


A Survey of Blockchain Applicability, Challenges, and Key Threats

Catalin Daniel Morar ^{1,*} and Daniela Elena Popescu ² 

¹ Department of Computers and Information Technology, Politehnica University of Timisoara, 2 V. Parvan Blvd, 300223 Timisoara, Romania

² Department of Computers and Information Technology, Faculty of Electrical Engineering and Information Technology, University of Oradea, 410087 Oradea, Romania; depopescu@uoradea.ro

* Correspondence: catalin-daniel.morar@student.upt.ro

Abstract: With its decentralized, immutable, and consensus-based validation features, blockchain technology has grown from early financial applications to a variety of different sectors. This paper aims to outline various applications of the blockchain, and systematically identify general challenges and key threats regarding its adoption. The challenges are organized into even broader groups, to allow a clear overview and identification of interconnected issues. Potential solutions are introduced into the discussion, addressing their possible ways of mitigating these challenges and their forward-looking effects in fostering the adoption of blockchain technology. The paper also highlights some potential directions for future research that may overcome these challenges to unlock further applications. More generally, the article attempts to describe the potential transformational implications of blockchain technology, through the manner in which it may contribute to the advancement of a diversity of industries.

Keywords: blockchain; blockchain applicability; blockchain challenges; smart contracts; security; privacy; IoT; AI



Citation: Morar, C.D.; Popescu, D.E. A Survey of Blockchain Applicability, Challenges, and Key Threats. *Computers* **2024**, *13*, 223. <https://doi.org/10.3390/computers13090223>

Academic Editor: Hamed Taherdoost

Received: 15 July 2024

Revised: 26 August 2024

Accepted: 4 September 2024

Published: 6 September 2024



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

1. Introduction

Blockchain has quickly turned out to be an integral part of a variety of fields; its characteristics include decentralization, immutability, and consensus-based validation processes; it was originally developed for cryptocurrencies like Bitcoin. Because of these characteristics, it has rapidly developed further into many fields and has provided widespread applications, all of which increase transparency, security, and trust without central authorities. Noted to have the ability to transform the existing business models and operations, it also provides a sound framework for integrity and data security in transactions [1].

Our motivation comes from the considerable number of advantages of and the increasing interest in blockchain technology, beyond the level of mere transactions. Figure 1 highlights the yearly evolution of published blockchain-related articles. Results shown in the figure are based on findings of article [2]. The authors of this paper gathered articles related to blockchain technology from IEEE, SPRINGER, ELSEVIER, and ACM publishers, from 2016 to 2022, outlining the considerable interest increasing in this technology over the years.

From this clear upward evolution of engagement in researching blockchain technology over time, we can conclude as a result of new approaches or solutions to existing issues that there is an increasing applicability in diverse domains.

The key contributions of this article are the following:

1. It emphasizes the different applications that have leveraged blockchain technology across diverse sectors and society in general, showing the main benefits and challenges;
2. It offers an identification of the main challenges, and key threats to blockchain technology adoption, and a broad categorization of the challenges, to deliver a clearer overview and better understanding;

3. It suggests possible solutions and future research directions for areas that need further exploration.

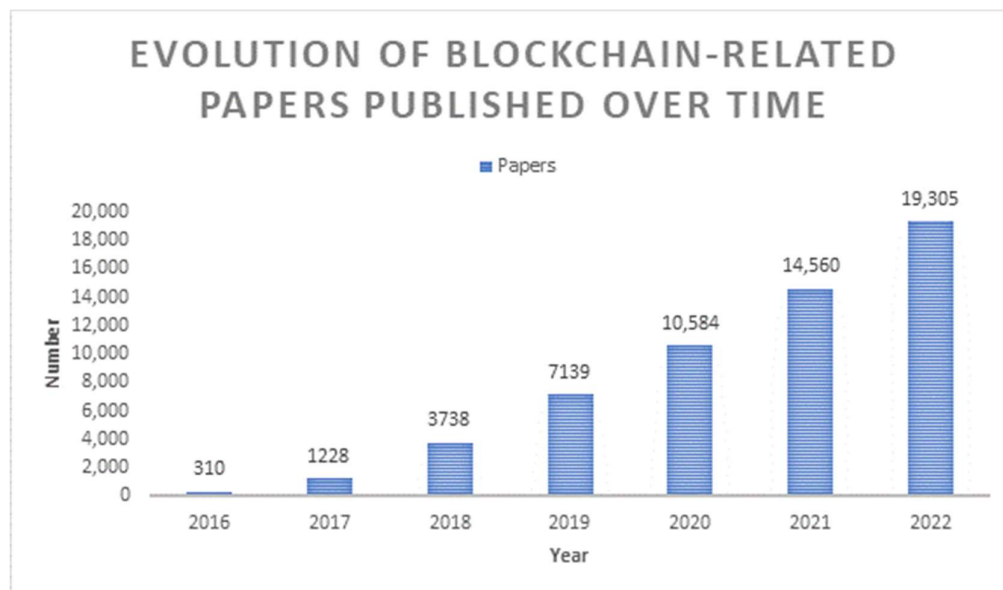


Figure 1. Evolution of blockchain-related papers published over time. Source: own illustration, based on the findings related to article [2].

In addition, compared to our survey, similar reviews focus on specific areas of applicability [3–5], solutions to challenges [6,7], security and privacy challenges [8,9], fewer areas of applicability, challenges, and solutions [10,11], similar areas of applicability but fewer technical details, challenges, and solutions [12–14], and more areas of applicability but fewer technical details, challenges, and solutions [15–17]. The review [18] employs a similar approach to our survey, in terms of the structuration of applicability domains, challenges, and possible solutions. However, our paper presents a larger number of applicability domains and highlights for each one a practical application that is functional in the real world at the time of writing this paper. In addition, the challenges and key threats are structured in broader challenge categories, which could offer a better visualization of interconnected issues.

The search for relevant studies in the literature was conducted in reputable databases: MDPI, IEEE Xplore, and Elsevier. Articles included in this review had to pass the exclusion and inclusion criteria outlined in Table 1.

Table 1. Exclusion and inclusion criteria for literature articles.

Exclusion Criteria	Inclusion Criteria
Older than five years Written in a different language than English	Addresses the applicability of blockchain technology
	Outlines the challenges that blockchain poses Proposes solutions for the blockchain issues

For the initial search of the literature, the following keys were used: blockchain, security issues, consensus, smart contract, interoperability, data storage, identity, and network. Figure 2 presents a detailed, step-by-step depiction of the literature-selection process. It highlights each stage, from the initial identification of articles to the final inclusion as initial resources. The selection of the articles during the initial search was conducted based on the title and abstract, which resulted in 123 selected articles. Exclusion criteria and duplicate removal led to 85 papers left. After the full-text review of these articles,

50 articles passed to inclusion criteria screening. In the end, 29 articles were selected as base resources, with “backward snowballing” and “forward snowballing” approaches applied to gather additional relevant sources.

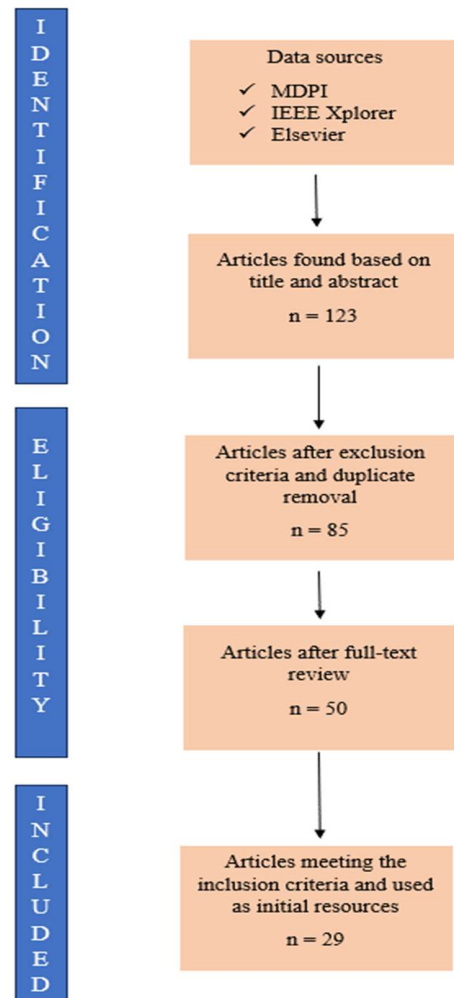


Figure 2. Resource-identification methodology.

The rest of the article is structured in such a way that the wide applicability of blockchain technology across multiple sectors is discussed in Section 2. This is then followed by an elaboration of challenges, key threats, and solutions in Section 3. In Sections 4 and 5, an outlook of the field of blockchain technology is given comprehensively, through the synthesis of the findings and some proposed future research directions.

2. Applicability

This section presents examples of areas for major characteristics of blockchain technology from the literature review are relevant, highlighting the discovered applicability, benefits, and one sector-related practical application. For clarity, the summary of the findings is presented in Table 2, arranged according to the number of references.

Table 2. Blockchain applicability.

Sector	Applicability	Benefits	Articles
IoT Environments	Decentralized, privacy-preserving, and fair data-management systems Governance mechanisms Blockchain-based authentication protocols	Enhanced security and privacy Efficient data management Improved transparency and governance Streamlined operations and infrastructure monitoring	[19–33]
Healthcare	Encrypted data sharing Decentralized systems for health data management	Improved data privacy and security Scalability and performance Enhanced interoperability of EHR	[23,27,29,32,34–37]
Cybersecurity and Data Management	ACE-BC framework Blockchain-based special key security model (BSKM) Integration with cloud computing Blockchain for IoT big data DAuth authentication system	Enhanced data integrity and security Increased performance metrics Cost reduction and efficiency	[12,24,31,32,38,39]
Supply Chain	Wine supply chain management	Improved efficiency Increased transparency Reduced operational costs Monitoring of greenhouse gas emissions	[21,27,29,32]
Smart Transportation	Bus transportation framework Blockchain with 5G for V2X communications	Enhanced management, efficiency, security, and data integrity Decentralized data storage	[22,29,30]
Education	Education data management	Decentralization Transparency and traceability Security and reliability	[40]
Digital and Financial Management	Digital currencies and cross-border transactions NFT marketplaces	Reduced transaction times and costs Increased security, reliability, and traceability	[32]
Internet of Drones	Robust authentication processes Decentralized data management	Enhanced privacy and security Secure data collection, transaction logging, and communication	[33]
Maritime Shipping	Blockchain-based JIT and green operation system	Improved efficiency and transparency in maritime operations Significant reduction in emissions	[41]
Distributed Agile Software Development	AgilePlus blockchain framework	Improved transparency and traceability Increased security Streamlined development processes	[42]

2.1. IoT Environments

IoT environments are emerging as a new area of technology development where the role of blockchain technology is very important in empowering the inherent decentralization and immutability features for better security and trust.

With time, technology such as blockchain in the IoT environment will greatly enhance the system's security, privacy, and data among the users. A model described in [19] has the potential to offer a decentralized and privacy-preserving fair transaction data system while emphasizing authentic data so that security issues do not crop up. The model leverages a consortium blockchain, facilitating end-to-end communication between IoT devices and reducing the risk of single-point failures. A consortium blockchain is a type

of blockchain operated by a group of entities, combining elements of public and private blockchains [43,44].

Figure 3 highlights the components of the model. Local differential privacy is a technique where the participants perturb their data with random noise before the actual sharing [45,46]. An adaptive local differential privacy algorithm called MDLDP is employed in the model to perturb the data before they are recorded to the blockchain, enhancing privacy by performing multiple perturbations on the dataset and selecting the result that offers the best privacy protection. Additionally, the participants have to pay a deposit, and are penalized in cases of dishonest behavior and rewarded if they act fairly. The combination of verifiable encrypted signatures and threshold signature techniques empowers the arbitration committee to effectively manage disputes in the data-transaction process. Verifiable encrypted signatures allow a signer to encrypt their digital signature with a third party's public key, ensuring that only the third party can decrypt it to enforce the transaction if needed [47,48], while the threshold signature technique allows a subgroup of a group of participants to jointly produce a digital signature [49,50]. Despite the visible benefits of the model in terms of privacy and dispute resolution, it depends on the honesty and maximum availability of committee members to avoid unfair behavior among the participants and transaction delays. Furthermore, cryptographic operations could be resource-intensive.

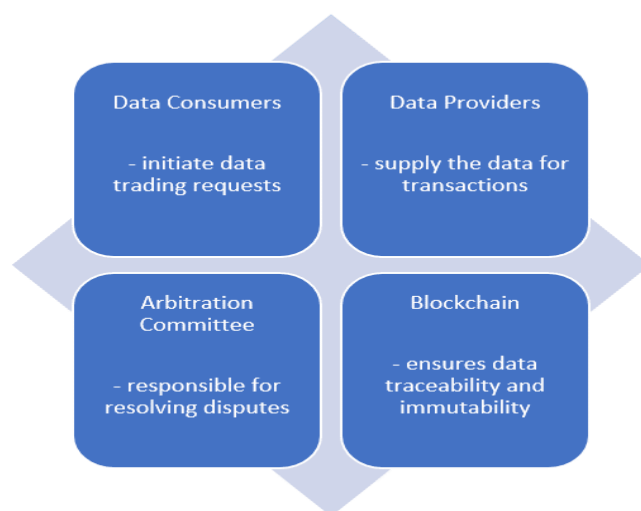


Figure 3. Components of the model proposed in the article [19].

In [20], the governance mechanism used the technology of blockchain and smart contracts to manage the logistics of IoT in a way that is flexible and reliable, thus helping in linking the planning, execution, and monitoring of infrastructure effectively. The approach uses a blockchain-enabled six-layer IoT architecture, as presented in Figure 4.

The Blockchain Layer serves as the intermediary between the Network and Middleware Layers, ensuring immutability, traceability, and automation of the execution of rules. The article emphasizes the usage of permissioned blockchain and cryptographic mechanisms, such as k-anonymity, ring signatures, secure multi-party computation, homomorphic encryption, Zero-Knowledge Proof, and data obfuscation, which can enhance the level of privacy and anonymity [51]. The model leverages a variable geometry approach that allows flexible participation and varying levels of commitment among stakeholders, facilitating proper cooperation [52]. For the testing of the model, the authors implemented a two-node Ethereum blockchain and the voting mechanism written in Solidity, along with the usage of Raspberry Pi to simulate IoT devices, in a Smart Logistic scenario. However, while the test demonstrates the feasibility of the model, it is insufficient in demonstrating practical effectiveness and efficiency.

