International Journal of Multidisciplinary Research and Growth Evaluation.

Blockchain Meets Cloud: Reinventing Decentralization and Secure Transactions

Bhanu Raju Nida
Independent Researcher, Philadelphia, United States

* Corresponding Author: **Bhanu Raju Nida**

Article Info

ISSN (online): 2582-7138
Volume: 06
Issue: 02
March-April 2025
Received: 28-01-2025
Accepted: 25-02-2025
Page No: 408-413

Abstract
The integration of blockchain and cloud computing is reshaping the way we think about data security, trust, and decentralization. While cloud computing offers scalability, efficiency, and cost-effectiveness, its centralized nature raises concerns about data privacy, security vulnerabilities, and dependency on third-party providers. Blockchain, known for its decentralized, immutable, and cryptographically secure structure, presents a promising solution by enhancing trust, reducing reliance on intermediaries, and ensuring secure transactions.

This paper explores the potential and challenges of integrating blockchain with cloud computing, examining how blockchain can strengthen cloud security, storage, and identity management. A theoretical framework is proposed where blockchain acts as a security layer within cloud infrastructure. Through real-world case studies, including Amazon QLDB and Microsoft Azure Confidential Ledger, we analyze blockchain's role in secure storage, transparent data logging, and automated access control. Additionally, an experimental evaluation tests blockchain's effectiveness in automating cloud transactions, improving data integrity, and enhancing cost efficiency.

Despite its potential, blockchain-cloud integration faces hurdles like scalability, interoperability, and regulatory concerns. However, innovations such as Layer-2 scaling solutions, AI-driven automation, and quantum-resistant cryptography offer promising ways to address these challenges. This study contributes to the growing research on secure and decentralized cloud solutions, identifying adoption barriers and outlining future directions for trustless and efficient cloud computing.

DOI: https://doi.org/10.54660/.IJMRGE.2025.6.2.408-413

Keywords: Blockchain, Cloud Computing, Security, Decentralization, Smart Contracts, Data Integrity, Identity Management

1. Introduction

In the modern world, cloud computing has become the fundamental for IT infrastructure, providing easy and scalable access to computing resources. People and companies use cloud services for data storage, processing and application hosting because it is cheaper and more convenient. However, the centralization of cloud computing is the source of many concerns about security, trust, and data ownership. Problems such as single points of failure, unauthorized access, and data loss have highlighted the need for better and more decentralized solutions.

Blockchain technology, which made its debut with Bitcoin in 2008, is now considered a revolutionary platform for trustless and secure transactions. Blockchain is decentralized, immutable, and secure by cryptography. It eliminates intermediaries and ensures data integrity with a consensus mechanism. Public and private blockchain networks have many applications after bitcoin and include supply chain management, banking, healthcare and identity management. The advantages of the blockchain are such that it can be used effectively to solve the problems of traditional cloud computing security.

The integration of blockchain and cloud computing opens new opportunities for decentralized cloud services, secure storage, automated smart contracts and access control. Blockchain can enhance cloud security by establishing trust, reducing reliance on third parties, and enabling digital identities. However, challenges like scalability, interoperability, and energy consumption

need to be addressed for the effective adoption of blockchain. This paper aims to explore the relationship between blockchain and cloud computing by exploring how blockchain can enhance the security, transparency, and decentralization of cloud computing. The study particularly aims to establish whether blockchain frameworks can address cloud risks, improve data reliability, and enable trustless cloud computing.

The key objectives of this study are:

- To examine the fundamental principles of blockchain and their applicability to cloud security.
- To analyze the limitations of traditional cloud computing and how blockchain can address them.
- To explore real-world use cases where blockchain enhances cloud security, storage, and identity management.
- To evaluate the challenges and future directions in integrating blockchain with cloud architectures.

Contributions and structure of the paper

This paper contributes to the growing body of research on blockchain-enabled cloud solutions by offering a comprehensive review of existing literature, identifying potential implementation challenges, and proposing a framework for secure, decentralized cloud services. The structure of the paper is as follows: Section 2 presents a literature review on blockchain and cloud computing, highlighting prior research and existing integration models. Section 3 outlines the theoretical framework and methodology used in this study. Section 4 explores various blockchain-cloud applications, including secure storage, decentralized identity management, and automated smart contracts. Section 5 discusses the challenges and future research directions, followed by Section 6, which concludes the paper and provides key takeaways.

