blockchains

MDPI

Article

Navigating Blockchain's Twin Challenges: Scalability and Regulatory Compliance

Shezon Saleem Mohammed Abdul

School of Business, University of Southern Queensland, Toowoomba, QLD 4350, Australia; shezonsaleem.mohammedabdul@unisq.edu.au

Abstract: Blockchain technology promises transformative potential across diverse sectors, facilitating innovations in areas ranging from finance to healthcare. Despite its many promising applications, several barriers—including scalability challenges, regulatory complexities, and technical hurdles—limit its widespread adoption. This systematic literature review delves into scalability enhancements and explores the legal and regulatory landscapes impacting blockchain deployment in ten key sectors: IoT, healthcare, finance, education, social media, genomics, supply chain, vehicular networks, e-voting, and tourism. These sectors were selected based on their significant engagement with blockchain technology and their prominence in the analyzed literature. We examine key technological advancements such as Layer-2 techniques, sharding, consensus algorithm optimization, and rollups, and discuss their implications for throughput, latency, and compliance with regulatory standards such as the General Data Protection Regulation (GDPR). The review details these technological and regulatory developments and discusses their broader implications for industry and academia, emphasizing the need for interdisciplinary research and innovation. By identifying gaps in current research and suggesting future directions, this study serves as a roadmap for researchers, practitioners, and policymakers to develop secure, scalable, and compliant blockchain systems. Our comprehensive examination provides valuable insights into enhancing the efficiency, security, and regulatory compliance of blockchain technology.

Keywords: blockchain; scalability; regulatory compliance; layer-2 solutions; sharding; consensus algorithms; rollups; network latency; GDPR

check for updates

Citation: Mohammed Abdul, S.S. Navigating Blockchain's Twin Challenges: Scalability and Regulatory Compliance. *Blockchains* **2024**, *2*, 265–298. https://doi.org/10.3390/blockchains2030013

Academic Editor: Keke Gai

Received: 21 June 2024
Revised: 10 July 2024
Accepted: 18 July 2024
Published: 21 July 2024

Copyright: © 2024 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Blockchain technology is revolutionizing the way data are stored and managed. As a decentralized distributed ledger system, blockchain offers built-in security and transparency features that enable information handling through networks of computers without the need for a central authority. Each transaction is integrated into an immutable log within a chain of cryptographically linked blocks, ensuring a high level of data integrity and network robustness. Initially designed for Bitcoin in 2008, blockchain has since expanded beyond cryptocurrencies, finding applications in various fields, including online identity authentication, logistics planning, and election procedures. This innovative approach eliminates intermediaries or central authorities typically required for transaction verification, enhancing overall security and reducing risks from malicious actors exploiting infrastructure weaknesses. Consequently, blockchain technology has the potential to transform the management of sensitive information across various sectors.

One of the key characteristics of blockchain is decentralization. Blockchain technology is essentially a decentralized database collectively maintained by all nodes, enhancing the credibility of Trusted Third-Party Auditors (TPAs) and improving the overall security of data auditing processes. Another significant benefit of blockchain is its immutability. The ability of blockchain to create an immutable record of transactions ensures the integrity of data and auditing results, making it difficult for malicious actors to tamper with the information stored on the blockchain. Additionally, blockchain provides traceability, allowing

for transparent and auditable records of transactions. This traceability feature is beneficial in data auditing processes, as it enables stakeholders to track and verify the history of data transactions and integrity checks [1].

Despite its numerous advantages, blockchain technology faces significant challenges related to scalability. Current limitations in transaction processing capacity, throughput, and latency can restrict its applicability in industries that require high-performance systems [2]. One key factor contributing to scalability issues is the need for each network node to sequentially verify transactions before they are added to the blockchain [3]. Blockchain's potential to address the security challenges posed by traditional centralized service models is particularly relevant, especially as scalable solutions are necessary for managing large-scale data and business services that single blockchains struggle to support effectively [4]. This inherent trade-off between security, decentralization, and efficiency has driven the exploration of various solutions, such as sharding [5] and off-chain solutions like the Lightning Network [6], which have shown promising results in enhancing blockchain's efficiency and practicality [7]. Off-chain solutions, in particular, address blockchain storage limitations, enhancing scalability, storage efficiency, and verification speed. By utilizing off-chain storage for certain data, blockchain systems can improve their performance and scalability [8]. Selecting suitable data to be stored on-chain is crucial for balancing security and scalability issues. Storing excessive data on-chain can hinder scalability and efficiency, so determining the appropriate data to be stored on-chain is essential for optimizing blockchain systems [8].

In addition to scalability challenges, regulatory compliance poses another significant hurdle for blockchain technology. The decentralized and immutable nature of blockchain can conflict with existing regulatory frameworks, such as the General Data Protection Regulation (GDPR), which emphasizes the right to be forgotten and strict data privacy standards. Navigating these regulatory landscapes requires innovative approaches to ensure blockchain implementations meet legal requirements while maintaining their inherent advantages. Integrating blockchain technology with existing systems may introduce regulatory compliance challenges, as the decentralized nature of blockchain may conflict with centralized management models, leading to regulatory hurdles. Ensuring data security and privacy is crucial for meeting regulatory requirements, and addressing these security issues is essential for regulatory compliance [9].

This study aims to fill the gap by providing a comprehensive analysis of both scalability and regulatory compliance issues across different industries. By conducting a systematic literature review, we aim to identify the most pressing challenges in various domains and evaluate the solutions being proposed to address these issues. Our research synthesizes insights from diverse industries to offer a holistic perspective on the scalability and regulatory compliance of blockchain technology. This approach not only highlights the current state of blockchain technology but also identifies emerging trends and future research directions. The findings of this study have significant implications for the future development and adoption of blockchain technology, providing a foundation for addressing scalability and regulatory challenges in its deployment.

The study's methodology is detailed in Section 2, covering the review planning, research question formulation, search strategy definition, and criteria for inclusion and exclusion. In Section 3, we explore prominent blockchain scalability challenges across various sectors and discuss strategies being employed to facilitate wider adoption (RQ1). Section 4 examines the legal and regulatory compliance issues associated with blockchain technology, highlighting the complexities and potential solutions (RQ2). Section 5 navigates through the prevailing trends in blockchain scalability and regulatory compliance, examining prevalent strategies being utilized to address these issues across various sectors, along with future research directions (RQ3). Finally, Section 6 concludes our study, discussing its limitations, highlighting key insights, and offering implications for future research and practice.

2. Research Methodology

The process for this systematic review is meticulously designed, involving a series of stages: planning the review, executing the research, defining crucial research questions, outlining search criteria, choosing data sources, and presenting the findings. Each of these phases is explored in detail in this section.

2.1. Planning the Review

The main objective of this study is to comprehensively examine the status of blockchain scalability issues, their solutions, and regulatory compliance across various industries. Additionally, we aim to discern trends and predict future research trajectories based on the existing body of literature. The review protocol necessitates the formulation of research questions, selection of suitable databases for our search, and the development of techniques for identifying and appraising relevant evidence. We adopt select components from the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) statement to present a transparent, quantifiable, and comprehensive evaluation of blockchain scalability and regulatory compliance across a multitude of sectors.

2.2. Crafting Research Questions

To analyze the existing literature on blockchain scalability challenges, solutions, and regulatory compliance effectively, we have defined a set of research questions to guide our review process. These research questions aim to address the most prominent challenges and potential future directions in blockchain scalability and regulatory compliance across various industries. Table 1 presents the research questions driving our study and their respective motivations.

Table 1. Research questions and the motivations behind them.

Research Question	Motivation
RQ1: What are the key scalability challenges of blockchain technology across various industries, and how are these challenges being addressed?	To understand the scalability issues inherent in blockchain technology and investigate strategies for broader adoption across diverse fields.
RQ2: What are the legal and regulatory compliance challenges associated with blockchain technology across different industries, and what solutions are being implemented to address these challenges?	To explore the complexities of legal and regulatory compliance in blockchain technology and suggest effective navigation strategies.
RQ3: What trends are emerging in blockchain scalability and regulatory compliance solutions across various domains, and what future research directions can be derived from the existing literature?	To identify current trends in blockchain scalability and regulatory compliance, and propose future research directions.

2.3. Search Strategy

To conduct a systematic literature review on blockchain scalability and regulatory compliance, including their challenges, solutions, and trends across varied industries, we explored multiple databases to gain a comprehensive perspective and increase the likelihood of finding highly relevant articles. The electronic sources used in this investigation include Science Direct, Web of Science, IEEE Xplore, PubMed, ACM Digital Library, Springer Link, and Google Scholar. Our objective in searching these databases was to encompass a wide range of publications and compile information pertinent to our research questions, with an emphasis on blockchain scalability and regulatory compliance challenges and solutions across various industries. The search strings we employed were as follows:

- Query string 1 (QS1): (“blockchain” OR “block chain”) AND (scalability OR scale OR regulatory OR compliance)

- Query string 2 (QS2): (QS1) AND (challenge OR problem OR issue OR adoption) AND (industry OR domain OR sector)
- Query string 3 (QS3): (QS1) AND (trend OR future research direction OR solution OR approach OR method)

These query strings were used to search the selected databases, ensuring a comprehensive and concise search strategy that provided a robust examination of blockchain scalability and regulatory compliance challenges and solutions across different industries.

2.4. Inclusion and Exclusion Criteria

To ensure a systematic and comprehensive literature review on blockchain scalability challenges, regulatory compliance, solutions, trends, and future research directions across different industries, it is crucial to establish a set of inclusion and exclusion criteria. These criteria help in filtering the search results and selecting the most relevant and high-quality studies that align with our research questions. Table 2 outlines the criteria employed for including and excluding studies in our systematic literature review.

Table 2. Criteria for inclusion and exclusion of studies in the systematic literature review.

Criteria	Inclusion	Exclusion
Timeframe	Studies published from 2019 to 31 March 2023	Studies published before 2019
Language	Studies written in English	Studies not written in English
Publication	Peer-reviewed articles, conference papers, and journal publications	Non-peer-reviewed publications (e.g., blog posts, opinion pieces)
Focus	Studies focusing on blockchain scalability challenges, regulatory compliance, solutions, trends, and future research directions across various industries	Studies not focusing on blockchain scalability or regulatory compliance, or not addressing the research questions
Content	Articles providing empirical data or practical examples of blockchain scalability and regulatory compliance solutions; studies addressing both technical and non-technical aspects of blockchain scalability and regulatory compliance	Studies lacking a sound methodology or providing insufficient data to support their findings

2.5. Selection Process

The selection process for this systematic review was conducted in several stages to ensure a rigorous and comprehensive assessment of the literature. Initially, titles and abstracts of the articles retrieved from the database searches were screened to exclude those clearly irrelevant to the research questions. This step helped in narrowing down the pool of potential studies. The remaining articles then underwent a full-text review to confirm their relevance and quality. During this phase, each article was evaluated to determine if it addressed blockchain scalability and regulatory compliance challenges, solutions, trends, or future research directions. Only those articles that provided empirical data or practical examples relevant to the research questions were considered for final inclusion. Studies that lacked a sound methodology or provided insufficient data to support their findings were excluded to maintain the integrity of the review. This thorough selection process ensured that the final set of 70 papers included in the review offered high-quality insights into blockchain scalability and regulatory compliance across various industries.

2.6. Data Extraction and Analysis

For the selected studies, data extraction was performed using a standardized form to systematically collect relevant information. The extracted data included publication details, study objectives, methodologies, key findings related to blockchain scalability and regulatory compliance, and any proposed solutions or future research directions. This structured approach ensured consistency and comprehensiveness in capturing the critical

insights from each study. The extracted data were then analyzed to identify common themes, challenges, and trends across the studies. This analysis provided a robust foundation for discussing the current state of blockchain scalability and regulatory compliance, as well as identifying gaps and opportunities for future research.

3. Addressing Scalability Challenges (RQ1)

In this section, we explore the first research question (RQ1): What are the key scalability challenges of blockchain technology across various industries, and how are these challenges being addressed? Scalability is a fundamental issue that affects the performance, efficiency, and usability of blockchain systems. The ability to handle a growing number of transactions and users without compromising speed, security, or decentralization is critical for the broader implementation of blockchain technology.

We will examine these challenges and the innovative solutions being deployed across ten key sectors: IoT, healthcare, finance, education, social media, genomics, supply chain, vehicular networks, e-voting, and tourism. Each of these sectors presents unique scalability issues and has adopted various strategies to overcome them. By analyzing these sectors individually, we aim to provide a comprehensive overview of the current state of blockchain scalability and identify best practices and emerging trends that could inform future developments.

Through this detailed examination, we aim to shed light on the specific scalability hurdles encountered in each sector and the creative approaches being employed to tackle them. This analysis will highlight the diversity of scalability solutions and underscore the importance of sector-specific strategies in achieving effective and sustainable blockchain adoption.

3.1. IoT: Scalability Challenges and Solutions

The Internet of Things (IoT) encompasses the vast network of interconnected physical devices that communicate and exchange data with one another. Its potential to connect billions of devices presents challenges in terms of security, privacy, and data management [10]. Centralized approaches to IoT management are often limited in their scalability, prompting researchers to explore blockchain-based distributed IoT management solutions [11]. Blockchain technology can enhance the security, privacy, and interoperability of IoT systems by providing a decentralized and tamper-resistant platform for data sharing and device management [12].