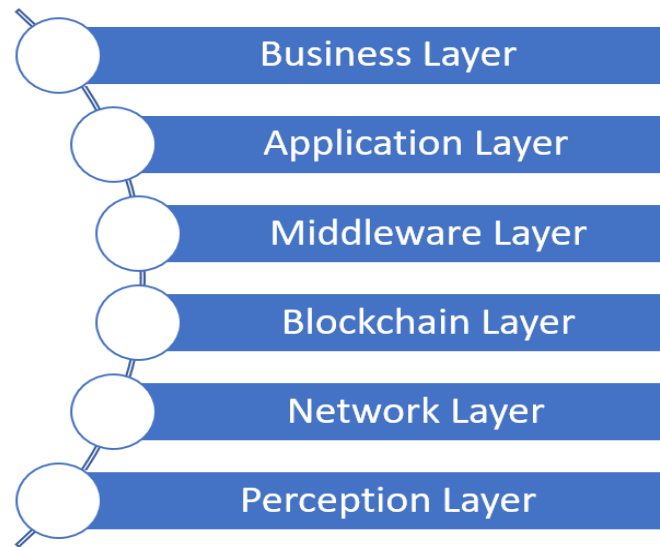


Figure 4. Components of the model proposed in the article [20].

In [25], a new authentication protocol based on a blockchain for wireless sensor networks uses Proof of Authentication (PoAh) to cover the whole process from different kinds of security threats, including the process requirements for energy consumption and delay. The Proof of Authentication consensus mechanism is designed for lightweight blockchains in resource-constrained environments, by utilizing trusted nodes to authenticate transactions through asymmetric cryptography [53,54]. This research highlights the benefits of using private blockchain structures for an application that has high-security needs besides needing to manage the network efficiently. The private blockchain is a type of blockchain controlled by a single entity, where access is restricted to authorized participants [26,55].

According to the authors, four primary actors are engaged in the model: Sensor Nodes, Cluster Nodes, Base Station, and User. Figure 5 highlights the methods of communication of the model: SN–CN, CN–BS/BCN, and U–BS/BCN. The communication is bidirectional and the data are stored at the BS level to address the storage limitations of SNs and CNs. While there are many benefits in terms of security and privacy, the result of the analysis showcases that the proposed model increases latency and energy consumption compared to the traditional solution. Additionally, the solution is compared against two other works, which may not provide a comprehensive view, and the reliance on the base station for blockchain storage could introduce a single point of failure.

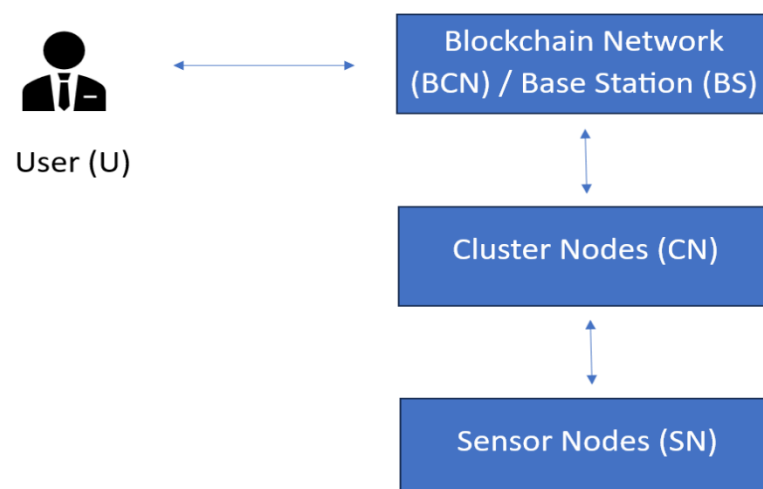


Figure 5. Components of the model proposed in the article [25].

The study of the state-of-the-art blockchain solutions meant for strengthening the security and privacy of IoT is encapsulated in a systematic review in [26], where several blockchain-based solutions addressing security and privacy in IoT are highlighted, most studies recommend private configurations of blockchains because they have enhanced control and security features. However, there are still challenges such as integration complexity, energy consumption, and security concerns. Finally, ref. [28] placed emphasis on deploying the blockchain as a safe and resilient solution for decentralized data management in IoT, with the focus on reducing security challenges by enabling transparency and governance capabilities in IoT networks. Furthermore, it also critiqued potential vulnerabilities, such as those seen in the DAO attack [56], and addressed challenges related to scalability and energy consumption. Similarly, the potential for integrating blockchain technology within the IoT ecosystem is underscored in [21–24,27,29–33].

These together not only prove the crucial role of blockchain technology in advancing IoT applications but also assure a security framework, preserve privacy, and maintain an efficient way to manage the system. Nevertheless, scalability, energy consumption, and integration complexity are still open concerns for this domain, leaving open doors for further improvements.

Practical application: IOTA is a distributed ledger technology that uses a unique architecture called Tangle to facilitate secure, feeless transactions and data transfers, making it particularly suitable for applications like the Internet of Things [57].

2.2. Healthcare

Healthcare is one of the most challenging environments due to such things as the sensitive protection of patients' data and interoperability between a large number of healthcare systems. Blockchain technology is offering very promising security solutions, and the decentralized nature can improve data privacy and operational efficiency.

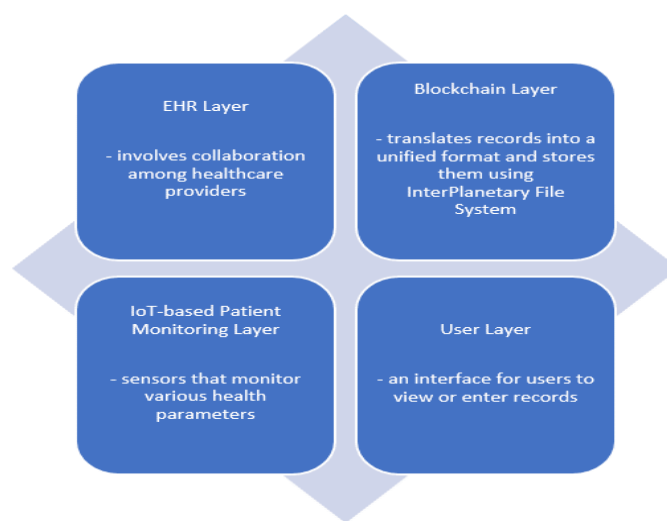
Examples of such solutions, based on blockchain, include Redact-Chain for Health [34]. It introduces the possibility of sharing encrypted data with features like chameleon hash and distributed trapdoor management, focusing on the protection of patient privacy and secured access to the data. The chameleon hash function is employed to enable fine-grained data editing on the blockchain, allowing transactions to be modified without altering the overall hash value of the blockchain [58,59]. Shamir's Secret Sharing scheme is leveraged for trapdoor management, which is a cryptographic method that divides a secret into multiple parts among the participants [50,60]. Along with the chameleon hash function, a symmetric encryption-based authentication algorithm is leveraged to protect against cyberattacks and to ensure the authenticity of user identities.

Table 3 highlights the participants and corresponding responsibilities in the proposed model. Additionally, the solution employed two main components: the redactable blockchain and the InterPlanetary File System (IPFS). The redactable blockchain is used to store sections of patients' EHRs, while the InterPlanetary File System is employed to store comprehensive EHRs. The model proposed by the authors has the potential to enhance the EHR systems in terms of decentralized data management. However, due to the need for decentralized coordination and trapdoor management, the system could bring additional complexity and security issues.

On the other hand, IoT and blockchain [23] have also been used as yet another way to optimize the security of, and integration with, EHRs using the Proof of Trust (PoT) consensus mechanism, which enhances blockchain security and efficiency by selecting validators based on trustworthiness, based on historical interactions, rather than computational power or wealth [61]. Additionally, the InterPlanetary File System (IPFS) is used to optimize the effective storage of data. The proposed model includes the components described in Figure 6.

Table 3. Participants of the model described in the article [34].

Participant	Responsibility
Administrator	Initializes the redactable blockchain network and establishes the key-generation center and verification institution
Verification Institution	Registers and verifies the identities of medical institutions and patients
Key Generation Center	Produces and distributes trapdoors and authentication keys to medical institutions
Medical Institutions	Provides medical services and manages information within the RCH network
Patients	Participates in the data-sharing scheme and collaborates with medical institutions to modify their EHRs

**Figure 6.** Components of the model proposed in the article [23].

The Elliptic Curve Cryptography method is emphasized in the article, which offers enhanced security with smaller sizes compared to traditional algorithms like RSA, making it suitable for resource-constrained environments [62,63]. Despite the potential benefits of the proposed solution, as the authors underscore, the following challenges still present an impediment: resource constraints, bandwidth constraints, connectivity constraints, memory constraints, and GDPR compliance.

Another exploration includes a decentralized system [35] that assures scalable and secured data transactions with a guarantee of privacy, integrity, and availability of data through sophisticated access control mechanisms. This framework leverages the Proof of Work (PoW) consensus mechanism, with a feature that automatically adjusts the number of nodes based on the new participants in the network, thus enhancing the scalability. However, energy consumption might pose an issue, as the Proof of Work mechanism requires miners to solve computationally intensive puzzles to validate a transaction [64,65]. Figure 7 presents the components of the proposed model: healthcare providers and consultants, registration control process, data access control, and digital human healthcare. Data integrity is maintained using SHA-256 hashing, which is a function that produces a 256-bit fixed-length hash value from input data [66,67]. At the same time, privacy is enhanced by RSA encryption, which is an asymmetric cryptographic algorithm that uses a pair of keys: a public key for encryption and a private key for decryption [68,69]. Regardless of privacy and security benefits, the proposed model might suffer from energy consumption and latency, a faster and low-resource-consumption consensus mechanism such as Proof of Stake or Proof of Trust represents a starting point for further improvements.

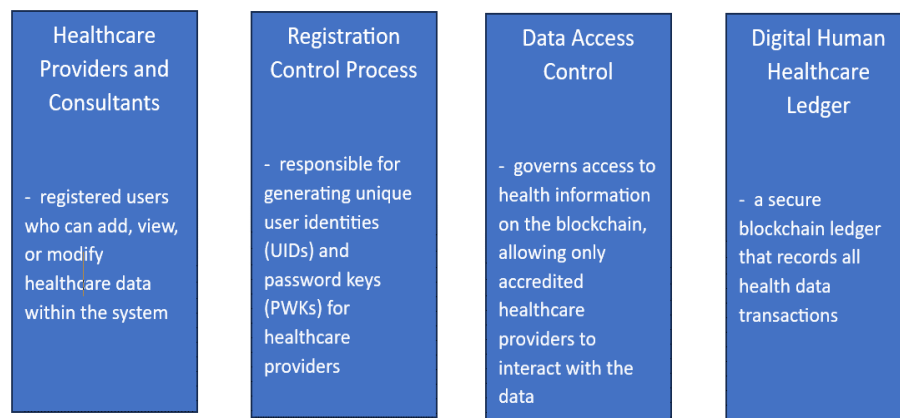


Figure 7. Components of the model proposed in the article [35].

Furthermore, the systematic review [36] suggested that since blockchain technology can advance the interoperability of EHR, it will be one of the contributing factors in securing big healthcare data sharing. It also highlights the benefits of federated learning, such as data privacy preservation, collaborative model training, decentralized data management, improved scalability and efficiency, and compliance with data regulations [37,70].

Articles [27,29,32] are other studies that mention the healthcare applicability of blockchain technology.

These applications highlight blockchain's potential to enhance system security, ensure data privacy, and improve interoperability in healthcare. However, integrating blockchain technology may introduce additional complexity, and increase energy consumption and latency.

Practical application: Solve.Care is a platform that improves the coordination, transparency, and efficiency of healthcare services, by utilizing a decentralized system to securely manage and share health information [71].

2.3. Cybersecurity and Data Management

In the area of cyber security and data management, problems like data breaches, unauthorized access, and non-transparency in recording transactions are very common. Blockchain technology could help by providing immutable, transparent, and secure data-storage solutions, ensuring data integrity and enhancing trust.

The ACE-BC [24] framework exploits the blockchain to enhance data security and privacy. It is an approach to providing enforcement mechanisms in information sharing using attribute-based encryption, which ensures that only users with appropriate attributes can decrypt and access specific data, thus providing secure and flexible access control [72,73]. This resulted in increases in performance metrics, like throughput and data confidentiality, and mitigated the issue of the single points of failure posing risks to centralized systems.

The components and corresponding responsibilities of the proposed model are highlighted in Table 4. The experimental results highlighted by the authors illustrated that the ACE-BC framework significantly enhanced data confidentiality, throughput, efficiency, and reduced latency compared to other models. However, the complexity of implementing and managing attribute-based encryption, and the resource-intensive nature of the system may limit its practical adoption.

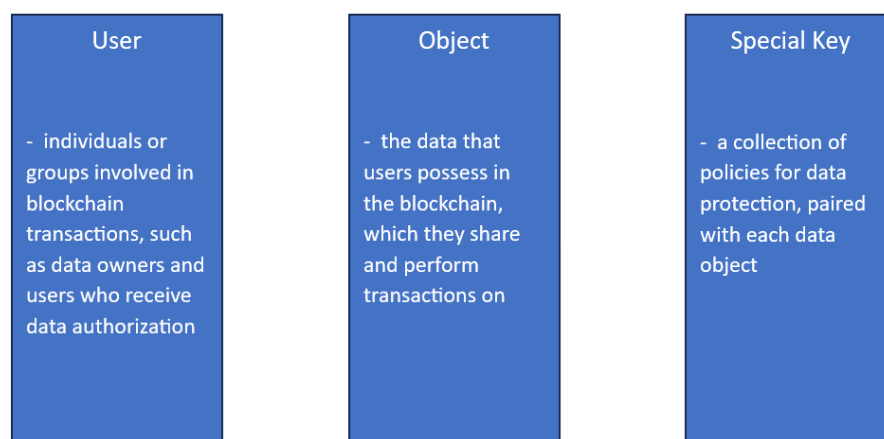
The merging of the blockchain with cloud computing opens doors for robust solutions that better the data security system, hence reducing the cost of breaches and better control of user access [12]. However, scalability issues and energy-consumption concerns have to be taken into consideration, thus exploring different types of solutions that fit the system requirements.