2. Literature Review

Blockchain and cloud computing are two groundbreaking technologies that are gradually being integrated to address security and trust challenges in distributed systems. Blockchain provides decentralization, immutability, and cryptographic security [1], [2], while cloud computing delivers scalable, on-demand resources [3].

By working together, these technologies can improve cloud efficiency, particularly in areas like data integrity, resource management, and security [4], [6]. This makes them particularly valuable for industries such as supply chain management, financial services, and healthcare [6]

Despite their potential, challenges such as scalability, interoperability, and regulatory compliance remain [7], [8]. To address these, major cloud providers now offer Blockchain-as-a-Service (BaaS) solutions [5], making integration more accessible.

While obstacles persist, combining blockchain with cloud computing has the potential to revolutionize data management and collaboration across multiple industries [6], [8].

This paper explores how integrating blockchain technology with cloud computing can help address cloud security challenges, such as data breaches and the loss of sensitive information. It provides a deep dive into blockchain technology—its origins, key components, applications, benefits, and challenges—while also analyzing its role in cloud computing.

The study reviews existing applications of blockchain in cloud systems, highlighting research gaps and potential areas for further development. It also discusses the differences between public and private blockchains and their relevance to cloud computing.

By combining blockchain with cloud computing, organizations can enhance network control, security, and service reliability. However, this integration also comes with technological hurdles. The paper examines these potential synergies, emphasizing how they can lead to better system security and improved customer satisfaction.

3. Theoretical framework and methodology

3.1 Theoretical Framework

The integration of blockchain with cloud computing is based on the principles of decentralization, trustless security, and cryptographic validation with an aim of solving major flaws in the conventional cloud frameworks. This theoretical framework is based on Distributed Ledger Technology (DLT), Zero Trust Security Models and Decentralized Identity Management which collectively enhance the security, transparency and efficiency of cloud services.

3.1.1 Proposed model for blockchain-cloud integration

This model envisions blockchain as a security and trust layer over existing cloud infrastructure, featuring:

a) Decentralized Cloud Storage: Uses blockchain-based storage networks (like IPFS, Filecoin) to prevent data from being stored in a single, vulnerable location.
b) Smart Contracts for Cloud Services: Automates service agreements and resource management with Ethereum or Hyperledger smart contracts, making cloud operations more transparent and efficient.
c) Decentralized Identity & Access Control: Introduces Self-Sovereign Identity (SSI) to reduce dependence on centralized identity providers and minimize credential theft risks.
d) Immutable Audit Logs: Stores cloud transactions and access records on blockchain, ensuring tamper-proof logs for compliance and traceability.
e) Interoperability: Enables seamless interaction between blockchain and cloud platforms through APIs, middleware, and sidechains for better performance and scalability

3.1.2 Key evaluation parameters

The model's effectiveness is measured based on:

- Security: Blockchain ensures data integrity, decentralized authentication, and strong cyber threat resistance.
- Scalability: Investigates how Layer-2 solutions (e.g., sidechains, sharding) can help blockchain handle high transaction volumes.
- Efficiency: Assesses computational impact, latency, and data retrieval speed to balance security with performance.
- Cost-Effectiveness: Compares cost savings from reduced third-party security needs against added blockchain-related expenses like transaction fees.

3.1.3 Comparison with traditional cloud models

Table 1: Traditional Cloud Computing vs. Blockchain-Integrated Cloud

Feature	Traditional Cloud Computing	Blockchain-Integrated Cloud
Data Storage	Centralized servers	Decentralized storage (IPFS, Filecoin)
Security	Vulnerable to single points of failure	Tamper-proof cryptographic security
Identity Management	Managed by third-party providers	Self-sovereign, decentralized identity
Trust Mechanism	Relies on cloud providers	Trustless verification via consensus
Cost Structure	Subscription-based, third-party fees	Reduced third-party reliance, but blockchain fees apply

3.2 Methodology

Research Approach

This study employs a multi-method approach, combining case study analysis and experimental validation to assess blockchain's role in securing cloud systems.

3.2.1 Case study analysis

Selected real-world implementations, such as Amazon QLDB, Microsoft Azure Confidential Ledger, and Filecoin, are examined to assess their practical applications, security benefits, and adoption challenges.

