applied sciences

MDPI

Review

Security Challenges and Performance Trade-Offs in On-Chain and Off-Chain Blockchain Storage: A Comprehensive Review

Haluk Eren [1], Özgür Karaduman [2,*] and Muharrem Tuncay Gençoğlu [3]

[1] Department of Air Traffic Control, School of Civil Aviation, Fırat University, Elazig 23200, Türkiye; heren@firat.edu.tr
[2] Department of Software Engineering, Faculty of Engineering, Fırat University, Elazig 23119, Türkiye
[3] Department of Machine Program, Vocational School of Technical Sciences, Fırat University, Elazig 23119, Türkiye; mt.gencoglu@firat.edu.tr
* Correspondence: okaraduman@firat.edu.tr

Abstract: Blockchain-based data storage methods offer strong data integrity, decentralized security, and transparent access control but also face scalability challenges, high computational costs, and complex data management. This study provides a comprehensive review of on-chain, off-chain, and hybrid storage architectures, analyzing their security vulnerabilities, performance trade-offs, and industry-specific applications. On-chain data storage ensures immutability, data integrity, and high security by storing data directly on the blockchain; however, it is associated with high transaction costs and scalability limitations. In contrast, off-chain solutions reduce costs and enhance performance by storing data outside the blockchain but introduce risks related to data integrity and access security in decentralized environments. Hybrid approaches aim to balance security, cost, and scalability by integrating the strengths of both on-chain and off-chain solutions. This study examines the fundamental components of blockchain-based data storage systems, their sector-specific applications, and the technical challenges they present. Additionally, it explores the trade-offs between security, cost, and decentralization, offering insights into blockchain storage optimization strategies. As a result, this study evaluates the optimization of security protocols, the efficiency of hybrid systems, and the sustainability of distributed storage solutions, contributing to future research in this field.

Keywords: blockchain; data storage; on-chain storage; off-chain storage; hybrid storage; cloud storage; data security; decentralized authentication; access control; scalability; edge computing

Academic Editors: Hajar Moudoud and Zakaria Abou El Houda

Received: 14 February 2025
Revised: 12 March 2025
Accepted: 14 March 2025
Published: 15 March 2025

Citation: Eren, H.; Karaduman, Ö.; Gençoğlu, M.T. Security Challenges and Performance Trade-Offs in On-Chain and Off-Chain Blockchain Storage: A Comprehensive Review. *Appl. Sci.* **2025**, *15*, 3225. https://doi.org/10.3390/app15063225

1. Introduction

Blockchain technology has transformed industries by enhancing data security and management [1–3]. Rapidly adopted in sectors such as finance, healthcare, education, and logistics, this technology enhances transparency, security, and efficiency in data storage and sharing processes [4–7]. The immutability feature of blockchain ensures the secure storage and traceability of sensitive information, while its decentralized architecture preserves data integrity and strengthens access control mechanisms [8,9].

Blockchain-based data storage methods provide innovative solutions to the challenges faced by various industries concerning security, scalability, and cost efficiency [10–12]. Issues such as security vulnerabilities in centralized systems, high transaction costs, and data privacy concerns can be mitigated through blockchain's distributed and secure framework [13]. Additionally, emerging blockchain security solutions such as Zero-Knowledge

Proofs (ZKP) and Fully Homomorphic Encryption (FHE) are being widely studied to ensure both privacy and computational efficiency [14]. However, a critical trade-off between performance and security arises when choosing between on-chain and off-chain storage methods [15,16]. Therefore, understanding the advantages and limitations of different blockchain-based storage solutions has become a critical necessity for system designers. To address the scalability limitations of blockchain, Layer-2 solutions have become increasingly essential. These advanced frameworks improve network efficiency by optimizing data flow and enhancing overall performance [17–20].

Recent research has explored data compression and encryption methods for enhancing blockchain storage security. For example, the use of Discrete Cosine Transform (DCT) compression and nonlinear dynamics provides high-quality reconstruction mechanisms, ensuring data privacy while minimizing storage overhead [7].

However, blockchain-based data storage systems face challenges not only in terms of scalability but also in terms of security and cost. In this context, systematically reviewing different blockchain-based storage approaches is crucial for understanding the future direction of this field.

This study is a comprehensive review of blockchain-based data storage methods and provides an in-depth examination and classification of existing approaches, highlights their advantages and limitations, and identifies potential research gaps. Blockchain-based data storage methods present significant opportunities and challenges in terms of security, scalability, and cost. However, balancing the trade-offs between different approaches remains an open research question. By synthesizing blockchain storage approaches, this work contributes to a deeper understanding of the existing literature and highlights key areas that require further research.

1.1. On-Chain and Off-Chain Data Storage Paradigms

Data storage capacity and performance in blockchain systems depend on the chosen storage methods [1,2]. On-chain storage ensures immutability and reliability by storing data directly on the blockchain; however, due to high transaction costs and scalability limitations, it is not suitable for large datasets [17,18,21,22]. Off-chain storage, on the other hand, offers cost and performance advantages by keeping data outside the blockchain but introduces risks related to data integrity and access control [12,15]. Hybrid approaches integrate both on-chain and off-chain solutions to establish a balanced model that optimizes security, cost, and scalability [6,16,23–37].

1.2. The Role of Blockchain Technology in Secure Data Management of Data Storage

With the acceleration of digitalization, data security has become a critical concern for many industries [3]. Data stored in centralized systems is vulnerable to cyberattacks and security breaches [14]. Blockchain's distributed nature ensures secure and traceable data sharing while maintaining privacy and security [5,38,39]. In particular, access control models such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are widely implemented in blockchain-based systems to enforce access policies. Data encryption, access control, and integrity verification improve blockchain reliability and require industry-specific solutions [16,40–44].

1.3. Objectives and Structure of the Study

This study presents a comparative analysis of on-chain, off-chain, and hybrid data storage methods from a security perspective [12,16,37]. First, the advantages and limitations of these methods are analyzed, followed by an evaluation of their contributions to data security, access control, and authentication [15,45,46]. Additionally, hybrid approaches and their impact on scalability, cost, and performance are examined, along with an assessment

of their applicability across different industries [18,22,47]. Finally, the potential benefits of blockchain-based data storage methods in sectors such as healthcare, finance, and education are discussed, and sector-specific recommendations are provided [7,43,48–52].

1.4. Contributions

This study provides a comprehensive evaluation of blockchain-based data storage methods, addressing critical challenges related to security, scalability, and cost efficiency. By systematically comparing on-chain, off-chain, and hybrid approaches, this work highlights their applicability in various industry domains and security-sensitive environments. The following are the key contributions of this study:

- *Comparative Analysis of Blockchain Data Storage Methods*: On-chain, off-chain, and hybrid data storage methods have been systematically compared in terms of security, cost, scalability, and performance. This comparative framework provides an in-depth analysis of security trade-offs, filling a critical gap in the literature. Additionally, the study offers insights into the scalability and cost efficiency challenges in blockchain storage solutions.
- *Security, Performance, and Industry-Specific Applicability of Hybrid Approaches*: Hybrid storage solutions, combining the strengths of on-chain and off-chain methods, have been analyzed in detail regarding their security, performance, and cost implications. Their applicability in high-security and flexible environments, such as healthcare, finance, and the Internet of Things (IoT) industries, has been specifically examined.
- *Comparative Analysis of Cryptographic Security Mechanisms and Guidelines for Blockchain Integration*: Blockchain storage methods are evaluated based on encryption, access control, and data integrity. This study explores how hashing mechanisms ensure data integrity and how access control models (e.g., RBAC, ABAC) mitigate security vulnerabilities in sector-specific applications. It also examines the role of Zero-Knowledge Proofs (ZKP) and Homomorphic Encryption in enhancing blockchain-based storage security. Furthermore, blockchain-integrated solutions like IPFS, Swarm, and Blockweave are analyzed for their security and scalability. This work provides a novel perspective on addressing data security and efficiency challenges in blockchain storage.
- *Methodological Recommendations for Sector-Specific Security Requirements*: The applicability of blockchain storage solutions across various industries has been analyzed by considering the security and scalability requirements of different sectors. The study identifies the appropriate selection criteria for on-chain, off-chain, and hybrid storage solutions based on sector-specific constraints. Additionally, the integration of authentication, access control, and encryption techniques with blockchain has been systematically evaluated.
- *Analysis of Decentralized Blockchain-Based Data Storage Systems*: The technical infrastructure, use cases, and security mechanisms of decentralized blockchain-based data storage projects, including Filecoin, Arweave, Swarm, Sia, Ankr, and Storj, have been compared in detail. Their advantages in terms of data integrity, access control, and scalability have been thoroughly examined.
- *Systematic Classification of Blockchain Data Storage Methods*: This study presents a structured classification framework that evaluates the advantages, disadvantages, and industry-specific use cases of on-chain, off-chain, and hybrid storage models. By utilizing visualization tools such as tables and diagrams, the relationships between different storage methods and their implications for security and performance are clearly demonstrated. This framework serves as a valuable reference for academic research and contributes to existing literature on blockchain storage methodologies.

- *Future Perspectives on Blockchain-Based Data Storage Solutions*: The study provides a comprehensive assessment of the limitations of current blockchain-based data storage solutions and explores potential future advancements in the field. Scenarios in which hybrid storage solutions could gain broader adoption are discussed, along with strategies for optimizing security, scalability, and cost efficiency. This study provides a theoretical and practical basis for future blockchain storage research.

1.5. Methodology

This study systematically examines blockchain-based data storage methods by evaluating their security, scalability, and performance aspects. The study focuses on on-chain, off-chain, and hybrid approaches, analyzing their strengths and weaknesses according to basic criteria. The methodology consists of the following basic stages:

1. *Selection of Literature and Data Sources*: The literature review used leading scientific databases such as IEEE Xplore, Elsevier ScienceDirect, MDPI, Wiley, Taylor & Francis, and Springer. However, no particular publisher was given priority, and the selection was made based on the content compatibility, contribution to the subject, and up-to-dateness of the studies.
2. *Publication Year Criteria*: Instead of setting a specific year range in the selection of articles, emphasis was placed on recent studies, but basic studies on the subject were also included. In this way, articles considered basic in the literature were also evaluated along with current research trends. In the review process, studies that would provide a comparative evaluation of blockchain data storage solutions in terms of security, scalability, and cost were particularly preferred. In order for the selected references to represent our research scope, it was taken into consideration that they included experimental studies, theoretical frameworks and case studies on different data storage methods.
3. *Search Method*: The literature review process has been carried out with keyword-based searches and key terms such as "blockchain storage", "on-chain vs. off-chain", "hybrid blockchain models", "Layer-2 scalability", "blockchain data security", "distributed ledger storage models", "blockchain cryptographic techniques", and "blockchain storage in healthcare and finance" have been used. These keywords provided focus on the subject and allowed the inclusion of new trends in the literature.
4. *Comparative Analysis of On-chain and Off-chain Methods*: To establish a solid foundation for the study, a conceptual analysis of on-chain and off-chain storage methods has been conducted in the initial phase. This comparative assessment has facilitated a deeper understanding of the trade-offs involved in different data storage approaches. The study begins with a detailed analysis of on-chain and off-chain data storage methods:
    - The advantages and disadvantages of both methods have been identified and analyzed based on performance, cost, scalability, and data security;
    - These insights have contributed to a clearer evaluation of their suitability for different use cases, ultimately supporting the examination of hybrid solutions.
5. *Security Assessment in Blockchain Data Storage Systems*: In this study, various security-related parameters have been systematically examined to assess their implications for blockchain data storage. This evaluation includes the following:
    - Symmetric and asymmetric encryption techniques and their impact on data privacy;
    - RBAC and ABAC access control models, comparing their suitability for various applications;
    - Hash-based data integrity mechanisms and their effectiveness in preventing security vulnerabilities.

6. *Sectoral Applications of Blockchain Storage Solutions*: In the later stages of the study, the sectoral applicability of blockchain storage solutions has been analyzed. Given the increasing adoption of blockchain technology across different industries, the study particularly evaluates the following:
   - The use of on-chain, off-chain, and hybrid solutions in key sectors, including healthcare, finance, education, and public administration;
   - The potential of hybrid approaches in optimizing the balance between security and performance, ensuring practical applicability in real-world scenarios.
7. *Performance Metrics and Layer-2 Solutions*: To address scalability concerns, Layer-2 solutions have been analyzed as an alternative to enhance blockchain efficiency. Specifically, the study has examined the following:
   - Transaction speed, evaluating the processing efficiency of different storage approaches;
   - Storage cost, comparing economic feasibility across on-chain, off-chain, and hybrid methods.

By evaluating these performance metrics, the study provides insights into how various blockchain storage models impact real-world implementations.

8. *Systematic Presentation of Findings*: To ensure clarity and accessibility, the findings of the study have been systematically visualized using tables and diagrams.
   - On-chain, off-chain, and hybrid storage methods have been comprehensively compared in terms of security, scalability, and cost efficiency.
   - The comparative analysis has been structured to highlight key advantages and limitations of each approach, supporting future research directions in blockchain-based storage.

2. Blockchain-Based Data Storage Methods: On-Chain, Off-Chain, and Hybrid Approaches

Blockchain-based data storage methods offer various approaches to ensure secure, transparent, and sustainable data storage [12,15]. These methods vary between storing data directly on the blockchain, storing it off-chain, or adopting hybrid approaches that combine the advantages of both [16,37]. The distinct advantages and disadvantages of on-chain and off-chain methods are particularly critical in domains such as healthcare, where the secure storage of sensitive data are essential [39,46]. These approaches are detailed in Figure 1, followed by an in-depth analysis of the operational mechanisms, advantages, and challenges associated with different blockchain-based data storage methods.

2.1. On-Chain Data Storage Methods

A blockchain is a data structure composed of blocks that are chronologically and cryptographically linked. Each block contains transactions occurring on the network along with relevant metadata. This structure ensures immutability, transparency, and verifiability, enabling secure data storage on the blockchain [21]. The structure of a block is illustrated in Figure 2. Each blockchain block consists of three main components:

- *Block Header*: Contains the unique hash value that identifies the block and maintains the integrity of the chain by referencing the previous block's hash. The timestamp records the time the block was created, while the Merkle root serves as a cryptographic summary that ensures the integrity of all transactions within the block;
- *Transaction Data*: Represents the primary data component stored within the block, including sender and receiver addresses, transaction amounts, and additional metadata.

Transactions are structured in a Merkle tree, allowing them to be efficiently hashed and verified;

- *Block Metadata*: Includes the nonce value, which is used in the Proof-of-Work (PoW) mechanism to find the correct hash, and the block size, which defines the total amount of data stored within the block.

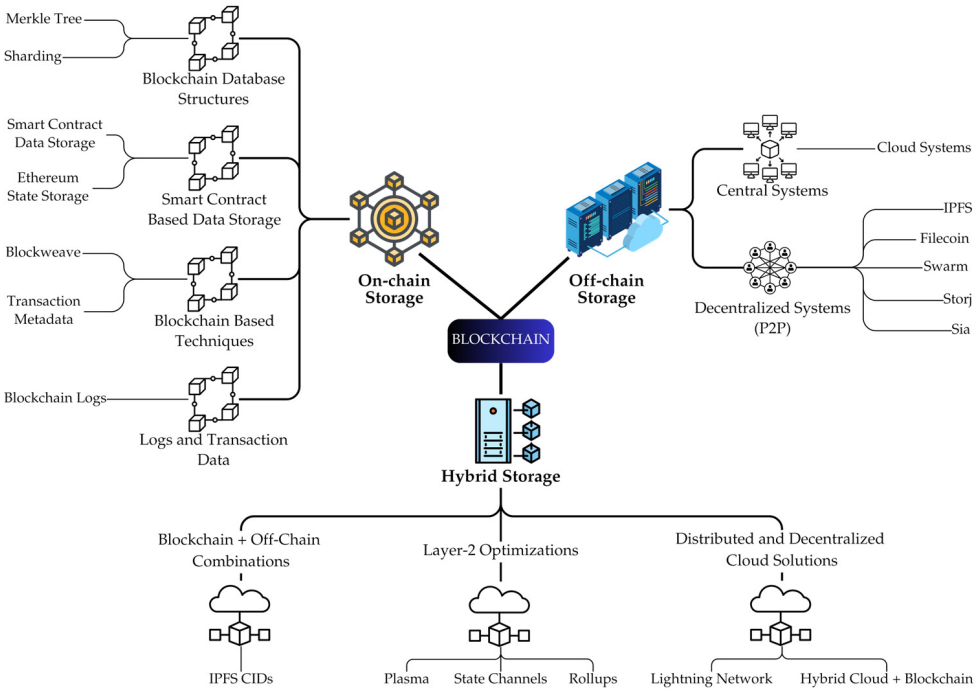

Figure 1. Blockchain-based data storage models: On-chain (all data stored on the blockchain), Off-chain (data stored externally with only references or hashes on-chain), and Hybrid (critical data on-chain, larger datasets off-chain).

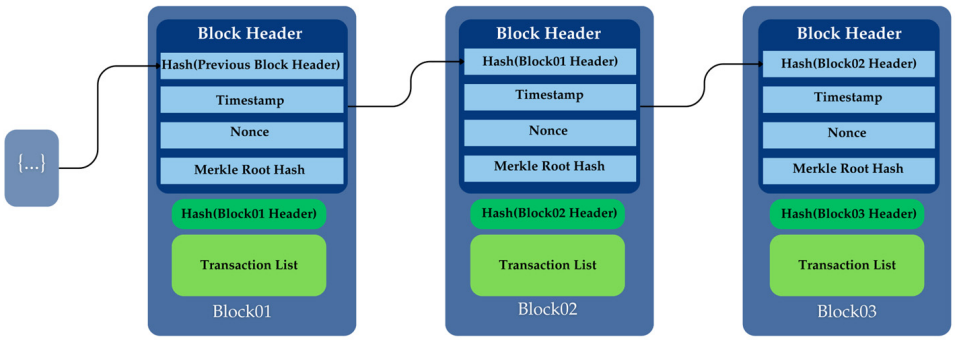

Figure 2. Blockchain block structure for on-chain data storage. Each block comprises a header (hash linking to the previous block for integrity), transaction data (records all transactions), and metadata (includes nonce and Merkle root for consensus and verification).

Data storage on the blockchain is achieved by maintaining information in a structured and encrypted format within blocks. This structure not only preserves data integrity but also guarantees decentralization [1,53]. Merkle trees facilitate the verification of stored data, while each node retains a copy of the block data, thereby enhancing network security [45,54]. However, on-chain data storage presents scalability challenges when dealing with large datasets. Since all network nodes are required to store a full copy of the blockchain, storage demands continuously increase, potentially impacting transaction processing times [18,47].

On-chain data storage offers security, immutability, and transparency by recording data directly on the blockchain [12,37]. Since blockchain-stored data is verifiable and

tamper-proof across the entire network, it provides a significant security advantage, particularly for sensitive data storage in sectors such as healthcare [55]. Due to its decentralized architecture, data are more resistant to attacks targeting centralized servers [39,48]. Furthermore, all transactions are cryptographically signed and distributed across all nodes in the blockchain, which ensures data integrity and prevents unauthorized access [1,46,56]. However, on-chain data storage methods come with several critical limitations. Firstly, storing data directly on the blockchain is highly costly, as each transaction must be propagated across the network and requires transaction fees paid to miners [57–59]. Additionally, recording large datasets on the blockchain increases network load, leading to longer transaction processing times and a reduction in overall efficiency [47,54]. As the blockchain expands, every node must store a complete copy of the ledger, thereby escalating storage requirements and limiting scalability [18,47].

Considering these advantages and challenges, while data storage methods on the blockchain provide high security and immutability, they have significant limitations in terms of cost and scalability. Alternative approaches such as off-chain and hybrid solutions have been developed to address these disadvantages, especially when it comes to large datasets.

Besides the mentioned advantages and disadvantages of storing data on the blockchain, on-chain methods are implemented with various mechanisms that increase the performance, security and scalability of the blockchain network. Table 1 provides a detailed classification and examples of these mechanisms.

Table 1. This table summarizes on-chain data storage mechanisms, detailing their descriptions, advantages, disadvantages, and real-world applications in blockchain systems. It highlights key storage structures and techniques for secure and efficient data management.

Data Storage Environment	Storage Mechanism	Description	Advantages	Disadvantages	Examples
Blockchain Database Structures	Merkle Tree [21]	Hash-based tree structure used for data verification in Blockchain.	Data integrity and ease of verification.	Scalability is limited.	Bitcoin, Ethereum
	Sharding [17,18,22]	A scalability method where data are distributed across different nodes	High performance and network capacity	Technical complexity	Ethereum 2.0, Zilliqa, Polkadot, Harmony, Elrond, Solana, Near Protocol
Smart Contract Based Data Storage	Smart Contract Data Storage [60,61]	Data storage in smart contracts	Direct access and flexibility	Direct access and flexibility	NFT metadata, ERC-20 token data
	Ethereum State Storage [62,63]	State of accounts and contracts on Ethereum	Fast access and constant updates	Blockchain may become state bloat	Ethereum, Polygon, Algorand, Solana, Sonic, Avax, Bsc
Blockchain Based Techniques	Blockweave [64–66]	Blockchain structure optimized for permanent data storage	Long-term data retention, immutability	Data cannot be updated and can be costly	Arweave.
	Transaction Metadata [67–70]	Additional information and hash data associated with the transaction	Small size additional data storage	Not suitable for big data	OP_RETURN (Bitcoin), Input Data (Etherium)

Table 1. *Cont.*

Data Storage Environment	Storage Mechanism	Description	Advantages	Disadvantages	Examples
Logs and Transaction Data	Blockchain Logs [71–73]	Maintaining transaction history and event records	Transparency and transaction traceability	Scalability issues in big data	Ethereum event logs

2.1.1. Blockchain Database Structures

Blockchain ensures secure data storage by providing a decentralized and immutable structure. Two fundamental techniques that optimize on-chain data management are Merkle Trees and Sharding:

- *Merkle Tree*: A hash-based structure used to verify the integrity of transaction data. It is widely utilized in blockchain networks such as Bitcoin [21] and Ethereum [74] to enable fast and reliable transaction verification. While Merkle trees ensure data integrity, they have limitations when handling complex data structures. Besides maintaining data integrity, enhancing blockchain scalability is equally critical.
- *Sharding*: A technique that partitions blockchain data into smaller fragments, reducing network load and improving transaction throughput. This approach is particularly advantageous for high-transaction-volume networks, as it enables parallel processing across shards. While sharding enhances scalability, it also requires additional security measures to prevent data vulnerabilities [17,18,22].