Table 4. Components of the model highlighted in the article [24].

Component	Responsibility
Edge Gateways	The interface between IoT devices and the blockchain network
5G Base Station	Provides fast connection between edge gateways and cloud
Certificate Authority	Provides permission to edge gateways to join the blockchain
Blockchain Network	Consortium blockchain, used for decentralized storage and access control

The Blockchain-based Special Key Security Model (BSKM) [38] is proposed for addressing challenges such as scalability and transaction speed in large-scale data. The model provides efficient and dynamic access control using special keys. These special keys are a collection of policies paired with a data object, employed for the protection of the data. Each owner of the data object can define or modify their security policies. Additionally, a path-compression algorithm is leveraged, which is used to shorten data access paths in a blockchain by updating node references to point directly to the current data location, thereby enhancing retrieval speed and reducing access costs [74].

Figure 8 outlines the components of the proposed model. The tests conducted on the model reveal enhanced performance and efficiency. However, although the tests were conducted on a large dataset, the scalability of the model, considering that the network size and transaction volume increase over time, has not been thoroughly explored, similar to the computational overhead that might be introduced by the path-compression algorithm.

**Figure 8.** Components of the model proposed in the article [38].

On the other hand, the use of blockchain in IoT big data management [31] involves highly sophisticated security measures, through fragmentation and encryption techniques, while at the same time allowing for a blockchain-based access control mechanism. Fragmentation is the technique of dividing information into smaller, separate pieces called fragments, making it difficult for unauthorized users to gain access to complete information [75,76]. In the proposed framework, fragmentation is employed based on sensitivity level, which is determined by the data owner, and the Mapping Array necessary for reconstruction is stored in the blockchain, at the metadata level. For highly sensitive data, the AES encryption standard [77] is used along with fragmentation.

Table 5 highlights the main entities and corresponding responsibilities of the proposed framework. The experiments conducted by the authors demonstrate that the proposed model could enhance big data security with acceptable performance overhead. However, the framework might not be well-suited for applications requiring real-time processing due to the added latency, and dependency on the data owner's sensitivity assessment could lead to unnecessary overhead if the sensitivity level is not determined correctly. Additionally, although the framework scales well with increasing data size in the tested range, it is not

clear how it performs with extremely large data volumes. Blockchain’s relevance in this domain is also noted in [32].

Table 5. Entities of the model outlined in the article [31].

Entity	Responsibility
Data Owner	Owns and controls access to the data
User	Requests access to data with granted authorization
Blockchain-based Security Manager	Manages blockchain operations and ensures event authenticity
Big Data Distributed Storage	Responsible for storing fragmented and encrypted data
Blockchain	Stores metadata and permission lists to ensure tamper resistance and audibility

In [39], the authors present DAAuth, a decentralized web authentication system that leverages the Ethereum blockchain as a secure alternative to OAuth 2.0. The model employs smart contract functionality and user signatures to achieve the authentication process. Figure 9 represents the architecture of the proposed model.

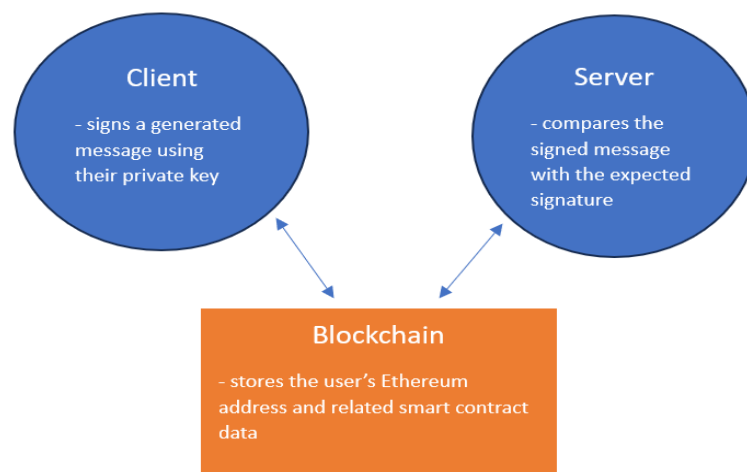


Figure 9. The architecture of the model proposed in the article [39].

Despite the benefits of such an approach as the DAAuth model, it might face adoption challenges and additional costs, due to poor user experience—especially for users that are not familiar with the blockchain context—and gas fees, respectively.

These applications of blockchain technology in this sector have massive improvements in how the data are managed and safeguarded, guaranteeing high integrity and reliability at large in cybersecurity and data management. However, scalability issues and overhead for large data volumes, along with integration and management complexity, are concerns that have to be taken into consideration.

Practical application: Acronis offers complete cybersecurity solutions, utilizing advanced technologies such as blockchain, to ensure the authenticity and integrity of stored data [78].

2.4. Supply Chain

Transparency, inefficiency in tracking the goods, and susceptibility to fraud and counterfeits are the main challenges of the supply chain. Blockchain technology, through the use of a tamper-proof decentralized ledger, can bring in an improvement that will strengthen the process of tracking, hence making it more traceable and accountable across the whole supply chain.

The inclusion of blockchain in IoT and AI of the wine supply chain [21] brings several improvements such as enhanced efficiency, transparency, and a decrease in operational

costs. In addition, it can monitor greenhouse gas emissions, which is beneficial with respect to environmental sustainability efforts. Accordingly, deploying such technologies provides a fair competitive environment and sets a transparent marketplace for any consumer to verify confidently whether a product is the original one or its quality. The components of the model are highlighted in Figure 10.

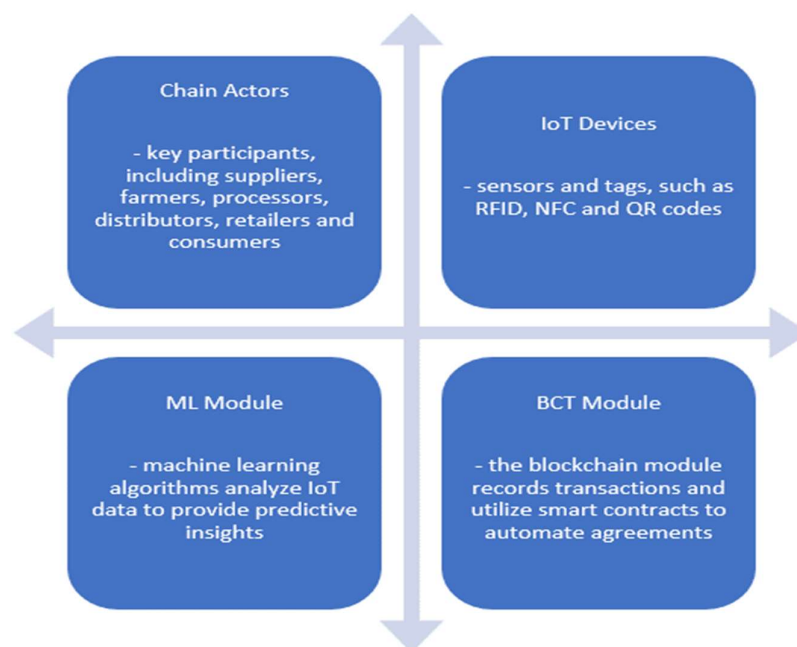


Figure 10. Components of the model proposed in the article [21].

The authors emphasize the usage of consortium blockchain, along with smart contracts, which are self-executing contracts with the terms of the agreement directly written into the code, executed automatically without the need for intermediaries [79,80]. In spite of the theoretical benefits outlined in the study, it lacks empirical tests and in-depth technical details of the proposed framework.

Articles [27,29,32] also underscored the integrative potential of blockchain technology in this sphere.

These comprehensive methods point towards the potential for blockchain technology to truly revolutionize supply chain management, thereby improving transparency, efficiency, and trust among the shareholders. However, in-depth analysis of technical details and empirical tests are a must to balance the disadvantages and benefits of such integration.

Practical application: IBM Food Trust is a blockchain-based supply chain solution that enhances traceability in the food sector. It allows all parties involved to securely access and share data regarding the origin, processing, and distribution of food products [81].

2.5. Smart Transportation

The smart transportation sector is increasingly facing challenges with its data security, privacy, and operations conducted across complexly growing networks. This is where blockchain technology provides assistance, in the form of secure and decentralized vehicle-to-everything (V2X) communication solutions that boost the integrity, transparency, and traceability of the data-flow process while guaranteeing more reliable transactions and coordination among various stakeholders within the transportation ecosystem.

The use of the blockchain in the bus transportation framework [22] incredibly improves management, efficiency, and security. In so doing, the system reduces the risks associated with fake data presentations and guarantees correct records, hence even enhancing dependability to improve systems in urban transportation. The architecture has been worked on with Ethereum's main net blockchain and the Aurora test network, for experi-

mental comparisons, highlighting that storing heavy data, like photos and documents, on decentralized storage items like IPFS [82], has many benefits. The architecture emphasized by the authors is highlighted in Table 6.

Table 6. The architectural components of the model outlined in the article [22].

Entity	Responsibility
HTTP Browser Layer	Users interact with the system via a web browser
User Interface Layer	The intuitive web interface for users
Business Logic Layer	Handles business logic through smart contracts
Data Access Layer	Ensures decentralized and secure data storage through IPFS

The authors tested the proposed framework using techniques such as the stochastic algorithm to analyze time complexity and optimization solutions [83,84], and DEMATEL for the identification and evaluation of critical factors [85]. However, a more comprehensive exploration of critical factors and a broader range of performance metrics would strengthen the findings and applicability.

Additionally, ref. [30] argues that 5G and future advanced communication systems are key enabling technologies in supporting the further move forward of vehicle-to-everything communications. It firmly supports the concept of Intelligent Transportation Systems (ITSs) employing enhanced road safety, efficiency of traffic, and user experiences, based on storage that can be relied upon. Blockchain systems will therefore perfectly contribute to technologies on advanced traffic management and autonomous driving, ensuring, amongst other aspects, the secure management of huge volumes of data that will be involved in those areas. The authors emphasized the generic architecture detailed in [86] and a permissioned blockchain to control access to information [87]. The authors outline the benefits of symmetric-key cryptography as a more resource-efficient alternative for ensuring data confidentiality [88], while for the authentication schema, mentioned techniques such as RSA-based public key cryptosystem [89], SHA [90], AES [91], and ECC [92] are better options. However, the article lacks in-depth technical explorations, such as hardware limitations, and network-integration complexities. Blockchain technology advantages in this area are also referenced in [29].

All these applications show how blockchain technology could solve important problems pertinent to the smart transportation domain, and increase system reliability, security, and efficiency while paving the way for next-generation transportation systems. Despite these advantages, comprehensive exploration of critical factors and in-depth technical analysis are encouraged to employ the best techniques and solutions.

Practical application: Mobi is a consortium of companies that leverages blockchain technology to develop a new economy of movement, focusing on smart transportation solutions [93].

2.6. Education

The challenges faced by the education sector include the maintenance of integrity, secure storage of sensitive students' data, and ease in transferring credits between institutions. These problems could be assisted with the help of blockchain technology, which has the potential to deliver a secure, immutable, and transparent solution for records' issuance and storage.

The study [40] highlights the application of blockchain in this area and identifies inherent advantages such as decentralization, transparency, traceability, security, and reliability that come with the usage of blockchain technology. These qualities, therefore, portend better management in the realm of educational records, verification of credentials, and security of the data environment within academic institutions. Different types of blockchains are highlighted for their usability in this domain, such as Hyperledger

Fabric [94], Ethereum [95], and Stellar [96], with corresponding limitations. Ring signatures, secure multi-party computation, commitment schemes, zkSNARK, homomorphic encryption, and zero-knowledge proofs are addressed for enhanced privacy [97].

The article concludes that the main focus regarding the challenges faced by the integration of blockchain technology in this domain is the technological one, as shown in Figure 11, which might represent a gap for broader adoption in real use cases, as the environmental and organizational challenges are also of high importance. However, the study could benefit from a more balanced analysis by including detailed case studies and more in-depth technical information.

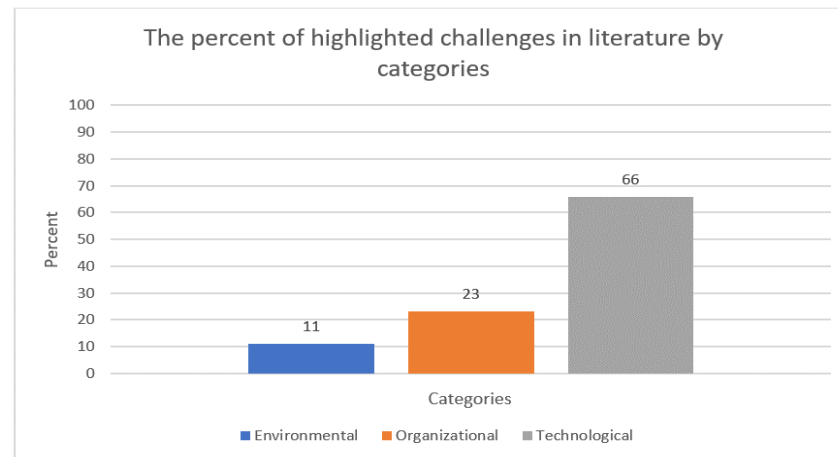


Figure 11. The percent of highlighted challenges in the education domain. Own illustration, based on the results from [40].

Practical application: Blockcerts is a blockchain-based open-source project that allows participants to receive and share their diplomas and other documents in a secure and verifiable manner, ensuring the authenticity and integrity of their achievements [98].

2.7. Digital and Financial Management

In this century of digital and financial management, there are tremendous grave challenges of fraud, inefficiency in transaction processes, and data integrity and transparency failures. Blockchain technology provides a decentralized ledger that might help improve transparency and reduce fraud through its immutable record-keeping.

