ISSN: 2182-2069 / E-ISSN: 2182-2077

Zero-Knowledge Proof (ZKP) Techniques Within Blockchain Technology

K.N. Unnikrishnan[1*], and P. Victer Paul[2]

[1*]Department of Computer Science and Engineering, Indian Institute of Information Technology, Kottayam, Kerala, India. kalleli@gmail.com, https://orcid.org/0000-0003-4389-5564

[2]Department of Computer Science and Engineering, Indian Institute of Information Technology, Kottayam, Kerala, India. victerpaul@gmail.com, https://orcid.org/0000-0001-9607-1409

Received: March 08, 2025; Revised: April 17, 2025; Accepted: May 15, 2025; Published: May 30, 2025

Abstract

Distributed trust systems have been transformed by blockchain technology; however, scalability and privacy preservation remain major obstacles. Blockchain-based ridesharing platforms, which provide decentralization, privacy, and enhanced user control inside the system, have been offered as a solution to these problems. Blockchain-based ridesharing services have scaling problems in spite of these benefits. These systems' performance declines with an increase in users, which restricts their usefulness in high-volume marketplaces. To overcome these constraints, this study investigates how blockchain topologies can use zero-knowledge proof (ZKP) approaches. We provide a thorough examination of the current ZKP implementations in blockchain systems, such as zk-Rollups and Bulletproofs, assessing their theoretical underpinnings, real-world uses, and performance indicators. Our study shows that although ZKP integration can increase throughput through rollup technologies and greatly improve privacy guarantees, computational overhead and implementation difficulties continue to be obstacles to broad adoption. Provide a framework for ZKP integration that is tailored to balance privacy, scalability, and usability. This could move blockchain technology closer to more useful real-world applications.

Keywords: Blockchain Technology, Zero-knowledge Proof, Blockchain Trilemma.

1 Introduction

A blockchain (BC) is a data format that can be shared and replicated by group members that are spread out throughout a network. As a result, the word "Blockchain" is also commonly used to refer to the system and protocol that manages this type of distributed data (Hasnaoui et al., 2025). The main feature of a BC is that its members can alter the distributed data structure (i.e., transact) even if they don't trust one other. Because of this, BC also operates without a trustworthy clearinghouse, mediator, or authority, and participants are still guaranteed that the transaction has been accepted by the members (Stephan et al., 2025). Blockchain is a decentralized, immutable distributed digital ledger that maintains assets or transactions (Andersson & Bergström, 2025).

When compared to the existing approaches, blockchain promises to increase the effectiveness, precision, and security of public, governmental, and social services (Alharbi & Alabdulatif, 2023). Based

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 926-941.
DOI: *10.58346/JISIS.2025.I2.061*

*Corresponding author: Department of Computer Science and Engineering, Indian Institute of Information Technology, Kottayam, Kerala, India.

on their use and application, blockchains can be categorized into three generations: 1.0, 2.0, and 3.0 (Gokulakrishnan & Sinha, 2025). Bitcoin and Litecoin belong to the first generation of cryptocurrencies, which are believed to be the most popular and well-known (Huang et al., 2024). The second generation of blockchain technology uses smart contracts in a wide range of decentralized apps (DApps), including crowdfunding, autonomous organizations, land management, philanthropy, and many more (Gogol et al., 2025). Blockchain deployment in public sectors and industries is referred to as third-generation applications, which explore how blockchain interacts with the real world and employ the Internet of Things (IoT) (Gajmal & Udayakumar, 2021). Data management and storage are being revolutionized by blockchain technology (Moreau & Sinclair, 2024). Data may be managed over computer networks without a central authority thanks to blockchain, a decentralized distributed ledger system with built-in security and transparency characteristics (Alizadeh et al., 2020). Every transaction in a sequence of cryptographically connected blocks is recorded in an immutable log, ensuring a high level of network resilience and data integrity.

The system uploading the required certificates to a distributed database known as a blockchain is the responsibility of the certificate supplier (Chlaihawi, 2024). Work: A blockchain document check system was developed using the aforementioned technologies (Figure 1). The ability of dispersed networks, like blockchain, to execute numerous transactions quickly is referred to as scalability (Habib, 2025). To appropriately define this blockchain attribute, two measurements are needed. (i) throughput, or how quickly transactions are completed on the blockchain, and (ii) memory needs. These two elements are interrelated and work together to make blockchain networks more scalable (Gogol et al., 2025). For instance, increasing the block size is necessary to boost a blockchain-based system's throughput because each block needs to store more transactions (Huang et al., 2024). Unfortunately, issues with bloated memory arise when the block size is increased. Because of this problem, sending a specific block to the network for verification and storage takes a long time. Because the block size is expanded to accommodate more transactions, the process ultimately slows down (Wen et al., 2024). Additionally, as it gets harder for recently connected nodes to duplicate the complete main register to the system, the blockchain's overall size grows. For example, the current size of the Bitcoin blockchain is around 386 GB, and all users who are ready to join this network must download the entire ledger data, which usually takes 240 hours (Wang et al., 2023).

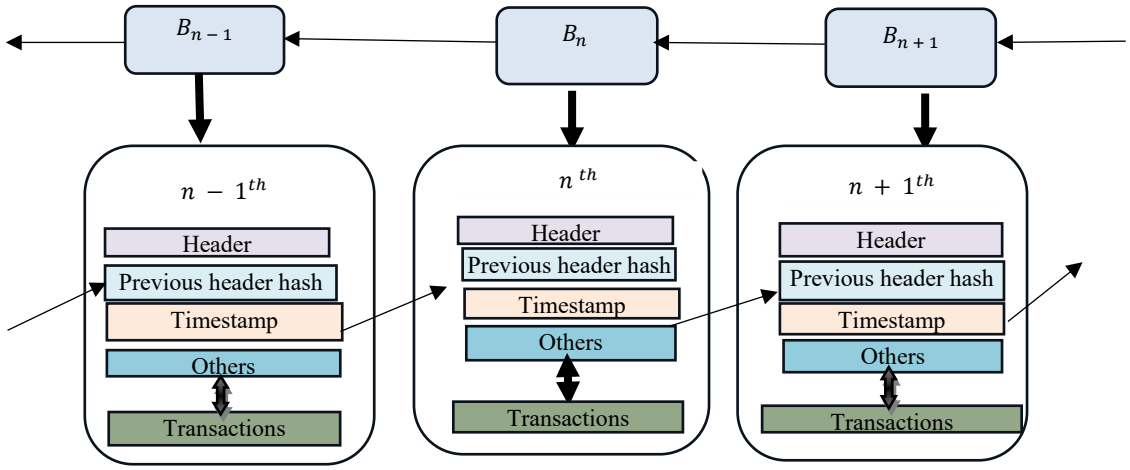


Figure 1: Traditional Blockchain Design

Assume that we reduce the adverse consequences of raising the block size to transaction per second (TPS). In this scenario, the network's miners should be fewer in number, as should the number of participating nodes. The ultimate goal of this is to centralize the system.

