Article

Blockchain Future in Cloud Computing: The Challenges to Implement Blockchain Technology in Cloud Computing

Yuxin Liu [1,*]

[1] Corporate Treasury-Chief Investment Office, JPMorgan Chase, Newark, Delaware, 19107, USA
[*] Correspondence: Yuxin Liu, Corporate Treasury-Chief Investment Office, JPMorgan Chase, Newark, Delaware, 19107, USA

Abstract: With the rapid development of cloud computing technology, more and more industries are starting to utilize data to make meaningful business decisions. Digital innovation has profoundly enhanced business performance. As a result, a more powerful data solution is required to enhance the data management process. Blockchain technology is one of the cutting-edge technologies that has recently been deployed in the cloud computing industry. There are difficulties in implementing blockchain technology that need to be understood by both cloud providers and cloud users.

Keywords: blockchain technology; cloud computing; decentralized database

Received: 09 May 2025
Revised: 20 May 2025
Accepted: 23 June 2025
Published: 28 June 2025

1. Introduction

1.1. Industry Overview

In recent years, reliance on information systems has increased dramatically [1]. Cloud computing has become a popular solution for data storage and business operations due to its flexibility and diverse services [2]. However, challenges such as data security, privacy, high costs, and network dependency remain critical.

Blockchain technology offers a decentralized cloud network that improves data security, reduces third-party trust issues, lowers communication latency, and decreases power consumption [3]. Major cloud providers like AWS and Oracle have integrated blockchain frameworks into their platforms. Various industries, including healthcare, supply chain, banking, and real estate, are adopting blockchain to enhance data safety and process efficiency [4]. Understanding blockchain's impact on cloud computing is vital for providers and users.

1.2. Problem Definition

Integrating blockchain with traditional cloud computing is challenging due to their fundamental operational differences. Centralized cloud databases face security risks, high costs, and vulnerability to attacks, motivating providers to explore blockchain-based solutions [5]. However, issues such as data migration difficulties, resource constraints of IoT devices, and immature blockchain architectures remain [6].

Moreover, decentralization disrupts existing vendor lock-in models, affecting profitability and security — if a majority of nodes control over 50% of computing power, the system's integrity is threatened. Providers must consider both technical benefits and human/economic factors [7].

1.3. Formal Problem Statement

Cloud computing widely supports business data storage and connectivity but faces challenges in security, trust, bandwidth, and cost. Blockchain is a promising solution to overcome these limits. Both providers and users need to understand its strengths and weaknesses for effective integration [8].

1.4. Purpose of Study

This study aims to help cloud providers grasp the future trends in cloud computing, especially regarding digital transformation's reliance on cloud services and blockchain's potential to reshape data management [9].

1.5. Research Question

This research investigates the limitations of current cloud computing and explores how blockchain can optimize cloud services to improve business performance [10]. It focuses on cloud security and ownership issues, blockchain's role in mitigating these problems, and the limitations and solutions of blockchain technology to reduce risks in digital innovation [11].

2. Literature Review

Compared with traditional data storage, cloud computing offers greater flexibility and efficiency. However, with widespread cloud adoption, its limitations become apparent [12]. This review examines current cloud computing challenges, shows how blockchain technology mitigates these issues, and discusses blockchain's own limitations and possible solutions.

2.1. Limitations of the Current Cloud Computing System

Cloud computing has been widely adopted since the early 2000s, valued for scalability and intellectual capital storage [13]. However, cloud reliance presents risks for both providers and users. The primary concern is security: centralized data management by cloud providers creates vulnerabilities and potential unauthorized access [13]. Infrastructure ownership lies with providers, limiting organizations' ability to monitor data, increasing risks of data leakage via public links.

Downtime is another major issue; for example, Facebook's 2021 one-hour outage reportedly caused $65M loss [14]. Centralized infrastructure contributes to such risks, as data stored in provider-owned global data centers faces threats including cyberattacks, vendor lock-in, and limited flexibility [15]. Malicious actors exploit cloud vendors to inject malware, and API abuses can further compromise security.

