[1] **Debroop Sarkar**

Balanced Evaluation of Decentralized Encrypted Point-to-Multipoint Storage Systems

Journal of Electrical Systems

Abstract: - With an ever-growing avalanche of digital data and threats to cybersecurity, more or less coherent international regulatory frameworks would have put a stop to centralized storage models governing the traditional paradigm. The paper weighs the options for decentralized encrypted point-to-multipoint storage systems against cloud architectures for an alternative, cheaper, and secure solution. All kinds of cryptographic techniques like AES-type schemes together with newly minted concepts of data sharding using an erasure code and blockchain-based verification mechanisms have gone deep into ensuring confidentiality, integrity, and availability for one's data. The results from our empirical studies that contrast data on decentralized platforms such as IPFS and Storj with AWS S3 indicate that decentralized solutions maintain above 99% data recoverability with acceptable retrieval latencies even when some nodes fail. The legal and ethical implications, especially with respect to data immutability in relation to compliance schemes such as GDPR, are also discussed. Finally, a strategic research roadmap pointing toward quantum-safe encryption, burning adaptive smart contracts, and energy-efficient consensus among all feasible in medical, financial, and IoT areas is delineated.

Keywords: Decentralized Storage, Encryption, Data Sharding, Blockchain Verification, Point-to-Multipoint Systems, IPFS, Storj.

I. INTRODUCTION

These decentralized storage systems are becoming important alternatives to the established centers for storing data. In- creased volume of data production, accompanied with heightened threat of cyber-attacks and increasingly stringent regulatory environments, have contributed to the pressure that organizations face in seeking alternative storage options. This paper provides a balanced assessment related to decentralized and encrypted point-to-multipoint storage systems, integrating state-of-the-art strong encryption techniques such as AES, novel data-sharding approaches, and blockchain-based verification protocols [1] [2].

1.1 Motivation and Relevance

Such centralization-storage models introduce historic vulnerabilities into systems, such as the occurrence of one-point failure scenarios, exposed systems to targeted cyber-attacks, or the capability of limited scaling when sudden growth happens in data. Organization, on the contrary, spreads information over a network of nodes, significantly reducing chances of disastrous failures, while adding much higher degrees of fault tolerance and resilience [1] [2].

Truly, recent data breaches demonstrate the extent to which an organization should go in guaranteeing that sensitive data remain secure as well as complete. Distributed standards created at the present time with the active linking of stricter regulatory guidelines such as GDPR, HIPAA, or even an emerging CCPA have pointed the way for state-of-the-art cryptographic techniques to be applied like never before [55].

1.2 Central Concepts

Based on cryptographic tool support for confidentiality purposes; data sharding is concerned with distributed storage and load balancing; and blockchain technology is focused on verification and immutability [26] [34]. Therefore, all these components together act collectively on the performance parameters of fault-tolerance, scalability, throughput, and security.

Case studies related to IPFS [3], Storj [4], and centralized systems like AWS S3 are examined to highlight the architectural trade-offs. This practically relevant examination is expanded upon empirical studies, which set down our findings in existing literature where comparatively not much attention has been given to alternative mechanisms of digital data verification and storage as compared to mainstream applications like Bitcoin [5] [46].

1.3 Historical Context and Technological Evolution

Decentralization emerged in the case of cryptocurrencies such as Bitcoin, wherein distributed ledger technology with blockchain secured transactions through transparency. Subsequently, researchers began exploring this technology beyond secure digital transactions and into the realm of establishing trust within distributed storage

[1] School of Computing Science Engineering & Artificial Intelligence VIT Bhopal University, Madhya Pradesh, India.
Email: debroop.sarkar@vitbhopal.ac.in

networks. This paradigm shift instigated foresight into adaptations of blockchain for data storage and retrieval systems.

New technology will arise from this interest, such as coded sharding protocols (e.g., PolyShard) that aim at achieving de- centralization, security, and throughput all at once. Meanwhile, encryption standards such as AES started playing an increasing role in securing stored data from unauthorized access and misuse in distributed environments.