Table 1: Methodologies and Contributions to the Blockchain Trilemma comparison

Study	Formal Proof	Consensus-Agnostic Framework	L2 Compatible	Addresses Full Trilemma
Namasudra & Sharma, 2022	✗	✗	✗	✗
Makhdomi & Gillani, 2025	✗	✓ (Conceptual)	✗	✗
(Melo et al., 2025)	✓	✗(PoW Limited)	✗	✗
(Stephan et al., 2025)	✗	✗	✗	✗
Our Method	✓	✓	✓	✓

The approaches and contributions of the work that was presented, along with its benefits and drawbacks with regard to handling the blockchain trilemma, are compiled in Table 1. Though there is frequently no consensus tag frame, compatibility with Shift-2 solutions, or full address for Tri-Lemas, prior research has yielded useful insights through empirical analysis, theoretical models, or conceptual frameworks (Tokkozhina et al., 2023). Our approach incorporates Shift-2 compatibility considerations and offers comprehensive formal details on the consensus mechanism that fully manages the three LEMAs (Konkin & Zapechnikov, 2023). They are perfect for facilitating and encouraging dubious transactions in many locations because to their manipulability and the invariance of national transition. For necessary and intelligent contracts, deterministic implementation is crucial. This depends only on the entry and the state of the blockchain at the moment. Reliable decision-making and preventing unforeseen repercussions depend on this predictability. The "Blockchain - Absent Triangle" or "Blockchain Trilemma" (Tokkozhina et al., 2023) idea suggests that blockchain technologies are unable to simultaneously attain the best possible scalability, decentralization, and security. This trirema summarizes the main issues that blockchain systems confront, as seen in existing implementations and industry practices, however it is not official proof of blockchain architecture (Dallal, 2024). Not all three categories apply to blockchain systems. The majority of blockchain systems have historically placed a higher priority on security and decentralization than on scalability (Gangwal et al., 2023), which severely restricts performance. Like other distributed systems, blockchain systems must account for availability, consistency, and the CAP-Theorem. Depending on the situation, these systems must balance scalability, decentralization, and security. Scalability is always regarded as the most crucial element and shouldn't be compromised. Our work's most significant contributions are:

- To create and assess a new, low-complexity off-chain scaling protocol to enhance Blockchain's performance in terms of resource usage and computational complexity
- To examine the benefits and drawbacks of Ethereum and Bitcoin in terms of scalability and performance by weighing the trade-offs suggested by the trilemma of decentralization, security, and scalability.
- To create and implement a more advanced, lightweight method for Zero Knowledge rollups.
- Designing a method to apply parallelism in the execution of off-chain transactions to be validated on the main chain, as well as analyzing and assessing the technique's performance in terms of scalability, computational complexity, and resource consumption

- To suggest a methodology that combines the distributed execution of off-chain transactions with the scaling advantages of improved lightweight techniques.

2 Related Work

Additionally, during the past ten years, blockchain's rise has been increasingly dynamic. Inspired mostly by blockchain features like security, decentralization, immutability, confusion, and anonymity as a pseudonym, they have even started in other recent domains (such the energy sector (Namasudra & Sharma, 2022)). The first is the number of transactions per second (TPS) and the cost of these transactions if the blockchain is highly decentralized. It is common practice to discuss the trinity of security, decentralization, and scalability (see Surya Viswanathan (Shivers et al., 2021)). Since 2019, rollups have become more and more popular as a practical way to address issues that come up when using blockchain.

ZK, or rollup with zero knowledge, has gained popularity as a way to scale blockchain systems. By combining layer 2 transactions and sending them as a single stack to a layer of a single blockchain, this improves transaction throughput and lowers costs. However, a significant element of ZK-rollups is the computational burden on the development of effectiveness results, which poses significant performance and decentralization difficulties (Baza et al., 2021). The existing approach restricts the scalability and decentralization of rollup systems by relying on a centralized infrastructure to carry out mathematical activities. In order to outsource computations to faulty raw material hardware used by a variety of small firms, this article suggests a prober orchestration layer (Makhdomi & Gillani, 2025). Use numbers to demonstrate the transaction stack of well-known ZK rollups. Community evidence demonstrates that services are achievable and, in certain situations, better than current centralized deployments, thanks to experimental evaluations. Our findings demonstrate that systems with modest hardware configurations can still function as well as central solutions. In other words, evidence from the community supports affordable and useful substitutes. Both rollup operators and community members have demonstrated that the cloud allows them to employ hardware to save infrastructure costs for their idle communities, and Community-Prover receives payment for their efforts.

The scalability perspective is not addressed in the polygon experimental testing reported in Chemaya and Liu's work. To the best of our knowledge, this paper is the first systematic investigation to conduct the most widely used one-year experimental analysis through the short- and long-term impacts on Ethereum Layer 2 systems, main chains, and transaction volumes. It provides an overview of how our study is contrasted with and enhanced by earlier studies. Our investigation demonstrates how a specific Layer 2 system affects user behavior and the main chain (i.e., how its state is synced with the main chain) (Melo et al., 2025). Although this isolates the Layer 2 system and accounts for the synchronization costs without viewing them as the primary chain, some Shift 2 plans assert that they can process thousands of transactions per second.

3 Materials and Methods

The Layer 2 is gathered from smart contract address for every system I had chosen. Next, we identified all main chain transactions across the whole Ethereum blockchain for a certain time period that Layer 2 deposits, drawers, control points, and other maintenance procedures matched. The process is loaded to the rollup level in the suggested model. A two-layer structure serves as the foundation for the suggested system. The roll-up layer is implemented as a ZK-Rollup, and this is the fundamental layer utilized by the Ethereum main set. The core infrastructure of the suggested paradigm, which offers distributed

systems and security, is the base layer that houses Ethereum Main set. It is made up of Ethereum-based intelligent contracts that carry out trust-dependent operations at slower execution speeds. This layer creates a secure network by using a variety of knots and Ethereum's consensus process. User registration and identity management are two of the Basic Layer's primary responsibilities. Upon joining the site, new users' identities are safely registered on the Ethereum blockchain. This procedure entails modifying public keys and generating a unique user identification.