2.2. How Blockchain Reduces Risks in Cloud Computing

Blockchain reduces risks inherent in centralized cloud systems by decentralizing data storage and control. Distributed networks improve fault tolerance by replicating data across nodes, enhancing resilience to attacks [16]. Notably, blockchain offers stronger access controls via cryptographic algorithms, helping prevent unauthorized access. Cyber threat detection improves due to blockchain's tamper-evident, real-time monitoring features.

Data integrity and consistency are better ensured by blockchain's elimination of third-party intermediaries and use of peer-to-peer encryption and zero-knowledge proofs to prevent unauthorized changes. This architecture grants enterprises more ownership and control over their data while enhancing transparency and reducing risks of breaches and duplication.

2.3. Limitations of Blockchain and Solutions

Despite advantages, blockchain faces challenges such as scalability and high energy consumption. The growing number of nodes hinders transaction throughput, especially with proof-of-work consensus mechanisms. For example, traditional payment systems handle thousands of transactions per second, while Ethereum and Bitcoin are limited due to node validation requirements [17].

Solutions include integrating distributed machine learning with frameworks like Hyperledger Fabric to boost throughput, potentially exceeding 30,000 transactions per second [18]. Alternative consensus mechanisms such as proof-of-history (Solana) and proof-of-space-time (Chia) also improve scalability and reduce energy costs.

Energy consumption and operational costs remain concerns. Proof-of-work requires significant computational power, with transaction energy use comparable to a U.S. household's daily consumption. Proof-of-stake mechanisms offer more energy-efficient validation by selecting validators based on network stake, lowering electricity and hardware demands.

3. Blockchain-Enabled Solutions in Cloud Computing

The integration of blockchain technology into cloud computing is gaining momentum as a strategic solution to overcome the limitations of centralized cloud architecture. Blockchain's decentralized nature, cryptographic foundations, and immutable ledger provide cloud services with enhanced security, transparency, and resilience [19,20]. This section reviews existing blockchain-enabled solutions that have been adopted or proposed in cloud computing environments, focusing on decentralized storage systems, authentication protocols, vendor integration efforts, and real-world applications across various industries.

3.1. Decentralized Storage Systems

One of the primary applications of blockchain in cloud computing is the decentralization of data storage. Traditional cloud providers store user data in centralized servers, which presents single points of failure and exposes data to unauthorized access or tampering [21]. Decentralized storage systems such as the InterPlanetary File System (IPFS) and Filecoin offer alternatives by distributing data across peer-to-peer networks [22]. In IPFS, files are broken into smaller chunks and stored across multiple nodes, with each chunk linked through cryptographic hashes. Filecoin builds upon IPFS by incentivizing users to contribute storage space, thereby creating a self-sustaining, secure, and scalable storage economy. These technologies not only reduce storage costs but also enhance fault tolerance and data integrity.

3.2. Identity Management and Data Security

Blockchain has also emerged as a powerful tool in improving identity verification and data access control within cloud systems. Traditional identity management mechanisms rely on centralized authentication servers, making them vulnerable to breaches and insider threats. Blockchain introduces decentralized identifiers (DIDs) and verifiable credentials that allow users to control their digital identities without relying on third parties [23]. Furthermore, smart contracts — self-executing codes stored on the blockchain — can automate and enforce access permissions [24]. Zero-Knowledge Proofs (ZKPs), a cryptographic technique enabling one party to prove knowledge of a secret without revealing it, enhance privacy-preserving authentication [25]. These technologies create a robust framework for secure, decentralized cloud identity and access management.

