Global Mainstream Journal of Innovation, Engineering & Emerging Technology
Vol. 03, Issue 04, August, 2024
e-ISSN:2998-3967
Page:58-68

DECENTRALIZED VS. CENTRALIZED DATABASE SOLUTIONS IN BLOCKCHAIN: ADVANTAGES, CHALLENGES, AND USE CASES

Siful Islam
https://orcid.org/0009-0009-0592-2059
Graduate Researcher, Master of Science in Management Information Systems, College of Business, Lamar University, Texas, US
Correspondence e-mail: sislam13@lamar.edu

Kutub Uddin Apu
https://orcid.org/0009-0009-3256-3354
Graduate Researcher, Master of Science in Management Information Systems, College of Business, Lamar University, Texas, US
e-mail: kapu@lamar.edu

Keywords

Decentralized Database
Centralized Database
Blockchain
Security
Scalability
Use Cases

Article Information

Received: *12, July, 2024*
Accepted: *24, August, 2024*
Published: *27, August, 2024*

Doi: 10.62304/jieet.v3i04.195

ABSTRACT

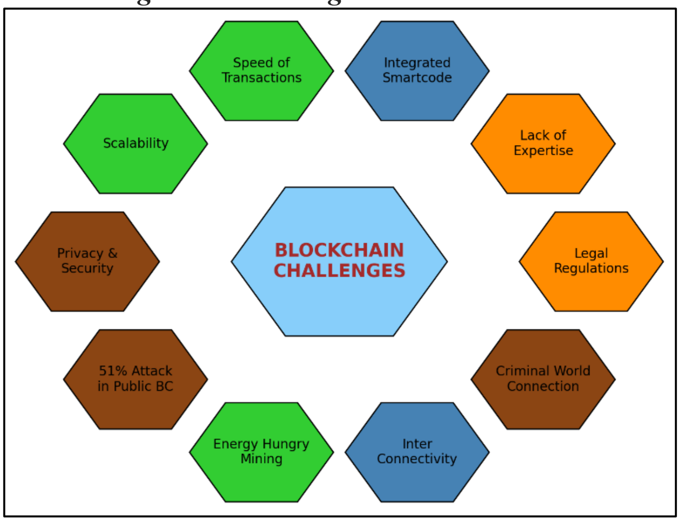
This study provides a comprehensive examination of decentralized and centralized database solutions within the realm of blockchain technology, exploring the inherent strengths and weaknesses of each approach and their implications for various industries. Decentralized databases, characterized by distributed ledger technology, offer robust security and transparency by eliminating the need for a central authority, thereby reducing the risk of data tampering and fostering trust among participants. However, these benefits come with significant trade-offs, particularly in terms of scalability and performance, as the consensus mechanisms required in decentralized systems often result in slower transaction processing and higher resource consumption. In contrast, centralized databases, typically used in private or permissioned blockchains, excel in operational efficiency and scalability, enabling faster transaction processing and more streamlined management due to the presence of a central authority. Nevertheless, centralized systems introduce vulnerabilities, such as single points of failure and reduced transparency, which can undermine trust and compromise data integrity. The study also highlights industry-specific preferences, with sectors like healthcare and public governance leaning towards decentralized solutions for their emphasis on data integrity, while industries such as finance and logistics favor centralized systems for their superior performance and low latency. Moreover, the research identifies a critical gap in the literature regarding hybrid database models that could potentially integrate the strengths of both decentralized and centralized systems, offering a balanced approach that mitigates their respective weaknesses. These findings underscore the necessity for a tailored approach to database selection in blockchain implementations, aligned with the specific needs and goals of different industries, and suggest that further exploration of hybrid models could lead to more effective and adaptable blockchain solutions in the future.

Doi: 10.62304/jieet.v3i04.195

1 Introduction

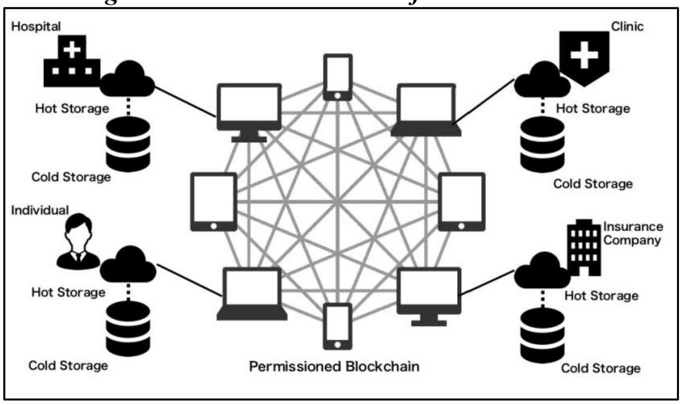
Blockchain technology has become a revolutionary force in the realm of data storage, management, and security, offering transformative potential across a wide array of industries (Kuo et al., 2017). At its core, blockchain is distinguished by its decentralized structure, which leverages distributed ledger technology to ensure transparency, security, and efficiency in handling data transactions (Muzammal et al., 2019). The adoption of blockchain technology, however, requires organizations to navigate a critical decision: whether to implement a decentralized or centralized database solution. This decision is not purely technical; it carries profound implications for the scalability, security, and overall functionality of the blockchain system (Mytis-Gkometh et al., 2017).
Decentralized databases, which are commonly associated with public blockchains such as Bitcoin and Ethereum, operate on the principle of distributing data across a network of nodes, each maintaining a copy of the entire ledger (Lakhan et al., 2022; Mohanta et al., 2019). This decentralized architecture is lauded for its ability to enhance security by eliminating single points of failure, thus making data tampering or unauthorized access significantly more difficult (McGhin et al., 2019). Moreover, the transparency afforded by decentralized databases, where all transactions are recorded and visible to all network participants, has been highlighted as a key advantage in industries where trust and verification are paramount (Li et al., 2018).

