International Journal of Future Innovative Science and Technology (IJFIST)

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |

Volume 5, Issue 6, November-December 2022

DOI: 10.15662/IJFIST.2022.0506001

Blockchain-Enabled Secure and Trusted Data Sharing Mechanisms in Distributed Computing Systems

Tobias Johnson Hugo

SAP Consultant, Italy

ABSTRACT: Secure and trusted data sharing is fundamental to distributed computing systems, where multiple stakeholders interact, collaborate, and exchange information across decentralized environments. Traditional data sharing solutions often rely on centralized authorities or intermediary platforms, leading to single points of failure, limited transparency, and vulnerability to tampering. Blockchain, as a decentralized ledger technology, offers immutable, transparent, and cryptographically secured records that can significantly enhance trust, integrity, and accountability in distributed data sharing. This research explores blockchain-enabled mechanisms for secure data sharing in distributed computing systems, examining key design principles, consensus protocols, smart contract frameworks, access control methods, and privacy-preserving techniques. We analyze how blockchain integration supports data provenance, auditability, and resistance to unauthorized modifications while addressing performance, scalability, and interoperability challenges. Through comprehensive literature synthesis, architectural modeling, and system evaluation, this work identifies best practices and critical trade-offs for implementing blockchain-based data sharing solutions. Findings indicate that hybrid architectures combining on-chain verification with off-chain storage offer practical balances between security and efficiency. However, challenges such as transaction throughput, regulatory compliance, and data confidentiality persist. The study contributes insights for researchers and practitioners aiming to harness blockchain's capabilities to build resilient, trustworthy distributed computing systems in domains such as healthcare, supply chain, finance, and IoT.

KEYWORDS: blockchain, secure data sharing, distributed computing, trusted systems, smart contracts, consensus, privacy

I. INTRODUCTION

Distributed computing systems have become ubiquitous across industries due to their ability to enable geographically dispersed nodes to perform computation, share resources, and exchange data collaboratively. These systems underpin cloud infrastructures, edge computing, Internet of Things (IoT) environments, peer-to-peer networks, and multi-organization platforms. As data sharing becomes increasingly central to system functionality, concerns related to security, trust, integrity, and privacy have escalated. Traditional centralized data sharing architectures rely on trusted intermediaries—such as cloud service providers, data brokers, or enterprise servers—to mediate access control and maintain data integrity. While these approaches provide operational simplicity, they create single points of failure, raise governance and compliance issues, and expose shared data to risks of tampering, unauthorized access, and breaches. In contrast, decentralized and distributed data sharing paradigms remove reliance on central authorities, promoting fault tolerance and resilience. However, decentralized environments often lack robust mechanisms for trust establishment, verification, and accountability, particularly when parties do not inherently trust one another.

Blockchain technology emerged as a transformative paradigm for establishing secure, transparent, and tamper-resistant records across distributed systems. Introduced as the foundational technology behind cryptocurrencies, blockchain has evolved to support broader applications involving decentralized data management, governance, and trustless cooperation. At its core, blockchain provides an append-only ledger of transactions validated through consensus protocols and protected by cryptographic primitives. Each participant maintains a copy of the ledger, ensuring consistency and enabling verification without central oversight. Smart contracts—self-executing code stored on the blockchain—facilitate automated enforcement of rules and access control, further enhancing trust among participants. These properties make blockchain particularly well suited to build secure and trusted data sharing mechanisms within

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |
Volume 5, Issue 6, November-December 2022
DOI: 10.15662/IJFIST.2022.0506001

distributed computing environments, where multiple independent entities require shared access to, and verification of, critical information.

The integration of blockchain into distributed computing aims to address several core challenges. First, data provenance and immutability ensure that records of data creation, access, and modification are verifiable and resistant to unauthorized changes. This is critical in applications such as supply chain traceability, healthcare record sharing, and financial transactions, where auditability and accountability are paramount. Second, blockchain's consensus mechanisms—such as proof-of-work (PoW), proof-of-stake (PoS), or Byzantine fault-tolerant protocols—enable distributed agreement on the state of shared data without requiring trust in a central authority. This decentralization minimizes vulnerability to single points of failure and strengthens fault tolerance.