Scalability is a major concern in IoT applications, notably due to the management of potentially tens of millions of devices, as illustrated by large-scale cyberattacks like those conducted using the Mirai botnet, and the handling of data volumes reaching into petabytes. Traditional public blockchains may not be suitable for IoT applications due to their limited transaction throughput and high latency [13]. These scalability challenges can significantly impact IoT systems in multiple ways:

Firstly, the limited transaction throughput and high latency can hinder the efficiency of IoT systems, as they struggle to process and manage the vast amount of data generated by billions of devices in a timely manner. This can lead to delays in data processing and decision-making, affecting the overall performance of the IoT network.

Secondly, the scalability challenges can compromise security and privacy in IoT systems. As the network becomes more congested due to the increasing number of devices, maintaining the security and privacy of data and communications may become more difficult. This can potentially expose sensitive information or create vulnerabilities in the network that malicious actors can exploit, leading to security breaches and unauthorized access to the system.

Lastly, these scalability challenges can slow down the adoption of blockchain-based IoT solutions. The inability to effectively scale the blockchain to handle the massive volume of transactions and data in IoT applications can deter organizations from implementing blockchain technology in their IoT systems. As a result, the potential benefits of using

blockchain in IoT, such as improved security, privacy, and interoperability, may not be fully realized, and the widespread adoption of blockchain-based IoT solutions could be delayed.

To address the scalability challenge in IoT, researchers have proposed various solutions, including the use of hierarchical architectures, off-chain transactions, and sharding techniques to increase the scalability of blockchain systems for IoT applications [14]. While some progress has been made in this area, further research is needed to develop more efficient consensus mechanisms and optimize system delays and throughput rates for large-scale IoT networks [15]. Research into sharding and off-chain storage solutions is also being conducted to address the scalability issues in the IoT domain [11]. Consequently, IoT can benefit from a combination of solutions, including permissioned blockchains, off-chain storage, and data partitioning to ensure the scalability of the network without compromising security and privacy.

3.2. Healthcare: Scalability Challenges and Solutions

Blockchain technology has shown the potential to revolutionize the healthcare industry by enhancing efficiency, access control, and data security [16]. It can ensure data integrity, privacy, and security while facilitating seamless information sharing among different healthcare providers, leading to improved patient care, reduced costs, and increased trust among stakeholders [6]. However, integrating blockchain technology with existing healthcare systems faces several challenges, including scalability and the need for real-time transaction processing [15].

Scalability in healthcare applications poses significant challenges, particularly due to the extensive and sensitive nature of patient data that necessitates secure and efficient storage and sharing mechanisms. Housing such voluminous information on a public blockchain is formidable, mainly due to constraints associated with transaction throughput and storage capacity [7]. In the realm of IoT in healthcare, these scalability issues are even more pronounced, as managing a high volume of transactions swiftly is crucial. The deployment of lightweight nodes, mini-blockchains, and alternative solutions like Litecoin may offer some respite. Moreover, the integration of blockchain technology in healthcare must also consider the energy consumption and computational limitations of IoMT sensors [6].

To overcome this, researchers have proposed using permissioned blockchains or consortium blockchains, which restrict access to authorized parties, reducing the amount of data that needs to be processed and stored [17]. Researchers are also actively exploring the use of cryptographic solutions, hashing algorithms, and novel consensus strategies to address these issues and improve scalability in healthcare applications [18]. The adoption of off-chain storage and sharding techniques is being considered to handle the massive amounts of data generated in healthcare settings [16]. Data management techniques like data pruning or partitioning can help address the scalability challenges in healthcare by reducing the amount of data stored on the blockchain and improving data retrieval times.

In summary, addressing the scalability challenge in healthcare requires a combination of solutions, including permissioned blockchains, off-chain storage, and data management techniques. This will enable the healthcare industry to leverage the full potential of blockchain technology while maintaining the security, privacy, and efficiency of sensitive patient data.

3.3. Genomics: Scalability Challenges and Solutions

The rapidly expanding field of genomics, which involves examining an organism's entire genetic makeup, presents unique challenges when it comes to scaling blockchain. Blockchain technology has the potential to provide a secure and transparent platform for sharing genomic data, promoting collaboration among researchers, patients, and healthcare providers, and accelerating personalized medicine [17]. Yet, the immense size of genomic data, which can range from hundreds of gigabytes to several terabytes for a single indi-

vidual, poses a scalability issue. The impracticality and inefficiency of storing such large datasets on a blockchain is quite evident [7].

To tackle this, researchers have suggested strategies such as employing distributed file storage systems like the InterPlanetary File System (IPFS) for storing the actual genomic data, while the blockchain only holds the metadata and access control information [19]. This method considerably reduces the storage and processing demands on the blockchain, thus enhancing its scalability for genomics applications. Other possible solutions include integrating blockchain with technologies like distributed hash tables (DHTs) or content addressable storage (CAS) to increase storage efficiency and lessen the blockchain's burden.

The use of permissioned or consortium blockchains, which restrict access to authorized parties and often employ more efficient consensus mechanisms, can provide improved scalability and performance compared to public blockchains [17]. By amalgamating blockchain technology with distributed storage solutions like IPFS, DHTs, or CAS, and by utilizing permissioned or consortium blockchains, we can create scalable, secure, and efficient platforms for managing and sharing genomic data.

3.4. Supply Chain: Scalability Challenges and Solutions

The decentralized nature of blockchain can significantly enhance transparency, traceability, and collaboration among various supply chain stakeholders, leading to improved efficiency and reduced costs. The supply chain industry has begun to leverage blockchain to address issues related to transparency, traceability, and trust [20]. However, managing over a million transactions daily and data volumes in excess of several terabytes in supply chains leads to scalability concerns [21]. Storing all these data on a blockchain can lead to increased storage and computational requirements, negatively impacting performance and escalating transaction costs.

To tackle these challenges, researchers have emphasized improving transaction throughput and reducing block times. They are also exploring innovative approaches such as reinforcement learning (RL) to enhance the efficiency of blockchain-enabled supply chain networks. Several solutions, including data pruning techniques, sharding, and sidechains, have been proposed to address scalability in supply chain management. These methods can scale blockchain systems for supply chain applications without compromising security or decentralization [22]. Furthermore, off-chain storage solutions and data partitioning are being considered to address scalability issues while preserving data integrity and security [20]. By incorporating these approaches, supply chain management can effectively harness the potential of blockchain technology while addressing scalability challenges and maintaining the integrity and security of the supply chain data.

3.5. Vehicular Networks: Scalability Challenges and Solutions

Vehicular networks, which enable vehicles to exchange information with each other and with infrastructure components, present unique challenges when it comes to scaling blockchain. Blockchain technology can enhance the security, privacy, and trustworthiness of these networks by providing a decentralized and tamper-resistant platform for data sharing and vehicle management. The rapid proliferation of technologically advanced vehicles in smart cities adds to the complexity, as each vehicle, equipped with various sensors and devices, generates significant amounts of data. Arshad et al. [23] highlight the challenges posed by the high volume of data and the extensive network of vehicles, which necessitate scalable blockchain solutions to ensure robust, secure, and efficient vehicular communication networks.

Researchers are exploring reputation systems, incentive mechanisms, and priority-based strategies to address these issues. Yet, further investigation is needed to optimize these approaches and ensure their viability in real-world vehicular network deployments. One possible solution to address the scalability challenge in vehicular networks is the use of permissioned or consortium blockchains, which can provide superior scalability and performance compared to public blockchains [24]. Additionally, off-chain storage and data

management techniques have been proposed to decrease the amount of data stored on the blockchain, which in turn improves its scalability [17]. By moving some transactions off the main blockchain, we can effectively reduce the overall load on the system, leading to improved throughput and reduced latency.

Another potential solution lies in integrating machine learning techniques to optimize resource allocation and prioritize transactions based on specific requirements [25]. By leveraging a mix of permissioned blockchains, off-chain storage solutions, and machine learning techniques, vehicular networks can ensure high transaction throughput and low latency, effectively addressing the scalability challenges in this domain.

3.6. E-Voting: Scalability Challenges and Solutions

The adoption of blockchain technology in e-voting systems promises to enhance transparency, immutability, and security [26]. Blockchain technology can improve the transparency, security, and efficiency of e-voting systems by providing a decentralized, tamper-resistant platform for vote recording and tallying. Blockchain-based e-voting systems can reduce the risk of fraud and ensure the integrity and verifiability of election results [27]. However, scalability concerns need to be addressed to ensure the successful implementation of blockchain-based e-voting systems.

Given the sheer number of voters participating globally in 2024—as at least 64 countries, representing nearly half of the world's population, are expected to conduct national elections [28]—scalability becomes a significant hurdle in e-voting applications. Researchers are exploring solutions such as sharding, layer-2 solutions, and innovative consensus algorithms to tackle these issues [26]. Sharding partitions the blockchain network into smaller, more manageable pieces, each responsible for processing a subset of transactions, thereby increasing throughput and reducing latency. Layer-2 solutions like the Lightning Network build upon existing blockchain infrastructure to enable faster, more scalable transactions, which are essential in real-time processing and high throughput rate contexts like e-voting. Permissioned or consortium blockchains can offer superior scalability and performance compared to public blockchains, and using ZK-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) can enable vote aggregation without revealing individual votes, reducing blockchain storage and processing requirements [3].

In the e-voting context, ZK-SNARKs can enable privacy-preserving voting and improve scalability. By combining permissioned blockchains, sharding, layer-2 solutions, and privacy-preserving mechanisms like ZK-SNARKs, blockchain-based e-voting systems can effectively address scalability challenges, facilitating secure, transparent, and efficient election processes.

3.7. Education: Scalability Challenges and Solutions

Blockchain technology could revolutionize education by providing secure, verifiable, and tamper-proof records of academic achievements, credentials, and other critical information. As discussed in recent research, blockchain enables academic records, certifications, and credentials to be transparent, secure, and accessible, which reduces fraud risks, boosts the efficiency of the credential verification process, and promotes lifelong learning [29]. However, as emphasized in "Unlocking the power of blockchain in education", the scalability of blockchain-based education systems remains a significant challenge, especially given the vast amount of data generated by an ever-growing number of users [30].

The scalability concerns are primarily due to the large number of students, institutions, and records that need to be managed on a blockchain. The article notes that implementing blockchain in education requires robust hardware, sophisticated software, and efficient data management strategies to handle the high volume of transactions and data storage needs effectively. The integration of blockchain into the education system must address these scalability issues to fully realize its potential in making educational processes more secure and transparent [30].

To address these challenges, researchers and developers are examining various techniques, including the use of permissioned blockchains, off-chain storage solutions, and advanced consensus algorithms [29]. Permissioned blockchains, which restrict the number of participants and employ more efficient consensus mechanisms, can significantly improve scalability in educational applications by reducing the load on the network. Off-chain storage solutions can help manage the bulk of data while preserving data integrity and security, thus enhancing the blockchain's performance and scalability. Furthermore, the article suggests that employing sidechains—separate blockchains running parallel to the main chain—can offload transactions and data, improving scalability and efficiency [2].

By integrating these technologies—permissioned blockchains, off-chain storage, and sidechains—the education sector can effectively mitigate the scalability challenges associated with blockchain. This multifaceted approach fosters a more secure, transparent, and efficient system for managing academic records and credentials, as highlighted in the discussed article, supporting the broader adoption and application of blockchain technology in education [30].

3.8. Social Media: Scalability Challenges and Solutions

In the realm of social media, blockchain technology could be transformative. It presents an opportunity to decentralize traditional platforms, give users more control over their data, as well as enhance privacy and resist censorship [31]. With over 5 billion global social media users and an average daily engagement of 151 min per user [32], blockchain systems must be capable of handling enormous loads. Researchers are re-exploring advanced consensus mechanisms, investigating off-chain storage solutions, and even considering hybrid approaches that combine blockchain with other distributed technologies.

The deployment of second-layer solutions, like payment channels or sidechains, aims to improve transaction throughput and reduce the burden on the main blockchain [22]. Layer-2 solutions such as state channels and plasma are being researched to increase transaction speed and decrease latency in blockchain-based social media platforms. Additionally, the concept of sharding—dividing the blockchain network into smaller segments—is gaining traction as a potential solution for enhancing scalability while maintaining user privacy and data integrity [33].

One of the promising solutions for scalability and data management in social media platforms is the use of decentralized storage solutions, particularly the InterPlanetary File System (IPFS). IPFS offers a resilient, peer-to-peer method of storing and managing data, providing an alternative to centralized cloud storage with enhanced security and reduced costs. This approach aligns well with the decentralized nature of blockchain, aiming to enhance system resilience and reduce dependency on centralized infrastructures. A recent study by Sangeeta et al. (2023) delved into the use of IPFS integrated with blockchain technology to address data storage challenges in vehicular networks, highlighting its potential for high-integrity and secure data management [34]. This study is particularly relevant to social media as it demonstrates the robustness of IPFS in handling large-scale data across a distributed network, ensuring data integrity and availability even in high-demand scenarios. The research suggests that IPFS can effectively support the demands of social media platforms where vast amounts of data need secure, scalable, and cost-effective storage solutions. Moreover, the Sangeeta et al. (2023) study introduced the concept of keyword search capabilities within IPFS, enhancing the usability of this storage method for social media applications where quick and efficient data retrieval is crucial. By enabling keyword search, users can efficiently navigate through large data sets, improving the user experience and accessibility of stored data.

By integrating these advanced storage solutions with blockchain's inherent security and transparency features, social media platforms can achieve greater scalability and efficiency. This integration not only helps in managing vast volumes of data typical of social media platforms but also ensures that the data remains secure from tampering and privacy breaches.

3.9. Financial Sector: Scalability Challenges and Solutions

The financial sector, as one of the earliest adopters of blockchain technology, has showcased significant promise in transforming traditional financial systems which are plagued by inefficiencies, high transaction costs, and delays due to intermediaries [35]. Blockchain technology enables direct peer-to-peer transactions, reducing costs and increasing transparency, potentially resolving these longstanding issues.