Figure 1: Challenges in blockchain



However, the adoption of decentralized databases is not without its challenges. One of the most significant issues is scalability. Decentralized networks, due to their consensus mechanisms, often struggle to handle large volumes of transactions efficiently, leading to delays and increased costs (Liu et al., 2019). This limitation has been extensively discussed in the literature, with studies such as those by (Mettler, 2016) and (Muzammal et al., 2019) emphasizing that while decentralization enhances security, it often comes at the expense of performance and scalability. In contrast, centralized databases, which are typically employed in private or permissioned blockchains, offer a different set of trade-offs. These systems, where control is vested in a single entity or a group of entities, provide greater efficiency and faster transaction processing capabilities (Muzammal et al., 2019). Centralized databases are also easier to manage and scale, making them more suitable for applications that require high throughput and low latency, such as financial transactions and supply chain management (Mettler, 2016; Muzammal et al., 2019). The literature supports these observations, with studies such as those by (Nathan et al., 2019) and (Nizamuddin et al., 2019) highlighting the operational efficiencies gained through centralized control, particularly in scenarios where performance is prioritized over decentralization.

Figure 2: Basic architecture of i-Blockchain



Despite these advantages, centralized databases are often criticized for their inherent vulnerabilities. The centralization of control can lead to security risks, such as single points of failure, which can be exploited by malicious actors (Kotobi & Bilén, 2018). Moreover, centralized systems are less transparent than their decentralized counterparts, potentially leading to trust issues among stakeholders, especially in environments where transparency and accountability are critical (Li et al., 2018). The choice between decentralized and centralized database solutions in blockchain technology is therefore not a straightforward one. As demonstrated by studies from diverse fields, including finance, healthcare, and supply chain management, the decision must be informed by the specific needs and constraints of the organization (Chen et al., 2018; Tseng et al., 2020). For instance, industries that prioritize security and transparency may lean towards decentralized solutions, while those requiring high efficiency and scalability may prefer centralized systems.

The objective of this study is to conduct a comprehensive review and comparative analysis of decentralized and centralized database solutions within the context of blockchain technology. By examining the fundamental characteristics, advantages, and challenges associated with each approach, this study aims to provide a detailed understanding of how these database solutions influence the performance, security, and scalability of blockchain systems. Additionally, the study seeks to explore real-world use cases across various industries to illustrate the practical implications of adopting either a decentralized or centralized database architecture. Ultimately, the goal is to offer insights that can guide organizations in making informed decisions when selecting the most suitable database solution for their specific blockchain applications.

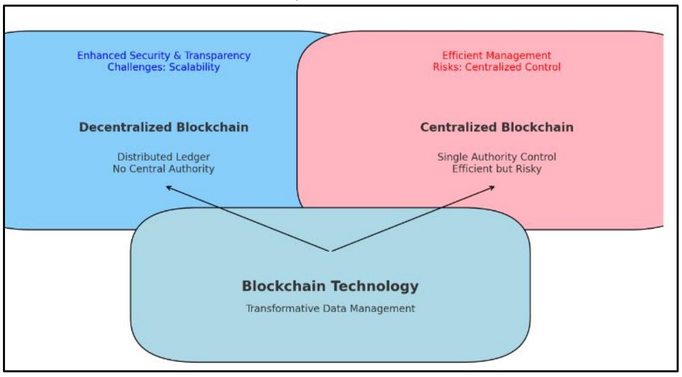
2 Literature Review

The literature on blockchain technology reveals a growing interest in the comparison between decentralized and centralized database solutions. Decentralized databases, often associated with public blockchains like Bitcoin and Ethereum, are lauded for their ability to enhance data security through distributed ledger technology. In contrast, centralized databases, which are more commonly used in private or permissioned blockchains, are praised for their efficiency and ease of management. However, each approach comes with its own set of challenges, including scalability issues in decentralized systems and security vulnerabilities in centralized systems. This review synthesizes existing research on these topics, providing a foundation for the subsequent analysis of their practical applications.

2.1 Introduction to Blockchain Technology

Blockchain technology represents a transformative shift in data management, offering innovative solutions for the storage, processing, and security of information (El-Hindi et al., 2019). At the heart of blockchain is its decentralized digital ledger, which records transactions across a distributed network of computers, ensuring immutability and transparency in the recorded data. This decentralized structure eliminates the need for a central authority, thereby reducing vulnerabilities associated with single points of failure and enhancing overall data security (Kleinaki et al., 2018; Vainshtein & Gudes, 2021). Blockchain's potential to create a tamper-proof record of transactions has been particularly impactful in industries where data integrity and trust are paramount, such as finance, supply chain management, and healthcare (Tseng et al., 2020).

Figure 3: Decentralized and Centralized Blockchain Systems



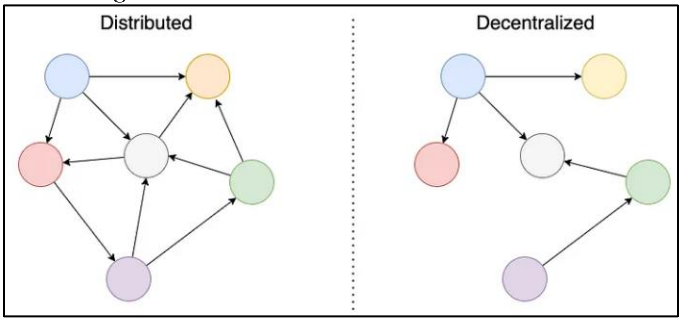
The concepts of decentralized and centralized databases are fundamental to understanding the mechanisms of blockchain technology. Decentralized databases distribute data across multiple nodes, with each node maintaining a complete copy of the ledger. This architecture is characteristic of public blockchains like Bitcoin and Ethereum, where the absence of a central authority ensures that no single entity can control or alter the data, thus promoting enhanced security and transparency (Chen et al., 2018). In contrast, centralized databases, often utilized in private or permissioned blockchains, are managed by a single authority or a consortium, offering advantages in efficiency and scalability. The centralization allows for faster transaction processing and easier management but introduces potential security risks due to the centralization of control (Chen et al., 2018; Hao et al., 2019; Wang et al., 2020).