As stated in [32], blockchain revolutionizes this area in various ways that enable the use of digital currencies and transformation to work efficiently even across national borders. These are adaptations that aim to reduce operational time and costs. The authors present a generic blockchain architecture, composed of the components presented in Table 7.

Table 7. Components of the generic blockchain architecture presented in [32].

Component	Functionality
Nodes/Users	Transaction requesters and receivers. They maintain a copy of the entire blockchain ledger [99]
Miners	Nodes that have the ability to add new blocks to the blockchain. Responsible for validating and verifying transactions [100]
Blocks	A fundamental unit of the blockchain, representing transaction details [101]
Verification Mechanism	Involves two steps verification, using a smart contract [102] and a consensus mechanism [103]

In addition to financial management, other applications are highlighted related to digital and financial management, such as NFT marketplaces. An NFT is a unique digital asset stored on a blockchain that represents ownership or proof of authenticity of a specific

item [104]. Notwithstanding different operational and interoperability issues outlined, the article lacks in-depth specific case studies and results that could substantiate the claims.

Practical application: Ripple is the company behind the XRP Ledger, a blockchain solution used to facilitate fast and low-cost international payments. It ensures transparency, security, and efficiency in financial transactions, providing a reliable solution for cross-border transfers [105].

2.8. Internet of Drones

Security challenges faced in the field of the Internet of Drones (IoD) have been well addressed by blockchain technology, as described in ref. [33]. The very first challenge laid down is the openness of IoD, which is quite prone to risks like interception, manipulation, or unauthorized access to data. Blockchain enhances communication between drones and ground stations, allowing for strong procedures of authentication and ensuring that the collected data and transactions are effectively logged. The main types of IoD blockchain-powered schemes outlined by the authors are shown in Figure 12. They are as follows: Blockchain-Powered Access Control or Authentication [106,107], Blockchain-Powered Architecture/Framework [108–111], Blockchain-Powered Data Management [112–115], and Blockchain-Powered Autonomous IoD [116–118]. The article mentions Elliptic Curve Cryptography and Attribute-Based Encryption as examples of encryption algorithms. Despite the benefits, challenges, and future directions outlined by the authors, a more in-depth technical analysis of the solutions and empirical tests could strengthen the results.

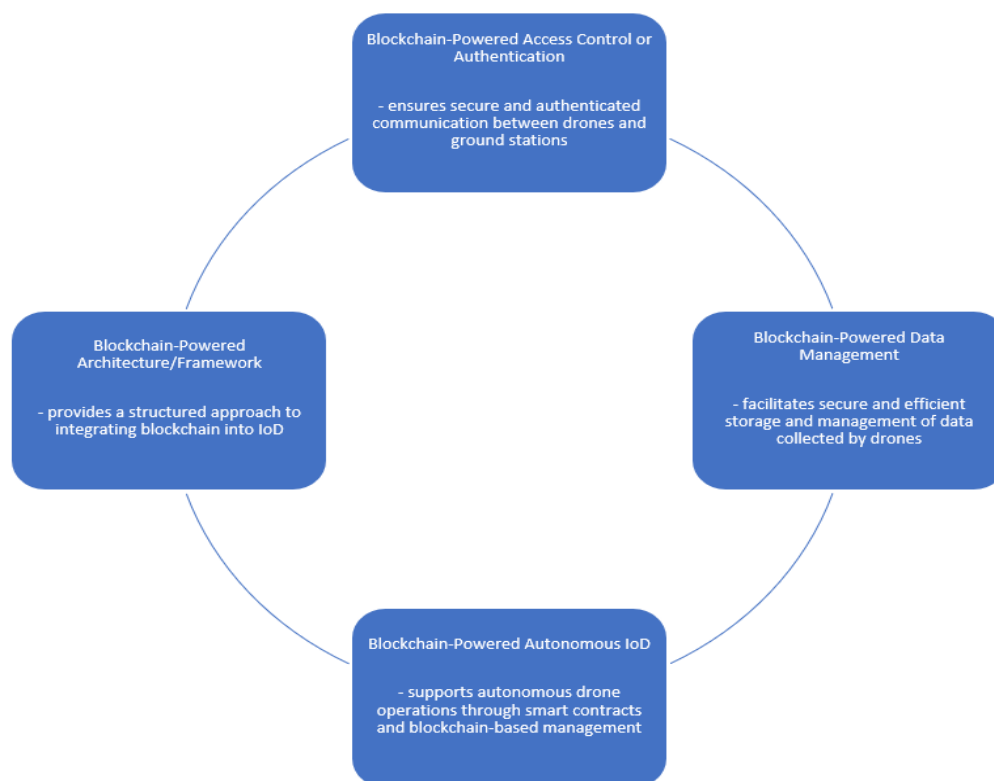


Figure 12. The types of IoD blockchain-powered schemes described in [33].

Practical application: SkyGrid is a platform that uses blockchain technology to manage drone traffic and ensure safe and efficient airspace. By integrating advanced technologies, SkyGrid enhances the transparency, security, and coordination of drone operations [119].

2.9. Maritime Shipping

As for maritime shipping, this sector faces huge challenges, among which are inefficiency in logistics, lack of clear visibility for cargo tracking, difficulty in compliance, and documentation management. Blockchain technology offers an immutable ledger, thus enhancing transparency and traceability in cargo movements.

Study [41] exemplifies a system using blockchain technology to incentivize Just in Time (JIT) and green operations within maritime shipping. This system carried out in the Solana blockchain [120] at the Proof of Concept (PoC) level serves to increase efficiency in maritime operations, such as traffic-flow management, and effective utilization of port resources, thus reducing their level of emission to a great extent.

The proposed framework is composed of three main components, as outlined in Table 8. A two-token model is leveraged to incentivize the participants: JRT for operation efficiency and GRT for decarbonization reduction. Notwithstanding the conducted tests demonstrating the feasibility of the framework, as the authors highlight, several challenges need further exploration, such as interoperability, security, regulatory compliance, and token lifecycle.

Table 8. Components of the system proposed in [41].

Component	Functionality
Data source	This includes various inputs necessary for the system's functioning, such as vessel operation data
On-chain	Responsible for storing critical data in a decentralized manner, and operation execution through smart contracts
Off-chain	Handles data that are either too large or sensitive to be stored directly on the blockchain

Practical application: CargoSmart is a blockchain-based solution for maritime transportation, enhancing coordination and optimizing port operations to improve cargo management and reduce waiting times [121].

2.10. Distributed Agile Software Development

The challenges in the Distributed Agile Software Development (DASD) field are those of coordinating the teams between locations, showing transparency in the process of development, and providing security to the code repositories. Blockchain technology has the potential to facilitate that with a decentralized platform and to ensure clear visibility from the beginning to the end of the development lifecycle.

In ref. [42], the authors proposed AgilePlus: a blockchain-based framework specifically designed to enhance transparency, trust, traceability, and security in DASD. The proposed framework uses smart contracts on a private Ethereum blockchain to support and enhance many key processes within the agile development life cycle.

The architecture of the framework is comprised of seven layers, as outlined in Table 9. The InterPlanetary File System [122] is leveraged as an off-chain solution. Conducted tests demonstrate the feasibility of the framework. Energy consumption and difficulty in data modification once it is stored in the blockchain are highlighted limitations. Empirical tests could provide additional validation of the obtained results.

Practical application: Gitopia is a code collaboration platform powered by a decentralized network. It aims to enhance the open-source software-development process through effective collaboration, incentivization, and transparency [123].

Table 9. Layers of the model proposed in [42].

Layer	Responsibility
Interface Layer	Includes user-facing applications, decentralized applications, and a web portal that connects users to the system
Application Layer	Manages metadata of transactions, payments, and records such as posts, prototypes, and project agreements
Business Logic Layer	Contains smart contracts that govern the terms and conditions for transactions
Trust Layer	Manages the consensus algorithm and smart contract security analysis
Transaction Layer	Handles the initiation and validation of transactions, as well as mining and block validation
Infrastructure Layer	Consists of a peer-to-peer network for distributing, verifying, and forwarding transactions
Security Layer	Protects the network from attacks such as 51% attacks and includes security algorithms and protocols

3. Challenges and Key Threats

Notwithstanding the huge potential of blockchain across various sectors, some common challenges are associated with the technology. This section brings forth such broad areas containing related specific challenges. For each, the relevant key threats and related articles are outlined, as can be seen in Table 10. Subsequent sections will explore the potential solutions to effectively mitigate these issues.

Table 10. Blockchain challenges and key threats.

Broad Challenges	Related Challenges	Key Threats	Articles
Technical and Performance Issues	Scalability Gas fees and memory constraints Redundancy	Network spamming Slower transaction verification Resource-heavy operations	[12,22–30,32,33,35,36,40–42,124–126]
Security and Protocol Integrity	Consensus mechanism Smart contract Immutability Privacy and data security Criminal activity	51% attack Double spending Eclipse attack Sybil attack Spoofing attack Selfish mining attack BGP hijacking attack Balance attack Transaction malleability Sandwich attack Liveness attack Man in the middle attack DoS/DDoS attack	[12,23,25–29,32,35,36,40,42,125–130]
Operational and Global Management	Governance Interoperability	Unequal participant influence Difficulties in system communication Financial losses	[19,28,32,36,40–42,131]
Legal and Regulatory Compliance	Regulatory concerns	Non-compliance risks Operational disruptions due to regulatory changes	[23,28,36,40,41]
Adoption and Knowledge Barriers	Educational materials Immaturity	Lack of understanding and awareness of blockchain technology	[21,40]

3.1. Technical and Performance Issues

Scalability still poses a big problem when blockchain networks grow, therefore leading to an increase in transaction processing time and very big storage needs, practically affecting the use and adoption of the blockchain in several sectors [22,23,25–27,30,32,33,36,41,42,125].

The limited block size leads to a small number of transactions [40] and the duplication of data across multiple nodes might increase the costs without any benefits, in some cases [28].

At the same time, they are heavily resource-oriented, plaguing those blockchain applications deployed in energy-sensitive environments and frameworks of the IoT, thus bringing about high costs of transaction and computational bounds [12,32,33]. Further, the problems of network spamming and slower transaction verifications increase the scalability issues [35,41].

Solutions: To address these scalability and performance challenges, off-chain storage solutions like IPFS manage data scalability without compromising performance, which is more apt in the case of high-volume data management [42]. IPFS is a decentralized, peer-to-peer file system designed to store and share data across a distributed network. It uses content-addressed storage, meaning each file is identified by a unique cryptographic hash rather than its location on a specific server. Despite its decentralized advantages, the network can experience slower content-retrieval times compared to traditional CDNs [132,133].

Other studies suggest the use of lightweight blockchain architectures that reduce both computational and communication overhead [12,33]. This is achieved through optimized consensus mechanisms [134], such as HPoC [135]. However, the simplification of the consensus mechanism could lead to potential security threats.

Additionally, the literature offers solutions like sharding techniques and efficient consensus mechanisms [32]. Sharding is a technique that divides the network into disjoint groups of nodes, each responsible for processing a subset of the total transactions. A simple illustration of this technique is represented in Figure 13. This approach leads to a parallel processing of the transactions which increases transaction throughput [136,137]. Despite the advantages, this method could lead to cross-shard communication overhead [138] and other potential problems [126].

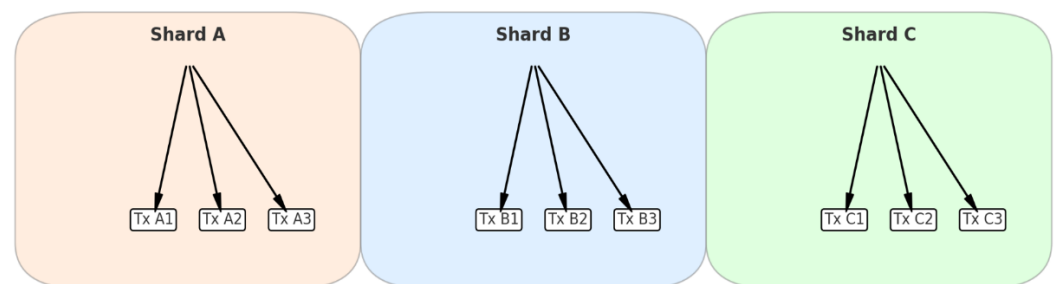


Figure 13. Sharding technique.

Another investigative approach is the pruning of the outdated blocks and their resource-conserving balancing [27]. The pruning method refers to removing “spent transactions” from the blockchain for size reduction [139]. Nevertheless, it is unclear how the deletion of obsolete transactions and the migration of UTXOs buried in the chain should occur [140].

Likewise, different architectural patterns shaped by the application needs have the potential to reduce these concerns [124]. The ACE-BC framework provides an improved throughput ratio, enhanced data confidentiality, and lower computation time, as an alternative to the existing approaches [24]. In addition, an adaptive function of a Proof of Work (PoW) consensus might increase its scalability by automatically adjusting the number of nodes to accommodate the new members [35]. Artificial intelligence and machine learning might be helpful in support of transaction processing, heightened security, and

management of the ever-increasing complexity of data and optimization of network operations [29]. However, each of these solutions still has disadvantages: empirical experiments and in-depth technical analysis represent pre-requisites for their actual integration and future improvements.

3.2. Security and Protocol Integrity

Several types of consensus mechanisms have been studied [23,25,35]; around 30 mechanisms exist [126], each with its own type of advantages and vulnerabilities, such as high consumption of energy and inefficiency in processing transactions [12], and exposure to potential security breaches: 51% attacks [27,40], eclipse attacks [28,40], double spending [28,29], and sandwich attacks [127], among others [27,29,40,42,125,126].

Smart contracts are an important constituent of blockchain operation but fall prey to a series of vulnerabilities due to bugs or errors that happen during their coding, which can compromise the entire network and lead to financial losses. These vulnerabilities are decentralized and tamper-proof by nature, and hence hard to patch once deployed [26,27,128].

On the other hand, the privacy and confidentiality concerns are related to the loss of the private key [28,29] and blockchain transparency, which might lead, therefore, to the leaking of sensitive data, such as sensible health information [27,28,36,40].