Amazon QLDB Case Studies:

- Specright's Traceable Supply Chain Network: Specright utilized Amazon QLDB to create the Specright Network, enabling brands, retailers, and manufacturers to share critical supply chain and packaging specification data. This implementation enhanced transparency and traceability across their supply chain [9].
- BungkusIT's Logistics Platform: BungkusIT integrated Amazon QLDB with VeriDoc Global's technology to develop a centralized, transparent platform for inter-industry communication. This solution provided an immutable and cryptographically verifiable transaction log, improving the customer and delivery agent experience [10].

Microsoft Azure Confidential Ledger Overview Case Study:

- Microsoft's Azure Confidential Ledger is a highly secure service designed for managing sensitive data records. It offers tamperproof storage backed by blockchain technology, ensuring data integrity and protection from unauthorized modifications. The service is ideal for scenarios requiring regulatory compliance, audit trails, and protection against insider threats [11].

3.2.2 Experimental Validation

A prototype system is developed to test blockchain integration in cloud environments, focusing on:

- Smart contract-based SLA enforcement – Evaluating automated cloud service agreements.
- Cloud storage performance testing – Comparing traditional vs. blockchain-powered storage solutions in terms of data retrieval speed, redundancy, and security.
- Cost-benefit analysis – Assessing the financial impact of decentralized storage compared to conventional cloud services.

3.2.3 Data collection & evaluation

A combination of qualitative insights (e.g., security risks, user trust) and quantitative performance metrics (e.g., latency, transaction costs, energy consumption) is used to evaluate the feasibility and effectiveness of blockchain integration.

3.2.4 Study Limitations

While the study provides both theoretical and experimental insights, practical adoption is influenced by regulatory constraints, interoperability issues, and energy consumption concerns, which remain areas for future research

4. Blockchain-cloud synergies and use cases

Blockchain technology combined with cloud computing has produced creative ideas improving security, decentralization, and operational effectiveness. This part looks at main synergies and useful applications resulting from this convergence.

4.1 Secure cloud storage with blockchain

4.1.1 Data integrity and decentralized file storage

Traditional cloud storage systems often rely on centralized servers, making them susceptible to single points of failure and unauthorized access. Blockchain introduces decentralized file storage solutions, such as the Interplanetary File System (IPFS) and File coin, which distribute data across a network of nodes, ensuring redundancy and resilience [12].

- IPFS: A peer-to-peer hypermedia protocol designed to improve data integrity and accessibility by storing and sharing data across a distributed network [13].
- Filecoin: Built on top of IPFS, Filecoin incentivizes users to contribute storage space to the network, creating a decentralized storage marketplace that enhances data availability and security by eliminating reliance on centralized providers [12].

4.1.2 Encryption and Access control

Strong encryption and access control systems included in blockchain improve cloud storage security. Before being kept on the blockchain, data is encrypted such that only authorized users with the proper decryption keys may access it. By automating permissions and thereby lowering the danger of illegal data access, smart contracts can enforce access control restrictions.

4.2 Decentralized identity management in cloud services

4.2.1 Self-Sovereign identity and zero-trust frameworks

Decentralized Identity (DID) solutions enable people to own and manage their digital identities free from depending on centralized authority. Operating on the idea of confirming every access demand, regardless of source, this self-sovereign identity model fits zero-trust security systems [14].

- Self-Sovereign Identity (SSI): Allows users to manage their identities through blockchain-based platforms, providing greater privacy and control over personal data [15].
- Zero-Trust Security: A security model that assumes no implicit trust and requires continuous verification of user identities and devices, enhancing security in cloud environments [16].

4.2.2 Applications in authentication and access control

Blockchain-based identity management solutions improve access control in cloud services and simplify authentication methods. Organizations can use more safe and effective authentication systems by means of distributed IDs and

verifiable credentials, therefore lowering the danger of identity theft and illegal access [17].

4.3 Smart contracts for automated cloud transactions

4.3.1 Blockchain-Based cloud service agreements

Smart contracts are self-executing agreements containing straight code language terms. In cloud computing, they can automate service-level agreements (SLAs), therefore guaranteeing that clients and cloud service providers follow pre-defined terms free from middlemen. [18].

4.3.2 Trustless execution of cloud resource allocation and payments

Smart contracts automatically execute activities when criteria are satisfied, therefore enabling trustless transactions. This capacity can automate resource allocation, billing, and payments in cloud systems so lowering administrative cost and improving transparency [19].