3.3. Integration by Major Cloud Service Providers

Several leading cloud service providers have begun integrating blockchain frameworks into their offerings to expand their security and transparency features. Amazon Web Services (AWS) provides managed blockchain services supporting Hyperledger Fabric and Ethereum, enabling enterprises to deploy scalable and secure blockchain networks with minimal setup overhead. Oracle offers the Oracle Blockchain Platform, a pre-configured solution for managing smart contracts, transactions, and digital assets, particularly for supply chain use cases [26]. IBM has also introduced blockchain-enabled hybrid cloud environments through IBM Blockchain Platform, supporting decentralized applications (dApps) across regulated industries. These integrations signify the growing acceptance of blockchain as a complementary layer to conventional cloud services.

3.4. Real-World Industry Applications

The practical implementation of blockchain in cloud environments is evident across a variety of industries. In healthcare, decentralized data storage and blockchain-based consent mechanisms protect patient privacy while facilitating secure data sharing among providers. For example, Medicalchain leverages blockchain to manage electronic health records with patient-controlled access [27]. In the financial sector, blockchain enhances transaction transparency, supports automated compliance, and accelerates cross-border payments. JPMorgan's Quorum, a permissioned blockchain, exemplifies this in enterprise banking. Meanwhile, supply chain management benefits from immutable record-keeping and real-time tracking; platforms such as VeChain enable end-to-end visibility across complex logistics networks. These use cases demonstrate how blockchain can reshape data governance, reduce operational risks, and improve trust in cloud-based services.

4. Technical Integration Challenges

While blockchain technology offers significant potential for transforming cloud computing, its technical integration into existing cloud infrastructures remains fraught with challenges [28]. The inherently decentralized, consensus-driven architecture of blockchain conflicts with the high-speed, high-throughput demands of modern cloud services. This section explores the primary technical barriers to blockchain adoption in cloud environments, focusing on performance constraints, cost implications, scalability limitations, and legal compliance complexities.

4.1. Performance Bottlenecks

One of the most critical challenges in blockchain-cloud integration is the issue of performance degradation. Most public blockchain networks rely on consensus algorithms such as Proof of Work (PoW) or Proof of Stake (PoS) to validate transactions. These mechanisms, while secure, introduce significant latency and limit throughput. For instance, the Bitcoin network processes only 7 transactions per second (TPS), while Ethereum supports around 30 TPS — far below the thousands of TPS required by cloud-based applications. These constraints become even more problematic when real-time processing or high-frequency data exchange is essential, as seen in IoT-enabled environments or financial services. Although newer consensus models like Practical Byzantine Fault Tolerance (PBFT) and Delegated Proof of Stake (DPoS) aim to address these issues, their deployment at scale remains experimental and context-specific.

4.2. Cost Overhead

The cost of integrating blockchain into cloud computing is also a significant concern. Blockchain operations, particularly in public networks, can incur substantial energy and computational costs. For example, PoW-based systems require vast amounts of processing power to solve cryptographic puzzles, resulting in high electricity consumption. Even private or permissioned blockchains, while more efficient, may still demand dedicated hardware and continuous node synchronization, which raises infrastructure and maintenance costs. Furthermore, as smart contract execution and data storage on-chain are resource-intensive, cloud providers may face cost inflation when scaling blockchain-enabled services. Balancing operational costs with security and transparency gains becomes a critical concern for enterprise adoption.

4.3. Scalability Limitations

Scalability remains a persistent barrier to the widespread use of blockchain in cloud services. As the volume of data generated and processed in cloud environments grows exponentially, storing large-scale datasets on a blockchain becomes technically and economically infeasible. Most blockchains impose block size and transaction rate limits, making it difficult to accommodate the high-speed, high-volume data flows characteristic of cloud-based systems. Moreover, blockchain's immutable nature means that storage cannot be reclaimed, leading to ledger bloat and increasing synchronization times for new nodes. Layer-2 solutions and off-chain storage techniques (e.g., combining blockchain with IPFS) are under development to mitigate these issues, but practical implementation remains complex and context-dependent .