The decision between adopting a decentralized or centralized database solution is critical in the implementation of blockchain technology, as it directly affects the system's performance, security, and scalability. This choice must align with the specific requirements and objectives of the organization. For industries where security and transparency are paramount, decentralized databases may offer the most benefit, despite potential challenges in scalability (Huang et al., 2022). Conversely, for applications requiring high efficiency and ease of management, centralized databases might be preferable, even though they come with increased security risks (Tsoulias et al., 2020). Therefore, understanding the implications of this decision is essential for organizations aiming to maximize the benefits of blockchain technology while effectively managing its associated risks.

2.2 Decentralized Database Solutions

Decentralized database solutions are integral to the architecture of many blockchain systems, particularly those that operate on public blockchains such as Bitcoin and Ethereum (Ruan et al., 2019). These databases are defined by their distributed nature, where data is stored across multiple nodes in a network, each of which holds a complete copy of the ledger. This decentralization eliminates the need for a central authority, thereby enhancing the security and resilience of the system. The key characteristic of decentralized databases is their reliance on distributed ledger technology, which ensures that any change to the data must be validated by a majority of the network, making unauthorized alterations virtually impossible (Jia et al., 2019; Mettler, 2016).

Figure 4: Decentralized database solutions



Public blockchains like Bitcoin and Ethereum are prime examples of decentralized database solutions in action. In these systems, the absence of a central controlling entity means that no single party can manipulate the data, which significantly enhances trust and transparency within the network (Croman et al., 2016; Gorenflo et al., 2020). The security advantages of decentralized databases are particularly evident in their resistance to cyberattacks, as the distributed nature of the ledger means that compromising the entire system would require attacking a majority of the nodes simultaneously—a task that is highly resource-intensive and impractical (Mettler, 2016). This level of security is one of the primary reasons decentralized databases are favored in applications where data integrity and trust are of paramount importance.

However, despite these advantages, decentralized databases also face significant challenges, particularly in terms of scalability and performance. As the number of transactions on a decentralized network increases, the process of validating and recording these transactions across all nodes can become slow and resource-intensive. This issue is compounded by the fact that consensus mechanisms, which are essential for maintaining the integrity of the ledger, often require substantial computational power and time, leading to delays and inefficiencies (Ruan et al., 2019). Studies have shown that while decentralized databases excel in security and transparency, these benefits often come at the cost of reduced performance and scalability, making them less suitable for applications requiring high transaction throughput (Jia et al., 2021; Zheng et al., 2019).

Key studies in the field have explored these dynamics in detail. For instance, research by (Li et al., 2022) highlights the trade-offs between security and scalability in decentralized databases, noting that while these systems are robust against attacks, their performance can be significantly hindered as they scale. Similarly, (Muzammal et al., 2019) emphasize the importance of balancing security with efficiency, particularly in environments where rapid transaction processing is critical. These studies underscore the need for ongoing innovation in decentralized database technology to address these challenges and enhance their applicability across a broader range of use cases databases.

2.3 Centralized Database Solutions

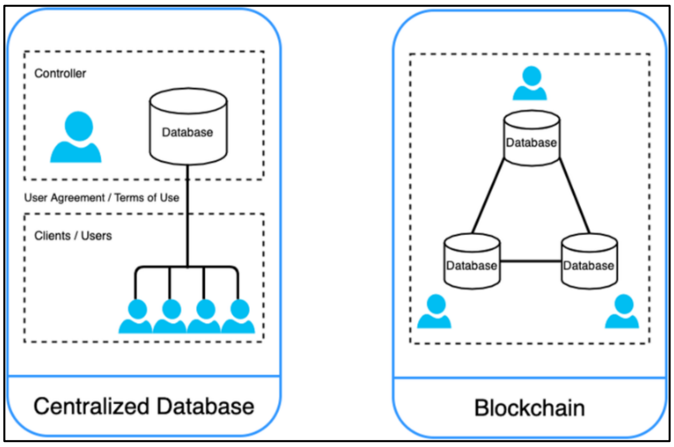
Centralized database solutions are a key component of private or permissioned blockchains, where data management is controlled by a single entity or a consortium of entities. Unlike decentralized databases, centralized databases operate under a hierarchical structure in which a central authority has the power to manage, control, and update the data. This centralization allows for greater efficiency and ease of management, as decisions can be made quickly without the need for consensus among a distributed network of nodes (Li et al., 2022). The streamlined nature of centralized databases often results in faster transaction processing and enhanced scalability, making them particularly suitable for applications that require high throughput and low latency.

Private or permissioned blockchains, such as those used in enterprise environments, are common examples of centralized database solutions. In these systems, access to the network is restricted, and only authorized participants can engage in the validation and updating of the ledger. This controlled environment facilitates better performance and scalability compared to public blockchains, where every node must participate in the consensus process. The centralized control also simplifies the management of the database, allowing for more straightforward implementation of updates and changes to the system (Zheng et al., 2019). These characteristics make centralized databases an attractive option for industries where efficiency and quick decision-making are prioritized, such as in financial

Global Mainstream Journal of Innovation, Engineering & Emerging Technology
Volume 03, Issue 04, August, 2024, **Page**: 58-68

services and supply chain management.

Figure 5: Centralized database solutions and Blockchain



However, centralized database solutions are not without their challenges. One of the primary concerns is the potential for security risks due to the concentration of control in a single point of authority. This centralization creates a single point of failure, which can be exploited by malicious actors to compromise the entire system (Thatikonda et al., 2023). Additionally, the lack of transparency in centralized systems can lead to trust issues among participants, particularly in scenarios where the integrity of the data is critical. These security concerns are a significant drawback of centralized databases and are often highlighted in discussions comparing them to decentralized alternatives (Shamim, 2022).