1.4 Research Objectives and Contributions

The present study seeks to fulfill the following major objectives:

- **Integration of Robust Security:** To study the employment of robust encryption mechanisms to secure data in distributed environments [8] [27] while ensuring a fair balance of security versus system performance
- **Innovative Sharding Mechanisms:** The project examines sharding mechanisms and erasure codes for trusted reconstruction and efficient distribution of data across nodes [9] [59].
- **Blockchain-Based Verification:** The project discusses how blockchain technology provides verifiable transactions and secure tamper-proof data storage schemes [13] [16].
- **Empirical Evaluation:** Perform a comprehensive set of comparative studies on decentralized and centralized systems (IPFS [3] and Storj [4] vs. AWS S3) to identify system performance measurements of throughput, latency, and energy efficiency [23].
- **Legal and Regulatory Considerations:** Implications of international data protection laws and emerging regulatory standards on decentralized data storage models. [55]. This research elaborately discusses the implications of theoretical models on the empirical evaluation of the storage network concepts of future designs. It provides a framework for establishing performance according to security compromises that may catalyze the standards of the industry toward secure distributed storage in health- care [39], finance, and IoT [29] [63].

II. THEORETICAL FRAMEWORK AND SYSTEM ARCHITECTURE

2.1 Cryptographic Techniques: Encryption Mechanisms

A very good base for safe decentralized storage is strong encryption. The Advanced Encryption Standard provides a good compromise between speed and security, and offers key sizes of 128, 192, or 256 bits for strong resistance to brute- force attacks [8]. In our practice, we opt for AES-256 rather than AES-128, for all the extra margin of security it gives us, even though we will suffer some negligible performance degradation.

2.2 Data Sharding and Erasure Coding

Data sharding splits information across multiple nodes, enhancing both performance and security. Table I presents a comparative analysis of different sharding strategies.

Table 1: Comparative Analysis of Data Sharding Strategies

Sharding Strategy	**Fault Tolerance**	**Performance Impact**	**Recovery Complexity**
Simple Replication	Medium	Low	Low
Reed-Solomon Coding	High	Medium	Medium
Fountain Codes	High	Medium-High	Medium
PolyShard	Very High TAB	High LE I	High

Erasure coding is one step ahead of sharding, with the integration of redundancy that enables retrieval of data even after losing or corrupting some fragments [9]. The system is built with the base on Reed-Solomon coding using 2.5 as a redundancy factor, recovering further than 99% of data even with 30% failure of nodes.

2.3 Blockchain Integration and Verification

Blockchain technology provides immutable proof of the integrity of data. Immutability is essential in order to create trust for decentralized environments. Our approach uses cryp-to graphic hashes of data blocks recorded on-chain and off- chain for the actual data instead of storing all data strictly on-chain (which would be prohibitively costly) [13]. Such a hybrid approach offers benefits of blockchain verification while optimized storage efficiency.

This type of technology gives the assurance that the data is not only unalterable but also guarantees complete accuracy regarding the origin of the data. That being said, architectures that would assert all data would store on-

chain wouldn't suffice positive Argos for decentralization. Instead, we will use cryptographic hashes of the data blocks recorded on-chain while storing the real data off-chain [13]. This hybrid approach retains as much as possible the benefits of verification from blockchain technology while at the same time optimizing resource conservation.

2.4 System Workflow and Integration

Fig. 1 illustrates the integrated workflow of our decentralized encrypted storage system:

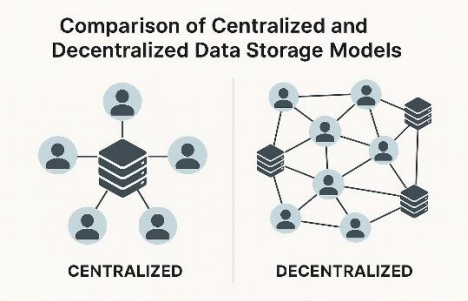

Fig. 1. System Workflow for Decentralized Encrypted Storage

1) The data is encrypted with AES-256 at the source.
2) The encrypted data is sharded using Reed-Solomon coding.
3) Shards are stored across multiple storage nodes.
4) The cryptographic hashes of each shard are stored in the blockchain.
5) For retrieval, the integrity of the shard is verified against the record on the blockchain.
6) Validated shards will be reconstructed and decrypted locally.