These two fundamental techniques form the backbone of blockchain-based data management. However, blockchain technology extends beyond database structures. Smart contracts play a crucial role in making data storage processes more flexible and user-friendly, further enriching blockchain-based data management.

2.1.2. Smart Contract Based Data Storage

Smart contracts are self-executing code segments that operate on the blockchain and are triggered when predefined conditions are met. This mechanism enables secure and decentralized data storage and management. Smart contract-based storage methods are particularly suitable for managing small datasets on-chain.

- *Smart Contract Data Storage*: Stores small-sized data directly on the blockchain and is commonly used for NFT metadata, ERC-20 token information, and similar applications. While it provides security and decentralization, it incurs high transaction costs and is not suitable for large-scale data storage [60,61].
- *Ethereum State Storage*: Essential for managing dynamic data in DeFi applications. It enables fast access but can lead to blockchain bloat over time, affecting long-term scalability [62,63].

Apart from smart contracts and database structures, blockchain technology also integrates persistent data storage and transaction-related metadata management. These techniques enhance blockchain functionality and accommodate various application scenarios.

2.1.3. Blockchain Based Techniques

Blockchain-based techniques have been developed to ensure permanent, secure, and efficient data storage on-chain. These techniques introduce innovative solutions to enhance the functionality of blockchain networks:

- *Blockweave*: A blockchain structure developed by the Arweave platform, designed for long-term data storage. It enables low-cost permanent data storage, but data cannot be modified, and storage costs remain relatively high [64–66]. In addition to permanent

data storage, the use of transaction-related metadata in blockchain improves data management and provides supplementary on-chain information.

- *Transaction Metadata*: Used to store additional information related to transactions. In Bitcoin, the OP_RETURN field is a widely adopted method for storing small-sized data. While it enhances verifiability, it is not suitable for large-scale data storage [67–70].

In addition to how blockchain-based techniques store data, the traceability and transparency of on-chain transactions are equally significant. In this context, logs and transaction data play a crucial role in ensuring auditability and system integrity.

2.1.4. Logs and Transaction Data

Blockchain logs record the history of all transactions occurring on the network, as well as events triggered by smart contracts. These logs not only reinforce the transparency and traceability of blockchain but also serve as a critical source of information for network participants.

- *Blockchain Logs*: Used as event logs in networks like Ethereum, they record smart contract events, providing transparency and traceability for decentralized applications (DApps). They enhance usability in DApp development and facilitate debugging for developers. However, scalability challenges may arise when dealing with large datasets [71–73].

2.2. Off-Chain Data Storage Methods

Off-chain data storage refers to the practice of storing data outside the blockchain infrastructure while keeping only data references or cryptographic hashes on-chain. In this approach, the actual data are stored in external systems that offer greater storage capacity and reduced costs [75,76]. This method addresses blockchain scalability and cost concerns, making it a practical solution for handling large datasets while reducing network transaction load [22,37]. However, storing data off-chain introduces certain security and data continuity risks [15,46]. Off-chain storage systems can be designed using either centralized or decentralized infrastructures, providing a critical perspective on the advantages and limitations of different storage environments [12,47]. Off-chain storage methods can be broadly classified into centralized systems (cloud-based storage) and decentralized systems (P2P-based storage), each offering unique advantages and trade-offs [42,43]. Off-chain data storage methods are shown in Figure 3.

- *Centralized Storage Systems*: These involve storing data in large data centers, typically managed by commercial providers such as Amazon Web Services (AWS), Google Cloud Platform, or Microsoft Azure [42,43]. Centralized storage solutions offer high-speed access, reliability, and extensive service options. However, dependence on a central authority can limit data control, creating a single point of failure, which raises concerns about data security and continuity [15,46].
- *Decentralized Storage Systems*: Aligned with blockchain's decentralization principle, these systems store data distributed across multiple nodes. P2P-based storage operates on a network where data are shared among users and is commonly represented by technologies such as IPFS [77,78], Swarm, Storj [79], and Sia [80]. These solutions eliminate reliance on centralized servers, offering benefits such as lower costs and enhanced security. However, factors like data persistence and network performance depend on active user participation, making long-term sustainability a key consideration.

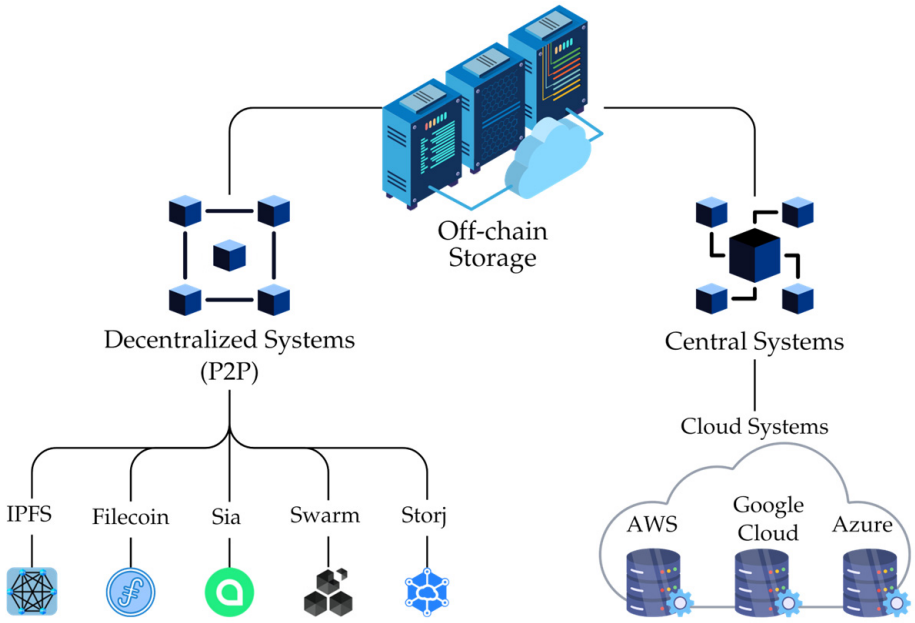

Figure 3. Off-chain data storage methods. Off-chain storage keeps data outside the blockchain while ensuring security and verifiability through cryptographic techniques. Methods include decentralized networks like IPFS, Arweave, and Filecoin, as well as blockchain-integrated cloud solutions. Transactions reference off-chain data via cryptographic hashes or smart contracts, preserving integrity and optimizing efficiency.

Off-chain data storage reduces blockchain transaction loads, creating a more scalable and cost-effective infrastructure. However, storing data outside the blockchain introduces security vulnerabilities. These risks can be mitigated through cryptographic techniques such as hashing and encryption. Storing only hash values on-chain while keeping encrypted data in external storage enhances security and ensures data integrity [8,38]. Large datasets used in various industries, such as healthcare, can be securely and efficiently stored using off-chain solutions. For example, IPFS-based architectures provide a secure and efficient mechanism for storing large-scale digital health records. This approach expands the system's capabilities while preserving data protection [10,81]. Table 2 presents a detailed classification of off-chain storage methods, highlighting their advantages, disadvantages, and real-world applications.

Table 2. The table classifies off-chain data storage methods in blockchain technologies, distinguishing between centralized and decentralized (P2P) systems. It outlines their mechanisms, advantages, disadvantages, and real-world applications, addressing scalability, cost, and accessibility challenges.

Data Storage Environment	Storage Mechanism	Description	Advantages	Disadvantages	Examples
Centralized Data Storage Systems	Cloud storage systems [82–85]	Data are stored in central data centers	Fast access, high performance. Reliability and scalability. Easy integration, wide range of services	Dependency on central authority, high cost. Data security depends on an external provider. Risk of single point of failure due to centralized structure.	Amazon Web Services, Google Cloud Platform, Azure Storage.

Table 2. *Cont.*

Data Storage Environment	Storage Mechanism	Description	Advantages	Disadvantages	Examples
Decentralized Systems **(P2P)**	IPFS [78,86]	Content-based data storage system in a distributed network	Decentralized, low cost	Data continuity depends on user participation.	IPFS
	Filecoin [75,76]	Blockchain-based data storage and incentive mechanism built on IPFS	Strong data continuity with incentive model	High transaction costs	Filecoin
	Swarm [87]	Ethereum-based P2P data storage protocol	Flexible and compatible with Ethereum	Performance limitations may exist	Swarm protocol
	Storj [79]	Blockchain integrated P2P storage solution.	Strong security and incentive model	Difficulty in coordination between users	Storj network
	Sia [80]	Blockchain-based P2P data storage platform.	Low cost, supports data encryption	The scalability of the marketplace may be limited	Siacoin

2.2.1. Centralized Data Storage Systems

Centralized systems refer to data storage methods where information is maintained on traditional servers and cloud infrastructures. These systems offer high availability, reliability, and scalability. However, their primary drawback is dependence on a central authority.

- *Cloud Storage Systems*: Cloud systems facilitate the storage of data in large-scale data centers, typically managed by a centralized authority. Leading cloud providers such as Amazon Web Services (AWS), Google Cloud Platform, and Microsoft Azure are key examples of this infrastructure. These systems provide fast access, high performance, and seamless integration with a broad range of services. They excel in reliability and scalability. However, dependence on a central entity limits data control, leading to higher costs and external security risks. Additionally, a centralized structure introduces a single point of failure, posing a risk to data continuity and security [82].

Despite the advantages of centralized systems, blockchain technology, which is built on the principle of decentralization, is shifting toward distributed data storage solutions to ensure enhanced security, transparency, and autonomy.

2.2.2. Decentralized Systems (P2P)

Decentralized systems align with the core philosophy of blockchain technology by ensuring that data are stored across multiple nodes rather than relying on a central authority. These peer-to-peer (P2P)-based systems eliminate dependency on a centralized entity and enhance data security through user participation.

- *Off-chain Data Storage with IPFS*: The InterPlanetary File System (IPFS) is a content-addressable data storage protocol that operates on a decentralized network. Data are addressed based on its content and is shared across all nodes in the network. It provides a low-cost and secure data storage solution. However, data availability depends on the active participation of network users. More specifically, IPFS offers a decentralized file storage system that addresses blockchain scalability challenges. Storing large datasets directly on-chain is often costly and inefficient. To mitigate this issue, IPFS enables off-chain storage by maintaining data separately from the

blockchain while storing only hash values on-chain. This approach ensures data integrity while significantly reducing storage costs [10,48,78].

Figure 4 illustrates the working mechanism of IPFS. Each data fragment is assigned a unique cryptographic hash, which is used to retrieve the data. This mechanism guarantees data authenticity and immutability while allowing for transparent and verifiable data access. Unlike traditional centralized storage solutions, IPFS distributes data across multiple nodes, ensuring persistent accessibility without reliance on a single server [10,78]. IPFS has significant applications in industries handling sensitive data, such as healthcare. Specifically, it enhances security, privacy, and traceability of patient records. In blockchain-integrated IPFS, data are fragmented and encrypted, providing higher levels of security and confidentiality. This structure not only protects sensitive healthcare data but also offers a robust defense against potential data breaches [48]. Additionally, IPFS's cost-efficient model enables the affordable storage of large datasets, making it a viable solution for industries requiring secure and scalable data management.

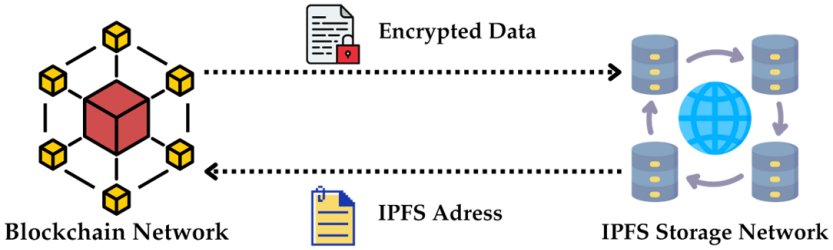

Figure 4. Blockchain network interaction with IPFS network [10,78]. Encrypted data are stored off-chain via IPFS, with its content identifier recorded on-chain. This ensures data integrity and verifiability while reducing on-chain storage overhead. Encryption is applied before IPFS storage for confidentiality, and the blockchain records the reference for secure retrieval.

- *Off-chain Data Storage with Filecoin*: Filecoin is a blockchain-based storage solution that utilizes the IPFS infrastructure to facilitate off-chain data storage. In this system, data contracts are stored on the blockchain, while the actual data are distributed across the IPFS network. Filecoin offers a decentralized architecture while ensuring verifiability of stored data. However, high transaction costs remain a limitation, as users must pay fees for data storage operations on the network.
- *Off-chain Data Storage with Swarm*: Swarm is an Ethereum-based P2P data storage protocol designed to store large datasets off-chain in a decentralized manner. It fragments and distributes data across network nodes, ensuring security and scalability. Fully integrated with the Ethereum ecosystem, Swarm enables secure storage of large files, while encryption mechanisms protect data confidentiality. It provides ease of access and flexibility, although performance limitations may arise due to network constraints [87].
- *Off-chain Data Storage with Storj*: Storj is a P2P-based decentralized cloud storage solution that allows users to rent out unused storage space, contributing to the network. Data are encrypted, fragmented into smaller pieces, and distributed across multiple nodes, minimizing the risk of data loss. With a strong security infrastructure, Storj ensures data traceability and verifiability through blockchain integration. However, coordination challenges among network participants may arise [88].
- *Off-chain Data Storage with Sia*: Sia is a blockchain-based data storage platform that enables users to rent storage space via a decentralized marketplace. It offers a low-cost, encryption-supported model that enhances data security. Data are sharded into smaller fragments and stored across multiple providers, with access restricted to the user's private key. Additionally, smart contracts facilitate secure agreements between storage

providers and users. However, compared to traditional cloud storage solutions, Sia presents scalability and usability challenges [80].

2.3. Hybrid Storage Approaches

Hybrid storage solutions, which integrate on-chain and off-chain approaches, provide a balanced trade-off between security and performance. In this model, small and critical data are stored on the blockchain, while large datasets are maintained in external storage solutions. This approach reduces costs and improves system performance, while preserving the security advantages of blockchain [89,90]. By storing large datasets off-chain and keeping only verification hash values on-chain, hybrid storage optimizes cost efficiency and system scalability [91]. In sectors like healthcare, hybrid solutions help preserve data privacy while reducing costs and enhancing performance. For instance, large-scale electronic health records can be securely stored in off-chain storage infrastructures [13].

Hybrid storage combines blockchain and off-chain systems, balancing security, scalability, and cost [16,37]. These methods retain blockchain's immutability and security while leveraging the flexibility and expanded storage capacity of external systems [46,48]. Hybrid storage works by storing a portion of the data on-chain (e.g., references or cryptographic hashes) and the remaining data in external platforms (e.g., cloud storage or P2P networks) [15,47]. This approach is particularly effective for managing large datasets and reducing storage costs. By integrating the security of decentralized networks with the high scalability of external storage solutions, hybrid storage creates a versatile framework for various industries [42,43]. This model enhances data integrity, accessibility, and performance, making it an efficient and adaptable storage solution for blockchain-based applications. Table 3 presents the classification of hybrid data storage solutions for blockchain technologies.

Table 3. This table categorizes hybrid storage solutions combining blockchain with off-chain methods, decentralized cloud, and Layer-2 scaling. These approaches optimize security, cost, and scalability through on-chain and off-chain strategies, leveraging IPFS CIDs, hybrid clouds, rollups, and state channels for efficient data management.

Data Storage Environment	Storage Mechanism	Implementation Strategy	Advantages	Disadvantages	Examples
Blockchain + Off-chain Integrations	IPFS CIDs [15,92]	Reference information on the blockchain for off-chain data	Verifiability of data	The data itself is not stored on the blockchain	IPFS integrations
Distributed and Decentralized Cloud Solutions	Hybrid Cloud + Blockchain [42,93]	Integrated use of cloud infrastructures and blockchain	High scalability, low cost	Security may depend on external providers	Ankr, Ocean Protocol
	Lightning Network [94]	Channel-based transactions, results integration with blockchain	Fast transactions, low costs.	Only suitable for micro transactions	Bitcoin Lightning Network
Layer-2 Optimizations	Rollups [19,20]	Processing transactions at Layer-2 and saving summary data at Layer-1	High scalability	Technical complexity	Arbitrum, zkSync
	Plasma [52,95]	Processing data on subchains and recording digests to the main blockchain	A reliable Layer-2 solution	Coordination between sub-chains can be difficult	OMG Network
	State Channels [96,97]	Off-chain transactions are on the summary blockchain only	Very low latency	Complicated installation	Lightning Network

2.3.1. Blockchain and Off-Chain Integration Approaches

This storage method enables the integration of smart contracts and transaction records on the blockchain with off-chain data storage mechanisms. While data integrity is guaranteed on the blockchain, physical storage is handled by external systems.

IPFS CIDs: InterPlanetary File System (IPFS) Content Identifiers (CIDs) store only references to data on the blockchain, while the actual data are kept within the IPFS network. Since the references are stored on-chain, the data remains verifiable and secure. This method is a cost-effective solution for storing large datasets; however, as the data itself is not stored on-chain, the system is not fully decentralized [15,92].

Beyond blockchain-off-chain system integration, distributed and decentralized cloud solutions represent another key component of hybrid storage strategies.

2.3.2. Distributed and Decentralized Cloud Solutions

This method refers to the combination of traditional cloud infrastructures with blockchain technology. While data can be processed in a decentralized manner, cloud infrastructures provide high capacity and scalability.

- *Hybrid Cloud + Blockchain*: Hybrid cloud models are integrated with blockchain to facilitate data storage within an extensive infrastructure. This approach leverages the advantages of traditional cloud services while benefiting from blockchain's security features. However, data security depends on third-party providers, introducing certain risks [42,93].
- *Lightning Network*: The Lightning Network is a protocol that combines blockchain with off-chain transactions, enabling fast and low-cost microtransactions. Transactions occur off-chain, while only summary data are recorded on the blockchain. However, the Lightning Network is not suitable for managing large datasets, as it is primarily designed for microtransaction processing [94].

Beyond hybrid cloud solutions, Layer-2 optimizations offer high-performance data management solutions on the blockchain.

2.3.3. Layer-2 Optimizations

Layer-2 solutions reduce transaction loads on the main blockchain, providing a more scalable and faster infrastructure. These solutions involve processing data on a secondary layer while storing only summary information on the main blockchain.

- *Rollups*: Rollups process transactions on Layer-2 and store summary data on Layer-1. This method offers high scalability, making it particularly effective for networks with high transaction volumes. However, technical complexity and implementation challenges can hinder widespread adoption [19,20].
- *Plasma*: Plasma is based on processing data on subchains while storing transaction summaries on the main blockchain. This mechanism provides a secure Layer-2 solution, but coordination challenges between subchains introduce operational complexities [52,95].
- *State Channels*: State Channels allow transactions to be executed off-chain, with only the final results recorded on the blockchain. This method provides low latency and high transaction speed. However, the setup process is complex, requiring additional technical knowledge for users [96,97].

Layer-2 solutions play a crucial role in enhancing the scalability of blockchain networks by processing transactions off-chain while ensuring security through various cryptographic mechanisms [52,97]. Technologies such as ZK-Rollups, Optimistic Rollups, Plasma, and

State Channels offer different trade-offs in terms of decentralization, performance, and security [95,96].

However, despite their advantages, Layer-2 solutions introduce certain technical and security challenges. One significant concern is data availability attacks, particularly in Optimistic Rollups, where malicious validators may delay fraud proofs [96]. While ZK-Rollups eliminate this risk, they require substantial computational resources, leading to high operational costs and verification delays [95]. Similarly, Plasma chains suffer from exit fraud risks and complex withdrawal mechanisms, which make them less practical for real-time applications [97].

Additionally, state channels require counterparties to be online for transactions to be settled, which limits their use cases compared to fully decentralized Layer-1 solutions [97]. The table below presents a detailed comparison of different Layer-2 scaling solutions, highlighting their security models, advantages, and limitations. A comparative analysis of Layer-2 scaling solutions is provided in Table 4.

Table 4. A comparative analysis of Layer-2 scaling solutions, examining their security models, advantages, and associated challenges or limitations in optimizing blockchain performance.