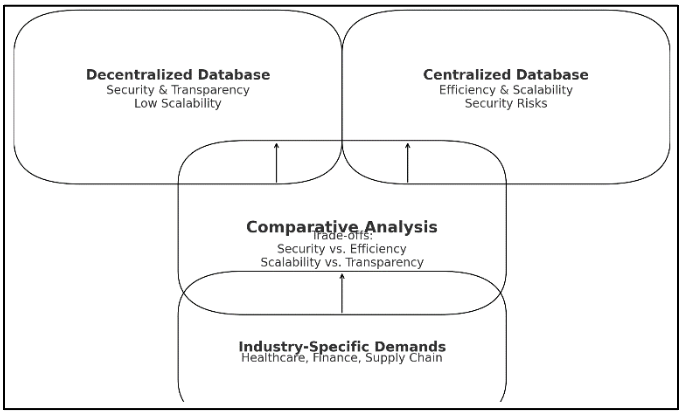
Key studies have explored the trade-offs associated with centralized database solutions in blockchain technology. For instance, (Hong et al., 2020) discusses the inherent vulnerabilities of centralized systems, particularly in the context of their susceptibility to attacks that could compromise the entire network. Meanwhile, (Beirami et al., 2019) provide a comprehensive overview of the advantages of centralized databases, emphasizing their operational efficiencies and suitability for environments where performance is a critical factor. These studies collectively underscore the need for a careful assessment of the specific requirements of an application when choosing between centralized and decentralized database solutions.databases.

2.4 Comparative Analysis of Decentralized and Centralized Solutions

The comparative analysis of decentralized and centralized database solutions in blockchain technology reveals distinct strengths and weaknesses inherent in each approach, as well as critical trade-offs between security, scalability, and efficiency. Decentralized databases, characterized by their distributed ledger technology, excel in providing robust security and transparency. The absence of a central authority reduces the risk of data tampering and ensures that all participants have equal access to the data, fostering trust and integrity in the system (Aswathy & Lakshmy, 2019; Lian et al., 2021). However, these security benefits often come at the cost of scalability and performance, as the need for consensus among numerous nodes can lead to slower transaction processing and increased resource consumption (Beirami et al., 2019). These limitations make decentralized databases less suitable for applications requiring high throughput and rapid data processing.

In contrast, centralized database solutions offer significant advantages in terms of efficiency and scalability. By consolidating control within a single entity or a small group of entities, centralized systems can process transactions more quickly and manage large volumes of data with greater ease (Dinh et al., 2018). This efficiency makes centralized databases particularly attractive for industries where performance and speed are critical, such as in financial services and supply chain management (Yan et al., 2021). However, the centralization of control introduces vulnerabilities, including the risk of single points of failure and potential security breaches. The lack of transparency in centralized systems can also lead to trust issues, particularly in environments where data integrity is paramount (El-Hindi et al., 2019).

Figure 6: Comparative Analysis of Decentralized vs. Centralized Solutions



The choice between decentralized and centralized database solutions often hinges on the specific requirements and priorities of the industry in question. For example, industries that prioritize security and transparency, such as healthcare and public sector organizations, may prefer decentralized solutions despite their scalability challenges (Chickerur et al., 2015). On the other hand, sectors that require high efficiency and low latency, such as financial services, may opt for centralized systems, accepting the associated security risks in exchange for better performance (Gorenflo et al., 2020). Ultimately, the decision between decentralized and centralized approaches involves balancing the trade-offs between security, scalability, and efficiency, with the optimal solution varying depending on the specific application and industry needs.

Key studies have provided valuable insights into these trade-offs and industry-specific preferences. For instance, (Islam, 2024)highlights the operational efficiencies of centralized systems in high-performance environments, while (Tsoulias et al., 2020) discuss the scalability challenges faced by decentralized networks. Similarly, (Zhang et al., 2015)emphasize the importance of aligning database architecture with organizational goals, whether that means prioritizing security or optimizing for speed and efficiency. These findings underscore the complexity of selecting the appropriate database solution for blockchain applications and the necessity of a tailored approach based on industry-specific demands.

2.5 Synthesis of Existing Research

The synthesis of existing research on decentralized and centralized database solutions within blockchain technology highlights a complex landscape of trade-offs, where the choice of database architecture significantly influences the overall performance, security, and scalability of blockchain systems. The reviewed literature consistently underscores the strengths of decentralized databases in enhancing security and transparency through distributed ledger technology. Studies have shown that decentralized systems, by virtue of their distributed nature, provide robust protection against data tampering and unauthorized access, making them particularly valuable in applications where trust and data integrity are critical (Ge et al., 2022; Rani & Sharma, 2019). However, these benefits are often accompanied by significant challenges, particularly in terms of scalability and transaction speed, as the need for consensus among multiple nodes can lead to performance bottlenecks (Almeida et al., 2019; Muzammal et al., 2019; Tan et al., 2015).

Conversely, centralized database solutions are praised for their efficiency, ease of management, and ability to handle large volumes of transactions with minimal delay. The literature highlights that centralized systems, often employed in private or permissioned blockchains, offer a level of operational efficiency that is difficult to achieve with decentralized architectures (Xinying et al., 2020). This efficiency makes centralized databases well-suited for industries where high transaction throughput and low latency are essential. However, the centralization of control also introduces vulnerabilities, such as the risk of single points of failure and potential security breaches, which are less prevalent in decentralized systems (Almeida et al., 2019).

Despite the extensive research on the comparative advantages and disadvantages of these database solutions, several gaps remain in the current literature. One notable gap is the lack of comprehensive studies that explore hybrid models combining the strengths of both decentralized and centralized databases. Such hybrid approaches could potentially mitigate the weaknesses of each system while maximizing their respective benefits, yet this area remains underexplored. Additionally, there is a need for more industry-specific research that examines how different sectors can best leverage these database solutions to meet their unique needs. While some studies have begun to address these issues, further research is required to provide more detailed guidance on the practical implementation of blockchain technology across various industries (Muzammal et al., 2019; Thatikonda et al., 2023).

