NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 4, Issue – 1, June 2025
E – ISSN – 2583-7559
International Conference on Role of Blockchain
in Digital Forensics and Cyber Security - 2025

Scalable Blockchain Solutions for Digital Evidence Management: A Comprehensive Review

Shital Pathar
Research scholar,
Dept. of Computer Engg,
Dharmsinh Desai University,
Nadiad ,Gujarat ,India.

Bhavika Gambhava
Associate Professor,
Dept. of Computer Engg,
Dharmsinh Desai University,
Nadiad,Gujarat,India.

C. K. Bhensdadia
Professor,
Dept. of Computer Engg,
Dharmsinh Desai University,
Nadiad , Gujarat , India.

Abstract— **The need for secure, transparent, and immutable digital evidence has increased, as it is an essential component of criminal investigations. The integrity, transparency, and security of digital evidence are frequently compromised by the conventional system. Blockchain technology has proven to be a transformative solution for maintaining digital evidence in a secure and transparent manner. However, the application of blockchain is limited by its scalability in handling the vast amounts of digital data. To preserve large amounts of digital evidence, this paper thoroughly examines the current Layer 1 and Layer 2 scalability methods, such as sharding, state channels, and roll-ups. We have observed that hybrid scalability solutions can be employed to solve the scalability issues. In this paper, various scalability solutions and consensus mechanisms related to digital evidence are compared. This paper provides a comprehensive literature review, identifies the research gap also suggests future directions for developing scalable digital evidence management solutions.**

Keywords— Blockchain , Consensus mechanism, Scalability, Digital Forensics, Digital Evidence, Chain Of Custody, Scalability solution

I. INTRODUCTION

In today's digital world, as cybercrimes and digital frauds keep on increasing rapidly, the investigation process requires an efficient way of managing the evidence. For tracking, reconstructing, and presenting the evidence in court, the investigation committee heavily depends on digital evidence. The digital evidence must be maintained such that its integrity and authenticity are preserved. [1] The digital evidence will be used by all the committee members of the investigation. In a traditional system, the digital evidence is stored, maintained, and verified by a centralized system. [1], [2], [3] The centralized system provides various methods of storing the evidence. But it faces the problems of preserving the integrity and security of the evidence. The integrity , security, and privacy of the digital evidence can be ensured by using the blockchain technology. Digital evidence management can use blockchain by using its fundamental features. The blockchain's immutable, transparent, and distributed features can be used for digital evidence such that no one can tamper with it. The smart contract can be defined to automate the chain of custody process. [2]The smart contracts will automate the process by ensuring the security and integrity of digital evidence. The scalability problem of blockchain is due to the fast-growing volume of data. The initial proposal for blockchain was for secure and decentralized cryptocurrency. As day by day the amount of data generated by digital evidence is increasing rapidly, the key concepts of blockchain can be utilized to manage the large volume of data. [1], [2], [3]

This paper provides a thorough overview of existing research and existing scalability approaches. Section I of the paper provides an overview of blockchain technology and digital evidence management. Section II of the paper provides an overview of traditional digital evidence management process. Section III provides a detailed discussion of blockchain technology and scalability. Along with the concepts we have discussed the existing literature survey in Section IV. This paper discussed various scalability challenges in existing solutions in Section V. Section VI provides a comparison of various scalability techniques along with gap in existing research Finally, in Section VII we have given the future direction, which depicts how scalability improves the performance of existing digital evidence systems.

II. DIGITAL EVIDENCE MANAGEMENT

Digital forensics plays crucial role in identifying criminal investigations and fraud detection. The digital forensics must ensure proper handling of the digital evidence. Digital evidence refers to the information that can be used as proof for legal proceedings.[2]The source of digital evidence can be digital files like text, documents, images, videos, logs or

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 4, Issue – 1, June 2025
E – ISSN – 2583-7559
International Conference on Role of Blockchain
in Digital Forensics and Cyber Security - 2025

digital devices such as mobile phones, computer hard drives, etc. The digital forensic process consists of four stages to handle the digital evidence as shown in Fig 1. [2]

