Review

Securing Large Healthcare Files in Cloud-Blockchain Integration: A Comprehensive Review

Leonardo Juan Ramirez Lopez * , David Felipe Millan , Luis Hernando Martinez , Andres Carbonell , Wilson Mauro Rojas Reales

Posted Date: 7 February 2024

doi: 10.20944/preprints202402.0453.v1

Keywords: Blockchain; Cloud; Security; Healthcare; Integrity

Review

Securing Large Healthcare Files in Cloud-Blockchain Integration: A Comprehensive Review

Leonardo J Ramirez Lopez *, David Millan, Luis Hernando Martinez, Andres Carbonell and Wilson Rojas

Engineering Faculty. Osiris & Bioaxis Research Group. Universidad El Bosque. Bogota, Colombia; osiris@unbosque.edu.co

* Correspondence: ljramirezl@unbosque.edu.co; Tel.: +573114905014

Abstract: The management of large medical files is a critical challenge in the health sector. Conventional systems have security, scalability, and efficiency deficiencies. This project proposes a hybrid architecture between blockchain and cloud computing to address these challenges. Blockchain ensures the immutability and traceability of medical records, while the cloud allows scalable and efficient storage. Together, these technologies can transform data management in electronic health record applications. The essential objective of this research is to thoroughly look at the existing strategies, devices, and conventions that encourage a secure interaction between blockchain applications and the cloud. Special emphasis is set on maintaining the integrity and security of the blockchain while tackling the potential and efficiency of cloud infrastructures. Through a meticulous investigation of these approaches, along with their successful usage and encountered challenges, this paper offers a comprehensive overview of the present state of this integration. Altogether, this paper does not propose new concepts or developments. Its central focus is to provide a comprehensive and insightful examination of the modern landscape concerning the integration of blockchain and cloud advances. By shedding light on the existing approaches and assessing their viability, this work aims to highlight the current challenges and build up a solid establishment for future development. This, in turn, will cultivate a consistent integration of blockchain security with the dynamic potential of cloud computing while guaranteeing information integrity and security remain uncompromised. In conclusion, this paper serves as a important resource for analysts, specialists, and partners looking for to dig into and development the integration of blockchain and cloud innovations, subsequently contributing to a more secure and productive cloud environment.

Keywords: Blockchain; Cloud; Security; Healthcare; Integrity

1. Introduction

The integration of blockchain technology and cloud computing has emerged as a promising innovation to address the data storage challenges in our increasingly digital world. As the volume of data continues to grow exponentially, securely storing, managing, and retrieving large files has become a critical issue. Blockchain's immutability and cryptographic security make it well-suited to ensure data integrity and trustworthiness [1,2]. Meanwhile, cloud computing offers scalable and cost-effective data storage solutions [3]. However, concerns around data security and privacy exist due to the centralized nature of cloud storage [4].

Bridging the security of blockchain with the practical data storage capacity of the cloud represents an opportunity. This study explores the complex interplay between these two transformative technologies with the goal of devising a novel solution that balances both security and scalability [3]. We analyze existing research on blockchain and cloud computing integration to understand the methodologies and insights needed to create this hybrid paradigm [3,5–19]. We thoroughly examine pertinent literature, drawing from numerous scholarly contributions on this

 doi:10.20944/preprints202402.0453.v1

topic. Our exploration covers the technical dimensions of blockchain, including its service models and security frameworks, along with analyzing the performance implications when integrated with cloud data centers [20,21].

1.2. Discussion of challenges and limitations in the field of study

- **Efficiency and Scalability:** Transaction efficiency and scalability are essential issues in blockchain. Adding interactions with the cloud can increase complexity and the time required to complete transactions, which can reduce efficiency. Scalability becomes a problem when handling large volumes of data from the cloud to the blockchain, leading to network congestion and longer processing times [22,23].
- **Costs and Sustainability:** Implementing blockchain and cloud solutions can be costly, both in terms of infrastructure and energy consumption. Sustainability and energy efficiency are important considerations, especially at a time when the carbon footprint of blockchain is under scrutiny. Researching more energy-efficient solutions is crucial [24].
- **Interoperability and Standards:** Interoperability between different blockchains and cloud providers can be a problem. The lack of common standards and protocols can hinder seamless integration. Researching and developing standards to ensure smooth interaction is essential [2].
- **Quantum computing resistance:** With the development of quantum computing, resistance to quantum attacks becomes a concern. Blockchain and the cloud must be resilient to these emerging technological challenges [25].
- **Centralization vs Decentralization:** Striking the balance between centralization and decentralization is a dilemma. Some solutions may require a degree of centralization, which goes against the fundamental principles of blockchain. Finding the right balance is essential [25–27].

1.3. Study Objectives and Motivation Behind Them

The study aims to examine and provide a comprehensive review of research that integrate Cloud and Blockchain technologies. This with the objective of explore and learn the existing ways of accomplishing a successful integration between these two technologies and large healthcare files. Therefore, to achieve this, the PRISMA methodology is used to explore and sort the papers among the databases. For this reason, the following databases were selected among others due to the relevance and amount of content that can be found in them. Scopus, Engineering village, MDPI, Elsevier, Google Scholar and IEEE were the selected databases from which the papers were extracted along this review. As a result of this overarching objective the investigation to address specific research questions (RQ):

RQ1: What is the distribution of papers across different years?

RQ2: How are the chosen papers related to the proposed keywords?

RQ3: Which of the papers explores blockchain and cloud computing as review?

RQ4: Which papers explore the blockchain-cloud computing and healthcare?

RQ5: In the current landscape of secure blockchain and cloud integration, what constitutes the primary challenges that organizations and practitioners face?

1.4. Contributions

Throughout this study, we conduct a comprehensive review of papers related to blockchain, cloud, security, and healthcare. This involved carefully selecting papers that met specific parameters established by us, from among thousands available. Our criteria for paper selection dictated that only papers released between 2017 and 2023 were considered, aimed at avoiding outdated architectures or methodologies.

The study aims to provide an extensive overview of the secure integration of blockchain technology and cloud computing in the contemporary landscape. The primary contributions of our research can be summarized as follows:

 doi:10.20944/preprints202402.0453.v1

- Synthesis of key findings to provide a comprehensive understanding of the current state of secure integration in the given domains. Classification based on topics and keywords.
- Recommendations for future research and potential areas for improvement in the integration of blockchain technology and cloud computing for enhanced security in healthcare applications.
- Analysis of emerging trends and innovative approaches in the secure integration of blockchain and cloud computing.
- Explore challenges and field limitations.

2. Material and Methods

Extensive prior work exists exploring Blockchain-Cloud integration with an emphasis on security and chain integrity has been extensively explored with a hybrid blockchain architecture for Cloud Manufacturing-as-a-Service (CMaaS) platforms, emphasizing improved data storage efficiency. As mentioned previously a hybrid blockchain architecture for Cloud Manufacturing-as-a-Service platforms to improve data storage efficiency. This seminal work demonstrated the advantages of a hybrid blockchain approach for enhanced data management [23].

Likewise, another paper explores regulatory compliance in multi-cloud blockchain deployment. By decentralizing identity, their user-centric model aimed to follow GDPR while exploiting blockchain's security properties across interconnected clouds. Their insights advanced compliance along with unlocking blockchain's potential [28,29].

Healthcare data integrity motivated new techniques like it is proposed in [30], who proposed a blockchain-enabled bioacoustics signal authentication system for cloud-based electronic medical records. This work emphasized the importance of securing medical data through innovative authentication techniques.

Moreover, the reviews presented in papers [2,31], provided a comprehensive overview of blockchain technology in healthcare, emphasizing its role in ensuring data security and privacy. Their authoritative overview illuminated blockchain's prospects and challenges, cementing foundational knowledge.

Looking beyond healthcare, [32–37] explored the role of blockchains and decentralized oracle networks in technology-enabled financing for sustainable infrastructure. Their focus on secure and decentralized financial transactions within a blockchain context contributed to understanding the broader applications beyond healthcare.

Additionally, studies such as Berdik D. et al. [38] and Taghavi et al. [33] delved into secure access frameworks and reliability models for blockchain oracles, respectively, shedding light on crucial security aspects in blockchain-enabled systems.

Collectively, this extensive research reinforces the rising significance of security and chain integrity in multi-disciplinary blockchain-cloud integration, with far-ranging potential from healthcare to finance.

2.1. PRISMA

Is an evidence-based minimum set of items for reporting in systematic reviews and meta-analyses. It primarily focuses on the reporting of reviews evaluating the effects of interventions but can also be used as a basis for reporting systematic reviews with objectives other than evaluating interventions (e.g., evaluating aetiology, prevalence, diagnosis, or prognosis) [39]. Serving as a foundational tool for systematic reviews across various fields.