Layer-2 Solution	Security Model	Advantages	Challenges/Limitations
ZK-Rollups	Cryptographic proofs (zero-knowledge) [95]	High security, fast verification [95]	High computational cost, proof generation delays [95]
Optimistic Rollups	Fraud proof mechanism [96]	Lower costs, Layer-1 security [96]	Fraud proof verification delay (up to a week) [96]
Plasma	Child chains linked to Layer-1 [97]	Faster transaction processing [97]	Exit fraud risks, complex withdrawals [97]
State Channels	Off-chain transaction channels (e.g., Lightning Network) [97]	Instant transactions, high scalability [97]	Reduced decentralization, requires online counterparties [97]

These challenges suggest that while Layer-2 solutions provide significant scalability improvements, their limitations must be considered when designing blockchain-based storage models [95–97].

2.4. Practical Integration of On-Chain, Off-Chain, and Hybrid Blockchain Storage Approaches

Blockchain technology is rapidly being adopted across various industries due to its data security, transparency, and immutability [1,2,55,98,99]. However, challenges such as managing large datasets, scalability limitations, and high transaction costs have made it impractical to rely on a single data storage approach [17,18,47]. As a result, the integration of on-chain, off-chain, and hybrid data storage solutions has become a critical necessity for enhancing the efficiency and flexibility of blockchain systems [15,16,37,46]. From a practical perspective, on-chain storage is typically used for small-sized and high-security data, whereas off-chain solutions enable the cost-effective storage of large datasets [47,48,100]. Hybrid models, on the other hand, combine the strengths of both approaches, offering a balanced trade-off between security and performance [16,37,46]. For instance, in the healthcare sector, storing sensitive patient records on an off-chain platform such as IPFS, while keeping their integrity references on the blockchain, exemplifies the real-world benefits of such integrations [10,77,101].

In Table 5, a comparative analysis of on-chain, off-chain, and hybrid data storage methods is presented through literature-based examples and practical scenarios across different industries. The advantages and challenges of integration processes are examined in detail, along with their impact on sector-specific solutions, providing insights into the future de-

velopment potential of blockchain-based data storage systems. Each data storage approach offers unique advantages and drawbacks, making context-specific selection crucial.

Table 5. Comparison of on-chain, off-chain, and hybrid data storage methods in blockchain systems: application areas, advantages, and challenges.

Reference Number	Storage Approach	Application Domains	Technology	Advantages	Disadvantages	Scenarios
[33,102,103]	Hybrid	Supply Chain and Logistics	Blockchain + IoT	Traceability, Automation, Secure Logistics	Implementation Complexity	Secured Supply Tracking, Food Traceability
[43,100]	Hybrid	Financial Data Security and Compliance	Distributed Ledger and Cryptography	Secure Transactions, Privacy	Regulatory Complexity	DeFi, Corporate Auditing
[104,105]	Hybrid	Public Administration, e-Government	Self-Sovereign Identity Management	Transparency, Corruption Prevention	Large-Scale Complexity	Digital Identity and Public Record Management
[50,93]	Hybrid	IoT and Blockchain Security	Cryptographic Authentication, Decentralized Spectrum Sharing	Trust, Secure Connectivity	Interoperability Issues	IoT and Smart Device Security
[10,77]	Off-chain	Decentralized Cloud Storage	IPFS	Scalable, Low Cost, Data Redundancy	Retrieval latency	P2P Cloud Storage, Enterprise Backup
[80]	Off-chain	Decentralized Cloud Storage	P2P Storage (Sia)	Low-cost, encrypted storage	Dependence on network participants	Decentralized cloud, personal data storage
[64–66]	On-chain	Permanent Data Storage	Blockweave (Arweave)	Immutability, Long-Term Data Retention	High Transaction Costs	Long-Term and Public Data Storage
[12]	Off-chain	Blockchain-based Storage Networks	Decentralized Networks	Security, Distributed Storage	High Latency	Distributed File Storage
[38,106,107]	Hybrid	Secure IoT Data Sharing	Blockchain and Privacy-Preserving Tech	Secure Access, Data Protection	High Processing Costs	IoT Smart Cities and Industries
[108]	Hybrid	Cyber Threat Data Sharing	Blockchain + Edge Computing	Security, Trust	High Processing Overhead	Secure Cybersecurity Infrastructure

On-chain storage method involves storing all data directly on the blockchain, ensuring immutability, transparency, and reliability. However, it also introduces high transaction costs and scalability limitations. As a result, on-chain storage is primarily preferred for small and critical data that require high security and integrity [1,2,55].

Off-chain data storage methods provide cost efficiency and performance benefits when managing large datasets. Storing data in distributed off-chain storage systems significantly reduces the burden on the blockchain, lowering transaction costs. Systems such as IPFS are commonly used for storing large-scale data [10,77]. For instance, Electronic Health Records (EHRs) can be managed off-chain to enhance security and cost efficiency.

Hybrid models combine on-chain and off-chain methods, offering a balanced solution for security and performance [16,37,46]. While small and sensitive data are kept on-chain, large datasets are stored in external storage systems. This approach improves system performance while maintaining secure data storage. IPFS-integrated hybrid mod-

els, particularly when combined with smart contracts, enhance privacy, scalability, and cost efficiency for managing patient records. However, integrating these systems can be technically complex [10,16,37,46,77].

To enhance IoT security, encryption-based authentication methods [50,93] ensure trusted connections but may introduce compatibility challenges in device-to-device data transmission. Hybrid models merge blockchain-based security with decentralized file systems and traditional data storage methods, preserving high security levels while optimizing transaction costs.

In the decentralized finance (DeFi) ecosystem, distributed ledger and cryptography-based financial solutions [43,100] enhance transaction privacy but also introduce regulatory complexity. Similarly, in supply chain management, the integration of blockchain and IoT [33,102,103] ensures secure product tracking and logistics management. Projects such as IBM Food Trust leverage these technologies to track the origin and transportation conditions of food and pharmaceutical products.

In public administration, self-sovereign identity (SSI) frameworks [104,105] allow for decentralized digital identity management, promoting transparency and secure access control. Decentralized cloud storage solutions are emerging as an alternative to traditional storage systems.

Hybrid cloud architectures that integrate IPFS and blockchain-based solutions [10,77] balance cost efficiency and data security but may face latency challenges in data retrieval. In cybersecurity, blockchain-enabled threat intelligence sharing systems [108] provide real-time attack detection mechanisms to mitigate ransomware attacks and prevent data breaches.

As summarized in Table 5, blockchain-based data storage methods offer distinct advantages across various application scenarios. On-chain storage is an ideal solution for data verification and integrity preservation, while off-chain storage provides performance advantages for managing large datasets. Hybrid approaches, combining both methodologies, ensure a balance between security and performance, maintaining data confidentiality and integrity while optimizing cost efficiency and operational scalability.

2.5. Future Development Potential of Blockchain-Based Data Storage Systems

Blockchain-based data storage methods, particularly through the integration of on-chain, off-chain, and hybrid models, have the potential to revolutionize data management in the future [16,37]. While on-chain methods provide high security and data integrity, they also face significant challenges related to cost and scalability [2,55]. Off-chain solutions, on the other hand, enable the cost-effective and efficient storage of large datasets but require secure integration with blockchain to maintain data verifiability and protection [10,77]. Hybrid models, by combining these two approaches, offer a strategic balance between security and performance, making them a highly viable alternative for scalable blockchain applications [46,101].

Scalability improvements like sharding, rollups, and plasma can enhance blockchain data processing efficiency [18,19,52]. Innovative cryptographic methods like ZKP and homomorphic encryption will boost data privacy and access control [109,110]. The seamless integration of these innovations in sectors such as healthcare, finance, and IoT will facilitate the secure storage, processing, and exchange of sensitive data, further expanding the applicability of blockchain-based storage solutions [101–104,108].

However, several key challenges must be addressed to ensure the widespread adoption of these systems. Hybrid models, while offering flexibility and scalability, require complex infrastructure and significant cost investments for seamless integration of on-chain and off-chain data processing workflows. Additionally, the lack of regulatory frameworks

and standardization poses major compatibility and compliance issues for sector-specific applications [107,111]. Furthermore, the dual objective of enhancing data security while minimizing energy consumption and transaction costs remains a critical research focus in blockchain-based solutions [97,112]. Successfully overcoming these barriers will accelerate the sectoral adoption of blockchain-based data storage systems and unlock the full innovative potential of distributed ledger technology in data management.

3. Security Implications and Fundamental Approaches of Blockchain-Based Data Storage Methods

Blockchain-based storage methods enhance security, playing a key role in strengthening access control and authentication mechanisms [40,46,113]. Understanding the security implications of on-chain and off-chain data storage methods is essential for determining how core data security components are integrated into blockchain infrastructure [16,37,101]. This section examines encryption techniques, authentication protocols, and access control mechanisms aimed at enhancing data security. Additionally, it explores the security impacts of on-chain and off-chain data storage approaches, providing insights into how these methods influence the overall security architecture of blockchain-based systems [50,93,109,110].

3.1. Data Security and Encryption Methods

In blockchain-based systems, data security is a fundamental criterion that ensures data integrity, confidentiality, and protection [110,114]. These technologies rely on various cryptographic techniques to maintain secure and tamper-proof data management [109,115,116]. Security and privacy are particularly critical in sensitive data environments, such as the healthcare sector, where strict data protection measures are required [24,101,103].

3.2. The Role of Cryptographic Methods in Blockchain-Based Data Storage Systems

Cryptographic techniques employed in blockchain-based data storage systems play a critical role in enhancing the security and efficiency of both on-chain and off-chain storage solutions.

Off-chain Data Storage and Security: Storing large datasets off-chain reduces the computational burden on the blockchain, addressing scalability and cost issues. Systems such as IPFS enable secure distributed storage, which is particularly beneficial for managing large-scale healthcare datasets efficiently and securely [10,12,77,101]. However, off-chain storage introduces potential security vulnerabilities. To mitigate these risks, hybrid verification and encryption techniques are employed to ensure data integrity and confidentiality.

On-chain Data Storage and Security: Storing data on-chain leverages blockchain's immutability and transparency, ensuring secure and verifiable data management. Keeping data directly on the blockchain allows network participants to verify data accuracy and integrity [46,50,103]. The on-chain method is particularly ideal for high-security applications, such as financial transactions, smart contract data, and sensitive healthcare records. However, on-chain data storage presents cost and scalability limitations, as it increases blockchain size, making large-scale data management more complex. Despite these challenges, cryptographic techniques such as Merkle trees and blockchain hashing facilitate secure and efficient data storage [58,109,115].

Blockchain systems employ both asymmetric and symmetric encryption techniques to ensure data security. While each method offers distinct advantages, they also come with specific trade-offs in terms of performance, security, and use cases.

3.2.1. Asymmetric Encryption

Asymmetric encryption secures data using a public–private key pair, where information encrypted with the public key can only be decrypted by the corresponding private

key. This mechanism ensures data confidentiality and integrity, allowing only authorized entities to access the encrypted data [58,110,117].

In blockchain-based systems, asymmetric encryption plays a critical role in authentication, data integrity, and access control [102]. It is particularly essential for securing smart contracts, verifying digital signatures, and managing authorized access in on-chain environments [118]. High-security sectors such as finance and healthcare rely on asymmetric encryption to ensure data accuracy and confidentiality. However, processing large datasets with this method can lead to increased computational overhead and extended processing times [114]. To address these performance limitations, asymmetric encryption is often integrated with off-chain solutions for more efficient large-scale data management. Digital signatures serve as a fundamental cryptographic tool for verifying the authenticity of blockchain transactions [53]. Algorithms such as ECDSA and Ed25519 provide fast and secure transaction verification, making them widely adopted in networks like Bitcoin and Ethereum [119]. These methods enhance data security and transaction transparency across various industries, including finance, healthcare, and IoT [120]. While the high computational cost and performance constraints are notable drawbacks, asymmetric encryption remains a cornerstone of blockchain security [112,121].

3.2.2. Symmetric Encryption

Symmetric encryption employs a single key for both encryption and decryption, making it significantly faster and computationally efficient. However, secure key management and distribution remain critical challenges [109,115]. This approach is particularly useful for encrypting large datasets and supporting high-speed data transmission. For instance, symmetric encryption facilitates the secure and rapid transfer of large-scale healthcare records, preserving data confidentiality and integrity. Additionally, cryptographic hash functions are often used to verify data integrity and detect unauthorized modifications [58,110,113].

Symmetric encryption is predominantly applied in off-chain solutions, where its speed advantage is crucial for large-scale data transfers [122,123]. It is widely used in sectors such as education and logistics, where significant volumes of off-chain data require secure storage and transmission [124]. By ensuring high-speed data processing, symmetric encryption enhances scalability, despite its complex key management requirements [116,117]. However, for seamless integration with blockchain, symmetric encryption requires additional security layers [112]. While it is not directly suitable for on-chain use, it remains an effective tool for securing off-chain data [125].

In Table 6, the relationship between these storage methods and blockchain systems is analyzed in terms of storage environments and security considerations.

Table 6. Blockchain-based cryptographic solutions and applications for data security.

Reference Number	Cryptographic Method	Storage Type	Application Domain	Security Requirement	Sectoral Applications	Advantages	Disadvantages
[114,118, 126–128]	Asymmetric Encryption	On-chain, Off-chain	Authentication and data integrity	High	Healthcare, finance	High security, authorized access	Processing time is high
[117,122–124,129]	Symmetric Encryption	Off-chain	Big data transfer	Medium	Healthcare, education, logistic	Provides fast data transfer	Key management issues
[56,109, 115,119, 130–132]	Zero-Knowledge Proof (ZKP)	On-chain, Off-chain, Hybrid	Authentication and access control	High	Public sector, finance	Ensures privacy, verifies data	High computational cost

Table 6. *Cont.*

Reference Number	Cryptographic Method	Storage Type	Application Domain	Security Requirement	Sectoral Applications	Advantages	Disadvantages
[120,125, 133–136]	Homomorphic Encryption	Off-chain, Hybrid	Performing operations on encrypted data	High	Healthcare, IoT	Protects data privacy, provides analysis	Implementation complexity
[16,23–25]	Blockchain Hashing	On-chain	Data integrity and validation	Medium	Education, healthcare	Provides immutability	Inefficient on large datasets
[58,59]	Threshold Cryptography	On-chain, Off-chain, Hybrid	Access control, key management	High	Healthcare, IoT	Provides decentralized key management	Implementation complexity
[137–140]	Multi-Party Computation (MPC)	Off-chain, Off-chain, Hybrid	Private data sharing, access control	High	Healt, finance, IoT	Enables secure computation with data privacy	Computational complexity, high transaction cost
[121,141–143]	Post-Quantum Cryptography	On-chain, Off-chain	Quantum-resistant data security	High	IoT, public sector, health	Resistant to quantum threats	Limited application in standardization

3.2.3. Zero-Knowledge Proof (ZKP)

Zero-Knowledge Proof (ZKP) is an innovative cryptographic method used for authentication and access control. Zero-Knowledge Proof (ZKP) is a cryptographic protocol that allows one party to prove the validity of information to another party without disclosing the actual data. In on-chain systems, ZKP enables users to verify their credentials without revealing sensitive data. For instance, in the healthcare sector, a patient's medical records can be validated without disclosing personal information, ensuring data privacy and security [109,115]. This method is widely utilized in public and financial sectors for blockchain-based identity verification [119,130–132]. Despite its high security benefits, ZKP is computationally expensive, which limits scalability. In hybrid models, ZKP performs privacy-focused off-chain computations, while the verification process takes place on-chain [56,113,133]. This approach is particularly effective for use cases where identity verification is required without exposing personal credentials, such as secure system access control.

3.2.4. Homomorphic Encryption

Homomorphic Encryption allows data to be processed while remaining encrypted, enabling privacy-preserving computations. This technique is particularly useful in off-chain solutions for industries like healthcare and IoT, where sensitive data must be analyzed without decryption [110,120,125]. By maintaining data confidentiality, it allows external systems to perform secure computations [116]. However, its high computational complexity makes it resource intensive [135]. Homomorphic Encryption is primarily suited for off-chain data processing and can be integrated with blockchain-based applications [121,141]. In hybrid models, encrypted data are processed off-chain, while only computation results or cryptographic references are stored on-chain [142]. A practical example includes IoT-generated data being processed securely off-chain, with summary results stored on the blockchain [136].

3.2.5. Blockchain Hashing

Hashing is a fundamental method for ensuring data integrity and authenticity in blockchain systems [16,101]. This technique is primarily used in on-chain systems for validating transactions and ensuring data immutability [24]. Hashing enhances security and transparency, preventing unauthorized data modifications [25]. However, managing

large datasets using hashing alone can be inefficient, making it less effective for large-scale data storage [101]. Hashing is directly related to on-chain reference storage and is commonly used for on-chain data verification solutions [23].

3.2.6. Threshold Cryptography

Threshold Cryptography is a technique that splits a cryptographic key into multiple fragments, requiring a subset of authorized participants to reconstruct it. This method is widely applied in blockchain-based systems for access control and key management. A notable example is digital wallet security, where funds can only be accessed by multiple authorized parties, ensuring decentralized security. While implementation complexity and management challenges are key drawbacks, it is widely used in high-security industries such as healthcare and finance. In hybrid architectures, off-chain key sharing and management are combined with on-chain access control and authentication mechanisms. A practical use case involves verifying multiple authorized digital signatures on-chain before granting access [58,59].

3.2.7. Multi-Party Computation (MPC)

Multi-Party Computation (MPC) is a privacy-preserving cryptographic method that allows multiple parties to jointly compute a function without revealing individual private inputs. This approach is particularly effective in industries such as healthcare and finance, where sensitive data must be analyzed across multiple entities while preserving confidentiality. MPC is often integrated with off-chain computation, allowing data from different institutions to be securely processed, with only verification results stored on-chain [137,139]. Its advantages include ensuring data privacy and establishing trust among participants, whereas high computational overhead and scalability challenges remain key limitations [138,140].

3.2.8. Post-Quantum Cryptography

Post-Quantum Cryptography is a security framework designed to protect against quantum computing attacks that could break traditional cryptographic algorithms [112,121]. It is increasingly being adopted in blockchain-based systems to ensure long-term security against quantum threats [141,142]. Since widely used cryptographic schemes like RSA and ECDSA are vulnerable to quantum attacks, post-quantum encryption offers a future-proof security solution [121,143]. Its primary advantages include enhanced resistance to quantum-based threats and long-term cryptographic security. However, ongoing standardization efforts and computational efficiency challenges currently limit its widespread adoption [141,142]. Post-Quantum Cryptography is particularly relevant for public and financial sectors, where blockchain security must be strengthened against future quantum computing risks [112,141].

3.2.9. Security vs. Performance Trade-Offs in Cryptographic Techniques

Ensuring the security of blockchain-based storage requires employing cryptographic techniques that offer strong confidentiality, integrity, and authentication. However, these techniques vary in their computational overhead, which affects processing time, CPU utilization, and memory efficiency. Understanding the trade-offs between security and performance is essential when selecting the appropriate cryptographic approach for real-world applications.

To provide a structured evaluation, Table 7 presents a comparative analysis of cryptographic techniques based on their security level, computational overhead, performance impact, and practical use cases. This analysis allows us to assess the balance between cryptographic robustness and system efficiency.

Table 7. Security vs. Performance Trade-offs in Cryptographic Techniques.

Cryptographic Technique	Security Level	Computational Overhead	Performance Impact	Use Cases	References
Asymmetric Encryption (RSA, ECDSA, Ed25519)	High	High due to key size and modular exponentiation	Slow for large-scale transactions, high processing cost	Digital signatures, secure authentication, blockchain consensus mechanisms	[114,118,126–128]
Symmetric Encryption (AES-256, ChaCha20)	High	Low, optimized for speed and efficiency	Fast and efficient, suitable for real-time processing	Encrypted storage, secure messaging, VPN encryption	[117,122–124,129]
Zero-Knowledge Proofs (ZKP–SNARKs, STARKs)	Very High	Very High, requires complex proof generation	Slows down authentication due to proof verification time	Anonymous transactions, identity verification, privacy-focused blockchain applications	[56,109,115, 119,130–132]
Homomorphic Encryption (Fully Homomorphic Encryption—FHE)	Very High	Extremely High, impractical for real-time operations	Extremely slow, impractical for large-scale blockchain storage	Cloud computing, privacy-preserving smart contracts	[120,125,133–136]
Hashing Mechanisms (SHA-256, Keccak, Blake2)	Medium	Low, designed for quick computation	Minimal impact, designed for rapid verification	Blockchain transaction integrity, data verification, proof-of-work mechanisms	[16,23–25]

This comparative evaluation highlights key trade-offs in cryptographic techniques: Asymmetric Encryption (RSA, ECDSA, Ed25519)

- Offers strong security but incurs high computational overhead due to modular exponentiation.
- Slower than symmetric encryption, making it less suitable for large-scale transactions.

Symmetric Encryption (AES-256, ChaCha20)

- Designed for speed and efficiency, offering high security with low processing costs.
- Used extensively for secure storage and fast encrypted communication.

Zero-Knowledge Proofs (ZKP–SNARKs, STARKs)

- Provide privacy-preserving authentication but require significant computation.
- Proof generation and verification are resource intensive, slowing down transactions.

Homomorphic Encryption (FHE)

- Enables computations on encrypted data, offering maximum security.
- Extremely high resource consumption makes it impractical for large-scale blockchain storage.

Hashing Mechanisms (SHA-256, Keccak, Blake2)

- Lightweight and efficient, designed for rapid data integrity verification.
- Low computational overhead, making it ideal for blockchain transaction verification.