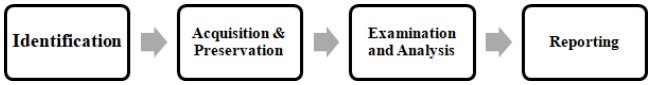

Fig 1 . Digital Evidence investigation process

The initial phase is digital evidence identification, in which the investigator identifies the type of cybercrime and recognizes the potential sources of digital evidence. The investigator collects and retains the evidence by using standard operating procedure. The evidence must guard against data loss, manipulation, or damage. [4] Forensics tools like EnCase or FTK (Forensic Toolkit) can be used. The next step in the process is examination and analysis, where the committee members retrieve, examine, and evaluate the crucial information. They can use specialized tools for investigation and must provide documentation for each step.

The investigation process must be clear , comprehensive, and lawful. The chain of custody is the methodological process of managing the digital evidence. [4]The key elements of custody include who, where, how, and how long.[4] The process includes basic information of the investigator, such as name and role, along with location and timestamp.After the chain of custody, the digital evidence is presented to the court.[4]

III. Basics of Blockchain Technology

A. Origin And Growth of Blockchain

The decentralized, distributed ledger known as blockchain securely, irrevocably, and transparently documents transactions across numerous computers. Each transaction is stored in a block ,all such blocks are connected to the previous block using cryptographic techniques which forms a chain. Due to its tamper-proof record-keeping structure, blockchain is a great choice for applications that need security, transparency, and trust.[5], [6]

The concept of blockchain was first introduced by a whitepaper published by Satoshi Nakamoto named ―Bitcoin: A Peer-to-Peer Electronic Cash System‖.[7] Nakamoto proposed a currency named Bitcoin. He proposed a platform which does not require any trust of third parties.

The cryptocurrency uses the concept of digital signature to verify the authenticity of the transaction. Nakamoto removed the need for third parties from electronic transactions. In order to check the authenticity of the transaction , the transaction is broadcasted into the public. All the nodes in a network are peer to peer connected. Each node will group transactions together which is known as a block. All nodes receive the transaction details which are yet to confirm . The Full node will then combine all unconfirmed transactions and start mining of a block. The mining is a process in bitcoin blockchain to solve the cryptographic puzzle called as proof of work.[7]The miner who is able to mine the block successfully receives the incentive. The incentive mechanism was introduced in order to increase adoption of blockchain technology. Blockchain was initially used in cryptocurrency but nowadays it receives widespread adoption in various domain like supply chain, healthcare, energy trading, identity management and digital forensic.[6]

B. Types of Blockchain

Public, private, and consortium blockchains are three types of blockchain technology as shown in Fig 2, each of which offers different types of application[6].

Anyone can join, validate transactions, and access the ledger on public blockchains, which are open, decentralized networks. Private blockchains are networks with permissions that are managed by a single person or group. Consortium blockchains are semi-decentralized networks that are managed by a number of groups working together.

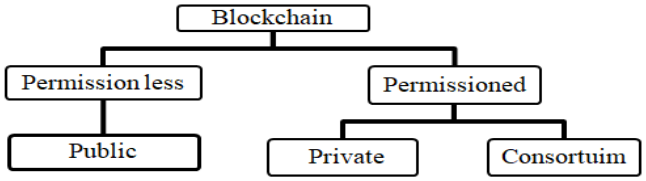

Fig 2 . Various categories of blockchain

C. Application Of Consortium and Private Blockchain In Digital Forensics

The consortium blockchain allows multiple organizations to collaborate. In digital forensics, the forensic labs, judicial bodies and crime investigator teams can use blockchain for transparent digital evidence management.

Private blockchain is suitable for one organization where the sensitive information is required to be stored like secure evidence [8] .Table I shows the trade off in various factors of blockchain.