Despite these advantages, scalability remains a critical challenge for the broader adoption of blockchain in the financial sector. The Bitcoin blockchain, for instance, is significantly limited in transaction processing capacity compared to traditional systems like Visa [24]. To address these limitations, several innovative solutions have been proposed. The Lightning Network, which facilitates off-chain transactions, and sharding, which divides the blockchain into smaller, manageable segments for parallel processing, is among the notable strategies aimed at enhancing transaction throughput without compromising security [33].

Further expanding on these strategies, the research by Weerawarna et al. (2023) underscores the importance of innovative architectural solutions and advanced consensus mechanisms in overcoming these scalability hurdles [36]. The study highlights the use of permissioned blockchains and consortium blockchains, which restrict network participation to improve efficiency and scalability. It also discusses the potential of delegated Proof of Stake (DPoS) and Proof of Stake (PoS) mechanisms in reducing the computational and energy demands of blockchain operations, making them more suitable for financial applications [2,36]. Moreover, the research stresses the ongoing need for optimizing blockchain architectures to better suit the financial sector, identifying the lack of exploration into blockchain's full potential within financial services as a gap in the current literature. Their systematic review of blockchain in finance highlights how these technologies not only address scalability but also provide a competitive edge by enhancing security, reducing fraud, and improving the efficiency of financial transactions [36].

In conclusion, while the scalability of blockchain technology presents challenges, ongoing research and development are poised to transform financial systems significantly. By leveraging advanced blockchain solutions such as off-chain storage, sidechains, and efficient consensus algorithms, the financial sector can achieve greater throughput and efficiency, paving the way for a more robust and scalable blockchain infrastructure [36].

3.10. Tourism Sector: Scalability Challenges and Solutions

The tourism industry, a crucial driver of global economic activity, is experiencing a transformative shift through the integration of blockchain technology. This transition is propelled by the technology's capacity to enhance scalability, security, and transparency across various facets of the industry [37].

Scalability challenges in the tourism industry are prominent, especially due to the fluctuating volumes of transactions during peak seasons and major events. To address these challenges, Layer-2 solutions such as off-chain transaction handling can be particularly effective in managing the high volume of bookings and payments, ensuring faster and cheaper transactions without overloading the main blockchain network [38]. Additionally, sharding techniques can enhance scalability by dividing the blockchain into smaller, parallel processing segments. This approach is beneficial for managing transactions from different geographical locations or various aspects of the industry simultaneously, thereby increasing the overall capacity of the network [39]. Permissioned blockchains offer a tailored scalability solution in tourism by restricting the number of nodes involved in transaction validation. This not only ensures efficient transaction processing but also maintains security and data integrity, akin to the solutions adopted in industrial sectors for managing high-volume data from smart manufacturing and asset tracking [5**?**]. Additionally, the tourism sector employs innovative blockchain applications such as smart contracts to automate customer relationship management and loyalty programs. These contracts execute transactions based

on predefined conditions, reducing the need for intermediaries, which in turn lowers costs and streamlines operations [40].

Blockchain's role in enhancing transparency and mitigating fraud in tourism is pivotal. By establishing an immutable ledger for all transactions, where each entry is verified by multiple nodes, it becomes nearly impossible to alter any information retroactively without network consensus. This security feature is crucial for booking and payment processes, significantly mitigating risks such as overbooking and fraudulent transactions [40]. The integration of digital currencies in tourism operations offers another layer of scalability and security. Tourists can utilize cryptocurrencies for payments, simplifying transactions and reducing fees associated with currency exchange. Companies like Expedia and Webjet have already started accepting Bitcoin, indicating a growing acceptance of digital currencies in the tourism sector [40]. Further, blockchain's ability to securely manage customer identities and personalize services enhances the overall customer experience. It ensures that all personal preferences and history are verified reliably, enabling tourism providers to offer customized services without risking unauthorized access or data breaches [40]. Research by Dadkhah et al. (2022) and the systematic review by Banerji (2021) elaborate on current and potential applications of blockchain in tourism, such as removing intermediaries in bookings and ensuring the authenticity of customer reviews. This not only simplifies the booking process but also ensures that feedback is reliable and verifiable, fostering trust among consumers [40,41].

In conclusion, while blockchain presents effective scalability solutions that address inherent challenges in the tourism sector, continuous advancements and tailored technology applications are essential. The integration of blockchain technology with traditional tourism operations holds the potential to transform the sector into a more resilient and customer-focused industry [37,40] a more resilient and customer-focused industry [37,40].

3.11. Summary of Scalability Challenges and Solutions (RQ1)

In this section, we have delved into the scalability challenges that blockchain technology faces across various sectors and explored the innovative scalability approaches currently being employed to address these challenges. Table 3 summarizes these scalability challenges and the corresponding solutions across different industries. For instance, in the IoT sector, managing the vast number of interconnected devices and their data volumes necessitates hierarchical architectures and permissioned blockchains. Healthcare faces the challenge of handling extensive patient data securely and efficiently, prompting the use of permissioned blockchains and off-chain storage. Genomics deals with massive data sizes that require distributed file storage systems like IPFS. The supply chain sector, with its high transaction volumes, benefits from data pruning techniques and consortium blockchains, while vehicular networks leverage reputation systems and incentive mechanisms. E-voting systems, which need to process votes securely and efficiently on a large scale, are exploring sharding and Layer-2 solutions. The education sector, handling large volumes of academic records, is turning to permissioned blockchains and sidechains. Social media platforms, with their enormous user bases, benefit from decentralized storage solutions like IPFS. The financial sector, seeking to enhance transaction throughput, is adopting off-chain solutions and sharding. Lastly, the tourism sector, facing fluctuating transaction volumes, is implementing hybrid blockchain models and smart contracts.

As observed from our analysis, each sector presents unique scalability challenges and requires tailored solutions. These findings, summarized in Table 3, highlight the necessity for sector-specific approaches to address the diverse scalability issues effectively. Overcoming these challenges is pivotal to unlocking the full potential of blockchain technology across various industries. However, it is crucial to recognize that even the most advanced scalability solutions may encounter significant hurdles if regulatory frameworks are not supportive. This brings us to our second research question: What are the legal and regulatory compliance challenges associated with blockchain technology across different industries, and what solutions are being implemented to address these challenges? Ad-

dressing this question will allow us to explore how regulations influence the deployment and effectiveness of blockchain solutions, providing a comprehensive understanding of the factors that shape the future of blockchain technology.

Table 3. Summary of blockchain scalability issues and approaches.

Industry	Scalability Challenges	Impacts on Industry	Scalability Approaches
IoT	Management of up to tens of millions of devices; data volumes reaching petabytes [13]	Affects efficiency, security, and privacy of IoT systems; slows down the adoption of blockchain-based IoT solutions	Hierarchical architectures; efficient consensus mechanisms; permissioned blockchains [14]
Healthcare	Management of extensive volumes of sensitive patient data; need for real-time transaction processing [7]	Affects efficiency, security, and privacy of healthcare systems; limits the adoption of blockchain-based healthcare solutions	Permissioned or consortium blockchains; off-chain storage and sharding techniques [16]
Genomics	Handling genomic data ranging from hundreds of gigabytes to several terabytes per individual [7]	Impedes secure, efficient sharing and management of genomic data; slows down progress in personalized medicine	Distributed file storage systems like IPFS; integration with existing storage solutions [19]
Supply Chain Management	Daily transactions over a million and data volumes in excess of several terabytes [21]	Reduces performance and increases transaction cost; affects efficiency and cost-effectiveness of supply chain operations	Data pruning techniques; consortium blockchains [22]
Vehicular Networks	Management of an extensive network of smart vehicles, each generating significant data [23]	Impacts the management of vehicular network infrastructure; affects security, privacy, and trustworthiness of vehicular network	Reputation and incentive systems; permissioned blockchains [24]
E-Voting Systems	Millions of voters participating in global elections; high demand for secure, efficient vote processing [26]	Impacts transparency, security, and efficiency of e-voting systems; potential risk of voter fraud	Layer-2 solutions like Lightning Network; ZK-SNARKs for privacy-preserving voting [3]
Education	Tens of thousands of institutions and students; large data volumes for records [30]	Impacts transparency, security, and accessibility of academic records; risk of fraud; affects credential verification process	Permissioned blockchains; sidechains for offloading transactions [2]
Social Media	Over 5 billion users; average daily engagement of 151 min per user [32]	Impacts user privacy and control over data; affects resistance to censorship and data breaches	Second-layer solutions; sharding and decentralized storage solutions like IPFS [34]
Finance	Transactions significantly lower than systems like Visa; high demand for real-time transaction processing [24]	Impacts transaction speed and cost; affects trust and transparency in financial transactions	Off-chain solutions like the Lightning Network; sharding for parallel processing [36]
Tourism Applications	Management of high transaction volumes during peak seasons and events [37,40]	Challenges in handling seasonal traffic spikes and maintaining data integrity; impacts customer trust and service efficiency	Hybrid blockchain models; Permissioned blockchains for efficient processing; Smart contracts for automated transactions [33,36]

4. Legal and Regulatory Compliance (RQ2)

As we explore scalability solutions that blockchain technology offers across diverse sectors, it is equally critical to address the legal implications and data protection challenges

intrinsic to this technological integration. This review encompasses ten key sectors—IoT, healthcare, finance, education, social media, genomics, supply chain, vehicular networks, e-voting, and tourism—each selected for its significant engagement with blockchain technology and representation in the analyzed literature. For each sector, we examine both the unique legal challenges and the innovative solutions that could enhance compliance and operational viability, especially in environments regulated for personal data protection.

Blockchain's immutability poses significant challenges regarding compliance with data protection regulations such as the General Data Protection Regulation (GDPR) in the European Union, which advocates for the right of data subjects to have their personal data erased upon request. This requirement is fundamentally at odds with the permanent nature of blockchain records [9]. Moreover, blockchain's decentralized architecture complicates data governance by eliminating a central authority, thereby making it challenging to enforce data deletion requests across all network nodes [9]. While decentralization enhances data security and reduces failure points, it raises intricate issues concerning accountability and data ownership. The deployment of blockchain in decentralized operations introduces ethical dilemmas related to privacy, transparency, and the potential redefinition of employer-employee dynamics. Literature highlights the disruptive potential of blockchain as it challenges traditional governance models and competes with established economic institutions, requiring regulatory bodies to adapt and possibly intervene as market structures and data management practices are reshaped [42].

This section explores potential legal conflicts and compliance challenges that could arise as blockchain technologies scale across these diverse sectors. Innovative solutions might include the development of mutable blockchain architectures that allow some level of data editability without undermining the system's integrity, or new cryptographic methods that enhance data privacy while preserving blockchain's core features [9]. Proactive engagement with regulatory authorities and legal experts during the design and implementation phases is crucial for establishing standardized frameworks that address both scalability and compliance requirements, potentially leading to broader acceptance and implementation of blockchain technologies.

This section emphasizes the importance of integrating technological innovation with regulatory compliance. It highlights that the true measure of blockchain's scalability will depend as much on its technical attributes as on its ability to conform to diverse legal environments. Achieving this balance is essential for ensuring the sustainable and responsible expansion of blockchain applications in sectors where personal data protection is paramount [9,42,43].

4.1. Blockchain in IoT: Legal, Privacy, and Regulatory Compliance

The Internet of Things (IoT) introduces a complex layer of legal considerations, particularly around data protection and privacy laws, which are paramount when integrating IoT with blockchain technology. The decentralized nature of blockchain can complicate compliance with data protection regulations such as the General Data Protection Regulation (GDPR), which mandates rigorous data protection measures and gives individuals the right to have their data erased [9].

The use of IoT devices, which often collect and transmit personal data across networks, intensifies these challenges. According to Fabiano (2017), the IoT ecosystem evolves rapidly, incorporating applications that may compromise privacy if not properly managed. This necessitates a Privacy by Design approach, ensuring that privacy and data protection are considered in the design phase of IoT applications [44].

Fabiano (2017) highlights the introduction of Data Protection Impact Assessments (DPIA) by the GDPR, which are critical when deploying new technologies such as IoT in conjunction with blockchain. These assessments help identify and mitigate risks related to data privacy at the outset of system design [44].

Furthermore, the integration of IoT with blockchain must address the potential for increased surveillance and data security vulnerabilities. IoT devices can act as points of

data collection, feeding into larger blockchain networks that permanently record these data, thus raising significant privacy concerns. Blockchain's immutable ledger, while ensuring data integrity and transparency, also means once data are recorded, they cannot be altered or deleted, complicating compliance with privacy laws like the GDPR [9].

In this context, legal experts and technologists need to collaborate closely to devise systems that uphold privacy standards while leveraging the technological benefits of blockchain and IoT. The development of such systems should be guided by comprehensive legal frameworks that anticipate the dynamic interplay between evolving technological landscapes and stringent regulatory requirements [9,44].

This exploration underscores the critical need for robust legal and regulatory frameworks that can adapt to the innovative potential of IoT and blockchain, ensuring that technological advances do not outpace the protections necessary to safeguard personal privacy and data security.

4.2. Blockchain in Healthcare: Legal, Privacy, and Regulatory Compliance

Blockchain technology in healthcare introduces significant legal considerations, especially concerning data protection and privacy within the context of European healthcare systems. The decentralized and immutable nature of blockchain poses unique challenges to compliance with stringent data protection regulations, such as the General Data Protection Regulation (GDPR). These regulations mandate robust data protection measures and grant individuals extensive rights over their personal data, including the right to erasure, which conflicts with blockchain's permanent record-keeping [45].

