
| RESEARCH ARTICLE

Blockchain and Microsoft Azure: A Secure Framework for Decentralized Cloud Data Management

Shekar Rao Lakavath

Independent Researcher, Bonneylake, Washington, USA

Corresponding Author: Shekar Rao Lakavath, **E-mail:** Shekar.lakavath@gmail.com

| ABSTRACT

Centralized cloud architectures, while operationally efficient, concentrate control of enterprise data in a single administrative domain, creating a single point of failure and a persistent trust dependency between data owners and the cloud provider. Blockchain technology offers a complementary model of distributed trust, in which records are validated collectively by a network of participants and rendered immutable through cryptographic hash-linking. This article proposes and analyzes a secure framework for decentralized cloud data management that integrates permissioned blockchain networks with Microsoft Azure's cloud services. The framework separates responsibilities across four layers: an off-chain Azure layer for scalable data storage, identity management, and threat monitoring; an integration layer built on the Azure Blockchain Development Kit and Logic Apps; a consortium blockchain layer in which multiple stakeholders operate validating nodes; and a distributed ledger layer that records immutable transaction hashes and enforces smart-contract logic. Spanning blockchain fundamentals, Blockchain-as-a-Service (BaaS) platforms, and cloud security research, the article compares Azure Blockchain Service against competing BaaS offerings and maps common decentralized data management risks to specific mitigations available within the Azure ecosystem. The analysis suggests that combining Azure's mature identity, storage, and monitoring services with a permissioned blockchain layer can reduce single-point-of-failure risk, strengthen data provenance, and improve auditability across multi-organizational data-sharing arrangements, provided that organizations invest in smart-contract verification, key management discipline, and clear consortium governance agreements. The article concludes with practical recommendations for organizations evaluating a blockchain-on-Azure approach to decentralized data management.

| KEYWORDS

Blockchain, Microsoft Azure, decentralized cloud computing, data management, smart contracts, Blockchain-as-a-Service, distributed ledger technology.

| ARTICLE INFORMATION

ACCEPTED: June 30, 2025

PUBLISHED: August 20, 2025

DOI: <https://doi.org/10.61424/jcsit.v2i2.1072>

1. Introduction

Cloud computing has become the default infrastructure model for organizations seeking scalability, cost efficiency, and rapid deployment of digital services. Yet the very feature that makes cloud computing efficient, namely the centralization of storage, compute, and administrative control within a single provider's infrastructure, also introduces structural risks: a single compromised administrative account, a misconfigured access policy, or a provider-side outage can affect the availability, integrity, or confidentiality of an entire organization's data (Takabi, Joshi, & Ahn, 2010). These risks are compounded in multi-organizational settings, such as supply chains, healthcare

Copyright: © 2025 The Author(s). This open access article is distributed under the terms and conditions of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC- BY-NC-SA) License (<https://creativecommons.org/licenses/by-nc-sa/4.0/>), published by Bluemark Publishers.

data-sharing consortia, or financial clearing networks, where no single participant is willing to fully trust another party's cloud environment to be the sole custodian of shared records.

Blockchain technology, first popularized as the ledger underlying Bitcoin, offers a structurally different trust model. Rather than a single administrator validating and storing transactions, a blockchain distributes this responsibility across a network of participating nodes that must reach consensus before a record is appended to an immutable, cryptographically linked chain (Zheng, Xie, Dai, Chen, & Wang, 2018). This property makes blockchain a natural complement to cloud computing in contexts where multiple, mutually distrustful organizations need to share and verify data without ceding full control to a single party (Dorsala, Sastry, & Chapram, 2021).

Microsoft Azure has responded to this convergence by offering Blockchain-as-a-Service (BaaS) capabilities, including Azure Blockchain Service and the Azure Blockchain Development Kit, that allow organizations to provision permissioned blockchain networks while continuing to rely on Azure's existing identity, storage, and monitoring infrastructure for everything that does not need to live on-chain (Onik & Miraz, 2019). This hybrid approach, sometimes referred to as an on-chain/off-chain architecture, aims to capture the trust and immutability benefits of blockchain while avoiding the cost, latency, and storage inefficiency of placing large volumes of raw data directly on a distributed ledger.