TABLE I. Trade off in private and consortium blockchain

Factor	Private	Consortium
Security	High (single organization)	Medium (group of organization)
Scalability	High	High (limited participants)
Decentralization	Low (single organization)	Limited (group of organization)
Privacy	Very high	Moderate

D. Blockchain Scalbility

Due to the widespread adoption of blockchain technology, the number of users of blockchain systems increases extensively, creating scalability issues in public platforms (e.g., Bitcoin and Ethereum). Blockchain scalability refers to handling the growing number of transactions without compromising the performance of the system. [9] The scalability measures how well the blockchain system can maintain high throughput, low latency, and security. Scalability is an important factor in blockchain technology adoption in various industries and its practical implementation. [10], [11], [12]

After several research studies, the researchers identified a trade-off in blockchain scalability, known as the blockchain trilemma. The idea of the blockchain trilemma was first proposed by Vitalik Buterin (co-founder of Ethereum) via a blog in 2017. [12] Later on, several researchers have discussed the same idea. [10], [13], [14]

The blockchain trilemma is the trade-off between the key concepts of blockchain as shown in the Fig.3 . The trilemma was derived from the concept of the CAP theorem by Vitalik Buterin. As per the trilemma, in any blockchain system we can have at most two of the characteristics at a time, and we need to compromise the third property. For example, improving scalability by increasing the size of a block or reducing confirmation time may lead to vulnerabilities or a more centralized network. [15]

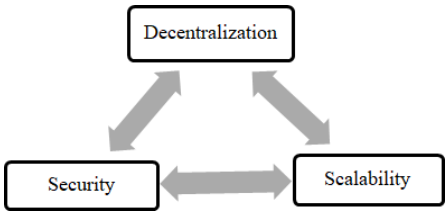

Fig 3 . Blockchain Trilemma

E. Blockchain Existing Scalbility Solutions

1 .Layer 1 Solutions

Layer 1 solutions include the improvements in existing blockchain protocol. Different approaches have been proposed so far to change the existing blockchain protocol.[15]

1.1 Sharding[16]

Sharding is the process of dividing the blockchain into smaller and manageable sections called shards. Each shard stores a specific number of transactions into a group. Sharding allows the parallel execution of transactions, which can enhance the transaction throughput and reduce the latency. Sharding enhances scalability by increasing the number of shards, thereby distributing the workload more efficiently. However, a higher number of shards can introduce vulnerabilities and may lead to a more centralized network.

1.2 Segregated Witness (SegWit)[9]

The segregated witness reduces the size of a block by separating the signature (witness) from the block. This separation of witnesses can accommodate more transactions in a block. The SegWit can increase the block size by accommodating more transactions rather than actually increasing the size of the block, while SegWit reduces the size of transactions stored in blocks, but nodes must still store the witness data. It may increase the blockchain storage requirements for full nodes that verify the witness data.

1.3 Block size compression[9], [15]

To improve the throughput of blockchain, various solutions have been proposed. All these methods try to reduce the redundant information of a block. All existing solutions are enhancing the throughput but require optimization for scalability.

2. Layer 2 Solutions

Layer 2 solutions have been proposed on top of layer 1 solution. Layer 2 solutions provide off chain transactional solution. It increases transaction throughput by reducing the load on the main chain.[17]

2.1 State Channels: [18, p. 2]

It is the off-chain mechanism that allows transaction verification without using the main chain. In state channel mechanism the private channel is created for different transactions. Only the final settlement is required on the main chain which minimizes the number of online transactions.

2.2 Sidechains[18, p. 2]

It is a separate blockchain that is connected to the main chain. The side chain is running parallel to the main chain. The primary goal of sidechain is to reduce the load on main chain.

2.3 Rollup[18, p. 2]

Rollup uses compressing techniques over layer1. The transactions are executed on off chain and after that it aggregate multiple transactions in a batch. This increase throughput and reduce transaction processing fees.