The integration of blockchain in healthcare settings requires careful attention to patient consent, data security, and compliance with legal standards. Key issues include ensuring that patient data are handled in a manner that respects privacy rights and complies with regulatory frameworks. Data protection, security, consent, liability, and compliance are highlighted as major legal hurdles in adopting blockchain technology across different European countries [45].

Moreover, the variability in legal frameworks across Europe suggests a need for harmonization to facilitate the broader adoption of blockchain technologies in healthcare. The study by Farouk and Alsamara (2023) underscores the potential for legal harmonization that could support innovation while protecting patients' rights and ensuring compliance with health regulatory standards [45].

Given the complexity and rapid development of blockchain applications in healthcare, there is a pressing need for legal experts and technologists to collaborate closely. This cooperation aims to develop systems that not only leverage the benefits of blockchain technology but also adhere to the high standards of privacy and data protection required by law [46].

This exploration into blockchain technology in healthcare emphasizes the necessity for robust legal frameworks that are adaptable enough to encompass the innovative potentials of blockchain while ensuring that technological advancements do not compromise the stringent protections required to safeguard patient privacy and data security [46].

4.3. Blockchain in Genomics: Legal, Privacy, and Regulatory Compliance

In the rapidly evolving field of genomics, blockchain technology presents a promising solution to the ethical and legal challenges posed by large-scale biomedical data management. The integration of blockchain can potentially enhance privacy protections and streamline consent processes in genomics research, which involves highly sensitive personal health information [47].

Blockchain's inherent properties such as immutability, decentralization, and data provenance offer a technical framework that can support the secure and transparent handling of genomic data. These features ensure that data alterations are traceable and that all access and changes to data are recorded, addressing major concerns about data integrity and traceability in genomics research [47].

However, the implementation of blockchain technology in this context also raises significant concerns, particularly around the issue of consent and data ownership. Traditional models of consent may be inadequate for the dynamic and expansive nature of genomic databases, where data may be used across multiple research projects over many years. Blockchain could support innovative consent models that are dynamic and specify individual preferences, potentially increasing participants' control over their personal data [47].

Furthermore, the legal frameworks surrounding data protection and patient privacy, such as the General Data Protection Regulation (GDPR) in Europe, pose additional challenges to the adoption of blockchain in genomics. The GDPR emphasizes individuals' rights to access and erase their personal data, which conflicts with the immutable nature of blockchain. This highlights the need for regulatory adaptations that can reconcile the benefits of blockchain with the stringent requirements of data protection laws [47].

In conclusion, while blockchain technology offers significant advantages for managing genomic data, it also necessitates careful consideration of ethical, legal, and practical challenges. Integrating blockchain into genomics research requires not only technological innovation but also a supportive regulatory environment and new models of consent and data governance to fully realize its potential [47].

4.4. Blockchain in Supply Chain Management: Legal, Privacy, and Regulatory Compliance

Blockchain technology continues to offer transformative potential for supply chains, enhancing transparency, efficiency, and dispute-resolution mechanisms. The integration of blockchain simplifies complex supply chains by digitalizing documents and facilitating real-time information sharing, thus improving operational efficiency and assisting in dispute avoidance within intricate networks of stakeholders, such as those in construction projects [48].

The introduction of smart contracts, as outlined by the studies referenced [48,49], provides an automated means to enforce contract terms, significantly reducing disputes and increasing efficiency across different industries, including construction. These smart contracts, along with blockchain's capability to offer a transparent and immutable record of transactions, contribute to a robust framework for managing complex supply chains [48,49]. However, the deployment of blockchain in supply chains faces substantial legal, data, and regulatory challenges that can hinder its broader implementation. Compliance with multi-jurisdictional legal frameworks and regulatory standards remains a critical hurdle, as non-compliance can lead to legal risks and operational disruptions. Additionally, the restrictive nature of smart contracts and the challenges associated with data access and ownership on shared blockchain platforms present ongoing legal barriers [48].

From a data management perspective, blockchain facilitates the standardization and traceability of data across the supply chain, which is essential for maintaining the integrity and reliability of supply data from origin to destination. This increased traceability aids in enhancing visibility and accountability, crucial for sectors like construction where tracking the origin and history of materials is vital. Privacy also plays a critical role, particularly in how sensitive data are handled within the supply chain. Balancing transparency with confidentiality is crucial; while blockchain enhances transparency, it is imperative to ensure that sensitive data remains confidential to protect competitive advantages and intellectual property [50].

Moreover, the review [50] highlights the importance of navigating regulatory landscapes effectively to manage compliance with data protection and financial regulations. The ability to manage regulatory and legal risks proactively is essential for minimizing disruptions and leveraging the full capabilities of blockchain technology in supply chain operations.

Both the referenced studies [48,49] along with the insights from the latest research [50] underline the necessity of understanding the enablers and barriers to blockchain adoption. Addressing these challenges through compliance measures, data standardization,

robust privacy protections, and effective regulatory adherence will be key to harnessing blockchain's potential to transform supply chain operations across various industries.

4.5. Blockchain in Vehicular Networks: Legal, Privacy, and Regulatory Compliance

The implementation of blockchain technology in vehicular networks has introduced advanced solutions to address a myriad of legal, regulatory, privacy, and data security concerns. The technology not only enhances mechanisms for managing data sovereignty but also significantly improves privacy in digital identity management, enabling transactions that are both anonymous and verifiable. This is particularly crucial in environments where the security of blockchain infrastructure, including the safeguarding of private keys, is paramount to prevent irreversible damage to digital assets.

Legal challenges in vehicular networks, such as the establishment of clear data ownership and liability in accidents involving autonomous and connected vehicles, are being transformed by blockchain. The technology's capacity to create transparent and immutable ledgers helps in recording data transactions securely, thus clarifying ownership rights and simplifying the enforcement of liability terms through smart contracts. These contracts automatically execute agreements based on coded conditions, thereby enhancing accountability and reducing disputes over liability [51]. Concerning data management, vehicular networks involve the handling of sensitive data that must be robustly protected against unauthorized access and tampering. Blockchain's cryptographic algorithms and its decentralized architecture play a pivotal role in securing data. The immutable nature of blockchain ensures that once data are recorded, they are nearly impossible to alter, thus preserving the integrity and reliability of information crucial for vehicular operations. These features are essential for maintaining a high trust level among network participants, ensuring that data manipulation and breaches are minimized [51,52]. Privacy issues are particularly paramount in vehicular networks where both location data and personal information require stringent protection measures. Blockchain addresses these concerns with its advanced encryption capabilities and decentralized structure, which safeguard against unauthorized surveillance and data breaches. Moreover, the technology provides for the management of personal data in compliance with privacy regulations, balancing transparency needs with confidentiality requirements [51].

Finally, the regulatory landscape for vehicular networks is complex due to the decentralized nature of blockchain. Compliance with existing data protection, privacy, and cybersecurity laws is facilitated by blockchain's inherent auditability, which provides transparent and verifiable records of data transactions. Furthermore, ensuring interoperability with traditional vehicular network systems and international regulatory standards is facilitated by blockchain's standardized protocols and smart contracts, which help in navigating the diverse regulatory environments and aligning different technological frameworks [51]. In conclusion, the integration of blockchain technology within vehicular networks marks a pivotal advancement in addressing the multifaceted challenges associated with these systems. By leveraging the inherent security features and decentralized nature of blockchain, stakeholders can significantly enhance the integrity and confidentiality of data transactions. These technological attributes are crucial for safeguarding against unauthorized access and ensuring the reliability of data communications across vehicular networks. Moreover, blockchain's capability to enforce transparent and immutable record-keeping practices introduces a new level of efficiency in managing legal and regulatory compliance. This is particularly relevant in scenarios involving multi-jurisdictional regulations and the complex liability structures of autonomous vehicular operations. Additionally, the strategic implementation of blockchain's privacy-preserving mechanisms, such as advanced encryption and smart contracts, supports the delicate balance between operational transparency and the protection of personal user data. As the landscape of connected vehicles and intelligent transportation systems continues to evolve, blockchain technology offers indispensable tools for navigating the increasing complexity of digital interactions within

vehicular networks, thereby fostering a more secure, compliant, and efficient transportation infrastructure.

4.6. Blockchain in E-Voting Systems: Legal, Privacy, and Regulatory Compliance

The integration of blockchain technology into electronic voting systems marks a significant evolution in how elections are conducted, enhancing security, transparency, and integrity. Yet, this technology introduces substantial legal, privacy, and regulatory challenges that must be meticulously addressed to ensure successful implementation and broad acceptance.

Establishing clear legal frameworks that align with existing electoral laws and data protection regulations is fundamental to the adoption of blockchain for e-voting. Blockchain's ability to ensure the immutability of voting records boosts election integrity by preventing tampering and fraud. However, this same immutability raises compliance issues with privacy laws such as the GDPR, which mandates rights such as data erasure [53]. Developing blockchain e-voting systems requires balancing transparency with legal requirements to protect voter privacy and anonymity. Consequently, legal frameworks must evolve to accommodate these technological changes without undermining democratic principles [54].

Ensuring the security and integrity of voting data is paramount in blockchain-based e-voting systems. The decentralized and tamper-resistant nature of blockchain provides a robust platform for securing voting data against unauthorized access and cyber threats. Achieving this requires the implementation of advanced cryptographic techniques, including encryption and secure hashing algorithms. Regular audits and security assessments are essential to maintain the integrity of the voting process and to verify the accuracy of the stored data. Technical solutions must ensure that data are accessible for verification while being protected against manipulation or unauthorized disclosure [55].

A critical aspect of e-voting systems is protecting voter privacy while maintaining ballot secrecy. Blockchain's transparent nature can potentially conflict with voter anonymity needs. Privacy-enhancing technologies such as ring signatures, zero-knowledge proofs, and homomorphic encryption are crucial. These technologies enable voters to cast their votes anonymously while allowing for the transparency needed to audit and verify election results [53]. Implementing these technologies helps reconcile the requirements for open and verifiable elections with strict privacy mandates [54].

Navigating the complex regulatory landscape is also crucial. The decentralized nature of blockchain complicates regulatory compliance, especially in jurisdictions with stringent data protection laws. Efforts to develop standardized regulatory frameworks that address the unique challenges posed by blockchain technologies are necessary. This includes establishing protocols ensuring interoperability with traditional voting systems and adherence to international data protection standards [55].

In conclusion, while blockchain offers significant advantages for improving the integrity and efficiency of e-voting systems, the successful integration of this technology into electoral processes heavily depends on resolving extensive legal, privacy, and regulatory issues. A comprehensive and multidisciplinary approach involving continuous technological innovation alongside dynamic legal and regulatory adaptation is required. Only through such a balanced approach can blockchain-based e-voting systems achieve the necessary standards of reliability and acceptance [53–55].

4.7. Blockchain in Education: Legal and Regulatory Compliance

The integration of blockchain technology in educational systems introduces a multifaceted landscape of legal, privacy, and regulatory challenges. The potential of blockchain to transform educational processes through enhanced security, transparency, and efficiency is significant. However, its characteristics such as immutability and decentralization, while beneficial, bring forth complex legal challenges. The stringent requirements of data protection laws such as the General Data Protection Regulation (GDPR) necessitate robust privacy controls and afford extensive rights to individuals, including the right to data erasure. This

right poses a fundamental challenge to blockchain's permanent record-keeping features, creating a critical area of legal tension that educational institutions must navigate [56,57].

The transparency inherent in blockchain technology, which is crucial for data integrity and security, simultaneously raises substantial privacy concerns. This transparency means that once information is added to the blockchain, it becomes easily accessible and permanently recorded, which can include sensitive educational data. To address these concerns, it is imperative for educational institutions to deploy advanced privacy-enhancing technologies. These technologies should aim to strike a balance between the immutable nature of blockchain and the need for confidentiality and privacy compliance. By doing so, institutions can protect individual privacy rights while leveraging the benefits of blockchain technology [56,57].

Moreover, ensuring data security in blockchain-based educational systems is paramount. The decentralized nature of blockchain significantly reduces risks associated with centralized data storage, such as single points of failure that can lead to data breaches. However, this same decentralization introduces new challenges, such as the need for secure management of private keys and the potential vulnerabilities in smart contract implementations. Educational institutions must, therefore, implement stringent security protocols, including regular updates and audits, to safeguard against these unique threats. This will enhance the overall trustworthiness and reliability of blockchain systems in educational settings [56,57]. Sustainability is another critical aspect of blockchain's implementation in education. Traditional blockchain implementations, particularly those utilizing consensus mechanisms like Proof of Work, are known for their high energy consumption. This presents a sustainability concern that cannot be overlooked in today's environmentally conscious world. Adopting alternative consensus mechanisms such as Proof of Stake can significantly reduce the environmental footprint of blockchain systems, making them more suitable for sustainable educational practices. Additionally, these mechanisms can enhance the scalability and efficiency of blockchain applications, facilitating broader adoption in education [57].

Finally, the readiness of the market and the educational ecosystem for blockchain technology is essential for its successful integration. The adoption of blockchain in education requires more than just technological readiness; it involves preparing the entire educational community, including educators, administrators, and policymakers, to embrace these changes. This preparation involves extensive education on blockchain technology, collaboration on pilot projects, and the development of supportive policies that foster an environment conducive to innovation. Such comprehensive readiness efforts will ensure that blockchain technology can be effectively integrated into educational practices, thereby maximizing its benefits while adhering to legal and ethical standards [56,57].

