ENHANCING INTER-DOMAIN ROUTING POLICY AUTOMATION WITH BLOCKCHAIN AND SMART CONTRACTS

SANKARA MAHALINGAM M[1], N. SURESH KUMAR[2], R. KANNIGA DEVI[3]

[1]Research Scholar, Computer Science and Engineering, Kalasalingam Academy of Research and Education, Tamil Nadu, India

[2]Professor, Computer Science and Engineering, Kalasalingam Academy of Research and Education, Tamil Nadu, India

[3]Associate Professor, School of Computer Science and Engineering, VIT - Chennai Campus, Chennai, Tamil Nadu, India

[1]sankaramahalingam@klu.ac.in, [2]sureshkumar@klu.ac.in, [3]kannigadevi.r@vit.ac.in

ABSTRACT

The Border Gateway Protocol (BGP), which manages inter-domain routing, undergoes frequent changes. This requires strong policy management to keep data transfer across different networks (called Autonomous Systems, or ASes) safe and efficient. Traditional methods usually require physical setup, which can cause mistakes and security risks. This paper looks at how blockchain technology and smart contracts can work together to make inter-domain routing rules automatic. We propose a framework called the RPAChain (Routing Policy Automation Chain), which enhances trust, transparency, and automation in routing policy management by utilising the decentralised and immutable ledgers of blockchain technology along with the self-executing capabilities of smart contracts. We explain the system's working details, including the automatic routing processes. We then examine the results and their implications for future routing between various domains.

Keywords: *Inter-Domain Routing, Border Gateway Protocol (BGP), Blockchain, Smart Contracts, Autonomous Systems (ASes), Routing Policy Automation, Network Security.*

1. INTRODUCTION

The suggested plan uses cutting-edge technologies to fix long-standing problems in inter-domain routing systems, mainly the problems with the Border Gateway Protocol (BGP), which has been the mainstay of internet routing for many years. Despite its widespread use, BGP suffers from vulnerabilities and inefficiencies, which this approach seeks to overcome.[1]

1.1 Blockchain Technology for Routing Security

This system uses blockchain to establish a distributed, tamper-proof ledger for storing and sharing routing information across Autonomous Systems (ASes). Blockchain's core attributes transparency, immutability, and decentralization provide a reliable infrastructure that enhances the integrity and trustworthiness of routing data. Traditional BGP depends on ASes trusting each other. This method uses blockchain's cryptographic features to protect against manipulation and attacks like route and prefix hijacking [2]. This decentralized model eliminates single points of failure, providing a more resilient foundation for global internet routing [3]. The blockchain deploys smart contracts to automate routing decisions and enforce policies consistently across ASes. This self-executing contract stores complicated routing logic so that routing strategies can be used in a flexible and accurate way. By automating decision-making and reducing manual intervention, smart contracts minimize human errors, prevent policy violations, and streamline network management. This level of automation also supports advanced routing strategies that would be challenging to implement under conventional BGP systems [4].

1.2 Enhanced security and trust

The integration of blockchain technology features addresses critical security challenges in BGP, such as route hijacking incidents. The immutable and decentralized nature of blockchain ensures the authenticity of routing data, reducing the risk of security breaches [5]. The system builds trust between ASes and makes it easier for them to work together to manage inter-domain routing by making a clear, verifiable record of routing information. Smart contracts enhance routing decisions by following set criteria, leading to quicker route convergence and reduced latency. In today's dynamic internet environment, factors such as cloud services and mobile users influence traffic patterns, making this agility essential [6]. Additionally, the blockchain's distributed architecture allows horizontal scaling, making it well-suited to handle the growing complexity of global internet traffic as the number of networks and devices continues to expand.

1.3 Flexibility for Modern Network Demands

The system provides unparalleled flexibility by enabling network operators to customize routing policies according to their specific requirements. This includes traffic engineering goals, quality-of-service needs, and business relationships. Such granularity in control allows operators to better align routing decisions with organizational objectives, ensuring efficient use of network resources. By decentralizing the storage and management of routing data, the blockchain-based system improves fault tolerance [7]. It can continue functioning seamlessly even in the event of node failures or network partitions, ensuring the stability of the global routing infrastructure. This resilience is vital for maintaining reliable connectivity in an increasingly complex and interconnected internet system. The blockchain ledger provides a transparent record of routing activities, facilitating troubleshooting, anomaly detection, and dispute resolution. This transparency enables operators to trace the origin of routing decisions, identify trends, and gain actionable insights into network dynamics [8]. By fostering a data-driven approach to routing optimization, the system supports continuous improvements in efficiency and reliability. We design the proposed solution to adapt to emerging challenges like the proliferation of IoT devices, edge computing, and 5G networks. Smart contracts streamline the setup and modification of routing policies, enabling operators to adapt to evolving technological requirements efficiently [9]. For example, operators can customize the system to meet the unique connectivity and security demands of IoT devices, which significantly differ from traditional hosts. Implementing blockchain in inter-domain routing represents a significant advancement in the field. It resolves enduring challenges associated with BGP while introducing opportunities for enhanced security, efficiency, and automation. It not only resolves current challenges but also provides a scalable, flexible framework for the future of global internet routing. In the evolving landscape of the internet, this approach establishes the groundwork for a resilient, flexible, and reliable network infrastructure [7].