IV. RELATED WORK

This paper examines a comprehensive survey of various solution of blockchain scalability. The initial goal of blockchain was to develop a secure and decentralized network. As soon as the number of users is increasing the blockchain network is difficult to scale up. For addressing the challenge of blockchain scalability researchers first started to optimize the main blockchain network, that is known as on chain

solution. The first proposal for on chain solution was block data alternatives. J.Gobel ,A.E. Krzesinski, proposed an alternative to increase the size of block. They have tries to increase the bitcoin blockchain size which can increase the number of transactions in a block, but may have storage overhead due to large size of blocks.[19] Jeff and Garzik have shown by increasing the block size to 2MB.[20] They have shown that how larger blocks can be used to increase transaction Throughput but that may face transmission delay.[21]

Due to the limit on the size of block, E. Lombrozo, J. Lau, and P. Wuille proposed a method, SegWit(Segregated Witness) ,in which the size of the block remains the same but they have removed the witness from the main block. As per the study shown the 20% of the block consists of the metadata information related to the block, which may limit the size of block. The non-witness unit and witness unit may be equivalent to 1MB; therefore this technique is not widely adopted [22].

The first on-chain solution was introduced, called "sharding." Sharding was initially proposed in databases to optimize performance. Sharding is introduced in blockchain , where the different types of transaction are distributed across different shards; this can increase the transaction processing by concurrent execution of transactions across shards [4]. More no of shards may lead to centralization [5]; also aggregating the final result from all shards is difficult. The main challenge in sharding is cross-shard communication and inter shard communication [6] [7]. Several literature surveys have shown that sharding increases the load on the main blockchain network. [5] The paper [24] shown the optimization on cross chain Sharding using PYRAMID increased the TPS up to 3.2 times compared to other conventional approaches.

Layer 1 solutions are increasing the burden on the main chain; therefore, several off-chain solutions are proposed that work on top of layer 1 solutions. Several works, such as [6] and [9] , have shown the work done on layer 2 solutions. The Bitcoin Lightning Network was proposed by Bitcoin, which is considered an off-chain solution for Bitcoin. Ethereum 2.0 is using layer 2 solutions. The study shows that it increases the scalability of traditional conventional systems. State channel, side chain, and roll-up are considered the important innovations in blockchain.

Few surveys are also related to digital evidence, but most of them have used cloud or IoT solutions for off chain storage. The use of AES encryption for digital evidence can be utilized for tamper-proof digital evidence storage. [2] The studies shows that using IPFS storage scheme, the throughput increases. Although there is no consensus algorithm designed for digital evidence management.[19] Instead of using the decentralized storage like IPFS or File coin the layer 2 solutions can be utilized. The Layer 2 solutions are also facing the problem synchronization with the main chain.

V. SCALABILITY CHALLENGES IN BLOCKCHAIN FOR DIGITAL FORENSICS

A. Data Volume Management

Blockchain was designed for decentralization and security. The Blockchain faces several challenges for on chain storage The Block size is limited thus the large size of evidence cannot be stored into a single block.[16]Storing large amount of data includes high transaction processing cost. Uploading large amounts of data increases the latency and network congestion. Large size of data requires more storage overhead on each node , which decreases the number of nodes in blockchain. Due to less number of nodes it leads to centralization. Sensitive information requires a more secure algorithm due to privacy concerns. To overcome the problems of on chain storage the off chain storage can be used. The off chain storage reduces the burden on the main chain. Thus it increases transaction processing time which improves the throughput. Off chain storage provides scalable and secure solutions . [15]Moreover both on chain and off chain storage are having their pros and cons, for that we can use hybrid approach which can improve the scalability.

B. Transaction Throughput and Latency

The total number of transactions that can be processed per second is called Throughput. Each transaction requires a verification time. The time required to confirm the transaction and add into a block is called latency.[10], [12] In blockchain high latency and low throughput may delay the digital evidence registration process. If the transaction remains unconfirmed the evidence may be tampered with. The public blockchain like Ethereum and bitcoin demands high transaction fees for processing large transactions as shown in TABLE II. Low throughput may limit the cross border evidence sharing.