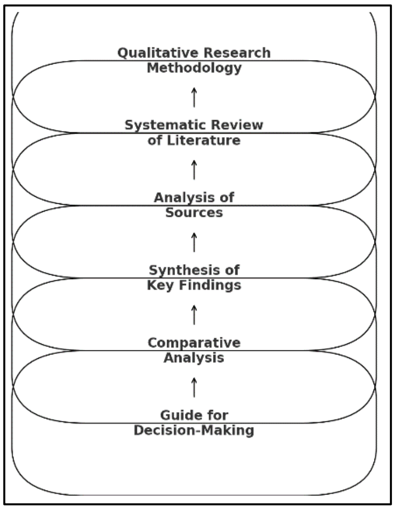
The findings from the reviewed literature are highly relevant to the objectives of this study, which seeks to provide a detailed comparative analysis of decentralized and centralized database solutions in blockchain technology. By synthesizing existing research, this study aims to contribute to a deeper understanding of how these solutions can be optimized for different use cases, addressing the specific challenges and requirements of various industries. The identification of research gaps also highlights areas for future investigation, suggesting avenues for further study that could enhance the practical application of blockchain technology and inform decision-making processes in database selection.

3 Methodology

This study employs a qualitative research methodology, grounded in a systematic review of existing literature to explore the implementation of decentralized and centralized database solutions within blockchain technology. The approach involves a comprehensive analysis of peer-reviewed journal articles, industry reports, and case studies, aiming to identify and synthesize key trends, patterns, and insights that are critical to understanding the strengths and weaknesses of each database solution. By systematically reviewing and synthesizing a wide range of sources, this research ensures a thorough and nuanced understanding of the subject matter.

The qualitative nature of this study allows for an in-depth exploration of the complexities and nuances associated with decentralized and centralized databases, which is essential for developing a balanced perspective on their respective advantages and challenges. The systematic review process involves identifying relevant literature, critically appraising the quality of the studies, and extracting key findings that contribute to the overall understanding of the topic. This method enables the research to draw on a diverse array of sources, ensuring that the analysis is comprehensive and grounded in the most current and relevant evidence available.

Figure 7: Methodology for this study



The comparative analysis within this study is structured to highlight the trade-offs between decentralized and centralized database solutions, focusing on aspects such as security, scalability, and efficiency. By synthesizing insights from multiple studies, the research provides a balanced view that can guide organizations in making informed decisions when selecting a database solution for their blockchain implementations. This approach not only illuminates the key factors that should be considered in the decision-making process but also identifies potential areas for future research, particularly in the development of hybrid models that may combine the strengths of both decentralized and centralized systems.

4 Results

The findings of this study, based on a systematic review of existing literature, reveal significant insights into the comparative strengths and weaknesses of decentralized and centralized database solutions in blockchain technology. The analysis highlights that decentralized databases, while offering superior security and transparency due to their distributed ledger architecture, face substantial challenges in scalability and performance. This is particularly evident in public blockchains like Bitcoin and Ethereum, where the need for consensus across numerous nodes results in slower transaction processing and higher resource consumption. These limitations underscore the trade-offs involved in opting for a decentralized approach, where the benefits of enhanced security and trust come at the expense of efficiency and scalability.

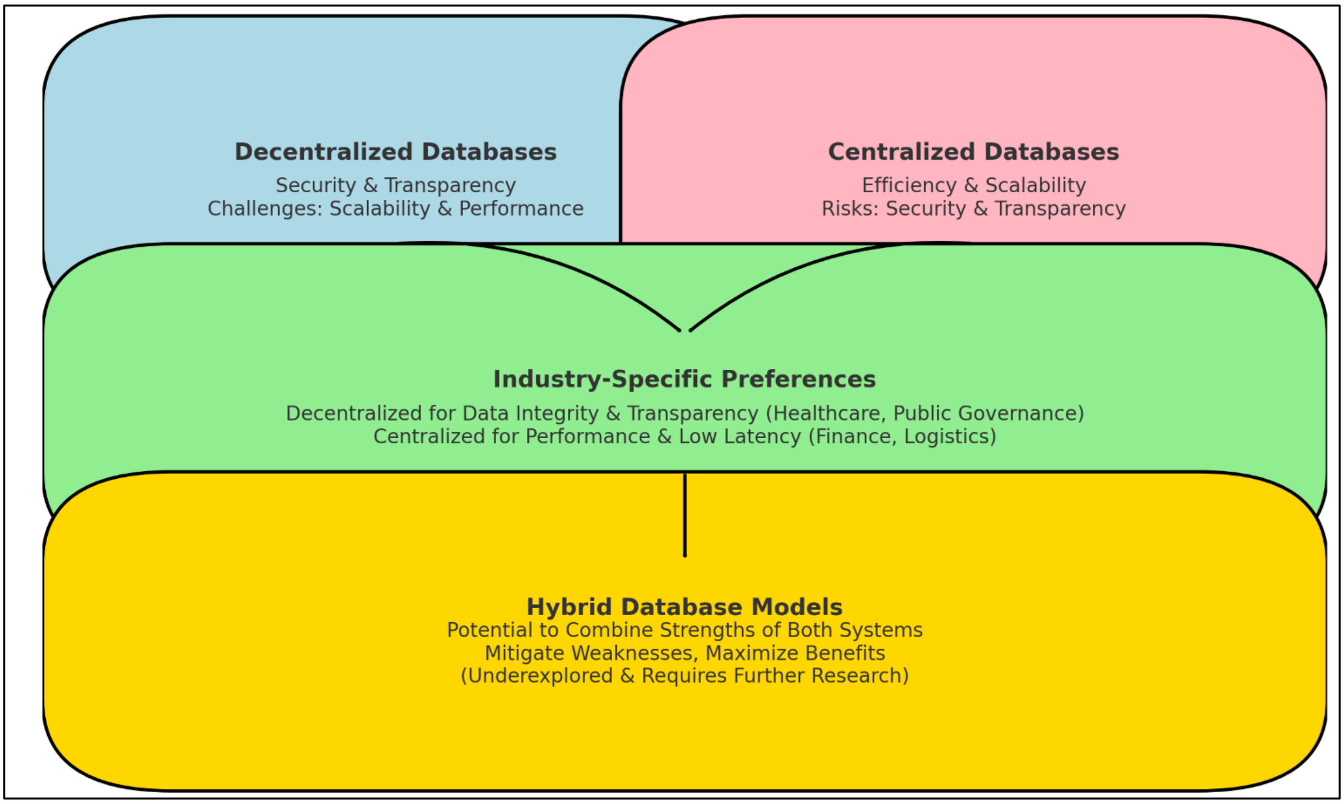
In contrast, centralized database solutions demonstrate clear advantages in terms of operational efficiency and scalability. The review of literature indicates that centralized systems, which are commonly implemented in private or permissioned blockchains, enable faster transaction processing and more manageable system oversight due to the presence of a central authority. This efficiency makes centralized databases particularly attractive for applications that require high throughput and low latency, such as in financial services and supply chain management. However, the study also identifies significant security risks associated with centralized databases, including the potential for single points of failure and reduced transparency, which can undermine trust among participants.

