International Journal of Management and Humanities (IJMH)
ISSN: 2394-0913 (Online), Volume-10 Issue-7, March 2024

Review on Data Privacy, Protection, and Security Challenges in Blockchain Adoption Across Diverse Domains

Shailja Garg, Tamal Mondal

Abstract: ***This paper examines how blockchain technology can transform data management, particularly in addressing privacy and security concerns. Blockchain's immutability, transparency, and decentralisation make it a potentially valuable tool for addressing the growing problems associated with data security and integrity. However, the slow adoption of blockchain technology is influenced by a complex interplay of developing privacy concerns, legislative uncertainty, and technological subtleties. The current study aims to identify key data privacy, protection, and security challenges associated with blockchain adoption in various domains, assess the adequacy of the current data privacy, safety, and security laws to address these challenges, and propose potential solutions and areas for further research to mitigate data privacy, safety, and security risks in blockchain applications. Additionally, the study has examined the adaptability and dependability of the two main kinds of blockchain—public and private—as well as the variations in their reach and visibility.***

Keywords: Blockchain, Adoption, Challenges, Privacy, and Domains.

I. INTRODUCTION

Amid the digital revolution, the rapid advancement of technology is putting our world on the verge of revolutionary transformation. Data is the precious currency at the centre of this paradigm shift. When data powers economic engines, drives direct decision-making, and intertwines the fabric of our globalised communities, data security, privacy, and protection have become critical issues. Current data management paradigms need to be reevaluated in light of the growing amount and importance of data in our daily lives [6] [7]. In this context, blockchain technology shows great promise as a decentralized [14], unchangeable ledger with the potential to completely transform data management in a variety of industries like Healthcare, Transportation, Supply chain, Government Sectors etc. The intrinsic qualities of blockchain, i.e. immutability, transparency, and decentralization, make it a transformative tool that can effectively tackle growing issues related to data security and integrity [11].

Manuscript received on 24 February 2024 | Revised Manuscript received on 13 March 2024 | Manuscript Accepted on 15 March 2024 | Manuscript published on 30 March 2024.

**Correspondence Author(s)*
Shailja Garg*, Department of Symbiosis Centre for Information Technology, Symbiosis International University, Pune (Maharashtra), India. E-mail: shailja.garg@associates.scit.edu, ORCID ID: 0009-0000-9422-3739
Tamal Mondal, Department of Symbiosis Centre for Information Technology, Symbiosis International University, Pune (Maharashtra), India. E-mail: tamal@scit.edu

However, a methodical and cautious approach has been taken along the way toward the broad adoption of blockchain technology, impacted by a complex interplay of developing privacy concerns, legislative uncertainty, and technological subtleties [9]. Data plays a pivotal role in the digitization process and influences the course of both economies and societies. The smooth operation of financial systems, the development of healthcare and governance, and the smooth operation of industries demonstrates its ability to transform [3] [4] [8]. However, the susceptibility of centralised data repositories to security lapses, unauthorised entries, and malicious attacks highlights the pressing need for alternatives and secure solutions. Blockchain technology offers a decentralized, impenetrable structure for data transport and storage, which by design aims to address these problems [1][2][11]. Blockchain's appeal stems from its capacity to redefine trust in transactions and relationships, in addition to its cryptographic foundations. Data cannot be changed or tampered with once it has been recorded, thanks to immutability, which promotes an integrity level that is unmatched in conventional systems [10]. Accountability is enhanced and participant confidence is nurtured when transparency is promoted through the use of a shared and distributed ledger. The core idea behind blockchain technology is decentralisation, which eliminates the need for intermediaries and enhances system security by reducing the likelihood of single points of failure. [1][3][4]. Blockchain versatility spans diverse industries and revolutionizes operations in critical sectors. The supply chain ensures unprecedented transparency and traceability, effectively mitigating fraud and errors. Healthcare experience enhances patient data security and interoperability through blockchain, guaranteeing privacy and seamless data sharing. In finance, technology streamlines transactions, reduces fraud, and fosters transparency in banking systems. Blockchain has contributed to improved governance by enhancing the transparency and security of government records and processes. Furthermore, in real estate, it facilitates transparent and secure property transactions while maintaining robust record-keeping practices. The transformative impact of blockchain resonates across these domains, reshaping traditional practices and bolstering security measures. Notwithstanding these attractive attributes, the assimilation of blockchain technology into conventional operations is distinguished at a slow pace. Organisations have adopted a cautious stance due to technological complexity, a lack of established frameworks, and unclear regulations.

Due to its decentralised structure, blockchain technology poses challenges in balancing data protection regulations with its transparent and immutable architecture. Privacy issues, in particular, have emerged as significant roadblocks to the rapid adoption of technology. The intricate balance between the advantages of blockchain technology and the barriers to its widespread adoption is made clear when taking data privacy and security concerns into account [13]. Although blockchain technology is decentralised and secure, integrating it with existing legal and regulatory structures can be challenging. The inherent and immutable nature of the technology creates a complex environment that requires careful navigation and raises concerns about compliance with data protection laws. As a result, businesses must choose between the revolutionary potential of blockchain technology and the requirement to ensure data security and privacy.

Contribution: To examine data privacy, protection, and security issues that arise when blockchain technology is implemented in various industries, the current study conducts a thorough literature analysis. Its goals are to identify the main obstacles, evaluate how well the existing legal systems meet those needs, and suggest ways to reduce the risks associated with blockchain applications. This study aims to address the current research gaps and provide guidance to scholars, decision-makers, and business partners on strategies for increasing blockchain adoption in relevant domains. More specifically, it clarifies the relationship between blockchain adoption and regulatory frameworks, addresses key questions, and offers guidance on this emerging subject. The goal of this work is to facilitate the responsible and secure integration of blockchain technology, thereby shaping the course of our digital future, by carefully examining the complex web of technology adoption.

A. Objective of the Study

1. Key data privacy, protection, and security challenges associated with blockchain adoption in various domains are identified and analyzed.
2. Assess the adequacy of the current data privacy, protection, and security laws to address these challenges.
3. Propose potential solutions and areas for further research to mitigate data privacy, protection, and security risks in blockchain applications.

B. Research Questions:

RQ1: What are the prominent data privacy, protection, and security challenges impeding widespread blockchain adoption?

RQ2: How do existing legal frameworks align with blockchain's decentralized nature, and to what extent do they address identified challenges?

RQ3: What potential solutions and future research directions can be proposed to mitigate the risks in blockchain applications?

II. REVIEW OF LITERATURE

The flexibility and dependability of blockchain technology are ensured by its decentralisation, consensus mechanisms, provenance, immutability, and finality, which guarantee its adaptability and reliability. Because the blockchain is decentralized, transactions are decided by participant consensus rather than by a single entity. Provenance guarantees traceability, enhances security, and logs particular data in each block. Immutability improves security by preventing changes. The scope and visibility of the two primary forms of blockchain — public and private — vary. A widely distributed public blockchain preserves data integrity and confidentiality but jeopardizes privacy[2]. Private and consortium blockchains, on the other hand, are limited to particular areas chosen by businesses, meaning that data access is more tightly controlled. This distinction represents a trade-off between consortium and private blockchains' limited accessibility and public blockchains' openness [11]. With its applications in healthcare, the Internet of Things (IoT), finance, and smart cities, this technology fosters openness and confidence among stakeholders. Due to its special qualities, blockchain is positioned as a transparent and safe solution in a variety of industries [11] [15]. The consideration of social influence, cost, trust, and security suggests a holistic perspective on blockchain adoption. The technological elements, obstacles, and facilitators of implementing blockchain technology in supply chain management [1]. The application of blockchain technology in guaranteeing food safety, quality, and intellectual property protection is highlighted by highlighting its features, which include traceability, immutability, and security. Processes are automated using smart contracts [16], increasing productivity and privacy. However, the challenges include scalability [23], latency concerns, and lack of interoperability. While blockchain provides enhanced cybersecurity [18], vulnerabilities such as 51% attacks and data breaches persist. Immutability has become a double-edged sword, as it prevents data removal, posing challenges for data quality and regulatory compliance. Cybersecurity risks and issues related to data quality and privacy regulations further complicate blockchain adoption [3] [17]. The adoption of blockchain by the government faces significant challenges. Government employees often lack the necessary skills, clear regulations are usually missing, and awareness is limited. Other hurdles include resistance to change, resource constraints, and security concerns [5]. Blockchain adoption for healthcare waste management faces significant challenges. Incompatible systems and data formats, security concerns, unclear regulations, high costs, and a lack of awareness hinder their use. Developers must address these technological and regulatory challenges to bring blockchain's potential to healthcare waste management [4].

Integrating blockchain with the Internet of Things (IoT) offers benefits in terms of security, transparency, and automation, but it also presents challenges. Smart contracts and blockchain networks lack complete security, thereby causing vulnerabilities. High data volumes and transaction-overload systems hinder scalability. Data storage and access raise privacy concerns. Finally, different platforms lack standardization and interoperability, creating incompatibility barriers. Addressing these challenges is crucial for successful blockchain-IoT integration [6] [12].

Examining the implementation and adoption challenges across diverse domains reveals that issues related to data privacy, security, and cybersecurity threats stemming from the open-

source nature of blockchains consistently emerge as prominent barriers.

The inherent characteristics of blockchain, such as its openness, present significant obstacles to ensuring robust data protection and safeguarding against cybersecurity risks, posing considerable challenges to its widespread adoption.

GDPR regulations play a crucial role in safeguarding user data by providing guidelines for the transparent and fair use of personal data. Personal data, encompassing identifiable information such as names, phone numbers, and IP addresses, falls under the jurisdiction of the General Data Protection Regulation (GDPR). Compliance with the GDPR is essential for digital services, as providers assume the roles of controllers, collectors, and processors. Responsibilities included swift data transfer, obtaining permission for data processing, and ensuring a holistic understanding of third-party data management. GDPR compliance for digital services necessitates adherence to principles such as data minimization, fairness, accuracy, transparency, and confidentiality [11]. The identified research gap in the literature pertains to the insufficient exploration of the clash between blockchain's characteristics—emphasising transparency and immutability—and existing legal standards, particularly exemplified by the General Data Protection Regulation (GDPR) (Table 1: GDPR vs. Blockchain). While there is recognition of the conflict in priorities between blockchain's focus on data transparency and immutability, and GDPR's emphasis on individual data rights and control, the specific implications, challenges, and potential solutions at the intersection of these two frameworks remain inadequately addressed. There is a need for further research that delves deeper into understanding, resolving, or mitigating the conflicts arising from this misalignment to facilitate the effective coexistence of blockchain technology and legal standards.

