Blockchain Integration in Modern Cloud Computing: A Comprehensive Survey of Security and Efficiency

Waqas Ahmed

Premier Journal of Data Science

Premier Science

Air University Islamabad, Islamabad, Pakistan

Correspondence to: Waqas Ahmed, waqaskhattak99@gmail.com

Additional material is published online only. To view please visit the journal online.

Cite this as: Ahmed W. Blockchain Integration in Modern Cloud Computing: A Comprehensive Survey of Security and Efficiency. Premier Journal of Data Science 2025;2:100003

DOI: https://doi.org/10.70389/PJDS.100003

Received: 1 January 2025
Revised: 17 January 2025
Accepted: 18 January 2025
Published: 27 January 2025

Ethical approval: N/a
Consent: N/a
Funding: No industry funding
Conflicts of interest: N/a
Author contribution: Waqas Ahmed – Conceptualization, Writing – original draft, review and editing
Guarantor: Waqas Ahmed
Provenance and peer-review: Commissioned and externally peer-reviewed
Data availability statement: N/a

ABSTRACT

Blockchain technology integration into cloud computing has evolved into a transformative methodology to solve problems such as security, transparency, data integrity, operational efficiency, and trust. This review explores how blockchain meets key use cases for healthcare data management, financial services, supply chain optimization, and e-governance. We critically analyze challenges to scalability limitations, interoperability with legacy systems, regulatory hurdles, and cost barriers alongside emerging solutions such as sharding, Layer 2 protocols, and standardized application programming interfaces (APIs). The findings highlight that blockchain can transform cloud systems while underscoring the importance of cooperative action in researching, developing, and shaping policy to overcome existing barriers.

Keywords: Blockchain integration, Cloud computing security, Decentralized ledger technology, Interoperability challenges, Smart contracts

Introduction

Cloud computing and blockchain are game-changers in the modern IT world. In cloud computing, service delivery is based on central servers that provide Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) to businesses for scaling dynamically and decreasing their on-premises infrastructure costs. Thanks to this scalability and efficiency, platforms such as Amazon Web Services (AWS) and Microsoft Azure serve as prime examples in this field. Despite having strong security frameworks, cloud systems are not immune to attacks such as Distributed Denial of Service attacks and unauthorized access due to their decentralized nature.[1]

In contrast, blockchain is based on decentralized ledger technology (DLT) to ensure data and security through cryptographic methods, making data transparent and resistant to tampering. Consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS) are used in blockchain to verify transaction spread on distributed networks. Blockchain was originally built for cryptocurrencies but has since spread through healthcare, finance, supply chain, and more into government systems. For example, IBM's Food Trust enables more traceability and fraud prevention in supply chains using blockchain.[2]

This paper explores literature, case studies, and technical insights regarding blockchain's decentralized architecture's ability to address cloud computing security and efficiency challenges. It also perceives synergies and future possibilities for blockchain's use in the cloud computing area.

Problem Statement

Although adopted, cloud computing has not addressed modern security and efficiency needs. Such storage architecture becomes a single point of failure for the system and most often leads to cyberattacks. Cloud systems are usually the target for 2022. The report says global cybercrime damages could reach $10.5 trillion a year by 2025. Risks such as data leakage and cross-tenant attacks are multiplied in multitenant environments, and 81% of data breaches are due to misconfigured cloud storage, according to Gartner's 2023 report.[3] Latency is also an additional operational issue that hinders the performance of critical applications. For more advanced threats, traditional, reactive security measures fall short, and proactive solutions are necessary. Figure 1 highlights the key differences and synergies between cloud computing and blockchain technologies.

Research Aim and Objectives

The purpose of this study is to explore the integration of blockchain technology into cloud computing systems to enhance security and operational efficiency. The specific objectives are:

i. to explore the integration of blockchain technology in modern cloud computing;
ii. to identify and evaluate the security challenges in cloud computing and how blockchain addresses them;
iii. to assess the impact of blockchain on the efficiency of cloud computing services; and
iv. to review real-world implementations and use cases of blockchain in cloud computing.

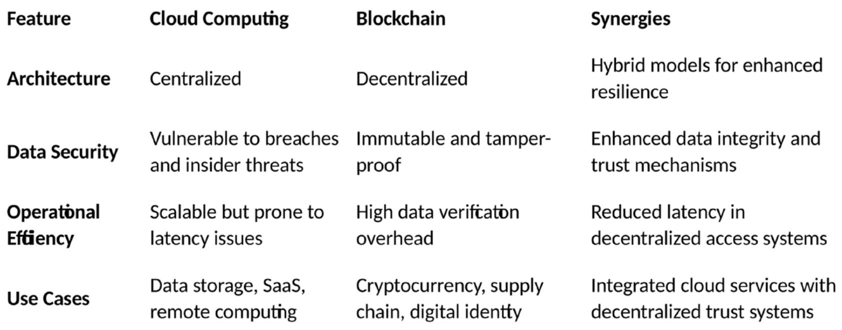
Methodological Framework

Literature and Case Study Selection Criteria

To provide a thorough review, this study employed a structured method to select literature and case studies. The selection process involved the following steps:

Inclusion Criteria:

i. Peer-reviewed journal articles (from 2018 to 2023), conference proceedings, and reputable industry reports.
ii. Research on the integration of blockchain in cloudy computing together with security and efficiency aspects.
iii. Real-world implementations and use cases for the practical use of blockchain in the cloud computing environment.