2.1.1. Why PRISMA?

Preferred Reporting Items for Systematic Reviews and Meta-Analyses -PRISMA is a valuable tool in research due to its role in enhancing the transparency, reliability, and overall quality of systematic reviews and meta-analyses. By providing a standardized reporting framework, PRISMA ensures that researchers clearly articulate their methods, from the systematic search process to study selection and data extraction. Also, offers several benefits in online training for students, educators, researchers, and readers:

- Reduction of Bias: PRISMA includes guidelines that aim to reduce bias in systematic reviews. Transparent reporting helps readers assess the risk of bias in the included studies, leading to a more accurate interpretation of the evidence.
- It enables self-regulated learning by providing systematic search procedures (identification, screening, eligibility, inclusion) via online platforms.
- Serves as a valuable guide for postgraduate students and researchers in conducting comprehensive searches to find necessary papers.
- Aids readers by offering a clear understanding of the process, enabling easy tracking of information sources through systematic review records, and simplifying the evaluation of reported systematic reviews.
- Support for Evidence-Based Practice: PRISMA contributes to the production of high-quality evidence that can be used to inform evidence-based practice, clinical guidelines, and policy decisions.

2.2. Search engines and search equations

Towards the selection of the papers, various criteria and filters established by us were taken into account, aiming to separate those papers that could contain outdated information or focus on other areas of study. The first step was to formulate the search equations, which focused on the proposed keywords that are mostly related to our research questions:

- "Blockchain and Cloud Storage Integration" OR "Blockchain and Cloud Computing" OR "Secure Cloud Storage with Blockchain" OR "Decentralized Cloud Storage" OR "Blockchain-Based Data Security in Cloud" OR "Blockchain for Large File Storage" OR "Blockchain and Cloud Security" OR "Cloud-Based Blockchain Applications" OR "Blockchain for Data Integrity in Cloud" OR "Cloud Exchange with Blockchain" OR "Blockchain and Supply Chain Management" OR "Blockchain in Operations and Supply Chain" OR "Blockchain and Cloud Services" OR "Blockchain in Cloud Infrastructure" OR "Blockchain-Based Cloud Services" OR "Blockchain-Based Cloud Storage Solutions."
- Blockchain AND Security AND Cloud
- ("All Metadata": Blockchain) AND ("All Metadata": Cloud)
- Blockchain and cloud and security and Healthcare
- Blockchain AND oracles

The search engines used were Elsevier (ScienceDirect), Google Scholar, IEEE Xplore, and MDPI. As mentioned before only papers from 2017 onwards were selected, in the first stage, we encounter with a massive number of papers, above 23 thousand, this adding up all the 4 selected data bases. As a result of this huge number of papers we stablish criteria to separate those papers that moved away from our purpose and objective. After this first year of publish filter, we decided to remove all those scripts that talked about crypto currencies or any other topic, but secure Blockchain applied to cloud computing. After applying some other filters (Figure 1), for further information about PRISMA check the Appendix A, where the PRISMA for each database will be found) we ended up having over 100 papers that serve our purpose.

 doi:10.20944/preprints202402.0453.v1

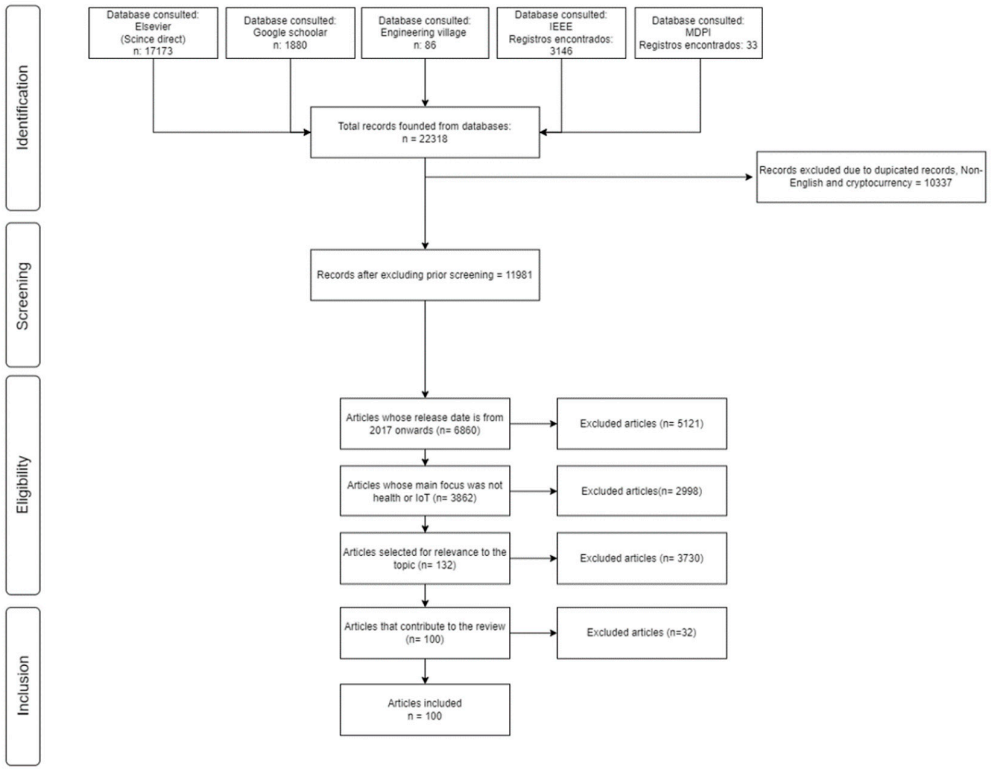


Figure 1. Flowchart for selected papers based on PRISMA.

2.3. Incorporation and Exclusion Parameters

Studies incorporated in our comprehensive review should suggest an investigation around a secure integration of blockchain and cloud computing or suggest viable ways to connect a chain of blocks with data stored in cloud. Also, we take into account those papers that mention cloud, Blockchain and healthcare. Table 1 provides more details about inclusion/exclusion criteria used on the papers.

Table 1. Criteria of inclusion/exclusion.

Papers included	Papers excluded
Papers must talk about Blockchain and cloud integration. Papers that mention ways of securely connect cloud with blockchain and show the process. Review papers that help the purpose and objective of this paper.	Papers that focus on cryptocurrencies or its focus is Internet of Things. Papers published before 2017 Papers that proposed storing the chain in cloud.

3. Results

In this section, we present the outcomes of our comprehensive review focused on the integration of blockchain and cloud technologies within the healthcare domain. Our analysis, involving an exhaustive examination of over 100 selected papers, aimed to discern patterns, trends, and insights pertaining to the current landscape of blockchain-cloud secure integration in managing large healthcare files.

The results presented herein are encapsulated through a series of tables and graphics meticulously crafted by our team. These visual representations serve to categorize and dissect the

 doi:10.20944/preprints202402.0453.v1

diverse range of papers we scrutinized, shedding light on key themes, methodologies, and emerging areas of interest within the intersection of blockchain, cloud, and healthcare.

3.1. Results based on the proposed reasearch questions

RQ1: What is the distribution of papers across different years?

As shown in the Table 2 there are no papers included before 2017 due to the lack of papers that talk about blockchain and cloud integration. Besides of the lack of papers those few papers that can be found before 2017 could have outdated data or propose solutions that nowadays are not viable because they can become obsolete. The data reveals a progressive increase in scholarly contributions over time, reaching a peak in 2022 with 23 papers. The surge in publications from 2020 onwards suggests a growing interest and heightened focus on the integration of blockchain and cloud technologies within the context of healthcare. This temporal trend underscores the contemporary relevance and evolving nature of research in this domain, showcasing the increasing importance and recognition of blockchain-cloud integration in managing large healthcare files.

Table 2. Distribution of papers by years.

Years	Number of papers
2017	4
2018	4
2019	10
2020	20
2021	16
2022	23
2023	24

RQ2: How are the chosen papers related to the proposed keywords?

During the research for papers, we encounter that the majority of the good papers were trying to go beyond a simple connection between Blockchain and cloud, they were exploring options not only to make a connection but to make it secure while keeping the integrity of the chain. As it is shown in Table 3 most of the papers talk about security and Block-chain-Cloud or chain integrity. On the other hand, the Figure 2 shows in percentage how the topics of the papers are distributed, based on the graph we can say that most of them speaks of blockchain-cloud security.

Table 3. Classification of research papers on blockchain and cloud based on given keywords.

Work	Security	Review/ Survey	Blockchain-Cloud	Chain Integrity	Healthcare
[40,41]	X	X	X	X	
[4,15,26,28,30,40–58]	X		X	X	
[3,5,10–14,16,18–23,29,32–35,37,59–82]			X	X	
[43,83,84]	X		X		
[25,85–88]			X		
[1,6,7,9,17,27,89–91]		X	X	X	
[92]	X				
[10,58]			X	X	X

RQ3: Which of the papers explores blockchain and cloud computing as review?