Table 1: GDPR vs. Blockchain

GDPR vs. Blockchain		
Feature	**GDPR**	**Blockchain**
Objective	Empower individuals with data control and privacy in the EU.	Provide a decentralized platform for secure and transparent data recording and management.
Data Ownership and Control	People are entitled to see, amend, remove, limit, and refuse the processing of their personal information.	Varies depending on permission level. Permissioned blockchains offer more control, while permissionless prioritize openness and immutability.
Data Access and Transparency	Requires transparency in data collection, processing, and storage. Individuals have the right to request information about their data.	Offers inherent transparency due to its public ledger system, unless privacy-enhancing features are implemented.
Data Security and Privacy	Enforces strict security measures to protect personal data. Organisations must implement appropriate safeguards to ensure compliance.	Provides inherent security through cryptography and consensus mechanisms, but vulnerabilities in smart contracts or protocols can expose data to risks.
Compliance and Accountability	Holds organizations accountable for protecting personal data and complying with the regulation. Non-compliance leads to significant fines.	Decentralized nature makes enforcement challenging. Existing legal frameworks may not readily apply to this situation.
Scalability and Interoperability	Applies to all organisations that process data of individuals within the EU, regardless of size or location.	Scalability and interoperability vary across different platforms, posing challenges for global compliance and data exchange.
Evolution and Adaptability	A relatively new regulation with ongoing interpretations and updates to address evolving technologies and privacy concerns.	A rapidly evolving technology with diverse use cases and ongoing development of privacy- enhancing features and protocols.

III. METHODOLOGY

A. Literature Selection

This study reviewed earlier studies on blockchain adoption using a systematic review methodology. This approach provides a comprehensive synthesis of the subject under study, identifying relevant resources on the topic. The current investigation complied with other pertinent systematic reviews and Kitchenham and Charters' guidelines for systematic reviews [21]. The ensuing subsections provide a detailed description of each stage involved in the review process.

Establishing a suitable search protocol is one of the most effective ways to identify relevant publications. The fundamental elements for an exploration strategy are keywords. Typically, research questions lead to the creation of keywords. Additionally, some of the technical term replacements were employed. Both "AND" and "OR" Boolean operators were employed.

Keywords: Blockchain, Adoption, Challenges, Privacy, Cyber Security, Data Privacy, IoT (Internet of Things), Supply Chain Management, Healthcare, Government Data Protection Regulation

Abstracts, keywords, and titles were searched. The search results were extracted on December 10, 2023.

The databases searched were IEEE and Scopus. Scopus is a reputable database that indexes top-notch research articles. This is a globally renowned database used as a standard by scholars worldwide. To broaden the search, we also ran a search on the IEEE Xplore Digital Library. The inclusions as well as the exclusion criteria, which are covered in greater detail in the following sections, were used to filter the findings after the extraction procedure.

We conducted a search using the selected terms we had chosen. Once the search results were identified, we applied several filters and criteria to exclude articles that were not as relevant. To correctly answer the research questions, a final list of publications was created and examined.

Inclusion Criteria

- Possibly released after 2015.
- It has to be written in English.
- Digital databases contain the entire text.
- A journal, magazine, or conference proceeding must publish the article.
- Including a theoretical foundation for blockchain evaluation.
- Need to monitor the adoption, recognition, or long-term use of blockchain technology.

Exclusion Criteria

- Studies not in English.
- Research on blockchain without a theoretical foundation.
- Research that uses a theoretical model devoid of blockchain.
- Article duplication.
- Reviews of articles and books.
- Articles that don't include subjects about compliance, Discourse on blockchain and GDPR.

In addition, a modified version of the nine-criteria checklist from Alqudah et al. [24] and Al-Emran et al. [23] was employed to assess the calibre of the thirty research papers (n = 30) that were retained for further examination.

- Was the purpose of the study achieved?
- Is it true that change was taken into account in this study?
- Is the study's discipline and substance well defined?
- Is the content sufficiently specialised? How is data collected? Are the indicators' validity and dependability described clearly?
- Is the explanation of the statistical techniques utilised to examine the data adequate?
- Are these findings documented in more detail?
- Did this research improve your understanding or knowledge?

With the use of the above-specified search techniques, 527 objects were found. Eighty-two of them were duplicates; therefore, we removed them from the analysis. As a result, 445 studies were completed. For each survey, the acceptance criteria were applied.

Therefore, thirty articles that met these criteria were retained for the study. “Private Reference Material for Systematic Reviews and Meta-analyses (PRISMA)” was used during the search and curation process [22]. Figure 1 shows the flowchart of PRISMA.

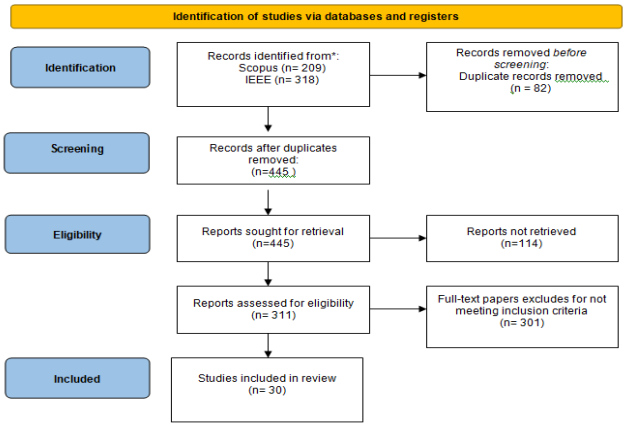

Figure 1: Research Methodology

B. Steps of Research

Each step addresses the question, and answering it will help you gain a better understanding of the problem. This step was created after a comprehensive review of existing data on the blockchain campaign for adoption. We analyse the researcher's design process as involving two main stages: identification and classification. The researchers first describe the benefits of blockchain and then outline its challenges, focusing on specific challenges in areas such as government, healthcare, supply chain, and the Internet of Things. In the event of a conflict analysis, any violation of the data privacy policy is examined. Problem-solving strategies and future research directions are presented, and conclusions are drawn that suggest areas for further research. Our study modelled this by breaking it down into five phases: analysis, classification, conflict analysis, available solutions, and conclusion. Each phase is based on a specific research question and aims to solve various challenges affecting blockchain implementation.

1. Identification: Challenges in Blockchain Adoption:

- What are the specific challenges faced in the government sector when adopting blockchain technology?
- What challenges does the healthcare industry encounter in integrating blockchain solutions?
- What are the hurdles in implementing blockchain in supply chain management?
- What challenges arise when applying blockchain in IoT?

2. Separation: Security and Privacy Concerns:

- What are the primary security concerns associated with implementing blockchain in government processes?
- How do security and privacy concerns manifest in healthcare blockchain applications?
- What specific privacy issues arise when deploying blockchain in supply chain operations?
- What security issues arise frequently when blockchain technology is used in Internet of Things applications?

3. Conflict identification: Elements of Blockchain Contradicting Data Privacy and Security Requirements:

- Which elements of blockchain technology may conflict with legal and regulatory data privacy requirements in government applications?
- How does blockchain architecture contradict healthcare data privacy and security regulations?
- What aspects of blockchain technology pose challenges in meeting data privacy requirements in supply chain management?
- In what ways do IoT blockchain implementations contradict data security and privacy standards?

4. Existing Solutions: Means to Enhance Blockchain Adoption:

- What strategies can be employed to overcome government-related challenges and enhance blockchain adoption?
- How can healthcare institutions allay worries about privacy and security while encouraging the use of blockchain technology?
- What approaches, keeping in

mind the existing roadblocks, can improve the application of blockchain technology in supply chain management?
- Given the security and privacy concerns, what strategies may be used to support the adoption of blockchain in the Internet of Things?

5. Conclusion: Areas of Research and Development for Increased Blockchain Adoption:
- What are the current gaps in research regarding blockchain adoption in government, and how can they be addressed?
- What specific areas in healthcare require further research to facilitate secure blockchain adoption?
- In supply chain management, what aspects need more attention in terms of blockchain technology adoption?
- What innovative solutions can be developed for secure blockchain adoption in IoT applications?

C. Mapping Overarching Research Questions to Research

Each of the five steps focused on data security and privacy challenges in blockchain adoption across Government, Health Care, Supply Chain, and IoT domains is mapped to the research question in Figure 2 and Figure 3

Research Question 1: What are the prominent data privacy, protection, and security challenges impeding widespread blockchain adoption?
- Separation: Security and Privacy Concerns in Blockchain Adoption in Government, Health Care, Supply Chain, and IoT domains

This directly addresses the security and privacy challenges in different domains.
- Conflict identification: What are the elements of blockchain and its working that contradict data privacy and security requirements set by legal and regulatory bodies?

This aligns with the identification of elements in blockchain that may conflict with legal and regulatory requirements.

Research Question 2: How do existing legal frameworks align with blockchain's decentralized nature, and to what extent do they address identified challenges?
- Identification: What are the challenges in Blockchain in Government, Health Care, Supply Chain, and IoT domains

This indirectly contributes to understanding the challenges in various domains, particularly in light of legal frameworks.
- Conflict identification: What are the elements of blockchain and its working which contradict data privacy and security requirements set by legal and regulatory bodies?

This aligns with RQ2 by exploring how legal frameworks interact with the elements of blockchain and identifying contradictions.
- Existing Solutions: What are the existing means which can enhance and increase the blockchain adoption rate?

This explores means and strategies to enhance blockchain adoption, including legal considerations.

Research Question 3: What potential solutions and future research directions can be proposed to mitigate risks in blockchain applications?
- Conclusion: What are the potential areas of research and development, and blockchain working frameworks where changes can be brought in to increase the rate of blockchain adoption

This is aligned with identifying potential areas of research and development to address challenges and enhance adoption.
- Identification: What are the challenges in Blockchain in Government, Health Care, Supply Chain, and IoT domains?

This aligns with RQ3 by emphasizing challenges that can be addressed through potential solutions.
- Existing Solutions: What are the existing means which can enhance and increase the blockchain adoption rate?

This aligns with RQ3 by focusing on existing means and solutions to enhance blockchain adoption.

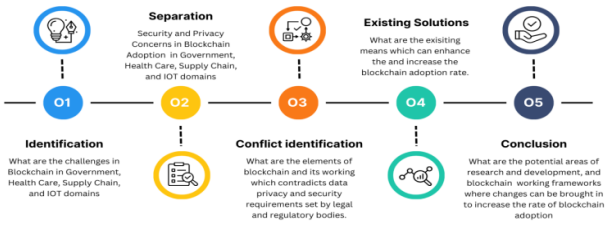

Figure 2: Methodology Steps

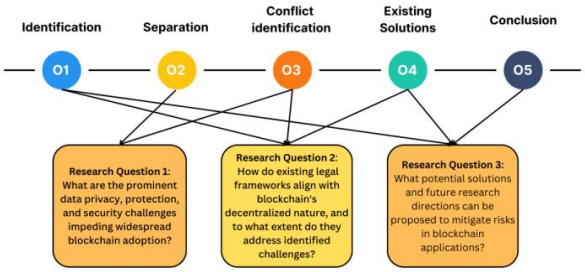

Figure 3: Mapping Overarching Research Questions to the Research Process

IV. ANALYSIS

A. External Factors Influencing the Blockchain Technology Adoption

A review of the collected literature reveals the primary external variables influencing the adoption of blockchain technology. Trust was shown to be the most crucial factor, followed by perceived cost and social impact. Performance expectations, effort expectations, and information security closely follow facilitating conditions. Security and privacy concerns, high energy and investment costs, organizational barriers, and technical challenges are also mentioned [1]. Notably, political restrictions have received little attention, indicating a potential avenue for future research [11].