Moreover, the research uncovers industry-specific preferences that further delineate the practical applications of these database solutions. For instance, industries that prioritize data integrity and transparency, such as healthcare and public governance, are more inclined to adopt decentralized systems despite their scalability challenges. Conversely, sectors that demand high performance and swift data processing, like finance and logistics, tend to favor centralized databases, accepting the associated security risks for the sake of operational efficiency. These findings illustrate the importance of aligning database architecture with organizational goals and industry requirements, highlighting the necessity for a tailored approach when implementing blockchain technology. Finally, the study identifies a gap in the current research concerning hybrid database models that could potentially combine the strengths of both decentralized and centralized systems. While some literature suggests that such hybrid solutions could offer a balanced approach, mitigating the weaknesses of each while maximizing their benefits, this area remains underexplored and warrants further investigation. These significant findings contribute to a deeper understanding of the critical factors influencing the choice between decentralized and centralized database solutions, providing valuable insights for organizations looking to leverage blockchain technology effectively.

.

Global Mainstream Journal of Innovation, Engineering & Emerging Technology
Doi: 10.62304/jieet.v3i04.195

Figure 8: Key findings: Decentralized vs. Centralized Database Solutions in Blockchain



5 Discussion

The discussion of this study, grounded in the systematic review of literature and the significant findings, underscores the complex trade-offs that organizations must navigate when choosing between decentralized and centralized database solutions in blockchain technology. The methodology of this study, which involved a thorough analysis of peer-reviewed articles, industry reports, and case studies, provided a comprehensive understanding of how these database solutions function in different contexts, revealing both their strengths and limitations. The findings clearly demonstrate that while decentralized databases excel in providing enhanced security and transparency through distributed ledger technology, they struggle with scalability and efficiency, particularly in environments requiring high transaction throughput (Almeida et al., 2019; Peng et al., 2020; Sharma et al., 2019). This trade-off is crucial for industries like healthcare and public governance, where data integrity and trust are paramount, but where the limitations in scalability could hinder broader adoption.

Conversely, centralized database solutions offer substantial advantages in terms of efficiency and ease of management, particularly in private or permissioned blockchains where control is centralized. These systems allow for faster processing times and greater scalability, making them well-suited for sectors such as finance and supply chain management, where speed and performance are critical (Sui et al., 2019). However, the discussion highlights that these benefits come with increased security risks, including the potential for single points of failure and reduced transparency, which could undermine trust among stakeholders (Beirami et al., 2019). This inherent vulnerability of centralized systems suggests that while they may be more efficient, they may not always be the most secure option, especially in applications where data security is non-negotiable.

The discussion also points to the varying industry-specific preferences that influence the choice between decentralized and centralized database solutions. For instance, sectors that prioritize data security and transparency are more likely to favor decentralized databases, despite their operational challenges, whereas industries focused on performance and scalability might prefer centralized systems, accepting the trade-offs in security for greater efficiency (Dinh et al., 2018; Wang et al., 2022). These findings emphasize the importance of aligning database architecture with organizational goals and the specific demands of the industry.

Furthermore, the study's identification of a gap in the literature regarding hybrid database models opens up new avenues for research and development. The potential for hybrid solutions that combine the strengths of both decentralized and centralized databases could address many of the challenges identified in this study, offering a balanced approach that mitigates the weaknesses of each while capitalizing on their respective benefits (Thatikonda et al., 2023). This discussion highlights the need for continued exploration and innovation in blockchain technology, particularly in the development of database solutions that can meet the diverse needs of different industries without compromising on security, scalability, or efficiency.

6 Conclusion

In conclusion, this article highlights the critical role that database solutions play in the successful implementation of blockchain technology. The choice between decentralized and centralized databases should be guided by a thorough understanding of their respective advantages, challenges, and use cases. By aligning these solutions with organizational objectives, businesses can optimize their blockchain implementations, ensuring both security and efficiency. Future research should continue to explore the evolving landscape of blockchain technology, particularly the development of hybrid models that may offer the best of both worlds.

References:

Almeida, F., Silva, P. S. P., & Araújo, F. (2019). Performance Analysis and Optimization Techniques for Oracle Relational Databases. *Cybernetics and Information Technologies*, *19*(2), 117-132. https://doi.org/10.2478/cait-2019-0019

Aswathy, S. V., & Lakshmy, K. V. (2019). SSCC - BVD - A Blockchain Based Vehicle Database System. In (Vol. NA, pp. 220-230). https://doi.org/10.1007/978-981-13-5826-5_16

Beirami, A., Zhu, Y., & Pu, K. (2019). Trusted relational databases with blockchain: design and optimization. *Procedia Computer Science*, *155*(NA), 137-144. https://doi.org/10.1016/j.procs.2019.08.022

Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2018). Blockchain-Based Medical Records Secure Storage and Medical Service Framework. *Journal of medical systems*, *43*(1), 5-5. https://doi.org/10.1007/s10916-018-1121-4