The Figure 2 shows the percentage that represents the application fields of the papers. It should be noted that in the graph the lowest percentage is in those papers that include healthcare. Nonetheless, we were able to find 4 papers that are reviews and have a similar focus in their research.

 doi:10.20944/preprints202402.0453.v1

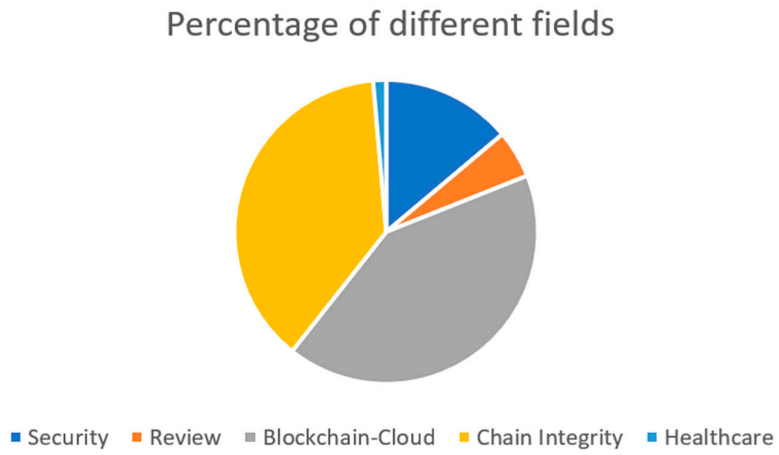


Figure 2. Application fields of the papers.

Table 4. Papers that explore blockchain and cloud computing as review.

Work	Title	Area of focus	Content
[91]	Integration of Block-chain and Cloud Computing: A Review.	Blockchain, Cloud Computing and security.	Explores the rising use of block-chain for enhancing cloud data security across various sectors. Suggests integrating blockchain to ad-dress vulnerabilities in centralized cloud computing systems. The focus is on reviewing the benefits and applications of cloud-based blockchain services, emphasizing current trends and security challenges.
[1]	Blockchain and Cloud Computing-A Review	Blockchain and Cloud Computing	Examine literature on blockchain-based enterprise solutions from 2008 to 2021. It explores three categories: Blockchain using IaaS, PaaS, and SaaS, discussing characteristics and their relation to cloud services. The study investigates cutting-edge applications in ledger storage, strategy creation, computation, data aggregation, micro-services, and extraction. The report concludes with current issues, expected obstacles, and potential opportunities in blockchain-based cloud technology, aiming to contribute to a comprehensive understanding and the future development of cloud computing environments.
[8]	Literature Review of Blockchain-based Cloud Computing: Data Security Issues and Challenges	Blockchain, Cloud Computing, Security Issues and Challenges	This paper highlights the growing acceptance of cloud computing for handling IT infrastructure and data services efficiently. Also, explores how blockchain technology, known for its incorruptible nature, can address security issues in cloud applications. As well the paper emphasizes the importance of security in realizing the benefits of both cloud computing and block-chain. It proposes a literature review to examine how academics utilize blockchain to enhance cloud data security.
[8]	Blockchain Technology Application in	Blockchain, Cloud Computing and security.	The study focuses on categorizing blockchain types, consensus mechanisms, smart contract usage, and integration with other software-based algorithms. The authors emphasize the increasing popularity of

 doi:10.20944/preprints202402.0453.v1

Security: A Systematic Review	blockchain beyond digital currencies, particularly in securing networks. The systematic review identifies the Internet of Things (IoT) as the primary field where blockchain enhances security.

RQ4: Which papers explore the blockchain, cloud computing and healthcare, and what they contribute?

The presented papers enlighten the challenges, intricacies, and prospective ways for exploration in the context of integrating blockchain and cloud technologies within the healthcare domain. These scholarly works provide comprehensive insights into the intricate dynamics, outlining the nuanced difficulties associated with such integration. Additionally, they articulate potential trajectories for navigating the complex landscape of merge blockchain and cloud in healthcare settings (Table 5).

Table 5. Analysis of blockchain and cloud Integration.

Work	Title	Contribution(s)
[2]	A Critical Analysis of Progress and Challenges in the Last Five Years	The paper significantly contributes by objectively evaluating the impact of blockchain technology in the healthcare sector, drawing insights from a thorough analysis of 124 papers published by MDPI over the past five years. Its noteworthy identification of advancements, such as improved data security and interoperability, adds depth to our understanding of blockchain's positive influence on healthcare.
[31]	A. Modernizing the Legacy Healthcare System to Decentralize Platform Using Blockchain Technology.	The authors aim to address challenges related to complex medical procedures, large-scale medical data management, and cost optimization. The paper reviews existing literature and proposes workflows for better data management, implemented using the Ethereum blockchain platform. The feasibility of the proposed system is analyzed in terms of associated costs, and a model-driven engineering approach is used to recover the architecture of traditional healthcare systems.
[93]	Design of Secure Protocol for Cloud-Assisted Electronic Health Record System Using Blockchain	Addresses the challenges of electronic health record (EHR) management in traditional systems and proposes a secure protocol using blockchain and cloud computing. The authors highlight the potential of blockchain technology to enable sharing of EHRs across various medical service centers, promoting decentralization and data integrity. However, the integration of cloud computing into the EHR system introduces security vulnerabilities, as sensitive data is transmitted over public channels. The proposed secure protocol aims to address these challenges by using blockchain for data integrity and access control, while the cloud server manages and stores patient EHRs securely. Elliptic curve cryptosystems (ECC) are employed for secure health data sharing within the cloud computing environment.

RQ5: In the current landscape of secure blockchain and cloud integration, what con-constitute the primary challenges that organizations and practitioners face?

As it was previously mentioned there are several challenges to accomplish a secure integration between blockchain and cloud, that's why the papers that will come up next are the most valuable for the purpose of this research. Within Table 6 the most relevant challenges will be shown for each paper mention along the Table 6.

 doi:10.20944/preprints202402.0453.v1

Table 6. Main challenges in the current landscape of secure blockchain and cloud integration.

Work	Title	Challenges
[27]	Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges	Cloud computing introduces new security challenges in secure service management and control, privacy protection, data integrity protection in distributed databases, data backup, and synchronization. Blockchain can be leveraged to address these challenges, partly due to the underlying characteristics such as transparency, traceability, decentralization, security, immutability, and automation. Also, the team explores how cloud computing can affect blockchain, especially about the performance improvements that cloud computing can provide for the blockchain.
[87]	Toward Decentralized Cloud Storage With IPFS: Opportunities, Challenges, and Future Considerations	Content availability: IPFS relies on peers to host content, which can lead to content unavailability if the peers hosting the content go offline. Content discovery: IPFS uses content addressing to locate content, which can be challenging when the content is not popular or has not been accessed recently. Content integrity: IPFS does not provide any guarantees about the integrity of the content, which can be compromised if the content is modified by a malicious peer. Content privacy: IPFS does not provide any privacy guarantees, which can lead to privacy violations if the content is accessed by unauthorized parties. Content distribution: IPFS does not provide any mechanisms for incentivizing peers to host content, which can lead to uneven distribution of content.
[8]	Literature Review of Blockchain-based Cloud Computing: Data Security Issues and Challenges	Data privacy: Blockchain-based cloud computing presents challenges in ensuring data privacy, as the data is stored in a decentralized manner and is accessible to all nodes in the network. Data integrity: Ensuring data integrity is a challenge in blockchain-based cloud computing, as the data is stored in a decentralized manner and is accessible to all nodes in the network. Scalability: Blockchain-based cloud computing presents scalability challenges, as the number of nodes in the network increases, the time required to reach consensus increases. Interoperability: Interoperability is a challenge in blockchain-based cloud computing, as different blockchains may have different protocols and standards. Regulatory compliance: Blockchain-based cloud computing presents regulatory compliance challenges, as the regulatory framework for blockchain technology is still evolving.
[94]	Blockchain and Healthcare: A Critical Analysis of Progress and Challenges in the Last Five Years	Data privacy: Blockchain-based cloud computing presents challenges in ensuring data privacy, as the data is stored in a decentralized manner and is accessible to all nodes in the network. Data integrity: Ensuring data integrity is a challenge in blockchain-based cloud computing, as the data is stored in a decentralized manner and is accessible to all nodes in the network.

 doi:10.20944/preprints202402.0453.v1

		Scalability: Blockchain-based cloud computing presents scalability challenges, as the number of nodes in the network increases, the time required to reach consensus increases. Interoperability: Interoperability is a challenge in blockchain-based cloud computing, as different blockchains may have different protocols and standards. Regulatory compliance: Blockchain-based cloud computing presents regulatory compliance challenges, as the regulatory framework for blockchain technology is still evolving.
[31]	A. Modernizing the Legacy Healthcare System to Decentralize Platform Using Blockchain Technology	Migrated classes: Ensure that the migrated classes are compatible with the blockchain platform. This requires a deep understanding of the blockchain architecture, and the programming languages used to write smart contracts. Patient mobility: When patients move from one hospital to another, their data may be dispersed among multiple hospitals, making it difficult for them to access their medical records.

4. Discussion

This comprehensive review of almost 100 recent papers provides valuable insights into the current landscape and progress of secure blockchain-cloud integration for healthcare data management. Our analysis reveals several notable themes and trajectories that warrant further discussion.

Overall, the steady increase in publications over recent years highlights the growing recognition of the potential benefits between blockchain and cloud technologies. The predominant focus on security, integration approaches, and chain integrity underscores the importance of these factors in realizing the benefits of this merger.