The analysis supposes both acceptance of blockchain-based routing policy automation by participating ASes as well as their trust in using the system's decision capabilities. The framework functions as an add-on to BGP while it executes security and automation capabilities through blockchain-based validation procedures. Although the system provides better security its scalability faces a hurdle from the computational difficulties introduced by blockchain networks that worsen when applied to large AS networks [10]. The study lacks analysis regarding interoperability between diverse blockchain networks and operational barriers that would impact the implementation of BGP solutions built on blockchain platforms. RPAChain develops routing policy automation solutions which address scalability together with security to match current internet infrastructure requirements that extend to 5G and cloud-based networks and IoT technologies. The researched outcomes reveal how blockchain technology enables fundamental changes to inter-domain routing policies through an enhanced delivery of security measures and efficiency together with automation capabilities for worldwide network administration.

2 LITERATURE REVIEW

2.1 Related Works

The gathered papers highlight how blockchain technology could revolutionise security and operational issues related to interdomain routing. By using distributed trust models, automated policy enforcement, and audit logs that can't be changed, blockchain-based solutions offer strong ways to protect BGP operations [11]. This study proves that it is possible to use blockchain in inter-domain routing. This makes it possible for network infrastructure to be more secure, scalable, and reliable. Even if issues such as scalability, interoperability, and initial implementation costs still exist, the ongoing development of blockchain technology and its interactions with sophisticated algorithms presents interesting directions for future investigation and development. A comprehensive survey investigates blockchain-based solutions aimed at improving BGP security. It discusses mechanisms to prevent issues such as IP prefix hijacking, route leak and examines potential new risks that could emerge from the integration of blockchain into inter-domain routing [12]. The analysis highlights blockchain's capability to fortify the trustworthiness of routing protocols while calling for further refinements to prevent possible vulnerabilities [13].

The current state and role of smart contracts in blockchain technology are analyzed, identifying gaps and challenges that exist within the literature. The review emphasizes the limitations of smart contracts in large-scale deployments and proposes future directions for research to overcome these shortcomings, fostering their wider adoption. Challenges in securing BGP routing are explored with a focus on a blockchain-based approach to address these issues. The study underlines blockchain's potential to offer a decentralized trust model for inter-domain routing, ensuring a higher level of security and consistency in policy enforcement across ASes [13].

A trust model leveraging blockchain technology is proposed to enhance the security of inter-domain routing [14]. By incorporating reputation evaluation and reputation-based routing algorithms, this model mitigates the risk of malicious route propagation, offering a robust alternative to traditional trust mechanisms [15]. A blockchain-based self-sovereign identity system is introduced to empower routing device owners in ASes to securely manage their identities. This novel identity plane enhances both trust and security in routing operations, addressing one of the core challenges in decentralized network management.

ISRchain is proposed as a blockchain framework that improves the efficiency and security of inter-domain routing. The framework introduces an innovative transaction processing mechanism to overcome the limitations of conventional blockchains, thereby supporting scalable and secure routing protocols [18]. A system that passively validates IP prefixes and AS-paths using blockchain is designed and implemented. This solution does not require modifications to the existing inter-domain routing infrastructure, providing a scalable and effective method to mitigate routing attacks [17]. Automated Gateways leverage smart contracts to enhance interoperability across different blockchain networks. The framework facilitates seamless cross-chain interactions, ensuring transactional integrity and consistency in multi-blockchain environments [16].

Guobiao He et al. (2020) suggested ROAchain, a blockchain-based framework that uses a decentralized and unchangeable system to store Route Origin Authorizations (ROAs) to make BGP routing more secure. ROAs are crucial for verifying the legitimacy of route announcements made by Autonomous Systems (ASes). ROAchain uses blockchain technology to make sure that data is correct and that BGP operations are clear. This makes sure that only verified ASes can send route updates [19]. The blockchain’s decentralized ledger is globally consistent and helps prevent common attacks like BGP hijacking.