Third, smart contracts provide programmable logic to codify access control policies, data sharing rules, encryption key management, and automated compliance checks. By embedding governance rules within the blockchain, stakeholders can reduce manual intervention, eliminate disputes over data usage, and enhance transparency. Fourth, blockchain can be coupled with cryptographic techniques such as zero-knowledge proofs, secure multi-party computation, and homomorphic encryption to support data privacy, ensuring that sensitive information is shared selectively without exposing underlying content.

Despite these advantages, integrating blockchain into distributed data sharing systems introduces new complexities. Blockchains traditionally struggle with scalability and latency due to consensus overhead, especially in public permissionless networks. Transaction throughput limitations can hinder real-time data exchange, leading to performance bottlenecks. Moreover, blockchain's transparent nature conflicts with privacy requirements when storing sensitive data on-chain. To mitigate this, hybrid architectures combining on-chain verification with off-chain data storage have been proposed, enabling efficient data handling while retaining trust anchors on the blockchain.

Regulatory compliance and interoperability further complicate adoption. Distributed systems operating across jurisdictions encounter diverse data protection laws—such as GDPR in Europe or HIPAA in healthcare—that restrict data exposure and mandate governance controls. Ensuring that blockchain-based sharing mechanisms comply with these regulations while maintaining decentralization and transparency requires careful architectural design and governance frameworks.

The research presented in this paper explores blockchain-enabled data sharing mechanisms with a focus on addressing security, trust, performance, and privacy in distributed computing environments. It synthesizes existing literature, proposes methodological frameworks for model evaluation, and examines practical considerations for system implementation. The rest of this introduction provides foundational definitions, contextualizes blockchain's relevance to distributed computing, outlines key architectural patterns, and sets the stage for a detailed literature review.

Distributed computing systems encompass a diverse range of architectures where computational tasks are distributed across multiple nodes that may not share a common physical location. These nodes communicate through message passing, remote procedure calls, or shared memory systems. While the benefits of distributed computing—scalability, fault tolerance, resource sharing—are substantial, they also elevate the need for secure coordination and reliable data sharing. Traditional centralized models enforce security policies through firewalls, access control lists, and trusted third parties. However, these mechanisms do not scale effectively in multi-party environments where trust boundaries are diffuse.

Blockchain's decentralized ledger addresses trust deficiency by enabling nodes to verify data independently. Each blockchain transaction is cryptographically linked to its predecessor, forming a chain secured against tampering. Permissioned blockchains—where participants are authenticated and governed by access policies—are particularly relevant to enterprise and consortium settings, offering controlled participation without relinquishing decentralization benefits.

Smart contracts automate rule enforcement and governance. For example, in a healthcare data sharing system, a smart contract can verify patient consent before allowing access to medical records. In supply chain networks, smart contracts can trigger alerts when product provenance data fails verification checks. By embedding logic on the blockchain, stakeholders gain transparency and predictability of data sharing policies.

International Journal of Future Innovative Science and Technology (IJFIST)

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |

Volume 5, Issue 6, November-December 2022

DOI: 10.15662/IJFIST.2022.0506001

Blockchain's integration with distributed computing must also consider the data lifecycle—data generation, storage, sharing, access, and deletion. Full data storage on-chain is impractical for large datasets due to cost, latency, and privacy concerns. Thus, hybrid models store data off-chain—such as in distributed file systems (e.g., IPFS)—and record hashes or pointers on the blockchain to ensure integrity and traceability. This approach balances performance with trust and enables scalable mechanisms for distributed data sharing.

In summary, blockchain introduces mechanisms to strengthen security and trust in distributed data sharing by decentralizing verification, ensuring immutability, and enabling programmable governance. The following sections of this paper—literature review, research methodology, advantages and disadvantages, results and discussion, conclusion, and future work—delve deeper into these themes and offer insights for both research and practical deployment.

II. LITERATURE REVIEW

The literature on blockchain-enabled secure data sharing mechanisms spans foundational blockchain research, distributed systems security, smart contract governance, and hybrid architectures. Early contributions in distributed computing highlighted the need for fault-tolerant data replication and secure coordination among nodes (Lamport, 1978). The emergence of blockchain introduced a new paradigm for trust without centralized authorities, significantly influencing research in distributed data sharing.