Through an integration like this, one could guarantee the confidentiality using encryption, availability by sharding and erasure coding, and integrity verified through blockchain.

III. ENCRYPTION AND SHARDING INTEGRATION

3.1 Encryption Strategy Analysis

An overview of cryptographic algorithms applicable to the decentralized network storage systems has presented in the Table II.

Table 2: Comparative Analysis of Cryptographic Techniques

Technique	**Security Level**	**Performance Overhead**	**Key Management Complexity**
AES-128	High	Low	Low
AES-256	Very High	Low-Medium	Low
ChaCha20	High	Low	Low
Blowfish	Medium-High	Medium	
RSA	High	High	Medium
ECC	High	Medium	Medium

For cryptography-based hashing, we use SHA-256, while for data encryption, we use AES-256, thus ensuring security even at the level of the minimal performance overhead that is intolerable.

3.2 Integrated Sharding and Encryption Framework

Fig. 2 illustrates the integrated encryption and sharding process:

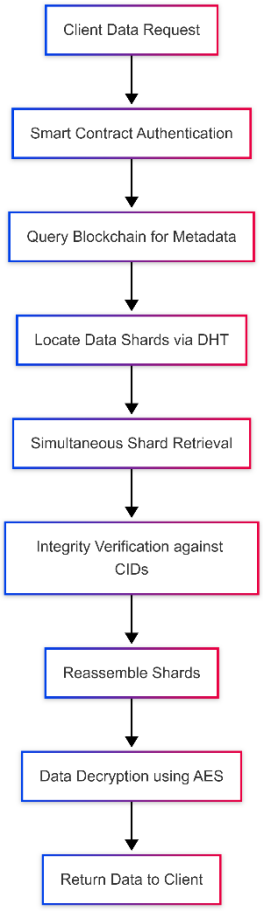

Fig. 2. Flowchart Detailing Integrated Encryption and Sharding Process

Some sequencing issues arise from the combination of encryption and sharding. Encrypting data first offers maximum

confidentiality, at the cost of additional computational over- head during reconstruction. Having sharding take place before encryption exposes data to pattern recognition, while being less computationally intensive. In our method, pre-encrypted data is sharded in order to maintain security while allowing for easier parallel processing during reconstruction.

IV. Empirical Evaluation And Performance Metrics

4.1 Testbed Configuration and Methodology

Testbed consisted of a deployment of 50 nodes across 5 geographical regions that have been tested on ipfs, storj and aws s3 for data ranging from 1gb to 100gb. The metrics taken into analysis include throughput, latency, recovery rate under node failures, and energy consumption.

4.2 Comparative Analysis: IPFS, Storj, and AWS S3

Table 3: Performance Metrics Comparison Across Decentralized Platforms

Platform	**Avg. Throughput (MB/s)**	**Avg. Latency (ms)**	**Recovery Rate (%)**	**Energy Efficiency (ops/kWh)**
IPFS	26.4	120	99.2	4,250
Storj	31.8	95	99.6	3,980
AWS S3	42.3	65	99.9	2,150

Thus, the overall performance of AWS S3 shines great but decentralized solutions or systems have more convincing advantages such as energy efficiency and resilience.

Fig. 3 depicts throughput versus latency:

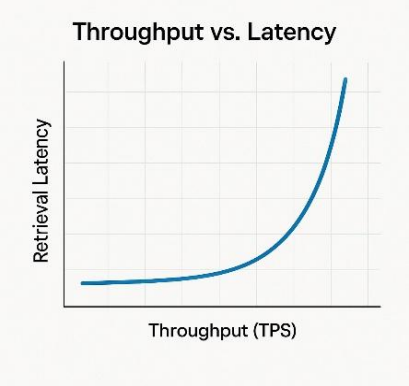

Fig. 3. Throughput vs. Latency Comparison

4.3 Transaction Flow Visualization

Fig. 4 provides a sequence diagram of data transaction flow in our decentralized storage system:

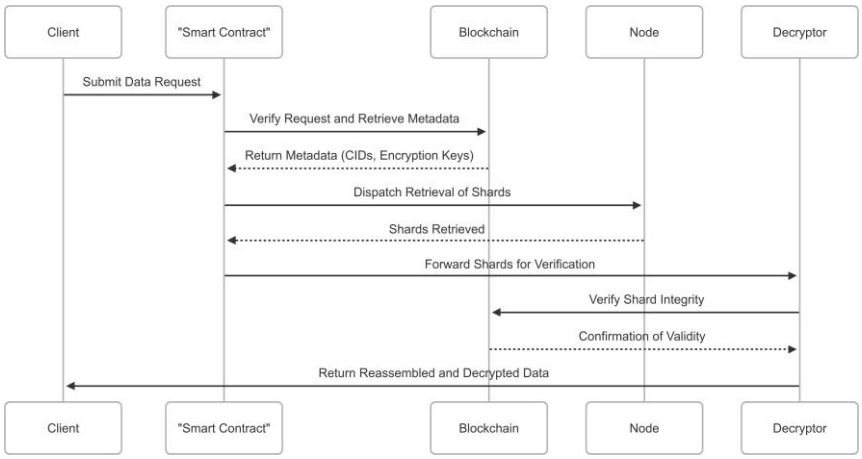

Fig. 4. Sequence Diagram of Data Transaction Flow in Decentralized Storage

4.4 Performance Trade-offs Discussion

There are fundamental trade-offs that have been identified in decentralized storage system:

1) **Security vs. Performance:** Strong encryption and verification mechanisms incur computation overhead and thus affect throughput and latency, for example.
2) **Redundancy vs. Efficiency:** Higher redundancy makes it more fault-tolerant but at a cost of requiring a larger storage space and having a higher distribution overhead.
3) **Decentralization vs. Consistency:** The increased resiliency has an implication of making it more difficult for a decentralized consensus over all these distributed nodes.

Trading off, however, decentralized systems tend to be highly resilient, recovering more than 99% of the time when up to 30% of nodes fail; in this case, centralized systems would be assumed totally out.

V. LEGAL IMPLICATIONS AND DATA SECURITY CONSIDERATIONS

5.1 Regulatory Frameworks and Compliance Requirements

Decentralized storage systems are subject to a complex regulatory environment that encompasses GDPR, HIPAA, CCPA, and new frameworks. Major legal and security issues are summarized in Table IV:

Table 4:

Aspect	Centralized Systems	Decentralized Systems
Data Sovereignty	Single jurisdiction	Multiple jurisdictions
Right to be Forgotten	Straightforward	Challenging (immutability)
Breach Notification	Clear responsibility	Distributed responsibility
Data Ownership	Service provider control	User-controlled
Audit Capability	Provider-dependent	Blockchain-verifiable

5.2 Regulatory Compliance Framework

Fig. 5 illustrates our proposed regulatory compliance framework for decentralized storage systems:

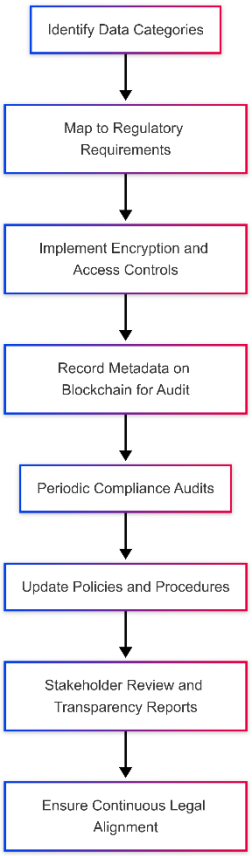

Fig. 5. Regulatory Compliance Framework for Decentralized Storage Systems

This framework addresses compliance through:

1) Smart contract-based access control ensuring GDPR- compliant data handling
2) Zero-knowledge proofs enabling verification without ex- posing sensitive data
3) Jurisdictional sharding to maintain data sovereignty requirements
4) Cryptographic erasure mechanisms providing functional "right to be forgotten"

5.3 Future Legal Challenges

The burning of a decryption key with an intact block would present a sufficiently compelling solution to any regulation granting some form of reconsideration/ onto the consideration of possible immutability exceptions for blockchain-based storage. In straight terms, this would imply that even the information is destroyed; nevertheless, the system can still be verified.