4.4. Legal and Data Sovereignty Issues

Beyond technical constraints, integrating blockchain with cloud systems also raises legal and regulatory concerns, particularly around data ownership, privacy, and jurisdiction. Cloud services often operate across multiple regions and legal domains, while blockchain's decentralized nature makes it difficult to enforce data residency and compliance rules. Once data is recorded on a blockchain, especially public or consortium chains, it becomes nearly impossible to modify or delete, posing risks under data protection laws such as the General Data Protection Regulation (GDPR) in the European Union. The concept of "the right to be forgotten" contradicts the immutability principle of blockchain. Furthermore, questions regarding data sovereignty — who has the right to control data in a cross-border, multi-node environment — complicate the adoption of blockchain in highly regulated industries such as healthcare, finance, and public administration.

5. Comparative Evaluation

As cloud computing evolves, organizations must weigh the trade-offs between centralized cloud services and blockchain-enhanced alternatives. This section provides a structured comparison across key dimensions, including availability, security, cost, auditability, and network architecture. The comparative insights aim to assist stakeholders in selecting appropriate cloud models based on business priorities.

5.1. Availability vs. Security

Traditional cloud platforms offer high availability through globally distributed infrastructure and advanced failover mechanisms. However, centralized architecture poses greater risks of data breaches due to the presence of single points of failure. In contrast, blockchain-enabled cloud services enhance security through decentralization and consensus-based validation but may suffer from latency in transaction processing.

Table 1 presents a comparative overview of availability and security between the two architectures.

Table 1. Comparison of Availability and Security between Centralized and Blockchain Cloud Systems.

Aspect	Centralized Cloud	Blockchain-Enhanced Cloud
Uptime	High (with failover)	Medium (consensus latency)
Data Breach Risk	Higher (single point)	Lower (decentralized ledger)
Trust Model	Third-party reliance	Trustless (peer-based)

5.2. Cost vs. Traceability

Centralized cloud systems generally provide cost-effective scalability through economies of scale, though they offer limited audit trails. Blockchain-enhanced platforms, on the other hand, offer robust traceability and transparent logging, which is particularly valuable in regulated industries. However, these benefits often come at the cost of higher resource consumption and infrastructure complexity.

Table 2 outlines the trade-offs between operational cost and traceability.

Table 2. Comparison of Cost and Traceability in Cloud vs. Blockchain-Enhanced Services.

Aspect	Centralized Cloud	Blockchain-Enhanced Cloud
Operational Cost	Lower	Higher (energy&computation)
Auditability	Limited	High (immutable ledger)
Smart Contract Support	External (via APIs)	Native (e.g., Ethereum)

5.3. Network Architecture: Centralized vs. Distributed

The structural differences between centralized and distributed cloud environments significantly influence data governance, latency, and resilience. Centralized cloud networks provide streamlined management and predictable performance but limit user control. Distributed blockchain networks promote autonomy and resilience, albeit with increased complexity and coordination overhead.

Table 3 compares the core architectural attributes of both models.

Table 3. Comparison of Network Architecture: Centralized vs. Blockchain-Based Distributed Systems.

Aspect	Centralized Network	Distributed Blockchain Network
Control	Cloud vendor	Peer-managed
Fault Tolerance	Moderate (via redundancy)	High (no single point of failure)
Latency	Low	Medium to High (varies by consensus)

5.4. SWOT Analysis

To offer a holistic comparison, Table 4 presents a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis of centralized and blockchain-enhanced cloud infrastructures. This analysis helps highlight strategic opportunities and potential risks when adopting blockchain in cloud services.

Table 4. SWOT Analysis: Centralized vs. Blockchain-Enhanced Cloud Systems.

Category	Centralized Cloud	Blockchain-Enhanced Cloud
Strengths	Performance, ease of integration	Security, transparency, auditability
Weaknesses	Vendor lock-in, lower traceability	High cost, integration difficulty
Opportunities	AI integration, hybrid cloud	Smart contracts, DApps, IoT synergy
Threats	Security breaches, legal compliance	Regulatory uncertainty, 51% attacks

6. Future Directions and Open Research Issues

While blockchain technology has demonstrated its potential in enhancing cloud computing, several technical and theoretical challenges remain unresolved. This section outlines the current research gaps and highlights promising directions for future exploration. Addressing these issues will be critical for realizing the full potential of blockchain-enhanced cloud environments.