This evaluation demonstrates that higher security often comes with a significant performance cost. FHE and ZKP offer advanced security but impose high computational

overhead, making them less practical for real-time blockchain applications. In contrast, symmetric encryption and hashing mechanisms balance security and performance efficiently, making them the preferred choices for scalable blockchain storage and authentication systems. Selecting an appropriate cryptographic technique depends on the specific application requirements, available computational resources, and performance constraints.

3.3. Authentication Methods

Authentication is a key element of data security in blockchain-based systems, especially in sectors managing sensitive data such as healthcare, finance, and government [40,45,104,105,107,118,126]. Blockchain enhances security and privacy by providing decentralized, tamper-proof authentication [56,115,144,145]. On-chain methods ensure immutability, off-chain solutions offer scalability, and hybrid models combine both for flexible, secure authentication [16,27,32,37,77,146]. In the next section, decentralized authentication methods using blockchain are explored.

Decentralized Authentication, Applications, and Security Enhancements

Blockchain-based authentication removes central authority dependence and secures identity data. By leveraging blockchain's immutability and transparency, authentication records are securely stored, preventing unauthorized modifications and ensuring data integrity [1,104,144].

Decentralized authentication systems record each verification process immutably on the blockchain, reinforcing identity protection and preventing data tampering. Self-Sovereign Identity (SSI) solutions enable users to manage their credentials independently, leveraging blockchain's distributed nature to prevent unauthorized modifications [1,104,105]. Authentication processes rely on asymmetric encryption, where users sign credentials with a private key, and verification occurs via a public key before being recorded on-chain, ensuring both security and integrity [53,102,144].

Blockchain authentication seamlessly adapts to different data storage models, balancing security, scalability, and efficiency. On-chain storage offers high security and ensures data integrity, making it ideal for critical identity records. However, it presents challenges in scalability and cost, particularly for large identity datasets [16,37,101]. Off-chain storage mitigates these issues by storing identity data externally while keeping cryptographic references on-chain, ensuring cost-effective scalability [10,77,89]. Hybrid approaches integrate both strategies, maintaining detailed records off-chain (e.g., in IPFS) while keeping verification data on-chain, ensuring transparency, security, and efficiency [16,32,37].

Decentralized authentication plays a crucial role in sensitive sectors such as healthcare and finance. In healthcare, patients securely share identity credentials with authorized professionals, ensuring privacy and controlled access [1,48,147–149]. Hybrid models enhance both security and scalability by maintaining access logs on-chain while managing sensitive health records off-chain. In the financial sector, blockchain authentication strengthens fraud-resistant identity verification and transaction security [43,100,139].

A key advancement in blockchain authentication is the Zero-Knowledge Proof (ZKP) technique, which enables identity verification without exposing personal data, significantly improving privacy in authentication processes [40,56,132]. In hybrid models, ZKP can validate credentials off-chain while storing only verification proofs on-chain, enhancing both security and efficiency [109,115,119].

By providing decentralized, secure, and privacy-preserving authentication, blockchain solutions drive trust and resilience across diverse industries, including healthcare, finance, and IoT, paving the way for robust identity management in decentralized ecosystems [1,104,147,150].

3.4. Access Control Mechanisms in Relation to Blockchain Storage Types

In blockchain-based data storage systems, access control mechanisms provide decentralized and secure methods to ensure that only authorized individuals can access sensitive data while preserving data confidentiality. Access control is particularly critical in industries handling sensitive data, such as healthcare, financial services, and government sectors, where strong security measures are required to prevent unauthorized access [40,41,44]. Access control mechanisms are closely linked to the fundamental data storage methods used in blockchain systems. On-chain storage ensures immutability and transparency for access control records, enabling auditable and tamper-proof access management. In contrast, off-chain storage allows for the scalable processing of large datasets, requiring additional security layers for access control enforcement [16,37,46]. Figure 5 shows the use of data storage systems with access control mechanisms.

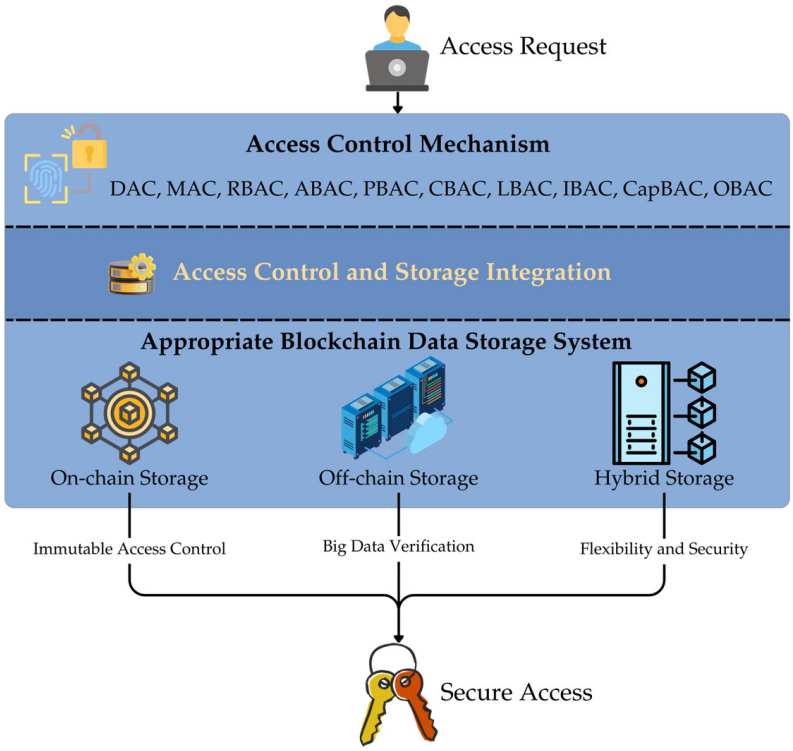

Figure 5. Use of data storage systems with access control mechanisms. Blockchain-based storage systems integrate access control to regulate data access. Authentication ensure only authorized users can retrieve or modify data. Smart contracts enforce access policies, while cryptographic techniques enhance security and integrity.

It plays a critical role in protecting sensitive data, particularly in the healthcare, finance, and public sectors [39,151,152]. Hybrid approaches, such as IPFS and blockchain integration, ensure high security while optimizing transaction costs [32,37,46,113]. The transparency and immutability of blockchain enhance the traceability of access operations, making it easier to detect unauthorized access attempts [1,104,153]. For instance, in Ethereum-based systems, access logs are stored on-chain, while large datasets are processed off-chain, balancing security and cost efficiency [43,53].

On-chain access control mechanisms enhance security by storing access policies immutably on the blockchain. Mandatory Access Control (MAC) enforces strict policies to limit access [154]. Role-Based Access Control (RBAC) grants role-based permissions [44,155,156]. Identity-Based Access Control (IBAC) enhances security by managing access based on user identities [44,45,154]. Lattice-Based Access Control (LBAC) provides hierarchical authorization, commonly used in defense industries [44,154].

Off-chain solutions improve scalability for large data processing while relying on blockchain references for security. Discretionary Access Control (DAC) allows data owners to manage access rights [44,111,156]. Capability-Based Access Control (CapBAC) provides flexibility with token-based authentication mechanisms, frequently used in distributed cloud systems [157–161].

Hybrid systems combine on-chain security with off-chain flexibility, enabling dynamic access control. Attribute-Based Access Control (ABAC) and Policy-Based Access Control (PBAC) manage access rights through on-chain policies and off-chain dynamic updates [40,45,111,162]. Context-Based Access Control (CBAC) regulates access based on factors such as device, location, or time [111,162]. Organization-Based Access Control (OBAC) optimizes access permissions within an organization [44].

The integration of these access control mechanisms with blockchain systems ensures high security and scalability across domains such as finance, healthcare, IoT, and supply chain management [104,150–152]. Table 8 summarizes the integration of blockchain-based access control mechanisms with different storage strategies.

Table 8. Classification of access control mechanisms compatible with on-chain, off-chain, and hybrid storage methods [44,111,113].

Access Control Mechanism	On-Chain	Off-Chain	Hybrid	Operational Characteristics of the Mechanisms
DAC (Discretionary Access Control)	✗	✔	✔	DAC allows users to flexibly modify access rights but cannot be implemented on-chain due to blockchain's immutability. Off-chain systems are suitable as they provide user authorization without requiring a central authority. Hybrid models enhance security by managing authorization off-chain while maintaining access records on-chain.
MAC (Mandatory Access Control)	✔	✗	✔	MAC, which requires centralized authorization, aligns well with blockchain's immutable and auditable structure. Off-chain solutions are unsuitable due to their decentralized nature. Hybrid models balance policy enforcement by storing access control rules on-chain while processing decision mechanisms off-chain for greater flexibility.
RBAC (Role-Based Access Control)	✔	✔	✔	Since roles can be stored immutably on the blockchain, on-chain implementation is feasible. However, for large-scale organizations, off-chain storage is preferable. Hybrid models provide flexible solutions by balancing security and scalability.
ABAC (Attribute-Based Access Control)	✔	✔	✔	On-chain storage is appropriate for immutable attributes, but off-chain solutions improve update speed for frequently changing attributes. Hybrid models ensure flexibility by keeping static attributes on-chain while dynamically managing updates off-chain.
PBAC (Policy-Based Access Control)	✔	✔	✔	For transparent policy recording, on-chain storage is ideal. Off-chain solutions enable quick responses to dynamic policy changes. Hybrid models maintain core policies on-chain while updating dynamic components off-chain to ensure balance.

Table 8. *Cont.*

Access Control Mechanism	On-Chain	Off-Chain	Hybrid	Operational Characteristics of the Mechanisms
CBAC (Context-Based Access Control)	✔	✔	✔	Context-based access management can be implemented on-chain using immutable data. Off-chain storage provides real-time processing of contextual data, making it advantageous. Hybrid models log contextual changes on-chain while utilizing off-chain solutions to enhance processing speed.
LBAC (Lattice-Based Access Control)	✔	✘	✔	Lattice-based hierarchical access levels require immutable definitions, making on-chain storage suitable. Off-chain management is less effective. Hybrid models ensure on-chain security while managing updates off-chain, improving flexibility.
IBAC (Identity-Based Access Control)	✔	✔	✔	For user authentication, on-chain storage ensures immutable identity verification records. However, off-chain solutions are more practical for large-scale identity management. Hybrid models keep verification records on-chain while handling dynamic identity management off-chain.
CapBAC (Capability-Based Access Control)	✔	✔	✔	Capability-Based Access Control (CapBAC), which governs token-based access rights, ensures on-chain security. Off-chain solutions are preferable for managing large datasets. Hybrid models enhance the scalability and security of capability-based access control mechanisms.
OBAC (Organization-Based Access Control)	✔	✔	✔	Organization-Based Access Control (OBAC) policies are secured by storing them on-chain, but off-chain solutions are advantageous for frequently updated policies. Hybrid models integrate secure on-chain records with flexible off-chain processing mechanisms for dynamic policy management.

In off-chain systems, users have greater control over their own data. However, in large-scale blockchain systems, DAC operates efficiently when data are stored off-chain [44,111,156]. On-chain structures support MAC's high-security requirements, but its centralized and rigid nature limits flexibility in dynamic applications [59,65]. In on-chain systems, roles and access permissions can be immutably recorded, ensuring tamper-proof access control [155]. Hybrid systems provide scalability by allowing dynamic role modifications [16,37,101]. Off-chain solutions can store large datasets related to roles, though this approach is less common [111,161]. On-chain structures ensure transparency through immutable attribute records [44,45,111]. Off-chain applications enable fast attribute updates, improving real-time adaptability. Hybrid systems combine the security of on-chain storage with the flexibility of off-chain processing. For example, dynamic attributes like user age and location can be effectively managed within a hybrid system [16,37,101]. On-chain applications facilitate transparent policy recording, while off-chain systems enable rapid implementation of dynamic policy changes. Hybrid architectures optimize policy updates by balancing performance and security [111,162,163]. Context-Based Access Control (CBAC) dynamically manages context changes. On-chain implementations securely store immutable context data, while off-chain systems efficiently process real-time context variations. Hybrid approaches ensure flexibility and security in context-aware access con-

trol [111,162]. Lattice-Based Access Control (LBAC) is well-suited for on-chain storage, supporting immutable hierarchical access level definitions. Hybrid models integrate hierarchical structures with large-scale external systems for enhanced scalability [154,164]. On-chain systems provide tamper-proof identity verification, while off-chain solutions facilitate large-scale identity management. Hybrid models strike a balance between performance and security. On-chain mechanisms ensure the secure recording of capability tokens [44,45,154]. Off-chain systems optimize token-based access control for large datasets. Hybrid models offer decentralized and scalable token management, improving access control flexibility [44,157,162]. On-chain storage secures organization-based access policies through immutable records. Off-chain solutions handle complex, large-scale organizational policies. Hybrid models combine security and flexibility for efficient organizational access control [22,44,161].

3.5. Blockchain-Based Data Integrity and Traceability Solutions

Blockchain-based data storage systems offer robust mechanisms for ensuring data integrity and traceability [26,28,30]. These systems guarantee data accuracy and immutability, while also enabling transparent tracking of access and usage records [28,31,33]. However, the applicability of these mechanisms varies depending on the chosen data storage method [32,34]. On-chain approaches provide full traceability and verifiable authenticity, but they come with high transaction costs [6,36]. In contrast, off-chain methods offer lower costs and greater efficiency, but they may be less secure in terms of data integrity and accessibility [35,165]. Hybrid systems combine the strengths of both on-chain and off-chain solutions, delivering a balanced approach in terms of cost efficiency and security [37,47]. Table 9 summarizes the advantages and disadvantages of these storage mechanisms by evaluating data storage methods, data integrity mechanisms, and traceability levels across various industry sectors.

Table 9. Comparative overview of data integrity and traceability solutions in blockchain-based storage methods.

Storage Method	Data Integrity Mechanism	Traceability	Sectoral Applications	Advantages	Disadvantages	Reference Number
On-chain	Hash-based verification	High	Healthcare, finance	Reliable verification, full traceability	High transaction cost	[31]
Off-chain	Only hash data on blockchain	Medium	Education, Healthcare, logistic	Low cost, efficiency	Inadequate in areas requiring data security	[36]
Hybrid	On-chain and off-chain integration	High	Healthcare, IoT	Provides balanced cost and safety	Requires complex configuration	[6,28,32–35,37,47,165]

3.5.1. Ensuring High Data Integrity with On-Chain Methods

On-chain data storage methods utilize hash-based verification mechanisms to provide high reliability and full traceability. These methods are particularly suitable for applications in healthcare and finance, where data integrity is critical [31]. However, high transaction costs and scalability limitations can restrict their usability in large datasets or high-volume processing scenarios [29].

3.5.2. Balancing Efficiency and Security in Off-Chain Approaches

Off-chain solutions reduce costs and processing overhead by storing only data references on the blockchain. This method offers a cost-effective and efficient alternative for sectors such as education, healthcare, and logistics [35]. However, in applications requiring high security, off-chain solutions are not as reliable as on-chain methods. Particularly in scenarios where critical data protection is necessary, off-chain storage provides only a limited level of security [36].

3.5.3. Achieving Flexibility with Hybrid Storage Solutions

Hybrid approaches combine the advantages of on-chain and off-chain methods, providing a balanced solution between security and cost [26,28,37,47]. These methods are especially practical for managing large datasets in healthcare and IoT applications [6,33]. However, complex configuration requirements may limit their applicability and require technical expertise [24,32].

The selection of blockchain-based data storage methods depends on data integrity requirements, cost constraints, and sector-specific needs [26,35,47]. On-chain methods are preferred in high-security environments, whereas off-chain solutions offer cost advantages [36]. Hybrid approaches, by integrating both methods, provide a broader range of applications [6,32,33]. These insights contribute to optimizing blockchain-based data storage systems across various industries [26,28,47].

3.6. Sectoral Applications and Perspectives Regarding On-Chain, Off-Chain, and Hybrid Data Storage Methods

The adoption of blockchain-based data storage solutions has transformed how industries approach security, scalability, and efficiency in managing sensitive data. Depending on the industry, the choice of storage method (on-chain, off-chain, or hybrid) plays a critical role in addressing specific challenges and requirements. For instance, the healthcare sector prioritizes privacy and real-time access to patient records [151,152,166–170], whereas the financial sector focuses on immutability and data integrity [43,100]. Similarly, supply chain management requires traceability and logistical efficiency [103,171–173], while IoT applications emphasize efficiency and high-speed data processing [50,51]. Each of these sectors leverages the strengths of various data storage approaches while using blockchain technology to address unique challenges.

Table 10 summarizes the applications, use cases, security requirements, advantages, and disadvantages of on-chain, off-chain, and hybrid data storage solutions across different industries. This comprehensive analysis provides valuable insights into how blockchain technology is adapted to meet industry-specific demands. The classification aims to illustrate how blockchain-based storage methods align with sectoral needs, offering perspectives on real-world applications, and future potential blockchain-based data storage solutions are being implemented through various methods tailored to the specific needs of different industries. Healthcare, finance, education, supply chain, government, and IoT each require different technologies based on data security requirements, transaction costs, integration demands, and scalability concerns.

Table 10 evaluates blockchain-based data storage methods across different industries, identifying which technologies ensure the highest security and efficiency for each sector.

Table 10. Sectoral perspective on data security and applications of on-chain, off-chain, and hybrid data storage methods.

Reference Number	Sector	Recommended Storage Method	Application Domains	Security Need	Security Advantages	Disadvantages	Sample Projects
[151,152,166–170]	Healthcare	Hybrid (Blockchain + IPFS and Smart Contracts)	Patient data, electronic health records (EHR)	High	Ensures privacy and security, legal data protection	Integration challenges	MedRec, FHIRChain
[43,100]	Finance	On-chain (DLT and Cryptography)	Credit history, transaction records	Medium	Provides data integrity and immutability	Costly and slow transaction speeds	Hyperledger Fabric
[7,49,174]	Education	Off-chain (Blockchain + IPFS)	Sharing certificates, diploma, and degree	Low	Cost effectiveness, high data access speed	Dependency on centralized systems	IPFS Education Projects
[103,171–173]	Supply Chain	Hybrid (Blockchain + IoT)	Product traceability, logistics management	High	Traceability, fast data processing	Complex configuration	IBM Food Trust
[104,105,175]	Public Sector	On-chain (Self-Sovereign Identity and Digital ID Management)	Authentication, records management	High	Transparency, secure access	High transaction cost and speed limitations	Civic
[50,51]	Internet of Things (IoT)	Hybrid (Blockchain + Cryptographic Authentication)	Sensor data, location data	Medium	Efficiency, low cost	Lack of data integrity and traceability	Helium Network

Real-World Implementations of Blockchain Storage Solutions

Blockchain storage solutions have been widely adopted across various industries, demonstrating their potential to enhance data security, transparency, and operational efficiency. In this section, real-world case studies are presented to illustrate how on-chain, off-chain, and hybrid blockchain storage models have been utilized in sectors such as healthcare, finance, education, supply chain management, public administration, and IoT applications.

In healthcare, the secure and decentralized storage of patient data and electronic health records (EHRs) is essential [151,166]. Hybrid solutions, combining blockchain with decentralized storage systems like IPFS, protect data integrity while preventing unauthorized access through encryption [168,169]. Projects like MedRec and FHIRChain facilitate secure patient data sharing between healthcare institutions while ensuring immutability [167–170]. For instance, FHIRChain has been piloted in major hospital networks, demonstrating its ability to provide tamper-proof patient records while complying with the HIPAA and the GDPR. Its integration with existing hospital management systems has shown significant improvements in data accessibility and integrity, and the adoption of standardized frameworks may enhance real-time data sharing while maintaining patient privacy, facilitating hybrid integration [151,152,166,168]. Additionally, advanced security technologies such as homomorphic encryption are further strengthening health record security [110,135].

In the financial sector, transaction accuracy and data integrity are paramount. On-chain solutions, using distributed ledger technology (DLT) and advanced cryptographic security mechanisms, ensure the protection of financial transactions. Platforms like Hyperledger Fabric enable immutable storage of credit histories and transaction records within the decentralized finance (DeFi) ecosystem, but complex regulatory requirements and high transaction costs limit widespread adoption [43,100]. A practical implementation of this is found in JPMorgan's Quorum blockchain, which enables secure interbank set-

tlements and cross-border transactions by leveraging permissioned DLT. This showcases how blockchain enhances security in financial data storage while overcoming traditional banking inefficiencies. Future Layer-2 solutions may help reduce scalability and transaction cost concerns, promoting broader blockchain adoption in finance [19,20,97]. Optimistic Rollup and ZK-Rollup technologies will enhance transaction speeds and efficiency in DeFi ecosystems [95,96].

In education, blockchain ensures the immutability of academic certificates and diplomas, helping to combat fraud and enhance reliability in recruitment processes. Off-chain solutions, integrating IPFS-based education projects, enable secure document storage while allowing authorized users to access encrypted records [7,49]. However, integration with centralized education systems and long-term storage costs present challenges [7,174]. The University of Nicosia, one of the first institutions to adopt blockchain for academic credentials, has successfully issued digital diplomas that are verifiable via blockchain explorers. This initiative has proven to reduce diploma fraud and increase employer trust in academic certifications. In the future, greaization in blockchain-based education solutions is expected. Particularly, Self-Sovereign Identity (SSI) models will simplify document verification [49,174].