4.3.3 Edge computing and decentralized cloud solutions

Edge computing brings computation and data storage closer to data sources, reducing latency and bandwidth usage. Integrating blockchain with edge computing enables decentralized cloud solutions, where data processing occurs at the network's edge, enhancing speed and security [19].

Emerging Trends:

- Fog Computing: Extends cloud computing to the network edge, allowing data to be processed locally on devices rather than being sent to centralized data centers. This approach reduces latency and enhances real-time data processing capabilities [20].
- Edge Blockchain Networks: Implementing blockchain at the edge ensures data integrity and security in decentralized applications, supporting use cases like IoT device management and secure data sharing [21].

5. Challenges and Future directions

The integration of blockchain and cloud computing has the potential to transform industries by making systems more decentralized, secure, and transparent. However, before this vision can be fully realized, several obstacles need to be addressed. At the same time, emerging technologies like AI-driven blockchain solutions and quantum-resistant security offer promising ways to overcome these hurdles. This section explores the key challenges and future advancements in blockchain-cloud integration.

5.1 Scalability: Can blockchain keep up with cloud computing?

One of the biggest challenges is scalability—blockchain transactions are much slower than traditional cloud-based systems. For instance, while Ethereum processes around 15 transactions per second (TPS), cloud-based systems can handle thousands [22].

- Why This Matters: Cloud computing is built for speed, handling massive amounts of data in real-time. When blockchain is added to the mix, its slow transaction speeds could create bottlenecks, making cloud applications less efficient.
- Possible Solutions: Technologies like Layer-2 scaling solutions (e.g., rollups, state channels) allow transactions to be processed off-chain before being added to the blockchain. This speeds things up while keeping blockchain's security intact.

5.2 Making blockchain and cloud systems work together

Blockchain and cloud platforms don't naturally speak the same language. Different blockchains (Ethereum, Bitcoin, Hyperledger) use unique rules and formats, making it difficult to connect them seamlessly with cloud services like AWS, Azure, or Google Cloud.

- The Challenge: Since blockchains follow their own protocols, they don't integrate easily with cloud platforms. This makes it harder to use blockchain for cloud-based applications like decentralized finance (DeFi) or blockchain-based cloud storage [23].
- What's Next? Developers are working on cross-chain protocols like Polkadot and Cosmos, which allow different blockchains to communicate with each other. Also, major cloud providers now offer Blockchain-as-a-Service (BaaS) to simplify integration [24].

5.3 The legal gray area: Regulation & compliance issues

Blockchain's decentralized nature doesn't fit neatly into traditional regulations. Laws like GDPR (data privacy) and AML (anti-money laundering) were designed for centralized systems, making it difficult to apply them to blockchain-based solutions.

- Data Privacy Issues: Blockchain records are permanent—once data is added, it can't be deleted. This directly conflicts with laws that allow users to request data deletion, like GDPR [25].
- What Needs to Happen: Governments and regulators need to modernize legal frameworks to account for blockchain's unique properties. Some countries are already working on blockchain-specific regulations, but a more global approach is needed to ensure smooth adoption [26].

5.4 AI and Blockchain: A smarter cloud?

The combination of Artificial Intelligence (AI) and blockchain could solve many existing challenges, making blockchain-powered cloud services smarter and more efficient.

- How AI Can Help: AI can predict transaction loads, detect security threats, and automate blockchain processes, improving performance and security [27].
- The Future of Autonomous Cloud Services: AI-powered cloud systems can predict demand, optimize network usage, and automate service management. Platforms like Microsoft Azure are already integrating AI and blockchain to create intelligent, decentralized cloud services [28].

5.5 The quantum threat: securing blockchain in a new era

Quantum computing is an exciting development—but it also poses a major security risk for blockchain and cloud systems. Future quantum computers could break current encryption methods, making today's blockchain security vulnerable.

- The Problem: Many blockchain and cloud security systems rely on mathematical encryption, which quantum computers could potentially crack [29].
- The Solution: Researchers are working on quantum-resistant cryptography to ensure that blockchain and cloud encryption remains secure. Another potential safeguard is Quantum Key Distribution (QKD), which could make it nearly impossible for hackers to intercept blockchain transactions [30].