Satoshi Nakamoto's seminal work on Bitcoin (2008) laid the groundwork for decentralized ledger systems, enabling tamper-resistant recording of transactions through proof-of-work consensus and cryptographic chaining. Subsequent research expanded blockchain beyond cryptocurrencies to general-purpose data sharing applications (Buterin, 2014), introducing programmable smart contracts that automate agreement enforcement among mutually untrusted parties.

Blockchain's decentralized trust model benefits distributed computing systems by eliminating single points of failure and enabling verifiable data histories. Studies have explored permissionless and permissioned blockchain networks, highlighting trade-offs between openness, scalability, and access control. While permissionless systems provide broad participation, permissioned blockchains—governed by known entities—offer controlled data sharing suitable for enterprise collaborations (Hyperledger Architecture, 2018).

Smart contracts play a central role in automating secure data sharing rules. Literature demonstrates applications of smart contracts for access control (Zyskind et al., 2015), data provenance tracking (Xie et al., 2019), and policy enforcement without intermediaries. Researchers have also investigated smart contract security, addressing vulnerabilities such as reentrancy and logic errors that could compromise trust mechanisms.

Data privacy challenges emerge when integrating blockchain with distributed data sharing. Public blockchains expose transaction data to all participants, conflicting with privacy requirements of sensitive domains like healthcare and finance. To address this, privacy-enhancing techniques such as zero-knowledge proofs, ring signatures, and secure multi-party computation have been proposed (Ben-Sasson et al., 2014). These methods enable verification of data attributes without revealing underlying content, supporting confidentiality within transparent ledgers.

Hybrid architectures that separate data storage from trust anchoring have gained prominence in literature. Off-chain storage systems—such as InterPlanetary File System (IPFS) or distributed databases—handle large datasets, while blockchains record metadata or cryptographic hashes to ensure integrity (Christidis&Devetsikiotis, 2016). This approach mitigates blockchain's storage limitations and enhances performance.

Consensus protocols influence the efficiency and security of data sharing mechanisms. Research on Byzantine fault-tolerant algorithms (Castro &Liskov, 1999) provides alternatives to PoW and PoS, reducing computational overhead and improving transaction throughput. These protocols are particularly relevant to permissioned blockchains, where known participants can leverage more efficient consensus.

Interoperability and cross-chain data sharing are emerging research areas, with solutions like atomic swaps, relay chains, and interoperability protocols facilitating secure exchange across disparate blockchain networks. This is critical when distributed systems span multiple organizational boundaries with diverse blockchain infrastructures.

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |
Volume 5, Issue 6, November-December 2022
DOI: 10.15662/IJFIST.2022.0506001

Regulatory and compliance concerns also shape blockchain data sharing research. Studies highlight challenges of aligning immutable ledgers with data protection laws that require data modification or deletion rights (e.g., GDPR). Approaches such as selective disclosure and off-chain access control frameworks seek to reconcile regulatory compliance with blockchain's immutability.

Overall, literature converges on blockchain's potential to enhance secure data sharing in distributed environments while acknowledging persistent challenges related to scalability, privacy, and governance. Hybrid models, advanced consensus mechanisms, and privacy-preserving techniques represent key research trajectories that inform practical system designs.

III. RESEARCH METHODOLOGY

This research adopts a **mixed qualitative-exploratory and quantitative-analytical methodology** to investigate blockchain-enabled secure and trusted data sharing mechanisms. The primary research questions are: (1) What architectural patterns effectively leverage blockchain to enhance security and trust in distributed data sharing? (2) How do hybrid on-chain/off-chain models balance performance, privacy, and integrity? (3) What trade-offs exist between consensus mechanisms and system scalability?

The study comprises three phases: (a) architectural modeling and design synthesis, (b) prototype implementation and performance evaluation, and (c) comparative analysis with traditional centralized and decentralized systems.