Our findings corroborate conclusions from previous seminal works regarding the role of blockchain in addressing vulnerabilities introduced by cloud computing through enhanced transparency, traceability, decentralization, and automation [27]. The reviewed papers also align with earlier studies emphasizing the need to balance blockchain's security with the performance and efficiency gains enabled by the cloud [23].

However, substantial challenges remain when it comes to practical implementation. Scalability is a persistent issue, as the volume of healthcare data continues to expand exponentially [22]. While some proposed solutions aim to improve transaction efficiency, network congestion and lag times persist. The lack of common standards and protocols also hinders interoperability between diverse blockchain implementations and cloud providers [2].

This review reveals a range of innovative techniques and architectures seeking to overcome these hurdles, from decentralized oracles [33] to bioacoustics authentication mechanisms [30]. However, regulatory uncertainties around emerging blockchain models present additional complications [8]. More research is needed to determine optimal frameworks that comply with data protection regulations.

Looking ahead, several promising trajectories can be discerned from this review. Hybrid on-chain/off-chain architectures could help address scalability limitations [23]. Advances in cryptography, trusted execution environments, and zero-knowledge proofs may expand privacy-preserving capabilities [25]. And decentralized storage networks with built-in incentives could reduce reliance on third-party cloud providers [87].

 doi:10.20944/preprints202402.0453.v1

The discussion surrounding the integration of blockchain and cloud computing encompasses critical aspects as presented in the reviewed papers. In Paper [31], emphasis is placed on the myriad architectures and models for this integration, recognizing the importance of adaptability to diverse contexts. However, Paper [43] raises concerns regarding potential interoperability challenges stemming from this diversity.

There is a convergence of opinions between Papers [31,43] regarding security. Both acknowledge the significance of addressing security challenges in cloud service management and decentralized storage.

Concerning performance, Paper [31] underscores improvements that cloud computing can offer to blockchain, while the authors of Paper [43] pose challenges that the decentralized nature of IPFS faces, raising scalability concerns.

Papers [53,95,96] extend the focus towards the application of blockchain in the healthcare sector. The authors of Paper [95] highlight advancements and challenges in incorporating blockchain in healthcare, emphasizing its benefits in ensuring data integrity and patient privacy. However, Paper [96] delves into the intricacy of medical procedures and large-scale data management through blockchain, highlighting potential associated costs.

In terms of costs, the authors of Paper [96] conduct an economic feasibility analysis and conclude that their proposal is practical and efficient. However, delving deeper into the economic considerations in the integration of blockchain and the cloud from the perspective of other authors would be insightful.

All papers recognize challenges in integrating blockchain and cloud computing, such as security issues, interoperability, and scalability. Identifying areas for improvement and providing recommendations for future research are consistent across [31,43,53,95,96].

The categorization of blockchain into public, private, and consortium types, as discussed in [99], has implications for the design and deployment of blockchain solutions. Understanding the selection criteria for these types can provide valuable insights for practitioners and researchers, reinforcing the importance of tailoring blockchain architecture to specific use cases.

Consensus mechanisms, explored in [99], are pivotal in maintaining a fair and decentralized network. The comparison of different algorithms, such as proof of work (PoW) and Practical Byzantine Fault Tolerance (PBFT), sheds light on the trade-offs involved in selecting consensus mechanisms. This aligns with the scalability discussions in [43,96], emphasizing the need for efficient and sustainable blockchain solutions.

The systematic review establishes a foundation for future research directions, as highlighted in [99]. The identified research gaps, coupled with the proposed future topics, can guide scholars and academics interested in advancing the field of blockchain security applications. This foresight adds depth to the ongoing discourse on the evolution of blockchain technology.

In summary, the integration of blockchain and cloud computing is a complex field presenting challenges and opportunities. There is a clear need for a balanced approach to address economic, technical, and security aspects. The dialogue among different authors provides a comprehensive insight that can guide future research towards more robust and effective solutions.

5. Conclusions

This comprehensive review aimed to examine the current landscape and state of secure integration between blockchain technology and cloud computing for managing large healthcare files. Through a systematic analysis of almost 100 recent research papers, key insights have been synthesized to provide an overview of the progress, open challenges, and future trajectories related to this merger. The study reveals a steady increase in publications on blockchain-cloud integration over the past five years, with a heavy focus on security, integration approaches, and chain integrity. While blockchain shows promise in addressing vulnerabilities introduced by centralized cloud architectures, substantial challenges persist around efficiency, scalability, interoperability, and regulatory compliance.

 doi:10.20944/preprints202402.0453.v1

Nevertheless, the reviewed papers highlight innovative techniques and architectures that could help overcome these hurdles. Hybrid on-chain/off-chain designs, advances in cryptography and trusted execution environments, and decentralized storage networks represent promising pathways forward. More research is still needed to optimize solutions that balance scalability and efficiency with the security and privacy assurances of blockchain technology. Our analysis outlines key challenges and opportunities that can inform future research and development in this domain. Overall, the integration of these technologies shows considerable potential, but ongoing work is required to enable the practical realization of secure, decentralized, and performant systems for healthcare data management. This review provides a foundation and reference point to guide progression in this emergent field. Through a comprehensive analysis of scholarly literature, we reviewed the contemporary landscape regarding blockchain-cloud convergence. In these conclusive remarks, we synthesize principal discoveries from across pertinent papers to highlight prevailing limitations, research gaps, and progress thus far. The intention underpinning these closures aims not to prescribe definitive solutions but rather survey the issues at hand to guide future advancement towards impactful integration for transformed clinical data practices. The paragraphs that follow encapsulate key conclusions and takeaways within this vital pursuit. That's why the following conclusions are proposed:

- This comprehensive review highlights the growing interest and importance of integrating blockchain and cloud technologies for securing large healthcare files. The number of relevant publications on this topic has steadily increased since 2017, peaking in 2022, indicating rising scholarly attention. Most examined papers emphasize the need for enhanced security, exploring blockchain's potential to ensure integrity and traceability of medical records, while leveraging the storage capacity and efficiency of the cloud.
- Analysis of the literature reveals pressing challenges that still need to be addressed, including efficiency, scalability, costs, interoperability, quantum computing resistance, and balancing centralization with decentralization. Overcoming these limitations is crucial for fully realizing the potential of blockchain-cloud integration.
- This review serves as a launch pad for scholars and practitioners seeking to further develop the secure convergence of blockchain and cloud computing in healthcare settings. By highlighting accomplishments thus far, and exposing knowledge gaps, it provides a foundation to build upon through continued exploration of this promising integration.

While progress has been made, as evidenced by some proposed techniques and models, there remain unanswered questions and ample room for innovation. More research is still required, especially surrounding standards, incentives, and sustainability of blockchain-enabled cloud systems managing large medical data.

Author Contributions: This review study has the following individual contributions: Conceptualization, LJRL and DM; methodology, LJRL, LHM; software, DM, LHM and AC; validation, LJRL and WR; formal analysis, LJRL and DM; research, LJRL, DM, LHM, AC and WR; resources, LJRL, DM, LHM, AC and WR; data curation, LJRL, DM and LHM; writing—original draft preparation, DM, and LHM; writing: review and editing, LJRL and DM; visualization, LJRL and LHM; supervision, LJRL; project management, LJRL and WR; acquisition financing, LJRL, DM, LHM, AC and WR. All authors have read and accepted the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: no new data were created.

Acknowledgments: The authors acknowledge Universidad El Bosque for support and access to scientific databases.