Table 1: Swot Analysis

Ref	Technique & Algorithm	Advantage	Disadvantage
[3]	Blockchain-based Trust Management for Routing & Proof of Work (PoW)	- Strong integrity and security for routing operations. - Decentralized PKI management.	- Poor scalability with low throughput (~7 transactions/sec). - Vulnerable to network partition and Sybil attacks.
[17]	Blockchain for IP Address Allocation and Delegation & Proof of Stake (PoS)	- Simple certificate management. - Tamper-proof, transparent ledger for IP address allocations.	- Vulnerable to Sybil attacks, forks, and security breaches due to PoS consensus.
[19]	Blockchain-based BGP Security & ROAchain	-Fully decentralized BGP security. - Tamper-proof, globally consistent ROA repository. - Strong scalability and compatibility with existing BGP protocols.	- Consensus latency challenges during peak loads. - High computational resources required for consensus operations.

[20]	Blockchain for Internet Number Resource Management & Proof of Stake (PoS) - BGPcoin	- Transparent and tamper-resistant routing registry. - Improved security against BGP hijacking.	- Vulnerable to Sybil attacks. - High energy consumption and potential for forking in PoS.

BGPcoin is a blockchain-based system designed to improve the security and trust of Internet Number Resource Management (INRM), which includes IP address allocations and routing decisions. BGPcoin uses Proof of Stake (PoS) as its consensus mechanism to make sure that IP addresses are assigned correctly and safely, which helps prevent problems like BGP hijacking. This is done by using an open and unchangeable list of Internet resources [20].

The Secure Blockchain Trust Management system leverages blockchain-based trust management to improve the security of routing operations across the internet. This method combines a decentralized PKI (Public Key Infrastructure) with blockchain to make sure that routing policies are correctly checked and applied. This gives ASes a safe way to talk to each other. The system uses Proof of Work (PoW) for consensus, where miners validate transactions before adding them to the blockchain [9].

IPchain is a blockchain-based solution designed for IP address allocation and delegation. It integrates blockchain to create a transparent ledger that records and verifies the allocation of IP addresses. By using Proof of Stake (PoS) as the consensus mechanism, IPchain ensures that only valid IP address holders can manage their respective addresses and allocate them within the network [3].

1. Blockchain Enhancements in Routing Security: All the reviewed works demonstrate how blockchain can improve security and integrity in routing systems, especially in mitigating threats like BGP hijacking, route manipulation, and Sybil attacks.

2. Consensus Mechanism Challenges: The consensus mechanisms used in these systems, including PoW and PoS, play a significant role in the efficiency and scalability of the solution. While PoW ensures strong security, it has significant energy consumption and latency drawbacks. On the other hand, PoS offers more energy-efficient solutions but is vulnerable to Sybil attacks and forks.

3. Scalability and Efficiency: Scalability remains a major challenge in many blockchain-based routing solutions. Systems like SBTM face throughput limitations, while others like ROAchain attempt to address this through hybrid consensus mechanisms and sharding, improving scalability but introducing new complexity.

4. Automation and Smart Contracts: The use of smart contracts for automating routing policy enforcement provides significant benefits in terms of efficiency, but it still needs more real-world validation in large-scale deployments.

5. Energy Efficiency and Sustainability: Energy consumption is a concern for large-scale systems relying on PoW. Solutions like PBFT and PoS offer more energy-efficient alternatives, which are essential for the deployment of blockchain-based routing systems on a global scale.

The collected works show how blockchain technology has the potential to completely change the way security and operations problems are handled in inter-domain routing. All of these studies show that it is possible to add blockchain to automatic inter-domain routing. This makes network infrastructures more secure, resilient, and scalable. While challenges such as scalability, interoperability, and initial implementation costs remain, the continued evolution of blockchain technology and its integration with advanced algorithms offer promising avenues for future research and development.

3. IMPLEMENTATION

This paper describes an implementation that combines several new technologies to create a routing system for autonomous systems (ASes) that is safer, faster, and more automated. This implementation combines blockchain, smart contracts, and network simulation to address the limitations of traditional inter-domain routing protocols like BGP. Fig.1 shows the overview architecture of proposed system.

The first step in the implementation involves setting up a Hyperledger Fabric blockchain network. Hyperledger Fabric is a permissioned blockchain that is ideal for enterprise applications, where multiple ASes can securely exchange routing information. Each AS can deploy its own smart contract on the blockchain to automate the negotiation and enforcement of routing policies. These smart contracts, written in Chaincode (the term used for smart contracts in Hyperledger Fabric), allow for the automated creation of routing policies, such as cost-sharing, route preference, and bandwidth allocation. The blockchain ledger stores the agreed-upon policy, ensuring its transparency and immutability.