TABLE II. Constraints in Existing Blockchain

Blockchain	Consensus Mechanism	Transaction Throughput (TPS)	Average Confirmation time
Bitcoin	POW	~7 -15	10 minute
Ethereum	POW	~100-200	13-15 second
Solana	POH	~65000	2.5 second
Polygon	POS	~7000	3 second

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 4, Issue – 1, June 2025
E – ISSN – 2583-7559
International Conference on Role of Blockchain
in Digital Forensics and Cyber Security - 2025

C. Network Congestion and Block propagation

Large number of transaction may decrease the throughput and increase latency. The block size is limited to store the data. All unconfirmed transactions are present in mempool which reduces the transaction processing time. High transaction Fees are required to perform the transaction. The more congested network often increases transaction processing time which may lead to delay in evidence registration. More time required for propagation may increase the chances for an attacker to attack the data.[12], [15]

D. Storage Overhead And Node Participation

The full nodes in the blockchain are responsible for block verification. With vast amounts of data the storage requirement of full nodes increased which may increase centralization.[10], [12], [15]

E. Limitations of Consensus Mechanism

TABLE III. Limitation of existing consensus algorithm

Consensus Mechanism	**Drawback**	**Impact on Digital Evidence Management**
Proof of Work (PoW)[9], [10], [25], [26]	- High energy consumption - Low transaction throughput - Centralization risk through mining pools - Environmental impact	- Inefficient for real-time evidence management - Delayed evidence verification - High operational costs
Practical Byzantine Fault Tolerance (PBFT)[10], [25], [26]	- Limited scalability - High network overhead - Centralization risks in permissioned networks	- Not suitable for large-scale forensic networks - Risk of validator collusion - Limited geographical reach
Proof of Stake (PoS)[10], [25], [26]	- Wealth-based centralization - Vulnerable to nothing-at-stake attacks - Initial token distribution issues	- Risk of manipulation by powerful validators - Reduced fairness in evidence management - Potential security threats

F. Interoperability

If the evidence exists in different blockchain is difficult to access. This requires a cross chain mechanism. Several cross chain solutions have been proposed so far which can be used to address the problem.Polkadot ,cosmos are some of the cross chain solutions. The permissioned blockchain can be used to store the sensitive information of evidence and we can use cross chain platforms to verify the transactions.[9]

VI. Comparative Analysis and Research Gap

A. Comparative Analysis of Existing Scalability solutions

The Table IV provides a comparison of various scalability solutions along with their application in digital forensics.

TABLE IV. Comparison of existing scalability solutions

Solution	Advantage	Drawback	Application in Digital Forensics
Sharding Layer 1 [12], [16], [24]	Improve transaction throughput and decrease network congestion	Cross shard communication issues	Suitable for large scale investigations with multiple sources
Segwit Layer 1 [12]	Larger size of blocks, improve transaction processing	Limited scalability	Suitable for evidence storage with hash
State channel Layer2 [18], [19]	Reduce on chain transactions	Synchronization between layer1 and layer 2	Real time evidence management
Side chain Layer 2 [18, p.2], [19]	Customized consensus algorithm, independent processing	Security risk	Good for single region investigation
Roll Up Layer2 [18, p.2], [19]	Cost effective, reduce verification cost, increase throughput	Final transaction confirmation requires on main chain	Suitable for large scale evidence data
Hybrid approach Layer 1 and Layer 2) [3], [10]	Combine transparency and security from Layer1 and scalability from Layer 2	Trust among organization is mandatory	Good for cross border investigation

B. Research Gap

Most of the research has been done on the financial sector for improving blockchain scalability. The current research on improving the scalability in digital forensic is still a less explored area. Moreover, the current innovation for scalability solution in digital evidence management uses the

decentralized file structure (IPFS). current work does not support real time evidence management and faces scalability problems. There is no consensus algorithm developed for digital forensic.

The forensic information is sensitive information, because of this current work still faces the problem of privacy and security. However there is a lot of work that has been done on this topic, but implementing this solution at large scale still faces several challenges. The storage mechanism needs to be explored to store the digital evidence. Currently developed consensus algorithms may compromise between scalability and security. Currently there is no cross-chain solution for digital forensic. Due to the large amount of data the transaction processing fee is very high.

VII. Conclusion And Future Directions

The aim of the paper is to study the fundamental property of blockchain scalability. The paper presents existing approaches to address the scalability. The conventional blockchain for evidence management faces several challenges like throughput, latency, and storage overhead. Further integration with machine learning algorithms can be prominent to automate the verification process of digital evidence.