Economic Influence on Adoption: Economic factors significantly shape the adoption of blockchain technology. High implementation and maintenance costs stand out as significant barriers, particularly for small and medium enterprises.

Paradoxically, the potential for cost reduction by eliminating intermediaries and enhancing

efficiency has acted as an enabler. Uncertainties regarding return on investment and adoption advantages were presented by the dual nature of expenses, which included both enablers and obstacles. Competition has become a powerful facilitator.

Sociocultural Dynamics: Sociocultural factors revealed intricate challenges and paradoxes in blockchain adoption. Trust creation through transparency faced resistance as companies struggled to handle sensitive information. Organisational culture, resistance to change, and a lack of knowledge emerged as barriers. In contrast, external stakeholder resistance, cultural differences, and the absence of real-world use cases further complicated the landscape. The hesitancy to experiment with blockchain, exacerbated by a lack of working cases, formed a self-reinforcing cycle.

Technological Hurdles and Opportunities: The technological aspects of blockchain were central to discussions, with traceability, immutability, and security being key enablers of its potential. Smart contracts were hailed to automate processes, reduce settlement times, and enhance privacy [16]. However, scalability, interoperability, and compatibility are recurrent barriers. Cybersecurity risks, including vulnerability to hacking and potential threats from quantum computing, pose additional hurdles [18]. The immutability of blockchain data has emerged as both an advantage and a barrier, complicating error correction and compliance with data protection regulations.

Legal and Regulatory Landscape: Blockchain transparency and immutability have been recognised for their potential in enhancing audit ability and contract enforcement. However, the absence of comprehensive legislation and regulations poses a barrier, leading to case-specific implementation. The global nature of blockchain networks has raised jurisdictional challenges and compliance risk.

Environmental Considerations: The ecological impact of blockchain showcases a dual nature. On the one hand, the digital nature of the technology reduced paperwork and facilitated the measurement of carbon footprints. However, its high energy consumption, particularly in proof-of-work consensus algorithms, has raised environmental concerns. This discussion highlights the importance of carefully evaluating the overall benefits of increased power usage. Customer perceptions of blockchain's ecological impact were deemed significant, suggesting the importance of effective communication strategies to address these concerns.

Awareness and Education Challenges: A lack of awareness has emerged as a significant challenge to blockchain adoption. Perceived awareness has been identified as a key influencer of citizens' willingness to adopt new technologies. The relative novelty of Blockchain technology contributed to a widespread lack of awareness, underscoring the importance of education and communication in fostering adoption.

B. Existing Challenges in Blockchain Adoption

The adoption of blockchain technology faces several challenges, including scalability, interoperability, regulatory compliance, complexity, and security. Integrating multiple platforms is difficult, while scalability and transaction speed limit large-scale implementation. Uncertainty management lags behind technological development. Blockchain's complexity and lack of governance hinder its adoption, while security concerns undermine trust. Addressing these issues requires collaboration among stakeholders, policymakers, and researchers to design and manage the adoption process effectively. These are challenges specific to government, healthcare, supply chain and IoT.

IoT.Domain: Various obstacles prevent the mainstream implementation of blockchain technology within the Internet of Things. One of the primary challenges is the lack of Internet of Things (IoT) devices. IoT devices are not a good fit for highly computational and time-consuming blockchain technologies, such as hash functions, cryptographic algorithms, consensus algorithms, and smart contracts in their pure form [25]. IoT devices generate a significant amount of data, which in turn raises the need for storage. Currently, the size of blockchain hashes is comparatively high for these devices. To overcome these resource constraints, researchers have suggested modifications and enhancements to the blockchain mechanism. Examples of these include the creation of blockchains tailored explicitly for the Internet of Things infrastructure and the virtualisation concept. A further major obstacle to blockchain adoption in the Internet of Things is security. Current cryptographic functions are considered too significant and unsuitable for blockchains in the Internet of Things (IoT), such as RSA-based public key encryption and elliptic curve cryptography. Additional obstacles are presented by issues pertaining to data confidentiality, availability, and integrity. Because it's thought that criminal entities are using blockchain to their advantage for financial gain, its reliability is called into question [25]. Furthermore, the absence of firmware and configuration update procedures makes IoT devices more vulnerable to hacking and creates security flaws. Scalability is, therefore, a crucial concern. Although blockchains' distributed architecture offers security advantages, their implementation must be done carefully to prevent scalability issues. IoT node storage is strained when a blockchain grows in size because of the corresponding increase in blockchain hash size. Semantic blockchains and scalable architectures for access control are among the suggested remedies, and utilising edge, cloud, or fog computing nodes is recommended to alleviate the strain on IoT devices and maintain a hybrid distributed architecture [25]. Concerns about privacy and anonymity occur when public keys or hashes are used in BIoT as identifiers. Applications such as competent healthcare, where users may not wish to reveal their identities or maintain data privacy, make anonymity essential. To address this issue, proposals for global privacy standards have been presented, suggesting the use of private blockchains to restrict user access to specific domains [25]. Smart contracts, consensus algorithms, and legal concerns exacerbate these difficulties. The implementation of consensus algorithms has become increasingly challenging due to the limited computational, storage, memory, and bandwidth resources of IoT devices. Despite the advantages of smart contracts, there is still a need for low-cost BIoT deployment. Legal issues have arisen in various applications, such as asset tracking and supply chains, due to regulatory concerns, including the lack of standards for blockchain technology.

Implementation of blockchain in IoT is further complicated by many issues such as device

heterogeneity in IoT, interaction between processes and models, throughput and latency, integration of Bio T, reliable firmware updates of IoT, and vulnerabilities in blockchain algorithms [25].

Healthcare Sectors**:** Blockchain adoption in healthcare faces many challenges that must be resolved for success. Limitations on Scalability: Scalability presents a significant difficulty. The trade-off between the amount of medical transactions and the available computational power may constrain the scalability of blockchain healthcare systems. The blockchain network has to be able to manage the increased volume of transactions effectively. High Development Costs: Implementing blockchain-based healthcare solutions may incur significant development and operating costs. Differentiating the development, operating, and deployment expenses for each stakeholder is crucial. For broad adoption, reducing total costs and maximising the use of available resources are essential. Standardisation Challenges: Standardisation bodies must create acceptable standards to ensure the successful adoption of standards in healthcare applications. This entails defining data formats, resolving interoperability concerns, and deciding which medical data can be kept on or off the blockchain.

Cultural Resistance: Current healthcare processes often rely on traditional methods or online services, such as Electronic Health Records (EHRs) and Electronic Medical Records (EMRs). Shifting towards decentralized blockchain-based data sharing requires overcoming cultural resistance. People are accustomed to centralised systems, and changing this behaviour involves education and awareness.

Regulatory Uncertainty: Regulatory organisations face challenges in formulating policies that consider the cooperation of various stakeholders within the existing regulatory framework. HIPAA and other privacy regulations must be modified to accommodate the unique applications of blockchain technology, particularly in the healthcare sector.

Privacy and Security Issues: Although blockchain has certain built-in security protections, concerns persist regarding data sharing and access. It is essential to guarantee that data sharing complies with privacy regulations and that authorized institutions can access data securely.

Reluctance to Share: Certain stakeholders, such as healthcare facilities and insurance providers, may be reluctant to exchange data with other organisations readily. Establishing trust across stakeholders is essential to creating a cooperative atmosphere where sharing data improves healthcare systems.

Government Sectors: The government's adoption of blockchain technology faces a multitude of challenges across three key dimensions: technological, organisational, and environmental. Technological challenges centre on security and interoperability concerns. The open-source nature of many blockchain platforms raises concerns about manipulation and unauthorised data access. Integrating blockchain with existing legacy systems also presents difficulties, requiring careful data mapping and quality assurance. Additionally, the scalability of some blockchain platforms and the high transaction costs associated with them can deter government adoption. Opposition to change inside government agencies is the root cause of organizational difficulties. A lack of top management buy-in and support, coupled with inadequate skills and training among civil servants, can significantly hinder progress. Outdated policies, weak infrastructure, and insufficient funding exacerbate these issues further. Additionally, complexities in IT governance, rigid organizational structures, and ethical concerns surrounding blockchain technology can act as roadblocks to adoption. Environmental challenges relate to the uncertain legal and regulatory landscape surrounding blockchain. The lack of comprehensive laws and standards governing blockchain use creates confusion and hinders the widespread adoption of this technology. Limited participation from other government departments and external stakeholders, as well as insufficient national and geographical infrastructure, can also pose significant challenges. Additionally, a lack of expertise in blockchain development and citizen privacy concerns can deter governments from embracing this technology [19].

Table 2: Challenges to Blockchain adoption using the TOE model

Challenges to Blockchain Adoption using the TOE Model		
Technological Dimension	**Organizational Dimension**	**Environmental Barriers**
Integration and interoperability	Resistance to change within the organization	Limited participation
Privacy of data	Lack of top management support or involvement	Government/jurisdiction policies or support
Ensuring data quality and integrity	Insufficient capability of human resources	Inadequate spatial and national infrastructure
Perceived scalability of the system	Inadequate organizational infrastructure	Insufficient knowledge from suppliers or private organizations outside forces
Cost implications	Financial constraints	Outside forces
The immutability of BCT	Issues related to IT governance	Concerns about trust based on institutional elements
Complexity of the technology	Limited organizational knowledge or understanding	Technological development in the industry
Distrust of technology	Organizational capacity and capabilities	Inter-organizational communication/coordination
System Maturity	Availability of training facilities	Competitive pressures
Transparency of operations	Perceived implementation risks	
Decentralization of control	Structural aspects of the organization	
Compatibility with existing systems	Lack of organizational innovativeness	
Perceived speed of transactions	Allocation of substantial resources	
Maintaining data confidentiality	Ethical concerns or considerations	

Design Issues: Governments face challenges in designing blockchain systems and deciding whether they should be public, private, or hybrid. This choice affects transparency and performance, and the complexity of these design decisions can lead to performance issues.

Process..Change Cost: Implementing blockchain systems necessitates modifications to rules and business procedures, which

in turn impact the costs of technical support, auditing, and training. Even while it might not be a top financial concern for governments, resource-constrained governments may find this to be a significant challenge [5].