This article examines how such a hybrid blockchain-on-Azure framework can be designed and governed to support secure, decentralized cloud data management. Three questions guide the analysis. First, what structural weaknesses in centralized cloud data management does blockchain integration address? Second, how does Microsoft Azure's Blockchain-as-a-Service offering compare with competing platforms in terms of the specific capabilities relevant to secure decentralized data management? Third, what practical risks and governance requirements must organizations address when combining blockchain and Azure cloud services? The remainder of the article reviews the relevant literature, proposes a four-layer architecture, compares BaaS platforms, maps data management risks to mitigations, and discusses practical implications.

2. Literature Review

2.1 Foundations of Blockchain Technology

Blockchain technology emerged as a mechanism for achieving consensus on the state of a shared ledger without relying on a trusted central authority. Yli-Huomo, Ko, Choi, Park, and Smolander (2016) conducted an early systematic review of blockchain research and found that, at the time, the majority of published work focused on scalability and privacy limitations rather than practical enterprise deployment, foreshadowing the challenges that later BaaS platforms would need to address. Underwood (2016) traced the extension of blockchain concepts beyond cryptocurrency into broader record-keeping applications, while Christidis and Devetsikiotis (2016) demonstrated how blockchains combined with smart contracts could automate multi-party agreements in the Internet of Things domain, a use case structurally similar to multi-organizational cloud data sharing.

Dinh, Liu, Zhang, Chen, Ooi, and Wang (2018) provided a systems-oriented analysis of blockchain platforms from a data-processing perspective, arguing that blockchains should be evaluated using the same performance criteria applied to conventional distributed databases, including throughput, latency, and fault tolerance. This data-processing lens is directly relevant to enterprise adoption decisions, since it reframes blockchain not as a replacement for cloud databases but as a complementary component optimized for a narrower set of guarantees, namely immutability and verifiable consensus, rather than high-throughput transactional processing.

2.2 Blockchain and Cloud Computing Integration

A growing body of literature has examined how blockchain and cloud computing can be combined rather than treated as competing paradigms. Casino, Dasaklis, and Patsakis (2019) conducted a systematic literature review of blockchain-based applications and identified supply chain management, healthcare, and identity management as the domains with the most mature cloud-blockchain integration patterns. Dorsala, Sastry, and Chapram (2021)

surveyed blockchain-based solutions specifically for cloud computing and categorized them according to which cloud security objective they addressed, including data integrity verification, access control, and auditability.

Rimba, Tran, Weber, Staples, Ponomarev, and Xu (2017) directly compared the cost and performance of executing business processes on a blockchain versus a conventional cloud service, finding that blockchain execution incurred meaningfully higher costs and latency, a finding that supports the hybrid on-chain/off-chain design favored by most enterprise BaaS platforms rather than fully on-chain data storage. Wei, Wang, Zhao, Tyagi, and Kumar (2019) proposed a blockchain-based cloud data integrity protection mechanism in which cryptographic proofs of storage correctness are anchored on-chain while the underlying data remains in conventional cloud storage, a pattern that closely mirrors the off-chain architecture examined later in this article.

2.3 Blockchain-as-a-Service Platforms

As cloud providers began packaging blockchain infrastructure as a managed service, researchers turned to comparing the resulting Blockchain-as-a-Service (BaaS) offerings. Onik and Miraz (2019) performed a detailed comparative analysis of BaaS platforms offered by Microsoft, Amazon, IBM, Oracle, and SAP, evaluating each along dimensions including supported ledger types, identity management integration, pricing model, and development tooling. Their analysis found that Microsoft Azure's BaaS offering benefited substantially from its ability to integrate blockchain nodes with existing Azure services such as Azure Active Directory, Azure Key Vault, and Power BI, reducing the additional infrastructure organizations needed to build around the blockchain layer itself.

Samaniego and Deters (2016) proposed an early model for blockchain as a service specifically for Internet of Things data management, arguing that fog and edge nodes could host lightweight blockchain clients while heavier validation and storage occurred in the cloud, a division of labor consistent with the layered framework proposed in this article. Lahiri, Chen, Wang, and Dillig (2018) addressed a distinct but related concern: the correctness of the smart contracts deployed on cloud-hosted blockchain networks. Their formal specification and verification tooling for Azure Blockchain smart contracts directly targets one of the most consequential risks in blockchain-based data management, namely logic errors in smart contracts that can produce unintended data exposure or incorrect access decisions.