Feature	Cloud Computing	Blockchain	Synergies
Architecture	Centralized	Decentralized	Hybrid models for enhanced resilience
Data Security	Vulnerable to breaches and insider threats	Immutable and tamper-proof	Enhanced data integrity and trust mechanisms
Operational Efficiency	Scalable but prone to latency issues	High data verification overhead	Reduced latency in decentralized access systems
Use Cases	Data storage, SaaS, remote computing	Cryptocurrency, supply chain, digital identity	Integrated cloud services with decentralized trust systems

Fig 1 | Key differences and synergies between cloud computing and blockchain technologies

Exclusion Criteria:

i. Articles without evidence from empirical data or with a case study validation.
ii. The studies that investigate blockchain or cloud computing in isolation without addressing their integration.
iii. Research outside of the newer research published after 2018 other than the foundational to the topic.

Data Sources and Analysis

Data from databases such as IEEE Xplore, ACM Digital Library, SpringerLink, and industry publications from institutions such as Gartner and Deloitte were leveraged. Findings were categorized into four key areas: security enhancements, efficiency improvements, and challenges through a thematic analysis approach. We picked case studies that are relevant to today's trends and innovations, such as hybrid architectures and AI-driven optimizations, providing a comprehensive understanding of the subject.

Cloud Computing and Blockchain: Fundamentals

Overview of Cloud Computing

IT services have become cloud-based and provide on-demand internet access to shared resources, allowing cost savings, scalability, flexibility, and performance.[4] Defined by NIST as access to configurable resources that can be quickly provisioned, cloud computing operates through three models:

IaaS: Provides virtualized resources, which build IT environments.

PaaS: Provides a managed platform for the ease of application development.[5]

SaaS: Makes online delivery of software, with no local maintenance required.[6]

It includes public cloud (shared resources with related security concerns), private cloud (dedicated control and security), hybrid cloud (blend of public and private benefits), and community cloud (shared for special efforts).[5]

Overview of Blockchain Technology

Blockchain offers a decentralized, secure alternative to traditional data management. As a distributed ledger, it validates and records transactions without intermediaries relying on cryptographic algorithms and consensus mechanisms. Its core principles are:

- **Decentralization:** Eliminates central points of failure.[7]
- **Immutability:** Ensures recorded data cannot be altered.
- **Transparency:** Enables transaction verification and trust.[8]

Blockchain types include:

- **Public:** Open to all, using PoW or PoS (e.g., Bitcoin, Ethereum).[9]
- **Private:** Restricted for confidentiality (e.g., Hyperledger Fabric).
- **Consortium:** Collaborative, balancing transparency and privacy for industries such as finance and supply chain.[10]

Comparative Analysis

Cloud computing and the philosophies of the blockchain are fundamentally different. We describe cloud computing as a centralized approach that not only is flexible and scalable in its resource management but also suffers single points of failure and is more vulnerable to cyberattacks.[11] However, blockchain distributes the data storage and the management of data across the network of nodes, which leads to resilience, 24-hour availability, and better integrity of data without the need for third parties.[9]

Traditionally, security in cloud computing has been reactive—though encryption, identity access management, firewalls, and the like are simple in conception, they are not simple to build, require complex deployment, consume significant engineering resources, and often prove ineffective at defending against advanced attack vectors.[5] However, blockchain provides proactive security through cryptographic hashing, and the consensus protocol of the data is tamper-proof. Furthermore, smart contracts that are deployed on blockchain not only automate compliance but also enforce prebuilt rules, lowering administrative errors and extra costs.[12]

In high throughput, centralized applications, cloud computing excels but leaves transparency and trust wanting. While slower, blockchain's decentralized framework has transparency and auditability, which are perfect for applications where there is trust and integrity in data, such as financial services (Figure 2). Cloud computing lacks the data privacy and control it needs, whereas blockchain finds itself struggling with its scalability and energy efficiency.[13] Securing cloud systems, in turn, may also be accomplished through the integration of both technologies, while blockchain's scalability issues can be solved through integration.

Security Challenges in Cloud Computing

Data Privacy and Protection

Data privacy is still an important issue in cloud computing, with sensitive data being transferred to a cloud, thereby increasing the probability of data breaches and unauthorized access. Many of these breaches are from weak encryption protocols, misconfigured systems, and a lack of access controls. A good example

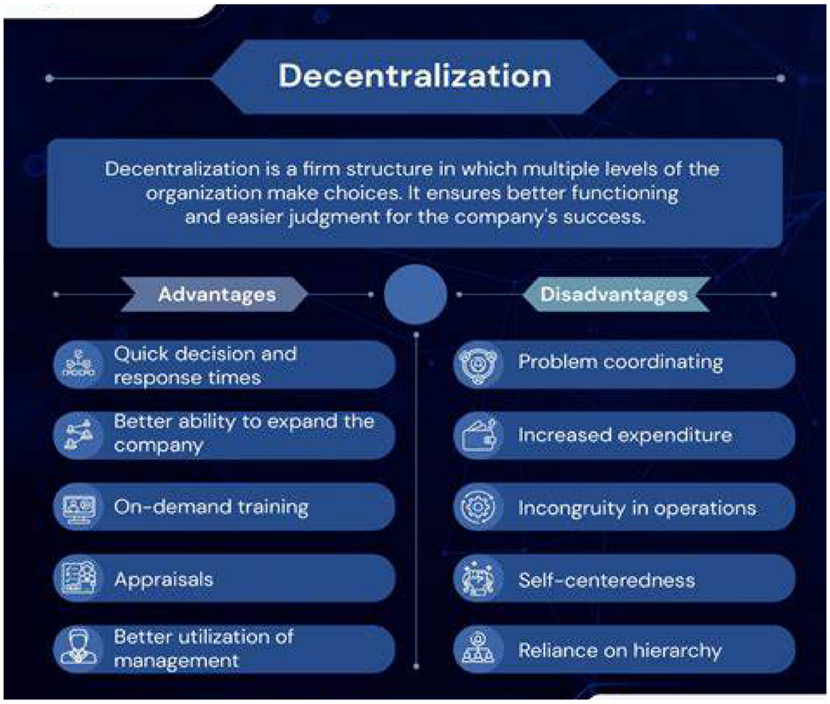

Decentralization
Decentralization is a firm structure in which multiple levels of the organization make choices. It ensures better functioning and easier judgment for the company's success.
Advantages
Disadvantages
Quick decision and response times
Better ability to expand the company
On-demand training
Appraisals
Better utilization of management
Problem coordinating
Increased expenditure
Incongruity in operations
Self-centeredness
Reliance on hierarchy