Low Throughput Rate: Compared to traditional databases, blockchain systems frequently process fewer transactions per second due to their limited throughput rate. This restriction may have an impact on the quality of the user experience and present a problem for governments seeking to deliver effective services [5].

Scalability: Scalability is a significant challenge in blockchain adoption, particularly in terms of storage capacity and network resources. As the number of transactions increases, scalability issues may arise, especially in public blockchains that are accessible to millions of users.

Security: Although blockchain technology is generally considered secure, it still poses security risks, such as the possibility of a 51% attack, where malicious parties control the majority of the blockchain's hash rate. Critical security issues may prevent the government from using blockchain technology [5].

Building Capacity: The government's inability to hire enough skilled personnel hinders its ability to implement innovative technologies, such as blockchain. To guarantee that blockchain systems are implemented successfully, governments need to solve capacity challenges [5].

Technical Skills: There is a scarcity of developers with the requisite experience since demand for technical skills in blockchain technology has outpaced supply. This lack of technical capabilities may hinder the early adoption of blockchain technology [5].

Opposition to Change: Users must embrace new technology, such as blockchain. Resistance to change, especially concerns about job losses, can make it more difficult for blockchain technology to be successfully used in government [5].

Collaboration among Government Agencies: Effective collaboration among government agencies is crucial for implementing blockchain. But as government organizations sometimes operate in silos, problems with data exchange, such as interoperability with blockchain systems, can be pretty problematic [5].

Supply Chain Management: One of the primary challenges to implementing supply chain management using blockchain technology is ensuring user privacy and data security. Due to the distributed nature and transparency of blockchain, concerns have arisen regarding the protection of user privacy and sensitive information.

Problems with Scalability: Complex supply chain networks encounter challenges in managing high volumes of transactions and information due to the scalability limitations of blockchain technology. This restriction may make it more challenging to use blockchain technology in large, networked supply chain systems.

Integration Complexity: Integrating blockchain into existing supply chain processes and IT infrastructures, especially for small and medium-sized enterprises, presents a technical challenge. Overcoming this complexity is essential for seamless adoption and integration without disrupting the current operations.

Linkage between Physical and Digital Records: Establishing a robust linkage between physical products and their corresponding digital records is crucial, particularly in food industries, where traceability is vital. The implementation of technologies such as paired RFID tags is necessary to close the distance between the digital and tangible facets of the supply chain.

Reluctance due to cryptocurrency associations; The negative reputation associated with cryptocurrencies, which share blockchain technology, contributes to reluctance among industry and finance stakeholders to adopt blockchain. Overcoming this perception challenge is crucial for the wider acceptance and understanding of the potential benefits of blockchain.

Educational and Training Gaps: The lack of educational and training platforms for non-technical experts hinders their understanding and adoption of blockchain. Bridging the gap is essential for empowering stakeholders with the knowledge needed to leverage blockchain technology effectively.

Lack of Standardisation: The absence of standardisation in traceability, certification processes, and quality requirements in the digital realm poses a significant barrier. Standardization is vital for ensuring interoperability and is a common framework for implementing blockchain across diverse supply chain scenarios.

Regulatory and Policy Challenges: The lack of clear regulations and policies surrounding blockchain adoption in supply chain management creates uncertainty and slows industry-wide acceptance. Addressing regulatory gaps is essential for providing a conducive environment for blockchain integration.

C. Existing Security Posture concerning Existing Security Laws

GDPR Articles: Concerns for Blockchain Integration? [11]

a. Data Modification and Deletion (Article 16, 17 & 18)

A recurring challenge in previous studies involves the conflict between Article 17 of the GDPR ("right to be forgotten") and the immutability of blockchain technology. This inconsistency led to the search for three possible solutions. In tombstone management, when the original data is saved outside the blockchain and the hash structure is stored within, the primary procedure involves storing data by severing the connection between the data and the information in the chain. Another solution consists of determining the consensus for removing blocks from the chain and allowing the removal to be confirmed. Finally, leveraging smart contracts provides a dynamic solution to modify or delete data based on predefined conditions and user consent, thus aligning GDPR requirements with blockchain technology [11].

b. Duty Of Processors and Controllers (Article 24, 26, and 28)

Article 4 of the GDPR introduces the concepts of pseudonymisation, controllers, and processors, as well as personal data, while Articles 24 and 28 outline the roles of data controllers and the relevant procedures. However, verifying compliance on the blockchain is difficult due to its distributed nature, where there is no central authority to monitor all nodes. Early research suggests several strategies to address this problem, including direct contact with participants, collaboration with service providers and miners, engaging leaders to facilitate transactions, exploring shared controllers for blockchains, and encouraging developers to manage smart contracts, all of which comply

with GDPR. In a decentralized blockchain ecosystem [11].

c. Design-Based Protection and Privacy (Article 25)

Several studies have examined the privacy and anti-competitive aspects of blockchain technology, demonstrating that blockchain services meet the requirements of Article 25 of the General Data Protection Regulation (GDPR). By default, blockchain ensures data integrity, confidentiality, and immutability, preventing unauthorized access, alteration, or destruction of data. The use of cryptographic hashing algorithms further enhances data transfer on the blockchain, increasing its compliance with GDPR standards. These findings therefore demonstrate that blockchain technology offers a framework that aligns with GDPR principles and provides a robust foundation for securing data and protecting privacy. [11].

d. Management of Consent (Article 7)

Article 7 of the GDPR introduces the need for consent management; however, in the decentralised environment of blockchain, determining who is responsible for processing data, as perceived by the user, still presents a problem. Storage users have the option to withdraw their consent or agree to the processing and storage of data, and the processing of data is subject to the user's consent. However, the absence of stable controllers or processes in a network of blockchains affects the control of users' rights in data processing. The use of smart contracts as a solution, claiming that legal authorizations can be stored on the blockchain and incorporated into smart contracts, providing proof-of-concept, Information processing agreements between users and controllers [11].

e. Principles Of Data Processing and Legality (Article 5, 6 and 12)

Articles 5 and 6 of the GDPR focus on protecting the integrity, confidentiality, and transparency of personal data, as well as the minimum requirements for data processing. In a blockchain context, information is distributed among network nodes, with each block linked together by a cryptographic hash. The chain remains unchanged as long as the security remains intact. However, the GDPR proposes a reduction in data processing to emphasise the importance of collecting only necessary personal data and limiting the scope. This shows a tension between blockchain data and the reduction of GDPR data, leading to further exploration of the process for improving these regulations [11].

f. Scope Of Territorial (Article 3)

Article 3 of the GDPR addresses the protection of user data processed and stored outside the EU, which can pose difficulties for public blockchains due to their international nature. When nodes are concentrated in a single location, the distinction between private and public blockchains becomes clear, influencing the strategy to be followed. To address these issues, private and government blockchains are recommended to comply with GDPR, including data transfer restrictions, and use appropriate security measures when processing and exchanging information on the site. This emphasises how crucial it is to take into account the special characteristics of blockchain architecture when creating plans to abide by international data protection regulations like GDPR [11].

1. IoT Domain:

The current state of security rules and regulations has a significant impact on the security posture employed in integrating blockchain and IoT. Global security regulations vary, and their applicability to blockchain and IoT technology is constantly evolving. Among the crucial factors are:

Data Protection Regulations: Security laws, such as the GDPR in the EU, impose stringent requirements for protecting personal data. In the context of BIoT, where sensitive information is often involved, compliance with data protection regulations is crucial. Blockchain's transparency and immutability features need to align with the principles of data protection laws.

Cybersecurity Standards: Compliance with existing cybersecurity standards is essential for ensuring the secure implementation of blockchain in IoT. Adherence to industry-specific cybersecurity frameworks and guidelines enables organisations to mitigate risks and enhance their security posture.

Identity and Access Management (IAM): Security laws often emphasize the need for robust identity and access management. In the BIoT context, where public keys or hashes are used for identification, IAM solutions must align with regulatory requirements to ensure secure and authorized access to IoT devices and data.

Incident Response and Reporting: Security laws typically mandate incident response and reporting mechanisms. In the event of a security breach or data compromise in BIoT, organisations must have robust processes in place to promptly detect, respond to, and report incidents, thereby complying with legal requirements.

Example 1:

Significant obstacles are found in current Blockchain-based Federated Learning (BCFL) systems designed for the Consumer Internet of Things (CIoT), according to the analysis reported in the article "An Optimised and Scalable Blockchain-Based Distributed Learning Platform for Consumer IoT". Notably, blockchain's intrinsic difficulties in handling high transaction volumes and ledger growth give rise to scalability problems. In CIoT contexts, it is also stressed how important it is to protect user privacy while enabling data aggregation for model training [27].

Proposed Resolution: The Gateway Peer (GWP), a crucial component of the suggested solution, is introduced into the blockchain network to address these issues. By selectively reducing local transactions, the GWP improves scalability by optimizing the ledger. Furthermore, a key component in protecting user data privacy throughout the machine learning process is the integration of sophisticated normalisation algorithms and differential privacy mechanisms.

Architecture and Technological Framework:

The architectural framework outlines the functions of various elements within the Internet of Things ecosystem.

- Internet of Things Devices: Take part in local model training and data collection.
- Edge Servers: Conduct local model creation and basic data processing. Gateway Peer (GWP): Reduces transaction burden, interfaces with the blockchain, and aggregates

local model changes, serving as a key component.

- Blockchain Platform: Acts as a haven for transaction records, model changes, and access control restrictions.
- Federated Learning Framework: Manages the coordination of operations between the GWP and edge servers during the training process.
- Differential privacy and advanced normalization are essential for safe model training and privacy-preserving data aggregation. Architectural Execution:

The architectural execution unfolds in a series of stages:

- Data Collection: Relevant data is locally gathered by CIoT devices.
- Preprocessing: The first processing and feature extraction are carried out by edge servers.
- Local Model Training: Using the data it has processed, each edge server individually trains a local model.
- Model Updates: Local models are sent to the GWP after being encrypted and differentially private.
- GWP Aggregation: Before sending encrypted changes to the blockchain, the GWP aggregates them using sophisticated normalization.
- Blockchain Storage: Provides safekeeping of model changes and blockchain-based access control guidelines.
- Global Model Update: The federated learning framework combines all blockchain updates to create a unified global model.
- Model Distribution: The updated model is securely sent to edge servers for deployment.
- Inference: For local tasks and insights, devices utilise the deployed model.

This comprehensive framework effectively addresses scalability and privacy concerns, thereby facilitating efficient and secure distributed learning within CIoT ecosystems.

Example 2:

The paper entitled "A Secured Framework for Blockchain Technology Adoption in IoT," authored by Maruthi et al., identifies substantial security challenges posed by the dynamic and distributed nature of IoT. Conventional security solutions encounter limitations in addressing issues related to data integrity, access control, and privacy concerns within this intricate IoT landscape [28].