6.1. Toward More Efficient Consensus Mechanisms

The conventional consensus protocols used in blockchain, such as Proof of Work (PoW), are energy-intensive and suffer from scalability issues. To support large-scale cloud services, there is an urgent need to adopt and improve more efficient consensus algorithms. Proof of Stake (PoS), Byzantine Fault Tolerance (BFT), and Directed Acyclic Graphs (DAG)-based models are being explored as scalable alternatives.

However, each model comes with trade-offs. For instance, PoS reduces energy consumption but may raise fairness and security concerns; DAG enables high transaction throughput but complicates ordering and finality. Future research should focus on hybrid or adaptive consensus frameworks that dynamically balance efficiency, security, and decentralization depending on application scenarios.

6.2. Integration with Artificial Intelligence and Big Data

The convergence of blockchain, artificial intelligence (AI), and big data analytics presents a fertile ground for innovation. Cloud platforms already rely on data-driven insights for optimization, and blockchain can add verifiability and transparency to these processes. Smart contracts can automate AI model governance, and blockchain can ensure data provenance and integrity for training datasets.

Future studies may explore blockchain-based federated learning systems, decentralized AI marketplaces, or edge computing scenarios where AI models and data are distributed across the blockchain-enabled cloud edge.

6.3. Emerging Privacy-Preserving Technologies

With growing concerns over data privacy, especially in regulated sectors like healthcare and finance, privacy-preserving computation has become a top priority. Advanced cryptographic techniques such as homomorphic encryption, multi-party computation (MPC), and zero-knowledge proofs (ZKP) offer new ways to perform computations on encrypted data without revealing its contents.

However, these technologies are still resource-intensive and difficult to scale. Future research needs to address the performance bottlenecks, usability issues, and real-world deployment of these techniques in blockchain-enabled cloud environments.

6.4. Standardization and Cross-Platform Interoperability

Lack of interoperability remains a major obstacle to the adoption of blockchain in cloud ecosystems. Most blockchain platforms operate in isolated silos with incompatible protocols, limiting data and asset transfer across systems. Standardized APIs, shared protocols, and cross-chain communication layers are required to enable seamless interaction between heterogeneous cloud and blockchain environments.

Efforts such as Polkadot, Cosmos, and Interledger Protocol (ILP) represent early steps in this direction, but industry-wide consensus on open standards is still lacking. Future work should aim to establish reference models and compliance frameworks that support integration across vendors and regulatory jurisdictions.

7. Conclusion

Blockchain technology has the potential to revolutionize the landscape of cloud computing by introducing a decentralized, secure, and transparent framework for data management and service delivery. Its ability to eliminate single points of failure, enhance data traceability, and enable tamper-proof record-keeping addresses some of the most persistent challenges faced by traditional centralized cloud architectures — especially regarding data security, trust, and privacy.

However, despite its promising features, the integration of blockchain into cloud computing environments remains fraught with significant challenges. Technical barriers such as low throughput, high energy consumption, and scalability limitations hinder real-time performance and cost efficiency. Additionally, regulatory uncertainties, data sovereignty concerns, and the lack of standardization further complicate widespread adoption.

To effectively leverage blockchain in cloud services, cloud providers must invest in research and pilot programs that explore scalable consensus mechanisms, hybrid cloud-blockchain architectures, and privacy-preserving protocols. Developers should prioritize interoperability and user-centric design while ensuring regulatory compliance. Researchers must continue to investigate new models of decentralized governance, cryptographic innovation, and cross-chain collaboration.