3.1. Enhanced lightweight technique for Zero Knowledge rollups

The foundation of ZK-Rollups is evidence of zero knowledge, a cryptographic approach that enables the statement to be verified by a third party (verification) without revealing the statement's authenticity. The rollup operator builds a ZK-SNARK, which stands for zero knowledge with respect to the arguments of non-interactive knowledge, in order to provide proof. The definition of an arithmetic switch or rank-1 limiting system (R1CS), which denotes the logical procedures necessary to verify each transaction in a batch, is one example of this. A circuit is a comprehensive schematic of the computations needed to verify transactions, including logic and arithmetic checks.

The roll-up intelligent contract is shown on the blockchain along with supporting documentation. Without actually doing the transaction stack proofs, checking ensures that they answer correctly and is arithmetically efficient. This is accomplished using a review key that is generated during a trustworthy see Figure 2: ZK Rollups Techniques. It enables the smart contract to verify the proof's validity within a predetermined window of time. Transactions are verified on the stack in this manner. By using ZK rollups, you may increase the scalability of your blockchain network while maintaining decentralization and security. The network can handle a high volume of transactions without compromising system security and performance because to its capacity to compress and verify transaction stacks. ZK-Rollups is a Layer 2 scaling solution for blockchains like Ethereum that greatly lessens the computational strain on the main chain by processing transactions and stacking out-of-chain without the need for proof of knowledge. It allows for quicker and less expensive transactions while maintaining the integrity and decentralization of the underlying blockchain (Figure 2).

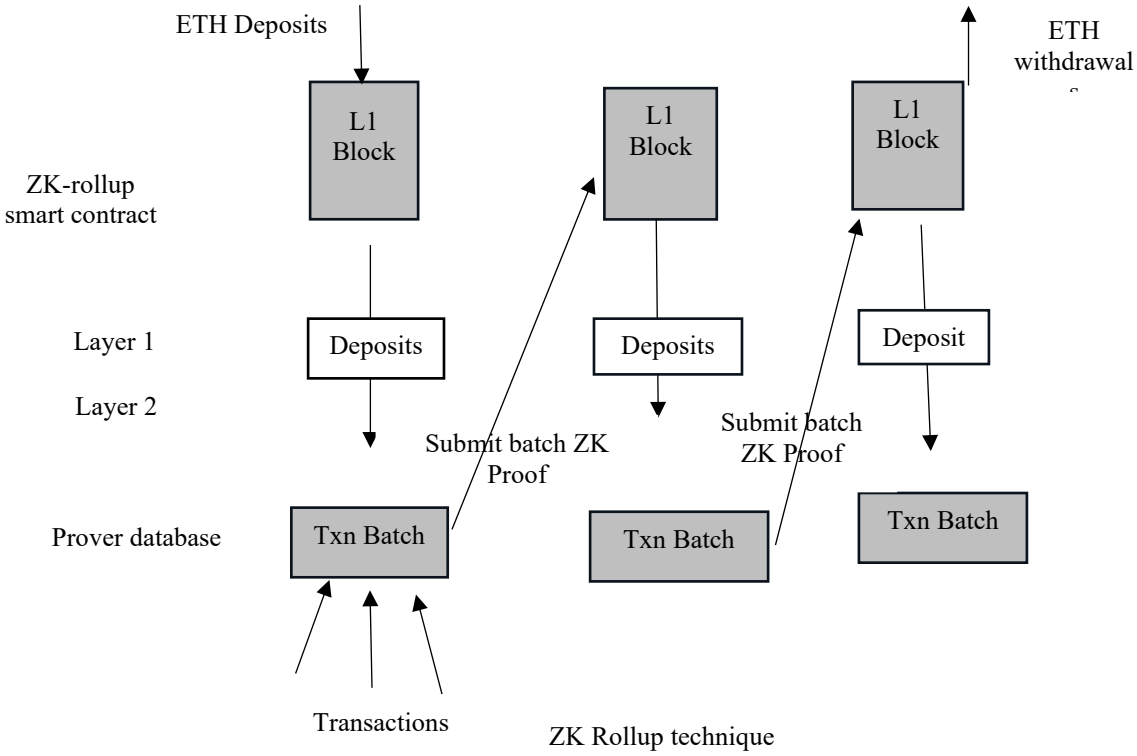


Figure 2: ZK Rollups Techniques

Additionally, the protocol functions as follows if the proof can only be verified by a certain verifier V1:

$$\forall a \in P, KeyGen(1\lambda) \rightarrow (\rho_{va}, t_{va}) \quad (1)$$

$$(P^k V_a, CHVa, \rho_{va}) \rightarrow Gen(1\lambda) \quad (2)$$

$$P_{va} \leftarrow (P^k V_a, CH_{va}, \rho Va) \quad (3)$$

The prover must employ CH in the commitment phase in order to permit a collision. Verifiers are also aware of the case tower's hashing capabilities, but the trap door button is unknown to outside parties.

$$blockchain\_Proof = Prove(Params, blockchain\_Proof\_Object) \quad (4)$$

$$Is\_Blockchain\_Proof\_of\_Valid = Verify(Blockchain\_Verification\_Params, Blockchain\_Address, blockchain\_Proof \quad (5)$$

where verify is the zk-rollups evidence verification feature designed for identity sharing on blockchain.

$$Verify(VerificationKey, stmt, \pi) \rightarrow \{0,1\} \quad (6)$$

The actual process of generating the proof:

$$P(S_p,) = x, \omega) \rightarrow \pi \quad (7)$$

The aggregated proof can be represented as:

$$\pi_{agg} = P_{agg}(\{(S_p, x_i, \omega_i)\}, i = 1 \ldots\ldots\ldots n) \quad (8)$$

During the verification of the aggregated proof, the function V_{agg} is used, which takes as input the aggregated proof, public inputs, and verifier parameters Sv :

$$V_{agg}(S_{v,}\{x_i\}, i = 1..n,)\pi_{agg}) \rightarrow \{accept\ or\ reject\} \quad (9)$$

3.2. ZK-Rollups

ZK rollups are used to ensure security and decentralization while improving the scalability. For a decentralized ridesharing platform that prioritizes scalability and user confidence, ZK rollups are superior to existing scaling solutions like sharding, sidechains, and optimistic rollups due to their security and instant finality, even though their complex proof generation process results in higher computational costs. On the other hand, XK-Rollups require that the layer-2 service deposit a security amount into the main chain's smart contract. Every time a transaction occurs in the layer-2 architecture, the resultant state and the raw transaction information are communicated on the main chain. This method keeps storage on the main chain while moving user interactions and computational costs (such as processing transactions) to layer-2. As a result, there is a continuous relationship between layer-2 transactions and main-chain storage. To do this, a smart contract on the main chain is used to store the security deposit, raw transaction data, and layer-2 state. If a user or other outside party detects any wrongdoing, the smart contract runs the raw transaction data and compares it to the public layer-2 state.