- Potential of Blockchain: Recognising the inadequacies of traditional approaches, the study highlights the potential of BCT as a robust solution for enhancing security in IoT ecosystems. The inherent features of distributed ledgers, including immutability and transparency within blockchain, offer promising avenues to address the multifaceted security challenges inherent in IoT environments.
- Proposed Secure Framework: The paper advocates a meticulously structured three-phased secure framework designed for the seamless integration of blockchain technology into IoT scenarios. This framework encompasses distinct phases, namely registration, transaction, and consensus, each tailored to address specific security aspects.
- Utilisation of Cryptographic Techniques: To enhance security, the proposed framework employs a range of cryptographic techniques, including digital signatures, secure hashing, and encryption. These techniques collectively ensure data integrity, confidentiality, and authentication, thereby contributing to a robust security foundation for IoT environments that adopt blockchain technology.
- Smart Contracts Integration: A pivotal element of the proposed framework involves the incorporation of programmable smart contracts. These intelligent, self-executing contracts automate specific actions and enforce access control policies, fostering secure and transparent interactions within the IoT network.

Architectural and Technological Framework:

- IoT Devices: Actively collect and communicate data within the network.
- Blockchain Platform: Functions as a distributed ledger, securely and immutably storing data and transaction logs.
- Consensus Mechanism: Implements consensus algorithms such as Proof-of-Work or Proof-of-Stake, ensuring unanimous agreement among participants on the validity of transactions within the blockchain.
- Cryptographic Modules: Provide a secure communication infrastructure, implement data encryption, and enable the use of digital signatures.
- Smart Contract Platform: Executes predefined rules and agreements encoded within smart contracts.

Architectural Execution:

- Registration Phase: Involves the registration of devices and participants on the blockchain using digital signatures. Simultaneously, access control policies and smart contracts are deployed.
- Transaction Phase: Encompasses the initiation of secure transactions by IoT devices through encrypted communication channels. The veracity and validity of data and transaction details are rigorously verified before incorporation into the blockchain. Smart contracts facilitate access control enforcement and the execution of predefined actions based on transaction conditions.
- Consensus Phase: In this critical phase, nodes within the network actively engage in the consensus mechanism, collectively reaching an agreement on \ transaction validity. An unchangeable record is thereafter created by safely adding the confirmed transactions to the blockchain. In summary, the presented framework provides a secure and transparent foundation, instilling trust and enabling effective data management in IoT ecosystems that leverage the capabilities of blockchain technology.

Mapping to GDPR Articles:

Table 3: Mapping GDPR Articles with Blockchain Adoption Challenges in IOT

Topic	Relevant GDPR Articles	Challenges/ Considerations
Data Modification and Deletion	Article 16, 17, 18	Challenges due to immutability. Solutions include off-chain data storage, consensus on block removal, and smart contracts for conditional modification.
Duty of Processors and Controllers	Article 24, 26, 28	Identifying roles in decentralised networks is a challenging task. Various approaches have been proposed, such as designating nodes as controllers, processors, or joint controllers.
Design-Based Protection and Privacy	Article 25	Blockchain inherently provides some data privacy benefits. Research emphasises minimising data collection and utilising privacy-enhancing techniques.
Management of Consent	Article 7	Identifying responsibility for managing consent in decentralised networks is a topic of debate. Smart contracts are seen as a potential solution for recording and enforcing consent.
Principles of Data Processing and Legality	Article 5, 6, 12	Blockchain data processing is automated and continuous, raising concerns about transparency and fairness. Researchers suggest minimising data collection and utilising AI or neural networks for data quality assessment.
Scope of Territorial	Article 3	Public blockchains with globally distributed nodes pose challenges. Private and federated blockchains with a defined geographic scope are recommended for compliance purposes.

2. HealthCare Domain:

The security posture in blockchain adoption aligns with existing security laws, taking into account considerations for data protection, integrity, and confidentiality. Laws like HIPAA, which safeguards the privacy and security of patients' medical information, are crucial. Blockchain solutions must comply with these laws to ensure legal and ethical practices.

• Possibilities include smart contracts, decentralization, enhanced security, and increased transparency.

• Restrictions: energy consumption, resource constraints, privacy issues, scalability, and legal and regulatory framework.

• Scalability issues, high development costs, standardization difficulties, cultural opposition, unclear regulations, security and privacy worries, and reluctance to exchange data are some of the potential roadblocks facing blockchain-based healthcare systems [20].

• Blockchain is now being used in the healthcare industry for secure electronic health record exchange, data analytics, pharmaceutical supply chain, secure remote patient monitoring, and healthcare insurance claims.

Example:

Problem: It is challenging to secure the exchange of Electronic Health Records (EHRs) while enabling practical search functions and maintaining access control. Drawbacks of current systems include coarse-grained access control, single points of failure, and placing heavy computational demands on devices with constrained resources [26].

Suggested Resolution: A novel blockchain-assisted searchable encryption system with fine-grained access control to ensure safe exchange of electronic health records. This plan utilises blockchain to manage fair access and ensure data integrity, while leveraging cloud-edge computing to reduce device computational demands.

Architecture and Technology:

- Edge Servers: Manage the first data processing and apply attribute-based encryption for Electronic Health Records.
- Cloud Server: Indexes that can be searched and encrypted EHRs are stored.
- Blockchain: Holds transaction logs, user attributes, and access control regulations.
- Searchable Encryption: Attribute-Based Searchable Encryption (ABSE) is used to provide fine-grained access control. Similar-quality users can now search for and decode relevant EHRs.
- Smart Contracts: Automating blockchain-based policy enforcement and access management.

Architectural Framework:

- EHR Owner: Uploads EHRs to the cloud server after encrypting them using ABSE by preset access policies.
- User: Uses the edge server to request access to particular EHR data attributes.
- Edge Server: Obtains encrypted EHRs, verifies user attributes, and retrieves indexes from the cloud server.
- Cloud Server: Provides blockchain-stored access control policies-based indexes and encrypted electronic health records.
- Blockchain: Assures equitable and safe access by validating user characteristics and access policies.
- Decryption: Using the private key linked to their attributes, users decrypt pertinent EHR data.

Benefits:

- Fine-grained Access Control: Guarantees that specific EHR data can only be accessed by authorized persons who meet the necessary requirements.
- Data Integrity: Unauthorised updates are prevented through blockchain, ensuring data immutability.
- Fairness: Access control regulations are immutably and transparently enforced by smart contracts.
- Smaller Device Burden: Heavy computing duties are relieved from devices with limited resources by edge servers.

GDPR Compliance Issues for Blockchain Integration with Healthcare:

Table 4: Mapping GDPR Articles with Blockchain Adoption Challenges in the Healthcare Sector

Topic	Relevant GDPR Articles	Challenges/ Considerations
Data Modification and Deletion	Article 16, 17, 18	Conflict with the immutability of the blockchain. Consensus techniques for block removal, off-chain data storage, and smart contracts for conditional modification.
Duty of Processors and Controllers	Article 24, 26, 28	It is challenging to identify roles in decentralized networks. A few of the techniques are designating nodes as processors or controllers, delegating innovative contract processing to developers, and establishing joint controllers for federated blockchains.
Design-Based Protection and Privacy	Article 25	Although there are certain privacy benefits inherent in blockchain technology, research recommends reducing data collection and utilising privacy-enhancing methods.
Design-Based Protection and Privacy	Article 25	Although there are certain privacy benefits inherent in blockchain technology, research recommends reducing data collection and utilising privacy-enhancing methods.
Principles of Data Processing and Legality	Article 5, 6, 12	Concerns are raised by blockchain-based automated data processing. Research suggests reducing the amount of data collected and evaluating data quality using artificial intelligence (AI).
Scope of Territorial	Article 3	Global distribution is a hurdle for public blockchains. It is advised to use federated and private blockchains with a clear geographic scope.

3. Government Domain:

Blockchain technology is generally considered secure; however, there are specific security concerns that require attention when integrating it with government systems. The existing security posture includes safeguards against potential threats such as 51% attacks, unauthorized access, and data tampering. Compliance with existing security laws, such as data protection regulations, is crucial.

- Ecosystem Building: Major hurdles include capacity building, legislative support, and raising awareness. Governments need to establish a supportive legal framework, develop technical capacity, and raise awareness to promote the adoption of blockchain technology.
- Organizational Challenges: Resistance to change among employees, lack of technical skills, and collaboration issues between agencies impede implementation. Training, skills development, and inter-agency collaboration are crucial.
- Technological Challenges: Design issues, scalability, standardization, interoperability, and security are less significant than ecosystem and organizational concerns. However, throughput rate remains a crucial challenge for government transactions.
- Existing cybersecurity frameworks and national laws do not explicitly address blockchain-specific challenges like immutability.
- Clear guidance on role allocation, data minimisation, and consent management for decentralised networks is currently unavailable.
- International cooperation and harmonization efforts are not available for regulating cross-border data transfers involving blockchains.

Blockchain technology has enormous potential to improve security, efficiency, and transparency in government processes. Concerns about data protection and adherence to laws such as the "General Data Protection Regulation" (GDPR) are also raised by this integration, though. This paper examines the challenges and potential solutions for government blockchain projects that comply with GDPR guidelines.

Example:

The European Blockchain Services Infrastructure (EBSI) is a revolutionary project led by the European Union and the European Blockchain Partnership. This ambitious initiative builds cross-border services for individuals, corporations, and governments by utilizing blockchain technology. By using digital wallets, decentralised IDs, and verifiable credentials, EBSI aims to transform the way people interact with governments and streamline the processes of information verification and trust establishment. This cutting-edge infrastructure paves the way for a time when obtaining and authenticating government services internationally will be safe and easy [29]. The following are the main obstacles to be overcome:

- Governance Onboarding for the EBSI Ecosystem: Simplifying procedures for welcoming new members into the governance structure.
- Standardized Digital Wallets and Data Schemes: Ensuring wallets and data structures that meet EBSI standards to provide safe and effective transcript validation.
- Digital identification system interoperability: resolving incompatibilities between various national or local systems of digital identity.

Mapping GDPR Articles to Challenges and Considerations:

Table 5: Mapping GDPR Articles with Blockchain Adoption Challenges in Government

Topic	Relevant GDPR Articles	Challenges/ Considerations
Data Modification and Deletion	Article 16, 17, 18	The right to edit or remove data clashes with the inherent immutability of blockchain data.
Duty of Processors and Controllers	Article 24, 26, 28	Role identification is a complicated process in decentralized blockchain networks. Assigning roles to nodes, joint controllers in federated blockchains, and treating developers as processors for smart contracts.
Design-Based Protection and Privacy	Article 25	While blockchain offers privacy benefits, minimising data collection and utilising privacy-enhancing techniques are essential.
Management of Consent	Article 7	It is challenging to determine consent management in decentralized networks. User consent can be recorded and enforced by smart contracts under specified circumstances.
Principles of Data Processing and Legality	Article 5, 6, 12	Blockchain's automatic data processing raises questions. Some of the techniques include minimizing data collection, using AI to assess data quality, and ensuring purpose limitation.
Scope of Territorial	Article 3	Globally distributed public blockchains pose challenges to national boundaries. It is advised to use private, federated blockchains with clearly defined borders.