In supply chain management, blockchain plays a critical role in product traceability and fraud prevention. Projects like IBM Food Trust enhance tracking for sensitive products such as food and pharmaceuticals [103,171]. However, integrating existing supply chain infrastructures with blockchain poses additional costs and complexity [172,173]. A real-world case study is Walmart's integration of IBM Food Trust for tracking pork supply chains in China. This blockchain solution reduced the time needed to track contaminated food sources from 7 days to just 2.2 s, highlighting blockchain's impact on safety and supply chain efficiency. Future AI-powered blockchain will optimize decision-making processes in global logistics networks, enhancing traceability and transparency [103,171,173]. Projects like IBM Food Trust and TPPSupply will be instrumental in fraud prevention and sustainable logistics management [6,33].

In the public sector, blockchain is revolutionizing identity verification and official record management [104]. On-chain identity management systems, using Self-Sovereign Identity (SSI) approaches, allow individuals to manage personal identity information without relying on a central authority [105,175]. Projects like Civic utilize blockchain to prevent identity fraud in digital authentication processes [104]. For example, Estonia's e-Residency program leverages blockchain to offer digital identity services to global citizens. This system has facilitated secure cross-border authentication and online business registration, making Estonia a leader in blockchain-based governance. However, the traditional centralized nature administration makes the adoption of blockchain-based identity management systems challenging [175]. In the future, new legal regulations and integration efforts may help mainstream blockchain-based identity management. E-government projects are expected to increasingly adopt blockchain for digital identity verification [104,175].

In the IoT sector, securing large datasets generated by smart devices and ensuring authorized data access are key challenges [50]. Hybrid solutions, integrating blockchain-based authentication mechanisms, facilitate secure IoT data exchanges [51]. Projects like Helium Network create decentralized wireless networks to enhance secure blockchain-based IoT operations [50,153]. However, data integrity and traceability limitations present scalability challenges in IoT networks [51]. One real-world implementation of blockchain in IoT is the Helium Network, which enables IoT devices to communicate securely over a decentralized network. This has led to improvements in smart city infrastructure, including environmental monitoring and asset tracking. In the future, advanced security protocols and control mechanisms will play a critical role in managing large-scale data

flows [50,51]. Blockchain-based authentication systems will enhance IoT device security, while decentralized architectures will minimize single points of failure [131,133,134].

These sector-specific applications highlight the versatility and adaptability of blockchain-based data storage solutions. Spanning IoT, finance, education, government, and supply chain management, blockchain technologies enhance data security and operational efficiency by providing a robust infrastructure. As industry evolves, blockchain-based storage solutions are expected to develop into more innovative and specialized strategies. The adaptability of on-chain, off-chain, and hybrid storage solutions has the potential to revolutionize various industries. The scalability, security features, and integration capabilities of blockchain enhance data management processes across multiple sectors [20,42,97,166]. In the future, the integration of AI-powered blockchain solutions, homomorphic encryption, and quantum-resistant cryptography will further advance the field [110,112,135,142].

3.7. Blockchain-Based Distributed Data Storage and File Sharing Projects

Distributed and blockchain-based data storage solutions vary based on their security features and application domains. Table 11 provides a detailed overview of prominent projects, storage methodologies, data retention strategies, and industry applications associated with these solutions.

Table 11. Features and usage areas of projects working on blockchain-based distributed data storage and file sharing.

Project Name	Underlying Infrastructure	Storage Type	Security Features	Application Domains	Advantages	Disadvantages	Reference Number
Filecoin	IPFS	Off-chain	Encryption, verifiable hashing	Distributed file storage	Decentralization, high security	Scaling challenges for big data	[75,76]
Storj	Has its own distributed network	Off-chain	Encryption, multi-node storage	Cloud file storage	Strong encryption, user incentives	Slow, dependency on node participation	[79]
Flux	IPFS, has its own infrastructure	Hybrid	Hash-based security	Decentralized applications (DApps)	High security and flexibility	High transaction costs	[30]
Arweave	Arweave Protocol	On-chain	Permanent storage, hashing	Long-term data retention	Permanent data storage, censorship resistance	High transaction costs	[64–66]
Sia	Has its own distributed network	Off-chain	Encryption, data shredding	Decentralized cloud storage	Economical storage, encryption support	Limitations in security protocols	[80]
BitTorrent	Swarm, P2P Protocol	Off-chain	Component-based distribution	File sharing, content transfer	Fast content delivery, low bandwidth usage	Risk of hacking, security vulnerabilities	[176]
Ankr	Has its own infrastructure	Hybrid	Encryption, source authentication	Enterprise solutions, cloud services	Resource efficiency, low cost	Complex configuration, intense competition	[162]
Holo	Holochain	Off-chain	Cryptographic signatures	Dapp hosting	High scalability, user control	Early development stage	[161]
Helium	Blockchain and IoT	Hybrid	Data transmission encryption	IoT data transfer, wireless network	Low-Cost Connectivity and Network Expansion Incentives	Limited coverage, limited to IoT	[153]
Civic	Blockchain	On-chain	Authentication, data privacy	IoT security, user data control	Secure authentication, user-specific access	Compatibility difficulties, delays	[177]

Table 11 provides a detailed analysis of how blockchain and distributed storage solutions are applied across various use cases.

Filecoin and Storj, which utilize off-chain storage, offer decentralized and secure cloud storage while ensuring data integrity through strong encryption techniques. However, these systems face scalability challenges and are dependent on node participation for reliability. Hybrid systems like Flux and Helium integrate blockchain infrastructure with their own specialized networks, providing high-security solutions for decentralized applications and IoT data transfer. While they offer flexibility and cost efficiency, complex configuration requirements pose integration challenges. On-chain storage solutions, such as Arweave and Civic, focus on permanent data storage and identity verification, addressing critical security needs. These platforms ensure long-term data retention and user-controlled data access. However, high transaction costs and regulatory compliance challenges limit their widespread adoption. Among off-chain systems, Sia and BitTorrent provide low-cost and fast content distribution but face security vulnerabilities and piracy risks. Hybrid and off-chain solutions like Ankr and Holo offer secure storage for decentralized application hosting and enterprise cloud services. However, they face challenges related to early-stage development and high market competition. These projects demonstrate how blockchain-based storage solutions can be adapted across different industries while highlighting the unique advantages and limitations of each approach.

4. Discussions

This study evaluates blockchain-based data storage solutions based on on-chain and off-chain approaches. The findings indicate that both methods provide distinct advantages, which vary depending on specific use cases. On-chain storage offers strong security and ensures data permanence, while Off-chain solutions reduce costs while enhancing processing capacity. Hybrid strategies integrate the strengths of both methods, offering a well-balanced solution in terms of data security and scalability. However, for blockchain-based data storage systems to achieve full adoption, challenges related to scalability, access control, and regulatory compliance must be addressed. In particular, integrating hybrid systems presents technical complexities in large-scale data management. To enhance data security and system efficiency, new protocols must be developed. In the future, blockchain-based data storage solutions are expected to see broader adoption in industries such as healthcare, finance, supply chain, and IoT.

4.1. Performance Comparison of Blockchain Data Storage Methods

Blockchain-based data storage methods have various advantages and limitations concerning key criteria such as transaction speed, scalability, cost, and security. These factors play a critical role in determining the suitability of blockchain-based solutions for sectoral applications and use cases.

On-chain storage ensures high security and data integrity by storing all data directly on the blockchain; however, it comes with significant limitations in terms of transaction costs and scalability. In contrast, off-chain storage improves transaction speed and reduces costs by storing data outside the blockchain, but it introduces certain risks regarding data integrity and security. Hybrid solutions aim to combine the advantages of both on-chain and off-chain methods to optimize performance while maintaining security. Table 12 compares these three different storage approaches based on four key criteria, presenting their advantages and limitations as established in the literature.

- *Transaction Speed*: On-chain data storage has a low transaction speed due to the requirement that all transactions be verified on the blockchain and undergo the mining process [17]. In networks such as Bitcoin and Ethereum, transaction times are inher-

ently constrained by mining mechanisms. In contrast, off-chain solutions significantly improve transaction speed by moving data outside the blockchain [19]. This approach is particularly supported by Layer-2 solutions such as the Lightning Network [22]. Hybrid methods, on the other hand, enhance security by keeping certain data on-chain while storing large volumes of data off-chain, thereby maintaining a balance in terms of speed.

- *Scalability*: On-chain data storage offers low scalability due to block size limitations and network congestion [18]. Off-chain solutions provide higher scalability by storing data outside the blockchain, as they are not constrained by the blockchain's transaction capacity [19]. Hybrid solutions create a balanced model by integrating both on-chain and off-chain methods to enhance scalability [97].
- *Cost*: On-chain data storage is costly due to mining expenses, transaction fees, and block size limitations [12]. In contrast, off-chain solutions are cost-effective since transactions are executed outside the blockchain [15]. Hybrid solutions reduce costs by offloading large volumes of data off-chain while preserving security by storing critical data on-chain, resulting in a moderate cost structure [22].
- *Security*: On-chain data storage offers the highest level of security due to its distributed ledger structure, which ensures data integrity and immutability [36]. Off-chain solutions, on the other hand, provide lower security levels as data are stored outside the blockchain and often controlled by centralized entities [47]. Hybrid solutions enhance security by leveraging on-chain verification mechanisms while storing the majority of data off-chain to optimize performance [109].

Table 12. Performance comparison of blockchain-based data storage methods in terms of transaction speed, scalability, cost, and security.

Criteria	On-Chain	Off-Chain	Hybrid	References
Transaction Speed	Low—Full node validation slows transactions	High—Off-chain solutions (Lightning Network, Rollups) improve speed	Medium-High—Hybrid balances both	[17,19,22]
Scalability	Low—Block size and network congestion limit scalability	High—Off-chain solutions significantly enhance scalability	Medium—Hybrid solutions mitigate scalability issues	[18,19,97]
Cost	Very High—Transaction fees depend on network demand	Low—Off-chain solutions lower transaction fees	Medium—Hybrid solutions balance cost factors	[12,15,22]
Security	Very High—Data integrity and security ensured by consensus mechanisms	Low—Relies on third-party trust	Medium—Hybrid maintains some on-chain security	[36,47,109]

4.2. Integration Challenges in Hybrid Blockchain Data Storage Systems

While hybrid data storage solutions provide advantages in security and cost efficiency, they also face technical challenges during integration. Key challenges involve synchronizing large-scale data, implementing robust access control mechanisms, and ensuring data security in hybrid environments. For seamless integration with existing systems, new protocols and optimized access control mechanisms must be developed. Smart contracts and off-chain storage technologies like IPFS can enhance the flexibility of these systems.

4.3. Regulatory and Security Evaluation of Blockchain-Based Data Storage Solutions

The adoption of blockchain-based data storage solutions must be evaluated within regulatory compliance frameworks. Regulations like the GDPR raise concerns as blockchain's

immutability conflicts with the right to data deletion. Security vulnerabilities in smart contracts and the absence of clear regulatory frameworks pose significant challenges to large-scale adoption. To enhance data security and privacy, integrating advanced cryptographic techniques such as Zero-Knowledge Proofs, Multi-Party Computation, and Post-Quantum Cryptography can significantly strengthen the security and resilience of blockchain-based storage systems.

4.4. Evolution, Future Trends, and Open Research Areas in Blockchain-Based Data Storage

Blockchain-based data storage systems have undergone significant evolution since the introduction of Bitcoin in 2008 [21]. Initially, Bitcoin adopted a fully on-chain storage model, where all transactions were recorded directly on the blockchain. However, as scalability limitations, transaction speed constraints, and cost concerns emerged, alternative data storage approaches, off-chain, and hybrid models began to evolve. These developments marked the transformation of blockchain storage technologies, enabling greater flexibility and efficiency.

Looking ahead, blockchain-based data storage systems are expected to become more scalable, flexible, and intelligent. The integration of AI-driven access control and security mechanisms has the potential to enhance intrusion detection systems, making them more adaptive and responsive to emerging threats. Furthermore, blockchain's application scope is anticipated to expand beyond healthcare, finance, and IoT into diverse sectors such as supply chain management, agriculture, and education. For instance, blockchain-powered pharmaceutical supply chains can significantly improve data security and transparency in tracking processes. Additionally, regulatory and policy advancements will play a crucial role in shaping the future of blockchain-based data storage. The establishment of international standards will enhance the reliability of these technologies, ensuring compliance with data security regulations and facilitating broader adoption. This will not only bolster blockchain's credibility but also expand its user base by fostering trust among stakeholders.

As blockchain storage systems continue to evolve, improvements in scalability, security, and cross-sector adoption will further enhance their potential to revolutionize data storage and management. Future research areas should focus on optimizing on-chain, off-chain, and hybrid storage models, addressing cost efficiency challenges, and integrating emerging technologies such as AI and privacy-preserving cryptographic techniques to solidify blockchain's role as a foundational pillar of next-generation data infrastructure. Table 13 presents the historical progression of on-chain, off-chain, and hybrid storage technologies.

Table 13. Evolution of On-Chain, Off-Chain, and Hybrid Data Storage Methods: Key Technological Advancements, Application Domains, and Underlying Innovations.

Year	Data Storage and Processing Model	Application Domain	Key Applications	Underlying Technologies	Reference Number
2008	On-chain	Finance	Bitcoin (Transaction Storage)	Merkle Trees, Proof-of-Work	[21]
2013, 2014	On-chain	Finance	Ethereum (Smart Contracts)	Ethereum State Storage, Solidity, and EVM	[74]
2014	Off-chain	Healthcare	IPFS, MedRec (EHR)	IPFS, Off-chain Hash Storage, Content Addressing	[78]

Table 13. *Cont.*

Year	Data Storage and Processing Model	Application Domain	Key Applications	Underlying Technologies	Reference Number
2017	Hybrid	Education	EduChain (Education records)	Blockchain-based Educaton Systems	[7,49]
2018	Off-chain	IoT	Blockchain-IoT Security	State Channels	[50,51]
2018	Layer-2	Finance	Plasma-Based Scaling Solutions	State Channels, Optimistic Rollups	[17,52]
2020	Hybrid	Public	Blockchain for Government Services	e-Government, Digital Identity, Blockchain Identity Management	[175]
2021	Layer-2	Finance	Zero-Knowledge Rollups	zk-SNARKs, zk-STARKs, Validity Proofs	[178,179]
2022	Hybrid	Cloud Computing	Hybrid Blockchain-Cloud Systems	Layer-2 Rollups, zk-SNARKs, Sharding	[42]
2023	Hybrid	Supply Chain	Blockchain-based drug supply chain	Plasma, Optimistic Rollups, Zero-Knowledge Proofs	[160,173]
2023	Layer-2	Finance	Zero-Knowledge Rollups (ZKsync, StarkNet, Polygon zkEVM)	zk-SNARKs, zk-STARKs, Validity Proofs	[17,19]
2024–2025	On-chain	Finance and AI	AI-based Smart Contracts	AI + Blockchain, Large Language Models (LLM) + Smart Contracts	[159]
2024–2025	Hybrid	Interoperability Solutions	Cross-Blockchain Data Integration	Polkadot, Cosmos, Axelar, Interoperability Protocols	[179–181]
2024–2025	Layer-2	Finance and Enterprise	Modular Blockchains (ZeroLayer, EigenLayer, Celestia)	Restaking, Data Availability Layers, Rollup-as-a-Service	[18]
2025	Layer-2	IoT	Blockchain-IoT Integration, Smart Device Security	IoT Blockchain Net, Data Oracles, Privacy-Preserving Smart Contracts	[51,121]
2025+	Edge-integrated Hybrid (Edge Storage + On-chain Metadata + Off-chain Distributed Storage)	Healthcare, Industry 5.0, Smart Cities, Autonomous Systems, IoE	Real-time data processing, Decentralized data storage, Edge data analytics, Secure IoT communications	Blockchain, Edge Computing, IPFS, Asymmetric and Symmetric Cryptography	[182–184]

Over the years, blockchain-based data storage has evolved significantly, driven by the need for greater scalability, efficiency, and interoperability. While early implementations primarily relied on on-chain models, increasing demands for cost reduction and performance optimization led to the adoption of off-chain and hybrid approaches. As shown in Table 13, this evolution spans multiple sectors, including finance, healthcare, education, supply chain, IoT, and cloud computing, with advancements in Layer-2 solutions, zero-knowledge proofs (ZKPs), and interoperability protocols. These developments not only address scalability concerns but also enhance security and real-time data processing capabilities.

4.4.1. The Emergence of Ethereum and Smart Contracts

With the launch of Ethereum in 2015, smart contracts were integrated into the blockchain ecosystem, providing a foundation for decentralized applications (DApps) [62,74]. However, as adoption increased, challenges such as scalability issues, transaction loads, and data storage costs became more prominent. During this period, permissioned blockchain solutions like Hyperledger Fabric were developed, offering flexible and modular data storage systems for the private sector [185]. As a result, industries such as finance, healthcare, and logistics began adopting blockchain-based data management solutions.

4.4.2. The Rise in Off-Chain Data Storage Solutions

By 2017, large-scale data management and transaction speeds had become major concerns for blockchain technology [1]. Off-chain solutions such as IPFS allowed large files to be stored externally while keeping only hash references on-chain, reducing transaction costs significantly [77,78]. This approach facilitated the cost-effective storage of large datasets in industries such as education, healthcare, and public administration. Around the same time, persistent data storage solutions like Arweave laid the groundwork for hybrid models [64].

4.4.3. Layer-2 Solutions and Hybrid Data Storage Models

Hybrid blockchain solutions gained traction in 2017. Projects like EduChain enabled decentralized sharing of academic credentials [7,49]. By 2018, blockchain was integrated with IoT, enhancing device security [50,51]. From 2019 onwards, Layer-2 solutions such as Plasma, State Channels, and Sidechains reduced transaction loads and improved scalability [17,52]. In 2021, ZK-Rollups technology leveraged Zero-Knowledge Proofs (ZKP) to process large amounts of data off-chain while recording only verification data on-chain [19]. These advancements improved Ethereum's transaction scalability by alleviating Layer-1 congestion. Cryptographic techniques like zk-SNARKs and zk-STARKs further accelerated transaction validation while significantly reducing network strain [19,178]. By 2022, Layer-2 solutions had become widespread across the finance, public, and IoT sectors, transforming blockchain-based data storage [17]. The same year, hybrid blockchain-cloud solutions allowed large datasets to be stored off-chain while managing access controls through blockchain [32,168]. In 2023, blockchain-based supply chain solutions were implemented in the pharmaceutical sector [160,173].

4.4.4. Ethereum 2.0, Sharding, and Advanced Hybrid Models

The introduction of Ethereum 2.0 in 2022 brought Sharding technology, significantly enhancing data storage capacity [22]. This was a crucial development for public record management and large-scale data processing. Simultaneously, projects like Cosmos and Polkadot introduced cross-chain solutions that facilitated seamless data transfers between blockchain networks [181]. These initiatives improved blockchain interoperability, integrating various data storage methods. By 2023, Zero-Knowledge Rollup solutions such as

ZKsync [186], StarkNet [187], and Polygon zkEVM enhanced the scalability of Ethereum and other blockchain networks [17,19].

In recent years, Layer-2 solutions have undergone rapid evolution. By 2023, solutions like ZKsync, StarkNet, and Polygon zkEVM were deployed to enhance the scalability of Ethereum and other blockchains [17,19]. These innovations hold transformative potential, particularly in decentralized finance (DeFi) and enterprise applications.

4.4.5. On-Chain AI and Blockchain Integration

The integration of artificial intelligence with blockchain has gained increasing importance in recent years. On-chain AI models have combined decentralized computing with blockchain-based data storage systems [159]. Projects such as Fetch.ai, Ocean Protocol, and SingularityNET have optimized blockchain-AI integration, leading to their merger under the Artificial Superintelligence Alliance in 2024 [188]. Additionally, projects like Chainlink, Polkadot, Cosmos, and Axelar have improved cross-chain data sharing, addressing interoperability challenges [179–181].

- *Enhancing Security and Automation*: The integration of AI and blockchain is playing an increasingly critical role in improving decision-making processes, detecting fraud, and ensuring data security in decentralized environments. AI models operating with blockchain-based smart contracts enable reliable computations and tamper-resistant data storage.

Real-world applications include:

- Fetch.ai: A system that optimizes logistics, finance, and supply chains using blockchain-based AI agents [188].
- Ocean Protocol: A decentralized data-sharing protocol that allows AI models to train on encrypted datasets [188].
- SingularityNET: A marketplace for AI services that enables commercialization without relying on a central provider [188].
- IBM Watson and Hyperledger Fabric: AI-powered blockchain-based fraud detection models that analyze financial transactions to identify anomalies [159].

This integration enables AI models to perform reliable data processing, transparent auditing, and autonomous decision-making within decentralized systems.

By 2025, blockchain-based data storage solutions are expected to play a crucial role beyond DeFi and enterprise applications, extending to IoT device security. Projects such as Helium Network [153], Chainlink [189], and IoTeX [190] have introduced new Layer-2 solutions focused on data privacy within the IoT ecosystem. This historical evolution highlights how blockchain-based data storage methods have undergone significant transformations in scalability, security, and flexibility.

In the coming years, blockchain's impact is expected to expand exponentially across artificial intelligence, IoT, supply chains, and finance. Modular blockchain architectures will drive the development of more efficient and secure systems. Projects like EigenLayer [191], Celestia [192], and ZeroLayer [193] are set to shape the blockchain ecosystem by introducing innovations in data availability, restaking mechanisms, and Rollup-as-a-Service models. Furthermore, the adoption of blockchain technology in AI, IoT, supply chains, and finance is expected to accelerate, enabling faster, more secure, and energy-efficient infrastructures through cross-chain integration and Layer-2 advancements.