2.4 Security, Identity, and Trust Management

Security research on cloud-blockchain integration has consistently emphasized identity and access management as a critical control point. Zhang and Lin (2018) proposed a consortium blockchain architecture for secure, privacy-preserving data sharing in e-health systems, demonstrating how blockchain-enforced access policies could allow multiple healthcare organizations to share patient data without a central intermediary holding unilateral control over access decisions. Li, Wu, Cao, Chen, Zhang, and Buyya (2021) proposed a taxonomy of blockchain-based trust management approaches for cloud computing systems, distinguishing between reputation-based, identity-based, and smart-contract-based trust mechanisms, and concluding that hybrid approaches combining identity federation with on-chain reputation scoring produced the most robust trust outcomes in multi-tenant cloud environments.

Puthal, Malik, Mohanty, Kougianos, and Yang (2018) offered a broader assessment of blockchain as a decentralized security framework, cautioning that blockchain should be deployed selectively, only in scenarios where its specific properties of immutability and distributed consensus provide a genuine security or business advantage over conventional centralized controls. Kshetri (2018) extended this analysis specifically to cybersecurity applications, arguing that blockchain's contribution to cybersecurity lies primarily in strengthening data integrity verification and reducing single points of failure in identity and access management systems, rather than in replacing encryption or network security controls outright.

Zyskind, Nathan, and Pentland (2015) proposed one of the earliest concrete architectures for decentralizing personal data privacy using blockchain, in which the blockchain stores only pointers and access-control policies while the actual data remains off-chain, an architecture that anticipated the off-chain storage pattern later adopted by most enterprise BaaS platforms, including Azure Blockchain Service. Sharma, Rathore, and Park (2018) applied a

similar distributed architecture concept to smart city networks, combining blockchain-based coordination with edge and cloud resources to manage large volumes of sensor data without a single centralized point of control.

2.5 Comparative Platform and Performance Studies

Finally, several studies have directly compared cloud platforms on dimensions relevant to blockchain deployment. Kotas, Naughton, and Imam (2018) benchmarked Amazon Web Services and Microsoft Azure compute instances using high-performance computing workloads, finding that relative cost-effectiveness depended heavily on workload characteristics, a finding with direct implications for organizations selecting a cloud provider to host blockchain validator nodes, which have distinct compute and networking requirements from typical web workloads. Gao, Hatcher, and Yu (2018) surveyed blockchain techniques and applications more broadly, providing a taxonomy of consensus mechanisms, including the Proof of Authority and Istanbul Byzantine Fault Tolerance mechanisms used by Azure Blockchain Service, and comparing their suitability for permissioned enterprise networks against the Proof of Work mechanism used in public cryptocurrency networks.

Taken together, this literature indicates that a secure, decentralized cloud data management framework should combine four elements: an off-chain cloud layer for scalable storage and identity management; a permissioned consensus layer suited to multi-organizational trust requirements; formally verified smart contracts to enforce data-sharing rules; and a governance structure that clearly allocates responsibility for node operation, key management, and consortium membership decisions. The following sections develop and analyze such a framework in the specific context of Microsoft Azure.

3. A Layered Framework for Blockchain-Based Decentralized Data Management on Azure

Building on the on-chain/off-chain design pattern identified across the literature (Rimba et al., 2017; Zyskind, Nathan, & Pentland, 2015), this article proposes a four-layer framework for decentralized cloud data management on Microsoft Azure. Figure 1 illustrates the framework, which separates concerns between conventional cloud services, blockchain integration tooling, consortium participants, and the distributed ledger itself.

Figure 1. Decentralized Framework Integrating Microsoft Azure Cloud Services with a Permissioned Blockchain Layer