Further research should emphasize developing the digital evidence management that balances security, scalability, and decentralization. The private or consortium blockchain may be proposed for digital evidence management in a decentralized manner. The on-chain storage (Layer 1) and off-chain storage (Layer 2) techniques may face several challenges. Integration of Layer 1 and Layer 2 solutions can significantly increase the scalability. The various types of digital data may be stored on separate shards , which disperses the data in a decentralized way. Additionally, we can use Roll-up with sharding to minimize the on-chain processing. This may reduce the load on the main chain, subsequently increasing the scalability. The integration of machine learning algorithms can be used to analyze the block's data or anomalies. The blockchain based digital evidence management must comply with the digital forensic standard. Further research should also focus on designing the framework that must comply with legal frameworks.

Acknowledgment
The authors acknowledge their sincere gratitude to Dr. Brijesh Bhatt for his technical assistance in conducting systematic literature review and providing motivation throughout entire process.

References

[1] A. Y. V. Krishna, N. Chaudhary, and A. Muzumdar, ―A Comprehensive Survey of Blockchain Usage in Digital Evidence Handling‖.

[2] D. P. Maragathavalli, A. Rs, K. R, H. M, and S. K. S, ―SECURING DIGITAL EVIDENCE: BLOCKCHAIN AND AES -ENCRYPTION FOR TAMPER-RESISTANT DATA INTEGRITY IN CYBERCRIME INVESTIGATIONS,‖ *Int. Educ. Res. J. IERJ*, vol. 10, no. 3, Mar. 2024, doi: 10.21276/IERJ24037421355530.

[3] S. S. Alqahtany and T. A. Syed, ―ForensicTransMonitor: A Comprehensive Blockchain Approach to Reinvent Digital Forensics and Evidence Management,‖ *Information*, vol. 15, no. 2, p. 109, Feb. 2024, doi: 10.3390/info15020109.

[4] Premanand Narasimhan and Dr.N.Kala, ―Ensuring the Integrity of Digital Evidence: The Role of the Chain of Custody in Digital Forensics,‖ *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 10, no. 6, pp. 2438–2450, Dec. 2024, doi: 10.32628/CSEIT2410612443.

[5] M. Belotti, N. Bozic, G. Pujolle, and S. Secci, ―A Vademecum on Blockchain Technologies: When, Which, and How,‖ *IEEE Commun. Surv. Tutor.*, vol. 21, no. 4, pp. 3796–3838, 2019, doi: 10.1109/COMST.2019.2928178.

[6] G. Tripathi, M. A. Ahad, and G. Casalino, ―A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges,‖ *Decis. Anal. J.*, vol. 9, p. 100344, Dec. 2023, doi: 10.1016/j.dajour.2023.100344.

[7] S. Nakamoto, ―Bitcoin: A Peer-to-Peer Electronic Cash System‖.

[8] N. Xiao, Z. Wang, X. Sun, and J. Miao, ―A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things,‖ *Alex. Eng. J.*, vol. 86, pp. 631–643, Jan. 2024, doi: 10.1016/j.aej.2023.12.021.

[9] A. Hafid, A. S. Hafid, and M. Samih, ―Scaling Blockchains: A Comprehensive Survey,‖ *IEEE Access*, vol. 8, pp. 125244–125262, 2020, doi: 10.1109/ACCESS.2020.3007251.

[10] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, ―Solutions to Scalability of Blockchain: A Survey,‖ *IEEE Access*, vol. 8, pp. 16440–16455, 2020, doi: 10.1109/ACCESS.2020.2967218.

[11] P. W. Eklund and R. Beck, ―Factors that Impact Blockchain Scalability,‖ in *Proceedings of the 11th International Conference on Management of Digital EcoSystems*, in MEDES '19. New York, NY, USA: Association for Computing Machinery, Jan. 2020, pp. 126–133. doi: 10.1145/3297662.3365818.

[12] M. H. Nasir, J. Arshad, M. M. Khan, M. Fatima, K. Salah, and R. Jayaraman, ―Scalable blockchains — A systematic review,‖ *Future Gener. Comput. Syst.*, vol. 126, pp. 136–162, Jan. 2022, doi: 10.1016/j.future.2021.07.035.