Chickerur, S., Goudar, A., & Kinnerkar, A. (2015). Comparison of Relational Database with Document-Oriented Database (MongoDB) for Big Data Applications. *2015 8th International Conference on Advanced Software Engineering & Its Applications (ASEA)*, *NA*(NA), 41-47. https://doi.org/10.1109/asea.2015.19

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A. E., Miller, A., Saxena, P., Shi, E., Sirer, E. G., Song, D., & Wattenhofer, R. (2016). Financial Cryptography Workshops - On Scaling Decentralized Blockchains. In (Vol. 9604, pp. 106-125). https://doi.org/10.1007/978-3-662-53357-4_8

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering*, *30*(7), 1366-1385. https://doi.org/10.1109/tkde.2017.2781227

El-Hindi, M., Binnig, C., Arasu, A., Kossmann, D., & Ramamurthy, R. (2019). BlockchainDB: a shared database on blockchains. *Proceedings of the VLDB Endowment*, *12*(11), 1597-1609. https://doi.org/10.14778/3342263.3342636

Ge, Z., Loghin, D., Ooi, B. C., Ruan, P., & Wang, T. (2022). Hybrid blockchain database systems. *Proceedings of the VLDB Endowment*, *15*(5), 1092-1104. https://doi.org/10.14778/3510397.3510406

Gorenflo, C., Lee, S., Golab, L., & Keshav, S. (2020). FastFabric: Scaling hyperledger fabric to 20 000 transactions per second. *International Journal of Network Management*, *30*(5), NA-NA. https://doi.org/10.1002/nem.2099

Hao, K., Xin, J., Wang, Z., Cao, K., & Wang, G. (2019). Blockchain-Based Outsourced Storage Schema in Untrusted Environment. *IEEE Access*, *7*(NA), 122707-122721. https://doi.org/10.1109/access.2019.2938578

Hong, A., Sun, C., & Chen, M. (2020). *SmartBlock - A Survey of Distributed Database Systems based on Blockchain* (Vol. NA). https://doi.org/10.1109/smartblock52591.2020.00042

Huang, H., Peng, X., Zhan, J., Zhang, S., Lin, Y., Zheng, Z., & Guo, S. (2022). BrokerChain: A Cross-Shard Blockchain Protocol for Account/Balance-based State Sharding. *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, *NA*(NA), NA-NA. https://doi.org/10.1109/infocom48880.2022.9796859

Islam, S. (2024). Future Trends in SQL Databases And Big Data Analytics: Impact Of Machine Learning And Artificial Intelligence. *International Journal of Science and Engineering*, *1*(04), 47-62. https://doi.org/10.62304/ijse.v1i04.188

Jia, D., Xin, J., Wang, Z., Guo, W., & Wang, G. (2019). *ELM - An Optimized Data Distribution Model for ElasticChain to Support Blockchain Scalable Storage* (Vol. NA). https://doi.org/10.1007/978-3-030-23307-5_9

Jia, D., Xin, J., Wang, Z., & Wang, G. (2021). Optimized Data Storage Method for Sharding-Based Blockchain. *IEEE Access*, *9*(NA), 67890-67900. https://doi.org/10.1109/access.2021.3077650

Kleinaki, A.-S., Mytis-Gkometh, P., Drosatos, G., Efraimidis, P. S., & Kaldoudi, E. (2018). A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval. *Computational and structural* *biotechnology journal*, *16*(NA), 288-297. https://doi.org/10.1016/j.csbj.2018.08.002

Kotobi, K., & Bilén, S. G. (2018). Secure Blockchains for Dynamic Spectrum Access: A Decentralized Database in Moving Cognitive Radio Networks Enhances Security and User Access. *IEEE Vehicular Technology Magazine*, *13*(1), 32-39. https://doi.org/10.1109/mvt.2017.2740458

Kuo, T.-T., Kim, H., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association : JAMIA*, *24*(6), 1211-1220. https://doi.org/10.1093/jamia/ocx068

Lakhan, A., Mohammed, M. A., Elhoseny, M., Alshehri, M. D., & Abdulkareem, K. H. (2022). Blockchain multi-objective optimization approach-enabled secure and cost-efficient scheduling for the Internet of Medical Things (IoMT) in fog-cloud system. *Soft Computing*, *26*(13), 6429-6442. https://doi.org/10.1007/s00500-022-07167-9

Li, D., Han, D., Zheng, Z., Weng, T.-H., Li, H., Liu, H., Castiglione, A., & Li, K.-C. (2022). MOOCsChain: A Blockchain-Based Secure Storage and Sharing Scheme for MOOCs Learning. *Computer Standards & Interfaces*, *81*(NA), 103597-NA. https://doi.org/10.1016/j.csi.2021.103597

Li, H., Zhu, L., Shen, M., Gao, F., Tao, X., & Liu, S. (2018). Blockchain-Based Data Preservation System for Medical Data. *Journal of medical systems*, *42*(8), 141-141. https://doi.org/10.1007/s10916-018-0997-3

Lian, J., Wang, S., & Xie, Y. (2021). TDRB: An Efficient Tamper-Proof Detection Middleware for Relational Database Based on Blockchain Technology. *IEEE Access*, *9*(NA), 66707-66722. https://doi.org/10.1109/access.2021.3076235

Liu, J., Li, W., Karame, G., & Asokan, N. (2019). Scalable Byzantine Consensus via Hardware-Assisted Secret Sharing. *IEEE Transactions on Computers*, *68*(1), 139-151. https://doi.org/10.1109/tc.2018.2860009

McGhin, T., Choo, K.-K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, *135*(NA), 62-75. https://doi.org/10.1016/j.jnca.2019.02.027

Mettler, M. (2016). HealthCom - Blockchain technology in healthcare: The revolution starts here. *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, *NA*(NA), 1-3. https://doi.org/10.1109/healthcom.2016.7749510

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy Challenges. *Internet of Things*, *8*(NA), 100107-NA. https://doi.org/10.1016/j.iot.2019.100107

Muzammal, M., Qu, Q., & Nasrulin, B. (2019). Renovating blockchain with distributed databases: An open source system. *Future Generation Computer Systems*, *90*(NA), 105-117. https://doi.org/10.1016/j.future.2018.07.042