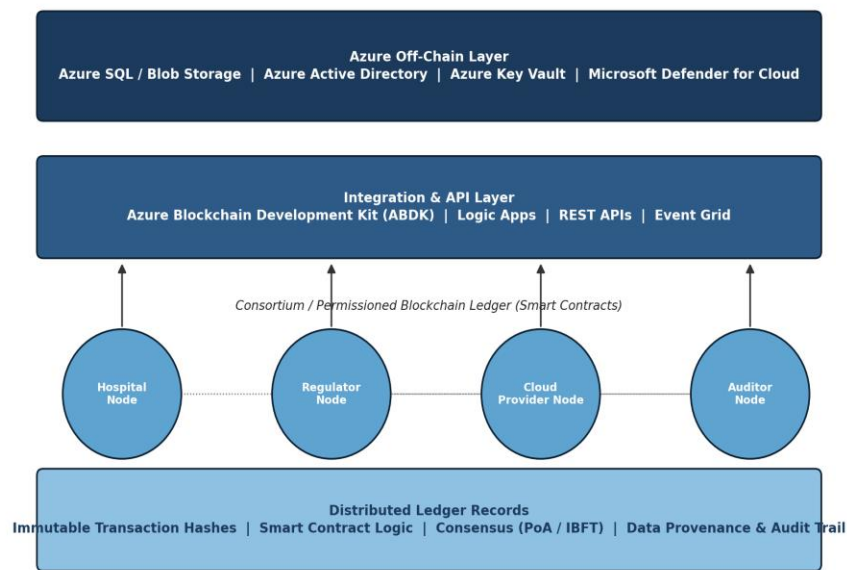


Figure 1. Decentralized framework integrating Microsoft Azure cloud services with a permissioned blockchain layer, showing the off-chain Azure layer, the integration and API layer, consortium validator nodes, and the distributed ledger records.

3.1 Azure Off-Chain Layer

The top layer of the framework retains conventional Azure services for tasks that do not require distributed consensus. Large data objects, such as medical images, financial statements, or IoT sensor logs, are stored in Azure SQL Database or Blob Storage rather than directly on the blockchain, consistent with the storage-efficiency argument advanced by Rimba et al. (2017). Azure Active Directory manages user and organizational identities across the consortium, while Azure Key Vault secures the cryptographic keys used to sign blockchain transactions. Microsoft Defender for Cloud provides continuous monitoring of the off-chain infrastructure, addressing the threat-detection gap that blockchain alone does not resolve (Puthal et al., 2018).

3.2 Integration and API Layer

The second layer bridges the off-chain Azure services and the blockchain network. The Azure Blockchain Development Kit provides connectors that allow smart contracts deployed on the ledger to trigger and respond to events in Logic Apps, enabling automated workflows such as notifying a data custodian when a new access request is approved on-chain. This layer operationalizes the interoperability requirement identified by Onik and Miraz (2019) as one of the distinguishing strengths of Azure's BaaS offering relative to competing platforms.

3.3 Consortium Validator Nodes

The third layer consists of the participating organizations that operate blockchain validator nodes, for example a hospital, a regulator, a cloud service provider, and an independent auditor in a healthcare data-sharing scenario. Each organization retains its own Azure subscription and validator node, and consensus among these nodes, rather than any single organization's decision, determines whether a transaction is accepted. This structure directly addresses the single-point-of-failure and central-authority concerns raised by Takabi, Joshi, and Ahn (2010) and echoed in later blockchain-specific analyses (Zheng et al., 2018).

3.4 Distributed Ledger Records

The bottom layer is the distributed ledger itself, which records only the cryptographic hashes of off-chain data, the outcomes of smart-contract executions, and an immutable, timestamped audit trail of every access decision. Consensus is achieved using Istanbul Byzantine Fault Tolerance or a comparable Proof of Authority mechanism, both of which are well suited to permissioned networks with a known, accountable set of validators, as opposed to public Proof of Work networks (Gao, Hatcher, & Yu, 2018).

4. Comparative Analysis of Blockchain-as-a-Service Platforms

To evaluate the relative strengths of Microsoft Azure's BaaS offering for the framework proposed above, Table 1 compares Azure Blockchain Service against two widely studied alternatives, Amazon Managed Blockchain and IBM Blockchain Platform, along the dimensions most relevant to secure decentralized data management.

Table 1. Comparison of Microsoft Azure, Amazon, and IBM Blockchain-as-a-Service Platforms

Feature	Microsoft Azure Blockchain Service	Amazon Managed Blockchain	IBM Blockchain Platform
Supported Ledgers	Ethereum (Quorum), Hyperledger Fabric, Corda	Hyperledger Fabric, Ethereum	Hyperledger Fabric
Consensus Mechanism	Istanbul Byzantine Fault Tolerance (IBFT), Proof of Authority	Practical Byzantine Fault Tolerance (via Fabric ordering service)	Practical Byzantine Fault Tolerance (via Fabric ordering service)
Identity & Access Management	Azure Active Directory, Role-Based Access Control	AWS Identity and Access Management (IAM)	IBM Cloud IAM, SecureKey digital identity
Off-Chain Data Integration	Native integration with Azure SQL, Blob Storage, Logic Apps, and Power BI	Integration with Amazon QLDB and AWS data services	Integration via IBM Cloud databases and APIs
Network Type	Consortium / multi-permissioned, subscription	Private, permissioned	Private, public, and hybrid
Development Tooling	Azure Blockchain Development Kit, Visual Studio Code extension, REST APIs	AWS SDKs, Amazon Managed Blockchain console	IBM Blockchain Platform extension, Hyperledger Composer