- *Blockchain and IoT: Securing Smart Devices and Data Exchange*: IoT devices generate vast amounts of data, requiring secure, immutable, and decentralized storage. Blockchain integration enhances security by protecting against unauthorized data access and mitigating cyber threats.

Real-world applications include the following:

- Helium Network: A decentralized IoT connectivity network that enables secure device communication [153];
- IoTeX: Utilizes blockchain-based authentication protocols to ensure encrypted data transmission for IoT devices [190];
- VeChain: Uses IoT sensors to track products in supply chains, securing data with blockchain technology [103];
- Bosch XDK and Ethereum: Smart sensors integrated with Ethereum-based smart contracts provide real-time monitoring in industrial environments [22,87].

Blockchain enhances security in IoT systems by eliminating central points of failure and increasing operational transparency.

4.4.6. The Road Ahead for Blockchain Storage: Emerging Paradigms in Edge Computing and the Internet of Everything Era

The evolution of data storage methods within blockchain systems is increasingly influenced by the convergence of the Internet of Everything (IoE) and edge computing technologies. As the volume of connected devices expands in sectors such as smart cities, healthcare, autonomous systems, and industrial automation, the demand for real-time data processing, decentralized storage, and secure device-to-device communication is expected to intensify [182,183].

Edge computing enables data to be processed and temporarily stored closer to its source, reducing latency and alleviating the burden on centralized servers. When integrated with blockchain technology, edge computing not only strengthens data security and integrity through decentralized consensus but also facilitates localized decision making [184]. This hybrid approach is particularly critical for IoE ecosystems, where billions of devices simultaneously generate and process sensitive data.

Future solutions are anticipated to adopt Edge-integrated Hybrid Storage Models, combining the following:

- On-chain metadata verification for ensuring immutability;
- Off-chain distributed storage systems (e.g., IPFS) for scalable data management;
- Edge storage and processing to enhance performance and minimize response times.

Recent studies suggest that this three-layered hybrid model will become the dominant architecture for data storage and security in future IoE environments. Such systems can offer low-latency responses, decentralized control, and improved data privacy, particularly in resource-constrained edge settings. However, interoperability challenges, device-level vulnerabilities, and data synchronization issues remain key obstacles requiring further research [182–184].

The ongoing convergence of blockchain and edge computing is expected to follow a structured development path:

- 2024–2025+: Increased adoption of blockchain-integrated edge computing solutions, especially in smart city infrastructures, industrial automation, and healthcare data systems [194];
- 2026–2028+: Standardization of hybrid storage architectures, where on-chain metadata verification is combined with off-chain and edge computing storage models for enhanced security and scalability [182];
- 2028–2030+: Full deployment of autonomous blockchain-based edge systems, enabling decentralized AI-driven decision making in IoE environments, reducing dependency on centralized cloud infrastructures [195].

Despite these advancements, scalability constraints, device-level security vulnerabilities, and interoperability challenges remain critical hurdles that require further research and industry collaboration [182–184,194,195].

4.5. Limitations and Future Works

Blockchain-based data storage solutions offer decentralization, security, and transparency, yet they still present several challenges. Scalability remains a major issue: while on-chain storage ensures high security, it suffers from high costs and limited transaction throughput. In contrast, off-chain storage methods enhance efficiency but introduce concerns regarding data availability and integrity. Additionally, security risks, such as access control vulnerabilities and key management complexities in decentralized storage systems, require further research. To address these challenges, future research should focus on the following:

- Enhancing Scalability: Optimizing Layer-2 solutions (e.g., Rollups, State Channels, Plasma) to improve transaction speed and reduce costs [19,20,52,95].
- Strengthening Security and Privacy: Improving blockchain-based access control mechanisms, such as Attribute-Based Access Control (ABAC) and Zero-Knowledge Proofs (ZKPs), for privacy-preserving storage [47,109].
- Integrating Blockchain with AI and ML: Exploring AI-driven data retrieval and adaptive storage mechanisms for optimizing blockchain efficiency [102,104].
- Expanding Industry-Specific Implementations: Investigating blockchain storage solutions for IoT-based secure data sharing and continuous authentication, as well as custom blockchain models for satellite communications and space data management [196].

These advancements are expected to enhance the efficiency, scalability, and security of blockchain-based storage solutions while unlocking new opportunities for decentralized data management.

4.5.1. Energy Consumption in Blockchain-Based Storage Systems

While blockchain technology offers advantages in decentralized data management and security, it also imposes significant energy costs. Proof-of-Work (PoW)-based blockchains are known for their high energy consumption due to mining processes that require substantial computational power [45,88]. In networks such as Bitcoin and Ethereum, mining activities consume large amounts of electricity, increasing their carbon footprint. In contrast, alternative consensus mechanisms such as Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), and Proof-of-Authority (PoA) improve blockchain sustainability by significantly reducing energy consumption [92,101].

Comparative Energy Consumption of Blockchain Consensus Mechanisms: Table 14 presents the energy consumption levels of different consensus mechanisms and their advantages in terms of sustainability. This comparison demonstrates that PoS and PoA-based blockchain solutions enhance energy efficiency, contributing to more sustainable blockchain storage systems.

- *Sustainability Strategies for Blockchain-Based Storage*: Several innovative strategies have been proposed to improve the sustainability of blockchain-based data storage solutions:
  1. Green Blockchain Networks: Developing carbon-neutral blockchain projects and promoting the use of sustainable energy sources [106];
  2. Layer-2 Solutions and Sharding: Reducing transaction load and minimizing energy consumption through Layer-2 scaling solutions and sharding mechanisms [94,108];

3. Hybrid Blockchain and Off-Chain Data Storage: Utilizing off-chain storage systems to reduce the data burden on the blockchain and lower transaction costs [85,99];
4. Renewable Energy for Mining: Transitioning to renewable energy sources in mining activities to mitigate the environmental impact of energy consumption [103].

Table 14. Comparative Energy Consumption of Blockchain Consensus Mechanisms.

Consensus Mechanism	Energy Consumption	Security Level	Scalability	Sustainability Impact	Examples
Proof-of-Work (PoW)	High [45,88]	Very High [92]	Low [101]	High carbon footprint [106]	Bitcoin, Ethereum (pre-merge) [21,22]
Proof-of-Stake (PoS)	Low [94]	High [103]	High [108]	Energy-efficient [99]	Ethereum 2.0 [22], Cardano
Delegated PoS (DPoS)	Very Low [85]	Medium [88]	Very High [92]	Sustainable [101]	EOS, TRON [190]
Proof-of-Authority (PoA)	Very Low [106]	Medium [94]	High [99]	Sustainable [108]	VeChain, BSC [103]

These strategies aim to enhance the long-term sustainability of blockchain-based data storage systems while minimizing their environmental footprint.

4.5.2. Limitations of Current Approaches

While blockchain storage models offer robust security and decentralization, they face several key limitations:

Scalability Constraints: On-chain storage requires network-wide validation, which limits transaction throughput and increases latency. Layer-2 solutions and sharding techniques have been proposed to mitigate this, but their implementation remains technically challenging [17,18,22].

Security Risks in Off-Chain Storage: Off-chain storage methods depend on external infrastructures (e.g., IPFS, cloud storage), which may introduce risks related to data integrity and availability [12,15,109].

Hybrid Implementation Complexity: Although hybrid models aim to balance scalability, security, and cost, their integration requires sophisticated cryptographic mechanisms and interoperability between on-chain and off-chain components, making large-scale adoption challenging [36,47,97].

4.5.3. Regulatory and Compliance Challenges in Blockchain Storage Solutions

Blockchain-based storage solutions offer enhanced security, transparency, and decentralization; however, regulatory and compliance challenges remain significant barriers to widespread adoption, particularly in highly regulated sectors such as healthcare and finance. The primary concerns are data sovereignty and jurisdictional compliance. Regulations such as the General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the United States impose strict requirements on data storage, access, and privacy, which may conflict with blockchain's immutable nature [115,127].

In healthcare, ensuring compliance with patient data protection laws while leveraging blockchain for secure electronic health records (EHRs) presents a challenge. While blockchain enables data integrity and tamper-proof record-keeping, its decentralized nature raises concerns regarding data retrieval rights and the right to be forgotten (as stipulated

in GDPR) [122]. Similarly, in the financial sector, compliance with anti-money laundering (AML) and know-your-customer (KYC) regulations requires adaptable access control mechanisms that balance security with regulatory requirements [126]. To address these challenges, hybrid blockchain models that incorporate off-chain storage for sensitive data while using on-chain mechanisms for verification and auditability are being explored as potential solutions. Additionally, zero-knowledge proofs (ZKP) and confidential smart contracts offer promising methods for ensuring compliance while maintaining privacy [170].

Future research should focus on developing regulatory frameworks tailored for blockchain-based storage systems, ensuring that decentralization and security advantages do not come at the expense of legal and ethical obligations [123].

4.5.4. Cost, Performance, and Security Comparison with Traditional Storage Solutions

While blockchain-based storage solutions provide decentralization, immutability, and cryptographic security, they introduce challenges in terms of cost, performance, and scalability when compared to traditional centralized storage systems [102,110]. A direct comparison is presented below to illustrate the trade-offs involved. Table 15 illustrates the comparison of traditional centralized storage and blockchain-based storage.

Table 15. Comparison of Traditional Centralized Storage vs. Blockchain-Based Storage.

Criteria	Traditional Centralized Storage	Blockchain-Based Storage
Cost	Lower cost, cloud-based storage (AWS, Google Cloud) has flexible pricing models [103].	Higher costs due to mining fees, redundancy, and data replication [97].
Performance	High performance, real-time processing [104].	Lower throughput due to consensus mechanisms [110].
Scalability	Easily scalable with cloud services [103].	Limited scalability, high transaction fees [97].
Security	Centralized security measures (firewalls, access control) [105].	Cryptographic security, tamper-proof records [102].
Data Integrity	Prone to data breaches and insider threats [104].	Data immutability ensures integrity [110].
Examples	SQL Databases, AWS S3, Google Cloud Storage [103].	Filecoin, IPFS, Arweave [97].

These findings suggest that while blockchain-based storage solutions provide enhanced security and data integrity, they may not be the most cost-effective or high-performance alternative for all applications [97,102–105,110].

Furthermore, centralized storage systems, such as SQL-based databases and cloud storage providers, offer lower operational costs and higher transaction speeds [97,103,104]. However, these systems remain vulnerable to data breaches and lack the transparency of blockchain-based models [102].

In contrast, blockchain storage solutions ensure data integrity and censorship resistance but at the cost of reduced efficiency and higher computational expenses. The integration of hybrid models, where blockchain is combined with traditional storage for critical data verification, is being explored as a potential solution to overcome these limitations [105].

4.5.5. Limitations of Layer-2 Solutions

While Layer-2 solutions provide a pathway to scale blockchain networks, they introduce critical challenges in terms of security, interoperability, and decentralization [95–97].

First, security concerns stem from off-chain transaction processing, where Layer-2 mechanisms do not fully inherit Layer-1 security guarantees. For example, Optimistic Rollups rely on fraud proofs, which introduce delays and potential risks in dispute resolution [96]. Similarly, Plasma chains require regular interactions with the main chain, which can lead to vulnerabilities in chain synchronization and fund withdrawals [97].

Second, Layer-2 solutions lack standardization, making cross-platform integration difficult. Since each Layer-2 framework operates differently (e.g., ZK-Rollups vs. State Channels), interoperability remains a key challenge for broader adoption [95].

Lastly, the computational cost of cryptographic techniques used in Layer-2 solutions remains high. ZK-Rollups, while offering high security, require complex proof-generation processes, making them resource intensive and potentially expensive for large-scale blockchain deployments [95].

The following table presents a detailed comparison of Layer-1 and Layer-2 solutions, highlighting their trade-offs in security, decentralization, and scalability. In Table 16, a comparison of Layer-1 and Layer-2 blockchain solutions is given.

Table 16. Comparison of Layer-1 and Layer-2 Blockchain Solutions.

Feature	Layer-1 Blockchain	Layer-2 Solutions
Security	Maximum security, but slow transaction finality [52]	Dependent on Layer-1, vulnerable to data availability attacks [96]
Transaction Speed	Low (~15–30 TPS on Ethereum) [97]	High (~2000 TPS with ZK-Rollups, near-instant with State Channels) [97]
Decentralization	Fully decentralized [52]	Partial decentralization (some Layer-2 solutions require trust assumptions) [96]
Scalability	Limited, high transaction fees [52,97]	High scalability, but off-chain storage risks [96]
Implementation Complexity	Directly operates on smart contracts [52]	Requires additional protocols and integration layers [95]
Examples	Ethereum, Bitcoin [97]	ZK-Rollups, Optimistic Rollups, Plasma, State Channels [95,96]

These challenges suggest that while Layer-2 solutions provide significant scalability improvements, their limitations must be considered when designing blockchain-based storage models [95–97].

4.5.6. Future Research Directions

To overcome these limitations, future research should focus on key advancements in scalability, security, and novel blockchain applications.

Scalability Enhancements with Layer-2 Solutions:

- Optimizing Rollups and Plasma to reduce transaction costs and improve on-chain efficiency [19,20,97].
- Developing data compression techniques to minimize blockchain state size [52,95].

Improving Security in Hybrid Blockchain Models:

- Designing cryptographic proof mechanisms (e.g., Zero-Knowledge Proofs, Merkle trees) for off-chain data verification without fully storing it on-chain [109,113].
- Developing automated auditing frameworks to detect unauthorized data modifications [36,47].

Continuous Authentication and IoT-Blockchain Integration:

- Future research should explore blockchain-based Continuous Authentication (CA) for IoT systems to enhance security and reduce trust dependencies. The integration of authentication mechanisms such as behavioral biometrics and real-time identity verification can strengthen IoT security models [197]
- Integrating biometric authentication with smart contracts for real-time device identity validation [12,36,42].

Custom Blockchain Models for Satellite Communications:

- Blockchain can be leveraged for secure and decentralized communication networks in satellite-based systems. Customized blockchain frameworks can facilitate secure inter-satellite communications while ensuring data integrity in space networks [196].
- Developing Proof-of-Authority (PoA) consensus models for low-latency satellite networks [15,47,93].

Leveraging AI and Blockchain for Smart Data Management:

- AI-driven storage optimization techniques to enhance data partitioning and retrieval [109,129].
- Machine learning-based anomaly detection to identify fraudulent data transactions in off-chain storage [113,115].

4.5.7. The Impact of Quantum Computing on Blockchain Storage Security

The rapid advancements in quantum computing pose a significant threat to blockchain security. Traditional cryptographic schemes such as RSA and ECDSA, which rely on the difficulty of integer factorization and discrete logarithm problems, are vulnerable to Shor's algorithm, enabling efficient decryption of private keys. This vulnerability could compromise blockchain networks by allowing attackers to forge digital signatures and alter transaction histories.

To mitigate this risk, Post-Quantum Cryptography (PQC) has been introduced, with cryptographic algorithms that remain secure against quantum adversaries. Among these, lattice-based cryptography, hash-based signatures (e.g., XMSS, SPHINCS+), and code-based cryptography (e.g., McEliece cryptosystem) are the most promising candidates for quantum-resistant blockchain systems.

While PQC provides robust security, its adoption in blockchain networks presents challenges such as computational overhead, key size expansion, and verification speed reduction. For instance, lattice-based encryption schemes significantly increase key sizes, leading to higher storage demands and slower verification times.

In response, blockchain projects such as Hyperledger Fabric, Ethereum's Ethereum 3.0 research, and NIST's Post-Quantum Cryptography Standardization project are actively investigating hybrid models that integrate PQC mechanisms while balancing security and performance.

Future research should focus on the following:

- Developing lightweight post-quantum cryptographic techniques that optimize performance while ensuring security.
- Implementing hybrid cryptographic models, integrating post-quantum and classical encryption methods for transition phases.
- Exploring quantum-resistant consensus mechanisms, ensuring blockchain integrity even in post-quantum environments.

The adaptation of PQC in blockchain-based storage systems will be crucial to ensuring long-term security, particularly in sectors such as finance, healthcare, and IoT, where data immutability and authentication mechanisms are of paramount importance.

5. Conclusions

This study presents a comprehensive review and systematic analysis of blockchain-based data storage methods, evaluating their security, scalability, and cost trade-offs. By classifying on-chain, off-chain, and hybrid storage approaches, this research has highlighted their advantages, limitations, and industry-specific applications. Furthermore, the study has examined the security challenges associated with blockchain storage and discussed cryptographic mechanisms that enhance data protection.

Key Insights and Implications.

- Hybrid storage solutions have emerged as a critical approach for balancing security, scalability, and cost efficiency in blockchain-based data management. While on-chain storage ensures data integrity and transparency, its scalability issues remain a bottleneck. Conversely, off-chain storage offers cost efficiency but poses challenges in decentralization and trust management. Hybrid models present a promising trade-off, particularly for use cases that demand both security and high-volume data processing.
- Layer-2 solutions have been identified as a viable method to enhance blockchain storage efficiency. Rollups, state channels, and sidechains demonstrate potential in reducing on-chain storage loads while maintaining security guarantees. However, their adoption across industries remains a challenge due to interoperability constraints and regulatory concerns.
- The security evaluation of blockchain storage mechanisms underscores the importance of cryptographic techniques such as Zero-Knowledge Proofs (ZKP), Homomorphic Encryption, and advanced access control models (RBAC, ABAC). These mechanisms play a crucial role in ensuring data confidentiality and integrity, particularly in sectors like healthcare, finance, and IoT.
- Decentralized storage networks (Filecoin, Arweave, Swarm, Sia, Storj) provide an alternative to traditional blockchain storage by leveraging distributed infrastructures for secure and scalable data management. However, their economic and governance models still require further optimization to achieve broader adoption in enterprise environments.
- Sectoral analysis of blockchain storage applications reveals that healthcare, finance, and IoT industries benefit the most from blockchain's secure and immutable architecture. However, regulatory frameworks, privacy concerns, and energy consumption challenges remain key barriers to mass adoption.

Implications and Future Directions

Based on these findings, future research should address the following critical areas:

- Optimizing hybrid blockchain storage models to maximize efficiency and security without compromising decentralization;
- Developing standardized interoperability protocols to enable seamless data exchange between different blockchain networks;
- Enhancing quantum-resistant cryptographic techniques to future-proof blockchain storage against emerging computational threats;
- Evaluating real-world implementation challenges and assessing the economic feasibility of blockchain storage solutions in various industries;
- Addressing regulatory and compliance challenges to facilitate broader adoption of blockchain storage technologies in highly sensitive domains;
- Edge Computing and Internet of Everything (IoE) should be studied for their potential in enhancing blockchain storage scalability and efficiency.

This study contributes to the field by systematically classifying blockchain storage approaches, identifying security trade-offs, and presenting a structured research roadmap

for future exploration. The insights gained from this study provide a foundation for improving the design and adoption of secure, scalable, and cost-efficient blockchain-based data storage solutions.

Author Contributions: Conceptualization and problem definition: H.E., Ö.K. and M.T.G.; Development of blockchain storage classification: H.E., Ö.K. and M.T.G.; Sectoral analysis of blockchain storage methods: Ö.K. and H.E.; Comparative analysis of on-chain, off-chain, and hybrid storage methodologies: H.E. and Ö.K.; Security framework design for access control models: M.T.G. and Ö.K.; Evaluation of industry-specific security models: H.E. and Ö.K.; Evaluation of cryptographic security mechanisms in blockchain storage: M.T.G.; Writing, original draft: Ö.K., H.E. and M.T.G.; Writing, review and editing: Ö.K., H.E. and M.T.G.; Visualization (tables, diagrams, and frameworks): Ö.K.; Supervision and final approval: H.E. and M.T.G. All authors have read and agreed to the published version of the manuscript.

Funding: This study is supported by Institution of Firat University Scientific Research Projects (FUBAP) under project number SHY.24.18, with the APC funded by FUBAP.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created.