4.8. Blockchain in Social Media: Legal, Privacy, and Regulatory Compliance

The integration of blockchain technology into social media platforms heralds a new era of user control and privacy. Traditional social media models have long been criticized for retaining extensive control over user data, leading to significant concerns about privacy and data ownership. Blockchain's decentralized nature offers a compelling alternative, enabling users to exert greater ownership and control over their data. Smart contracts can delineate data ownership rights and permissions, fostering an environment of transparency and accountability. However, this shift introduces legal complexities, particularly regarding the validity and enforceability of smart contracts across different jurisdictions. Addressing these legal issues requires international cooperation and the establishment of clear guidelines to ensure that blockchain-based social media platforms operate within a reliable legal framework [2].

Enhancing data privacy and security is a paramount concern in the realm of social media, where breaches and misuse of personal information are frequent. Blockchain's decentralized architecture, combined with robust encryption mechanisms, significantly bolsters data privacy and security. By decentralizing data storage, blockchain reduces vulnerabilities associated with central points of failure. Nonetheless, the immutable nature

of blockchain records presents a challenge in aligning with data protection regulations like the General Data Protection Regulation (GDPR). These regulations afford users the right to modify or erase their data, a provision that conflicts with blockchain's permanent record-keeping. Thus, there is a critical need for innovative privacy-enhancing technologies that can balance the immutability of blockchain with the flexibility demanded by privacy laws [58].

Regulatory compliance is another area where blockchain's adoption in social media presents significant challenges. The decentralized nature of blockchain complicates the application of traditional regulatory frameworks, which are often designed with centralized entities in mind. This necessitates a reevaluation of regulatory strategies to ensure that they can accommodate the unique aspects of blockchain technology while safeguarding user rights and promoting fair competition. Effective regulatory oversight will likely require collaborative efforts between industry stakeholders and regulators to navigate these complexities and foster an environment conducive to responsible blockchain deployment. This balance between innovation and regulation is crucial for the sustainable integration of blockchain in social media platforms [2,58]. The issue of content integrity is particularly pertinent in the age of misinformation and fake news. Blockchain's transparency and traceability features offer a promising solution to these problems by providing a verifiable audit trail for content. This capability can help verify the authenticity of information shared on social media, thereby enhancing the credibility of these platforms. In addition, blockchain can support more effective content moderation processes, ensuring that harmful or false information is identified and addressed promptly. By leveraging blockchain for content verification, social media platforms can build trust and integrity, which are essential for fostering a healthy online community [58].

Monetization models in social media stand to benefit significantly from blockchain technology. Traditional advertising models are fraught with issues such as fraud and lack of transparency. Blockchain can address these issues by enabling transparent and traceable transactions, thus reducing the risk of fraudulent activities in the advertising ecosystem. Moreover, blockchain empowers users to take control of their data, allowing them to monetize their personal information through tokenized incentives or data-sharing agreements. This shift towards user-centric data ownership not only enhances privacy and transparency but also provides a more equitable model for revenue sharing in social media interactions [58]. In conclusion, while blockchain technology holds significant promise for enhancing data security, privacy, and user empowerment in social media platforms, it also introduces a range of legal, regulatory, and ethical challenges. Successfully integrating blockchain into social media will depend on the ability of stakeholders to address these challenges through innovative solutions and collaborative efforts. By doing so, blockchain can help create a more secure, transparent, and user-focused social media environment [2,58].

4.9. Blockchain in Finance: Legal, Privacy, and Regulatory Compliance

The advent of blockchain technology in the financial sector introduces profound changes that challenge existing legal frameworks and necessitate new regulatory approaches. Blockchain, by its nature, decentralizes the control of transactional data, which traditional laws are not designed to manage. This decentralization offers unprecedented opportunities for transparency and efficiency but also introduces significant risks that can be exploited for money laundering, terrorism financing, and other illicit activities. The pressing need for updated regulations that address these risks while promoting technological advancements is evident [59].

Privacy issues in the context of blockchain are particularly complex. The technology inherently provides a transparent transaction ledger, which is beneficial for accountability and fraud prevention. However, this transparency also raises significant privacy concerns. Transactions on blockchain networks, though recorded pseudonymously, leave a permanent and public trail that, when combined with other data, can potentially lead

to the identification of individuals involved in these transactions. This characteristic of blockchain conflicts with privacy protection laws such as the General Data Protection Regulation (GDPR), which emphasizes the right to privacy and the control of personal data. Addressing these privacy concerns requires a nuanced approach that involves enhancing the privacy features of blockchain technologies without undermining the security and transparency that make them valuable [60].

The regulatory challenges posed by blockchain in the financial sector are further complicated by its global nature. Financial transactions using blockchain can cross multiple jurisdictions within a single transaction sequence, complicating compliance with diverse legal systems. This situation calls for international cooperation to establish unified regulatory standards that can accommodate the borderless operations of blockchain technologies. Such standards would need to cover a wide range of concerns from consumer protection to the prevention of financial crimes, ensuring a balanced approach that fosters innovation while protecting the public [59]. Moreover, the decentralized financial systems (DeFi) that blockchain enables represent a radical departure from traditional financial systems. DeFi platforms allow financial transactions to occur outside the jurisdiction of central banks and other regulatory institutions, which presents a unique set of challenges for regulators. These platforms can improve financial inclusivity and reduce transaction costs, but they also raise concerns regarding the stability of the financial system and the protection of consumers from fraud and other risks. Regulatory frameworks need to evolve to address these challenges effectively, possibly through the establishment of new oversight mechanisms that are adapted to the decentralized nature of blockchain technologies [60].

In conclusion, the integration of blockchain technology into the financial sector demands a comprehensive reevaluation of existing legal and regulatory frameworks. A robust approach to regulation would involve not only adapting current laws to meet the challenges posed by new technologies but also promoting international collaboration to create cohesive standards that ensure security, privacy, and efficacy across global financial systems. Such measures are crucial for leveraging the benefits of blockchain while safeguarding against its risks, thus ensuring that its integration into the financial sector is beneficial and sustainable [59,60].

4.10. Blockchain in Tourism: Legal, Privacy, and Regulatory Compliance

The deployment of blockchain technology within the tourism sector marks a significant shift in how transactions and data are handled, offering potential improvements in efficiency and trust. However, this technology also introduces a host of legal, privacy, and regulatory challenges that are intricate and multifaceted.

Legal challenges in implementing blockchain in tourism arise primarily from the use of smart contracts and the inherent jurisdictional complexities of a decentralized network that spans the globe. Smart contracts, which are agreements coded on blockchain to execute automatically under certain conditions, raise questions about their enforceability and compatibility with existing contractual laws. In the tourism sector, contracts govern a wide array of transactions from booking accommodations to hiring local services, making the legal recognition of these digital agreements critical. The decentralized nature of blockchain complicates this further as it can be unclear which country's laws govern a contract and how disputes should be resolved when they arise. This global aspect requires robust international legal frameworks that can adapt to the complexities of blockchain, ensuring that transactions are both transparent and compliant with laws across different jurisdictions [61].

Privacy concerns are particularly acute in the tourism industry due to the sensitive nature of the personal data involved. Blockchain's characteristic of immutability—while ensuring data integrity and transparency—poses significant challenges to privacy. Once information is added to the blockchain, it is difficult to alter or delete, potentially conflicting with privacy regulations such as the General Data Protection Regulation (GDPR), which enforces the right to erasure or 'the right to be forgotten'. The tourism sector, where

customer trust is paramount, must reconcile blockchain's transparency with the need to protect personal data. Innovations in blockchain privacy, such as enhanced encryption methods or the use of private, permissioned ledgers where access to data is controlled, are critical for maintaining consumer trust while leveraging the benefits of blockchain technology [61,62].

Regulatory compliance is another significant concern, as blockchain applications must navigate a complex landscape of international regulations that govern data protection, consumer rights, and financial transactions. The absence of a centralized authority in blockchain platforms complicates compliance with these regulations, often designed for traditional centralized businesses. For instance, the regulatory frameworks for anti-money laundering (AML) and combating the financing of terrorism (CFT) are challenging to enforce in a decentralized system that spans multiple legal territories. Additionally, the tourism sector faces unique challenges in licensing and certification for blockchain solutions, as regulatory bodies may not yet have clear guidelines for these emerging technologies. Ensuring that blockchain platforms in tourism are compliant with both local and international laws is essential to prevent legal repercussions and foster an environment conducive to the widespread adoption of this technology [62]. In conclusion, while blockchain technology presents exciting opportunities for innovation in the tourism sector, it also demands a proactive approach to address the legal, privacy, and regulatory challenges it introduces. Stakeholders must collaborate to develop and implement regulatory frameworks that accommodate the unique aspects of blockchain technology, ensuring that its deployment in tourism is both innovative and compliant with international standards. By doing so, the tourism industry can harness the potential of blockchain to create a more secure, transparent, and efficient service delivery system while safeguarding the rights and privacy of its customers [61,62].

4.11. Summary of Legal and Regulatory Compliance (RQ2)

In this section, we have examined the unique legal, privacy, and regulatory challenges that blockchain technology faces across various sectors. Table 4 summarizes these issues along with potential solutions and considerations. For instance, in healthcare, compliance with regulations like GDPR necessitates robust privacy controls and secure patient consent processes. The finance sector deals with regulatory uncertainties and privacy concerns due to blockchain's transparency, requiring standardized regulatory frameworks and enhanced privacy features. IoT faces challenges related to GDPR compliance and data management, addressed by Privacy by Design and secure integration strategies.

In summary, each sector demands tailored legal and regulatory approaches to effectively integrate blockchain technology. This highlights the necessity for ongoing collaboration between technologists, legal experts, and regulators to develop adaptable frameworks that support both innovation and compliance. Balancing these aspects is crucial for the sustainable and responsible adoption of blockchain across diverse industries. While scalability solutions are essential, they must be complemented by supportive regulatory environments. Even the most advanced blockchain technologies may falter without regulatory frameworks that accommodate their unique attributes. Therefore, our research now pivots towards our third research question: What trends are emerging in blockchain scalability and regulatory compliance solutions across various domains, and what future research directions can be derived from the existing literature? This next phase will allow us to explore how current innovations in scalability and regulatory compliance intersect and influence each other. Understanding these emerging trends will provide insights into how blockchain can achieve both technical efficiency and regulatory adherence, ensuring its practical and widespread application across different sectors.

Table 4. Summary of Blockchain Legal, Privacy, and Regulatory Challenges and Solutions.

Industry	Legal Challenges	Privacy and Data Security Concerns	Solutions and Regulatory Considerations
Healthcare	Compliance with GDPR, complex patient consent processes [45]	Security of sensitive patient data, ensuring confidentiality [46]	Implementation of blockchain with enhanced privacy features and legal harmonization [45,46]
Finance	Regulatory uncertainty, legal status of smart contracts [59]	Data privacy issues due to blockchain's transparency [60]	Developing standardized regulatory frameworks and enhancing privacy features of blockchain technologies [59,60]
IoT	GDPR compliance, device and data management [9]	Risks of increased surveillance and data breaches [44]	Privacy by Design, Data Protection Impact Assessments, secure IoT integration with blockchain [9,44]
Genomics	Ethical concerns around consent and data ownership [47]	Ensuring data integrity and patient privacy [47]	Dynamic consent models, regulatory adaptations for blockchain in genomic research [47]
Supply Chain	Legal barriers with smart contracts, multi-jurisdictional compliance [48]	Traceability vs. confidentiality dilemmas [50]	Data standardization, robust privacy protections, effective regulatory adherence [48,50]
Vehicular Networks	Data ownership, liability in autonomous vehicle accidents [51]	Balancing transparency with confidentiality [51]	Implementation of privacy-preserving technologies, compliance with cybersecurity laws [51,52]
Education	Balancing blockchain's immutability with the right to data erasure [56,57]	Protecting sensitive educational data, enhancing data security [56,57]	Advanced privacy-enhancing technologies, secure management of blockchain systems [56,57]
Tourism	Enforceability of smart contracts, jurisdictional complexities [61]	Reconciling blockchain transparency with privacy needs [62]	Use of private, permissioned ledgers, international legal frameworks for blockchain [61,62]
E-Voting Systems	Legal alignment with electoral laws, voter privacy [53,54]	Ensuring ballot secrecy and voter anonymity [53]	Privacy-enhancing technologies, regulatory frameworks for blockchain e-voting [53,55]
Social Media	Legal status of smart contracts, data ownership [2]	Addressing privacy concerns in a highly transparent system [58]	Regulatory adaptation, privacy-enhancing technologies, secure and transparent content management [2,58]

5. Trends and Future Research Directions (RQ3)

In this section, we delve into the emerging trends in blockchain scalability and regulatory compliance solutions based on our comprehensive literature review. By examining the latest strategies and methodologies, we aim to highlight how different sectors are addressing both scalability and regulatory challenges. This analysis will provide a roadmap for future research and development, ensuring that blockchain technology evolves in a manner that is both technically robust and legally compliant.

5.1. Trends and Future Directions in Blockchain Scalability Solutions

This subsection covers the emerging trends in scalability solutions, focusing on the latest advancements and techniques being developed to enhance blockchain performance across different industries. We will explore innovations such as sharding, off-chain solutions, and new consensus algorithms, and how these developments are addressing the scalability challenges identified in previous sections.

5.1.1. Layer-2 Solutions

Layer-2 solutions represent a significant advancement in blockchain technology, designed to enhance scalability and performance by processing transactions off the main chain, thus reducing load and speeding up processing times without sacrificing security or decentralization. These solutions, initially developed for the cryptocurrency sector to facilitate quick and cost-effective transactions, have expanded their applications due to their adaptability and effectiveness across various domains [63].