3.2.1. ZK-Rollups scalability

Scalability is addressed via ZK-Rollups, which use ZKPs to ensure security while shifting computation and state storage off-chain:

1. Batching transactions with concise validity proofs.
2. Notable increases in throughput (100–2000x, depending on implementation).
3. Immediate finality following verification of the proof

zkSync, StarkNet, and Loopring are notable implementations that use various ZKP systems and optimization techniques.

3.2.2. Validium and Volition Systems

ZKPs are used for validity in these hybrid techniques, although the solutions for data availability vary:

1. Validium: Requires data availability committees but maximizes throughput by storing data off-chain.
2. Volition: Gives consumers the option to store each transaction's data either off-chain or on-chain.

These solutions demonstrate how ZKP integration can be tailored to meet certain blockchain needs.

3.3. Blockchain Scalability

There is ongoing discussion regarding the definition of "scalability" in relation to blockchain. These days, most individuals divide the notions of scalability into two main categories. According to one school of thought, scalability encompasses a wide range of elements, including latency, throughput, data storage requirements, and other system parameters. Blockchain scalability is thought to reflect a system's improved performance when more participants (nodes) join, without impairing the system's overall performance, according to studies like. Layer-2 systems have been proposed as a possible remedy to the throughput issues observed in permissionless blockchains. Because deposits and withdrawals

necessitate frequent interactions with the main chain, the frequency of these transactions has a substantial impact on the systems' performance. Currently, it seems that no subsystem or application promotes users to avoid main-chain transfers and retain their assets solely in a single layer-2 system. Because of this, the majority of layer-2 systems often provide significantly poorer security assurances.

1 **Scalability Issues with Public Blockchains:** Scalability issues plague public blockchains such as Ethereum. Block size limitations, network congestion, and high transaction prices during peak hours are the causes of these problems. Consequently, these obstacles hinder the wider implementation of blockchain technology for real-world uses, particularly those requiring rapid processing and reaction times.

$$Scalability = \frac{SXN_B}{S_B} \tag{10}$$

$$= \min\left(\frac{N_{L2B}}{S_{L2B}}, \frac{\min\left(N_{Batch}, \frac{L_{Gas}}{C_{Gas}}\right)}{S_{Batch} + S_{ZKP} + S_{L1BU} + S_{NetL} + S_{VZKP} + S_{F1} + S_{Rollback}}\right)^{S_{Optimized}} \tag{11}$$

2 **zk-Rollup Solutions and EIP-4844:** By combining transactions off-chain and sending compressed proofs to the main blockchain for validation, zk-rollup solutions—such as those suggested in Ethereum Improvement Proposal (EIP) 4844—seek to address scalability issues.

$$(\pi, x) \leftarrow Prove(C, \omega), 0{,}1\ Verify(C, x, \pi) \tag{12}$$

However, zk-rollups use validity proofs to tackle the decentralization problem. These small bits of information verify that transactions have been handled correctly by the rollup operator. We concentrate on the intricate process of developing these validity proofs and how to decentralize it. Creating a validity proof requires a lot of resources and usually requires a lot more processing power than carrying out transactions. A variety of computing activities, each requiring specialized hardware, are part of the evidence generating process. Some activities can be completed in parallel and benefit from GPU support, while others require a lot of memory or a powerful CPU, depending on the proving system being used.

3.3.1. Decentralization (D)

Decentralization shows how all network participants share authority and decision-making. A highly decentralized system increases strength and fairness by preventing one person or a small group of people from holding excessive power:

$$D(N) = \frac{1}{n}\sum_{i=1}^{N} \blacksquare p_i \tag{13}$$

where p_i, which ranges from 0 (no participation) to 1 (full participation), is the node i's participation level. It displays the node's level of involvement in network functions including transaction validation and consensus. We explain it as follows because this may be used to any agreement or system. We define it as the most connections a node can have in our context.

$$p_{i=}\frac{Degree\ of\ Node\ i}{Maximum\ Possible\ Degree} \quad (14)$$

3.3.2. Layer-2 Solutions

By managing transactions outside of the primary blockchain, they hope to increase speed and scalability. By reducing the burden on the main chain, this method preserves decentralization and security while resulting in faster processing times. Considerations including scalability, security, efficiency, and privacy are critical when evaluating Layer-2 solutions. Using techniques like commit-chains, which aggregate transactions off-chain to increase scalability even if this may result in some delays, these solutions excel in environments that require fast transaction processing and low latency. By requiring bonds or collateral to preserve transaction integrity during off-chain processing and depending on the main blockchain to settle any disputes, they provide robust security. One significant advantage is privacy, which permits transactions to be partially concealed from the general public. However, the degree of privacy varies depending on the particular Layer-2 technology being employed. Furthermore Layer-2 solutions improve operational efficiency by reducing expenses and processing times through governmental and payment channels.