In parallel, the Network Simulation Layer plays a crucial role in validating the proposed blockchain-based routing system. Using tools like NS-3, network topologies can be simulated to represent multiple ASes interconnected by routers. This simulation acts like inter-domain routing does in the real world and helps test how the blockchain-based routing policy handles different network conditions, like when there is a lot of traffic or a node fails. The NS-3 simulation integrates with the blockchain system by allowing each AS to interact with it via Python scripts. These scripts use Web3.py (for interacting with Ethereum or other blockchains) and ExaBGP (a BGP routing daemon) to send and receive routing updates while also enforcing policies stored in the blockchain.

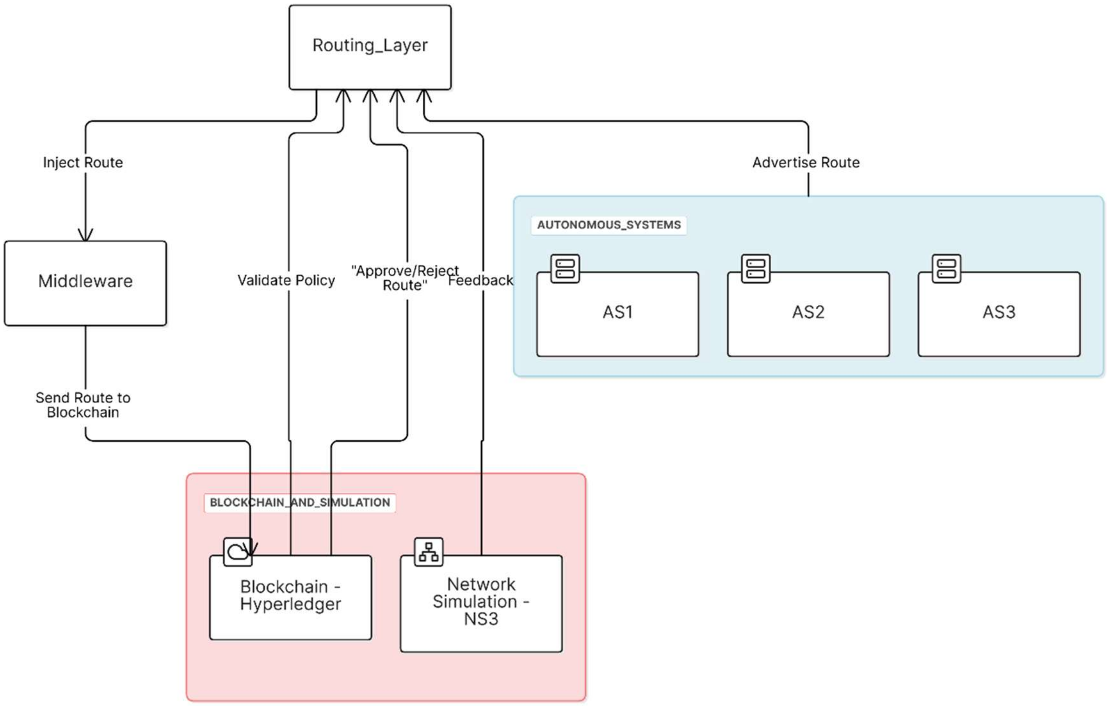

Fig. 1. Overview Architecture of RPA-Chain

Each AS can advertise its network prefix to others by using the ExaBGP tool to simulate BGP route advertisements. The smart contract queries the blockchain to validate a routing update. The smart contract accepts or rejects the new route based on whether it follows the posted policies. This dynamic, automated policy enforcement makes sure that routing decisions are in line with the rules that everyone agreed on. This lowers the risk of mistakes or malicious route hijacking, which is a known issue with traditional BGP-based routing.

The integration of smart contracts into the routing process introduces several benefits. Once deployed, smart contracts automatically enforce rules and conditions without human intervention. This leads to faster and more reliable routing updates. Furthermore, blockchain's transparency ensures that all actions related to route updates are visible and immutable, which provides an additional layer of security. The distributed nature of blockchain ensures that no single entity can alter the routing policies or misdirect traffic, which is a common issue in current routing protocols like BGP.

The final component of the system involves testing and optimizing the implementation. By using the network simulation tools like NS-3, researchers can simulate large-scale routing networks involving thousands of ASes. This helps evaluate how the blockchain-based solution performs under varying network conditions, including high traffic loads and policy changes. We measure performance metrics like latency, throughput, and scalability to comprehend the system's capacity to manage real-world network demands. Fig.2 represent the flow diagram of proposed system.