Mytis-Gkometh, P., Drosatos, G., Efraimidis, P. S., & Kaldoudi, E. (2017). Notarization of Knowledge Retrieval from Biomedical Repositories Using Blockchain Technology. In (Vol. NA, pp. 69-73). https://doi.org/10.1007/978-981-10-7419-6_12

Nathan, S., Govindarajan, C., Saraf, A., Sethi, M., & Jayachandran, P. (2019). Blockchain meets database: design and implementation of a blockchain relational database. *Proceedings of the VLDB Endowment*, *12*(11), 1539-1552. https://doi.org/10.14778/3342263.3342632

Nizamuddin, N., Salah, K., Azad, M. A., Arshad, J., & Rehman, M. H. u. (2019). Decentralized document version control using ethereum blockchain and IPFS. *Computers & Electrical Engineering*, *76*(NA), 183-197. https://doi.org/10.1016/j.compeleceng.2019.03.014

Peng, Y., Du, M., Li, F., Cheng, R., & Song, D. (2020). SIGMOD Conference - FalconDB: Blockchain-based Collaborative Database. *Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data*, *NA*(NA), 637-652. https://doi.org/10.1145/3318464.3380594

Rani, K., & Sharma, C. (2019). IC3 - Tampering Detection of Distributed Databases using Blockchain Technology. *2019 Twelfth International Conference on Contemporary Computing (IC3)*, *NA*(NA), 1-4. https://doi.org/10.1109/ic3.2019.8844938

Ruan, P., Chen, G., Dinh, T. T. A., Lin, Q., Ooi, B. C., & Zhang, M. (2019). Fine-grained, secure and efficient data provenance on blockchain systems. *Proceedings of the VLDB Endowment*, *12*(9), 975-988. https://doi.org/10.14778/3329772.3329775

Shamim, M. I. (2022). Exploring the success factors of project management. *American Journal of Economics and Business Management*, *5*(7), 64-72.

Sharma, A., Schuhknecht, F. M., Agrawal, D., & Dittrich, J. (2019). SIGMOD Conference - Blurring the Lines between Blockchains and Database Systems: the Case of Hyperledger Fabric. *Proceedings of the 2019 International Conference on Management of Data*, *NA*(NA), 105-122. https://doi.org/10.1145/3299869.3319883

Sui, Z., Lai, S., Zuo, C., Yuan, X., Liu, J. K., & Qian, H. (2019). Inscrypt - An Encrypted Database with Enforced Access Control and Blockchain Validation. In (Vol. NA, pp. 260-273). https://doi.org/10.1007/978-3-030-14234-6_14

Tan, K.-L., Cai, Q., Ooi, B. C., Wong, W.-F., Yao, C., & Zhang, H. (2015). In-memory Databases: Challenges and Opportunities From Software and Hardware Perspectives. *ACM SIGMOD Record*, *44*(2), 35-40. https://doi.org/10.1145/2814710.2814717

Thatikonda, R., Vaddadi, S. A., Arnepalli, P. R. R., & Padthe, A. (2023). Securing biomedical databases based on fuzzy method through blockchain technology. *Soft Computing*. https://doi.org/10.1007/s00500-023-08355-x

Tseng, L., Yao, X., Otoum, S., Aloqaily, M., & Jararweh, Y. (2020). Blockchain-based database in an IoT environment: challenges, opportunities, and analysis. *Cluster Computing*, *23*(3), 2151-2165. https://doi.org/10.1007/s10586-020-03138-7

Tsoulias, K., Palaiokrassas, G., Fragkos, G., Litke, A., & Varvarigou, T. (2020). A Graph Model Based Blockchain Implementation for Increasing Performance and Security in Decentralized Ledger Systems. *IEEE Access*, *8*(NA), 130952-130965. https://doi.org/10.1109/access.2020.3006383

Vainshtein, Y., & Gudes, E. (2021). *CSCML - Use of Blockchain for Ensuring Data Integrity in Cloud Databases* (Vol. NA). https://doi.org/10.1007/978-3-030-78086-9_25

Wang, H., Xu, C., Zhang, C., Xu, J., Peng, Z., & Pei, J. (2022). vChain+: Optimizing Verifiable Blockchain Boolean Range Queries. *2022 IEEE 38th International Conference on Data Engineering (ICDE)*, *NA*(NA), NA-NA. https://doi.org/10.1109/icde53745.2022.00190

Wang, J., Han, K., Alexandridis, A., Chen, Z., Zilic, Z., Pang, Y., Jeon, G., & Piccialli, F. (2020). A blockchain-based eHealthcare system interoperating with WBANs. *Future Generation Computer Systems*, *110*(NA), 675-685. https://doi.org/10.1016/j.future.2019.09.049

Xinying, Y., Yuan, Z., Wang, S., Benquan, Y., Li, F., Yize, L., & Wenyuan, Y. (2020). LedgerDB: a centralized ledger database for universal audit and verification. *Proceedings of the VLDB Endowment*, *13*(12), 3138-3151. https://doi.org/10.14778/3415478.3415540

Yan, D., Jia, X., Shu, J., & Yu, R. (2021). A Blockchain-based Database System for Decentralized Information Management. *2021 IEEE Global Communications Conference (GLOBECOM)*, *NA*(NA), NA-NA. https://doi.org/10.1109/globecom46510.2021.9685695

Zhang, H., Chen, G., Ooi, B. C., Tan, K.-L., & Zhang, M. (2015). In-Memory Big Data Management and Processing: A Survey. *IEEE Transactions on Knowledge and Data Engineering*, *27*(7), 1920-1948. https://doi.org/10.1109/tkde.2015.2427795

Zheng, W., Zheng, Z., Chen, X., Dai, K., Li, P., & Chen, R. (2019). NutBaaS: A Blockchain-as-a-Service Platform. *IEEE Access*, *7*(NA), 134422-134433. https://doi.org/10.1109/access.2019.2941905