Algorithm 1: Initiation of L2 layer off-chain
1. SCmain.deploy () is the first
2. L → list of users that want to take part in L2
3. While L eq EMPTY do
4. USER.L2account = {account. Pub key x, account. Pub key y, account. balance, account. nonce, account. Token type}
5. create (USER.L2address)
6. USER.L1balance → (USER.L1balance − account. balance)
7. USER. Locked fund ← account. balance
8. L1TXNS ← Fund Lock (USER)
9. finish when
10. SC verifier. Deploy ())

Layer-2 solutions can be used in a variety of domains outside of financial transactions, including supply chain management, healthcare, and the Internet of Things (IoT). These technologies improve supply chain transparency and efficiency, which are essential for logistics management and product authenticity verification. However, despite all of its advantages, Layer-2 solutions face difficulties include ensuring smooth synchronization with the main blockchain, managing off-chain computations, and preserving data integrity. To solve these problems, which sometimes need major improvements to the current infrastructure to enable compatibility and effective operation, strong technical solutions are required. As these technologies mature, future advancements in Layer-2 solutions will likely concentrate on improving scalability, security, and the appropriate ratio of decentralization. Wider acceptance will depend on improving encryption techniques and making integration with existing blockchain systems easier. It is anticipated that these advancements would significantly increase functionality and efficiency across a range of industries, encouraging wider adoption and use of this ground-breaking technology.

3.3. Scalability (C)

This feature is necessary for blockchains to be extensively adopted and support practical uses. Throughput and latency are the two primary metrics we use to understand scalability. A method known as polynomial interpolation, including Lagrange interpolation, is used to derive these. Once we have these polynomials, we compute h(x) and t(x), which are defined by:

$$(\sum_{j=1}^{n} s_j p_j(x_i)).(\sum_{j=1}^{n} s_j q_j(x) - (\sum_{j=1}^{n} \sum_{j=1}^{n} s_j r_j(x)) \quad (15)$$

where t(x) = (x − 1)(x − 2). . .(x − m).

Data collections that are substantially larger than what memory can normally manage are encountered by today's information technology. There is still a need to analyze these massive data sets despite the lack of computational capability. A segmentation technique was developed to overcome this difficulty, dividing large databases into manageable chunks (partitions) that may be controlled by a single database instance (server). Various criteria, like popularity, date, location, and price range, might influence how these partitions are made.

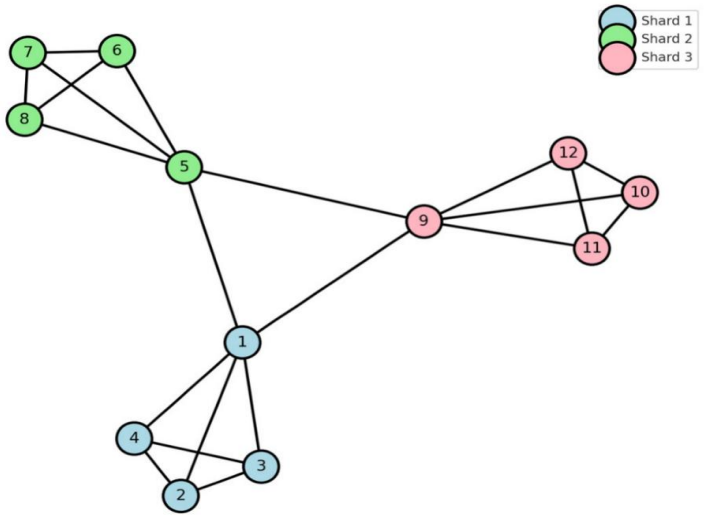


Figure 3: A network of 12 nodes sharded into three shards

One important factor is decentralization. With ns=NS nodes in each shard, a sharded network divides into S shards. Figure 3 above depicts a network with three shards, each of which has four nodes. The shards are connected to guarantee network-wide connectivity. Since segmentation does not ensure that portions operate independently, sharding makes sense after segmentation. If one server dies, the data it contains is rendered inaccessible (Figure 3). The process of dividing a database into discrete sections, or shards, and having a separate database instance run each part is known as sharding. This method not only solves fault tolerance problems but also increases throughput by enabling multiple processors to handle tasks in parallel.

1. Throughput (T): This is the quantity of transactions that are handled in a second (TPS). For real-time applications to handle a high number of transactions, high throughput is necessary.
2. Latency (L): This is the duration required to validate and finish a network transaction. Low latency is necessary to ensure quick transaction processing and a flawless customer experience.

However, establishing throughput and latency alone is insufficient; criteria that establish the desired performance must also be included for scaling to be meaningful:

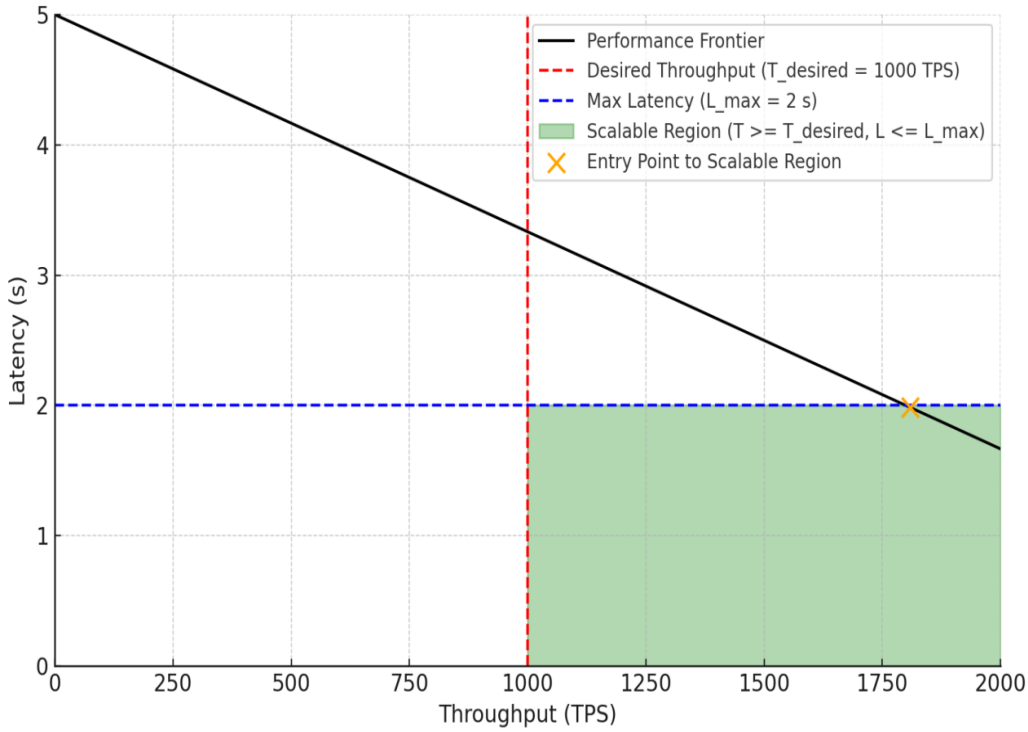


Figure 4: Blockchain performance frontier

To better understand how throughput and latency interact to determine scalability, look at the graph in Figure 4. The figure's performance frontier (black line) displays the optimal trade-offs between throughput (T) and latency (L) for various system configurations. The vertical red dashed line marks the desired throughput threshold ($T_{Desired}$), and the horizontal blue dashed line indicates the maximum acceptable latency (L_{max}). The shaded green region to the right of $T_{Desired}$ and below L_{max} highlights where both conditions are met, signaling the system's scalable operating range. This example not only demonstrates that the system can maintain an acceptable latency while achieving the required throughput, but it also shows how close the current configuration is to reaching and maintaining the ideal scalability zone.