Solutions: These issues are addressed with better and safer consensus mechanisms [130] such as PoT and DBFT that improve security, reduce energy consumption, and increase transaction speed [12,23]. Proof of Trust (PoT) selects the validators based on a trust score, determined by historical behavior and transaction history [141,142]. Delegated Byzantine Fault Tolerance (DBFT) combines Delegated Proof of Stake and Byzantine Fault Tolerance algorithms, where participants vote to elect delegates who achieve consensus on new blocks [143,144]. However, challenges such as centralization risk and potential security issues are still open for these solutions.

Moreover, several privacy-enhancing technologies, such as zero-knowledge proofs [145], homomorphic encryption [146], and secure multi-party computation [27,36,40] combined with various privacy-oriented frameworks like Hawk [28] have emerged to better the level of privacy without any compromise on the blockchain functionality. Nevertheless, these approaches increase integration complexity and might be resource-intensive.

The blockchain-based system that records malicious IP addresses in blockchain transactions and the client-server approach that dynamically configures static ARP entries are some of the highlighted solutions for DDoS and spoofing attacks, respectively [126]. In any case, such solutions should be carefully pre-analyzed, as they might introduce latency issues and centralization risks.

Defining and adopting game-theory-based frameworks might improve the security of decentralized transactions [127]. This approach allows the organizer to implement a mechanism between the market and the participants aiming to maximize the market's benefits. However, empirical analysis is necessary to prove the efficiency in a real-time application.

The development of robust key-management systems aims at increasing the security of cryptographic keys and avoiding unauthorized access [28,32]. Additionally, in the realm of smart contracts, rigorous testing and deployment of security templates and libraries are necessary to minimize the vulnerabilities in smart contracts [27,28,32,129]. Figure 14 presents some verification tools for smart contracts. Oyente [147], Securify [148], and Zeus [149] are employed for formal verification and vulnerability detection [28,128], with further constant monitoring and analysis post-deployment being a good practice.

In addition, the application of a private blockchain may lessen some of these risks, such as the 51% attack, thereby securing transactions between the parties [42]. Furthermore, SGX [125] is among the highlighted approaches to improve the security and privacy of blockchain systems. Intel Software Guard Extensions (SGXs) are trusted execution environment products that create secure enclaves within CPUs to protect data integrity and confidentiality [150], making them applicable in the blockchain for enhancing security,

privacy, and scalability. However, SGXs have limitations, including a 128 MB memory cap, side-channel attacks, and single-point attacks.

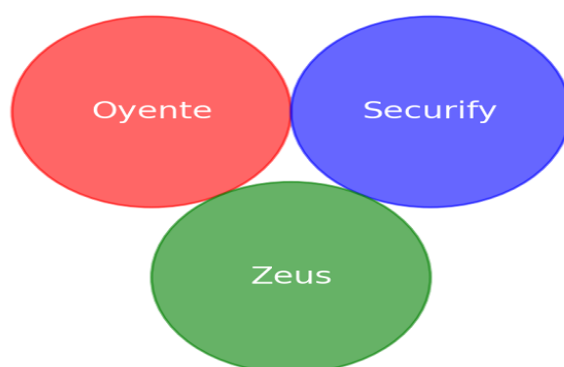


Figure 14. Verification tools for smart contracts.

Artificial intelligence and machine learning might be implemented to monitor anomalies, enable the strongest set of security items, and improve more efficient data management within blockchain networks [28,29]. Nevertheless, the integration complexity and privacy considerations are open issues.

3.3. Operational and Global Management

Both operational and global management in blockchain systems have several challenges, including fairness in transactions, integration with the existing systems, and ensuring interoperability across the diversification of blockchain networks. This makes the transaction mechanism and the financial incentive structures very important in maintaining fairness—on the one hand, avoiding malicious behavior from the data providers, while on the other hand, encouraging active and honest participation. Credible data providers should receive rewards, while dishonesty should attract some penalties [19]. Issues like the fairness of all parties in a public blockchain would point to the potential need for governance systems that can adjust the supply and rewards for proper equity in the treatment of all parties involved [41].

Several different blockchain networks not only find it challenging to communicate with each other, but to integrate into systems belonging to past ages due to the lack of common standards. It is, therefore, the very heterogeneity of blockchain protocols that presents a risk to the uniformity of basic processes and discourages their mass use [32,40]. For example, it is still very difficult to integrate blockchain technology with the existing systems in the health sector and guarantee interoperability with diverse EHR systems [36].

Solutions: To encounter such challenges in operational and global management, different approaches have been proposed. In ref. [19], the threshold signature [49,50] combined with the verifiable encrypted signature [47,48] employs an arbitrator committee for the protection of the rights of both parties of the transaction and assurance of fairness. The components of the solutions are highlighted in Figure 3. However, cryptographic operations could be resource-intensive, and the dependency on the honesty and availability of the committee might introduce delays and security issues.

Interoperability frameworks have also been designed, standardizing the interaction between different blockchain networks. The frameworks incorporate cross-chains [151,152], side-chains [153,154], proxy tokens [151], notary schemes [153], and atomic swaps [155] that facilitate the exchange of assets and data [32]. Nevertheless, such frameworks could introduce additional complexity and increase transaction costs.

Oracles provide a means of bridging the information gap between the on-chain and off-chain environments. An oracle is an intermediary system that securely retrieves, verifies, and transmits external data from real-world sources to smart contracts [156,157]. Figure 15

represents a simple illustration of Oracle communication. Trust and data integrity are some of the open concerns when it comes to oracles.

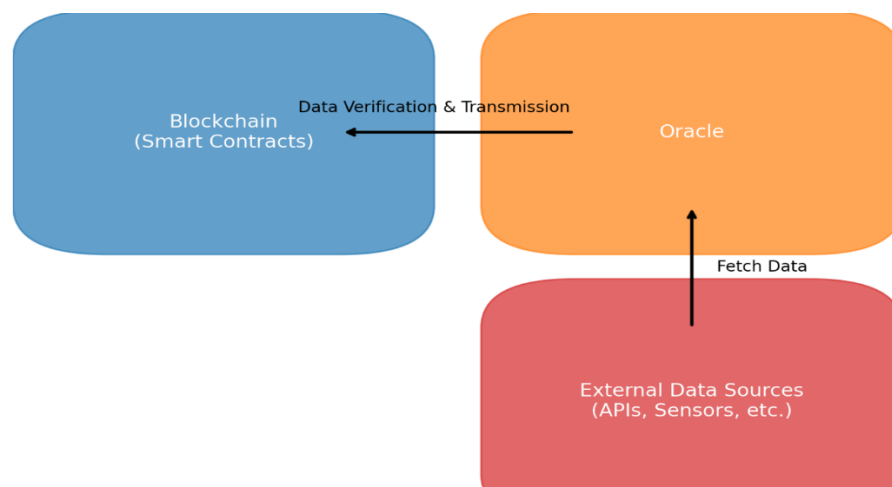


Figure 15. Oracle communication.

Newer trust and transparency solutions, such as the Lightning Network [158], allow double-signed transaction receipts, so the transactions can be validated between parties securely and transparently, without the interference of third parties [28]. This way, they establish trust and mitigate the risk of conflicts among the stakeholders.

Furthermore, the Kleros platform aims to resolve the conflicts that might arise between stakeholders, using an incentive-game-theory approach [131]. Kleros is a decentralized court system that allows dispute resolution encountered within smart contracts, based on crowdsourced jurors [159]. Juror quality might represent an impediment, especially in complex disputes.

AgilePlus [42], whose architecture is described in Table 9, could ensure the effective implementation of agile development processes, safety in payments, and automatic payment distribution. However, it lacks empirical tests and faces challenges such as energy consumption and data modification.

The development and adoption of different standards might enhance interoperability, such as HL7 and FHIR for EHR [36].

3.4. Legal and Regulatory Compliance

Legal and regulatory compliance is a serious roadblock to the wide adoption of the blockchain across various sectors. It is complicated and of great importance for the stakeholders to classify and establish which types of tokens bear regulatory implications against blockchain, basing such qualifications on their design and use cases [41].

The General Data Protection Regulation (GDPR) introduces stringent requirements regarding safety and data protection, quite difficult to fulfill due to the decentralized and transparent nature of the blockchain [23,40].

Additionally, the very absence of uniform standards compromises the security and reliability of blockchain systems, complicating the merger with diverse regulations, such as the California Consumer Privacy Act (CCPA) [160] and GDPR [161]. It even touches the educational sector, to the extent that the regulation educational authorities manage vital aspects like degree attestation, verification standards, and the candidate certificate integrity [40].

Compliance with laws for the protection of health data, such as the Health Insurance Portability and Accountability Act (HIPAA), continues to be an area riddled with problems within the health sector, due to the comprehensive requirements for the privacy and security of health information [36]. Further, the integration of blockchain in the legal and financial

sectors presents regulatory challenges, emanating from the application of the technology in a wider context than just cryptocurrencies [28].

Solutions: The key steps towards effective navigation of the complex regulatory landscape involve undertaking comprehensive studies, to ensure that the solutions meet the regulatory requirement, and taking on clear communication with the stakeholders [41,162].

The collaboration between stakeholders and government support is a necessity, where challenging regulations arise. One example is the education sector, which requires compliance with data-protection laws, such as GDPR [40,163]. Furthermore, in a field as delicate as healthcare, facing legal challenges, one viable solution seems to be the establishment of clear regulatory frameworks. That might allow for the decentralized aspects of the blockchain to comply with specific regulations, such as HIPAA [36,164].

In addition, the limitation of personal data storage on the blockchain, assessing the need for specific reasons, and adopting permissioned blockchains with more regulation in usage might make these systems work better for observance of the data-protection laws. These steps will help to align blockchain implementations with legal requirements and, at the same time, ensure that this technology is used responsibly and ethically [40,165].

3.5. Adoption and Knowledge Barriers

The adoption of blockchain technology faces massive challenges due to a lack of general awareness about its potential and functionalities. The said barrier is more pronounced for stakeholders who have little knowledge about the technology. In addition, because of skepticism regarding cryptocurrencies, often linked with Bitcoin, they refuse to accept the technology [166]. This skepticism has further been the reason for regulatory obstacles and outright prohibition in some jurisdictions, thus hampering its wide adoption [21].

Article [40] focuses on the fact that the low penetration of blockchain technology in education is seriously hampered by a lack of human and expert resources whose competencies allow for dealing with intricate systems of data. This contributes to the shortage of blockchain technology in the education area because most institutions do not want to venture into this technology without enough information and knowledge of how best it should be implemented and managed. What is more, blockchain technology is still immature [167], which is observable through the poor usability of applications, with an extreme focus on security and privacy at the expense of user-friendly interfaces and adequate training. Furthermore, the complexity of integrating blockchain into the current educational systems aggravates these issues [168].

Solutions: Successful tackling of the challenges related to the adoption of the technology requires a cohesive strategy, involving multiple facets of education and integration. Education and awareness need to be a prime focus area. Herein, the key is the development of complete educational materials and awareness programs, so that all those who are associated know what the functionalities of blockchain technology are and their potential [169,170]. This will also help to reduce skepticism on issues to do with cryptocurrencies, by emphasizing the huge applications that blockchain technology has, beyond financial transactions [21].

With increased training and development investment that relates to education, professionals will be equipped with the right set of skills for proper management and utilization of blockchain systems. Therefore, this is one way through which the skilled blockchain professional shortage can be overcome.

At the same time, a focus on user interfaces that make the functionality much easier for common people will improve usability, in turn improving adoption and effectiveness. Additionally, third-party services specializing in this technology might be considered with regard to dealing with complexity in the integration of blockchain in diverse systems [40,171].

4. Discussion and Future Directions

Integration of blockchain with AI, IoT, and Big Data Analytics still holds the key in solving scalability and performance issues. There is a need for continued innovation in

cryptographic solutions and consensus mechanisms in a bid to further improve the security and integrity of blockchain networks, which are continuously at risk of cyberattacks.

Another highly involved area is sustainability, which requires system designs that are both scalable and resource-efficient. Research should focus on developing blockchain architectures that can handle applications at a large scale, but at the same time with a minimal expenditure of resources.

Security is one of the major concerns for blockchain technology because, right from minor vulnerabilities to huge attacks that might lead to the entire network being compromised, everything is possible. To maintain the high security of the blockchain, it is a must to utilize standardized frameworks, conduct extensive testing, and keep up with the dynamic of cyber threats.

Governance is an important part of this technology as it evolves, and complex applications keep arising. Proper validation of certain activities and transparent, fair conflict resolution processes are of very high importance for the credibility and functioning of blockchain networks, especially in public and decentralized setups. The said point of blockchain governance is pivotal in nature and warrants a more in-depth exploration to devise mechanisms that can facilitate the dynamic character of decentralized operations.

The regulatory and compliance challenges require the navigation of very complicated, nontechnical policy landscapes. Simplified research into these frameworks must be conducted to ensure that blockchain activities will be aligned with very stringent rules. This makes educational initiatives of great importance. Strong facilitation on the part of academic and government institutions is needed to craft specific programs and public outreach efforts that will successfully raise blockchain knowledge and support broader adoption.

A comprehensive understanding of the potential and drawbacks of blockchain should, therefore, embrace a multilayered approach, blending technical, regulatory, and environmental research. AI applied to blockchains promises much in terms of efficient management, scalability, and security, but also introduces the disadvantages of complexity and ethical considerations. Interdisciplinary collaboration is required to ensure that the full potential of blockchain technology for the development of strong and sustainable solutions is realized to revolutionize industries and improve society in a significant way.

5. Conclusions

This review captured the broad scope of blockchain technology and underlined the significant potential and the diverse set of challenges it presents. We highlighted the critical role that blockchain technology plays in advancing technological frontiers and the capacity it has to impact several industries.

The proposed insights further open room for exploration and development. Apart from that, some light is shed on the continuous innovation in and careful attention paid to the complexities and capabilities of blockchain technology. It is to be noted that the paper presents most of the wide-range applications, challenges, threats, and possible solutions of blockchain technology; nevertheless, many others could exist. However, compared to other reviews, our survey comprises a large number of applicability domains, challenges, and possible solutions, along with a structure that offers a better visualization of interconnected challenges. That being said, this paper provides a comprehensive view of the actual situation of this technology, in terms of applicability, challenges, and possible solutions, opening paths for future research.