State channels and sidechains are the primary types of Layer-2 solutions. State channels allow transactions among participants to occur outside of the blockchain, requiring the blockchain only to open and close these channels. This is particularly beneficial in environments like gaming or trading, where numerous transactions occur rapidly. An exemplary implementation of this is the Lightning Network, which facilitates fast, scalable microtransactions within the Bitcoin ecosystem by allowing users to create private channels for transactions that only settle on the blockchain at the beginning and end of the interaction [63]. Sidechains operate as independent blockchains with their own consensus rules but are connected to the main blockchain, allowing assets to be transferred between them. This setup not only enhances the scalability of transactions but also supports complex smart contracts, making them suitable for a broad range of applications from financial services to sophisticated decentralized applications [64].

Layer-2 solutions are evaluated based on scalability, security, operational efficiency, and privacy. They excel in environments requiring high transaction throughput and low latency, with mechanisms like commit-chains enhancing scalability by batching transactions off-chain, although this can introduce slight delays. Security is robust, as these solutions employ collateral or bonding to ensure integrity while transactions are processed off-chain, with a strong reliance on the main blockchain for dispute resolution. Privacy is also a key advantage, as transactions are less visible to the public, although the degree of privacy varies depending on the specific Layer-2 technology employed [63]. Operational efficiency is another significant benefit of Layer-2 solutions, with state and payment channels reducing transaction costs and processing times. However, the involvement of third-party protocols in dispute resolution can complicate operations and potentially slow down transaction speeds depending on the dispute's complexity.

The applicability of Layer-2 solutions extends beyond financial transactions to sectors like supply chain management, healthcare, and the Internet of Things (IoT). In supply chains, they enhance transparency and efficiency, crucial for managing logistics and verifying the authenticity of goods [65]. In healthcare, these solutions facilitate the secure and efficient sharing of sensitive patient data across institutions [16]. IoT benefits from Layer-2 solutions in handling the large volumes of data generated by connected devices, ensuring efficient and secure data management [10]. Despite their extensive benefits, Layer-2 solutions face challenges such as managing off-chain computations, maintaining data integrity, and ensuring seamless synchronization with the main blockchain. Addressing these challenges requires robust technical solutions and often significant adjustments to existing infrastructure to ensure interoperability and efficient operation. As these technologies continue to evolve, future developments in Layer-2 solutions are likely to focus on enhancing their scalability, security, and decentralization balance. Improving cryptographic mechanisms and streamlining integration processes with existing blockchain frameworks will be crucial for broader adoption. These advancements promise to significantly enhance the functionality and efficiency of blockchain across multiple sectors, fostering greater acceptance and integration of this transformative technology [66].

5.1.2. Sharding and Partitioning Techniques

Sharding and partitioning techniques represent key strategies for overcoming the scalability limitations inherent in blockchain technologies. These methods partition the blockchain network into smaller, more manageable segments, enabling independent transaction processing within each segment. This approach significantly enhances the network's

throughput and reduces the storage demands on individual nodes. For example, sharding allows different segments of the network to handle distinct sets of transactions concurrently, which is particularly crucial for high-volume systems like Bitcoin and Ethereum where scalability challenges have historically posed significant bottlenecks [67]. Partitioning extends the capabilities of sharding by dividing the network's data and operations into even smaller, independent units. This finer division facilitates parallel processing of transactions, further boosting the scalability and operational efficiency of blockchain systems. By reducing the computational load on any single node, partitioning allows the network to expand and manage higher transaction volumes without corresponding increases in processing time or costs.

The comprehensive survey by Liu et al. (2023) delves into various sharding schemes, classifying them based on blockchain type and sharding technique. It assesses these schemes using criteria such as scalability, applicability, and reliability, highlighting the nuanced trade-offs between enhancing performance and maintaining the decentralized ethos of blockchain technology [68]. The study also points out the pressing need for improved security measures and reduced transaction latency to better balance decentralization with scalability and security. In practical applications, sharding proves to be invaluable across diverse sectors. The Internet of Things (IoT), it effectively manages the massive data flows from numerous devices, ensuring scalable and efficient blockchain support [10]. The ability to handle large volumes of data in parallel ensures that IoT devices can function seamlessly without causing bottlenecks in the network. In supply chain management, parallel transaction processing enabled by sharding facilitates smoother and more efficient operations, improving the speed and accuracy of logistics tracking and verification [65]. This is particularly important for tracking goods in real time and ensuring transparency throughout the supply chain. The financial sector benefits from sharding through enhanced transaction processing speeds and reduced operational costs, which collectively boost the efficiency of financial transactions [35]. Faster transaction times can lead to improved customer satisfaction and lower costs for financial institutions. Moreover, in healthcare, particularly in the field of genomics, sharding supports the secure and expedient processing of large-scale data sets, thereby advancing the privacy and processing speed of genomic information [17]. This ensures that sensitive genomic data can be handled efficiently and securely, facilitating advancements in personalized medicine.

Despite its advantages, the deployment of sharding technology introduces new challenges. Maintaining a consistent state across different network segments is crucial for ensuring the integrity and finality of transactions. This synchronization becomes increasingly challenging with higher transaction volumes, necessitating robust and effective inter-shard communication mechanisms to manage the complexity. Effective communication protocols must be established to ensure that all shards remain in sync, even as the number of transactions increases. Furthermore, the security landscape of sharded networks can become more vulnerable; smaller node groups within each shard may be easier to compromise, posing increased risks of security breaches [69]. Ensuring the security of each shard is critical to maintaining the overall security of the blockchain network.

The ongoing evolution of blockchain technology keeps sharding at the forefront of research and development efforts. Future enhancements are expected to focus on strengthening security measures, reducing transaction latencies, and optimizing the trade-offs between decentralization, scalability, and security. These advancements are essential for ensuring that sharding remains effective and viable as blockchain applications continue to expand and diversify, catering to the ever-growing demands of modern digital infrastructures without compromising core blockchain principles [69]. By addressing these challenges, sharding can continue to be a pivotal technology in the advancement of scalable and efficient blockchain systems.

5.1.3. Optimization of Consensus Algorithms

The optimization of consensus algorithms represents a critical focus area within blockchain technology aimed at addressing the inherent scalability challenges of various blockchain networks. Traditional consensus mechanisms such as Proof of Work (PoW) are notoriously resource-intensive, significantly limiting scalability due to their high energy and computational demands. This limitation is particularly problematic in blockchain networks like Bitcoin, where the scalability constraints have led to significant bottlenecks [67]. To counteract these drawbacks, the blockchain community has explored more efficient consensus mechanisms, such as Proof of Stake (PoS) and Delegated Proof of Stake (DPoS). These mechanisms not only reduce the computational load by eliminating the need for energy-intensive mathematical problems but also expedite the process of transaction validation. As a result, networks employing PoS or DPoS can achieve higher transaction throughput with lower energy consumption, thereby enhancing scalability [35].

Another significant advancement in consensus algorithms is the Practical Byzantine Fault Tolerance (PBFT), which is designed to offer fault tolerance in adversarial network environments. PBFT improves upon the traditional fault tolerance mechanisms by providing low latency and high throughput, making it an ideal choice for networks that require robust consensus without the high overhead of PoW [67]. The comprehensive review by Hussein et al. (2023) underscores the evolution and importance of these consensus mechanisms within the blockchain ecosystem. The review delineates various consensus algorithms by their efficiency, security implications, and adaptability to different blockchain configurations. It further discusses the trade-offs involved in selecting an appropriate consensus algorithm for a given blockchain application, emphasizing the balance between decentralization, scalability, and security [70]. In practical scenarios, optimized consensus algorithms have found applications across diverse sectors. For instance, the Internet of Things (IoT) enables the handling of large data flows from numerous devices efficiently and sustainably. In the financial sector, these algorithms facilitate faster transaction processing and enhance throughput, significantly boosting operational efficiency [10]. Similarly, in smart home technologies and vehicular networks, optimized consensus mechanisms improve communication security and data integrity, ensuring reliable and secure interactions across increasingly networked environments [5,23].

Despite the progress in optimizing consensus algorithms, challenges remain, particularly in maintaining consistent network synchronization and ensuring security in highly decentralized environments. The issue of scalability versus security presents a significant dilemma, as enhancing one often impacts the other. The ongoing evolution of consensus algorithms continues to be a pivotal area of research and development within the blockchain community. Future advancements are expected to focus on further reducing transaction latency, improving the energy efficiency of consensus processes, and strengthening the security measures to counteract emerging threats in decentralized networks [69].

5.1.4. Rollups

Rollups have rapidly gained prominence as a pivotal enhancement in blockchain scalability. These technologies address fundamental challenges in blockchain architecture by processing transactions off the main chain, thus reducing network congestion and significantly boosting throughput. Rollups work by aggregating multiple transactions into a single one that is processed off-chain, which not only speeds up transaction times but also lowers transaction costs. This makes them an essential development in the evolution of blockchain technologies, especially for high-demand applications [71].

The primary types of rollups, Zero-Knowledge (ZK) Rollups and Optimistic Rollups, cater to different security and performance needs. ZK-Rollups utilize zero-knowledge proofs to validate the correctness of transactions outside the blockchain, ensuring security and privacy without compromising the details of the transactions. This type is particularly useful in sectors where privacy and fast transaction clearance are crucial, such as finance and personal data management [72]. Optimistic Rollups, on the other hand, assume

transactions are valid unless challenged. They provide quicker transaction processing by reducing the number of validations needed but introduce a delay in finality if a transaction is disputed, which can be a suitable trade-off in less time-sensitive applications [71].

These rollup technologies have been integrated into various industrial applications, proving their versatility and efficiency. In the financial sector, ZK-Rollups are being employed to enhance transaction throughput and reduce costs, making blockchain solutions more viable for everyday financial operations and complex contract executions [71]. The technology also supports scalable solutions in the Internet of Things (IoT), where managing large arrays of device data without overwhelming the blockchain becomes possible. ZK-Rollups can efficiently handle the data demands of smart cities, optimizing everything from traffic management to energy distribution without sacrificing the security or integrity of the data [73]. The implementation of Rollups in healthcare offers promising improvements in the handling of sensitive medical records. By ensuring data are processed quickly and securely, Rollups can help healthcare providers offer better and more timely care, all while maintaining patient privacy and compliance with regulations [18]. In education and social media, Optimistic Rollups are being explored to manage user interactions and data exchanges securely and transparently, ensuring that content management and credential verifications are handled efficiently [29].

However, the deployment of Rollups is not without challenges. Technical complexities in integrating these systems with existing blockchain infrastructures require significant development effort and a deep understanding of both traditional and new blockchain architectures. Ensuring that Rollups seamlessly interact with the main chain and maintain data integrity and security during transactions is critical and demands ongoing innovation and refinement [72]. In summary, Rollups represent a transformative approach to enhancing blockchain functionality, providing a scalable, secure, and efficient method for handling transactions across various industries. As this technology continues to evolve, it is expected to become a cornerstone of blockchain infrastructure, expanding the potential applications of blockchain technology far beyond its current capabilities [72].

5.1.5. Integrating Scalability Solutions across Domains

We have explored various blockchain scalability solutions, evaluating their effectiveness and potential drawbacks as summarized in Table 5. This analysis helps us understand how these technologies can be applied effectively across different industries, as detailed in Table 6. Our findings show that scalability solutions such as Layer-2 technologies and Rollups significantly boost transaction speeds but also introduce challenges in managing off-chain computations and ensuring synchronization. For example, Layer-2 solutions reduce the main chain's load but require sophisticated management systems to handle off-chain activities, which can be complex in settings requiring tight data synchronization. On the other hand, sharding and partitioning enhance operational efficiency by processing transactions in parallel. This method, however, complicates the maintenance of a consistent state across network segments and increases security risks, especially within smaller node groups. Similarly, optimizing consensus algorithms reduces computational demands and increases sustainability but may affect network security and synchronization accuracy.

The use of these solutions is varied across different domains, each with its specific requirements and challenges. In sectors like healthcare and finance, where security and privacy are crucial, the benefits provided by Rollups and advanced consensus mechanisms are particularly valuable. Industries such as IoT and supply chain management gain from the high throughput and efficiency of Layer-2 solutions and sharding techniques.

To integrate these scalability solutions effectively, a strategic approach is essential. For example, combining sharding with Layer-2 solutions might optimize performance in fields like finance and supply chain management, where high transaction volumes and quick processing are critical. In contrast, in areas like healthcare, where the integrity and privacy of data are paramount, combining Rollups with consensus optimizations could provide the best balance between efficiency and security.

This straightforward approach to integrating blockchain scalability solutions highlights the need to align technological capabilities with the specific demands of various industries. As blockchain technology evolves, future research will likely focus on developing integration strategies that address scalability while improving the overall security and efficiency of blockchain systems. The aim is to support wider adoption across diverse sectors, enabling blockchain technology to meet the demands of modern digital infrastructures.

Table 5. Comparative Analysis of Blockchain Scalability Solutions.

Solution	Effectiveness	Potential Drawbacks
Layer-2 Solutions	Enhances transaction speed and reduces main chain load, significantly improving scalability [63].	Complex management of off-chain computations and synchronization issues may challenge integration and operation [66].
Sharding and Partitioning	Increases throughput by processing transactions in parallel across smaller segments, improving operational efficiency [67,68].	Maintaining consistent state across segments increases complexity and poses security risks from smaller node groups [69].
Optimization of Consensus Algorithms	Reduces computational and energy demands, facilitating faster and more sustainable transaction processing [35,67].	Potential impact on network security and synchronization, posing risks to network integrity [70].
Rollups	Reduces network congestion by off-chain transaction processing, significantly boosting throughput [71,72].	Integration challenges with existing blockchain frameworks and potential delays in transaction finality during disputes [72].