6. Conclusion

The integration of blockchain and cloud computing presents a powerful solution to many of the security and trust issues associated with traditional cloud services. While cloud computing is efficient and scalable, its reliance on centralized control makes it vulnerable to security breaches, data loss, and trust concerns. Blockchain's decentralized, tamper-proof, and cryptographically secure nature offers a compelling way to enhance trust, data security, and automation in cloud environments.

This paper examined how blockchain can strengthen cloud security, decentralized identity management, and automated service agreements. We proposed a hybrid framework where blockchain serves as a trust and security layer over cloud infrastructure. Through case studies like Amazon QLDB and Microsoft Azure Confidential Ledger, we explored practical applications where blockchain has improved data integrity, authentication, and compliance. Furthermore, our experimental evaluation highlighted how blockchain can enhance service automation, reduce dependency on intermediaries, and improve overall data security.

However, blockchain-cloud integration is not without challenges. Scalability remains a key concern, as blockchain transaction speeds are significantly slower than traditional cloud processing. Interoperability is another hurdle, as different blockchain and cloud platforms lack seamless communication. Additionally, regulatory uncertainties surrounding blockchain's decentralized nature create complications for data privacy laws, financial regulations, and compliance requirements.

Looking ahead, advancements in AI-driven automation, cross-chain interoperability, and quantum-resistant security will be crucial in making blockchain-cloud integration more efficient and widely adopted. AI can help optimize network performance, security monitoring, and automated decision-making, while quantum-resistant cryptography will safeguard blockchain systems against future threats from quantum computing.

7. References

1. Murthy CVN, Bharathi U, *et al* Blockchain based cloud computing: architecture and research challenges. IEEE Access. 2020; 8:205190–205205.
2. Blockchain integration in cloud computing: ensuring transparency and security. International Research Journal of Modernization in Engineering Technology and Science. 2024; n. pag.
3. Sarmah SS. Application of blockchain in cloud computing. International Journal of Innovative Technology and Exploring Engineering. 2019;8(12):4698–4704. doi:10.35940/ijitee.l3585.1081219
4. Habib G, Sharma S, Ibrahim S, Ahmad I, Qureshi S, Ishfaq M. Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet. 2022;14(11):341. doi:10.3390/fi14110341
5. Alshinwan M, Shdefat AY, Mostafa N, AlSokkar AAM, Alsarhan T, Almajali D. Integrated cloud computing and blockchain systems: a review. International Journal of Data and Network Science. 2023;7(2):941–956. doi: 10.5267/j.ijdns.2022.12.016
6. Nair SS. Blockchain and cloud services: exploring the potential synergies and applications of blockchain technology in cloud computing. International Journal of Advanced Research in Computer and Communication Engineering. 2023;12(12). doi:10.17148/ijarcce.2023.121209
7. Mechkaroska D, Popovska-Mitrovikj A, Mitrevska S. Overview of blockchain and cloud computing services integration. In: 2022 30th Telecommunications Forum (TELFOR). IEEE; 2022:1–4. doi:10.1109/telfor56187.2022.9983759
8. Rani M, Guleria K, Panda SN. Blockchain technology novel prospective for cloud security. In: 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). IEEE; 2022:1–6. doi:10.1109/icrito56286.2022.9964666
9. How Specright uses Amazon QLDB to create a traceable supply chain network. Amazon Web Services. 2022 Jan 22. Available from: https://aws.amazon.com/blogs/database/how-specright-uses-amazon-qldb-to-create-a-traceable-supply-chain-network/
10. BungkusIT uses Amazon QLDB and VeriDoc Global's ISV technology to improve the customer and delivery agent experience. Amazon Web Services. 2022 May 2. Available from: https://aws.amazon.com/blogs/database/bungkusit-uses-amazon-qldb-and-veridoc-globals-isv-technology-to-improve-the-customer-and-delivery-agent-experience/
11. MicrosoftDocs. Azure-security-docs/articles/confidential-ledger/overview.md at main. GitHub. n.d. Available from: https://github.com/MicrosoftDocs/azure-security-docs/blob/main/articles/confidential-ledger/overview.md
12. Team I. Blockchain-as-a-service (BAAS) meaning and major players. Investopedia. 2024 Jul 21. Available from: https://www.investopedia.com/terms/b/blockchainasaservice-baas.asp
13. Silicon Mechanics. Silicon Mechanics InterPlanetary File System (IPFS) infrastructure. n.d. Available from: https://www.siliconmechanics.com/solutions/ipfs#:~:text=How%20does%20the%20InterPlanetary%20File,security%2C%20integrity%2C%20and%20performance
14. Decentralized identity: the ultimate guide 2025. n.d. Available from: https://www.dock.io/post/decentralized-identity#:~:text=Decentralized%20identity%20is%20a%20type,electronic%20device%20that%20exists%20online
15. Hendrickson L. Your guide to self-sovereign identity (SSI). Identity. 2025 Mar 3. Available from: https://www.identity.com/self-sovereign-identity/#:~:text=Identity%20(SSI)?-,Self%2Dsovereign%20identity%20(SSI)%20is%20a%20digital%20identity%20model,particular%20transaction%20or%20verification%20process
16. Jadhav R. Zero trust: the absolute solution to cloud security challenges. AccuKnox. 2025 Jan 22. Available from: https://www.accuknox.com/blog/zero-trust-cloud-security-future
17. Punia A, Gulia P, Gill NS, Ibeke E, Iwendi C, Shukla PK. A systematic review on blockchain-based access control systems in cloud environment. Journal of Cloud Computing: Advances Systems and Applications. 2024;13(1). doi:10.1186/s13677-024-00697-7
18. Magazzo S. What are smart contracts and why are they good for your business? Mondo Staffing Agency. 2024 Aug 26. Available from: https://mondo.com/insights/what-are-smart-contracts-