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

 doi:10.20944/preprints202402.0453.v1

Appendix A

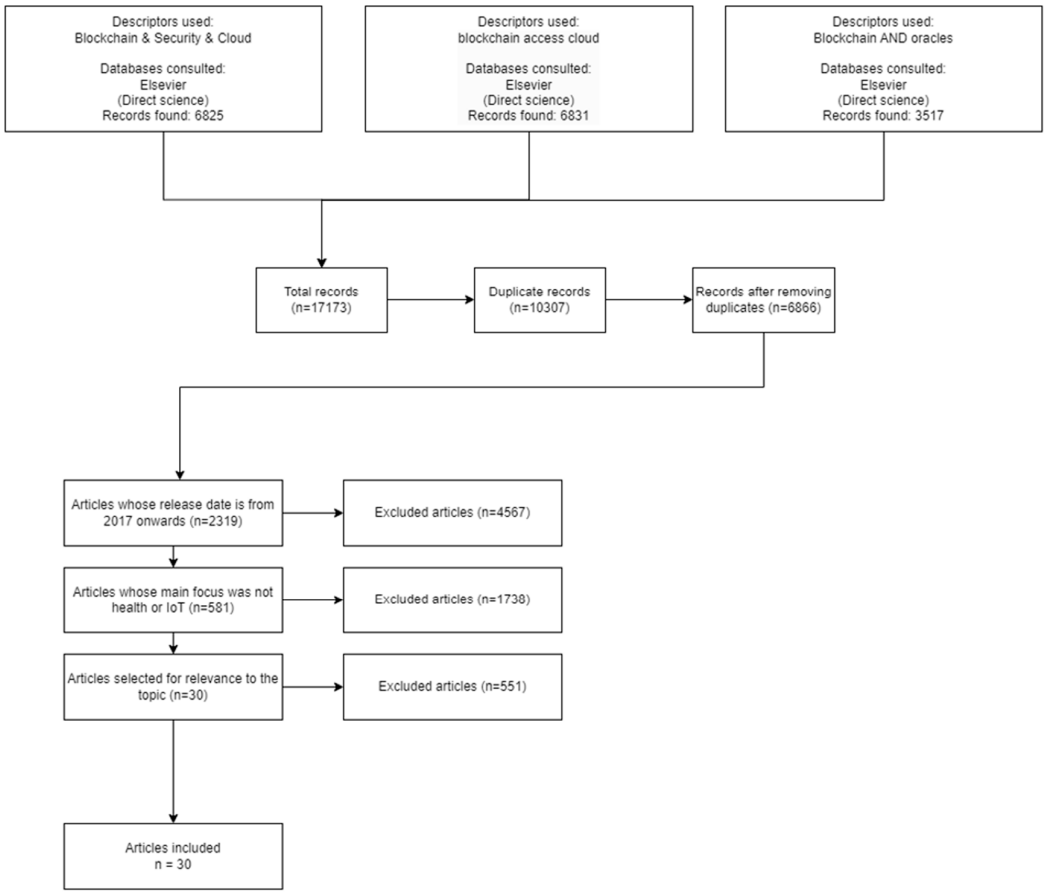
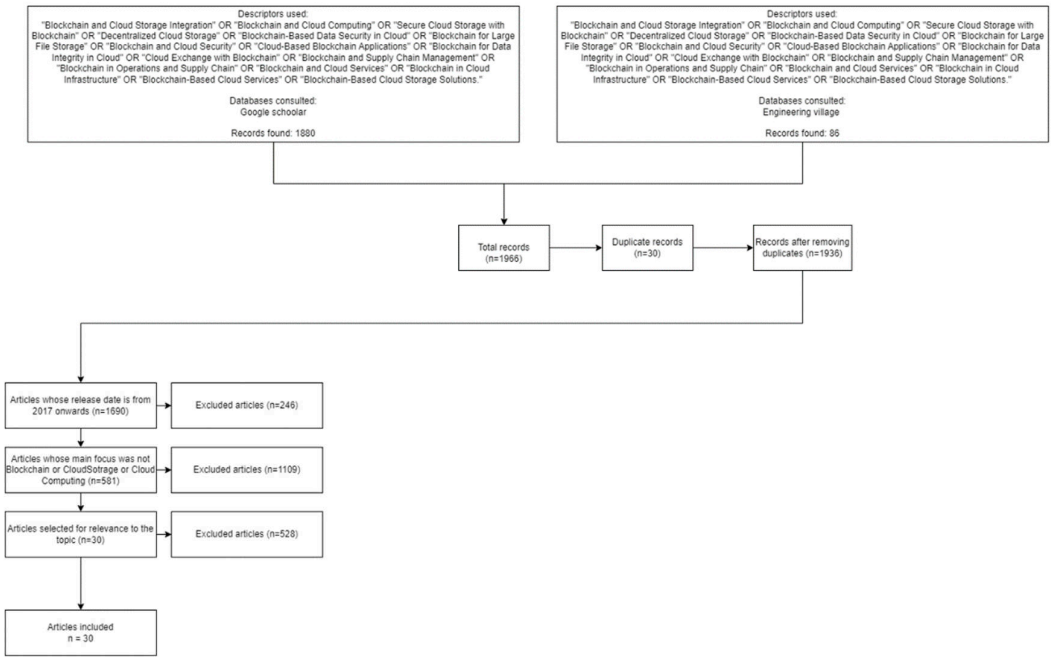


Figure A1. Flowchart for selected papers on Elsevier (ScienceDirect).



 doi:10.20944/preprints202402.0453.v1

Figure A2. Flowchart for selected papers on Google scholar **.**

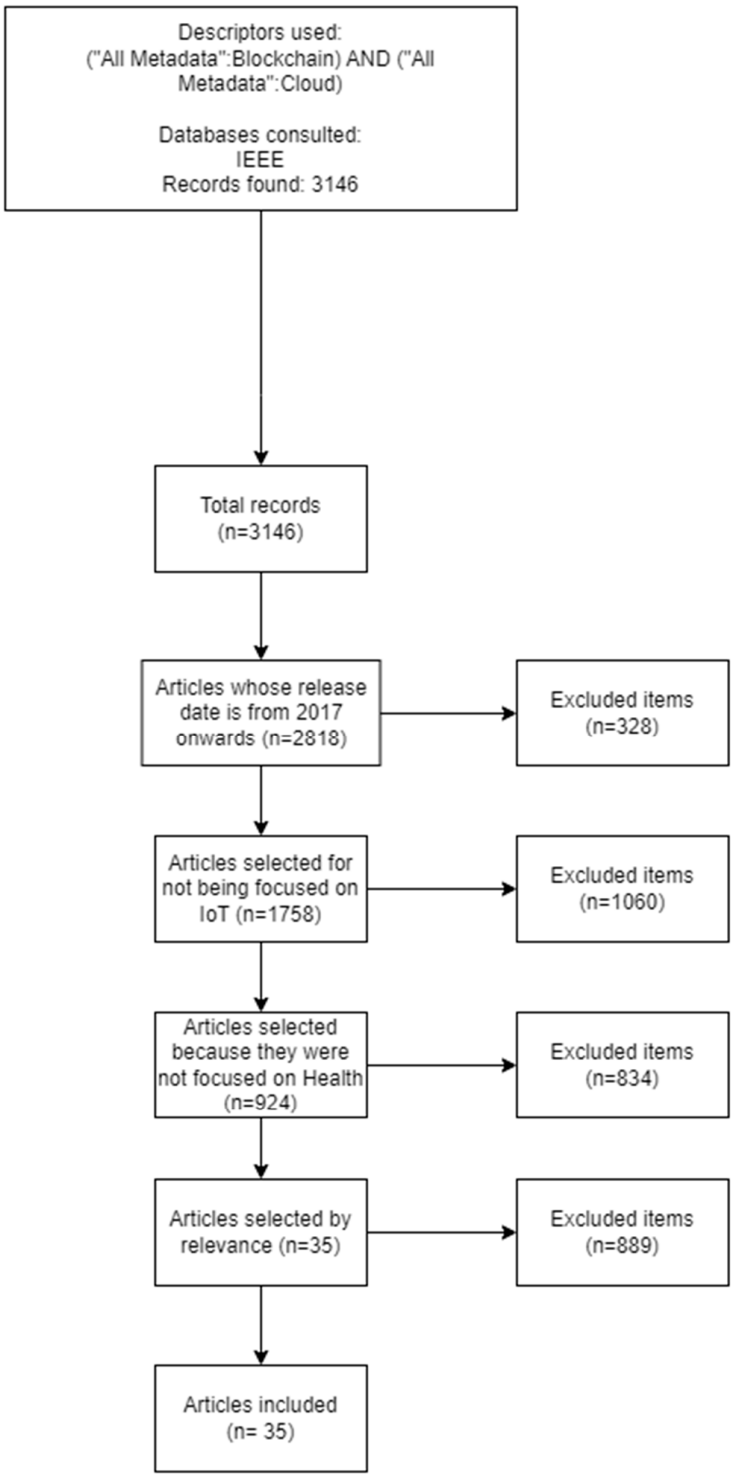


Figure A3. Flowchart for selected papers on IEEE.