As blockchain continues to evolve, it has the potential for a great impact on technology and society around us and calls for continued exploration and critical engagement by a panoply of stakeholders.

Author Contributions: Conceptualization, C.D.M.; methodology, C.D.M.; formal analysis, C.D.M.; investigation, C.D.M.; writing—original draft preparation, C.D.M.; writing—review and editing, C.D.M.; visualization, C.D.M.; supervision, D.E.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this paper:

IoT	Internet of Things
AI	Artificial Intelligence
ACE-BC	Access Control-Enabled Blockchain
BSKM	Blockchain-based Special Key Security Model
V2X	Vehicle-to-Everything
NFT	Non-Fungible Token
JIT	Just-in-Time
PoAh	Proof of Authentication
PoT	Proof of Trust
PoW	Proof of Work
DBFT	Delegated Byzantine Fault Tolerance
HPoC	Hierarchical Proof of Capability
IPFS	InterPlanetary File System
CDN	Content Delivery Network
UTXO	Unspent Transaction Output
ITS	Intelligent Transportation Systems
IoD	Internet of Drones
PoC	Proof of Concept
DASD	Distributed Agile Software Development
ARP	Address Resolution Protocols
SGX	Intel Software Guard Extensions
MDLDP	Multiple Disturbance of Local Differential Privacy
EHR	Electronic Health Records
GDPR	General Data Protection Regulation
HL7	Health Level 7
FHIR	Fast Healthcare Interoperability Resources
CCPA	California Consumer Privacy Act
HIPAA	Health Insurance Portability and Accountability Act

References

- Adere, E.M. Blockchain in Healthcare and IoT: A Systematic Literature Review. *Array* **2022**, *14*, 100139. [\[CrossRef\]](#)
- López-Sorribes, S.; Rius-Torrentó, J.; Solsona-Tehàs, F. A Bibliometric Review of the Evolution of Blockchain Technologies. *Sensors* **2023**, *23*, 3167. [\[CrossRef\]](#) [\[PubMed\]](#)
- Taherdoost, H. Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives. *SCI* **2023**, *5*, 41. [\[CrossRef\]](#)
- Ekinci, F.; Guzel, M.S.; Acici, K.; Asuroglu, T. The Future of Microreactors: Technological Advantages, Economic Challenges, and Innovative Licensing Solutions with Blockchain. *Appl. Sci.* **2024**, *14*, 6673. [\[CrossRef\]](#)
- Echikr, A.; Yachir, A.; Kerrache, C.A.; Sahraoui, Z. Exploring the Potential of Blockchain in Internet of Robotic Things: Advancements, Challenges, and Future Directions. In Proceedings of the 6th International Conference on Networking and Advanced Systems, (ICNAS 2023), Algiers, Algeria, 21–23 October 2023; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2023. [\[CrossRef\]](#)
- Mandal, M.; Chishti, M.S.; Banerjee, A. Investigating Layer-2 Scalability Solutions for Blockchain Applications. In Proceedings of the 2023 IEEE International Conference on High Performance Computing and Communications, Data Science and Systems, Smart City and Dependability in Sensor, Cloud and Big Data Systems and Application, (HPCC/DSS/SmartCity/DependSys 2023), Melbourne, Australia, 17–21 December 2023; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2023; pp. 710–717. [\[CrossRef\]](#)
- Mao, H.; Nie, T.; Sun, H.; Shen, D.; Yu, G. A Survey on Cross-Chain Technology: Challenges, Development, and Prospect. *IEEE Access* **2023**, *11*, 45527–45546. [\[CrossRef\]](#)
- Mohanta, B.K.; Jena, D.; Panda, S.S.; Sobhanayak, S. Blockchain Technology: A Survey on Applications and Security Privacy Challenges. *Internet Things* **2019**, *8*, 100107. [\[CrossRef\]](#)

9. Das, S.; Mohanta, B.K.; Jena, D. A State-of-the-Art Security and Attacks Analysis in Blockchain Applications Network. *Int. J. Commun. Netw. Distrib. Syst.* **2022**, *28*, 199–218. [[CrossRef](#)]
10. Guru, D.; Perumal, S.; Varadarajan, V. Approaches towards Blockchain Innovation: A Survey and Future Directions. *Electronics* **2021**, *10*, 1219. [[CrossRef](#)]
11. Lai, Y.; Yang, J.; Liu, M.; Li, Y.; Li, S. Web3: Exploring Decentralized Technologies and Applications for the Future of Empowerment and Ownership. *Blockchains* **2023**, *1*, 111–131. [[CrossRef](#)]
12. Habib, G.; Sharma, S.; Ibrahim, S.; Ahmad, I.; Qureshi, S.; Ishfaq, M. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet* **2022**, *14*, 341. [[CrossRef](#)]
13. Moosavi, N.; Taherdoost, H. Blockchain Technology Application in Security: A Systematic Review. *Blockchains* **2023**, *1*, 58–72. [[CrossRef](#)]
14. Douaioui, K.; Benmoussa, O. Insights into Industrial Efficiency: An Empirical Study of Blockchain Technology. *Big Data Cogn. Comput.* **2024**, *8*, 62. [[CrossRef](#)]
15. Rawat, D.B.; Chaudhary, V.; Doku, R. Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems. *J. Cybersecur. Priv.* **2021**, *1*, 4–18. [[CrossRef](#)]
16. Johar, S.; Ahmad, N.; Asher, W.; Cruickshank, H.; Durrani, A. Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey. *Appl. Sci.* **2021**, *11*, 6252. [[CrossRef](#)]
17. Alshamsi, M.; Al-Emran, M.; Shaalan, K. A Systematic Review on Blockchain Adoption. *Appl. Sci.* **2022**, *12*, 4245. [[CrossRef](#)]
18. Al-Megren, S.; Alsalamah, S.; Altoaimy, L.; Alsalamah, H.; Soltanisehat, L.; Almutairi, E.; Sandy Pentland, A. Blockchain Use Cases in Digital Sectors: A Review of the Literature. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; IEEE: New York, NY, USA, 2018; pp. 1417–1424. [[CrossRef](#)]
19. Zhou, W.; Zhang, D.; Han, G.; Zhu, W.; Wang, X. A Blockchain-Based Privacy-Preserving and Fair Data Transaction Model in IoT. *Appl. Sci.* **2023**, *13*, 12389. [[CrossRef](#)]
20. Ullah, I.; Havinga, P.J.M. Governance of a Blockchain-Enabled IoT Ecosystem: A Variable Geometry Approach. *Sensors* **2023**, *23*, 9031. [[CrossRef](#)]
21. Adamashvili, N.; Zhizhilashvili, N.; Tricase, C. The Integration of the Internet of Things, Artificial Intelligence, and Blockchain Technology for Advancing the Wine Supply Chain. *Computers* **2024**, *13*, 72. [[CrossRef](#)]
22. Khanzada, T.J.S.; Shahid, M.F.; Mutahhar, A.; Aslam, M.A.; Ashari, R.B.; Jamal, S.; Nooruddin, M.; Siddiqui, S. Authenticity, and Approval Framework for Bus Transportation Based on Blockchain 2.0 Technology. *Appl. Sci.* **2023**, *13*, 11323. [[CrossRef](#)]
23. Alam, S.; Bhatia, S.; Shuaib, M.; Khubrani, M.M.; Alfayez, F.; Malibari, A.A.; Ahmad, S. An Overview of Blockchain and IoT Integration for Secure and Reliable Health Records Monitoring. *Sustainability* **2023**, *15*, 5660. [[CrossRef](#)]
24. Alharbi, A. Applying Access Control Enabled Blockchain (ACE-BC) Framework to Manage Data Security in the CIS System. *Sensors* **2023**, *23*, 3020. [[CrossRef](#)] [[PubMed](#)]
25. Dener, M.; Orman, A. BBAP-WSN: A New Blockchain-Based Authentication Protocol for Wireless Sensor Networks. *Appl. Sci.* **2023**, *13*, 1526. [[CrossRef](#)]
26. Zubaydi, H.D.; Varga, P.; Molnár, S. Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. *Sensors* **2023**, *23*, 788. [[CrossRef](#)] [[PubMed](#)]
27. Bhutta, M.N.M.; Khwaja, A.A.; Nadeem, A.; Ahmad, H.F.; Khan, M.K.; Hanif, M.A.; Song, H.; Alshamari, M.; Cao, Y. A Survey on Blockchain Technology: Evolution, Architecture and Security. *IEEE Access* **2021**, *9*, 61048–61073. [[CrossRef](#)]
28. Singh, S.; Sanwar Hosen, A.S.M.; Yoon, B. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. *IEEE Access* **2021**, *9*, 13938–13959. [[CrossRef](#)]
29. Oumaima, F.; Karim, Z.; Abdellatif, E.G.; Mohammed, B. A Survey on Blockchain and Artificial Intelligence Technologies for Enhancing Security and Privacy in Smart Environments. *IEEE Access* **2022**, *10*, 93168–93186. [[CrossRef](#)]
30. Rao, P.M.; Jangirala, S.; Pedada, S.; Das, A.K.; Park, Y. Blockchain Integration for IoT-Enabled V2X Communications: A Comprehensive Survey, Security Issues and Challenges. *IEEE Access* **2023**, *11*, 54476–54494. [[CrossRef](#)]
31. Alhazmi, H.E.; Eassa, F.E.; Sandokji, S.M. Towards Big Data Security Framework by Leveraging Fragmentation and Blockchain Technology. *IEEE Access* **2022**, *10*, 10768–10782. [[CrossRef](#)]
32. Islam, S.; Islam, M.J.; Hossain, M.; Noor, S.; Kwak, K.S.; Islam, S.M.R. A Survey on Consensus Algorithms in Blockchain-Based Applications: Architecture, Taxonomy, and Operational Issues. *IEEE Access* **2023**, *11*, 39066–39082. [[CrossRef](#)]
33. Yang, W.; Wang, S.; Yin, X.; Wang, X.; Hu, J. A Review on Security Issues and Solutions of the Internet of Drones. *IEEE Open J. Comput. Soc.* **2022**, *3*, 96–110. [[CrossRef](#)]
34. Hu, J.; Huang, K.; Bian, G.; Cui, Y. Redact-Chain for Health: A Scheme Based on Redactable Blockchain for Managing Shared Healthcare Data. *Electronics* **2023**, *12*, 4240. [[CrossRef](#)]
35. Islam, M.S.; Ameen, M.A.B.; Rahman, M.A.; Ajra, H.; Ismail, Z.B. Healthcare-Chain: Blockchain-Enabled Decentralized Trustworthy System in Healthcare Management Industry 4.0 with Cyber Safeguard. *Computers* **2023**, *12*, 46. [[CrossRef](#)]
36. Zukaib, U.; Cui, X.; Hassan, M.; Harris, S.; Hadi, H.J.; Zheng, C. Blockchain and Machine Learning in EHR Security: A Systematic Review. *IEEE Access* **2023**, *11*, 130230–130256. [[CrossRef](#)]