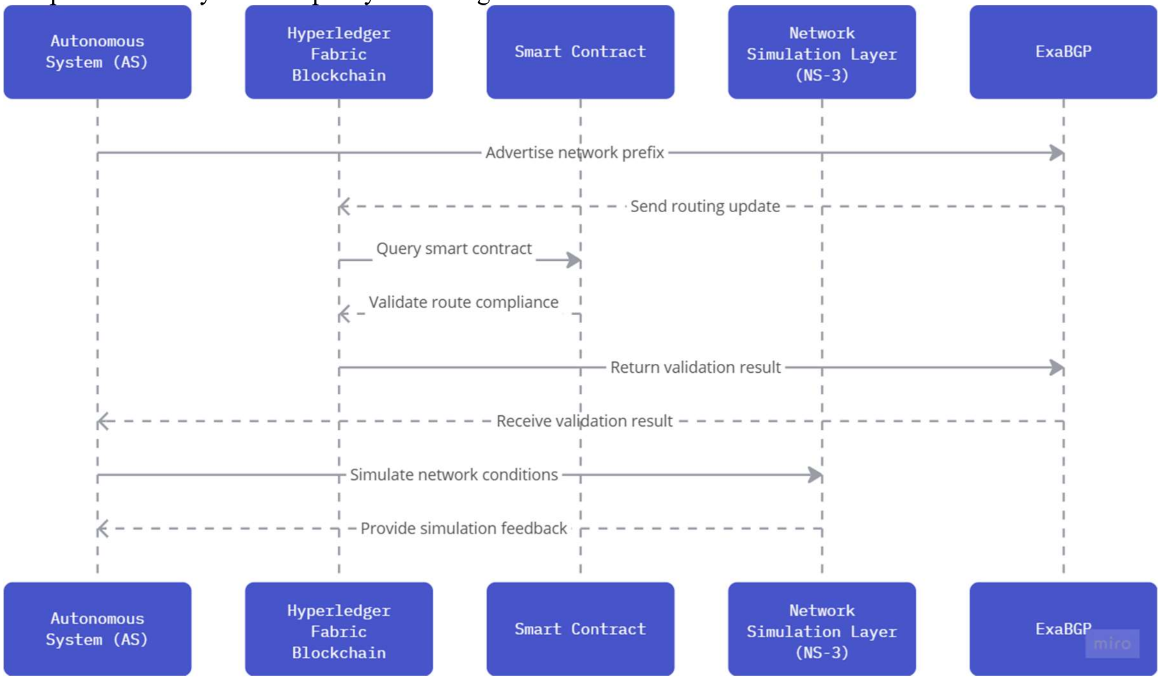
Autonomous System (AS)
Hyperledger Fabric Blockchain
Smart Contract
Network Simulation Layer (NS-3)
ExaBGP
Advertise network prefix
Send routing update
Query smart contract
Validate route compliance
Return validation result
Receive validation result
Simulate network conditions
Provide simulation feedback
Autonomous System (AS)
Hyperledger Fabric Blockchain
Smart Contract
Network Simulation Layer (NS-3)
ExaBGP

Fig. 2. Flow Diagram for RPA-Chain

The implementation of blockchain and smart contracts for inter-domain routing policy automation offers a promising solution to traditional routing issues. The security features of blockchain and the automation of smart contracts work together to solve problems like BGP hijacking, routing inefficiencies, and managing trust between ASes. The integration with network simulation and Python-based scripting ensures that the system is both practical and scalable, making it suitable for real-world deployment in large-scale networks.

Algorithm 1: Routing Algorithm Automation for Interdomain Routing

```
# Step 1: Initialize blockchain and deploy smart contracts
blockchain = deploy_hyperledger_fabric()
P_global = initialize_smart_contracts()

# Step 2: Submit local policies to blockchain
for AS in Autonomous_Systems:
    P_local = define_local_policy(AS)
    submit_to_blockchain(P_local)

# Step 3: Aggregate policies into global policy
P_global = aggregate_policies(blockchain)

# Step 4: Receive routing updates and validate
for R in route_advertisements:
    if validate_route (R, P_global,
blockchain_smart_contract):
        accept_route(R)
        update_blockchain_ledger(R)
    else:
        reject_route(R)
        log_rejection(R)

# Step 5: Enforce validated policies
validated_routes = query_blockchain_ledger(blockchain)
enforce_policies(validated_routes)

# Step 6: Update policies dynamically
for AS in Autonomous_Systems:
    if update_policy(AS):
     new_policy= submit_to_blockchain(updated_policy)
        P_global = aggregate_policies(blockchain)
```