 doi:10.20944/preprints202402.0453.v1

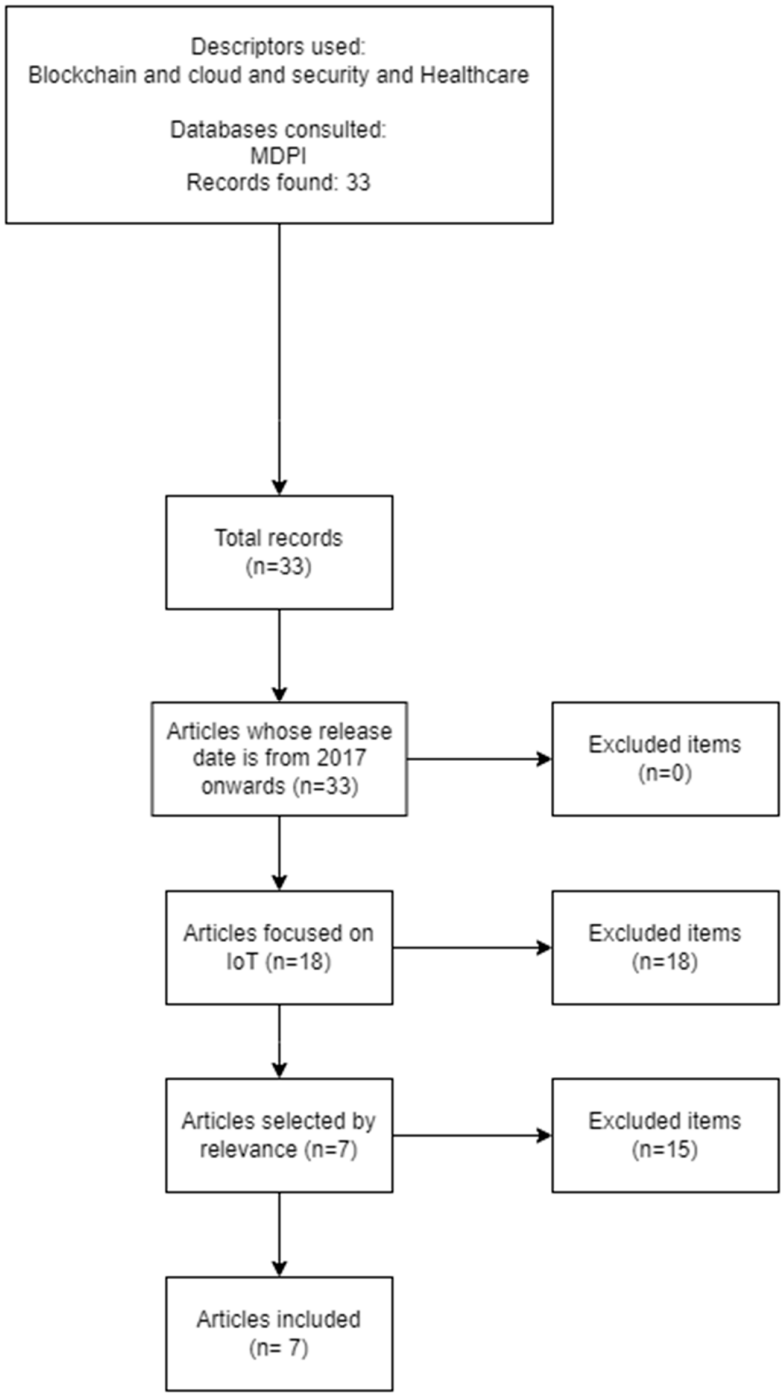


Figure A4. Flowchart for selected papers on MDPI.

References

1. S. Bhari and S. J. Quraishi, "Blockchain and Cloud Computing-A Review," in *2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing, COM-IT-CON 2022*, 2022. doi: 10.1109/COM-IT-CON54601.2022.9850499.
2. H. Taherdoost, "Blockchain and Healthcare: A Critical Analysis of Progress and Challenges in the Last Five Years," *Blockchains 2023, Vol. 1, Pages 73-89*, vol. 1, no. 2, pp. 73–89, Nov. 2023, doi: 10.3390/BLOCKCHAINS1020006.
3. D. Doshi and S. Khara, "Blockchain-Based Decentralized Cloud Storage," in *EAI/Springer Innovations in Communication and Computing*, 2021. doi: 10.1007/978-3-030-49795-8_54.

4. R. Pise and S. Patil, "Enhancing Security of Data in Cloud Storage using Decentralized Blockchain," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, IEEE, Feb. 2021, pp. 161–167. doi: 10.1109/ICICV50876.2021.9388521.
5. E. F. Coutinho, Di. E. Paulo, A. W. Abreu, and I. M. B. Carla, "Towards Cloud Computing and Blockchain Integrated Applications," in *Proceedings - 2020 IEEE International Conference on Software Architecture Companion, ICSA-C 2020*, 2020. doi: 10.1109/ICSA-C50368.2020.00033.
6. K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain Meets Cloud Computing: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, 2020, doi: 10.1109/COMST.2020.2989392.
7. H. Han, S. Fei, Z. Yan, and X. Zhou, "A survey on blockchain-based integrity auditing for cloud data," *Digital Communications and Networks*, vol. 8, no. 5, 2022, doi: 10.1016/j.dcan.2022.04.036.
8. N. Alromaihi, Y. Ismail, and W. Elmedany, "Literature Review of Blockchain-based Cloud Computing: Data Security Issues and Challenges," in *2022 International Conference on Data Analytics for Business and Industry, ICDABI 2022*, 2022. doi: 10.1109/ICDABI56818.2022.10041637.
9. S. Xie, Z. Zheng, W. Chen, J. Wu, H. N. Dai, and M. Imran, "Blockchain for cloud exchange: A survey," *Computers and Electrical Engineering*, vol. 81, 2020, doi: 10.1016/j.compeleceng.2019.106526.
10. S. G. Sharma, L. Ahuja, and D. P. Goyal, "Building Secure Infrastructure for Cloud Computing Using Blockchain," in *Proceedings of the 2nd International Conference on Intelligent Computing and Control Systems, ICICCS 2018*, 2018. doi: 10.1109/ICCONS.2018.8663145.
11. Y. Tang *et al.*, "ChainFS: Blockchain-Secured Cloud Storage," in *IEEE International Conference on Cloud Computing, CLOUD*, 2018. doi: 10.1109/CLOUD.2018.00152.
12. H. Zang and J. Kim, "A Comprehensive Study on Blockchain-based Cloud-Native Storage for Data Confidence," in *International Conference on Ubiquitous and Future Networks, ICUFN*, 2023. doi: 10.1109/ICUFN57995.2023.10200136.
13. J. Wan *et al.*, "Smart Contract Service Optimization in Blockchain-Cloud Collaborative Computing," in *Proceedings - IEEE International Conference on Mobile Data Management*, 2023. doi: 10.1109/MDM58254.2023.00052.
14. M. Xu, S. Liu, D. Yu, X. Cheng, S. Guo, and J. Yu, "CloudChain: A Cloud Blockchain Using Shared Memory Consensus and RDMA," *IEEE Transactions on Computers*, vol. 71, no. 12, 2022, doi: 10.1109/TC.2022.3147960.
15. S. Meng, L. Luo, P. Sun, and Y. Gao, "Reliability Service Assurance in Public Clouds based on Blockchain," in Proceedings - Companion of the 2020 IEEE 20th International Conference on Software Quality, Reliability, and Security, QRS-C 2020, 2020. doi: 10.1109/QRS-C51114.2020.00122.
16. N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain-based publicly verifiable cloud storage," in *Proceedings - 2019 IEEE International Conference on Smart Computing, SMARTCOMP 2019*, 2019. doi: 10.1109/SMARTCOMP.2019.00076.
17. M. R. Dorsala, V. N. Sastry, and S. Chapram, "Blockchain-based solutions for cloud computing: A survey," *Journal of Network and Computer Applications*, vol. 196. 2021. doi: 10.1016/j.jnca.2021.103246.
18. H. Zhu, Y. Wang, X. Hei, W. Ji, and L. Zhang, "A blockchain-based decentralized cloud resource scheduling architecture," in *Proceedings - 2018 International Conference on Networking and Network Applications, NaNA 2018*, 2018. doi: 10.1109/NANA.2018.8648712.
19. V. Reantongcome, V. Visoottiviseth, W. Sawangphol, A. Khurat, S. Kashihara, and D. Fall, "Securing and Trustworthy Blockchain-based Multi-Tenant Cloud Computing," in *ISCAIE 2020 - IEEE 10th Symposium on Computer Applications and Industrial Electronics*, 2020. doi: 10.1109/ISCAIE47305.2020.9108796.
20. N. Xi, J. Liu, Y. Li, and B. Qin, "Decentralized access control for secure microservices cooperation with blockchain," *ISA Trans*, vol. 141, 2023, doi: 10.1016/j.isatra.2023.07.018.
21. L. Duan, W. Xu, W. Ni, and W. Wang, "BSAF: A blockchain-based secure access framework with privacy protection for cloud-device service collaborations," *Journal of Systems Architecture*, vol. 140, 2023, doi: 10.1016/j.sysarc.2023.102897.
22. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 2017. doi: 10.1109/BigDataCongress.2017.85.
23. M. Hasan, K. Ogan, and B. Starly, "Hybrid blockchain architecture for Cloud Manufacturing-as-a-service (CMaaS) platforms with improved data storage and transaction efficiency," in *Procedia Manufacturing*, 2021. doi: 10.1016/j.promfg.2021.06.060.
24. Y. I. Alzoubi and A. Mishra, "Green blockchain – A move towards sustainability," *J Clean Prod*, vol. 430, p. 139541, Dec. 2023, doi: 10.1016/J.JCLEPRO.2023.139541.
25. S. Sharma, S. Sharma, and T. Choudhury, "A Study And Analysis Of Decentralized Cloud Based Platform," in *Proceedings of the Confluence 2022 - 12th International Conference on Cloud Computing, Data Science and Engineering*, 2022. doi: 10.1109/Confluence52989.2022.9734166.
26. F. Yang, L. Lei, and H. Zhu, "Overview of Blockchain and Cloud Service Integration," in Proceedings - 2022 IEEE 8th International Conference on Big Data Security on Cloud, IEEE International Conference on High

Performance and Smart Computing, and IEEE International Conference on Intelligent Data and Security, BigDataSecurity/HPSC/IDS 2022, 2022. doi: 10.1109/BigDataSecurityHPSCIDS54978.2022.00017.