Fig 2 | Centralized versus decentralized blockchain attributes

Source: Abrol[13]

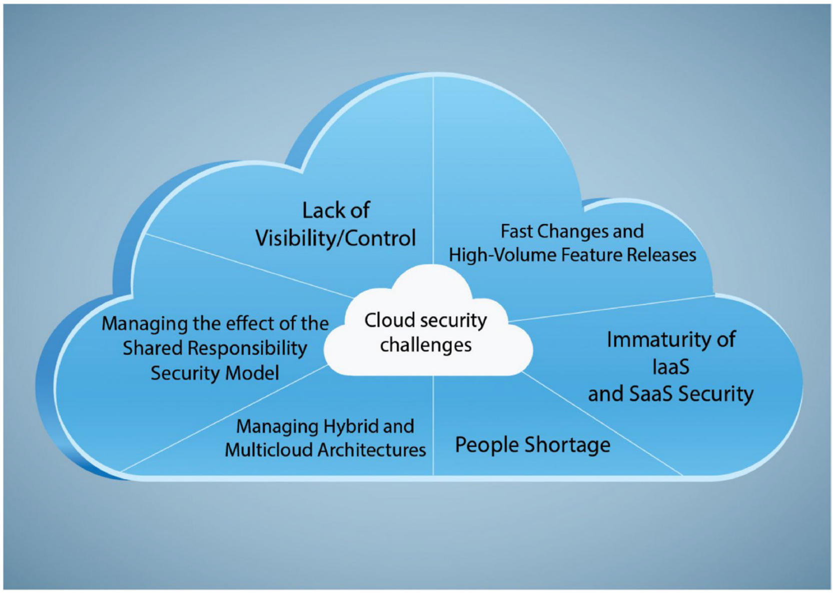

Cloud security challenges
Lack of Visibility/Control
Fast Changes and High-Volume Feature Releases
Managing the effect of the Shared Responsibility Security Model
Immaturity of IaaS and SaaS Security
Managing Hybrid and Multicloud Architectures
People Shortage

Fig 3 | Data security in cloud computing

Source: www.suntechnologies.com

is the 2021 misconfiguration in Microsoft Power Apps, which exposed millions of sensitive records and illustrated the vulnerabilities of a cloud system (Figure 3). The growing sophistication of attackers, coupled with their high economic impact, will propel cybersecurity costs to $10.5 trillion annually by 2025, according to Cybersecurity Ventures.[14]

Cloud security is built on encryption, but it is often being flouted by obsolete algorithms—and lacking end-to-end encryption. Then, there is the regulatory complexity driven by the General Data Protection Regulation (GDPR) in Europe or the CCPA in the United States, which often means that when data is stored in the cloud, it crosses jurisdictions. These regulations create a challenge for organizations to navigate through them and incur compliance and security risks to systems.[15]

Unauthorized Access and Insider Threats

For cloud security, unauthorized access, especially through insider threats, presents a special challenge. Such threats are hard to detect because insiders abuse legitimate credentials to breach data. According to a 2022 IBM Security study, insider threats are responsible for 20% of data breaches, and for 20% of data breaches, the cost of an incident averages out to be $4.6 million. Old-school defenses, such as role-based access control (RBAC) and activity logging, fail when attacked by sophisticated attacks as they are based on predefined rules that are exploited by systems insiders who have gained knowledge of the system.[16]

Decentralized identity management and immutable audit trails are employed for blockchain and the innovations that these bring to offer. Decentralized identifiers (DIDs) provide secure, verifiable digital identities that reduce ways of being exploited, such as identity theft.[2] The immutable ledger of blockchain guarantees that all access activities are always recorded, making it accountable and traceable. A 2021 financial services case study shows that blockchain-based access control systems reduced insider threats by 30% as a result of improved transparency.[1]

Vulnerabilities in Multitenant Environments

As cloud computing is a multitenant phenomenon, it witnesses unique vulnerabilities, such as cross-tenant data leakage and unauthorized access. Misconfigurations, hypervisor flaws, and insecure APIs all too often act as a first tier of attack, making these risks even more pronounced. This kind of unacceptable rate, highlighted in Gartner's 2022 report, which states that misconfigurations are the cause of 80% of cloud-related security incidents, proves that it should be taken more seriously.[15]

In the context of multitenant environments, data isolation is achieved using virtualization, but unwanted side-channel attacks (e.g., Meltdown and Spectre) expose their limits. Blockchain technology solves these vulnerabilities by removing shared points of failure for data storage and control.[17] Sharding and zero-knowledge proofs accelerate ways to isolate data and growth, while smart contracts automatize enforcement of tenant-specific policies that eliminate the likelihood of human error.