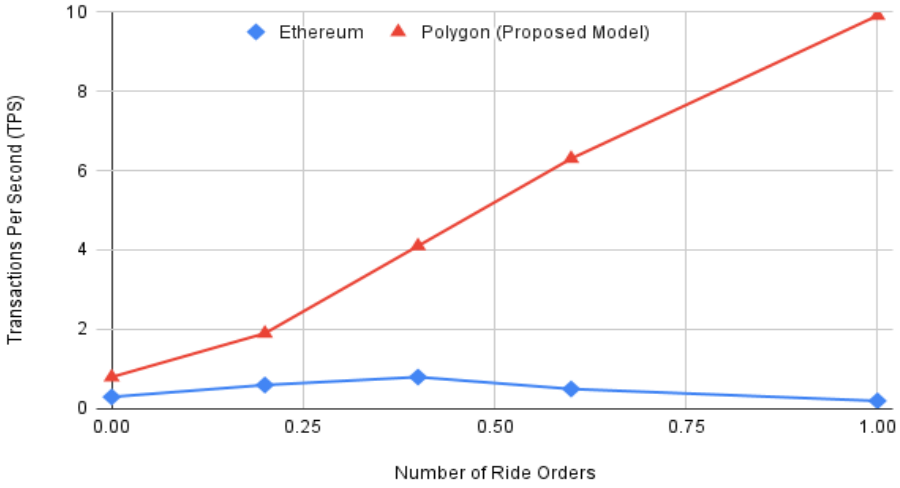
3 Result and Discussion

The Polygon zk EVM, a zero-knowledge scaling platform that integrates easily with Ethereum, is where we have deployed our approach. We used the Sepola test network to evaluate the efficacy of current models (Andersson & Bergström, 2025; Namasudra & Sharma, 2022, which run on Ethereum test networks. We used Polygons can and Ethers can, developer APIs that guarantee transparent access to blockchain data from their respective networks, to monitor and record the transactions for both our model and those that already exist. In our approach, the rollup operator maintains control over certain verification activities while delegating others to community members. Each task's orchestration remains centralized under the rollup operator in our suggested method. However, our partially decentralized solution allows community members to contribute processing power, which is advantageous to the rollup operator as well as the players.

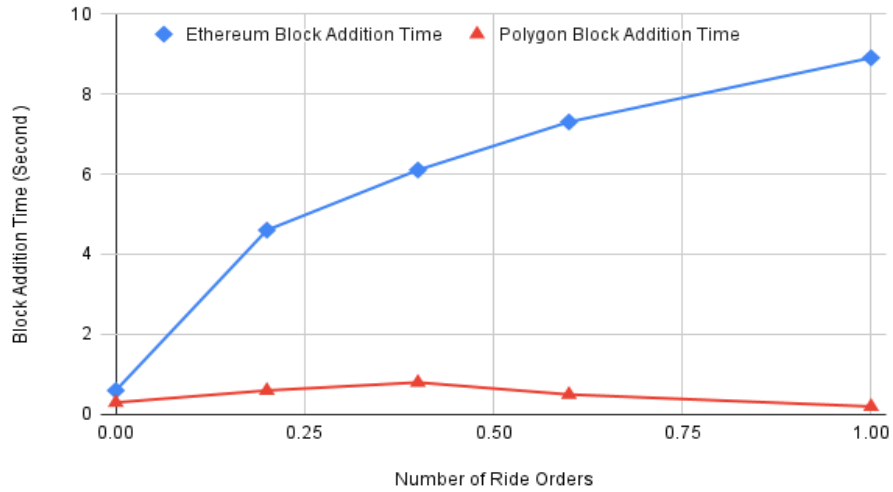
Table 2: Transaction Data Size (in bytes)

Field	Ethereum transaction	Rollup
Nonce	1 — 32	0
Gas Price	1 — 32	0.5
Gas Limit	1 — 32	0.5
Recipient	21	4
Amount	1 — 32	0.5

Unlike Rollups and ZK-Rollups achieve zero-knowledge by using hash functions instead of elliptic curve encryption. Finally, as seen in Table 2, it is usually several orders of magnitude greater.



a)



b)

Figure 5: Comparison of (a) Transaction Throughput and (b) Block Addition Time

The transaction throughput (TPS) of both systems is displayed as the number of ride orders increases in Figure 5 (a,b). Compared to the Ethereum-based alternative, our proposed architecture, which makes advantage of Polygon's ZK rollups, achieves a significantly greater throughput. Both systems function similarly when the number of ride orders is less than fifteen. However, our model's throughput grows exponentially with the number of orders, reaching up to 65,000 TPS, whereas the Ethereum model stays

constant at 15 TPS. These results demonstrate the exceptional scalability of our architecture, which can process more than 4,333 times as many transactions per second as the Ethereum option. Applications like ridesharing services that need to process data in real time and manage large volumes need this capability.

Table 3: First Circuit Comparison (c mean constraints, s seconds)

Block Chunk Size	**zkSync**		**Our Proposition**	
26	8,526,701c	71s	8,542,124c	71s
78 1	6,908,690c 1	42s	16,952,713c	144s
182	33,672,019c	289s	33,773,242c	289s
390	67,185,536c	588s	67,401,159c	588s

The addition of two additional operation types, group participation in transactions, and the alteration of public input essentially eliminates the prover's workload in the first circuit, while the second circuit stays the same. The proof time barely changes, and the initial circuit's size just slightly increases from 0.18% for the smallest blocks to 0.32% for the largest. These outcomes are shown in Table 3.