27. J. Zou, D. He, S. Zeadally, N. Kumar, H. Wang, and K. R. Choo, "Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges," *ACM Computing Surveys*, vol. 54, no. 8. 2022. doi: 10.1145/3456628.
28. A. Wilczyński and J. Kołodziej, "Modelling and simulation of security-aware task scheduling in cloud computing based on Blockchain technology," *Simul Model Pract Theory*, vol. 99, 2020, doi: 10.1016/j.simpat.2019.102038.
29. H. Ahmad and G. S. Aujla, "GDPR compliance verification through a user-centric blockchain approach in multi-cloud environment," *Computers and Electrical Engineering*, vol. 109, 2023, doi: 10.1016/j.compeleceng.2023.108747.
30. S. N. Prasad and C. Rekha, "Block chain based IAS protocol to enhance security and privacy in cloud computing," *Measurement: Sensors*, vol. 28, 2023, doi: 10.1016/j.measen.2023.100813.
31. A. Aljaloud and A. Razzaq, "Modernizing the Legacy Healthcare System to Decentralize Platform Using Blockchain Technology," *Technologies (Basel)*, vol. 11, no. 4, 2023, doi: 10.3390/technologies11040084.
32. S. K. Lo, X. Xu, M. Staples, and L. Yao, "Reliability analysis for blockchain oracles," *Computers and Electrical Engineering*, vol. 83, 2020, doi: 10.1016/j.compeleceng.2020.106582.
33. M. Taghavi, J. Bentahar, H. Otrok, and K. Bakhtiyari, "A reinforcement learning model for the reliability of blockchain oracles," *Expert Syst Appl*, vol. 214, 2023, doi: 10.1016/j.eswa.2022.119160.
34. A. Hassan, I. Makhdoom, W. Iqbal, A. Ahmad, and A. Raza, "From trust to truth: Advancements in mitigating the Blockchain Oracle problem," *Journal of Network and Computer Applications*, vol. 217. 2023. doi: 10.1016/j.jnca.2023.103672.
35. P. Kochovski, S. Gec, V. Stankovski, M. Bajec, and P. D. Drobintsev, "Trust management in a blockchain based fog computing platform with trustless smart oracles," *Future Generation Computer Systems*, vol. 101, 2019, doi: 10.1016/j.future.2019.07.030.
36. A. Gupta, R. Gupta, D. Jadav, S. Tanwar, N. Kumar, and M. Shabaz, "Proxy smart contracts for zero trust architecture implementation in Decentralised Oracle Networks based applications," *Comput Commun*, vol. 206, 2023, doi: 10.1016/j.comcom.2023.04.022.
37. K. H. Y. Chung, D. Li, and P. Adriaens, "Technology-enabled financing of sustainable infrastructure: A case for blockchains and decentralized oracle networks," *Technol Forecast Soc Change*, vol. 187, 2023, doi: 10.1016/j.techfore.2022.122258.
38. D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A Survey on Blockchain for Information Systems Management and Security," *Inf Process Manag*, vol. 58, no. 1, p. 102397, Jan. 2021, doi: 10.1016/j.ipm.2020.102397.
39. M. J. Page *et al.*, "Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas," *Revista Española de Cardiología (English Edition)*, vol. 74, no. 9, 2021, doi: 10.1016/j.rec.2021.07.010.
40. M. Seenivasan, V. Krishnasamy, and S. S. Muppudathi, "Data division using Fuzzy Logic and Blockchain for data security in cyber space," in *Procedia Computer Science*, 2022. doi: 10.1016/j.procs.2022.12.047.
41. F. Dai, Y. Shi, N. Meng, L. Wei, and Z. Ye, "From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues," in *2017 4th International Conference on Systems and Informatics, ICSAI 2017*, 2017. doi: 10.1109/ICSAI.2017.8248427.
42. Z. Yang, Y. Chen, Y. Huang, and X. Li, "Protecting personal sensitive data security in the cloud with blockchain," in *Advances in Computers*, vol. 120, 2021. doi: 10.1016/bs.adcom.2020.09.004.
43. J. Che, Y. Duan, T. Zhang, and J. Fan, "Study on the security models and strategies of cloud computing," in *Procedia Engineering*, 2011. doi: 10.1016/j.proeng.2011.11.2551.
44. N. Nahar, F. Hasin, and K. A. Taher, "Application of Blockchain for the Security of Decentralized Cloud Computing," in 2021 International Conference on Information and Communication Technology for Sustainable Development, ICICT4SD 2021 - Proceedings, 2021. doi: 10.1109/ICICT4SD50815.2021.9396921.
45. K. Meenakshi, B. Bharathi, S. J. J. Thangaraj, and S. Sivasubramanian, "Cloud Security Analysis using Blockchain Technology," in *Proceedings of the 2nd International Conference on Edge Computing and Applications, ICECAA 2023*, 2023. doi: 10.1109/ICECAA58104.2023.10212415.
46. H. Ren, G. Xu, H. Qi, and T. Zhang, "PriFR: Privacy-preserving Large-scale File Retrieval System via Blockchain for Encrypted Cloud Data," in *Proceedings - 2023 IEEE 9th International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing, and IEEE International Conference on Intelligent Data and Security, BigDataSecurity-HPSC-IDS 2023*, 2023. doi: 10.1109/BigDataSecurity-HPSC-IDS58521.2023.00014.
47. S. Gaba, I. Budhiraja, A. Makkar, and D. Garg, "Machine Learning for Detecting Security Attacks on Blockchain using Software Defined Networking," in *2022 IEEE International Conference on Communications Workshops, ICC Workshops 2022*, 2022. doi: 10.1109/ICCWorkshops53468.2022.9814656.

48. W. Cai and J. Qu, "Systematic Research on Information Security Based on Blockchain Technology," in *Proceedings of the International Conference on Electronics and Renewable Systems, ICEARS 2022*, 2022. doi: 10.1109/ICEARS53579.2022.9751814.
49. Z. Gong-Guo and Z. Wan, "Blockchain-based IoT security authentication system," in *Proceedings - 2021 International Conference on Computer, Blockchain and Financial Development, CBFD 2021*, 2021. doi: 10.1109/CBFD52659.2021.00090.
50. X. Wang, A. Badshah, S. Tu, and M. Waqas, "Blockchain Boundary Security Protection based on Trusted Computing," in *Proceedings - 2021 2nd Asia Symposium on Signal Processing, ASSP 2021*, 2021. doi: 10.1109/ASSP54407.2021.00042.
51. M. Fartitchou, H. El Marraki, L. Lafkir, A. Azzouz, K. El Makkaoui, and Z. El Allali, "Public-Key Cryptography behind Blockchain Security," in *Proceedings of the 5th International Conference on Networking, Information Systems and Security: Envisage Intelligent Systems in 5G/6G-Based Interconnected Digital Worlds, NISS 2022*, 2022. doi: 10.1109/NISS55057.2022.10085236.
52. F. R. Vidal, N. Ivaki, and N. Laranjeiro, "Advancing Blockchain Security: from Vulnerability Detection to Transaction Revocation," in *Proceedings - 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume, DSN-S 2023*, 2023. doi: 10.1109/DSN-S58398.2023.00048.
53. L. H. Bai and L. H. Liu, "Research on Software Defined Network Security Model Based on Blockchain," in *2021 IEEE 6th International Conference on Intelligent Computing and Signal Processing, ICSP 2021*, 2021. doi: 10.1109/ICSP51882.2021.9409008.
54. S. Sharma and K. Shah, "Exploring Security Threats on Blockchain Technology along with possible Remedies," in *2022 IEEE 7th International conference for Convergence in Technology, I2CT 2022*, 2022. doi: 10.1109/I2CT54291.2022.9825123.
55. I. Hammouti, A. Addaim, and Z. Guennoun, "Proposed Architecture of Cyber Security in Smart Grids, Blockchain as Solution," in *2022 IEEE Information Technologies and Smart Industrial Systems, ITSIS 2022*, 2022. doi: 10.1109/ITSIS56166.2022.10118374.
56. J. J. Kim, P. Lingga, J. P. Jeong, Y. Choi, and J. Park, "A Web-Based Monitoring System of Network Security Functions in Blockchain-Based Cloud Security Systems," in *International Conference on Information Networking*, 2022. doi: 10.1109/ICOIN53446.2022.9687177.
57. A. Tiwari, V. Agarwal, Y. Aggarwal, and U. Srivastava, "Server Security in Cloud Computing Using Blockchain," in *8th International Conference on Advanced Computing and Communication Systems, ICACCS 2022*, 2022. doi: 10.1109/ICACCS54159.2022.9785060.
58. A. Harshavardhan, T. Vijayakumar, and S. R. Mugunthan, "Blockchain technology in cloud computing to overcome security vulnerabilities," in *Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2018*, 2018. doi: 10.1109/I-SMAC.2018.8653690.
59. M. Ahmed, A. F. M. S. Akhter, A. N. M. B. Rashid, and A. S. K. Pathan, "A dependable and secure consensus algorithm for blockchain assisted microservice architecture," *Computers and Electrical Engineering*, vol. 109, 2023, doi: 10.1016/j.compeleceng.2023.108762.
60. Y. Zhang, L. Xiong, F. Li, X. Niu, and H. Wu, "A blockchain-based privacy-preserving auditable authentication scheme with hierarchical access control for mobile cloud computing," *Journal of Systems Architecture*, vol. 142, 2023, doi: 10.1016/j.sysarc.2023.102949.
61. G. J. Samuel Babu and M. Baskar, "Application of blockchain methodology in secure task scheduling in cloud environment," *Advances in Engineering Software*, vol. 172. 2022. doi: 10.1016/j.advengsoft.2022.103175.
62. N. Eltayieb, R. Elhabob, A. Hassan, and F. Li, "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud," *Journal of Systems Architecture*, vol. 102, 2020, doi: 10.1016/j.sysarc.2019.101653.
63. M. Kumar and A. K. Singh, "Distributed Intrusion Detection System using Blockchain and Cloud Computing Infrastructure," in *Proceedings of the 4th International Conference on Trends in Electronics and Informatics, ICOEI 2020*, 2020. doi: 10.1109/ICOEI48184.2020.9142954.
64. M. Shah, M. Shaikh, V. Mishra, and G. Tuscano, "Decentralized Cloud Storage Using Blockchain," in *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, IEEE, Jun. 2020, pp. 384–389. doi: 10.1109/ICOEI48184.2020.9143004.
65. L. Huang and H. H. Lee, "A Medical Data Privacy Protection Scheme Based on Blockchain and Cloud Computing," *Wirel Commun Mob Comput*, vol. 2020, 2020, doi: 10.1155/2020/8859961.
66. G. Qi *et al.*, "Blockchain based Consensus Checking in Cloud Storage," in *Proceedings - 2019 IEEE 14th International Symposium on Autonomous Decentralized Systems, ISADS 2019*, 2019. doi: 10.1109/ISADS45777.2019.9155713.
67. D. Mechkaroska, A. Popovska-Mitrovikj, and S. Mitrevska, "Overview of Blockchain and Cloud Computing Services Integration," in *2022 30th Telecommunications Forum, TELFOR 2022 - Proceedings*, 2022. doi: 10.1109/TELFOR56187.2022.9983759.
68. X. Liu, "Research on University Book Sharing Cloud Platform Based on Blockchain," in *ACM International Conference Proceeding Series*, 2021. doi: 10.1145/3469213.3470706.