Existing Security Mechanisms and Their Limitations

Now, the current cloud security measures such as firewalls, multifactor authentication (MFA), and intrusion detection systems (IDS) offer a baseline solution that acts on a very reactive and silo basis. First, sophisticated attackers can skip past static rule sets that firewalls require, and second, IDS is full of high false-positive rates that consume the security teams. MFA is great at increasing authentication, but even MFA-protected accounts have been compromised by advanced phishing and SIM-swapping attacks. Prolonging the presence of centralized identity providers only increases vulnerability to attackers looking at them.[18]

Security is decentralized, and blockchain does away with intermediaries. On blockchain-based identity verification, cryptographic signatures in the blockchain make it impossible for user credentials to be forged or misused. Furthermore, if the blockchain is considered decentralized, it is more resilient against DDoS attacks, a typical threat in centralized cloud systems. However, the adoption of blockchain will be hindered by the challenges of high latency and energy consumption.[6]

Blockchain Integration in Cloud Computing

Architectural Models

Blockchain integration into cloud computing necessitates moving away from centralized worldviews toward a hybrid model utilizing the traits from both blocks and clouds (Figure 4). On the other hand, the cloud offers its scalable and flexible storage system, and blockchain offers transparency and immutability on the decentralized ledger. Such cut-downs have been made by hybrid architectures that combine on-chain and off-chain storage. In such models, off-chain, cloud systems store the frequently accessed or sensitive data, and the blockchain is responsible for metadata, transaction logs, and data integrity verification.[19] Platforms such as Filecoin and IPFS exemplify this approach by using blockchain to manage data ownership while relying on distributed cloud environments for storage.[20]

However, such architectural integration brings with it challenges, including data synchronization, consensus management, and network compatibility. However, frameworks for these are promising. A 2022 study showed that to enhance data security of multitenant environments, integrity validation can be achieved through Merkle trees, and access control can be made automated using smart contracts, and thereby a drastic reduction in unauthorized access attempts has been demonstrated.[21]

Security Enhancements

Among these are multiple cryptographic techniques of the blockchain, such as hashing and digital signatures—methods that are robust mechanisms not only for ensuring data authenticity but also for their confidentiality. Data is hashed to uniquely fingerprint it, providing everyone the consent to change it, and the auditability if it has been changed, so that digital signatures secure transactions. However, these features are crucial to securing cloud data, which is considered highly sensitive to cyberattacks.[8]

Security is also further enhanced with smart contracts that automate compliance with predefined policies and procedures. These are self-executable scripts that enforce access controls and data-sharing agreements without human intervention. In 2023, we witnessed a healthcare

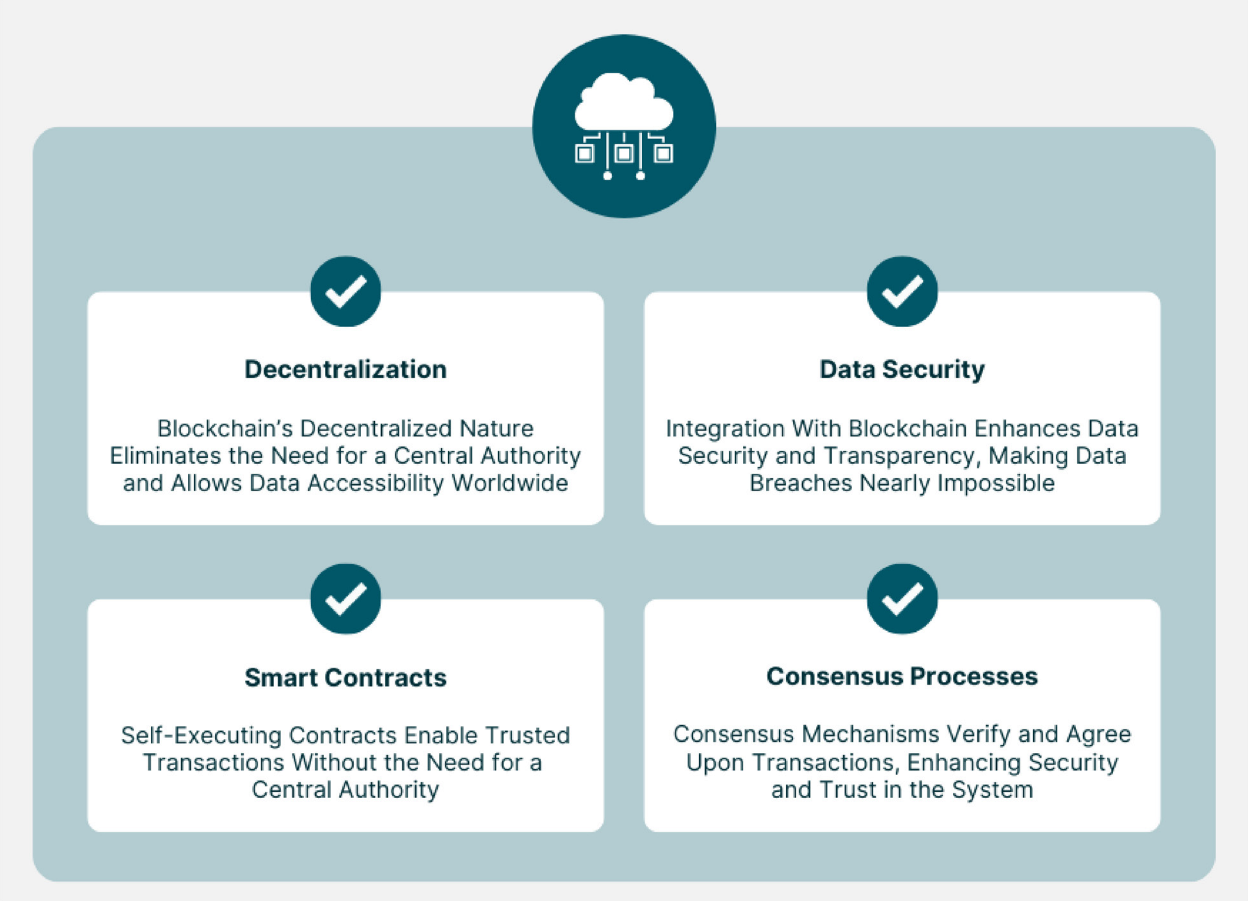

Decentralization
Blockchain's Decentralized Nature Eliminates the Need for a Central Authority and Allows Data Accessibility Worldwide
Data Security
Integration With Blockchain Enhances Data Security and Transparency, Making Data Breaches Nearly Impossible
Smart Contracts
Self-Executing Contracts Enable Trusted Transactions Without the Need for a Central Authority
Consensus Processes
Consensus Mechanisms Verify and Agree Upon Transactions, Enhancing Security and Trust in the System