[13] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, ―Blockchain and Scalability,‖ in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, Lisbon: IEEE, Jul. 2018, pp. 122–128. doi: 10.1109/QRS-C.2018.00034.

[14] G. A. F. Rebello *et al.*, ―A Survey on Blockchain Scalability: From Hardware to Layer-Two Protocols,‖ *IEEE Commun. Surv. Tutor.*, vol. 26, no. 4, pp. 2411–2458, 2024, doi: 10.1109/COMST.2024.3376252.

[15] D. Khan, L. T. Jung, and M. A. Hashmani, ―Systematic Literature Review of Challenges in Blockchain Scalability,‖ *Appl. Sci.*, vol. 11, no. 20, p. 9372, Oct. 2021, doi: 10.3390/app11209372.

[16] D. R. Kale, A. N. Jadhav, K. P. K, S. J. Salunkhe, S. Hirve, and C. Goswami, ―Sharding:A Scalability Solutions for Blockchain Networks,‖ in *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, Oct. 2024, pp. 1–8. doi: 10.1109/ICBDS61829.2024.10837088.

[17] S. Mazumdar and S. Ruj, ―Layer 2 Scaling Solutions for Blockchains,‖ in *Blockchains: A Handbook on Fundamentals, Platforms and Applications*, S. Ruj, S. S. Kanhere, and M. Conti, Eds., Cham: Springer International Publishing, 2024, pp. 261–300. doi: 10.1007/978-3-031-32146-7_9.

[18] A. Gangwal, H. R. Gangavalli, and A. Thirupathi, ―A Survey of Layer-Two Blockchain Protocols,‖ Jul. 26, 2022, *arXiv*: arXiv:2204.08032. doi: 10.48550/arXiv.2204.08032.

[19] S. Liu and Q. Zheng, ―A study of a blockchain-based judicial evidence preservation scheme,‖ *Blockchain Res. Appl.*, vol. 5, no. 2, p. 100192, Jun. 2024, doi: 10.1016/j.bcra.2024.100192.

[20] N. Singh and M. Vardhan, ―Multi-objective Optimization of Block Size Based on CPU Power and Network Bandwidth for Blockchain Applications,‖ in *Proceedings of the Fourth International Conference on Microelectronics, Computing and Communication Systems*, V. Nath and J. K. Mandal, Eds., Singapore: Springer, 2021, pp. 69–78. doi: 10.1007/978-981-15-5546-6_6.

[21] J. Garzik, ―Block size increase to 2MB,‖ *Bitcoin Improv. Propos.*, vol. 102, 2015, Accessed: Mar. 30, 2025. [Online]. Available: https://soapbox.nskelsey.com/res/Crypto-Cabal-L21.pdf

[22] E. Lombrozo, J. Lau, and P. Wuille, ―Segregated witness (consensus layer),‖ *Bitcoin Core Dev. Team Tech Rep BIP*, vol. 141, 2015.

[23] D. R. Kale, A. N. Jadhav, K. P. K, S. J. Salunkhe, S. Hirve, and C. Goswami, ―Sharding:A Scalability Solutions for Blockchain Networks,‖ in *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, Oct. 2024, pp. 1–8. doi: 10.1109/ICBDS61829.2024.10837088.

[24] Z. Hong, S. Guo, and P. Li, ―Scaling Blockchain via Layered Sharding,‖ *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3575–3588, Dec. 2022, doi: 10.1109/JSAC.2022.3213350.

[25] S. Liu and Q. Zheng, ―Research on Blockchain Consensus Mechanism for Judicial Depository Applications,‖ in *2023 3rd International Conference on Electronic Information Engineering and Computer Science (EIECS)*, Sep. 2023, pp. 913–918. doi: 10.1109/EIECS59936.2023.10435415.

[26] M. Lusetti, L. Salsi, and A. Dallatana, ―A blockchain based solution for the custody of digital files in forensic medicine,‖ *Forensic Sci. Int. Digit. Investig.*, vol. 35, p. 301017, Dec. 2020, doi: 10.1016/j.fsidi.2020.301017.