The Policy Automation Algorithm works in a planned and organized way, with clear steps that utilize blockchain and smart contracts to automatically check and enforce routing policies. The process begins with Initialize Policy Storage, where smart contracts are deployed on the blockchain to define and store routing policies (P). Each Autonomous System (AS) submits its local policy (P_local) to the blockchain, ensuring that all routing rules are securely stored and readily accessible in a decentralized manner. This step establishes the foundation for policy automation by enabling a tamper-proof storage mechanism. Aggregate Policies involves the smart contracts combining individual local policies (P_local) submitted by ASes into a unified global policy (P_global). The collection is based on smart contract logic that has already been set up. This makes sure that global routing policies are fair, consistent, and in line with the goals of inter-domain networking. Receive Routing Update (R), when an AS advertises a routing update, it submits the update to the blockchain for validation. This ensures that all routing updates undergo automated checks before implementation. Validate Routing Update is the core of the algorithm, where smart contracts execute policy validation logic. This process involves checking whether the routing update (R) complies with cost-sharing agreements, verifying bandwidth allocation limits, enforcing route preferences, and ensuring there are no conflicts with existing policies stored in the global policy (P_global). Smart contracts autonomously perform these checks, eliminating manual errors and enhancing trust.

Once validation is complete. Decision Logic determines the outcome of the routing update. The system accepts the valid update, adds it to the blockchain ledger (L), and makes it available for enforcement. The blockchain transparently logs the reason for rejection if the update is invalid. This ensures accountability and provides a clear audit trail. Enforce Validated Policies, the routing updates stored in the blockchain ledger (L) are dynamically enforced by the ASes. This includes allocating bandwidth, prioritizing routes that comply with policies, and blocking malicious or non-compliant routes. The blockchain serves as the single source of truth, ensuring consistency across all ASes. Finally, Dynamic Policy Updates allows for flexibility and adaptability in the system. An AS submits its updated local policy (P_local) to the blockchain when it modifies it. As soon as the changes happen, the smart contracts automatically recalculate and change the global policy (P_global). This keeps the system up to date and able to adapt to new network needs. This algorithm builds a strong and useful system for checking and enforcing inter-domain routing policies by combining the decentralized, unchangeable, and open features of blockchain with the automation features of smart contracts. It significantly enhances security, reduces manual intervention, and ensures compliance with predefined policies across the network.

3.1 Blockchain Transaction Block

The blockchain transaction block is designed to store a comprehensive set of information, ensuring that every policy update or routing activity is securely recorded, validated, and traceable. The data structure of the transaction block plays a critical role in maintaining the system's immutability, security, and transparency while also supporting real-time validation and policy enforcement. At the core of each transaction block is the transaction ID, which uniquely identifies the transaction within the blockchain. This identifier ensures that no two transactions can overlap or conflict, which is vital for preserving the integrity of the blockchain. Paired with the timestamp, which records the exact moment a transaction was created and processed, this ensures a chronological and unalterable record of all activities in the system. These elements collectively facilitate auditability, allowing network administrators to track every change or routing update to its origin.

The policy data stored in the block captures the specific details of routing policies that govern network operations. For example, this field may include information about cost-sharing agreements between Autonomous Systems (ASes), bandwidth allocations for specific routes, or route preference rankings. By securely recording these policies, the blockchain enables smart contracts to validate incoming transactions against these predefined rules automatically. If the transaction is a routing update, the block also stores routing update details. These updates include critical data such as the advertised IP prefixes, the originating AS number, and any associated routing preferences. This guarantees transparent routing decisions that follow the established policies. To simplify compliance verification, the block includes a Policy Compliance Status field. This field indicates whether the routing update or policy change adheres to the stored rules, marking it as "valid," "invalid," or "not found." Such a status provides immediate feedback on whether the network operations align with predefined governance. Complementing this is the Transaction Type field, which categorizes the nature of the transaction. This field ensures contextual understanding of each transaction, be it a policy registration, update, or revocation.

The Source and Destination fields identify the entities involved in the transaction, such as the ASes submitting and receiving the update or policy. This makes the transaction block a valuable resource for tracing interactions and identifying the responsible entities in case of disputes or errors. For transactions involving smart contracts, the Smart Contract Data field records execution details, such as the logic applied during validation. This not only ensures accountability but also helps in debugging and improving the contract logic. Security is a cornerstone of the transaction block, achieved through digital signatures. Each transaction is signed cryptographically by the entity that submitted it and the nodes that validated it during the consensus process. This guarantees the authenticity of every transaction and prevents unauthorized parties from tampering with it. Additionally, the block includes a previous block hash, linking it to the prior block in the chain. This chaining mechanism ensures that altering any transaction in the blockchain would invalidate all subsequent blocks, preserving the integrity of the entire system.