Fig 4 | Blockchain-cloud integration framework

Source: Tamplin[22]

cloud platform that was powered by blockchain-based access control reduce data breaches down by 40%. The system's ability to automatically validate permissions against immutable blockchain-stored rules eliminated human error and insider threats, leading to this success.[9]

Efficiency Improvements

Most importantly, blockchain integration further enhances the operation efficiency of cloud systems by addressing the common latency problem in traditional systems. In blockchain networks, data access is decentralized, which means that centralized intermediaries are no longer needed, and retrieval and processing times in geographically distributed systems are drastically reduced.[23]

Modern consensus mechanisms such as Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) are used prevalently, as they optimize further blockchain-enabled cloud systems. These models are more energy efficient than, say, Proof of Work (PoW), while more scalable and with higher throughput of transactions.[24]

In 2023, a study by IBM showed that hybrid blockchain-cloud performance in supply chain management could improve a company's operation by a full 25% (Figure 5). Through the increased retrieval and automated execution of data and contracts, respectively, the blockchain capability to enhance the efficiency of cloud hosting is demonstrated.[25]

Use Cases and Real-World Applications

Blockchain in Healthcare Cloud Systems

In MIT's MedRec project, blockchain offers a method that is decentralized and gives patients power over their electronic health records (EHRs) while still allowing healthcare providers to access up-to-date information. Researchers found in 2023 that 35% fewer data retrieval errors and 20% more patient satisfaction resulted when blockchain was used.[27] Furthermore, it is HIPAA compliant, with transparent, auditable access trails and cloud computing for secure, real-time data storage (Figure 6).

Blockchain in Financial Cloud Services

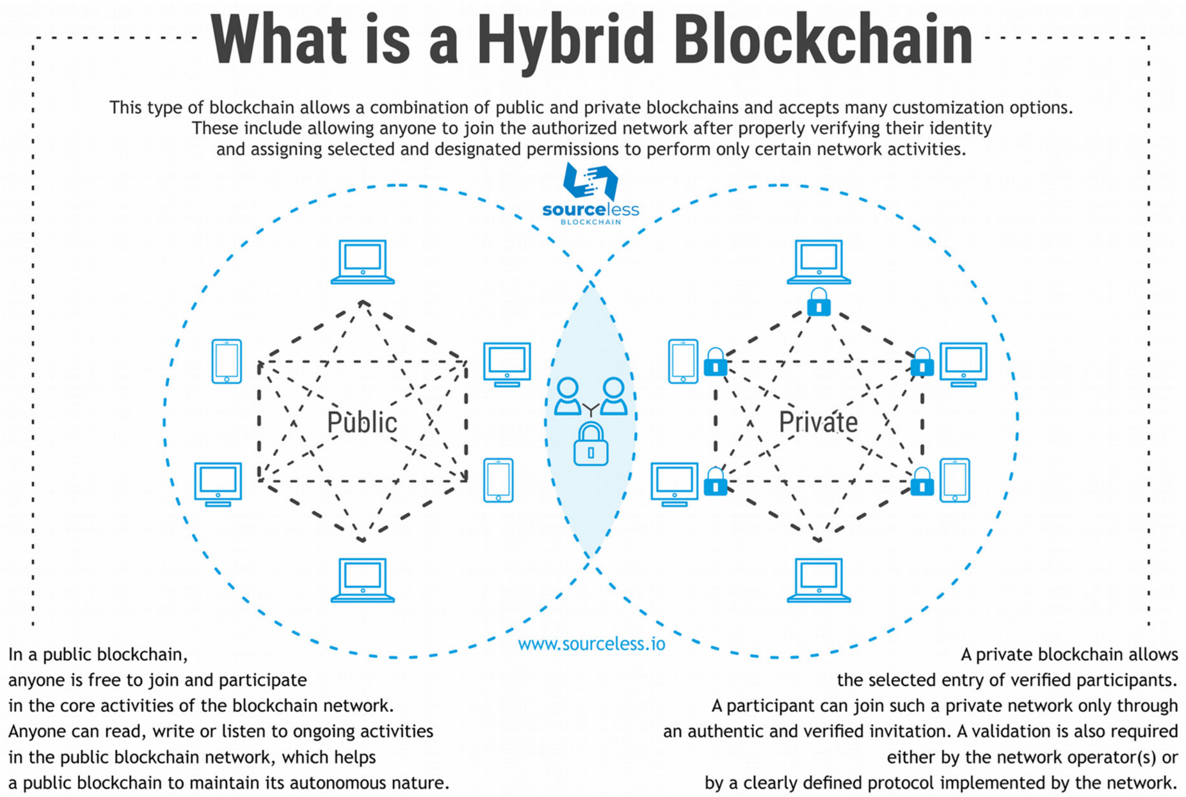
Integration blockchain into the financial sector enhances transaction security, prevents fraud, and improves operational efficiency. Services are optimized through the integration of J.P. Morgan Quorum with cloud infrastructure, decreasing transaction processing time by 40% and costs by 25%. Smart contracts also solve compliance problems and reduce the risk of disputes.[29]

Blockchain for Supply Chain Management

Blockchain is evolving to help address food supply challenges—from traceability, to keeping food fresh, to combating fraud—with IBM's Food Trust platform. It is a cloud storage solution that allows real-time access to large volumes of data. Blockchain means automating transactions where payments should follow successful delivery only, eliminating delays and disputes.[20]

Blockchain-Driven Government Cloud Solutions

With blockchain and cloud computing, governments are using blockchain to increase governance, digital



This type of blockchain allows a combination of public and private blockchains and accepts many customization options. These include allowing anyone to join the authorized network after properly verifying their identity and assigning selected and designated permissions to perform only certain network activities.