As Table 1 indicates, the three platforms converge on the use of permissioned Hyperledger Fabric-derived consensus for enterprise deployments, but differ in how tightly the blockchain layer integrates with each provider's broader identity and data ecosystem. Azure's integration with Azure Active Directory and native connectors to Azure SQL, Blob Storage, and Power BI gives organizations already standardized on Microsoft's cloud ecosystem a comparatively lower integration burden, a conclusion consistent with Onik and Miraz's (2019) comparative assessment of BaaS platforms.

5. Mapping Decentralized Data Management Risks to Blockchain-on-Azure Mitigations

Table 2 synthesizes the security and governance challenges most frequently associated with decentralized, multi-organizational cloud data management and maps each to the corresponding mitigation available within the blockchain-on-Azure framework, along with representative supporting literature.

Table 2. Decentralized Data Management Risks and Blockchain-on-Azure Mitigations

Security / Governance Challenge in Decentralized Cloud Data Management	Blockchain-on-Azure Mitigation	Supporting Literature
Single point of failure and central authority risk in traditional cloud storage	Permissioned blockchain ledger distributes trust across consortium nodes rather than a single administrator	Zheng, Xie, Dai, Chen, & Wang (2018); Yli-Huumo, Ko, Choi, Park, & Smolander (2016)
Data tampering and lack of verifiable provenance	Immutable, hash-linked transaction records provide a verifiable audit trail across the data lifecycle	Wei, Wang, Zhao, Tyagi, & Kumar (2019); Dinh et al. (2018)
Inefficient or opaque access control across multiple stakeholders	Smart contracts encode access rules directly on-chain, enforced automatically without manual intervention	Zhang & Lin (2018); Christidis & Devetsikiotis (2016)
Difficulty auditing data-sharing agreements between organizations	Consortium ledger combined with Azure AD identity produces an immutable, identity-linked audit trail	Li, Wu, Cao, Chen, Zhang, & Buyya (2021)
High cost and complexity of building blockchain infrastructure in-house	Azure Blockchain-as-a-Service abstracts node provisioning, consensus configuration, and network management	Onik & Miraz (2019); Samaniego & Deters (2016)
Smart contract logic errors leading to unintended data exposure	Formal specification and verification tooling for Azure Blockchain smart contracts	Lahiri, Chen, Wang, & Dillig (2018)
Vendor lock-in and lack of interoperability between cloud and blockchain layers	Standardized REST APIs and the Azure Blockchain Development Kit enable interoperability with existing enterprise systems	Rimba et al. (2017); Kotas, Naughton, & Imam (2018)

The mapping in Table 2 highlights that blockchain integration does not eliminate the need for conventional cloud security controls; rather, it adds a distributed verification layer on top of them. For example, smart contracts can enforce access rules automatically, but those contracts must still be formally verified to avoid the logic errors documented by Lahiri, Chen, Wang, and Dillig (2018), and the underlying data they govern still depends on Azure's conventional encryption and network security controls for protection at rest and in transit.

6. Discussion

The analysis presented above supports several practical conclusions for organizations considering a blockchain-on-Azure approach to decentralized data management. First, blockchain integration is most valuable in settings that already involve multiple, mutually distrustful organizations sharing data, such as healthcare consortia, cross-border payment networks, or multi-tier supply chains; in single-organization deployments, the added complexity of operating a blockchain network is unlikely to justify the benefit, a caution raised explicitly by Puthal, Malik, Mohanty, Kougianos, and Yang (2018).

Second, the on-chain/off-chain division of labor is essential for cost and performance reasons. As Rimba et al. (2017) demonstrated empirically, executing business logic and storing bulk data directly on a blockchain is substantially more expensive and slower than doing so in a conventional cloud database. The framework proposed in this article therefore keeps only cryptographic hashes, access-control decisions, and audit records on-chain, while leaving bulk data storage to Azure SQL and Blob Storage, consistent with the architecture proposed by Zyskind, Nathan, and Pentland (2015).