Table 6. Summary of blockchain scalability solutions across different domains.

Domain	Layer-2 Solutions	Sharding and Partitioning Techniques	Consensus Algorithm Optimization	Rollups	Key Benefits of Scaling Solutions
IoT	✓ [10,63]	✓ [10,67]	✓ [35]	✓ [73]	• Management of high volume data • Secure communication between devices • Improved energy efficiency
Healthcare	✓ [66]			✓ [18]	• Secure storage and sharing of medical records • Improved patient care • Ensured data privacy
Genomics		✓ [69]			• Secure storage and sharing of genomic data • Privacy assurance • Reduced processing times
Supply Chain Management	✓ [65,66]	✓ [65]			• Improved transparency, traceability, efficiency, and parallel processing of transactions
Vehicular Networks			✓ [35]		• Enhanced communication, security, and data sharing between vehicles
E-Voting Systems				✓ [26]	• Improved performance and efficiency • Enhanced security and transparency in the voting process
Education				✓ [29]	• Improved performance and efficiency of blockchain-based educational systems • Secure credential storage and sharing
Social Media				✓ [71]	• Secure, transparent, and efficient content sharing and management
Finance	✓ [63]	✓ [67]	✓ [35]	✓ [71]	• Faster, more secure transactions • Reduced transaction costs • Improved transaction processing times
Tourism	✓ [38]	✓ [39]			• Efficient transaction processing during peak seasons • Enhanced security and fraud reduction • Streamlined customer loyalty and reward programs

5.1.6. Future Research Direction in Blockchain Scalability Solutions

Future research in blockchain scalability could significantly benefit from focusing on the development and refinement of Layer-2 solutions tailored to the unique requirements of different domains. A deeper understanding of these domain-specific challenges will help in creating more efficient and effective scalability solutions. The customization of Layer-2 protocols to suit the specific needs of industries such as healthcare, finance, and IoT could lead to enhanced performance and broader adoption [35].

There is a growing need for improved security and privacy features in off-chain transaction methods. Thus, future investigations should focus on techniques that safeguard transaction confidentiality and deter unauthorized data access. Research could delve into advanced cryptographic techniques and privacy-preserving mechanisms to ensure that off-chain solutions do not compromise the integrity and confidentiality of transactions [15].

Another important research direction is exploring the interoperability between different Layer-2 approaches and other blockchain-based systems. This could lead to robust scalability solutions that harness the strengths of multiple methodologies. Interoperability will be crucial in creating seamless and cohesive blockchain ecosystems where different Layer-2 solutions can coexist and complement each other, enhancing overall scalability and functionality [63].

Additionally, the optimization and exploration of different types of rollups, and understanding their potential implications on the security, decentralization, and governance of blockchain systems, is another promising research area. Future research could investigate how to maximize the efficiency and security of ZK-Rollups and Optimistic Rollups, while also exploring new variants that could offer improved performance and scalability [71].

Future research could also delve into understanding the trade-offs between scalability and other blockchain features, such as security, decentralization, and governance. Gaining a deeper understanding of these trade-offs could contribute to the creation of more balanced and sustainable scalability solutions [67]. Research could focus on developing frameworks and models that help quantify these trade-offs, providing guidelines for designing more effective blockchain systems.

Exploring the potential benefits of combining different Layer-2 protocols to attain better scalability and security is another area for future research. By leveraging the strengths and mitigating the limitations of multiple Layer-2 protocols, it may be possible to develop more robust and efficient scalability solutions. Domain-specific challenges, such as those in healthcare, IoT, and finance, require tailored solutions that address the unique demands of each sector [2].

In summary, future research directions in blockchain scalability include a multitude of focus areas like refining Layer-2 solutions, enhancing off-chain transaction security, fostering Layer-2 interoperability, optimizing rollups, understanding scalability trade-offs, and tackling domain-specific challenges. By focusing on these areas, we can significantly contribute to the evolution of efficient, secure, and flexible blockchain scalability solutions across various domains.

5.2. Regulatory Compliance and Future Challenges in Blockchain Implementation

As blockchain technology matures and increasingly integrates into various sectors, the need for comprehensive legal frameworks and compliance mechanisms becomes more critical. These frameworks are essential to accommodate the decentralized nature of blockchain and ensure its alignment with international standards, such as the General Data Protection Regulation (GDPR). Innovations like Privacy by Blockchain Design advocate for embedding GDPR principles directly into the architecture of blockchain systems, making data protection and privacy fundamental components of technology deployment. This proactive approach aims to address privacy concerns and establish legal certainty within blockchain systems from the outset [74].

5.2.1. Standardization and Interoperability Challenges

One of the significant barriers to widespread blockchain adoption is the lack of universal standards, which affects interoperability between different blockchain systems and existing digital infrastructures. Developing global standards and clear regulatory guidelines is crucial for enabling seamless interactions and data exchanges across different platforms and jurisdictions. In sectors like healthcare and finance, where stringent regulatory compliance is mandatory, specialized standardization efforts are essential to ensure data integrity and confidentiality while maintaining adherence to industry-specific regulations. Fostering standardization can also facilitate broader adoption by enhancing compatibility with existing regulatory frameworks and operational protocols [75].

5.2.2. Navigating Regulatory Complexities

The evolving nature of blockchain introduces novel legal challenges, particularly around the enforcement of smart contracts and the operation of decentralized autonomous organizations (DAOs). These challenges necessitate a collaborative approach to regulatory development, involving regulators, industry stakeholders, and technology experts. Such collaborations are essential for crafting unified regulations that support innovation while safeguarding all parties' interests. Additionally, these cooperative efforts help in understanding and mitigating the risks associated with blockchain, including data privacy concerns, security vulnerabilities, and potential for cyber threats [76].

5.2.3. Future Trends and Recommendations

Looking ahead, the focus on blockchain development is likely to center on enhancing regulatory compliance and promoting standardization across various industries. Expected advancements include the creation of tools and frameworks that facilitate the adoption of blockchain technologies while meeting stringent regulatory standards. Organizations are anticipated to prioritize incremental technological improvements that tackle specific compliance challenges, bolster security features, and refine data privacy measures along with user authentication processes. Moreover, educational initiatives aimed at increasing blockchain literacy are critical for fostering its broader acceptance and effective implementation [75].

Integrating blockchain technology across diverse sectors offers promising opportunities tempered by significant regulatory and compliance challenges. By proactively developing refined regulatory frameworks and compliance mechanisms, and by fostering a thorough understanding of blockchain through educational efforts, industries can leverage the potential of blockchain to drive innovation and operational efficiency. These efforts will ensure that blockchain technology not only meets current regulatory expectations but is also well-equipped to adapt to future legal and compliance challenges [74–76].

6. Conclusions

Through this comprehensive systematic literature review, we have explored the complex landscape of blockchain scalability across key sectors such as finance, healthcare, the Internet of Things, and supply chain management. Our findings highlight the enormous potential of blockchain technology while also underscoring that scalability remains a significant obstacle to its widespread adoption. We have identified key trends in blockchain scalability solutions, including Layer-2 solutions, sharding, optimized consensus algorithms, and rollups. These approaches are effective in addressing issues related to throughput, latency, and storage in blockchain systems, thereby enhancing performance, efficiency, and user experience.

In addition to scalability, we examined critical legal, privacy, and regulatory compliance issues that arise with blockchain implementation across various domains. Our review emphasizes the necessity of robust legal frameworks and compliance mechanisms to ensure that blockchain technology aligns with regulations such as the General Data Protection Regulation (GDPR). Addressing these regulatory challenges is essential for fostering the

adoption and integration of blockchain technology in sectors that handle sensitive data, ensuring both technological advancement and legal adherence.

While our review provides valuable insights, several limitations should be acknowledged. The temporal scope of our study, which includes literature published only up to 31 March 2024, means that more recent advancements and developments might not be covered. Additionally, the selection of keywords and search strings, although designed to be comprehensive, might have resulted in the exclusion of relevant studies that used different terminology. Our focus on specific databases, including Science Direct, Web of Science, IEEE Xplore, PubMed, ACM Digital Library, Springer Link, and Google Scholar, while extensive, might have overlooked pertinent studies available in other databases. Furthermore, the screening and selection process, despite being rigorous, involved subjective judgment, which introduces the potential for bias. Lastly, by concentrating on scalability and regulatory compliance, other important aspects of blockchain technology, such as security, energy consumption, and user adoption, may not have been covered in sufficient depth.

These limitations notwithstanding, our review offers a solid foundation for understanding the current state of blockchain scalability and regulatory compliance. The detailed analysis of challenges and solutions across various industries provides critical insights necessary for developing targeted approaches to overcome existing barriers. We emphasize the importance of continued innovation through collaboration and interdisciplinary research to address these challenges comprehensively.

In conclusion, addressing blockchain scalability and regulatory compliance is crucial for its successful integration into different industries. Future research should focus on creating scalable and compliant blockchain systems tailored to sector-specific needs. This targeted approach will drive broader adoption and maximize blockchain's transformative impact, ultimately fostering a more secure, efficient, and legally compliant technological landscape. Despite the noted limitations, our study contributes significantly to the ongoing discourse on blockchain technology, highlighting the need for ongoing advancements and offering a roadmap for future research in this dynamic field.

Funding: This research was supported by an Australian Government Research Training Program (RTP) scholarship.

Data Availability Statement: No datasets were generated or analyzed during this study. This research is based entirely on publicly available information.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Miao, Y.; Gai, K.; Zhu, L.; Choo, K.K.R.; Vaidya, J. Blockchain-based Shared Data Integrity Auditing and Deduplication. *IEEE Trans. Dependable Secur. Comput.* **2023**, *21*, 3688–3703. [CrossRef]
2. Hisseine, M.A.; Chen, D.; Yang, X. The Application of Blockchain in Social Media: A Systematic Literature Review. *Appl. Sci.* **2022**, *12*, 6567. [CrossRef]
3. Malavolta, G.; Moreno-Sanchez, P.; Schneidewind, C.; Maffei, M. Anonymous Multi-Hop Locks for Blockchain Scalability and Interoperability. In Proceedings of the NDSS Symposium 2019, San Diego, CA, USA, 24–27 February 2019. [CrossRef]
4. Xie, T.; Gai, K.; Zhu, L.; Wang, S.; Zhang, Z. RAC-Chain: An Asynchronous Consensus-based Cross-chain Approach to Scalable Blockchain for Metaverse. *ACM Trans. Multimed. Comput. Commun. Appl.* **2024**, *20*, 1–24. [CrossRef]
5. Moniruzzaman, M.; Khezr, S.; Yassine, A.; Benlamri, R. Blockchain for Smart Homes: Review of Current Trends and Research Challenges. *Comput. Electr. Eng.* **2020**, *83*, 106585. [CrossRef]
6. Sharma, A.; Kaur, S.; Singh, M. A Comprehensive Review on Blockchain and Internet of Things in Healthcare. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4333. [CrossRef]
7. Khan, D.; Jung, L.T.; Hashmani, M.A. Systematic Literature Review of Challenges in Blockchain Scalability. *Appl. Sci.* **2021**, *11*, 9372. [CrossRef]
8. Gai, K.; Guo, J.; Zhu, L.; Yu, S. Blockchain Meets Cloud Computing: A Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2009–2030. [CrossRef]
9. De Filippi, P.; Mannan, M.; Reijers, W. The alegality of blockchain technology. *Policy Soc.* **2022**, *41*, 358–372. [CrossRef]