In a public blockchain, anyone is free to join and participate in the core activities of the blockchain network. Anyone can read, write or listen to ongoing activities in the public blockchain network, which helps a public blockchain to maintain its autonomous nature.

A private blockchain allows the selected entry of verified participants. A participant can join such a private network only through an authentic and verified invitation. A validation is also required either by the network operator(s) or by a clearly defined protocol implemented by the network.

Fig 5 | Hybrid blockchain-cloud architecture

Source: Zhong et al.[26]

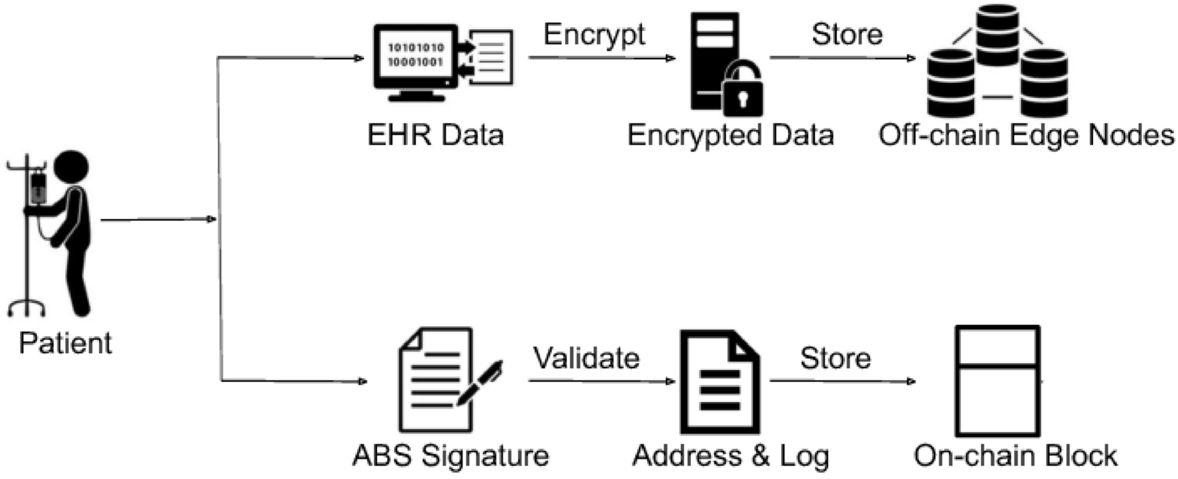


Fig 6 | Hybrid blockchain-cloud; off-chain storage

Source: Guo et al.[28]

identity verification, and electronic voting. The administrative cost of Estonia's e-residency program involving blockchain is 20% lower, and service quality is 30% improved. A pilot "voting on a blockchain" in West Virginia shows its application to electoral integrity.[26]

Challenges and Limitations

Scalability Issues

Transaction throughput presents a scalability challenge for blockchain. The Visa network processes 24,000 TPS, while Ethereum manages less than 15. Scalability is improved by solutions such as sharding and Layer 2 protocols such as the Lightning Network. In a 2023 study, it was shown that the sharding capability improved blockchain capacity for wider adoption by 300%.[28]

Interoperability with Existing Systems

A problem with integrating blockchain with legacy systems is that it is not compatible. To ensure such smooth integration, we need standardized protocols and APIs. According to a 2022 Deloitte study, 60% of the blockchain failures were a result of interoperability issues. Polkadot, Cosmos, and other similar efforts aim to bridge the gaps.[29]

Cost of Integration

Adopting blockchain requires SMEs to incur high upfront costs for infrastructure, software, and training. In a 2023 case study, blockchain integration did mean an initial investment increase of 25%—but operational costs were reduced by 15% over three years, a clear long-term saving.[11]

Regulatory and Compliance Challenges

GDPR is a set of regulations that require data to be erasable. However, blockchain's decentral nature clashes with that. New regulations are needed to harmonize between innovation and compliance. According to a 2023 World Economic Forum report, global blockchain adoption depends on regulatory harmonization.[32]

Recent Advances

Quantum-Resistant Blockchain Protocols

In recent years, cryptographic research has provided quantum-resistant blockchain protocols to address the vulnerabilities of quantum computing to current cryptographic systems. To future-proof their security, blockchain systems are integrating new protocols: lattice-based cryptography, hash-based cryptography, and code-based cryptography. NIST's ongoing Post-Quantum Cryptography Standardization project is providing a path to replacing insecure blockchain implementation with secure blockchain in a quantum world. While currently still under development, the protocols we are looking at show proactive steps being taken to increase blockchain's resilience against future technological challenges.

AI-Driven Optimizations for Blockchain-Cloud Systems

With blockchain-cloud systems, artificial intelligence (AI) has begun playing a major role. Reinforcement learning and federated learning are forcing their way into network bottleneck prediction, consensus algorithm optimization, and energy consumption minimization. For example, when discussing cloud-based blockchain networks, AI-driven predictive analytics can help predict traffic patterns and, hence, assist with dynamic resource allocation to maximize efficiency. Moreover, the usage of AI for detecting anomalies in blockchain-based security systems would help in giving warnings of possible cyberattacks at an early stage.

A 2023 case study for blockchain-powered cloud AI services turned out to be successful at integrating AI in the blockchain-powered cloud services by 30% efficiency of operations and 20% reduction in downtime.