Third, smart contract correctness is a first-order security concern that is easy to underestimate. Because smart contracts execute automatically and their logic becomes part of an immutable ledger once deployed, errors are considerably more costly to remediate than equivalent bugs in conventional application code. Formal verification tools of the kind proposed by Lahiri, Chen, Wang, and Dillig (2018) for Azure Blockchain smart contracts should be treated as a mandatory step in any production deployment, not an optional quality-assurance enhancement.

Fourth, consortium governance, meaning the rules by which organizations join, leave, and operate validator nodes within the network, is as important as the underlying technical architecture. Li, Wu, Cao, Chen, Zhang, and Buyya (2021) note that trust management in blockchain-based cloud systems depends on a combination of technical mechanisms and institutional agreements; a technically sound blockchain network governed by ambiguous or contested membership rules is unlikely to deliver the trust benefits that motivated its adoption in the first place. Organizations should therefore formalize consortium governance agreements, covering node operation responsibilities, dispute resolution procedures, and criteria for admitting or removing members, before deploying a production blockchain-on-Azure network.

Finally, the comparative platform analysis in Table 1 suggests that the choice of BaaS provider should be driven primarily by the organization's existing cloud investments and identity infrastructure, rather than by marginal differences in consensus algorithm performance. Kotas, Naughton, and Imam's (2018) benchmarking work illustrates that raw compute performance differences between providers are often workload-dependent and relatively modest compared with the integration costs of migrating an organization's existing identity, storage, and monitoring infrastructure to a new provider.

7. Recommendations

Organizations evaluating or implementing a blockchain-on-Azure framework for decentralized data management should: (1) restrict on-chain storage to cryptographic hashes, access decisions, and audit metadata, keeping bulk data in Azure SQL or Blob Storage; (2) commission formal verification of all smart contracts prior to production deployment, using tooling such as that proposed for Azure Blockchain by Lahiri et al. (2018); (3) integrate blockchain identity requirements with Azure Active Directory and enforce multi-factor authentication for all validator node operators; (4) establish a written consortium governance agreement covering node operation responsibilities, onboarding and offboarding procedures, and dispute resolution before go-live; (5) apply Microsoft Defender for Cloud and Azure Monitor to the off-chain infrastructure surrounding the blockchain network, since the ledger itself does not provide network-level threat detection; and (6) periodically benchmark the deployment against alternative BaaS platforms using workload-representative criteria, following the comparative methodology demonstrated by Kotas, Naughton, and Imam (2018), to confirm that the chosen platform continues to meet cost and performance requirements as the network scales.

8. Conclusion

Blockchain technology and cloud computing address complementary weaknesses: blockchain distributes trust and provides immutable verification across multiple organizations, while cloud platforms such as Microsoft Azure provide the scalable storage, identity management, and monitoring infrastructure that blockchain networks alone do not supply. This article has proposed a four-layer framework that combines Azure's off-chain cloud services with a permissioned blockchain layer, compared Azure's Blockchain-as-a-Service offering against competing platforms, and mapped common decentralized data management risks to specific mitigations available within this hybrid architecture. The literature reviewed indicates that the framework's success depends less on the specific blockchain

platform selected and more on disciplined engineering practices, including formal smart-contract verification, careful on-chain/off-chain data separation, and clear consortium governance. Future empirical work should measure the real-world performance, cost, and security outcomes of production blockchain-on-Azure deployments across different multi-organizational data-sharing contexts, to validate the conceptual risk-mitigation mapping proposed here against operational evidence.

Funding: This research received no external funding.

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

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers

Artificial Intelligence (AI) Use Disclosure: The authors declare that no artificial intelligence tools were used in the preparation of this manuscript.