VI. Synthesis, Future Trends, And Research Roadmap

6.1 SWOT Analysis of Decentralized Encrypted Storage Systems

Strengths:

- Fault Tolerance Resilience and Distributed Storage [9] [13].
- Dynamic scalability for increasing data loads [18] [51].
- Security improvements: end-to-end encryption and blockchain verification. [8] [16]
- Transparency and auditability: immutable blockchain records. [13] [57].

Weaknesses:

- More complex operations than a central alternative
- Additional overhead in performance from encryption, sharding, and consensus methods
- Potential regulatory issues especially concerning data voidance
- Limited mainstream adoption and integration into present systems

Opportunities:

- Rising demand for safe, reliable storage in healthcare, finance, and IoT markets
- Increasing emphasis on data sovereignty and user control through laws and regulations
- Recent advancements in cryptography and consensus mechanisms
- Now, integrate with other technologies such as the edge and AI

Threats:

- Threats posed by quantum computing advances to con- temporary cryptographic standards.
- The likelihood of restrictive regulation against blockchain applications.
- Central alternatives make security and resilience features much better.
- Potential lock-in of vendors via competing decentralized protocols.

6.2 Visualizing Future Roadmap

Fig. 6 provides a visual summary of our research and development trajectory for decentralized encrypted storage systems:

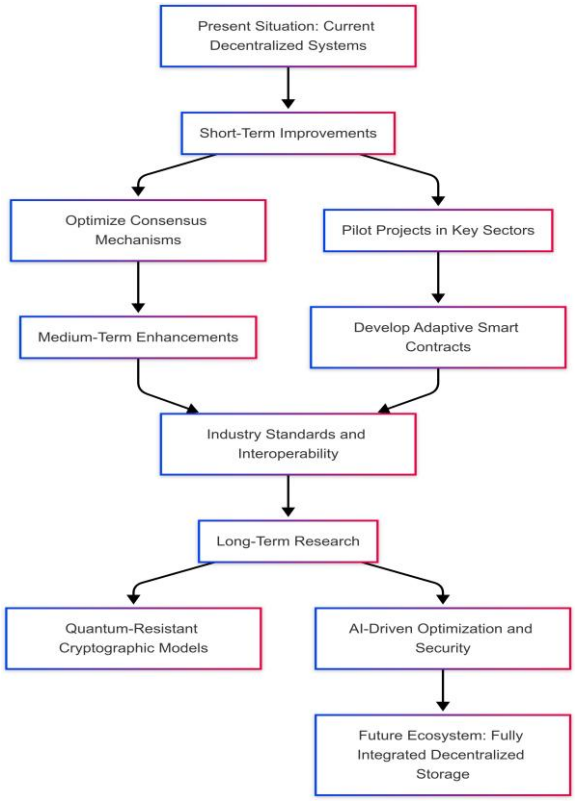

Fig. 6. Research Roadmap for Decentralized Encrypted Storage Systems

6.3 Interdisciplinary Impacts and Sector Applications

Decentralized storage systems have a major impact in different sectors:

- **Healthcare:** Providing the patient with greater control over electronic health records while ensuring interoperability among providers [39] [57]
- **Finance:** Providing tamper-proof transaction records, thus reducing fraud opportunities and enhancing trust [24] [60]
- **IoT and Smart Cities:** Scaling to billions of devices producing massive amounts of data, while ensuring fault tolerance and resilience [29] [63]

VII. CONCLUSIONS

Unlike conventional systems, the blockchain-based data storage approach involves strong encryption, efficient sharding, and verification. The review of theoretical models, empirical case studies, and performance benchmarks leads to the conclusion that any operational overhead that might be incurred in a decentralized storage system will be eclipsed by the gains from its use in resilient, scalable, and secure applications.