4. Supply Chain Management:

Incorporating blockchain into supply chain management can significantly improve security. Blockchain is designed to store immutable and transparent information, addressing significant security issues. Data in the blockchain is tamper-proof because changing a block requires updating all subsequent data.

Additionally, the fact that everyone on the network can access the information found creates a shared trust store. This is especially important for reducing the bullwhip effect, as sellers and retailers can collect information more easily and securely, leading to greater trust and more accurate forecasts. Compliance with existing security laws further strengthens the security posture of blockchain integration into supply chain management. The transparency and immutability aspects contribute to legal and regulatory compliance, ensuring responsible data handling practices.

Example:

Research Findings: The research in the article titled "Improving Healthcare Supply Chains with Blockchain Technology to Improve Healthcare Supply Chain Performance" [27] investigates the impact of blockchain technology (BCT) on the efficiency of healthcare chains. Written by Amit Vishwakarma and others. Stakeholder engagement (SI) and integration of healthcare sustainability practices (HSSCP) are important areas of focus [27]. According to the findings, BCT has a positive impact on SI and HSSCP, thereby improving the health of the supply chain.

Proposed Enhancement:

- The study emphasizes how BCT may improve healthcare supply chains without offering a specific remedy by doing the following:
- Transparency and accountability are strengthened by BCT, which creates an unchangeable record of every transaction in the supply chain.
- Process Automation: Smart contracts are essential for streamlining the supply chain and reducing costs by automating various functions, including order processing and payment.
- Collaboration is facilitated and overall coordination is improved through the safe information sharing that BCT provides amongst many parties.
- BCT facilitates the adoption of more environmentally friendly practices by making it more straightforward to track and manage the environmental impact of the supply chain.

Architecture and Technology Overview:

Beyond the vague reference to "blockchain technology," the document does not delve into specific architectural features or technologies. However, it is likely referring to a permissioned blockchain architecture designed explicitly for healthcare supply chains. Authorized users contribute data to the network in such a system, and access is restricted and regulated by pre-established guidelines.

Architectural Framework Components:

The study refers to several crucial elements that are essential to a healthcare supply chain facilitated by BCT, even if it does not explicitly lay out a complete framework:

- Blockchain Platform: Provides the essential distributed ledger technology for data management and archiving.
- Smart Contracts: Act as automated agents that carry out preset actions and enforce regulations in the supply chain.
- Sensors and IoT devices: Gather relevant information about products and procedures in the supply chain.
- Information Systems: Integrate seamlessly with the blockchain platform, facilitating the exchange and access of data within the healthcare supply chain ecosystem

GDPR Articles and Considerations:

Table 6: Mapping GDPR Articles with Blockchain Adoption Challenges in Supply Chain

Topic	Relevant GDPR Articles	Challenges/ Considerations
Data Modification and Deletion	Article 16, 17, 18	Data deletion and modification rights clash with blockchain data immutability. Privacy and data security issues in SCM. Ineffective methods for changing and removing data in the blockchain technology used today.
Duty of Processors and Controllers	Article 24, 26, 28	Role identification is a complicated process in decentralized blockchain networks. The focus of current legislation is on centralized data processors and controllers. Distributed nodes are involved in the SCM blockchain.
Design-Based Protection and Privacy	Article 25	Blockchain offers data integrity and confidentiality, but it's essential to minimise data acquisition and employ privacy-enhancing strategies. SCM privacy issues in light of GDPR's requirement for privacy by design. Due to the inherent data visibility of blockchain, additional privacy measures are required.
Management of Consent	Article 7	It is difficult to manage user consent in decentralized networks. GDPR addresses consent management; nonetheless, new strategies are needed to adapt it to decentralized blockchain in SCM.
Principles of Data Processing and Legality	Article 5, 6, 12	Blockchain's automated data processing raises concerns regarding legal processing and data minimisation. GDPR places a strong emphasis on data processing principles such as data reduction and purpose limitation. SCM procedures may need to be modified to comply with blockchain standards.
Scope of Territorial	Article 3	Globally distributed public blockchains pose challenges for adhering to national borders. In public blockchains, enforcing geographical limitations on data privacy rules can be challenging.

D. Existing Security Solutions

- Encryption techniques are used in security solutions to ensure secure data transfer and key management when combining blockchain with IoT. Blockchains with permissions limit involvement to approved parties, resolving privacy issues and adhering to security regulations. Blockchain-based decentralised identity solutions enhance privacy and comply with data protection laws. Necessary security precautions include implementing privacy-preserving algorithms, optimizing consensus methods for IoT devices, and auditing smart contracts for flaws.
- In the healthcare industry, data confidentiality, process automation, integrity maintenance, and privacy-preserving algorithms are made possible by smart contracts, permissioned blockchains, strong encryption, and practical consensus algorithms.

Encryption, secure consensus methods, identity management, smart contract audits, and regulatory compliance are valuable tools for government applications, as they provide user authentication and data protection.

Blockchain's built-in security, transparency, and smart contracts in supply chain management simplify procedures, eliminate intermediaries, and maintain confidence, thereby reducing costs and dispute risk. Together, these security measures lay the groundwork for blockchain technology to be successfully integrated into various industries.

E. Implementing Security Solutions to Enhance Blockchain Adoption Across Domains

A comprehensive approach to security is necessary for the implementation of blockchain technology in several areas, including supply chain management, healthcare, government, and the Internet of Things. Organisations in the IoT space must proactively adhere to compliance standards, conduct routine audits, and inform stakeholders about security procedures and relevant regulatory frameworks. The widespread acceptance of healthcare encompasses trust-building, adherence to standards, regulatory cooperation, investment in research and development, and education. Adoption by the government necessitates training initiatives, coordination with cybersecurity specialists, ongoing oversight, legislative frameworks, public education, and smooth integration. Education, teamwork, standardization, regulatory lobbying, and progressive adoption are crucial in supply chain management. Ensuring security and privacy in these domains requires incorporating thoughtful design, ensuring reliable data validation, and assessing organizational preparedness. Establishing legal frameworks, industry standards, and transparent governance structures is crucial, along with investing in secure infrastructure and enhancing scalability to support these frameworks. This multifaceted approach ensures a safe, legal, and trustworthy foundation for blockchain integration across industries, unlocking transformative potential.

Table 8 presents a comprehensive overview of security solutions designed to enhance blockchain adoption across diverse sectors. It outlines existing and potential solutions, their specific focus areas, key benefits, and implementation strategies. The table highlights the importance of encryption, permissioned blockchains, decentralized identity, smart contract auditing, and regulatory compliance as common themes across domains. It also emphasizes the need for privacy-preserving algorithms, consensus optimization, and self-sovereign identity in specific contexts. Addressing these challenges will be crucial for unlocking the full potential of blockchain technology in various industries.

Table 7: Potential Security Solutions and Their Implementation Strategy

Solution ID	Security Solutions	Focus	Benefits	Implementation Strategies
General				
SS1	Encryption Techniques	Data confidentiality, protection from unauthorized access	End-to-end encryption, secure key management	Compliance with encryption standards, regular key rotation
SS2	Permissioned Blockchains	Privacy, compliance with security laws	Controlled access, restricted participation	Define and enforce access control, and utilize identity management solutions
SS3	.Decen. tralized Iden.tity Solutions	Enhanced privacy, improved security	User control over personal data, compliance with data protection regulations	Integrate with existing identity management systems and develop user-friendly authentication protocols
SS4	.Smart. Contract and. regular Auditing	Increased security, prevention of malicious activities	Vulnerability identification and mitigation	Thorough code reviews, vulnerability assessments, and the use of automated tools
SS5	Personal Data Cloud (PDC)	Privacy Concerns, Enhanced Security, Data Monetisation, Transparency and Accountability, Enhanced Trust	GDPR Compliance: Individuals Hold the Keys to Their Own Data. This decentralized and tamper-proof ledger empowers users to store their data securely, choose who can access it, and even monetize it by selectively sharing with specific applications and services	Stand.ard. Dizat, Educatio, and Awareness, Regulatory Advocacy, Technology Development
SS6	Sybil and Double-Spending risks using the Security Risk Management (SRM) domain mode	Improve Security	Identify, analyse, and address security risks to increase trust in blockchain technology.	Security Tools and Training, Stakeholder Collaboration, Implement the framework in stages, starting with identifying critical risks and vulnerabilities, Continuous Monitoring and Assessment
SS7	.Priva. cy-Preserving. Algorithms	Confidentiality of patient data on private blockchains	Implement techniques like homomorphic encryption, secure multi-party computation	Collaborate with cybersecurity experts, invest in R&D for advanced algorithms

SS8	Public and Private Key Infrastructure	Secure authentication and access control	Secure user authentication and encryption of data	Implement PKI with strong cryptographic algorithms, and manage keys securely
SS9	Regulatory Compliance	Adherence to security laws and regulations	Protect sensitive information, ensure legal compliance	Conduct risk assessments, implement security measures that comply with relevant regulations
SS10	Identity Management	Grant authorized access to the blockchain	Secure authentication and access control, prevent unauthorized activity	Implement secure identity management systems and integrate with existing government infrastructure
SS11	Consensus Algorithm Optimization	Improved performance and energy-saving for resource-constrained environments	Efficient validation and agreement on transactions	Research and development of lightweight consensus mechanisms
SS12	Self-Sovereign Identity (SSI)	Decentralized identity management for devices	User control over device data, improved security and privacy	Integrate with existing identity management systems and develop secure device authentication protocols
SS13	Purpose Limitation	Data minimization and privacy by design	Reduce data collection and usage, increase transparency	Smart contracts for controlled modification: Utilizing conditional smart contracts.
IoT				
SS7	Privacy-Preserving Algorithms	Confidentiality of patient data on private blockchains	Implement techniques like homomorphic encryption, secure multi-party computation	Collaborate with cybersecurity experts, invest in R&D for advanced algorithms
SS4	Smart Contract and regular Auditing	Enforced conditions and automated processes	Trust, transparency, and reduced risk of disputes	Use of formal verification methods, secure multi-party execution of contracts
SS2	Permissioned Blockchain	Enhanced security and control over the network	Controlled access for authorized participants	Implement permissioned consensus mechanisms, define access levels and roles
SS1	.Encry. Option	Secure data storage	Confidentiality, data integrity	Utilize strong encryption algorithms,
	Technique. uses	and transmission		implement secure key management protocols
SS12	Self-Sovereign Identity (SSI)	Decentralized identity management for devices	User control over device data, improved security and privacy	Integrate with existing identity management systems and develop secure device authentication protocols
SS11	Consensus Algorithms	Transaction validation and network agreement	Data integrity, trust in the network	Choose secure consensus mechanisms, and optimize performance for resource-constrained devices
Health. hcare.				
SS1	Encr. yption Techniques	Secure storage and transmission of sensitive healthcare data	Utilize robust encryption algorithms, implement secure key management protocols	Adhere to healthcare data privacy regulations and conduct regular security audits
SS11	Consensus Algorithms	Ensure validation and agreement on transactions	Maintain data integrity, build trust in the network	Implement efficient consensus mechanisms, ensure data immutability
SS8	Public and Private Key Infrastructure	Secure authentication and access control	Secure user authentication and encryption of data	Implement PKI with strong cryptographic algorithms, and manage keys securely
SS2	Permissioned Blockchains	Enhanced security and control over the network	Restricted access for authorized participants	Define and enforce access control mechanisms, establish governance models
SS10	Identity Management	Ensure authorized access to the blockchain	Secure access control, prevent unauthorized data access	Implement secure identity management systems and integrate with existing healthcare infrastructure
SS9	Regulatory Compliance	Adherence to security laws and regulations	Protect sensitive information, ensure legal compliance	Conduct risk assessments, implement security measures that comply with relevant regulations
SS7	Privacy-Preserving Algorithms	Confidentiality of patient data on private	Implement techniques like homomorphic encryption, secure multi-	Collaborate with cybersecurity experts, invest in R&D for