Acknowledgments: The authors acknowledge the CHIST-ERA Di4SPDS project (CHIST-ERA-22-SPiDDS-01) and its national partner project, TUBITAK 223N142, conducted under the TUBITAK 1071 International Collaboration Program, within the CHIST-ERA Di4SPDS framework.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Banitalebi Dehkordi, A. EDBLSD-IIoT: A comprehensive hybrid architecture for enhanced data security, reduced latency, and optimized energy in industrial IoT networks. *J. Supercomput.* **2025**, *81*, 359. [CrossRef]
2. Lezzi, M.; Del Vecchio, V.; Lazoi, M. Using blockchain technology for sustainability and secure data management in the energy industry: Implications and future research directions. *Sustainability* **2024**, *16*, 7949. [CrossRef]
3. Taherdoost, H. Blockchain and healthcare: A critical analysis of progress and challenges in the last five years. *Blockchains* **2023**, *1*, 73–89. [CrossRef]
4. Almadadha, R. Blockchain technology in financial accounting: Enhancing transparency, security, and esg reporting. *Blockchains* **2024**, *2*, 312–333. [CrossRef]
5. Lin, I.-C.; Kuo, Y.-H.; Chang, C.-C.; Liu, J.-C.; Chang, C.-C. Symmetry in blockchain-powered secure decentralized data storage: Mitigating risks and ensuring confidentiality. *Symmetry* **2024**, *16*, 147. [CrossRef]
6. Li, L.; Qu, H.; Wang, H.; Wang, J.; Wang, B.; Wang, W.; Xu, J.; Wang, Z. A blockchain-based product traceability system with off-chain EPCIS and IoT device authentication. *Sensors* **2022**, *22*, 8680. [CrossRef]
7. Lin, Y.; Xie, Z.; Chen, T.; Cheng, X.; Wen, H. Image privacy protection scheme based on high-quality reconstruction DCT compression and nonlinear dynamics. *Expert Syst. Appl.* **2024**, *257*, 124891. [CrossRef]
8. Rani, D.; Gill, N.S.; Gulia, P.; Yahya, M.; Ahanger, T.A.; Hassan, M.M.; Abdallah, F.B.; Shukla, P.K. A secure digital evidence preservation system for an iot-enabled smart environment using ipfs, blockchain, and smart contracts. *Peer-to-Peer Netw. Appl.* **2025**, *18*, 5. [CrossRef]
9. Kaur, J.; Rani, R.; Kalra, N. Attribute-based access control scheme for secure storage and sharing of EHRs using blockchain and IPFS. *Clust. Comput.* **2024**, *27*, 1047–1061. [CrossRef]
10. Alizadeh, M.; Andersson, K.; Schelén, O. Efficient decentralized data storage based on public blockchain and IPFS. In Proceedings of the IEEE Asia-Pacific Conference on Computer Science and Data Engineering, Gold Coast, Australia, 16–18 December 2020; pp. 1–8.
11. Merlec, M.M.; In, H.P. Blockchain-based decentralized storage systems for sustainable data self-sovereignty: A comparative study. *Sustainability* **2024**, *16*, 7671. [CrossRef]
12. Benisi, N.Z.; Aminian, M.; Javadi, B. Blockchain-based decentralized storage networks: A survey. *J. Netw. Comput. Appl.* **2020**, *162*, 102656. [CrossRef]

13. Verma, G. Blockchain-based privacy preservation framework for healthcare data in cloud environment. *J. Exp. Theor. Artif. Intell.* **2024**, *36*, 147–160. [CrossRef]
14. Dhokrat, J.G.; Pulgam, N.; Maktum, T.; Mane, V. A Framework for Privacy-Preserving Multiparty Computation with Homomorphic Encryption and Zero-Knowledge Proofs. *Informatica* **2024**, *48*, 1–14. [CrossRef]
15. Doan, T.V.; Psaras, I.; Ott, J.; Bajpai, V. Toward decentralized cloud storage with IPFS: Opportunities, challenges, and future considerations. *IEEE Internet Comput.* **2022**, *26*, 7–15. [CrossRef]
16. Miyachi, K.; Mackey, T.K. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Inf. Process. Manag.* **2021**, *58*, 102535. [CrossRef]
17. Rebello, G.A.F.; Camilo, G.F.; de Souza, L.A.C.; Potop-Butucaru, M.; de Amorim, M.D.; Campista, M.E.M.; Costa, L.H.M. A survey on blockchain scalability: From hardware to layer-two protocols. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 2411–2458. [CrossRef]
18. Quan, B.L.Y.; Wahab, N.H.A.; Al-Dhaqm, A.; Alshammari, A.; Aqarni, A.; Abd Razak, S.; Wei, K.T. Recent advances in sharding techniques for scalable blockchain networks: A review. *IEEE Access* **2024**, *13*, 21335–21366. [CrossRef]
19. Tremblay Thibault, L.; Sarry, T.; Senhaji Hafid, A. Blockchain scaling using rollups: A comprehensive survey. *IEEE Access* **2022**, *10*, 93039–93054. [CrossRef]
20. Saif, M.B.; Migliorini, S.; Spoto, F. A survey on data availability in layer 2 blockchain rollups: Open challenges and future improvements. *Future Internet* **2024**, *16*, 315. [CrossRef]
21. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 8 February 2025).
22. Kudzin, A.; Toyoda, K.; Takayama, S.; Ishigame, A. Scaling Ethereum 2.0's cross-shard transactions with refined data structures. *Cryptography* **2022**, *6*, 57. [CrossRef]
23. Li, H.; Han, D. EduRSS: A blockchain-based educational records secure storage and sharing scheme. *IEEE Access* **2019**, *7*, 179273–179284. [CrossRef]
24. Verma, P.; Tripathi, V.; Pant, B. Secure Hashgraph for healthcare: Strengthening privacy and data security in patient records. *IEEE Trans. Consum. Electron.* **2024**, *70*, 1205–1213. [CrossRef]
25. Ramadan, R.A.; Khalifa, H.S.; Dessouky, M.; Aboshosha, B.W. Blockchain Technology for Enhanced Security of IoT Healthcare Devices: A Novel Lightweight Hash Function Approach and Secure Management System. 2024. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4680105 (accessed on 8 February 2025).
26. Musamih, A.; Salah, K.; Jayaraman, R.; Arshad, J.; Debe, M.; Al-Hammadi, Y.; Ellahham, S. A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE Access* **2021**, *9*, 9728–9743. [CrossRef]
27. Leal, F.; Chis, A.E.; Caton, S.; González–Vélez, H.; García–Gómez, J.M.; Durá, M.; Sánchez–García, A.; Sáez, C.; Karageorgos, A.; Gerogiannis, V.C.; et al. Smart pharmaceutical manufacturing: Ensuring end-to-end traceability and data integrity in medicine production. *Big Data Res.* **2021**, *24*, 100172. [CrossRef]
28. Zaabar, B.; Cheikhrouhou, O.; Jamil, F.; Ammi, M.; Abid, M. HealthBlock: A secure blockchain-based healthcare data management system. *Comput. Netw.* **2021**, *200*, 108500. [CrossRef]
29. Pandey, A.K.; Khan, A.I.; Abushark, Y.B.; Alam, M.M.; Agrawal, A.; Kumar, R.; Khan, R.A. Key issues in healthcare data integrity: Analysis and recommendations. *IEEE Access* **2020**, *8*, 40612–40628. [CrossRef]
30. Flux. The Decentralized Computational Network. Available online: https://fluxwhitepaper.app.runonflux.io/ (accessed on 13 February 2025).
31. Uddin, M.; Salah, K.; Jayaraman, R.; Pesic, S.; Ellahham, S. Blockchain for drug traceability: Architectures and open challenges. *Health Inform. J.* **2021**, *27*, 14604582211011228. [CrossRef]
32. Yu, J.; Zhang, X.; Wang, J.; Zhang, Y.; Shi, Y.; Su, L.; Zeng, L. Robust and trustworthy data sharing framework leveraging on-chain and off-chain collaboration. *Comput. Mater. Contin.* **2024**, *78*, 2159–2179. [CrossRef]
33. Sezer, B.B.; Topal, S.; Nuriyev, U. TPPSUPPLY: A traceable and privacy-preserving blockchain system architecture for the supply chain. *J. Inf. Secur. Appl.* **2022**, *66*, 103116. [CrossRef]
34. Hellani, H.; Sliman, L.; Samhat, A.E.; Exposito, E. On blockchain integration with supply chain: Overview on data transparency. *Logistics* **2021**, *5*, 46. [CrossRef]
35. Wu, L.; Lu, W.; Xue, F.; Li, X.; Zhao, R.; Tang, M. Linking permissioned blockchain to Internet of Things (IoT)-BIM platform for off-site production management in modular construction. *Comput. Ind.* **2022**, *135*, 103573. [CrossRef]
36. Jayabalan, J.; Jeyanthi, N. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *J. Parallel Distrib. Comput.* **2022**, *164*, 152–167. [CrossRef]
37. Tsang, Y.P.; Lee, C.K.M.; Zhang, K.; Wu, C.H.; Ip, W.H. On-chain and off-chain data management for blockchain-Internet of Things: A multi-agent deep reinforcement learning approach. *J. Grid Comput.* **2024**, *22*, 16. [CrossRef]
38. Hasan, H.R.; Salah, K.; Yaqoob, I.; Jayaraman, R.; Pesic, S.; Omar, M. Trustworthy IoT data streaming using blockchain and IPFS. *IEEE Access* **2022**, *10*, 17707–17721. [CrossRef]

39. Ali, M.S.; Vecchio, M.; Putra, G.D.; Kanhere, S.S.; Antonelli, F. A decentralized peer-to-peer remote health monitoring system. *Sensors* **2020**, *20*, 1656. [CrossRef]
40. Hu, V.C.; Kuhn, D.R.; Ferraiolo, D.F.; Voas, J. Attribute-based access control. *Computer* **2015**, *48*, 85–88. [CrossRef]
41. Sandhu, R.S. Role-based access control. *Adv. Comput.* **1998**, *46*, 237–286.
42. Khanna, A.; Sah, A.; Bolshev, V.; Burgio, A.; Panchenko, V.; Jasiński, M. Blockchain–cloud integration: A survey. *Sensors* **2022**, *22*, 5238. [CrossRef]
43. Liu, H.; Yang, B.; Xiong, X.; Zhu, S.; Chen, B.; Tolba, A.; Zhang, X. A financial management platform based on the integration of blockchain and supply chain. *Sensors* **2023**, *23*, 1497. [CrossRef]
44. Aftab, M.U.; Hamza, A.; Oluwasanmi, A.; Nie, X.; Sarfraz, M.S.; Shehzad, D.; Qin, Z.; Rafiq, A. Traditional and hybrid access control models: A detailed survey. *Secur. Commun. Netw.* **2022**, *2022*, 1560885. [CrossRef]
45. Ruj, S.; Stojmenovic, M.; Nayak, A. Decentralized access control with anonymous authentication of data stored in clouds. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *25*, 384–394. [CrossRef]
46. Liu, C.; Hou, C.; Jiang, T.; Ning, J.; Qiao, H.; Wu, Y. FACOS: Enabling privacy protection through fine-grained access control with on-chain and off-chain system. *IEEE Trans. Inf. Forensics Secur.* **2024**, *19*, 7060–7074. [CrossRef]
47. Zhang, Y.; Geng, H.; Su, L.; Lu, L. A blockchain-based efficient data integrity verification scheme in multi-cloud storage. *IEEE Access* **2022**, *10*, 105920–105929. [CrossRef]
48. Mohanta, B.K.; Awad, A.I.; Dehury, M.K.; Mohapatra, H.; Khan, M.K. Protecting IoT-Enabled Healthcare Data at the Edge: Integrating Blockchain, AES, and Off-Chain Decentralized Storage. *IEEE Internet Things J.* 2025, *in press*. [CrossRef]
49. Delgado-von-Eitzen, C.; Anido-Rifón, L.; Fernández-Iglesias, M.J. Blockchain applications in education: A systematic literature review. *Appl. Sci.* **2021**, *11*, 11811. [CrossRef]
50. Namane, S.; Ben Dhaou, I. Blockchain-based access control techniques for IoT applications. *Electronics* **2022**, *11*, 2225. [CrossRef]
51. Almarri, M.; Aljughaiman, A. Blockchain technology for IoT security and trust: A comprehensive SLR. *Sustainability* **2024**, *16*, 10177. [CrossRef]
52. Poon, J.; Buterin, V. Plasma: Scalable Autonomous Smart Contracts. 2017. Available online: https://www.plasma.io/plasma.pdf (accessed on 8 February 2025).
53. Chen, Z.; Gu, J.; Yan, H. HAE: A hybrid cryptographic algorithm for blockchain medical scenario applications. *Appl. Sci.* **2023**, *13*, 12163. [CrossRef]
54. Crosby, M.; Nachiappan; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain technology: Beyond bitcoin. *Appl. Innov. Rev.* **2016**, *2*, 6–19.
55. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where is current research on blockchain technology: A systematic review. *PLoS ONE* **2016**, *11*, e0163477. [CrossRef]
56. Ajayi, A.A.; Emmanuel, I.; Soyele, A.D.; Enyejo, J.O. Enhancing digital identity and financial security in decentralized finance (DeFi) through zero-knowledge proofs (ZKPs) and blockchain solutions for regulatory compliance and privacy. *Iconic Res. Eng. J.* **2024**, *8*, 373–394.
57. Xu, X.; Weber, I.M.; Staples, M. *Architecture for Blockchain Applications*, 1st ed.; Springer: Cham, Switzerland, 2019; pp. 1–307.
58. Yu, K.; Tan, L.; Yang, C.; Choo, K.-K.R.; Bashir, A.K.; Rodrigues, J.; Sato, T. A blockchain-based Shamir's threshold cryptography scheme for data protection in industrial internet of things settings. *IEEE Internet Things J.* **2022**, *9*, 8154–8167. [CrossRef]
59. Jose, J.T.; Anju, S. Threshold cryptography based secure access control for electronic medical record in an intensive care unit. *Int. J. Eng. Res. Technol.* **2013**, *2*, 457–464.
60. Jyoti, A.; Chauhan, R.K. A blockchain and smart contract-based data provenance collection and storing in cloud environment. *Wireless Netw.* **2022**, *28*, 1541–1562. [CrossRef]
61. Dwivedi, S.K.; Amin, R.; Vollala, S. Smart contract and IPFS-based trustworthy secure data storage and device authentication scheme in fog computing environment. *Peer-to-Peer Netw. Appl.* **2023**, *16*, 1–21. [CrossRef]
62. Ayub, M.; Saleem, T.; Janjua, M.U.; Ahmad, T. Storage State Analysis and Extraction of Ethereum Blockchain Smart Contracts. *ACM Trans. Softw. Eng. Methodol.* **2023**, *32*, 57. [CrossRef]
63. Khan, N.; Aljoaey, H.; Tabassum, M.; Farzamnia, A.; Sharma, T.; Tung, Y.H. Proposed model for secured data storage in decentralized cloud by blockchain Ethereum. *Electronics* **2022**, *11*, 3686. [CrossRef]
64. Williams, S.; Diordiiev, M. Arweave: The Permanent Information Storage Protocol. 2018. Available online: https://www.arweave.org/files/arweave-lightpaper.pdf (accessed on 8 February 2025).
65. Williams, S.; Diordiiev, M.; Berman, L.; Raybould, I.; Uemlianin, I. Arweave: A Protocol for Economically Sustainable Information Permanence. 2019. Available online: https://www.arweave.org/yellow-paper.pdf (accessed on 8 February 2025).
66. Frost, H. Incorporating Blockchain and Arweave Technologies into Archival Practices: An Exploration of the Rohingya Project's R-Archive. Ph.D. Thesis, University of California, Los Angeles, CA, USA, 2024.
67. Strehle, E.; Steinmetz, F. Dominating OP Returns: The Impact of Omni and Veriblock on Bitcoin. *J. Grid Comput.* **2020**, *18*, 575–592. [CrossRef]

68. Niu, Y.; Wei, L.; Zhang, C.; Liu, J.; Fang, Y. An anonymous and accountable authentication scheme for Wi-Fi hotspot access with the Bitcoin blockchain. In Proceedings of the 2017 IEEE/CIC International Conference on Communications in China (ICCC), Qingdao, China, 22–24 October 2017; pp. 617–622.
69. Zheng, P.; Zheng, Z.; Wu, J.; Dai, H.-N. XBlock-ETH: Extracting and Exploring Blockchain Data from Ethereum. *IEEE Open J. Comput. Soc.* **2020**, *1*, 95–106. [CrossRef]
70. Martha, G.I.R.; Prabowo, H.; Gaol, F.L.; Wiputra, R. Literature Review: Analysis of Essential Metadata Attributes of Digital Goods for Transaction in the Virtual World. In Proceedings of the 2024 International Conference on Information Management and Technology, Bali, Indonesia, 28–29 August 2024; IEEE: New York, NY, USA, 2024; pp. 299–304.
71. Li, W.; Feng, Y.; Liu, N.; Li, Y.; Fu, X.; Yu, Y. A secure and efficient log storage and query framework based on blockchain. *Comput. Netw.* **2024**, *252*, 110683. [CrossRef]
72. Di Ciccio, C.; Meroni, G.; Plebani, P. On the adoption of blockchain for business process monitoring. *Softw. Syst. Model.* **2022**, *21*, 915–937. [CrossRef]
73. Liu, Z.; Zhang, X.; Li, G.; Cui, H.; Wang, J.; Xiao, B. A Secure and Reliable Blockchain-based Audit Log System. In Proceedings of the ICC 2024 IEEE International Conference on Communications, Denver, CO, USA, 9–13 June 2024; pp. 2010–2015.
74. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform. 2014. Available online: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (accessed on 8 March 2025).
75. Sai, C.S.; Subramanian, N. Covert communication on IPFS using secured Filecoin-Slate blockchain. In Proceedings of the 2022 IEEE 19th India Council International Conference, Kochi, India, 24–26 November 2022; pp. 1–6.
76. Guidi, B.; Michienzi, A.; Ricci, L. Evaluating the decentralisation of Filecoin. In Proceedings of the 3rd International Workshop on Distributed Infrastructure for the Common Good, Quebec City, QC, Canada, 7 November 2022; pp. 13–18.
77. Jadhav, S.; Choudhari, G.; Bhavik, M.; Bura, R.; Bhosale, V. A Decentralized Document Storage Platform using IPFS with Enhanced Security. In Proceedings of the 2024 8th International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 23–24 August 2024; IEEE: New York, NY, USA, 2024; pp. 1–11.
78. Benet, J. IPFS-content addressed, versioned, p2p file system. *arXiv* **2014**, arXiv:1407.3561.
79. Wilkinson, S.; Boshevski, T.; Brandoff, J.; Buterin, V. Storj: A Peer-to-Peer Cloud Storage Network. 2014. Available online: https://storj.io/storjv2.pdf (accessed on 8 February 2025).
80. Vorick, D.; Champine, L. Sia: Simple Decentralized Storage. Nebulous Inc. 2014. Available online: https://sia.tech/sia.pdf (accessed on 8 February 2025).
81. Huang, H.-S.; Chang, T.-S.; Wu, J.-Y. A secure file sharing system based on IPFS and blockchain. In Proceedings of the International Electronics Communication Conference, Singapore, 8–10 July 2020; pp. 96–100.
82. Li, J.; Wu, J.; Jiang, G.; Srikanthan, T. Blockchain-based public auditing for big data in cloud storage. *Inf. Process. Manag.* **2020**, *57*, 102382. [CrossRef]
83. Mahalakshmi, K.; Kousalya, K.; Shekhar, H.; Thomas, A.K.; Bhagyalakshmi, L.; Suman, S.K.; Chandragandhi, S.; Bachanna, P.; Srihari, K.; Sundramurthy, V. Public auditing scheme for integrity verification in distributed cloud storage system. *Sci. Program.* **2021**, *2021*, 8533995. [CrossRef]
84. Chiniah, A.; Mungur, A. On the adoption of erasure code for cloud storage by major distributed storage systems. *EAI Endorsed Trans. Cloud Syst.* **2022**, *7*, e1. [CrossRef]
85. Nachiappan, R.; Calheiros, R.N.; Matawie, K.M.; Javadi, B. Optimized proactive recovery in erasure-coded cloud storage systems. *IEEE Access* **2023**, *11*, 38226–38239. [CrossRef]
86. Zhang, Q.; Zhao, Z. Distributed storage scheme for encryption speech data based on blockchain and IPFS. *J. Supercomput.* **2023**, *79*, 897–923. [CrossRef]
87. Tron, V.; Schonfeld, F. Swarm: The Decentralized Data Storage and Distribution Infrastructure for the Ethereum Web 3.0 Stack Whitepaper V0.3. 2019. Available online: https://www.ethswarm.org/The-Book-of-Swarm.pdf (accessed on 8 February 2025).
88. Niranjana, J.; Daniel, E.; Durga, S.; Kathiresan, V. Enhancing Storage Efficiency for Health Data Records through Block chain-Based Storj Mechanism. In Proceedings of the 2024 3rd International Conference on Intelligent Technologies, Control, Optimization, and Signal Processing, Krishnankoil, Tamil Nadu, India, 14–16 March 2024; IEEE: New York, NY, USA, 2024; pp. 1–7.
89. Lobo, P.A.; Sarasvathi, V. Distributed file storage model using IPFS and blockchain. In Proceedings of the 2021 2nd Global Conference for Advancement in Technology, Bangalore, India, 1–3 October 2021; IEEE: New York, NY, USA, 2021; pp. 1–6.
90. Kumar, R.; Marchang, N.; Tripathi, R. Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain. In Proceedings of the International Conference on Communication Systems and Network, Bengaluru, India, 7–11 January 2020; IEEE: New York, NY, USA, 2020; pp. 1–5.
91. Zhang, A.; Lin, X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *J. Med. Syst.* **2018**, *42*, 140. [CrossRef]