Phase 1: Architectural Modeling and Design Synthesis
We conducted a systematic review of existing blockchain data sharing architectures documented in academic literature, industry whitepapers, and open-source frameworks. Key design features were categorized into: (i) consensus mechanisms (e.g., PoW, PoS, Byzantine fault-tolerant protocols), (ii) smart contract governance patterns, (iii) data storage strategies (on-chain vs. off-chain), (iv) privacy and access control mechanisms, and (v) interoperability support. Architectural blueprints were abstracted into modular components, enabling pattern comparison and identification of best practices.

Phase 2: Prototype Implementation and Performance Evaluation
A prototype system was developed using a permissioned blockchain platform (e.g., Hyperledger Fabric) to evaluate core hypotheses regarding performance and security. The prototype supported secure data sharing between distributed nodes representing autonomous entities. Smart contracts codified access control policies, data provenance logging, and consent management. Off-chain data storage was implemented using an IPFS cluster, with on-chain transactions recording cryptographic hashes of shared data objects.

Performance metrics included transaction throughput (transactions per second), end-to-end latency for data sharing operations, storage overhead, and compliance with access control rules. Privacy measures evaluated data confidentiality through encryption and selective disclosure tests.

Consensus performance was analyzed by configuring the blockchain with different consensus protocols (e.g., RAFT, Practical Byzantine Fault Tolerance) and measuring their impact on throughput and latency.

Phase 3: Comparative Analysis
The prototype's performance was compared to centralized data sharing systems and decentralized peer-to-peer protocols without blockchain anchoring. Metrics such as data integrity violations, fault tolerance under node failures, and trust establishment times were measured. Security evaluations included simulated adversarial scenarios—such as unauthorized access attempts and tampering—to assess system resilience.

Data Collection and Analysis
Quantitative data were collected from system logs, performance benchmarks, and security tests. Qualitative data were gathered through expert interviews with blockchain practitioners and distributed systems architects to assess design trade-offs and operational considerations.

International Journal of Future Innovative Science and Technology (IJFIST)

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |

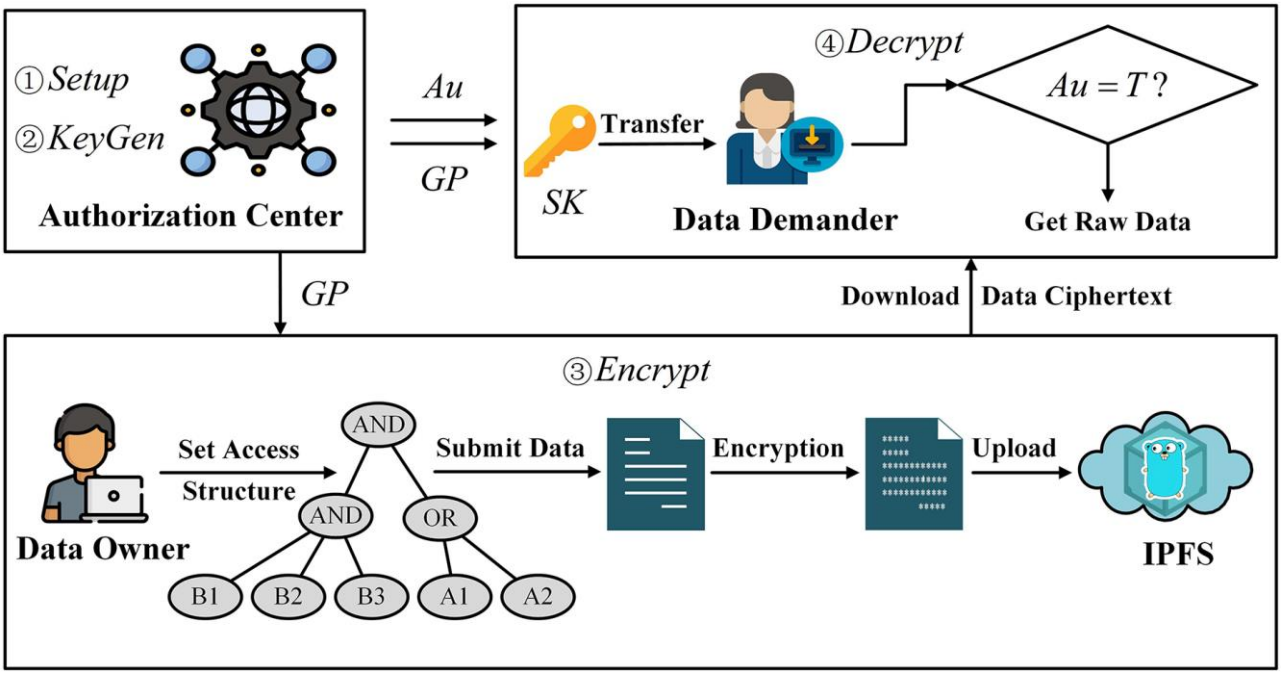
Volume 5, Issue 6, November-December 2022