and-why-are-they-good-for-your-business/#:~:text=Smart%20contracts%20are%20self%2Dexecuting,roles%20required%20for%20successful%20adoption
19. Seshadrinathan S, Chandra S. Trusting the trustless blockchain for its adoption in accounting: theorizing the mediating role of technology-organization-environment framework. Financial Innovation. 2025;11(1). doi:10.1186/s40854-024-00685-5
20. Calderon J. FoG computing: bridging the gap between cloud and edge. Nfina. 2024 Nov 1. Available from: https://nfina.com/fog-computing/#:~:text=Imagine%20your%20smart%20devices%20communicating%20intelligently%20without,analytics%20while%20minimizing%20latency%20and%20bandwidth%20issues
21. Snape G. Is blockchain finally coming for the insurance industry? Insurance Business America. 2023 Jan 24. Available from: https://www.insurancebusinessmag.com/us/news/technology/is-blockchain-finally-coming-for-the-insurance-industry-433879.aspx
22. Habib G, Sharma S, Ibrahim S, Ahmad I, Qureshi S, Ishfaq M. Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet. 2022;14(11):341. doi:10.3390/fi14110341
23. Gromyko A, Luca P, Chaijitwanitkul SMP, Rozowicz R, Shaheen T, Stelea M, Tao S. Blockchain technology and its implications. OxJournal. n.d. Available from: https://www.oxjournal.org/blockchain-technology-and-its-implications/
24. Wikipedia contributors. Polkadot (blockchain platform). Wikipedia. 2025 Feb 9. Available from: https://en.wikipedia.org/wiki/Polkadot_(blockchain_platform)
25. Abdul SSM. Navigating blockchain's twin challenges: scalability and regulatory compliance. Blockchains. 2024;2(3):265–298. doi:10.3390/blockchains2030013
26. Hakia. Emerging trends in blockchain and cryptocurrency regulation: future policy insights. Hakia: Covering All Angles of Technology. 2024 Sep 21. Available from: https://hakia.com/emerging-regulatory-trends-in-blockchain-and-cryptocurrency-policy-developments-and-future-outlook/#:~:text=However%2C%20strict%20regulatory%20measures%20can,in%20an%20uneven%20playing%20field
27. Venkatesan K, Rahayu SB. Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques. Scientific Reports. 2024;14(1). doi:10.1038/s41598-024-51578-7
28. How generative AI empowers cloud automation. Apex Systems. n.d. Available from: https://www.apexsystems.com/insights/article/how-generative-ai-empowers-cloud-automation#:~:text=AI%20aims%20to%20make%20cloud,intelligent%20security%2C%20and%20continuous%20improvement
29. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. Post-quantum cryptography standardization. CSRC. n.d. Available from: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization
30. S MG, Mulay C, Durai K, Murali G, Masood JAI, Vijayarajan V, *et al* Quantum blockchain: trends, technologies, and future directions. IET Quantum Communication. 2024;5(4):516–542. doi:10.1049/qtc2.12119.