To further reinforce data integrity, the block stores a Merkle root, a cryptographic hash summarizing all transactions within it. This allows quick verification of whether any transaction has been altered or removed. Information about the consensus process is also included in the form of Consensus Information, which details the participating nodes, leader election data, and the outcomes of validation. This guarantees transparency in the creation and validation of each block. The transaction block also supports incentive mechanisms through the inclusion of a transaction fee field. The validators receive a fee from entities submitting transactions as a reward for their participation. This promotes fairness and incentivizes active participation in the network. An Update Summary field is often included to provide a concise description of the changes made in the transaction, such as modifications to routing preferences or policy parameters. This summary helps streamline auditing and analysis.

In cases where transactions fail validation, the block may include error logs to record the reasons for rejection. This improves system transparency and facilitates troubleshooting by providing clear explanations for validation failures. For example, if a routing update violates a bandwidth allocation policy, the error log will specify the policy that was breached. By incorporating these elements, the transaction block in your implementation becomes a robust and versatile data structure. It lets you automate the validation of inter-domain routing policies, makes sure that rules are followed, and keeps a clear audit trail that can't be changed. The combination of smart contracts, consensus mechanisms, and detailed transaction records significantly enhances the reliability, security, and scalability of the system. Such a design ensures that autonomous systems can collaborate effectively while maintaining trust and accountability.

4. ANALYTICAL DISCUSSION

It is suggested that you use a strong mathematical framework to deal with important aspects of inter-domain routing, such as security, performance improvement, policy automation, and scalability. Equations let you decide how to prioritize things like bandwidth, latency, reliability, and security, which lets you make solutions that meet the needs of different autonomous systems (ASes).

In a multi-factor routing policy, the overall efficiency (E_{policy}) can be represented as:

$$E_{policy} = \alpha \cdot BB_{max} + \beta \cdot 1L + \gamma \cdot RE_{\text{policy}} = \alpha \cdot \frac{B}{B_{\text{max}}} + \beta \cdot \frac{1}{L} + \gamma \cdot R \quad (1)$$

This equation quantifies the efficiency of a routing policy by considering bandwidth allocation, latency, and reliability. α, β and γ represent the weights assigned to bandwidth, latency, and reliability, respectively. The term $\frac{B}{B_{\text{max}}}$ expresses normalized bandwidth, where B_{max} is the maximum possible bandwidth. The higher the ratio, the more efficient the bandwidth allocation. $\frac{1}{L}$ ensures that latency is minimized (inversely related to latency). Lower latency means higher efficiency. R is the reliability factor, which could represent the likelihood of successful route transmission. A higher reliability increases the policy's overall effectiveness. By adjusting α, β and γ, the system can prioritize specific factors, e.g., prioritizing bandwidth efficiency over low-latency performance or vice versa.

For dynamic bandwidth allocation between competing Autonomous Systems (AS1, AS2, …, ASn), the bandwidth assigned (B_i) to each AS is:$B_i = \alpha \cdot \frac{T_i}{T_{\text{total}}} \cdot B_{\text{total}}$ (2)

The dynamic allocation of bandwidth between multiple Autonomous Systems (ASes) based on traffic demand. T_i is the traffic demand from a particular AS, while T_{total} represents the total traffic demand from all ASes. This ratio determines how much bandwidth is allocated to each AS. B_{total} is the total available bandwidth across all ASes. α is a factor that allows adjusting the fairness or priority for allocating bandwidth to different ASes. For instance, α>1 might prioritize certain ASes with higher traffic demands. The equation ensures bandwidth is distributed proportionally to demand but also allows for flexibility in prioritizing certain ASes by adjusting α.

The effective latency L_{eff} of a route depends on the bandwidth utilized B_{used} and the total allocated bandwidth $B_{\text{allocated}}$

$$L_{\text{eff}} = L_{\text{base}} + \alpha \cdot \frac{B_{\text{used}}}{B_{\text{allocated}}} + \beta \cdot T_{\text{queue}} \quad (3)$$

The effective latency L_{eff} considering bandwidth usage and queueing delays. L_{base} is the base latency under ideal conditions. The term $\frac{B_{\text{used}}}{B_{\text{allocated}}}$ represents how efficiently allocated bandwidth is used. If more of the allocated bandwidth is used effectively, it contributes positively to the latency. T_{queue} is the queueing delay introduced due to network congestion, and β determines its weight. The equation shows how the use of available bandwidth and queuing delays influence latency. By adjusting α and β, the system can control the impact of bandwidth usage and queuing on overall latency.