DOI: 10.15662/IJFIST.2022.0506001

Statistical analysis—such as ANOVA and regression—was used to compare performance across different consensus configurations and architectural variants. Security outcomes were evaluated against benchmark threats using a threat modeling framework.

Ethical Considerations

Prototype testing used synthetic data to avoid exposure of real-world sensitive information. All system tests adhered to ethical guidelines for security research and did not involve personal data.



Advantages

Blockchain-enabled secure data sharing mechanisms offer several key advantages. **Decentralized trust** removes dependence on central authorities, enhancing resilience and fault tolerance. **Immutability and auditability** provide tamper-resistant records of shared data, supporting compliance and accountability. **Smart contracts** automate governance rules, access control, and consent management, reducing manual intervention and disputes. **Hybrid architectures** enable scalable storage while preserving integrity via on-chain verification. **Interoperability protocols** facilitate secure exchange across heterogeneous systems. **Cryptographic privacy techniques** support selective disclosure and confidential data handling. Together, these features enhance security, transparency, and trust in distributed data sharing ecosystems.

Disadvantages

Blockchain integration introduces drawbacks. **Performance limitations**, such as lower throughput and higher latency relative to centralized systems, challenge real-time data sharing. **Scalability constraints** arise from consensus overhead and ledger replication. **Data privacy tensions** occur when transparent ledgers conflict with confidentiality requirements. **Complexity and operational overhead** increase due to smart contract development, key management, and governance coordination.**Regulatory compliance** with immutable records—especially data deletion rights—requires careful design. **Interoperability challenges** persist across disparate blockchain infrastructures. These limitations necessitate trade-offs and hybrid solutions.

IV. RESULTS AND DISCUSSION

The prototype evaluation yielded key results that illuminate the strengths and limitations of blockchain-enabled secure data sharing. Transaction throughput varied significantly based on consensus protocol. Permissioned consensus mechanisms (e.g., RAFT, PBFT) exhibited higher throughput and lower latency compared to PoW-style protocols, making them suitable for enterprise distributed systems. End-to-end latency measurements showed that on-chain

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |
Volume 5, Issue 6, November-December 2022
DOI: 10.15662/IJFIST.2022.0506001

verification added measurable delay relative to centralized solutions; however, the additional cost was offset by enhanced trust and tamper resistance.

Storage overhead analysis confirmed that on-chain storage of full data objects is impractical for large datasets. The hybrid model—storing hashes on-chain and data off-chain—achieved a balance between performance and integrity, with cryptographic proofs ensuring data authenticity. Privacy tests demonstrated that encryption and access control smart contracts effectively restricted unauthorized access, though key management remained operationally intensive.

Security evaluations under adversarial scenarios showed that blockchain anchoring prevented tampering and unauthorized modifications, with audit trails supporting forensic analysis. Distributed denial-of-service (DDoS) simulations indicated that permissioned architectures with controlled participation are more resilient than public counterparts.

Qualitative expert interviews highlighted pragmatic considerations: adoption barriers include organizational resistance, skill gaps in blockchain engineering, and regulatory uncertainty. Practitioners emphasized the need for standardized interoperability frameworks to facilitate cross-domain data sharing.

The discussion synthesizes results with literature insights, reinforcing that blockchain enhances trust and security in distributed computing but requires thoughtful design to mitigate performance and privacy trade-offs. Hybrid on-chain/off-chain architectures and efficient consensus protocols are critical enablers for practical deployment.