In conclusion, blockchain is not a silver bullet, but rather a powerful enabler when thoughtfully applied. Its integration with cloud computing demands careful planning, ongoing evaluation, and collaborative innovation across disciplines. By addressing its current limitations and aligning with industry needs, blockchain can help shape the future of cloud computing into a more resilient, equitable, and secure digital ecosystem.

References

1. S. Akter, K. Michael, M. R. Uddin, G. McCarthy, and M. Rahman, "Transforming business using digital innovations: The Application of AI, Blockchain, Cloud and Data Analytics," *Ann. Oper. Res.*, vol. 308, no. 1–2, pp. 7–39, 2022, doi: 10.1007/s10479-020-03620-w.
2. A. Aleem and C. R. Sprott, "Let me in the cloud: Analysis of the benefit and risk assessment of cloud platform," *J. Financ. Crime*, vol. 20, no. 1, pp. 6–24, 2013, doi: 10.1108/13590791311287337.
3. D. Appelbaum, "Consensus Mechanisms and Related Issues," in *The Emerald Handbook of Blockchain for Business*, H. K. Baker, E. Nikbakht, and S. S. Smith, Eds. Emerald Publishing, 2021, pp. 99–120, doi: 10.1108/978-1-83982-198-120211010.
4. T. Clohessy and T. Acton, "Investigating the influence of organizational factors on blockchain adoption: An innovation theory perspective," *Ind. Manag. Data Syst.*, vol. 119, no. 7, pp. 1457–1491, 2019, doi: 10.1108/IMDS-08-2018-0365.
5. A. Dubovitskaya, "Blockchain Applications in Healthcare," in *The Emerald Handbook of Blockchain for Business*, H. K. Baker, E. Nikbakht, and S. S. Smith, Eds. Emerald Publishing, 2021, pp. 293–309, doi: 10.1108/978-1-83982-198-120211023.
6. A.-I. Florea, I. Anghel, and T. Cioara, "A Review of Blockchain Technology Applications in Ambient Assisted Living," *Future Internet*, vol. 14, no. 5, p. 150, 2022, doi: 10.3390/fi14050150.
7. D. Fu, S. Hu, L. Zhang, S. He, and J. Qiu, "An intelligent cloud computing of trunk logistics alliance based on blockchain and big data," *J. Supercomput.*, vol. 77, no. 12, pp. 13863–13878, 2021, doi: 10.1007/s11227-021-03800-w.
8. A. Jede and F. Teuteberg, "Investigating preconditions for a financially advantageous cloud usage," *Int. J. Account. Inf. Manag.*, vol. 24, no. 2, pp. 116–134, 2016, doi: 10.1108/IJAIM-04-2015-0018.
9. P. H. W. Jiang and W. Y. C. Wang, "Cloud ERP implementation: The lessons from the practitioners," 19, n.d.
10. J. H. Jo, S. Rathore, V. Loia, and J. H. Park, "A blockchain-based trusted security zone architecture," *Electron. Libr.*, vol. 37, no. 5, pp. 796–810, 2019, doi: 10.1108/EL-02-2019-0053.
11. A. Jyoti and R. K. Chauhan, "A blockchain and smart contract-based data provenance collection and storing in cloud environment," *Wirel. Netw.*, vol. 28, no. 4, pp. 1541–1562, 2022, doi: 10.1007/s11276-022-02924-y.
12. L. I. Khoruzhy et al., "A new trust management framework based on the experience of users in industrial cloud computing using multi-criteria decision making," *Kybernetes*, vol. 51, no. 6, pp. 1949–1966, 2022, doi: 10.1108/K-05-2021-0378.
13. P. Lal and S. S. Bharadwaj, "Understanding the impact of cloud-based services adoption on organizational flexibility: An exploratory study," *J. Enterp. Inf. Manag.*, vol. 29, no. 4, pp. 566–588, 2016, doi: 10.1108/JEIM-04-2015-0028.
14. C. Li, S. Liang, J. Zhang, Q. Wang, and Y. Luo, "Blockchain-based Data Trading in Edge-cloud Computing Environment," *Inf. Process. Manag.*, vol. 59, no. 1, p. 102786, 2022, doi: 10.1016/j.ipm.2021.102786.
15. P. M. Madhani, "Supply Chain Transformation with Blockchain Deployment: Enhancing Efficiency and Effectiveness," vol. 18, no. 4, p. 27, 2021.
16. R. Nair, S. N. Zafrullah, P. Vinayasree, P. Singh, M. M. A. Zahra, T. Sharma, and F. Ahmadi, "Blockchain-Based Decentralized Cloud Solutions for Data Transfer," *Comput. Intell. Neurosci.*, 2022, pp. 1–12, doi: 10.1155/2022/8209854.
17. S. P. and M. Venkatesan, "Scalability improvement and analysis of permissioned-blockchain," *ICT Express*, vol. 7, no. 3, pp. 283–289, 2021, doi: 10.1016/j.icte.2021.08.015.
18. J. Park and J. Park, "Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions," *Symmetry*, vol. 9, no. 8, p. 164, 2017, doi: 10.3390/sym9080164.
19. M. R. Patruni and P. Saraswathi, "Securing Internet of Things devices by enabling Ethereum blockchain using smart contracts," *Build. Serv. Eng. Res. Technol.*, vol. 43, no. 4, pp. 473–484, 2022, doi: 10.1177/01436244221078933.
20. P. Priyanka, B. Keswani, and R. Hussain, "Assimilation of blockchain over cloud computing," *J. Discret. Math. Sci. Cryptogr.*, vol. 24, no. 8, pp. 2267–2277, 2021, doi: 10.1080/09720529.2021.2009194.
21. R. Qiao, S. Zhu, Q. Wang, and J. Qin, "Optimization of dynamic data traceability mechanism in Internet of Things based on consortium blockchain," *Int. J. Distrib. Sens. Netw.*, vol. 14, no. 12, 2018, doi: 10.1177/1550147718819072.
22. K. Saurabh, N. Rani, and P. Upadhyay, "Towards blockchain led decentralized autonomous organization (DAO) business model innovations," *Benchmarking*, 2022, doi: 10.1108/BIJ-10-2021-0606.