92. Shi, R.; Cheng, R.; Han, B.; Cheng, Y.; Chen, S. A Closer Look into IPFS: Accessibility, Content, and Performance. *Proc. ACM Meas. Anal. Comput. Syst.* **2024**, *8*, 20. [CrossRef]
93. Liu, Y.; Liang, C.; Mang, G.; Dong, Z. Blockchain-based spectrum sharing over 6G hybrid cloud. In Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC), Harbin City, China, 28 June–2 July 2021.
94. Bartolucci, S.; Caccioli, F.; Vivo, P. A percolation model for the emergence of the Bitcoin Lightning Network. *Sci. Rep.* **2020**, *10*, 4488. [CrossRef]
95. Gangwal, A.; Gangavalli, H.R.; Thirupathi, A. A survey of layer-two blockchain protocols. *arXiv* **2022**, arXiv:2204.08032. [CrossRef]
96. Negka, L.; Spathoulas, G.P. Blockchain state channels: A state of the art. *IEEE Access* **2021**, *9*, 160277–160298. [CrossRef]
97. Khan, D.; Jung, L.T.; Hashmani, M.A. Systematic literature review of challenges in blockchain scalability. *Appl. Sci.* **2021**, *11*, 9372. [CrossRef]
98. Gordon, W.J.; Catalini, C. Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 224–230. [CrossRef]
99. Tahir, N.U.A.; Rashid, U.; Hadi, H.J.; Ahmad, N.; Cao, Y.; Alshara, M.A.; Javed, Y. Blockchain-based healthcare records management framework: Enhancing security, privacy, and interoperability. *Technologies* **2024**, *12*, 168. [CrossRef]
100. Li, D.; Han, D.; Crespi, N.; Minerva, R.; Sun, Z. A blockchain-based secure storage and access control scheme for supply chain finance. *J. Supercomput.* **2023**, *79*, 109–138. [CrossRef]
101. Mishra, R.K.; Yadav, R.K.; Nath, P. Integration of Blockchain and IPFS: Healthcare data management & sharing for IoT Environment. *Multimed. Tools Appl.* **2024**, 1–22.
102. Ugochukwu, N.A.; Goyal, S.B.; Rajawat, A.S.; Islam, S.M.N.; He, J.; Aslam, M. An innovative blockchain-based secured logistics management architecture: Utilizing an RSA asymmetric encryption method. *Mathematics* **2022**, *10*, 4670. [CrossRef]
103. Hong, Y. New model of food supply chain finance based on the Internet of Things and blockchain. *Mob. Inf. Syst.* **2021**, 7589964. [CrossRef]
104. Karaszewski, R.; Modrzyński, P.; Modrzyńska, J. The use of blockchain technology in public sector entities management: An example of security and energy efficiency in cloud computing data processing. *Energies* **2021**, *14*, 1873. [CrossRef]
105. Khan, S.; Shael, M.; Majdalawieh, M.; Nizamuddin, N.; Nicho, M. Blockchain for governments: The case of the Dubai government. *Sustainability* **2022**, *14*, 6576. [CrossRef]
106. Manzoor, A.; Braeken, A.; Kanhere, S.S.; Ylianttila, M.; Liyanage, M. Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. *J. Netw. Comput. Appl.* **2021**, *176*, 102917. [CrossRef]
107. Golightly, L.; Modesti, P.; Garcia, R.; Chang, V. Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. *Cyber Secur. Appl.* **2023**, *1*, 100015. [CrossRef]
108. Chadwick, D.W.; Fan, W.; Costantino, G.; De Lemos, R.; Di Cerbo, F.; Herwono, I.; Manea, M.; Mori, P.; Sajjad, A.; Wang, X.S. A cloud-edge based data security architecture for sharing and analysing cyber threat information. *Future Gener. Comput. Syst.* **2020**, *102*, 710–722. [CrossRef]
109. Sun, X.; Yu, F.R.; Zhang, P.; Sun, Z.; Xie, W.; Peng, X. A survey on zero-knowledge proof in blockchain. *IEEE Netw.* **2021**, *35*, 198–205. [CrossRef]
110. Kumar, R.; Kumar, J.; Khan, A.A.; Zakria; Ali, H.; Bernard, C.M.; Khan, R.U.; Zeng, S. Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images. *Comput. Med. Imaging Graph.* **2022**, *102*, 102139. [CrossRef]
111. Punia, A.; Gulia, P.; Gill, N.S.; Ibeke, E.; Iwendi, C.; Shukla, P.K. A systematic review on blockchain-based access control systems in cloud environment. *J. Cloud Comput.* **2024**, *13*, 146. [CrossRef]
112. Li, S.; Chen, Y.; Chen, L.; Liao, J.; Kuang, C.; Li, K.; Liang, W.; Xiong, N. Post-quantum security: Opportunities and challenges. *Sensors* **2023**, *23*, 8744. [CrossRef]
113. Goint, M.; Bertelle, C.; Duvallet, C. Secure access control to data in off-chain storage in blockchain-based consent systems. *Mathematics* **2023**, *11*, 1592. [CrossRef]
114. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]
115. Zhou, L.; Diro, A.; Saini, A.; Kaisar, S.; Hiep, P.C. Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges, and opportunities. *J. Inf. Secur. Appl.* **2024**, *80*, 103678. [CrossRef]
116. Akter, S.; Reza, F.; Ahmed, M. Convergence of blockchain, k-medoids and homomorphic encryption for privacy preserving biomedical data classification. *Internet Things Cyber-Phys. Syst.* **2022**, *2*, 99–110. [CrossRef]
117. Pareek, N.K.; Patidar, V.; Sud, K.K. Image encryption using chaotic logistic map. *Image Vis. Comput.* **2006**, *24*, 926–934. [CrossRef]
118. Odeh, A.; Keshta, I.; Al-Haija, Q.A. Analysis of blockchain in the healthcare sector: Application and issues. *Symmetry* **2022**, *14*, 1760. [CrossRef]
119. Zheng, H.; You, L.; Hu, G. A novel insurance claim blockchain scheme based on zero-knowledge proof technology. *Comput. Commun.* **2022**, *195*, 207–216. [CrossRef]

120. Ali, A.; Al-rimy, B.A.S.; Alsubaei, F.S.; Almazroi, A.A.; Almazroi, A.A. HealthLock: Blockchain-based privacy preservation using homomorphic encryption in Internet of Things healthcare applications. *Sensors* **2023**, *23*, 6762. [CrossRef]
121. Mansoor, K.; Afzal, M.; Iqbal, W.; Abbas, Y. Securing the future: Exploring post-quantum cryptography for authentication and user privacy in IoT devices. *Clust. Comput.* **2025**, *28*, 93. [CrossRef]
122. Bisht, A.; Das, A.K.; Niyato, D.; Park, Y. Efficient Personal-Health-Records Sharing in Internet of Medical Things Using Searchable Symmetric Encryption, Blockchain, and IPFS. *IEEE Open J. Commun. Soc.* **2023**, *4*, 2225–2244. [CrossRef]
123. Steffen, S.; Bichsel, B.; Baumgartner, R.; Vechev, M. ZeeStar: Private smart contracts by homomorphic encryption and zero-knowledge proofs. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 22–26 May 2022.
124. Hossain, G.; Yarra, D. Learning blockchain technology in high school: Towards cybersecurity education. In Proceedings of the 2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2024.
125. Ali, A.; Pasha, M.F.; Guerrieri, A.; Guzzo, A.; Sun, X.; Saeed, A.; Hussain, A.; Fortino, G. A novel homomorphic encryption and consortium blockchain-based hybrid deep learning model for industrial internet of medical things. *IEEE Trans. Netw. Sci. Eng.* **2023**, *10*, 2402–2418. [CrossRef]
126. Reddy, B.; Madhushree; Aithal, P.S. Blockchain as a disruptive technology in healthcare and financial services: A review-based analysis on current implementations. *Int. J. Appl. Eng. Manag. Lett.* **2020**, *4*, 142–155.
127. Ma, S.; Zhang, X. Integrating blockchain and zk-rollup for efficient healthcare data privacy protection system via IPFS. *Sci. Rep.* **2024**, *14*, 11746. [CrossRef] [PubMed]
128. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef] [PubMed]
129. Shruti, S.; Alapatt, J.; George, J. MediCrypt: A model with symmetric encryption for blockchain-enabled healthcare data protection. In Proceedings of the 2024 IEEE International Conference on Contemporary Computing and Communications (InC4), Bangalore, India, 15–16 March 2024.
130. Sánchez Ortiz, A. Zero-Knowledge Proofs Applied to Finance. Master's Thesis, University of Twente, Enschede, The Netherlands, 2020.
131. Pan, R. The Performance Impact of Zero-Knowledge Proof on Blockchain Frameworks. Master's Thesis, University of Amsterdam, Amsterdam, The Netherlands, 2023.
132. Al-Aswad, M.A.; Hasan, R.; Elmedany, W.; Ali, M.; Balakrishna, C. Towards a blockchain-based zero-knowledge model for secure data sharing and access. In Proceedings of the 2019 IEEE 7th International Conference on Future Internet of Things and Cloud (FiCloud), Istanbul, Turkey, 26–28 August 2019; pp. 76–82.
133. Babu, B.; Jothi, K.R. A secure framework for privacy-preserving analytics in healthcare records using zero-knowledge proofs and blockchain in multi-tenant cloud environments. *IEEE Access* **2024**, *13*, 8439–8455. [CrossRef]
134. Aissaoua, H.; Laouid, A.; Kara, M.; Bounceur, A.; Hammoudeh, M.; Chait, K. Integrating homomorphic encryption in IoT healthcare blockchain systems. *Ingénierie Des Systèmes D'information* **2024**, *29*, 1667–1677. [CrossRef]
135. Reddi, S.; Rao, P.M.; Saraswathi, P.; Jangirala, S.; Das, A.K.; Jamal, S.S.; Park, Y. Privacy-preserving electronic medical record sharing for IoT-enabled healthcare system using fully homomorphic encryption, IOTA, and masked authenticated messaging. *IEEE Trans. Ind. Inform.* **2024**, *20*, 10802–10813. [CrossRef]
136. Vanin, F.N.d.S.; Policarpo, L.M.; Righi, R.d.R.; Heck, S.M.; da Silva, V.F.; Goldim, J.; da Costa, C.A. A blockchain-based end-to-end data protection model for personal health records sharing: A fully homomorphic encryption approach. *Sensors* **2023**, *23*, 14. [CrossRef]
137. Muazu, T.; Mao, Y.; Muhammad, A.U.; Ibrahim, M.; Kumshe, U.M.M.; Samuel, O. A federated learning system with data fusion for healthcare using multi-party computation and additive secret sharing. *Comput. Commun.* **2024**, *216*, 168–182. [CrossRef]
138. Olakanmi, O.O.; Odeyemi, K.O. Trust-aware and incentive-based offloading scheme for secure multi-party computation in Internet of Things. *Internet Things* **2022**, *19*, 100527. [CrossRef]
139. Li, W.; Yang, B.; Song, Y. Secure multi-party computing for financial sector based on blockchain. In Proceedings of the 2023 IEEE 14th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 17–18 October 2023.
140. Seo, M. Fair and secure multi-party computation with cheater detection. *Cryptography* **2021**, *5*, 19. [CrossRef]
141. Mansoor, K.; Afzal, M.; Iqbal, W.; Abbas, Y.; Mussiraliyeva, S.; Chehri, A. PQCAIE: Post-quantum cryptographic authentication scheme for IoT-based e-health systems. *Internet Things* **2024**, *27*, 101228. [CrossRef]
142. Csenkey, K.; Bindel, N. Post-quantum cryptographic assemblages and the governance of the quantum threat. *J. Cybersecur.* **2023**, *9*, tyad001. [CrossRef]
143. Bernstein, D.J.; Lange, T. Post-quantum cryptography. *Nature* **2017**, *549*, 188–194. [CrossRef] [PubMed]
144. Liu, Y.; Zhang, J.; Zhan, J. Privacy protection for fog computing and the internet of things data based on blockchain. *Clust. Comput.* **2021**, *24*, 1331–1345. [CrossRef]

145. Boumezbeur, I.; Zarour, K. Privacy preservation and access control for sharing electronic health records using blockchain technology. *Acta Inform. Pragensia* **2022**, *11*, 105–122. [CrossRef]
146. Kaur, M.; Gupta, S.; Kumar, D.; Verma, C.; Neagu, B.-C.; Raboaca, M.S. Delegated proof of accessibility (DPOAC): A novel consensus protocol for blockchain systems. *Mathematics* **2022**, *10*, 2336. [CrossRef]
147. Kuo, T.T.; Kim, H.E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* **2017**, *24*, 1211–1220. [CrossRef]
148. Chenthara, S.; Ahmed, K.; Wang, H.; Whittaker, F.; Chen, Z. Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *PLoS ONE* **2020**, *15*, e0243043. [CrossRef]
149. Sonkamble, R.G.; Bongale, A.M.; Phansalkar, S.; Sharma, A.; Rajput, S. Secure data transmission of electronic health records using blockchain technology. *Electronics* **2023**, *12*, 1015. [CrossRef]
150. Taherdoost, H. Privacy and security of blockchain in healthcare: Applications, challenges, and future perspectives. *Sci* **2023**, *5*, 41. [CrossRef]
151. Rizzardi, A.; Sicari, S.; Cevallos Moreno, J.F.; Coen-Porisini, A. IoT-driven blockchain to manage the healthcare supply chain and protect medical records. *Future Gener. Comput. Syst.* **2024**, *161*, 415–431. [CrossRef]
152. Amanat, A.; Rizwan, M.; Maple, C.; Zikria, Y.B.; Almadhor, A.S.; Kim, S.W. Blockchain and cloud computing-based secure electronic healthcare records storage and sharing. *Front. Public Health* **2022**, *10*, 938707. [CrossRef] [PubMed]
153. Helium Systems Inc. Helium: A Decentralized Wireless Network. Available online: http://whitepaper.helium.com/ (accessed on 13 February 2025).
154. Samarati, P.; De Vimercati, S.C. Access Control: Policies, Models, and Mechanisms. In *Foundations of Security Analysis and Design*; International School on Foundations of Security Analysis and Design; Springer: Berlin/Heidelberg, Germany, 2001; pp. 137–196.
155. Osborn, S.L. Role-based access control. In *Security, Privacy, and Trust in Modern Data Management*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 55–70.
156. Vandenwauver, M.; Govaerts, R.; Vandewalle, J. Role based access control in distributed systems. *Commun. Multimed. Secur.* **1997**, *3*, 169–177.
157. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 30 October–3 November 2006; pp. 89–98.
158. Nakamura, S.; Enokido, T.; Takizawa, M. Information flow control based on the CapBAC (capability-based access control) model in the IoT. *Int. J. Mob. Comput. Multimed. Commun.* **2019**, *10*, 13–25. [CrossRef]
159. Kumar, R.; Aljuhani, A.; Javeed, D.; Kumar, P.; Islam, S.; Islam, A.N. Digital Twins-enabled Zero Touch Network: A smart contract and explainable AI integrated cybersecurity framework. *Future Gener. Comput. Syst.* **2024**, *156*, 191–205. [CrossRef]
160. Malik, H.; Anees, T.; Faheem, M.; Chaudhry, M.U.; Ali, A.; Asghar, M.N. Blockchain and Internet of Things in smart cities and drug supply management: Open issues, opportunities, and future directions. *Internet Things* **2023**, *23*, 100860. [CrossRef]
161. Harris-Braun, E.; Luck, N.; Brock, A. Holochain: Scalable Agent-Centric Distributed Computing. 2018. Available online: https://www.holochain.org/documents/holochain-white-paper-alpha.pdf (accessed on 8 February 2025).
162. Ankr Network Whitepaper. Available online: https://www.ankr.com/ (accessed on 13 February 2025).
163. Alhaqbani, B.; Fidge, C. Access control requirements for processing electronic health records. In *Business Process Management Workshops: BPM 2007 International Workshops, BPI, BPD, CBP, ProHealth, RefMod, semantics4ws, Brisbane, Australia, September 24, 2007, Revised Selected Papers*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 371–382.
164. Yu, S.; Wang, C.; Ren, K.; Lou, W. Achieving secure, scalable, and fine-grained data access control in cloud computing. In Proceedings of the IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010; pp. 1–9.
165. Chen, C.; Wang, L.; Long, Y.; Luo, Y.; Chen, K. A blockchain-based dynamic and traceable data integrity verification scheme for smart homes. *J. Syst. Archit.* **2022**, *130*, 102677. [CrossRef]
166. Liu, X.; Shah, R.; Shandilya, A.; Shah, M.; Pandya, A. A systematic study on integrating blockchain in healthcare for electronic health record management and tracking medical supplies. *J. Clean. Prod.* **2024**, *447*, 141371. [CrossRef]
167. Sharma, V.; Ramirez-Asis, E.; Ahmad, A.J.; Silva-Zapata, M.; Alvarado-Tolentino, J.; Kumar, H.; Krah, D. On the Internet of Things, blockchain technology for supply chain management (IoT). *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9185731. [CrossRef]
168. Lopez, L.J.R.; Millan Mayorga, D.; Martinez Poveda, L.H.; Amaya, A.F.C.; Rojas Reales, W. Hybrid architectures used in the protection of large healthcare records based on cloud and blockchain integration: A review. *Computers* **2024**, *13*, 152. [CrossRef]
169. Han, G.; Ma, Y.; Zhang, Z.; Wang, Y. A hybrid blockchain-based solution for secure sharing of electronic medical record data. *PeerJ Comput. Sci.* **2025**, *11*, e2653. [CrossRef]
170. Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G.; Rosenbloom, S.T. FHIRChain: Applying blockchain to securely and scalably share clinical data. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 267–278. [CrossRef] [PubMed]
171. Guo, L.; Chen, J.; Li, S.; Li, Y.; Lu, J. A blockchain and IoT-based lightweight framework for enabling information transparency in supply chain finance. *Digit. Commun. Netw.* **2022**, *8*, 576–587. [CrossRef]

172. Ahmad, A.Y.A.B.; Verma, N.; Sarhan, N.M.; Awwad, E.M.; Arora, A.; Nyangaresi, V.O. An IoT and blockchain-based secure and transparent supply chain management framework in smart cities using optimal queue model. *IEEE Access* **2024**, *12*, 51752–51771. [CrossRef]
173. Mangala, N.; Naveen, D.R.; Reddy, B.E.; Buyya, R.; Venugopal, K.R.; Iyengar, S.S.; Patnaik, L.M. Secure pharmaceutical supply chain using blockchain in IoT cloud systems. *Internet Things* **2024**, *26*, 101215.
174. Awaji, B.; Solaiman, E. Design, implementation, and evaluation of blockchain-based trusted achievement record system for students in higher education. *arXiv* **2022**, arXiv:2204.12547.
175. Lykidis, I.; Drosatos, G.; Rantos, K. The use of blockchain technology in e-government services. *Computers* **2021**, *10*, 168. [CrossRef]
176. BitTorrent Foundation. BitTorrent-Chain Whitepaper (Version 1.0). 2021. Available online: https://resources.cryptocompare.com/asset-management/818/1671203800359.pdf (accessed on 8 February 2025).
177. Civic Whitepaper. Available online: https://www.allcryptowhitepapers.com/civic-whitepaper/ (accessed on 13 February 2025).
178. Ben-Sasson, E.; Chiesa, A.; Genkin, D.; Tromer, E.; Virza, M. SNARKs for C: Verifying program executions succinctly and in zero knowledge. In *Advances in Cryptology—CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2013, Proceedings, Part II*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 90–108.
179. Polkadot Whitepaper. Available online: https://polkadot.com/papers/ (accessed on 13 February 2025).
180. Cosmos Whitepaper. Available online: https://cosmos.network/whitepaper (accessed on 13 February 2025).
181. Axelar Whitepaper. Available online: https://www.axelar.network/whitepaper (accessed on 13 February 2025).
182. Bentayeb, Y.; Chaoui, K.; Badir, H. Integrating Blockchain and Edge Computing: A Systematic Analysis of Security, Efficiency, and Scalability. *Int. J. Adv. Comput. Sci. Appl.* **2025**, *16*, 622–627. [CrossRef]
183. Veeramachaneni, V. Edge Computing: Architecture, Applications, and Future Challenges in a Decentralized Era. *Recent Trends Comput. Graph. Multimed. Technol.* **2025**, *7*, 8–23.
184. Oliveira, M.; Chauhan, S.; Pereira, F.; Felgueiras, C.; Carvalho, D. Blockchain protocols and edge computing targeting industry 5.0 needs. *Sensors* **2023**, *23*, 9174. [CrossRef]
185. Hasnain, M.; Albogamy, F.R.; Alamri, S.S.; Ghani, I.; Mehboob, B. The Hyperledger Fabric as a blockchain framework preserves the security of electronic health records. *Front. Public Health* **2023**, *11*, 1272787. [CrossRef]
186. ZKsync Whitepaper. Available online: https://docs.zksync.io (accessed on 13 February 2025).
187. Starknet Whitepaper. Available online: https://docs.starknet.io (accessed on 13 February 2025).
188. Fetch.ai Whitepaper. Available online: https://fetch.ai/ (accessed on 13 February 2025).
189. Chainlink Whitepaper. Available online: https://chain.link/whitepaper (accessed on 13 February 2025).
190. IoTeX Whitepaper. Available online: https://docs.iotex.io/readme/whitepaper (accessed on 13 February 2025).
191. EigenLayer Whitepaper. Available online: https://docs.eigenlayer.xyz/ (accessed on 13 February 2025).
192. Al-Bassam, M. Lazyledger: A distributed data availability ledger with client-side smart contracts. *arXiv* **2019**, arXiv:1905.09274.
193. LayerZero Whitepaper. Available online: https://layerzero.network/publications/ (accessed on 13 February 2025).
194. Gupta, T.; Patel, H.B. Integrating Blockchain Technology with Internet of Things and Edge Computing to Achieve Security. *J. Ecohumanism* **2024**, *3*, 5127–5136. [CrossRef]
195. Rupanetti, D.; Kaabouch, N. Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities. *Appl. Sci.* **2024**, *14*, 7104. [CrossRef]
196. Bhuva, D.R.; Kumar, S. Securing space cognitive communication with blockchain. In Proceedings of the 2023 IEEE Cognitive Communications for Aerospace Applications Workshop (CCAAW), Cleveland, OH, USA, 20–22 June 2023; pp. 1–6.
197. Bhuva, D.R.; Kumar, S. A novel continuous authentication method using biometrics for IOT devices. *Internet Things* **2023**, *24*, 100927. [CrossRef]