References

- [1] Almeshal, T. A., & Alhogail, A. A. (2021). Blockchain for businesses: A scoping review of suitability evaluations frameworks. *IEEE Access*, 9, 155425–155442. <https://doi.org/10.1109/ACCESS.2021.3128172>
- [2] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81. <https://doi.org/10.1016/j.tele.2018.11.006>
- [3] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access*, 4, 2292–2303. <https://doi.org/10.1109/ACCESS.2016.2566339>
- [4] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering*, 30(7), 1366–1385. <https://doi.org/10.1109/TKDE.2017.2781227>
- [5] Dorsala, M. R., Sastry, V. N., & Chapram, S. (2021). Blockchain-based solutions for cloud computing: A survey. *Journal of Network and Computer Applications*, 196, 103246. <https://doi.org/10.1016/j.jnca.2021.103246>
- [6] Gao, W., Hatcher, W. G., & Yu, W. (2018). A survey of blockchain: Techniques, applications, and challenges. In *Proceedings of the 27th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1–11). IEEE. <https://doi.org/10.1109/ICCCN.2018.8487348>
- [7] Khan, N., Aljoaey, H., Tabassum, M., Farzamnia, A., Sharma, T., & Tung, Y. H. (2022). Proposed model for secured data storage in decentralized cloud by blockchain Ethereum. *Electronics*, 11(22), 3686. <https://doi.org/10.3390/electronics11223686>
- [8] Kotas, C., Naughton, T., & Imam, N. (2018). A comparison of Amazon Web Services and Microsoft Azure cloud platforms for high performance computing. In *2018 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1–4). IEEE. <https://doi.org/10.1109/ICCE.2018.8326349>
- [9] Kshetri, N. (2018). Blockchain's roles in strengthening cybersecurity. *Telecommunications Policy*, 42(4), 273–283. <https://doi.org/10.1016/j.telpol.2017.09.003>
- [10] Lahiri, S. K., Chen, S., Wang, Y., & Dillig, I. (2018). Formal specification and verification of smart contracts for Azure Blockchain (arXiv:1812.08829). *arXiv*. <https://arxiv.org/abs/1812.08829>
- [11] Li, W., Wu, J., Cao, J., Chen, N., Zhang, Q., & Buyya, R. (2021). Blockchain-based trust management in cloud computing systems: A taxonomy, review and future directions. *Journal of Cloud Computing*, 10(1), 1–34. <https://doi.org/10.1186/s13677-021-00247-5>
- [12] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, 59(3), 183–187. <https://doi.org/10.1007/s12599-017-0467-3>
- [13] Onik, M. M. H., & Miraz, M. H. (2019). Performance analytical comparison of Blockchain-as-a-Service (BaaS) platforms. In *International Conference for Emerging Technologies in Computing* (pp. 3–18). Springer. https://doi.org/10.1007/978-3-030-23943-5_1
- [14] Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The blockchain as a decentralized security framework [Future directions]. *IEEE Consumer Electronics Magazine*, 7(2), 18–21. <https://doi.org/10.1109/MCE.2017.2776459>
- [15] Rimba, P., Tran, A. B., Weber, I., Staples, M., Ponomarev, A., & Xu, X. (2017). Comparing blockchain and cloud services for business process execution. In *2017 IEEE International Conference on Software Architecture (ICSA)* (pp. 257–260). IEEE. <https://doi.org/10.1109/ICSA.2017.44>
- [16] Samaniego, M., & Deters, R. (2016). Blockchain as a service for IoT. In *2016 IEEE International Conference on Internet of Things (iThings)* (pp. 433–436). IEEE. <https://doi.org/10.1109/iThings-GreenCom-CPSCoM-SmartData.2016.102>

- [17] Sharma, P. K., Rathore, S., & Park, J. H. (2018). DistArch-SCNet: Blockchain-based distributed architecture with Li-Fi communication for a scalable smart city network. *IEEE Consumer Electronics Magazine*, 7(4), 55–64. <https://doi.org/10.1109/MCE.2018.2816745>
- [18] Takabi, H., Joshi, J. B. D., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, 8(6), 24–31. <https://doi.org/10.1109/MSP.2010.186>
- [19] Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, 59(11), 15–17. <https://doi.org/10.1145/2994581>
- [20] Wei, P., Wang, D., Zhao, Y., Tyagi, S. K. S., & Kumar, N. (2019). Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems*, 102, 902–911. <https://doi.org/10.1016/j.future.2019.09.028>
- [21] Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. *IEEE Access*, 8, 131723–131740. <https://doi.org/10.1109/ACCESS.2020.3009876>
- [22] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PLOS ONE*, 11(10), e0163477. <https://doi.org/10.1371/journal.pone.0163477>
- [23] Zhang, A., & Lin, X. (2018). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of Medical Systems*, 42(8), 140. <https://doi.org/10.1007/s10916-018-0995-5>
- [24] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4), 352–375. <https://doi.org/10.1504/IJWGS.2018.095647>
- [25] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops* (pp. 180–184). IEEE. <https://doi.org/10.1109/SPW.2015.27>