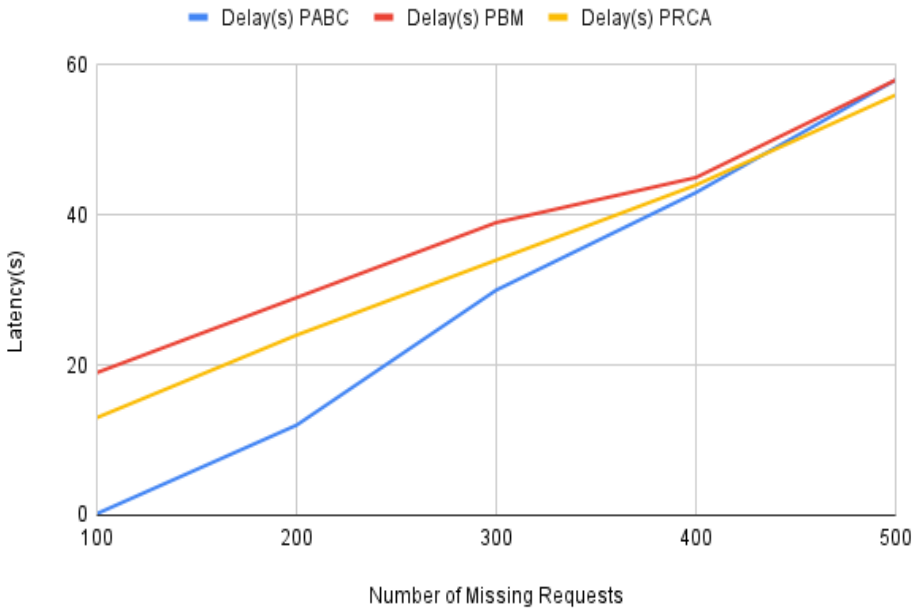


Figure 6: Bitcoin consensus mining delay on average

According to Figure 6, the proposed method reaches consensus on Bitcoin 23.5% faster than PABC, 24.2% faster than PBM, and 23.9% faster than PRCA. Java was used to run this model, and several parameters were estimated throughout the simulations.

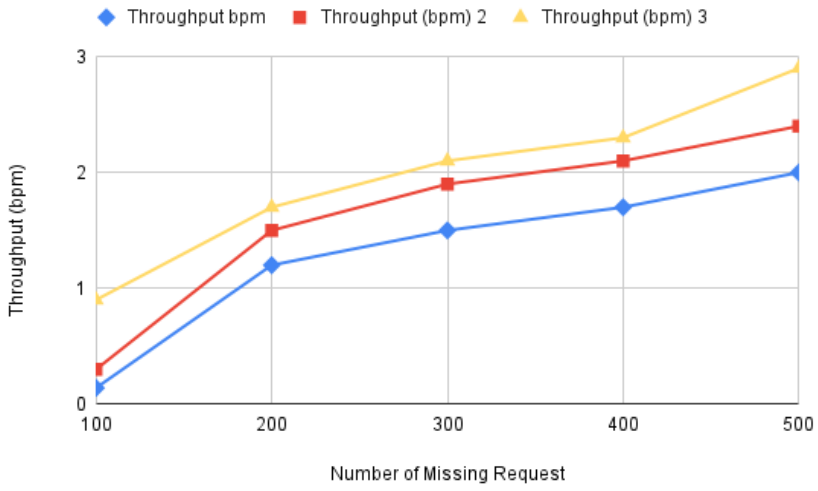


Figure 7: The average mining throughput for Ethereum, Omisego, and Populus consensus

According to the analysis in Figure 7, the proposed model outperforms PABC, PBM, and PRCA by 15, 16, and 18 percentage points, respectively, for agreements based on Ethereum, Omisego, and Populus. These improvements directly increase mining efficiency and make the suggested methodology noticeably scalable.

4 Conclusion

This paper offers a novel approach to decentralized ridesharing that addresses scalability concerns while preserving the crucial security and decentralization aspects of blockchain technology. It uses a two-tier structure: a rollup layer handles operations that require prompt execution, while the main chain handles non-time-sensitive processes. The rollup layer reduces the cost per transaction and speeds up processing times by combining multiple transactions into one and sending them to the main chain. The scaling techniques covered may also be used in other industries where safe and effective decentralized systems would be beneficial, such as food delivery and tourism. The throughput problems that permission blockchain networks have can now be successfully resolved with Layer-2 solutions. Even while prior study has focused on different elements of layer-2 technology, we plan to broaden our scope by investigating the layer-2 systems in several blockchain ecosystems, including Bitcoin's Lightning Network, to see if similar patterns exist there. Additionally, we will develop a synthetic workload that replicates the characteristics of layer-2 systems using the data gathered from our studies. This might therefore serve as a benchmark for constantly assessing various strategies.

References

[1] Alharbi, M., & Alabdulatif, A. (2023). Intelligent transport system based blockchain to preventing routing attacks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *14*, 126-143. https://doi.org/10.58346/JOWUA.2023.I1.011

[2] Andersson, S., & Bergström, N. (2025). Blockchain-Enabled E-Commerce Platforms: Enhancing Trust and Transparency. *International Academic Journal of Innovative Research*, *12*(3), 20-26. https://doi.org/10.71086/IAJIR/V12I3/IAJIR1221

[3] Baza, M., Lasla, N., Mahmoud, M. M. E. A., Srivastava, G., & Abdallah, M. (2021). B-Ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain. *IEEE Transactions on Network Science and Engineering, 8*(2), 1214–1229.

[4] Chlaihawi, M. O. A. (2024). Application of Blockchain Technology to Reduce Costs. *International Academic Journal of Social Sciences, 11*(1), 26–38. https://doi.org/10.9756/IAJSS/V11I1/IAJSS1104

[5] Dallal, H. R. H. A. (2024). Changes to Communication Infrastructure Caused by Blockchain Technology. *International Academic Journal of Science and Engineering*, *11*(1), 25-39. https://doi.org/10.9756/IAJSE/V11I1/IAJSE1105

[6] Gajmal, Y. M., & Udayakumar, R. (2021). Blockchain-based access control and data sharing mechanism in cloud decentralized storage system. *Journal of web engineering*, *20*(5), 1359-1388.

[7] Gangwal, A., Gangavalli, H. R., & Thirupathi, A. (2023). A survey of layer-two blockchain protocols. *Journal of Network and Computer Applications*, *209*, 103539.