		blockchains	party computation	advanced algorithms
SS4	Smart Contract and regular Auditing	Automate predefined processes and enforce conditions	Improve efficiency, reduce risk of errors, and build trust	Develop secure and reliable smart contracts, conduct thorough testing and auditing
Government				
SS1	Encryption	Secure data storage and transmission	Protect sensitive government information from unauthorized access	Implement robust encryption algorithms, adhere to data security standards
SS11	Consensus Mechanisms	Transaction validation and prevention of malicious activities	Ensure data integrity, prevent fraud and manipulation	Choose secure consensus mechanisms, monitor network activity for suspicious behavior
SS10	. tity Manageme	Grant authorized access to the blockchain	Secure authentication and access control, prevent unauthorized activity	Implement secure identity management systems and integrate with existing government infrastructure
SS4	Smart Contract and regular Auditing	Ensure the security of automated processes	Identify and mitigate vulnerabilities in smart contracts	Conduct regular audits by cybersecurity experts and implement testing frameworks
SS8	Public and Private Key Infrastructure	Secure authentication and access control	Secure user authentication and encryption of data	Implement PKI with strong cryptographic algorithms, and manage keys securely
SS9	Regulatory Compliance	Adherence to security laws and regulations	Protect sensitive information, ensure legal compliance	Conduct risk assessments, implement security measures that comply with relevant regulations
Supply Chain Management				
SS3	Decentralized and Transparent Nature	Trust, elimination of intermediaries	Increased accountability, improved efficiency	Develop user-friendly interfaces for interacting with the blockchain, and educate all stakeholders on its benefits
SS4	.Smart. Contract and. regular Auditing	Automatic enforcement of predefined rules	Reduced risk of disputes, trust in transactions	Thorough code reviews, vulnerability assessments, and the use of automated tools
SS13	Purpose Limitation	Data minimization and privacy by design	Reduce data collection and usage, increase transparency	Smart contracts for controlled modification: Utilizing conditional smart contracts

V. RESULTS

Numerous sectors, including supply chain management (SCM), healthcare, government services, and the Internet of Things (IoT), have been transformed by blockchain technology. However, as blockchain technology advances, it also introduces a range of challenges, particularly in terms of security and compliance with existing regulations and laws. This comprehensive analysis examines compliance issues, the current security landscape, and the security measures being implemented to ensure the safe and seamless use of blockchain technology. Recognizing the Current Security Attitude

In the Internet of Things (IoT) sphere, blockchain integration necessitates a coordinated development of security. While the decentralised nature of blockchain ensures data integrity, it also requires organisations to comply with specific legal frameworks and conduct audits to identify areas of vulnerability. It is therefore essential for stakeholders to receive proper education on aspects such as legal frameworks, data protection, and security procedures. Continuous monitoring and engagement with regulators are necessary, as flexible security policies should respond to changes in legislation, thereby maintaining a strong position in this regard.

However, the successful incorporation of blockchain technology can be achieved by implementing robust security measures that protect sensitive patient information. This includes educational programs, adherence to standards, collaboration with regulators, and investment in research and development. Collaboration with regulators ensures that there is concordance between existing laws and technology based on blockchain, while addressing upcoming challenges is facilitated through investment in R&D. Building confidence around such issues entails promoting transparency that meets relevant standards and demonstrates effectiveness through measurable outcomes. Government blockchain adoption requires a multifaceted approach that involves education, continuous monitoring, legal frameworks, public awareness, and seamless integration. Training programs enhance government personnel's understanding of blockchain security, while collaboration with cybersecurity experts ensures the development of tailored solutions that meet specific needs. Public awareness builds trust, and seamless integration with existing security infrastructure ensures robust measures against evolving threats.

Supply chain blockchain adoption demands education, collaboration, standardization, regulatory advocacy, and phased implementation. Education overcomes technical challenges, while collaborative standardisation addresses traceability, certification, and quality requirements; regulatory advocacy provides a supportive environment. Phased implementation through pilot

projects builds technical capacity, and the "Blockchain as infrastructure" model encourages collaboration for a more comprehensive adoption.

A. Compliance Issues with Existing Laws

Blockchain integration encounters specific compliance challenges, notably with the “General Data Protection Regulation” (GDPR), in various domains.

In healthcare, governed by laws such as the “Health Insurance Portability and Accountability Act” (HIPAA), blockchain faces challenges related to data deletion and modification due to its immutability. The roles and responsibilities of controllers and processors in decentralised networks necessitate innovative approaches.

Protection and privacy by design are inherent, but they demand minimising data collection. Consent management and data processing principles face challenges in the automated nature of blockchain. Territorial scope recommends private and federated blockchains to address GDPR requirements.

The government's adoption of blockchain raises security concerns related to rights such as rectification, erasure, and restriction of processing, which are complicated by the blockchain's immutability—the roles and responsibilities of controllers and processors in decentralised networks present complexities. Protection and privacy by design require minimising data collection, and consent management faces challenges due to the automated nature of blockchain technology. The territorial scope recommends private and federated blockchains to align with the GDPR.

Includes solutions related to GDPR compliance in supply chain management, data deletion and modification, integration with roles and responsibilities of controllers, protection by design and privacy, regulatory approval and processes in the field of competition. Solutions include purpose limitation, minimising data collection through the use of smart contracts, and utilising conditional smart contracts for controlled modification.

B. Implementing Security Solutions

Across diverse domains, implementing security solutions for blockchain adoption involves a strategic blend of education, collaboration, compliance, monitoring, and regulatory alignment. The multifaceted approach acknowledges the distinct challenges in each sector, providing a secure, legal, and trustworthy foundation for blockchain integration.

C. General Security Solutions:

Standard security solutions include encryption techniques for data confidentiality, permissioned blockchains for controlled access, decentralised identity solutions for enhanced privacy, and smart contract auditing for increased security and trust. The Personal Data Cloud (PDC) addresses privacy concerns, while Sybil and Double-Spending risks are mitigated using Security Risk Management (SRM) domain mode. Privacy-preserving algorithms and public and private key infrastructure enhance confidentiality and secure authentication.

D. IoT Security Solutions:

For blockchain integration in IoT, encryption techniques ensure secure data transmission. Permissioned blockchains restrict access, and decentralized identity solutions enhance privacy. Smart contract auditing and consensus algorithm optimization prevent malicious activities. Privacy-preserving algorithms safeguard patient data, and public and private key infrastructure ensure secure authentication.

E. Healthcare Security Solutions:

In healthcare, encryption techniques secure sensitive data, and consensus algorithms maintain data integrity. Public and private key infrastructure ensures secure authentication. Permissioned blockchains offer enhanced security, and identity management controls access. Regulatory compliance ensures adherence to laws, while privacy-preserving algorithms maintain the confidentiality of patient data. Smart contract auditing automates processes.

F. Government Security Solutions:

Government blockchain integration requires encryption for secure data storage and transmission. Consensus mechanisms prevent malicious activities, and identity management grants authorized access. Smart contract auditing ensures the security of automated processes. Public and private key infrastructure enables secure authentication. Regulatory compliance protects sensitive information, and privacy-preserving algorithms maintain confidentiality.

G. Supply Chain Management Security Solutions:

In supply chain management, the decentralised and transparent nature of blockchain helps establish trust. Smart contract auditing enforces predefined rules, and purpose limitation ensures data minimization. Encryption techniques secure data storage and transmission, and consensus algorithms validate transactions. Privacy-preserving algorithms maintain confidentiality, and public and private key infrastructure ensure secure authentication.

The integration of blockchain technology across diverse domains demands a holistic approach that encompasses understanding the existing security posture, addressing compliance challenges, and implementing robust security solutions. Navigating the intricate interplay of blockchain, security, and compliance requires continuous adaptation, collaboration, and adherence to evolving legal landscapes. As organisations embark on this transformative journey, the successful integration of blockchain will not only revolutionise their operations but also provide a secure, legal, and trustworthy foundation for the future of technology across various industries.

VI. CONTRIBUTION

By examining the relationship between established legal frameworks, including the General Data Protection Regulation (GDPR), and the intrinsic qualities of blockchain technology — such as transparency and immutability — this research aims to bridge a significant knowledge gap. Organizations exhibit caution in integrating blockchain due to technological complexities, regulatory uncertainties, and the inherent conflict between blockchain's transparency and GDPR's focus on individual data rights. The research addresses this gap by conducting a thorough literature analysis, focusing on the clash between blockchain and GDPR. It aims to propose solutions by mapping security challenges to

GDPR articles, providing insights into conflicting points that hinder blockchain adoption. The research objectives focus on understanding the data privacy challenges associated with blockchain adoption, evaluating existing legal frameworks, and developing strategies to mitigate these risks.

This study aims to make a significant contribution by examining the clash between blockchain and GDPR, providing insights into the challenges, proposing solutions for their harmonious coexistence, and highlighting the need for dedicated studies on information security and privacy challenges in blockchain adoption, along with existing technical solutions to enhance adoption rates.