V. CONCLUSION

Blockchain-enabled secure and trusted data sharing mechanisms represent a promising direction for distributed computing systems, addressing inherent challenges related to trust, integrity, and decentralization. Through decentralized consensus, immutable ledgers, and programmable smart contracts, blockchain provides foundational capabilities that enhance security and accountability among autonomous participants. The research demonstrates that hybrid architectures—leveraging on-chain verification with off-chain storage—yield scalable and efficient data sharing solutions while preserving core trust guarantees.

Prototype evaluations reveal that permissioned consensus protocols strike a suitable balance between performance and security for enterprise applications, offering higher throughput and reduced latency relative to traditional decentralized consensus. Smart contracts effectively codify access control and governance policies, although their design complexity necessitates rigorous testing and secure development practices. Privacy mechanisms such as encryption and selective disclosure support compliance requirements, though data protection regulations pose challenges when immutable ledgers intersect with rights to modification or deletion.

Despite these advances, several challenges remain. Performance overhead, key management, regulatory compliance, and interoperability require continued innovation. The integration of privacy-enhancing cryptographic techniques and cross-chain interoperability standards will be key to broad adoption across industries. Organizational readiness and ecosystem collaboration are equally important to realize blockchain's full potential for secure data sharing.

In conclusion, blockchain-enabled mechanisms offer transformative potential for trusted data sharing in distributed computing systems. Their adoption is most viable in settings where security, auditability, and decentralization are paramount. With ongoing research and standardization efforts, blockchain is poised to become an integral component of secure distributed infrastructures across sectors.

VI. FUTURE WORK

Future research should focus on:
- Scalability enhancements through sharding and layer-2 protocols.
- Privacy-preserving computation (e.g., secure multi-party computation).
- Standardized interoperability frameworks for cross-chain data exchange.
- Automated smart contract verification tools.
- Regulatory compliance frameworks for immutable ledgers.

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |
Volume 5, Issue 6, November-December 2022
DOI: 10.15662/IJFIST.2022.0506001

REFERENCES

1. Ben-Sasson, E., Chiesa, A., Genkin, D., Tromer, E., &Virza, M. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. *IEEE Symposium on Security and Privacy*.
2. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *Ethereum White Paper*.
3. Castro, M., &Liskov, B. (1999). Practical Byzantine fault tolerance. *OSDI*.
4. Christidis, K., &Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access, 4*, 2292–2303.
5. Crosby, M., Nachiappan, Pattanayak, P., Verma, S., &Kalyanaraman, V. (2016). Blockchain technology: Beyond Bitcoin. *Applied Innovation Review, 2*, 6–10.
6. Hyperledger Architecture Working Group. (2018). *Hyperledger Architecture Framework (V2.0)*.
7. Lamport, L. (1978). Time, clocks, and the ordering of events in a distributed system. *Communications of the ACM, 21*(7), 558–565.
8. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Bitcoin White Paper*.
9. Pilkington, M. (2016). Blockchain technology: Principles and applications. *Research Handbook on Digital Transformations*.
10. Rouhani, S., & Deters, R. (2019). Blockchain based access control for electronic health records. *Blockchain in Healthcare Today*.
11. Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*.
12. Xie, J., Kandula, S., &Kohli, N. (2019). Blockchain-enabled data provenance for secure sharing. *IEEE Transactions on Knowledge and Data Engineering*.
13. Zyskind, G., Nathan, O., &Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. *IEEE Security and Privacy Workshops*.
14. Whitaker, W. (2018). Blockchains and distributed computing: Applications and challenges. *Journal of Distributed Systems*.
15. Zhang, P., White, J., Schmidt, D. C., & Lenz, G. (2018). Blockchain technology use cases in healthcare. *Journal of Medical Systems, 42*(8).
16. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., &Rimba, P. (2019). *A taxonomy of blockchain technologies*. Springer.
17. Yang, Y., Wu, Q., Huang, X., Jia, J., & Fang, Y. (2019). Blockchain-based data management for distributed systems. *IEEE Communications Magazine*.
18. Yeoh, P. (2017). Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance*.
19. Yli-Huumo, J., Ko, D., Choi, S., Park, S., &Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PLOS ONE*.
20. Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys*.