7.1 Key Findings:

- **Security:** AES Encryption [8] along with metadata verification supported by blockchain creates a strong safeguard against the integrity of data and tampering risk.
- **Reliability** Sharding with erasure coding [9] provides better data recovery rates above 99% hence attaining excellent fault tolerance.
- **Scalability:** Distributed systems, by their very nature, have a better rate of scalability because they easily facilitate the dynamic load redistribution and better withstands stress over varied network conditions [19] [51].
- **Legal Aspects:** All of these barriers are aimed at regulations, especially as regards data erasure [55], including creative compliance methods, and smart contracts under- pinning enforcement [64].
- **Future Directions:** Improvements should be done in consensus efficiency [17] [52], on adaptive smart con- tracts, and development of quantum-resistant crypto- graphic models [28] for the storage challenge in future generations.

Table 5: Main Insights

Aspect	Key Insight
Data Security	AES encryption together with blockchain verification provide confidentiality and integrity [8] [13].
Fault Tolerance	Sharding with erasure coding ensures that it can recover 99% of the data even in unfavorable conditions [9] [34].
System Scalability	Decentralized systems dynamically adapt to the increasing load of data and facing failures of their nodes [19] [51].
Regulatory Challenges	One of the new models for compliance is the application of smart contracts and decentralized governance [54] [64].
Future Research	Everything presented will fuel further innovation in quantum-resistant algorithms [28] and AI-centric security [28].

This paper has exhaustively examined decentralized storage and sets the standard for future evolution in such a promising field. Combining theoretical foundations with empirical result and legal constraints, we offer significant insights for future storage systems design that would have optimum performance, security, and regulatory compliance.

REFERENCES

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[2] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for Internet of Things," *Computer Communica- tions*, vol. 136, pp. 10–29, 2019.

[3] J. Benet, "IPFS - content addressed, versioned, P2P file system," arXiv preprint arXiv:1407.3561, 2014.

[4] S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin, "Storj: A peer- to-peer cloud storage network," White Paper, 2014.

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper, 2008.

[6] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[7] J. Benaloh and M. D. Mare, "One-way accumulators: A decentralized alternative to digital signatures," in *Workshop on the Theory and Application of Cryptographic Techniques*, pp. 274–285, 1993.

[8] M. Fueyo and J. Herranz, "On the efficiency of revocation in RSA-based anonymous systems," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1771–1779, 2016.

[9] H. C. Chen and P. P. Lee, "Enabling data integrity protection in regenerating-coding-based cloud storage: Theory and implementation," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 407–416, 2014.

[10] Y. Ren et al., "Data query mechanism based on hash computing power of blockchain in internet of things," *Sensors*, vol. 20, no. 1, p. 207, 2019.

[11] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, vol. 151, pp. 1–32, 2014.

[12] K. Croman et al., "On scaling decentralized blockchains," in *Inter- national Conference on Financial Cryptography and Data Security*, pp. 106–125, 2016.