Comparative Analysis

Case Studies of Blockchain-Integrated Cloud Systems

Amazon Managed Blockchain helps businesses build scalable blockchain networks by supporting Hyperledger Fabric and Ethereum. Forrester Research's 2022 case study on a logistics company using this service reveals that this service reduced tracking errors by 30% and improved supply chain visibility by 20%, suggesting that blockchain may be a way forward in terms of increasing transparency, while also saving money in the process.[33]

A pharmaceutical supply chain integrated with IBM's cloud and IBM Blockchain Platform was used to demonstrate how blockchain can be used to improve compliance and traceability. A 2023 Gartner report showed it reduced audit time by 40% and operational costs by 25%.[34] Unfortunately, a number of these cases demonstrate blockchain's capabilities but also their shortcomings when it comes to adopting blockchain within organizations with legacy systems and working with hybrid architectures.

Comparative Metrics

Metrics with focused areas such as security, efficiency, and cost-effectiveness are needed to evaluate the system's blockchain-integrated cloud systems. According to a 2022 Deloitte study, using blockchain means data breaches are 40% less likely than with more traditional models, as its cryptographic elements, such as hashing and signing digitally guarantee that data is intact.

Another key metric is efficiency. When distributed, IBM's 2023 research showed that blockchain could improve data synchronization and retrieval by 25%. However, technologies such as Proof of Work (PoW) and Proof of Stake (PoS) introduce delays, especially in high-volume systems.[24]

Blockchain also reduces costs. According to a 2023 case study, blockchain systems saved 15% of costs over three years, thanks to reduced dependence on intermediaries and to smart contracts.[34] The main barrier to SMEs is the high cost of investment in infrastructure and training.

Conclusion

Summary of Key Findings

This review underscores the transformative potential of blockchain technology in addressing the security, efficiency, and reliability challenges of cloud computing. Key findings include the feasibility of decentralized architectures that combine blockchain's immutability and transparency with the scalability of cloud systems. Notable advancements, such as hybrid models leveraging on-chain and off-chain storage, demonstrate the practicality of integrating these technologies to achieve enhanced trust mechanisms and operational reliability.

Implications for Cloud Computing and Blockchain Development

From finance and supply chain management to healthcare, the integration of blockchain and cloud computing has huge potential. This synergy can be used to foster innovation and resilience and bring about major advances in the IT ecosystem. Regulatory challenges that need to be addressed by policymakers and technology providers include compliance with data privacy law and interoperability with legacy systems. The standardization of protocols and governance frameworks to support widespread adoption is an area where collaborative efforts between industry stakeholders, academic researchers, and regulatory bodies are crucial.

Final Thoughts on the Future of Blockchain in Cloud Computing

Given blockchain's continued growth as a technology and its potential for integration with cloud computing, there is an opportunity to create secure, efficient, and open systems. Emerging solutions such as Layer 2 protocols and sharding aim to address the inherent scalability challenges of crypto networks. However, significant research and development are still required to overcome technical limits and fully realize the full potential of blockchain technology. In the future, decentralization will significantly influence cloud computing. Achieving this requires blockchain to balance decentralization and performance effectively, enabling it to deliver innovative solutions that redefine traditional IT infrastructures.

References

1 Sviatun OV, Goncharuk OV, Roman C, Kuzmenko O, Kozych IV. Combating cybercrime: Economic and legal aspects. WSEAS Trans Busin Econ. 2021;18:751–62. https://doi.org/10.37394/23207.2021.18.72

2 Rybalchenko L, Ryzhkov E, Ohrimenco S. Economic crime and its impact on the security of the state. Philoso Econ Law Rev. 2021;2:78–91. https://doi.org/10.31733/2786-491X-2021-2-78-91

3 Belchior R, Vasconcelos A, Guerreiro S, Correia. A survey on blockchain interoperability: Past, present, and future trends. ACM Comput Surv (CSUR). 2021;54(8):1–41. https://doi.org/10.1145/3471140

4 Al-Rakhami M, Al-Mashari M. Interoperability approaches of blockchain technology for supply chain systems. Busin Proc Manage J. 2022;28(5/6):1251–76. https://doi.org/10.1108/BPMJ-04-2022-0207

5 Biswas S, Yao Z, Yan L, Alqhatani A, Bairagi AK, Asiri F, et al. Interoperability benefits and challenges in smart city services: Blockchain as a solution. Electronics. 2023;12(4):1036. https://doi.org/10.3390/electronics12041036

6 Brinkmann M. The realities of blockchain-based new public governance: an explorative analysis of blockchain implementations in Europe. Digi Govern Res Pract. 2021;2(3):1–14. https://doi.org/10.1145/3462332

7 Clavin J, Duan S, Zhang H, Janeja VP, Joshi KP, Yesha Y, et al. Blockchains for government: Use cases and challenges. Digi Govern Res Pract. 2020;1(3):1–21. https://doi.org/10.1145/3427097

8 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. Futu Intern. 2022;14(11):341. https://doi.org/10.3390/fi14110341

9 Bhatt P, Singh S, Sharma SK, Kumar V. Blockchain technology applications for improving the quality of electronic healthcare systems. In Blockchain for Healthcare Systems 2021;(pp. 97–113). CRC Press. https://doi.org/10.1201/9781003141471

10 Rayan RA, Zafar I, Tsagkari C. Blockchain technology for healthcare cloud-based data privacy and security. In Integration of WSNs into Internet of Things. 2021;(pp. 335–49). CRC Press. https://doi.org/10.1201/9781003107521

11 Adere EM. Blockchain in healthcare and IoT: A systematic literature review. Array. 2022;14:100139. https://doi.org/10.1016/j.array.2022.100139