37. Hiwale, M.; Walambe, R.; Potdar, V.; Kotecha, K. A Systematic Review of Privacy-Preserving Methods Deployed with Blockchain and Federated Learning for the Telemedicine. *Healthc. Anal.* **2023**, *3*, 100192. [[CrossRef](#)]
38. Bakir, C. New Blockchain Based Special Keys Security Model with Path Compression Algorithm for Big Data. *IEEE Access* **2022**, *10*, 94738–94753. [[CrossRef](#)]
39. Patel, S.; Sahoo, A.; Mohanta, B.K.; Panda, S.S.; Jena, D. DAAuth: A Decentralized Web Authentication System Using Ethereum Based Blockchain. In Proceedings of the 2019 International Conference on Vision towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, 30–31 March 2019; pp. 1–5. [[CrossRef](#)]
40. Mohammad, A.; Vargas, S. Challenges of Using Blockchain in the Education Sector: A Literature Review. *Appl. Sci.* **2022**, *12*, 6380. [[CrossRef](#)]
41. Nguyen, S.; Leman, A.; Xiao, Z.; Fu, X.; Zhang, X.; Wei, X.; Zhang, W.; Li, N.; Zhang, W.; Qin, Z. Blockchain-Powered Incentive System for JIT Arrival Operations and Decarbonization in Maritime Shipping. *Sustainability* **2023**, *15*, 15686. [[CrossRef](#)]
42. Farooq, M.S.; Kalim, Z.; Qureshi, J.N.; Rasheed, S.; Abid, A. A Blockchain-Based Framework for Distributed Agile Software Development. *IEEE Access* **2022**, *10*, 17977–17995. [[CrossRef](#)]
43. Chen, X.; He, S.; Sun, L.; Zheng, Y.; Wu, C.Q. A Survey of Consortium Blockchain and Its Applications. *Cryptography* **2024**, *8*, 12. [[CrossRef](#)]
44. Malla, T.B.; Bhattarai, A.; Parajuli, A.; Shrestha, A.; Chhetri, B.B.; Chapagain, K. Status, Challenges and Future Directions of Blockchain Technology in Power System: A State of Art Review. *Energies* **2022**, *15*, 8571. [[CrossRef](#)]
45. Fotiou, N.; Pittaras, I.; Siris, V.A.; Polyzos, G.C.; Anton, P. A Privacy-Preserving Statistics Marketplace Using Local Differential Privacy and Blockchain: An Application to Smart-Grid Measurements Sharing. *Blockchain Res. Appl.* **2021**, *2*, 100022. [[CrossRef](#)]
46. Zhao, Y.; Zhao, J.; Yang, M.; Wang, T.; Wang, N.; Lyu, L.; Niyato, D.; Lam, K.Y. Local Differential Privacy-Based Federated Learning for Internet of Things. *IEEE Internet Things J.* **2021**, *8*, 8836–8853. [[CrossRef](#)]
47. Asokan, N.; Schunter, M.; Waidner, M. Optimistic protocols for fair exchange. In Proceedings of the 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, 1–4 April 1997; pp. 7–17.
48. Yang, X.; Liu, M.; Au, M.H.; Luo, X.; Ye, Q. Efficient Verifiably Encrypted ECDSA-Like Signatures and Their Applications. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 1573–1582. [[CrossRef](#)]
49. Desmedt, Y. Society and group oriented cryptography: A new concept. In Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, Santa Barbara, CA, USA, 16–20 August 1987; Springer: Berlin/Heidelberg, Germany, 1987; pp. 120–127.
50. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [[CrossRef](#)]
51. de Haro-Olmo, F.J.; Varela-Vaca, Á.J.; Álvarez-Bermejo, J.A. Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review. *Sensors* **2020**, *20*, 7171. [[CrossRef](#)] [[PubMed](#)]
52. Peter, L. The Variable Geometry Approach to International Economic Integration. In Proceedings of the Seventh APEF Conference, Indonesia, Iran, 3–5 November 2008; University of Melbourne: Melbourne, Australia, 2008.
53. Puthal, D.; Mohanty, S.P.; Nanda, P.; Kougianos, E.; Das, G. Proof-of-authentication for scalable blockchain in resource-constrained distributed systems. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics, Berlin, Germany, 8–11 September 2019; pp. 1–5.
54. Puthal, D.; Mohanty, S.P. Proof of Authentication: IoT-Friendly Blockchains. *IEEE Potentials* **2019**, *38*, 26–29. [[CrossRef](#)]
55. Aslam, S.; Tošić, A.; Mrissa, M. Secure and Privacy-Aware Blockchain Design: Requirements, Challenges and Solutions. *J. Cybersecur. Priv.* **2021**, *1*, 164–194. [[CrossRef](#)]
56. Zhao, X.; Chen, Z.; Chen, X.; Wang, Y.; Tang, C. The DAO Attack Paradoxes in Propositional Logic. In Proceedings of the 2017 4th International Conference on Systems and Informatics (ICSAI), Hangzhou, China, 11–13 November 2017; pp. 1743–1746. [[CrossRef](#)]
57. IOTA. Available online: <https://www.iota.org/> (accessed on 13 June 2024).
58. Derler, D.; Samelin, K.; Slamanig, D. Bringing Order to Chaos: The Case of Collision-Resistant Chameleon-Hashes. *J. Cryptol.* **2024**, *37*, 1–44. [[CrossRef](#)]
59. Zhang, T.; Zhang, L.; Wu, Q.; Mu, Y.; Rezaeibagha, F. Redactable Blockchain-Enabled Hierarchical Access Control Framework for Data Sharing in Electronic Medical Records. *IEEE Syst. J.* **2023**, *17*, 1962–1973. [[CrossRef](#)]
60. Abdel Hakeem, S.A.; Kim, H. Centralized Threshold Key Generation Protocol Based on Shamir Secret Sharing and HMAC Authentication. *Sensors* **2022**, *22*, 331. [[CrossRef](#)]
61. Wang, C.; Tan, X.; Yao, C.; Gu, F.; Shi, F.; Cao, H. Trusted Blockchain-Driven IoT Security Consensus Mechanism. *Sustainability* **2022**, *14*, 5200. [[CrossRef](#)]
62. Maimuț, D.; Matei, A.C. Speeding-Up Elliptic Curve Cryptography Algorithms. *Mathematics* **2022**, *10*, 3676. [[CrossRef](#)]
63. Lahraoui, Y.; Lazaar, S.; Amal, Y.; Nitaj, A. Securing Data Exchange with Elliptic Curve Cryptography: A Novel Hash-Based Method for Message Mapping and Integrity Assurance. *Cryptography* **2024**, *8*, 23. [[CrossRef](#)]
64. Zhou, S.; Li, K.; Xiao, L.; Cai, J.; Liang, W.; Castiglione, A. A Systematic Review of Consensus Mechanisms in Blockchain. *Mathematics* **2023**, *11*, 2248. [[CrossRef](#)]
65. Sapra, N.; Shaikh, I.; Dash, A. Impact of Proof of Work (PoW)-Based Blockchain Applications on the Environment: A Systematic Review and Research Agenda. *J. Risk Financ. Manag.* **2023**, *16*, 218. [[CrossRef](#)]

66. Franck, L.D.; Ginja, G.A.; Carmo, J.P.; Afonso, J.A.; Luppe, M. Custom ASIC Design for SHA-256 Using Open-Source Tools. *Computers* **2024**, *13*, 9. [[CrossRef](#)]
67. Algreto-Badillo, I.; Morales-Sandoval, M.; Medina-Santiago, A.; Hernández-Gracidas, C.A.; Lobato-Baez, M.; Morales-Rosales, L.A. A SHA-256 Hybrid-Redundancy Hardware Architecture for Detecting and Correcting Errors. *Sensors* **2022**, *22*, 5028. [[CrossRef](#)]
68. Fatima, S.; Rehman, T.; Fatima, M.; Khan, S.; Ali, M.A. Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing. *Eng. Proc.* **2022**, *20*, 14. [[CrossRef](#)]
69. Adeniyi, E.A.; Falola, P.B.; Maashi, M.S.; Aljebreen, M.; Bharany, S. Secure Sensitive Data Sharing Using RSA and ElGamal Cryptographic Algorithms with Hash Functions. *Information* **2022**, *13*, 442. [[CrossRef](#)]
70. Lee, G.H.; Shin, S.Y. Federated Learning on Clinical Benchmark Data: Performance Assessment. *J. Med. Internet Res.* **2020**, *22*, e20891. [[CrossRef](#)]
71. Solve.Care. Available online: <https://solve.care/> (accessed on 13 June 2024).
72. Jemihin, Z.B.; Tan, S.F.; Chung, G.C. Attribute-Based Encryption in Securing Big Data from Post-Quantum Perspective: A Survey. *Cryptography* **2022**, *6*, 40. [[CrossRef](#)]
73. Huang, M.; Liu, Y.; Yang, B.; Zhao, Y.; Zhang, M. Efficient Revocable Attribute-Based Encryption with Data Integrity and Key Escrow-Free. *Information* **2024**, *15*, 32. [[CrossRef](#)]
74. BAKIR, Ç.; HAKKOYMAZ, V. Distributed Environment Modeling Using Path Compression Algorithm. *Int. J. Appl. Math. Electron. Comput.* **2020**, *8*, 226–231. [[CrossRef](#)]
75. Memmi, G.; Kapusta, K.; Qiu, H. Data Protection: Combining Fragmentation, Encryption, and Dispersion. In Proceedings of the 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, 5–7 August 2015; pp. 1–9. [[CrossRef](#)]
76. Heni, H.; Abdallah, M.B.; Gargouri, F. Combining Fragmentation and Encryption to Ensure Big Data at Rest Security. In *Hybrid Intelligent Systems, 17th International Conference on Hybrid Intelligent Systems (HIS 2017) held in Delhi, India, 14–16 December 2017; Advances in Intelligent Systems and Computing*; Springer: Cham, Switzerland, 2018; Volume 734, pp. 177–185. [[CrossRef](#)]
77. Singh, G. A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *Int. J. Comput. Appl.* **2013**, *67*, 33–38. [[CrossRef](#)]
78. Acronis. Available online: <https://www.acronis.com/en-eu/> (accessed on 13 June 2024).
79. Abubashim, A.; Tan, C.C. Smart Contract Designs on Blockchain Applications. In Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 7–10 July 2020; pp. 1–4. [[CrossRef](#)]
80. Montes, J.M.; Ramirez, C.E.; Gutierrez, M.C.; Larios, V.M. Smart Contracts for Supply Chain Applicable to Smart Cities Daily Operations. In Proceedings of the 2019 IEEE International Smart Cities Conference (ISC2), Casablanca, Morocco, 14–17 October 2019; pp. 565–570. [[CrossRef](#)]
81. IBM Food Trust. Available online: <https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust> (accessed on 14 June 2024).
82. 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, (GCAT 2021), Bangalore, India, 1–3 October 2021; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2021. [[CrossRef](#)]
83. Sastry, K.; Goldberg, D.; Kendall, G. Genetic Algorithms. In *Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques*; Burke, E.K., Kendall, G., Eds.; Springer: Boston, MA, USA, 2005; pp. 97–125, ISBN 978-0-387-28356-2. [[CrossRef](#)]
84. Glover, F.; Laguna, M. Tabu Search. In *Handbook of Combinatorial Optimization: Volume 1–3*; Du, D.-Z., Pardalos, P.M., Eds.; Springer: Boston, MA, USA, 1998; pp. 2093–2229, ISBN 978-1-4613-0303-9. [[CrossRef](#)]
85. Muhammad, M.N.; Cavus, N. Fuzzy DEMATEL Method for Identifying LMS Evaluation Criteria. *Procedia Comput. Sci.* **2017**, *120*, 742–749. [[CrossRef](#)]
86. Kiela, K.; Jurgo, M.; Navickas, R. Structure of V2X-IoT Framework for ITS Applications. In Proceedings of the 2020 43rd International Conference on Telecommunications and Signal Processing (TSP), Milan, Italy, 7–9 July 2020; pp. 229–234. [[CrossRef](#)]
87. Oham, C.; Michelin, R.A.; Jurdak, R.; Kanhere, S.S.; Jha, S. B-FERL: Blockchain Based Framework for Securing Smart Vehicles. *Inf. Process Manag.* **2021**, *58*, 102426. [[CrossRef](#)]
88. Deebak, B.D.; Memon, F.H.; Khowaja, S.A.; Dev, K.; Wang, W.; Qureshi, N.M.F.; Su, C. A Lightweight Blockchain-Based Remote Mutual Authentication for AI-Empowered IoT Sustainable Computing Systems. *IEEE Internet Things J.* **2023**, *10*, 6652–6660. [[CrossRef](#)]
89. Rivest, R.L.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [[CrossRef](#)]
90. Brown, R.H.; Good, M.L.; Prabhakar, A. *Federal Information Processing Standards Publication: Secure Hash Standard*; U.S. Department of Commerce: Washington, DC, USA, 1993. [[CrossRef](#)]
91. National Institute of Standards and Technology (NIST); Dworkin, M.J.; Barker, E.; Nechvatal, J.; Foti, J.; Bassham, L.E.; Roback, E.; Dary, J.F., Jr. *Advanced Encryption Standard (AES)*; NIST: Gaithersburg, MD, USA, 2001. [[CrossRef](#)]
92. Koblitz, N.; Menezes, A.; Vanstone, S. The State of Elliptic Curve Cryptography. *Des. Codes Cryptogr.* **2000**, *19*, 173–193. [[CrossRef](#)]
93. Mobi. Available online: <https://dlt.mobi/> (accessed on 14 June 2024).

94. Khan, A.A.; Laghari, A.A.; Shaikh, A.A.; Bourouis, S.; Mamlouk, A.M.; Alshazly, H. Educational Blockchain: A Secure Degree Attestation and Verification Traceability Architecture for Higher Education Commission. *Appl. Sci.* **2021**, *11*, 10917. [CrossRef]
95. Gräther, W.; Kolvenbach, S.; Ruland, R.; Schütte, J.; Torres, C.; Wendland, F. Blockchain for education: Lifelong learning passport. In Proceedings of the 1st ERCIM Blockchain Workshop 2018: European Society for Socially Embedded Technologies (EUSSET), Amsterdam, The Netherlands, 8–9 May 2018. [CrossRef]
96. Hillman, V.; Ganesh, V. Kratos: A Secure, Authenticated and Publicly Verifiable System for Educational Data Using the Blockchain. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019; pp. 5754–5762. [CrossRef]
97. Guo, H.; Yu, X. A Survey on Blockchain Technology and Its Security. *Blockchain: Res. Appl.* **2022**, *3*, 100067. [CrossRef]
98. Blockcerts. Available online: <https://www.blockcerts.org/> (accessed on 14 June 2024).
99. Tempsta, S. *Introduction to Blockchain for Azure Developers: Understanding the Basic. Foundations of Blockchain*; Springer Nature: Dordrecht, The Netherlands, 2019; ISBN 978-1-4842-5311-3. [CrossRef]
100. Dos Santos, S.; Chukwuocha, C.; Kamali, S.; Thulasiram, R.K. An Efficient Miner Strategy for Selecting Cryptocurrency Transactions. In Proceedings of the 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019, Atlanta, GA, USA, 14–17 July 2019; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2019; pp. 116–123. [CrossRef]
101. Rajasekaran, A.S.; Azees, M.; Al-Turjman, F. A Comprehensive Survey on Blockchain Technology. *Sustain. Energy Technol. Assess.* **2022**, *52*, 102039. [CrossRef]
102. Szabo, N. Formalizing and Securing Relationships on Public Networks. *First Monday* **1997**, *2*, 548. [CrossRef]
103. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of Blockchains in the Internet of Things: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1676–1717. [CrossRef]
104. Wang, Q.; Li, R.; Wang, Q.; Chen, S. Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges. *arXiv* **2021**, arXiv:2105.07447. [CrossRef]
105. Ripple. Available online: <https://ripple.com/> (accessed on 15 June 2024).
106. Bera, B.; Chattaraj, D.; Das, A.K. Designing Secure Blockchain-Based Access Control Scheme in IoT-Enabled Internet of Drones Deployment. *Comput. Commun.* **2020**, *153*, 229–249. [CrossRef]
107. Feng, C.; Liu, B.; Guo, Z.; Yu, K.; Qin, Z.; Choo, K.-K.R. Blockchain-Based Cross-Domain Authentication for Intelligent 5G-Enabled Internet of Drones. *IEEE Internet Things J.* **2021**, *9*, 6224–6238. [CrossRef]
108. Bera, B.; Saha, S.; Das, A.K.; Kumar, N.; Lorenz, P.; Alazab, M. Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment. *IEEE Trans. Veh. Technol.* **2020**, *69*, 9097–9111. [CrossRef]
109. Singh, M.; Aujla, G.S.; Bali, R.S. ODOB: One Drone One Block-Based Lightweight Blockchain Architecture for Internet of Drones. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 249–254. [CrossRef]
110. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Srivastava, G.; Aledhari, M. Enabling Drones in the Internet of Things With Decentralized Blockchain-Based Security. *IEEE Internet Things J.* **2021**, *8*, 6406–6415. [CrossRef]
111. Wazid, M.; Bera, B.; Das, A.K.; Garg, S.; Niyato, D.; Hossain, M.S. Secure Communication Framework for Blockchain-Based Internet of Drones-Enabled Aerial Computing Deployment. *IEEE Internet Things Mag.* **2021**, *4*, 120–126. [CrossRef]
112. Gupta, R.; Kumari, A.; Tanwar, S. Fusion of Blockchain and Artificial Intelligence for Secure Drone Networking Underlying 5G Communications. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4176. [CrossRef]
113. Yu, G.; Zha, X.; Wang, X.; Ni, W.; Yu, K.; Yu, P.; Zhang, J.A.; Liu, R.P.; Guo, Y.J. Enabling Attribute Revocation for Fine-Grained Access Control in Blockchain-IoT Systems. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1213–1230. [CrossRef]
114. Singh, M.; Aujla, G.S.; Bali, R.S. A Deep Learning-Based Blockchain Mechanism for Secure Internet of Drones Environment. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4404–4413. [CrossRef]
115. Allouch, A.; Cheikhrouhou, O.; Koubâa, A.; Toumi, K.; Khalgui, M.; Nguyen Gia, T. Utm-Chain: Blockchain-Based Secure Unmanned Traffic Management for Internet of Drones. *Sensors* **2021**, *21*, 3049. [CrossRef] [PubMed]
116. Muram, F.U.; Atif Javed, M. Drone-Based Risk Management of Autonomous Systems Using Contracts and Blockchain. In Proceedings of the 2021 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), Honolulu, HI, USA, 9–12 March 2021; pp. 679–688. [CrossRef]
117. Dawaliby, S.; Aberkane, A.; Bradai, A. Blockchain-Based IoT Platform for Autonomous Drone Operations Management. In Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, London, UK, 25 September 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 31–36. [CrossRef]
118. Satheesh Kumar, M.; Vimal, S.; Jhanjhi, N.Z.; Dhanabalan, S.S.; Alhummyani, H.A. Blockchain Based Peer to Peer Communication in Autonomous Drone Operation. *Energy Rep.* **2021**, *7*, 7925–7939. [CrossRef]
119. SkyGrid. Available online: <https://www.skygrid.com/> (accessed on 15 June 2024).
120. Pierro, G.A.; Tonelli, R. Can Solana Be the Solution to the Blockchain Scalability Problem? In Proceedings of the 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering, (SANER 2022), Honolulu, HI, USA, 15–18 March 2022; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2022; pp. 1219–1226. [CrossRef]
121. CargoSmart. Available online: <https://www.cargosmart.com/en-us/> (accessed on 15 June 2024).