69. P. A. D. S. N. Wijesekara and S. Gunawardena, "A Review of Blockchain Technology in Knowledge-Defined Networking, Its Application, Benefits, and Challenges," *Network*, vol. 3, no. 3. 2023. doi: 10.3390/network3030017.
70. D. Praveena Anjelin and S. Ganesh Kumar, "Blockchain Technology for Data Sharing in Decentralized Storage System," in *Advances in Intelligent Systems and Computing*, 2021. doi: 10.1007/978-981-15-5566-4_32.
71. P. Soares, R. Saraiva, I. Fernandes, A. Neto, and J. Souza, "A Blockchain-based Customizable Document Registration Service for Third Parties," in *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2022*, 2022. doi: 10.1109/ICBC54727.2022.9805500.
72. A. Fitwi, Y. Chen, and S. Zhu, "A lightweight blockchain-based privacy protection for smart surveillance at the edge," in *Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019*, 2019. doi: 10.1109/Blockchain.2019.00080.
73. Y. Yang, M. Hu, Y. Cheng, X. Liu, and W. Ma, "Keyword Searchable Encryption Scheme based on Blockchain in Cloud Environment," in *Proceedings - 2020 3rd International Conference on Smart BlockChain, SmartBlock 2020*, 2020. doi: 10.1109/SmartBlock52591.2020.00013.
74. S. Uthayashangar, T. Dhanya, S. Dharshini, and R. Gayathri, "Decentralized Blockchain Based System for Secure Data Storage in Cloud," in *2021 International Conference on System, Computation, Automation and Networking, ICSCAN 2021*, 2021. doi: 10.1109/ICSCAN53069.2021.9526408.
75. H. Spoorti, R. Sneha, V. Soujanya, K. Heena, S. Pooja, and D. G. Narayan, "Secure Access Control to Cloud Resources using Blockchain," in *2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics, DISCOVER 2021 - Proceedings*, 2021. doi: 10.1109/DISCOVER52564.2021.9663647.
76. P. Mendki, "Securing Cloud Native Applications Using Blockchain," in *2021 12th International Conference on Information and Communication Systems, ICICS 2021*, 2021. doi: 10.1109/ICICS52457.2021.9464583.
77. S. Lahoti and D. Singh, "Blockchain Technology Based Secure Data Sharing in Cloud Computing," in *IEEE International Conference on Knowledge Engineering and Communication Systems, ICKES 2022*, 2022. doi: 10.1109/ICKECS56523.2022.10060616.
78. X. Li, "Development of Cloud Information Platform based on Blockchain Public Service Platform," in *6th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2022 - Proceedings*, 2022. doi: 10.1109/I-SMAC55078.2022.9987372.
79. S. Yao *et al.*, "Blockchain-Empowered Collaborative Task Offloading for Cloud-Edge-Device Computing," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 12, 2022, doi: 10.1109/JSAC.2022.3213358.
80. T. H. Chee and M. E. Rana, "An Exploratory Study on the Impact of Hosting Blockchain Applications in Cloud Infrastructures," in *2023 15th International Conference on Developments in eSystems Engineering (DeSE)*, IEEE, Jan. 2023, pp. 381–386. doi: 10.1109/DeSE58274.2023.10100137.
81. X. Thipphonexai and Y. Guanghui, "Research on analysis and design of cloud ERP based on blockchain technology," in *Proceedings - 2020 International Conference on Virtual Reality and Intelligent Systems, ICVRIS 2020*, 2020. doi: 10.1109/ICVRIS51417.2020.00198.
82. Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information (Switzerland)*, vol. 8, no. 2, 2017, doi: 10.3390/info8020044.
83. E. Bacis, S. De Capitani Di Vimercati, S. Foresti, S. Paraboschi, M. Rosa, and P. Samarati, "Securing Resources in Decentralized Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol. 15, 2020, doi: 10.1109/TIFS.2019.2916673.
84. L. Karuppasamy and V. Vasudevan, "Security Management in Decentralized Cloud Storage via Improved Bees Swarm Optimisation Data Slicers," in *International Conference on Edge Computing and Applications, ICECAA 2022 - Proceedings*, 2022. doi: 10.1109/ICECAA55415.2022.9936491.
85. E. Bacis, S. De Capitani DI Vimercati, S. Foresti, S. Paraboschi, M. Rosa, and P. Samarati, "Dynamic allocation for resource protection in decentralized cloud storage," in *2019 IEEE Global Communications Conference, GLOBECOM 2019 - Proceedings*, 2019. doi: 10.1109/GLOBECOM38437.2019.9013354.
86. L. Karuppasamy and V. Vasudevan, "A novel double keys adapted elliptic curve cryptography and log normalized Gaussian sigmoid adaptive neuro-fuzzy interference system based secure resource allocation system in decentralized cloud storage," *Expert Syst*, vol. 40, no. 4, May 2023, doi: 10.1111/exsy.13206.
87. T. V. Doan, Y. Psaras, J. Ott, and V. Bajpai, "Toward Decentralized Cloud Storage With IPFS: Opportunities, Challenges, and Future Considerations," *IEEE Internet Comput*, vol. 26, no. 6, 2022, doi: 10.1109/MIC.2022.3209804.
88. P. Khatiwada and B. Yang, "An access control and authentication scheme for secure data sharing in the decentralized cloud storage system," in *5th Conference on Cloud and Internet of Things, CIoT 2022*, 2022. doi: 10.1109/CIoT53061.2022.9766634.
89. L. Golightly, P. Modesti, R. Garcia, and V. Chang, "Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN," *Cyber Security and Applications*, vol. 1. 2023. doi: 10.1016/j.csa.2023.100015.

90. G. Baranwal, D. Kumar, and D. P. Vidyarthi, "Blockchain based resource allocation in cloud and distributed edge computing: A survey," *Computer Communications*, vol. 209. 2023. doi: 10.1016/j.comcom.2023.07.023.
91. W. Tarannum and S. Abidin, "Integration of Blockchain and Cloud Computing: A Review," in Proceedings of the 17th INDIACom; 2023 10th International Conference on Computing for Sustainable Global Development, INDIACom 2023, 2023.
92. T. Feng and Y. Liu, "Research on PoW Protocol Security under Optimized Long Delay Attack," *Cryptography*, vol. 7, no. 2, 2023, doi: 10.3390/cryptography7020032.
93. M. Kim, S. Yu, J. Lee, Y. Park, and Y. Park, "Design of secure protocol for cloud-assisted electronic health record system using blockchain," *Sensors (Switzerland)*, vol. 20, no. 10, 2020, doi: 10.3390/s20102913.
94. H. Taherdoost, "Blockchain and Healthcare: A Critical Analysis of Progress and Challenges in the Last Five Years," *Blockchains 2023, Vol. 1, Pages 73-89*, vol. 1, no. 2, pp. 73–89, Nov. 2023, doi: 10.3390/BLOCKCHAINS1020006.