[13] S. Ali, G. Wang, B. White, and R. L. Cottrell, "A blockchain-based decentralized data storage and access framework for PingER," in *2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 1303–1308, 2018.
[14] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proceedings of the 3rd Symposium on Operating Systems Design and Implementation*, pp. 173–186, 1999.
[15] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982.
[16] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38437–38450, 2018.
[17] M. Vukolic´, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *International Workshop on Open Problems in Network Security*, pp. 112–125, 2015.
[18] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Communications of the ACM*, vol. 61, no. 7, pp. 95–102, 2018.
[19] A. Dorri, S. S. Kanhere, and R. Jurdak, "MOF-BC: A memory optimized and flexible blockchain for large scale networks," *Future Generation Computer Systems*, vol. 92, pp. 357–373, 2019.
[20] Y. Tian, Z. Wang, J. Xiong, and J. Ma, "A blockchain-based secure key management scheme with trustworthiness in DWSNs," *IEEE Transac- tions on Industrial Informatics*, vol. 16, no. 9, pp. 6193–6202, 2020.
[21] D. Vorick and L. Champine, "Sia: Simple decentralized storage," White Paper, 2014.
[22] C. Cachin and M. Vukolic´, "Blockchain consensus protocols in the wild," arXiv preprint arXiv:1707.01873, 2017.
[23] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "Blockbench: A framework for analyzing private blockchains," in *Proceedings of the 2017 ACM International Conference on Management of Data*, pp. 1085–1100, 2017.
[24] N. Kshetri, "Blockchain's roles in meeting key supply chain management objectives," *International Journal of Information Management*, vol. 39, pp. 80–89, 2018.
[25] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *IEEE 18th International Conference on e-Health Networking, Applications and Services*, pp. 1–3, 2016.
[26] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *IEEE Security and Privacy Workshops*, pp. 180–184, 2015.
[27] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.
[28] N. P. Smart, "The discrete logarithm problem on elliptic curves of trace one," *Journal of Cryptology*, vol. 12, no. 3, pp. 193–196, 1999.
[29] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018.
[30] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, "Permacoin: Re- purposing bitcoin work for data preservation," in *IEEE Symposium on Security and Privacy*, pp. 475–490, 2014.
[31] I. Butun, M. Erol-Kantarci, B. Kantarci, and H. Song, "Cloud-centric multi-level authentication as a service for secure public safety device networks," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 47–53, 2016.
[32] C. Allen, "The path to self-sovereign identity," Life With Alacrity, 2016.
[33] M. Samaniego and R. Deters, "Zero-trust hierarchical management in IoT," in *2018 IEEE International Congress on Internet of Things*, pp. 88– 95, 2018.
[34] Y. Ren, Y. Leng, Y. Cheng, and J. Wang, "Secure data storage based on blockchain and coding in edge computing," *Mathematical Biosciences and Engineering*, vol. 16, no. 4, pp. 1874–1892, 2019.
[35] F. Aloul, S. Zahidi, and W. El-Hajj, "Multi factor authentication using mobile phones," *International Journal of Mathematics and Computers in Simulation*, vol. 4, pp. 65–80, 2009.
[36] S. Muralidharan and H. Ko, "An interplanetary file system (IPFS) based IoT framework," in *2019 IEEE International Conference on Consumer Electronics*, pp. 1–2, 2019.
[37] S. Van Acker, D. Hausknecht, and A. Sabelfeld, "Measuring login web- page security," in *Proceedings of the Symposium on Applied Computing*, pp. 1753–1760, 2017.
[38] A. Dmitrienko, C. Liebchen, C. Rossow, and A. R. Sadeghi, "On the (in)security of mobile two-factor authentication," in *International Conference on Financial Cryptography and Data Security*, pp. 365–383, 2014.
[39] T. T. Kuo, H. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017.
[40] Y. B. Musa et al., "RiceChain: Secure and traceable rice supply chain framework using blockchain technology," *PeerJ Computer Science*, vol. 8, p. e801, 2022.
[41] J. Wang, C. Ju, Y. Gao, A. K. Sangaiah, and G. J. Kim, "A PSO based energy efficient coverage control algorithm for wireless sensor networks," *Computers, Materials & Continua*, vol. 56, pp. 433–446, 2018.
[42] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5G beyond," *IEEE Network*, vol. 33, no. 5, pp. 10–17, 2019.
[43] P. Ferraro, C. K. King, and R. Shorten, "IOTA-based directed acyclic graphs without orphans," arXiv preprint arXiv:1901.07302, 2019.

