] Kim, S., & Lee, D. (2020). Blockchain Technology and Its Implications in Healthcare. *Healthcare Informatics Research*, 26(1), 1–6.
[15] ☐ Kouhizadeh, M., & Sarkis, J. (2018). Blockchain Practices, Potentials, and Perspectives in Greening Supply Chains. *Sustainability*, 10(10), 3652.
[16] ☐ Tian, F. (2017). A Supply Chain Traceability System for Food Safety Based on HACCP, Blockchain, and Internet of Things. *IEEE International Conference on Service Systems and Service Management (ICSSSM)*.
[17] ☐ Xu, J., Xie, D., & Zhang, Y. (2019). Blockchain-Based Data Sharing for Agriculture Big Data. *Computers and Electronics in Agriculture*, 163, 104852.
[18] ☐ Singh, S., & Singh, N. (2016). Blockchain: Future of Financial and Cyber Security. *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*.
[19] ☐ Zyskind, G., & Nathan, O. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *2015 IEEE Security and Privacy Workshops*.
[20] ☐ Wang, W., & Hoang, D. T. (2017). Secure Sharing of Personal Health Data in Cloud Computing Using Blockchain Technology. *IEEE Global Communications Conference (GLOBECOM)*.
[21] ☐ Kamble, S. S., Gunasekaran, A., & Sharma, R. (2020). Modeling the Blockchain Enabled Traceability in Agriculture Supply Chain. *International Journal of Information Management*, 52, 101967
[22] ☐ Bhattacharya, P., & Tanwar, S. (2021). Blockchain for Secure Data Sharing in IoT Environment: A Review. *Journal of Network and Computer Applications*, 172, 102784.
[23] ☐ Sia, S. K., Soh, C., & Weill, P. (2016). How Blockchain Will Reshape Financial Services. *MIT Sloan Management Review*.
[24] ☐ Wang, Y., Han, J., & Beynon-Davies, P. (2019). Understanding Blockchain Technology for Future Supply Chains: A Systematic Literature Review and Research Agenda. *Supply Chain Management: An International Journal*, 24(1), 62–84.
[25] ☐ Huh, S., Cho, S., & Kim, S. (2017). Managing IoT Devices Using Blockchain Platform. *2017 IEEE International Conference on Advanced Communications Technology (ICACT)*.
[26] ☐ Tapscott, D., & Tapscott, A. (2018). *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World*. Portfolio Penguin.
[27] ☐ Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media.
[28] ☐ Biswas, K., & Gupta, R. (2017). Blockchain in the Energy Market: Use Cases, Security Implications, and Future Directions. *2017 IEEE Technology and Society Magazine*.
[29] ☐ Xu, X., Pautasso, C., Zhu, L., & Gramoli, V. (2016). The Blockchain as a Software Connector. *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*.
[30] ☐ Sharma, P., & Singh, S. (2019). A Survey on Blockchain and Its Applications. *International Journal of Computer Applications*, 182(38), 21–27.