122. Kumar, R.; Tripathi, R. Chapter 2—Blockchain-Based Framework for Data Storage in Peer-to-Peer Scheme Using Interplanetary File System. In *Handbook of Research on Blockchain Technology*; Krishnan, S., Balas, V.E., Julie, E.G., Robinson, Y.H., Balaji, S., Kumar, R., Eds.; Academic Press: Cambridge, MA, USA, 2020; pp. 35–59, ISBN 978-0-12-819816-2. [CrossRef]
123. Gitopia. Available online: <https://gitopia.com/> (accessed on 16 June 2024).
124. Alzhrani, F.; Saeedi, K.; Zhao, L. Architectural Patterns for Blockchain Systems and Application Design. *Appl. Sci.* **2023**, *13*, 11533. [CrossRef]
125. Bao, Z.; Wang, Q.; Shi, W.; Wang, L.; Lei, H.; Chen, B. When Blockchain Meets SGX: An Overview, Challenges, and Open Issues. *IEEE Access* **2020**, *8*, 170404–170420. [CrossRef]
126. Guru, A.; Mohanta, B.K.; Mohapatra, H.; Al-Turjman, F.; Altrjman, C.; Yadav, A. A Survey on Consensus Protocols and Attacks on Blockchain Technology. *Appl. Sci.* **2023**, *13*, 2604. [CrossRef]
127. Liang, Y.; Wang, X.; Wu, Y.C.; Fu, H.; Zhou, M. A Study on Blockchain Sandwich Attack Strategies Based on Mechanism Design Game Theory. *Electronics* **2023**, *12*, 4417. [CrossRef]
128. Huang, Y.; Bian, Y.; Li, R.; Zhao, J.L.; Shi, P. Smart Contract Security: A Software Lifecycle Perspective. *IEEE Access* **2019**, *7*, 150184–150202. [CrossRef]
129. Kushwaha, S.S.; Joshi, S.; Singh, D.; Kaur, M.; Lee, H.N. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract. *IEEE Access* **2022**, *10*, 6605–6621. [CrossRef]
130. Mohanta, B.K.; Samal, K.; Jena, D.; Ramasubbareddy, S.; Karuppiyah, M. Blockchain-Based Consensus Algorithm for Solving Security Issues in Distributed Internet of Things. *Int. J. Electron. Bus.* **2022**, *17*, 283–304. [CrossRef]
131. Gabuthy, Y. Blockchain-Based Dispute Resolution: Insights and Challenges. *Games* **2023**, *14*, 34. [CrossRef]
132. Zeng, R.; You, J.; Li, Y.; Han, R. An ICN-Based IPFS High-Availability Architecture. *Future Internet* **2022**, *14*, 122. [CrossRef]
133. Lin, I.C.; Tseng, P.C.; Chen, P.H.; Chiou, S.J. Enhancing Data Preservation and Security in Industrial Control Systems through Integrated IOTA Implementation. *Processes* **2024**, *12*, 921. [CrossRef]
134. Mahmoud, M.A.; Gurunathan, M.; Ramli, R.; Babatunde, K.A.; Faisal, F.H. Review and Development of a Scalable Lightweight Blockchain Integrated Model (LightBlock) for IoT Applications. *Electronics* **2023**, *12*, 1025. [CrossRef]
135. Nie, Z.; Zhang, M.; Lu, Y. HPoC: A Lightweight Blockchain Consensus Design for the IoT. *Appl. Sci.* **2022**, *12*, 12866. [CrossRef]
136. Wang, G.; Shi, Z.J.; Nixon, M.; Han, S. SoK: Sharding on Blockchain. In Proceedings of the 1st ACM Conference on Advances in Financial Technologies, Zurich, Switzerland, 21–23 October 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 41–61. [CrossRef]
137. Liu, C.; Wan, J.; Li, L.; Yao, B. Throughput Optimization for Blockchain System with Dynamic Sharding. *Electronics* **2023**, *12*, 4915. [CrossRef]
138. Chen, R.; Wang, L.; Peng, C.; Zhu, R. An Effective Sharding Consensus Algorithm for Blockchain Systems. *Electronics* **2022**, *11*, 2597. [CrossRef]
139. Dennis, R.; Owenson, G.; Aziz, B. A Temporal Blockchain: A Formal Analysis. In Proceedings of the 2016 International Conference on Collaboration Technologies and Systems, (CTS 2016), Orlando, FL, USA, 31 October–4 November 2016; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2016; pp. 430–437. [CrossRef]
140. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access* **2019**, *7*, 22328–22370. [CrossRef]
141. Awan, K.A.; Ud Din, I.; Almogren, A.; Kim, B.S. Enhancing Performance and Security in the Metaverse: Latency Reduction Using Trust and Reputation Management. *Electronics* **2023**, *12*, 3362. [CrossRef]
142. Liu, M.; Wu, Q.; Hei, Y.; Li, D. Blockchain-Based Licensed Spectrum Fair Distribution Method towards 6G-Envisioned Communications. *Appl. Sci.* **2023**, *13*, 9231. [CrossRef]
143. 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] [PubMed]
144. Platt, M.; McBurney, P. Sybil in the Haystack: A Comprehensive Review of Blockchain Consensus Mechanisms in Search of Strong Sybil Attack Resistance. *Algorithms* **2023**, *16*, 34. [CrossRef]
145. Hou, D.; Zhang, J.; Huang, S.; Peng, Z.; Ma, J.; Zhu, X. Privacy-Preserving Energy Trading Using Blockchain and Zero Knowledge Proof. In Proceedings of the 2022 IEEE International Conference on Blockchain, Blockchain 2022, Espoo, Finland, 2–5 May 2022; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2022; pp. 412–418. [CrossRef]
146. Mahmood, Z.H.; Ibrahim, M.K. New Fully Homomorphic Encryption Scheme Based on Multistage Partial Homomorphic Encryption Applied in Cloud Computing. In Proceedings of the 2018 1st Annual International Conference on Information and Sciences (AiCIS), Fallujah, Iraq, 20–21 November 2018; pp. 182–186. [CrossRef]
147. Luu, L.; Chu, D.-H.; Olickel, H.; Saxena, P.; Hobor, A. Making Smart Contracts Smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 254–269. [CrossRef]
148. Tsankov, P.; Dan, A.; Drachler-Cohen, D.; Gervais, A.; Bünzli, F.; Vechev, M. Securify: Practical Security Analysis of Smart Contracts. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 67–82. [CrossRef]

149. Kalra, S.; Goel, S.; Dhawan, M.; Sharma, S. ZEUS: Analyzing Safety of Smart Contracts. In Proceedings of the 25th Annual Network and Distributed System Security Symposium, (NDSS 2018), San Diego, CA, USA, 18–21 February 2018; The Internet Society: Reston, VA, USA, 2018. [CrossRef]
150. McKeen, F.; Alexandrovich, I.; Berenzon, A.; Rozas, C.V.; Shafi, H.; Shanhogue, V.; Savagaonkar, U.R. Innovative Instructions and Software Model for Isolated Execution. In Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy, Virtual, 18 October 2021; Association for Computing Machinery: New York, NY, USA, 2013. [CrossRef]
151. Lafourcade, P.; Lombard-Platet, M. About Blockchain Interoperability. *Inf. Process Lett.* **2020**, *161*, 105976. [CrossRef]
152. Pillai, B.; Biswas, K.; Muthukkumarasamy, V. Cross-Chain Interoperability among Blockchain-Based Systems Transactions. *Knowl. Eng. Rev.* **2020**, *35*, 314. [CrossRef]
153. Hardjono, T.; Lipton, A.; Pentland, A. Toward an Interoperability Architecture for Blockchain Autonomous Systems. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1298–1309. [CrossRef]
154. Pang, Y. A New Consensus Protocol for Blockchain Interoperability Architecture. *IEEE Access* **2020**, *8*, 153719–153730. [CrossRef]
155. Tan, C.; Bei, S.; Jing, Z.; Xiong, N. An Atomic Cross-Chain Swap-Based Management System in Vehicular Ad Hoc Networks. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6679654. [CrossRef]
156. Popchev, I.; Radeva, I.; Doukovska, L. Oracles Integration in Blockchain-Based Platform for Smart Crop Production Data Exchange. *Electronics* **2023**, *12*, 2244. [CrossRef]
157. Caldarelli, G. Understanding the Blockchain Oracle Problem: A Call for Action. *Information* **2020**, *11*, 509. [CrossRef]
158. Bhushan, B.; Sharma, N. Transaction Privacy Preservations for Blockchain Technology. In *International Conference on Innovative Computing and Communications, Proceedings of the ICICC 2020, Delhi, India, 21–23 February 2020*; Gupta, D., Khanna, A., Bhattacharyya, S., Hassanien, A.E., Anand, S., Jaiswal, A., Eds.; Springer: Singapore, 2021; pp. 377–393. [CrossRef]
159. Lesaege, C.; Ast, F.; George, W. Kleros. White Paper. 2019. Available online: <https://kleros.io/whitepaper.pdf> (accessed on 2 August 2024).
160. European Parliament: Directorate-General for Parliamentary Research Services; Finck, M. *Blockchain and the General Data Protection Regulation—Can Distributed Ledgers Be Squared with European Data Protection Law?* Publications Office of the European Union: Luxembourg, 2019. [CrossRef]
161. Lin, I.C.; Liao, T.C. A Survey of Blockchain Security Issues and Challenges. *Int. J. Netw. Secur.* **2017**, *19*, 653–659. [CrossRef]
162. Orji, I.J.; Kusi-Sarpong, S.; Huang, S.; Vazquez-Brust, D. Evaluating the Factors That Influence Blockchain Adoption in the Freight Logistics Industry. *Transp. Res. E Logist. Transp. Rev.* **2020**, *141*, 102025. [CrossRef]
163. Lutfiani, N.; Aini, Q.; Rahardja, U.; Wijayanti, L.; Nabila, E.A.; Ali, M.I. Transformation of Blockchain and Opportunities for Education 4.0. *Int. J. Educ. Learn.* **2021**, *3*, 222–231. [CrossRef]
164. Beutel, D.J.; Topal, T.; Mathur, A.; Qiu, X.; Fernandez-Marques, J.; Gao, Y.; Sani, L.; Li, K.H.; Parcollet, T.; de Gusmão, P.P.B.; et al. Flower: A Friendly Federated Learning Research Framework. *arXiv* **2020**, arXiv:2007.14390. [CrossRef]
165. Li, H.; Han, D. EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme. *IEEE Access* **2019**, *7*, 179273–179289. [CrossRef]
166. Chohan, U.W. Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability. In *Cryptofinance and Mechanisms of Exchange: The Making of Virtual Currency*; Goutte, S., Guesmi, K., Saadi, S., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 165–177, ISBN 978-3-030-30738-7. [CrossRef]
167. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain Technology and Its Relationships to Sustainable Supply Chain Management. *Int. J. Prod. Res.* **2019**, *57*, 2117–2135. [CrossRef]
168. Kosmarski, A. Blockchain Adoption in Academia: Promises and Challenges. *J. Open Innov. Technol. Mark. Complex.* **2020**, *6*, 117. [CrossRef]
169. Mirabelli, G.; Solina, V. Blockchain and Agricultural Supply Chains Traceability: Research Trends and Future Challenges. *Procedia Manuf.* **2020**, *42*, 414–421. [CrossRef]
170. Torky, M.; Hassanein, A.E. Integrating Blockchain and the Internet of Things in Precision Agriculture: Analysis, Opportunities, and Challenges. *Comput. Electron. Agric.* **2020**, *178*, 105476. [CrossRef]
171. Upadhyay, N. Demystifying Blockchain: A Critical Analysis of Challenges, Applications and Opportunities. *Int. J. Inf. Manag.* **2020**, *54*, 102120. [CrossRef]

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