[8] Gogol, K., Gurgul, S., Siddiqui, F. N., Branes, D., & Tessone, C. (2025). Scaling DeFi with ZK Rollups: Design, Deployment, and Evaluation of a Real-Time Proof-of-Concept.

[9] Gokulakrishnan, D., & Sinha, T. (2025, April). Scalable Supply Chain Product Source Verification Using Zero-Knowledge Proofs. In *2025 International Conference on Computing and Communication Technologies (ICCCT)* (pp. 1-5). IEEE.

[10] Habib, M. A. (2025). Analyzing Performance Bottlenecks in Zero-Knowledge Proof Based Rollups on Ethereum. *arXiv preprint arXiv:2503.22709*.

[11] Hasnaoui, I., Zrikem, M., & Elassali, R. (2025). Adaptive rollup execution: dynamic opcode-based sequencing for smart transaction ordering in Layer 2 rollups. *Annals of Telecommunications*, *80*(5), 533-546.

[12] Huang, C., Song, R., Gao, S., Guo, Y., & Xiao, B. (2024). Data availability and decentralization: New techniques for zk-rollups in layer 2 blockchain networks.

[13] Konkin, A., & Zapechnikov, S. (2023). Zero knowledge proof and ZK-SNARK for private blockchains. *Journal of Computer Virology and Hacking Techniques*, *19*(3), 443-449.

[14] Makhdomi, A. A., & Gillani, I. A. (2025, January). Decentralized Ridesharing: Overcoming Scalability Issues with Layer 2 Solution. In *Proceedings of the 26th International Conference on Distributed Computing and Networking* (pp. 319-324).

[15] Melo, C., Miqueias, J., Gonçalves, G., Silva, F. A., Soares, A., & Messias, J. (2025, May). Indo além da primeira camada: Modelagem e Avaliaçao de Desempenho de ZK-Rollups na plataforma Ethereum. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)* (pp. 770-783). SBC.

[16] Moreau, I., & Sinclair, T. (2024). A Secure Blockchain-Enabled Framework for Healthcare Record Management and Patient Data Protection. *Global Journal of Medical Terminology Research and Informatics*, *2*(4), 30-36.

[17] Namasudra, S., & Sharma, P. (2022). Achieving a decentralized and secure cab sharing system using blockchain technology. *IEEE Transactions on Intelligent Transportation Systems*, *24*(12), 15568-15577.

[18] Shivers, R., Rahman, M. A., Faruk, M. J. H., Shahriar, H., Cuzzocrea, A., & Clincy, V. (2021, December). Ride-hailing for autonomous vehicles: Hyperledger fabric-based secure and decentralize blockchain platform. In *2021 IEEE international conference on big data (Big data)* (pp. 5450-5459). IEEE.

[19] Stephan, J., Pavlovic, M., Locascio, A., & Livshits, B. (2025). CrowdProve: Community Proving for ZK Rollups. *arXiv preprint arXiv:2501.03126*.

[20] Sulfath, K. K., Ramakrishnan, P. R., Shareef, P. M., & Shanmugam, H. (2025). Enhancing IT Service Management in Indian IT Organizations: A Technological Integration of ISO 20000 with AI, Blockchain, Predictive Analytics, and Zero Trust Security. *Indian Journal of*

Information Sources and Services, 15(1), 267–273. https://doi.org/10.51983/ijiss-2025.IJISS.15.1.34

[21] Tokkozhina, U., Mataloto, B. M., Martins, A. L., & Ferreira, J. C. (2023). Decentralizing online food delivery services: A blockchain and IoT model for smart cities. *Mobile Networks and Applications, 1–11.*

[22] Wang, Q., Lai, C., Han, G., & Zheng, D. (2023). pdRide: Privacy-preserving distributed online ride-hailing matching scheme. IEEE Transactions on Intelligent Transportation Systems, 24(11), 12491-12505.

[23] Wen, X., Feng, Q., Lyu, H., Niu, J., Zhang, Y., & Feng, C. (2024). TeeRollup: Efficient Rollup Design Using Heterogeneous TEE.

Authors Biography

K.N. Unnikrishnan is a prospective Research Scholar in Blockchain in the Department of Computer Science and Engineering at Indian Institute of Information Technology Kottayam, Kerala, India, that have been established as "Institutions of National Importance" by Ministry of Education, Govt. of India. He has completed his B.Tech. in Information Technology from Cochin University of Science and Technology, Kochi, India and M.Tech in CSE from Anna University, Chennai, India. He started his career in the Software industry on application development with companies like IBM India Private Ltd., TCS, and Sonata Software, at Bangalore, India. He also worked with institutions like Viswajyothi College of Engineering and Technology, Muvattupuzha, India and Adi Shankara Institute of Engineering and Technology, Kalady, India where he was heading the respective departments as an Associate Professor. Having a total of 25 years of experience; where 8 years was in Industry and 12 years in Academics, he is a full-time researcher for the past 4 years, with a focus on the scalability of Blockchain by significantly improving the trade-offs on the security, privacy and decentralised nature of Blockchain. He is also into Blockchain development by setting up private Blockchains and developing decentralised apps in Ethereum for the qualitative analysis of his research. He has been closely working with expert Professors at IIT Guwahati, India in the area of Ethereum Zero Knowledge Rollups and zk-SNARKs.

Dr. P. Victer Paul is working as an Assistant Professor in the Department of Computer Science and Engineering at the Indian Institute of Information Technology Kottayam, Kerala, India, an Institute of National Importance of India. He is also heading the Data Analytics and Business Decisions Research Group at IIIT Kottayam. He has completed his Ph.D. in the Department of Computer Science (2015) from Pondicherry Central University, Pondicherry, India. He is a recipient of eminent INSPIRE fellowship from the Department of Science and Technology, New Delhi. He is a Winner of the MSME Idea Hackathon 2022 organized by MSME, Govt. of India and the Distinguished Alumni Award 2023 for Excellence in Academics from SMVEC, Puducherry. Currently, he is working with two Research/Innovative Projects funded under MSME, Govt. of India and the Core Research Grant scheme, SERB, Govt. of India. He has delivered invited talks on various technical topics and also organized an ATAL FDP program sponsored by AICTE, Govt. of India. He extended consultancy works to NeST Digital, Ernakulam to train the technical developers and also published an Indian patent in 2022. He has 14+ years of academic, research & industrial experience and published over 80 research articles in various International Journals & Conferences. Currently, he is working in the fields of Artificial Intelligence & Optimization and Data Analytics.