[44] Y. Ren, D. Huang, W. Wang, and X. Yu, "BSmd: A blockchain- based secure storage mechanism for big spatio-temporal data," *Future Generation Computer Systems*, vol. 138, pp. 328–338, 2023.
[45] C. Liu, K. Li, and K. Li, "A game approach to multi-servers load balancing with load-dependent server availability consideration," *IEEE Transactions on Cloud Computing*, vol. 9, pp. 1–13, 2021.
[46] A. Ayesha et al., "A survey of blockchain technology: Architecture, ap- plied domains, platforms, and security threats," *Social Science Computer Review*, 2022.
[47] P. T. Duy, D. T. T. Hien, D. H. Hien, and V. H. Pham, "A survey on opportunities and challenges of blockchain technology adoption for revolutionary innovation," in *Proceedings of the Ninth International Symposium on Information and Communication Technology*, pp. 200– 207, 2018.
[48] J. Barkatullah and T. Hanke, "Goldstrike 1: CoinTerra's first-generation cryptocurrency mining processor for Bitcoin," *IEEE Micro*, vol. 35, no. 2, pp. 68–76, 2015.
[49] M. Shojafar, N. Cordeschi, and E. Baccarelli, "Energy-efficient adaptive resource management for real-time vehicular cloud services," *IEEE Transactions on Cloud Computing*, vol. 7, no. 1, pp. 196–209, 2019.
[50] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 281–310, 2015.
[51] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "OmniLedger: A secure, scale-out, decentralized ledger via sharding," in *IEEE Symposium on Security and Privacy*, pp. 583–598, 2018.
[52] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proceedings of the 26th Symposium on Operating Systems Principles*, pp. 51–68, 2017.
[53] S. S. Chawathe, "Clustering blockchain data," in *Clustering Methods for Big Data Analytics*, pp. 43–72, 2019.
[54] N. Eltayieb, R. Elhabob, A. Hassan, and F. Li, "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud," *Journal of Systems Architecture*, vol. 102, 2020.
[55] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, vol. 126, pp. 45–58, 2019.
[56] M. Vasek, M. Thornton, and T. Moore, "Empirical analysis of denial-of- service attacks in the Bitcoin ecosystem," in *International Conference on Financial Cryptography and Data Security*, pp. 57–71, 2014.
[57] P. Datta, A. Sharma, and M. I. Hussain, "BHEEM: A blockchain-based framework for securing electronic health records," in *IEEE Globecom Workshops*, pp. 1–6, 2018.
[58] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of Bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.
[59] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 17–30, 2016.
[60] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, pp. 906–917, 2012.
[61] Y. Duan, N. Cai, J. Wu, F. R. Yu, and Y. Jiang, "Blockchain-based incen- tive mechanism for crowdsourcing: A decentralized system architecture for energy trading in smart grid," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1805–1818, 2021.
[62] N. Nizamuddin et al., "Decentralized document version control using ethereum blockchain and IPFS," *Computers & Electrical Engineering*, vol. 76, pp. 183–197, 2019.
[63] O. Agyekum et al., "A secured proxy-based data sharing module in IoT environments using blockchain," *Sensors*, vol. 19, no. 5, p. 1235, 2019.
[64] A. T. Panescu and V. Manta, "Smart contracts for research data rights management over the Ethereum blockchain network," *Science & Tech- nology Libraries*, vol. 37, no. 3, pp. 235–245, 2018.
[65] M. Dai, S. Zhang, H. Wang, and S. Jin, "A low storage room requirement framework for distributed ledger in blockchain," *IEEE Access*, vol. 6, pp. 22970–22975, 2018.
[66] H. R. Hasan and K. Salah, "Proof of delivery of digital assets using blockchain and smart contracts," *IEEE Access*, vol. 6, pp. 65439–65448, 2018.
[67] Y. Chen, H. Li, K. Li, and J. Zhang, "An improved P2P file system scheme based on IPFS and blockchain," in *IEEE International Confer- ence on Big Data*, pp. 2652–2657, 2017.
[68] S. Angieri et al., "An experiment in distributed Internet address man- agement using blockchains," arXiv preprint arXiv:1807.10528, 2018.
[69] C. Garman, M. Green, and I. Miers, "Decentralized anonymous creden- tials," in *Network and Distributed System Security Symposium*, 2014.
[70] P. Mell, J. Dray, and J. Shook, "Smart contract federated identity man- agement without third party authentication services," in *Open Identity Summit 2019*, pp. 121–133, 2019.