23. P. K. Senyo, J. Effah, and E. Addae, "Preliminary insight into cloud computing adoption in a developing country," *J. Enterp. Inf. Manag.*, vol. 29, no. 4, pp. 505–524, 2016, doi: 10.1108/JEIM-09-2014-0094.
24. G. Tang and H. Zeng, "Collaborative management and control of blockchain in cloud computing environment," *J. Intell. Fuzzy Syst.*, vol. 40, no. 4, pp. 5963–5973, 2021, doi: 10.3233/JIFS-189436.
25. Y. P. Tsang, C. H. Wu, W. H. Ip, and W.-L. Shiau, "Exploring the intellectual cores of the blockchain–Internet of Things (BIoT)," *J. Enterp. Inf. Manag.*, vol. 34, no. 5, pp. 1287–1317, 2021, doi: 10.1108/JEIM-10-2020-0395.
26. P. Wang, "A study on the intellectual capital management over cloud computing using analytic hierarchy process and partial least squares," *Kybernetes*, vol. 51, no. 6, pp. 2089–2108, 2022, doi: 10.1108/K-03-2021-0241.
27. J. Wu and J. Yu, "Blockchain's impact on platform supply chains: Transaction cost and information transparency perspectives," *Int. J. Prod. Res.*, pp. 1–14, 2022, doi: 10.1080/00207543.2022.2027037.
28. C. Yu, L. Zhang, W. Zhao, and S. Zhang, "A blockchain-based service composition architecture in cloud manufacturing," *Int. J. Comput. Integr. Manuf.*, vol. 33, no. 7, pp. 701–715, 2020, doi: 10.1080/0951192X.2019.1571234.

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