VII. CONCLUSION AND DISCUSSION

This research provides insight into the security and privacy challenges associated with blockchain adoption, with a specific focus on its intersection with the General Data Protection Regulation (GDPR). For its part, it does a deep dive into specific areas such as healthcare, government, and supply chain management, highlighting their unique security features and limitations. This contribution is to offer solutions to reduce the gap between the capabilities of blockchain and the complexities of GDPR, guiding decision-makers and promoting shared responsibility. However, some limitations are worth considering. First, focusing solely on the GDPR limits general understanding and overlooks many other international laws. Reliance on specific data may result in biased selection, as it excludes essential data from unvetted sources and industry data. An intersectional approach would ignore the inherent nature of blockchain and propose a more flexible approach. In the future, the integration of multi-stakeholder perspectives, the use of mixed-methods research, and the conceptualisation of expanded studies to understand beyond published data can support a deeper understanding. Additionally, delving deeper into specific solutions and exploring various blockchain platforms will provide more practical tips for overcoming the challenges of adoption. By addressing these limitations, future research can provide a better understanding of blockchain adoption and its organisational role as we navigate the various regulatory pathways.

FUTURE DIRECTIONS AND RECOMMENDATIONS

The report suggests several directions for further investigation to broaden our understanding of blockchain adoption and address current issues. First and foremost, the literature search should be expanded to encompass a wider variety of research from reputable sources such as ScienceDirect, Springer, MDPI, Google Scholar, and Web of Science, in addition to specialised databases like IEEE and Scopus. This addition would improve the review's inclusiveness and offer a more comprehensive examination of blockchain adoption. Further investigation into topics such as machine learning-based privacy and security solutions in BioT and vision applications is recommended due to the revolutionary potential of blockchain in the Internet of Things (IoT) and other domains. Challenges related to deployment, blockchain infrastructure, governance, regulation, and legislation must be addressed to enable safe, reliable, and secure deployment of BIOT.

The study emphasises the importance of considering how blockchain technology may impact global warming, as well as the challenges in maintaining the security of the metaverse. Subsequent investigations should explore these novel scenarios to offer insights into the ecological consequences of blockchain technology and its role in safeguarding emerging digital environments. Furthermore, academics are invited to create a theoretical model of blockchain adoption issues using the Interpretive Structural Modeling (ISM) approach. This approach can help us gain a deeper understanding of the complex connections and dynamics surrounding blockchain technology. Future research should utilise other frameworks that offer greater flexibility to capture the context and changes that influence blockchain adoption, thereby addressing the limitations of the current method. A detailed examination of issues unique to each nation and area will help clarify the particular choices that various administrations must make. Furthermore, it is crucial to address the scalability concerns in blockchain technology to facilitate extensive personal data storage and utilisation. Creating user-friendly tools and interfaces is essential for enabling non-technical individuals to utilise blockchain technologies. For decentralised data management solutions to effectively address data ownership and privacy concerns, existing legal and regulatory frameworks must be revised.

ACKNOWLEDGMENT

This research work is the outcome of a Research & Development work carried out by Ms. Shailja Garg under the supervision of Dr. Tamal Mondal at Symbiosis Centre for Information Technology, Pune, India.

DECLARATION STATEMENT

Funding	No, I did not receive.
Conflicts of Interest	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval or consent to participate, as it presents evidence that is not subject to interpretation.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	This research work is the outcome of a Research & Development work carried out by Ms. Shailja Garg under the supervision of Dr. Tamal Mondal at Symbiosis Centre for Information Technology, Pune, India

REFER.ENCES.

1. M. AlSha.msi, M. Al-Emran, and K. Shaalan, "A Systematic Review on Blockchain Adoption," Applied Sciences, 2022. https://doi.org/10.3390/app12094245
2. Kasireddy P. Fundamental challenges with public blockchains; 2017 Dec 13. [Accessed 2020 Feb 17]. https://www.preethikasireddy.com/post/fundamental-challenges-with-public-blockchains
3. H. Kafeel, V. Kumar, and L. Duong, "Blockchain in Supply Chain Management: A Synthesis of Barriers and Enablers for Managers," International Journal of Mathematical, Engineering and Management Sciences, 2023. https://doi.org/10.33889/IJMEMS.2023.8.1.002
4. S. Dhingra, R. D. Raut, V. S. Yadav, N. Cheikhrouhou, and B. K. R. Naik, "Blockchain adoption challenges in the healthcare sector: a waste management perspective," Springer, 2023.

https://doi.org/10.1007/s12063-023-00413-9
5. S. K. Sharma, Y. K. Dwivedi, S. K. Misra, and N. P. Rana, "Conjoint Analysis of Blockchain Adoption Challenges in Government," Journal of Computer Information Systems, 2023. https://doi.org/10.1080/08874417.2023.2185552
6. C. Nartey et al., "On Blockchain and IoT Integration Platforms: Current Implementation Challenges and Future Perspectives," Wireless Communications and Mobile Computing, 2021. https://doi.org/10.1155/2021/6672482
7. S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and E. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses' Resilience: Issues and Recommendations," Sensors, 2023. https://doi.org/10.3390/s23156666
8. W. S. Wibowo and S. Yazid, "UNVEILING ROADBLOCKS AND MAPPING SOLUTIONS FOR BLOCKCHAIN ADOPTION BY GOVERNMENTS: A SYSTEMATIC LITERATURE REVIEW," Interdisciplinary Journal of Information, Knowledge, and Management, 2023.
9. T. Tariq, F. Javaid, M. Zubair, B. Fayyaz, and S. Rizwan, "Challenges in Security and Privacy posed by Blockchain Technology," Journal of Independent Studies and Research Computing, 2022. https://doi.org/10.31645/JISRC.22.20.2.1
10. D. C. G. Valadares et al., "Privacy-Preserving Blockchain Technologies," Sensors, 2023. https://doi.org/10.20944/preprints202305.1874.v1
11. B. Haque, A. K. M. Najmul Islam, S. Hyrynsalmi, and K. Smolander, "GDPR Compliant Blockchains–A Systematic Literature Review," IEEE Access, 2021. https://doi.org/10.1109/ACCESS.2021.3069877
12. N. Fabiano, "The Internet of Things ecosystem: The blockchain and privacy issues. The challenge for a global privacy standard," IEEE Access, 2017. https://doi.org/10.1109/IoTGC.2017.8008970
13. C. Stach, C. Gritti, D. Przytarski, and B. Mitschang, "Can Blockchains and Data Privacy Laws be Reconciled?" Symposium on Applied Computing, 2022. https://doi.org/10.1145/3477314.3506986
14. B. Varghese, M. Villari, O. Rana, P. James, T. Shah, M. Fazio, and R. Ranjan, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," IEEE Internet Computing, vol. 24, no. 5, pp. 45–53, Nov. 2018, doi: 10.1109/MIC.2020.3014484.. https://doi.org/10.1109/MCC.2018.064181115
15. Q. Wu et al., "Understanding User Perception of Privacy in Blockchain Applications," Computers in Human Behavior, 2021.
16. Garcia et al., "Legal Implications of Data Privacy in Blockchain-based Contracts," International Journal of Law and Information Technology, 2019.
17. T. Nguyen et al., "Blockchain-enabled Privacy in Supply Chain Management," International Journal of Production Economics, 2023.
18. Liu M, Yeoh W, Jiang F, Choo KKR. Blockchain for Cybersecurity: systematic literature review and classification. J Comput Inf Syst., 2022;62(6):1182–98. doi:10.1080/08874417.2021.1995914. https://doi.org/10.1080/08874417.2021.1995914
19. S. Lee et al., "Governance Models for Data Privacy in Public Blockchains," Journal of Governance and Regulation, 2021.
20. R. Brown et al., "Scalable Privacy Solutions for Permissionless Blockchains," IEEE Transactions on Emerging Topics in Computing, 2018.
21. B. Kitchenham and S. Charters, "Guidelines for Performing Systematic Literature Reviews in Software Engineering," Keele University: Keele, UK, 2007.
22. D. Moher et al., "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," PLoS Med., 2009. https://doi.org/10.1371/journal.pmed.1000097
23. Kohad H, Kumar S, Ambhaikar A. Scalability issues of blockchain technology. Int J Eng Adv Technol., 2020;9:2385 91.
24. A. Alqudah, M. Al-Emran, and K. Shaalan, "Technology Acceptance in Healthcare: A Systematic Review," Appl. Sci., 2021. https://doi.org/10.3390/app112210537
25. Yeoh P. Regulatory issues in blockchain technology. J Financial Regul Compliance., 2017;25(2):196–208. doi:10.1108/JFRC-08-2016-0068. https://doi.org/10.1108/JFRC-08-2016-0068
26. T. Ali Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem and T. Alghamdi, "A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations," in IEEE Access, vol. 7, pp. 176838-176869, 2019, doi: 10.1109/ACCESS.2019.2957660. https://doi.org/10.1109/ACCESS.2019.2957660
27. H. Gao, H. Huang, L. Xue, F. Xiao, and Q. Li, "Blockchain-Enabled Fine-Grained Searchable Encryption With Cloud–Edge Computing for Electronic Health Records Sharing," IEEE Internet of Things Journal, doi: 10.1109/JIOT.2023.3279893, 2023. https://doi.org/10.1109/JIOT.2023.3279893
28. Z. Wang, X. Liu, X. Shao, A. Alghamdi, M. Alrizq, Md. S. Munir, and S. Biswas, "An Optimized and Scalable Blockchain-Based Distributed Learning Platform for Consumer IoT," in Mathematics, vol. 11, no. 23, p. 4844, Nov. 2023, doi: 10.3390/math11234844. https://doi.org/10.3390/math11234844
29. R. Maruthi, D. Piriadarshani, Sankar Padmanabhan, and M. Shanthi, "A Secured Framework for Blockchain Technology Adoption in IoT," in 2023 IEEE International Conference on Electrical, Computer, and Automation Technologies (ICECAA), pp. 1342-1347, doi: 10.1109/ICECAA58104.2023.10212185. https://doi.org/10.1109/ICECAA58104.2023.10212185

AUTHORS PROFILE

Shailja Garg is a dedicated student enrolled at Symbiosis Centre for Information Technology, Symbiosis International (Deemed University), Pune, India. Currently pursuing an MBA in Information Technology Business Management, Shailja demonstrates a keen interest in the intersection of technology and business. Her academic pursuits are complemented by practical experiences gained through internships and extracurricular engagements. With a proactive approach to learning and a strong foundation in both information technology and business management, Shailja aspires to make meaningful contributions to the evolving landscape of technology-driven enterprises.

Tamal Mondal is an accomplished academic, currently serving as Assistant Professor at the Symbiosis Centre for Information Technology, Symbiosis International (Deemed University), Pune, India. Dr. Mondal earned his doctoral degree in 2021 from the Department of Computer Science & Engineering at the National Institute of Technology Durgapur, West Bengal, India. His research expertise spans diverse domains including Data Mining, Natural Language Processing (NLP), and Crisis Management. Driven by a passion for advancing knowledge, he has contributed significantly to the academic community through publications and presentations.