10. Alfa, A.A.; Alhassan, J.K.; Olaniyi, O.M.; Olalere, M. Blockchain Technology in IoT Systems: Current Trends, Methodology, Problems, Applications, and Future Directions. *J. Reliab. Intell. Environ.* **2021**, *7*, 115–143. [CrossRef]
11. Novo, O. Scalable Access Management in IoT Using Blockchain: A Performance Evaluation. *IEEE Internet Things J.* **2019**, *6*, 4694–4701. [CrossRef]
12. Alrehaili, A.; Namoun, A.; Tufail, A. A Comparative Analysis of Scalability Issues within Blockchain-Based Solutions in the Internet of Things. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*. [CrossRef]
13. Abdelmaboud, A.; Ahmed, A.I.A.; Abaker, M.; Eisa, T.A.E.; Albasheer, H.; Ghorashi, S.A.; Karim, F.K. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. *Electronics* **2022**, *11*, 630. [CrossRef]
14. Ye, C.; Cao, W.; Chen, S. Security Challenges of Blockchain in Internet of Things: Systematic Literature Review. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4177. [CrossRef]
15. Bandara, E.; Liang, X.; Foytik, P.; Shetty, S.; Ranasinghe, N.; De Zoysa, K. Rahasak—Scalable Blockchain Architecture for Enterprise Applications. *J. Syst. Archit.* **2021**, *116*, 102061. [CrossRef]
16. Tandon, A.; Dhir, A.; Islam, N.; Mäntymäki, M. Blockchain in Healthcare: A Systematic Literature Review, Synthesizing Framework and Future Research Agenda. *Comput. Ind.* **2020**, *122*, 103290. [CrossRef]
17. Alghazwi, M.; Turkmen, F.; Velde, J.V.D.; Karastoyanova, D. Blockchain for Genomics: A Systematic Literature Review. *Distrib. Ledger Technol. Res. Pract.* **2022**, *1*, 1–28. [CrossRef]
18. Kumar, S.; Bharti, A.K.; Amin, R. Decentralized Secure Storage of Medical Records Using Blockchain and IPFS: A Comparative Analysis with Future Directions. *Secur. Priv.* **2021**, *4*, e162. [CrossRef]
19. Biswas, S.; Sharif, K.; Li, F.; Nour, B.; Wang, Y. A Scalable Blockchain Framework for Secure Transactions in IoT. *IEEE Internet Things J.* **2019**, *6*, 4650–4659. [CrossRef]
20. Alahmadi, D.H.; Baothman, F.A.; Alrajhi, M.M.; Alshahrani, F.S.; Albalawi, H.Z. Comparative Analysis of Blockchain Technology to Support Digital Transformation in Ports and Shipping. *J. Intell. Syst.* **2021**, *31*, 55–69. [CrossRef]
21. Xia, J.; Li, H.; He, Z. The Effect of Blockchain Technology on Supply Chain Collaboration: A Case Study of Lenovo. *Systems* **2023**, *11*, 299. [CrossRef]
22. Li, W.; Feng, C.; Zhang, L.; Xu, H.; Cao, B.; Imran, M.A. A Scalable Multi-Layer PBFT Consensus for Blockchain. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *32*, 1146–1160. [CrossRef]
23. Arshad, U.; Shah, M.A.; Javaid, N. Futuristic Blockchain Based Scalable and Cost-Effective 5G Vehicular Network Architecture. *Veh. Commun.* **2021**, *31*, 100386. [CrossRef]
24. Marko, V. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In *Open Problems in Network Security*; Springer International Publishing, 2016; pp. 112–125. Available online: https://link.springer.com/chapter/10.1007/978-3-319-39028-4_9 (accessed on 5 June 2024).
25. Nasir, M.H.; Arshad, J.; Khan, M.M.; Fatima, M.; Salah, K.; Jayaraman, R. Scalable Blockchains—A Systematic Review. *Future Gener. Comput. Syst.* **2022**, *126*, 136–162. [CrossRef]
26. Jafar, U.; Aziz, M.J.A.; Shukur, Z.; Hussain, H.A. A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. *Sensors* **2022**, *22*, 7585. [CrossRef]
27. Tyagi, D.; Ghosh, S.; Rana, A.; Kansal, V. A Comparative Analysis of Potential Factors and Impacts that Affect Blockchain Technology in Software-Based Applications. In Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends (SMART), Moradabad, India, 4–5 December 2020; pp. 127–136. [CrossRef]
28. Magazine, T. The Ultimate Election Year: All the Elections Around the World in 2024. Available online: https://time.com/6550920/world-elections-2024/ (accessed on 5 June 2024).
29. Mohammad, A.; Vargas, S. Challenges of Using Blockchain in the Education Sector: A Literature Review. *Appl. Sci.* **2022**, *12*, 6380. [CrossRef]
30. Koshiry, A.E.; Eliwa, E.; El-Hafeez, T.A.; Shams, M.Y. Unlocking the power of blockchain in education: An overview of innovations and outcomes. *Blockchain Res. Appl.* **2023**, *4*, 100165. [CrossRef]
31. Chauhan, A.; Malviya, O.P.; Verma, M.; Mor, T.S. Blockchain and Scalability. In Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018; pp. 122–128. [CrossRef]
32. Statista. Social Media-Statistics & Facts. 2024. Available online: https://www.statista.com/topics/1164/social-networks/#editorsPicks (accessed on 5 June 2024).
33. Gopalan, A.; Sankararaman, A.; Walid, A.; Vishwanath, S. Stability and Scalability of Blockchain Systems. *Proc. ACM Meas. Anal. Comput. Syst.* **2020**, *4*, 1–35. [CrossRef]
34. Sangeeta, N.; Nam, S.Y. Blockchain and Interplanetary File System (IPFS)-Based Data Storage System for Vehicular Networks with Keyword Search Capability. *Electronics* **2023**, *12*, 1545 . [CrossRef]
35. Ali, O.; Ally, M.; Clutterbuck.; Dwivedi, Y. The State of Play of Blockchain Technology in the Financial Services Sector: A Systematic Literature Review. *Int. J. Inf. Manag.* **2020**, *54*, 102199. [CrossRef]
36. Weerawarna, R.; Miah, S.J.; Shao, X. Emerging advances of blockchain technology in finance: a content analysis. *Pers. Ubiquitous Comput.* **2023**, *27*, 1495–1508. [CrossRef]

37. Prados-Castillo, J.F.; Guaita Martínez, J.M.; Zielińska, A.; Gorgues Comas, D. A Review of Blockchain Technology Adoption in the Tourism Industry from a Sustainability Perspective. *J. Theor. Appl. Electron. Commer. Res.* **2023**, *18*, 814–830. [CrossRef]
38. Muharam, I.N.; Tussyadiah, I.P.; Kimbu, A.N. Decentralising Airbnb: Testing the acceptability of blockchain-based sharing economy systems. *Tour. Manag.* **2024**, *102*, 104871. [CrossRef]
39. Sharma, M.; Sehrawat, R.; Daim, T.; Shaygan, A. Technology assessment: Enabling Blockchain in hospitality and tourism sectors. *Technol. Forecast. Soc. Chang.* **2021**, *169*, 120810. [CrossRef]
40. Banerji, D.; Rashideh, W.; Arora, B.; Pratihari, A.R. Application Potential of Blockchain Technologies in the Travel and Tourism Industry. In *Blockchain Applications in IoT Ecosystem*; Choudhury, T., Khanna, A., Toe, T.T., Khurana, M., Gia Nhu, N., Eds.; EAI/Springer Innovations in Communication and Computing; Springer: Cham, Switzerland, 2021. [CrossRef]
41. Dadkhah, M.; Rahimnia, F.; Filimonau, V. Evaluating the opportunities, challenges and risks of applying the blockchain technology in tourism: a Delphi study approach. *J. Hosp. Tour. Technol.* **2022**, *13*, 922–954. [CrossRef]
42. Yeoh, P. Regulatory issues in blockchain technology. *J. Financ. Regul. Compliance* **2017**, *25*, 196–208. [CrossRef]
43. Sharif, M.M.; Ghodoosi, F. The Ethics of Blockchain in Organizations. *J. Bus. Ethics* **2022**, *178*, 1009–1025. [CrossRef]
44. Fabiano, N. Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; pp. 727–734. [CrossRef]
45. Farouk, G.; Alsamara, T. Legal View on Blockchain Technologies in Healthcare: A European States Case Study. *Int. J. Sociotechnology Knowl. Dev.* **2023**, *15*, 1–13. [CrossRef]
46. Saeed, H.; Malik, H.; Bashir, U.; Ahmad, A.; Riaz, S.; Ilyas, M.; Bukhari, W.A.; Khan, M.I.A. Blockchain technology in healthcare: A systematic review. *PLoS ONE* **2022**, *17*, e0266462. [CrossRef]
47. Rubeis, G. Ethical implications of blockchain technology in biomedical research. *Ethik Med.* **2024**. *Forthcoming*. First online: 28 March 2024. [CrossRef]
48. Ma, A. Emerging Legal Issues in Blockchain for Construction Supply Chains. In Proceedings of the 2020 4th International Conference on Vision, Image and Signal Processing (ICVISP), Bangkok, Thailand, 9–11 December 2020; pp. 1–7. Article No. 60. [CrossRef]
49. Agi, M.A.N.; Jha, A.K. Blockchain technology in the supply chain: An integrated theoretical perspective of organizational adoption. *Int. J. Prod. Econ.* **2022**, *247*, 108458. [CrossRef]
50. Kumari, P.; Kumar, R.; Lohan, A.; Patel, N.K.; Jain, P. Designing Supply Chain Management System Using Blockchain: A Review. In Proceedings of the 2023 World Conference on Communication & Computing (WCONF), RAIPUR, India, 14–16 July 2023; pp. 1–6. [CrossRef]
51. Tandon, R.; Verma, A.; Gupta, P.K. Blockchain enabled vehicular networks: A review. In Proceedings of the 2022 5th International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT), Aligarh, India, 26–27 November 2022; pp. 1–6. [CrossRef]
52. Peng, C.; Wu, C.; Gao, L.; Zhang, J.; Yau, K.L.A.; Ji, Y. Blockchain for Vehicular Internet of Things: Recent Advances and Open Issues. *Sensors* **2020**, *20*, 5079. [CrossRef]
53. Hajian Berenjestanaki, M.; Barzegar, H.R.; El Ioini, N.; Pahl, C. Blockchain-Based E-Voting Systems: A Technology Review. *Electronics* **2024**, *13*, 17. [CrossRef]
54. Khudoykulov, Z.; Tojiakbarova, U.; Bozorov, S.; Ourbonalieva, D. Blockchain Based E-Voting System: Open Issues and Challenges. In Proceedings of the 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 3–5 November 2021; pp. 1–5. [CrossRef]
55. Pawlak, M.; Poniszewska-Marańda, A. Trends in blockchain-based electronic voting systems. *Inf. Process. Manag.* **2021**, *58*, 102595. [CrossRef]
56. Park, J. Promises and challenges of Blockchain in education. *Smart Learn. Environ.* **2021**, *8*, 33. [CrossRef]
57. Rani, P.; Sachan, R.K.; Kukreja, S. A systematic study on blockchain technology in education: Initiatives, products, applications, benefits, challenges and research direction. *Computing* **2024**, *106*, 405–447. [CrossRef]
58. Liu, L.; Zhang, W.; Han, C. A survey for the application of blockchain technology in the media. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 3143–3165. [CrossRef]
59. Divyashree, K.S.; Mishra, A. Blockchain Technology in Financial Sector and Its Legal Implications. In *Emerging IT/ICT and AI Technologies Affecting Society*; Chaurasia, M.A., Juang, C.F., Eds.; Lecture Notes in Networks and Systems; Springer: Singapore, 2023; Volume 478. [CrossRef]
60. Pal, A.; Tiwari, C.K.; Behl, A. Blockchain technology in financial services: a comprehensive review of the literature. *J. Glob. Oper. Strateg. Sourc.* **2021**, *14*, 61–80. [CrossRef]
61. Sarnacchiaro, P.; Luongo, S.; Sepe, F.; Corte, V.D. The role of blockchain technology in the tourism industry: analyzing the factors affecting its adoption. *Qual. Quant.* **2024**. *Forthcoming*. [CrossRef]
62. Balasubramanian, S.; Sethi, J.S.; Ajayan, S.; Corte, V.D. An enabling Framework for Blockchain in Tourism. *Inf. Technol. Tour.* **2022**, *24*, 165–179. [CrossRef]
63. Gangwal, A.; Gangavalli, H.R.; Thirupathi, A. A Survey of Layer-Two Blockchain Protocols. *J. Netw. Comput. Appl.* **2023**, *209*, 103539. [CrossRef]

64. Mandal, M.; Chishti, M.S.; Banerjee, A. Investigating Layer-2 Scalability Solutions for Blockchain Applications. In Proceedings of the 2023 IEEE International Conference on High Performance Computing & Communications, Data Science & Systems, Smart City & Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), Melbourne, Australia, 17–21 December 2023; pp. 710–717. [CrossRef]
65. Hussain, M.; Javed, W.; Hakeem, O.; Yousafzai, A.; Younas, A.; Awan, M.J.; Nobanee, H.; Zain, A.M. Blockchain-Based IoT Devices in Supply Chain Management: A Systematic Literature Review. *Sustainability* **2021**, *13*, 13646. [CrossRef]
66. Neiheiser, R.; Raimundo, G.I.; Rech, L.; Montez, C.; Matos, M.; Rodrigues, L. Practical Limitations of Ethereum's Layer-2. *IEEE Access* **2023**, *11*, 8651–8662. [CrossRef]
67. Sanka, A.I.; Cheung, R.C. A Systematic Review of Blockchain Scalability: Issues, Solutions, Analysis and Future Research. *J. Netw. Comput. Appl.* **2021**, *195*, 103232. [CrossRef]
68. Liu, X.; Xie, H.; Yan, Z.; Liang, X. A survey on blockchain sharding. *ISA Trans.* **2023**, *141*, 30–43. [CrossRef] [PubMed]
69. Li, Y.; Wang, J.; Zhang, H. A survey of state-of-the-art sharding blockchains: Models, components, and attack surfaces. *J. Netw. Comput. Appl.* **2023**, *217*, 103686. [CrossRef]
70. Hussein, Z.; Salama, M.A.; El-Rahman, S.A. Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms. *Cybersecurity* **2023**, *6*, 30. [CrossRef]
71. Thibault, L.T.; Sarry, T.; Hafid, A.S. Blockchain Scaling Using Rollups: A Comprehensive Survey. *IEEE Access* **2022**, *10*, 93039–93054. [CrossRef]
72. Lavaur, T.; Detchart, J.; Lacan, J.; Chanel, C.P.C. Modular zk-rollup on-demand. *J. Netw. Comput. Appl.* **2023**, *217*, 103678. [CrossRef]
73. Lavaur, T.; Lacan, J.; Chanel, C.P.C. Enabling Blockchain Services for IoE with Zk-Rollups. *Sensors* **2022**, *22*, 6493. [CrossRef]
74. König, L.; Korobeinikova, Y.; Tjoa, S.; Kieseberg, P. Comparing Blockchain Standards and Recommendations. *Future Internet* **2020**, *12*, 222. [CrossRef]
75. Alam, S.; Shuaib, M.; Khan, W.Z.; Garg, S.; Kaddoum, G.; Hossain, M.S.; Zikria, Y.B. Blockchain-based Initiatives: Current state and challenges. *Comput. Netw.* **2021**, *198*, 108395. [CrossRef]
76. Al-Jaroodi, J.; Mohamed, N. Blockchain in Industries: A Survey. *IEEE Access* **2019**, *7*, 36500–36515. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.