12 Khan SN, Loukil F, Ghedira-Guegan C, Benkhelifa E, Bani-Hani A. Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-Peer Netw Appl. 2021;14:2901–25. https://doi.org/10.1007/s12083-021-01127-0

13 Abrol A. Decentralization vs. centralization. Blockchain Council. 2024. Available from: https://www.blockchain-council.org/blockchain/decentralized-vs-centralized/

14 Al-Rakhami MS, Al-Mashari M. A blockchain-based trust model for the Internet of Things supply chain management. Sensors. 2021;21(5):1759. https://doi.org/10.3390/s21051759

15 Wang L, Xu L, Zheng Z, Liu S, Li X, Cao L. Smart contract-based agricultural food supply chain traceability. IEEE Access. 2021;9:9296–307. https://doi.org/10.1109/ACCESS.2021.3050112

16 Fugkeaw S. Achieving a decentralized and dynamic SSO-identity access management system for multi-application outsourced in the cloud. IEEE Access. 2023;11:25480–91. https://doi.org/10.1109/ACCESS.2023.3255885

17 Hashim W, Hussein NAHK. Securing cloud computing environments: An analysis of multi-tenancy vulnerabilities and countermeasures. SHIFRA. 2024;8–16. https://doi.org/10.70470/SHIFRA/2024/002

18 Zou J, He D, Zeadally S, Kumar N, Wang H, Choo KR. Integrated blockchain and cloud computing systems: A systematic survey, solutions, and challenges. ACM Comput Surv (CSUR). 2021;54(8):1–36. https://doi.org/10.1145/3456628

19 Murthy ChVNUB, Shri ML, Kadry S, Lim S. Blockchain-based cloud computing: Architecture and research challenges. IEEE Access. 2020;8:205190–205. https://doi.org/10.1109/ACCESS.2020.3036812

20 Grabowska A. Decentralized file storage systems: Studying decentralized file storage systems (e.g., IPFS, Filecoin) for secure, censorship-resistant storage and sharing of digital content. J AI-Assist Scientif Discov. 2022;2(2):1–9. https://scienceacadpress.com/index.php/jaasd/article/view/55

21 Mohan AP, Gladstone A. Merkle tree and blockchain-based cloud data auditing. Int J Cloud Appl Comput (IJCAC). 2020;10(3):54–66. https://doi.org/10.4018/IJCAC.202007010

22 Tamplin T. Blockchain in cloud computing | Overview, how it works, impact. Finance Strategists. 2023. Available from: https://www.financestrategists.com/wealth-management/blockchain/blockchain-in-cloud-computing/#:~:text=Blockchain%20in%20Cloud%20Computing%20is%20a%20fusion%20of,decentralized%20method%20of%20storing%20data%20-and%20conducting%20transactions

23 Albshaier L, Budokhi A, Aljughaiman A. A review of security issues when integrating IoT with cloud computing and blockchain. IEEE Access. 2024;12:109560–95. https://doi.org/10.1109/ACCESS.2024.3435845

24 Pan J, Song Z, Hao W. Development in consensus protocols: From PoW to PoS to DPoS. In 2021 2nd International Conference on Computer Communication and Network Security (CCNS) 2021;(pp. 59–64). Available from: https://ieeexplore.ieee.org/abstract/document/9387918

25 Panwar A, Bhatnagar V, Khari M, Salehi AW, Gupta G. A blockchain framework to secure personal health record (PHR) in IBM cloud-based data lake. Comput Intellig Neurosci. 2022;2022(1):3045107. https://doi.org/10.1155/2022/3045107

26 Zhong B, Pan X, Ding L, Chen Q, Hu X. Blockchain-driven integration technology for the AEC industry. Autom Construct. 2023;150:104791. https://doi.org/10.1016/j.autcon.2023.104791

27 Raju N, Quazi F, Gorrepati N, Kareem SA. Blockchain applications in electronic health records (EHRs). Int J Glob Innovat Solut. (IJGIS), 2024;2024:15. http://dx.doi.org/10.21428/e90189c8.5043b7de

28 Guo H, Li W, Meamari E, Shen CC, Nejad M. Attribute-based multi-signature and encryption for EHR management: A blockchain-based solution. In 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) 2020;(pp. 1–5); IEEE. Available from: https://ieeexplore.ieee.org/abstract/document/9169395/

29 Khan D, Jung LT, Hashmi MA. Systematic literature review of challenges in blockchain scalability. Appl Sci. 2021;11(20):9372. https://doi.org/10.3390/app11209372

30 Shevchenko E, Lunsford R. Blockchain disruption in finance: JPMorgan Chase's success story and the transfer of Quorum to ConsenSys. J Finan Account. 2023;32:1–12. Available from: https://edeconomy.com/wp-content/uploads/2023/08/Blockchain-Disruption-in-Finance-JPMorgan-Chases-Success.pdf.

31 Leese M. AI and interoperability. In Handbook on Public Policy and Artificial Intelligence 2024;(pp. 146–57). Edward Elgar Publishing. https://doi.org/10.4337/9781803922171.00018

32 Haque AB, Islam AN, Hyrynsalmi S, Naqvi B, Smolander K. GDPR compliant blockchains—A systematic literature review. IEEE Access. 2021;9:50593–606. https://doi.org/10.1109/ACCESS.2021.3069877

33 Forrester S, Barbose GL, O'Shaughnessy E, Darghouth NR, Crespo Montañés C. Residential solar-adopter income and demographic trends: November 2022 Update. 2022. Available from: https://escholarship.org/uc/item/7zh2t3xx.

34 Putters J, Hashemi JB, Yavuz A. Demystifying public cloud auditing for IT auditors. In Advanced Digital Auditing 2023;(p. 185). Available from: https://library.oapen.org/bitstream/handle/20.500.12657/59385/1/978-3-031-11089-4.pdf#page=195