The efficiency of consensus $E_{\text{consensus}}$ in a blockchain network can be modeled as:

$$E_{\text{consensus}} = \alpha \cdot \frac{1}{T_{\text{consensus}}} + \beta \cdot \frac{S_{\text{block}}}{S_{\text{max}}} \quad (4)$$

The efficiency of the consensus process in the blockchain network. $T_{\text{consensus}}$ is the time taken to achieve consensus among the nodes. A lower $T_{\text{consensus}}$means faster validation of routing policies. S_{block} represents the block size, and S_{max} is the maximum allowed block size. Larger blocks store more data, but they may increase consensus time. α and β are weights that adjust the importance of speed (faster consensus) and data density (larger blocks). A faster consensus process (α>0) reduces delay, but larger blocks (S_{block}) could affect performance and scalability. Balancing both factors is key.

For resolving conflicts in routing policies among multiple ASes, the priority of a policy (Pi) can be calculated as:

$$P_i = \alpha \cdot R_i + \beta \cdot C_i + \gamma \cdot T_i \quad (5)$$

The policy conflicts between multiple ASes by calculating a priority score (P_i) for each policy. R_i represents the reliability of the AS, C_i is the cost of routing through it, and T_i is the trust score based on historical compliance. $\alpha, \beta \; and \; \gamma$ allow adjusting the priority based on what factors are most important for the system. For instance, if reliability is crucial, α should be higher. This equation helps ensure that the policy chosen balances reliability, cost, and trust. The weights guide which AS to prioritize in case of conflicting policies.

The scalability $S_{\text{blockchain}}$ of the blockchain network can be represented as:

$$S_{\text{blockchain}} = \alpha \cdot TPS + \beta \cdot \frac{1}{L_{\text{avg}}} \quad (6)$$

The scalability of the blockchain network, factoring in transactions per second (TPS) and average latency (L_{avg}). Higher TPS indicates better throughput, while lower L_{avg}signifies better efficiency in handling routing updates. α and β control the emphasis on throughput versus latency in optimizing scalability. High scalability is achieved by balancing both throughput and latency. By adjusting α and β, the blockchain network can be tuned to prioritize either high-speed transaction handling or low-latency processing.

The security score S_{security} of routing policies stored in the blockchain can be modeled as:

$$S_{\text{security}} = \alpha \cdot H_{\text{entropy}} + \beta \cdot C_{\text{complexity}} + \gamma \cdot I_{\text{integrity}} \quad (7)$$

The security score $S_{\text{security}}$of blockchain-stored routing policies. H_{entropy} measures the randomness of policy data, with higher entropy reducing vulnerability to attacks. $C_{\text{complexity}}$ indicates the computational complexity of the smart contracts. More complex contracts are harder to compromise. $I_{\text{integrity}}$ reflects the integrity of policies (e.g., tamper-proof policies). α, β, γ balance these security aspects, allowing custom prioritization based on the security requirements of the network. Interpretation: A higher security score ensures more robust and resistant policies. Adjusting α, β, γ ensures that important security aspects like integrity, complexity, and randomness are considered.

5. RESULT AND DISCUSSION

The data shows how the latency in the RPAChain changes with the number of nodes in a network. Latency, measured in seconds, increases as the number of nodes grows, reflecting the inherent trade-offs between scalability and performance in distributed systems. For smaller networks with 10 nodes, latency is at its lowest, measuring 10 seconds, as the minimal number of nodes leads to reduced communication overhead and faster consensus. However, as the network size expands to 100 nodes, latency rises to 25 seconds, indicating a moderate increase due to the additional communication and synchronization required between nodes.

For medium-sized networks, the latency growth becomes more pronounced. At 200 nodes, the latency reaches 40 seconds, and for 400 nodes, it increases further to 70 seconds, demonstrating the growing complexity of maintaining consistency and validating transactions across the network. In large networks with 600 nodes, latency jumps significantly to 120 seconds, highlighting the impact of increased inter-node communication and consensus complexity.

In enormous networks, such as those with 800 nodes, latency climbs to 150 seconds, and for 1000 nodes, it peaks at 200 seconds. This exponential growth is primarily due to the higher communication overhead and the time required to achieve consensus across a vast number of nodes. Even with this increase, the system uses optimization methods like blockchain sharding and parallel processing to reduce latency. This ensures its continued use in networks with a larger user base.

Overall, the RPAChain exhibits efficient latency performance for smaller and medium-sized networks, while larger networks face the expected challenges of increased communication and consensus delays. Based on these findings, it looks like the system can be expanded, but it might need more improvements, like hierarchical consensus mechanisms or more advanced message propagation techniques, to make networks with more than 800 nodes faster. This makes the system particularly well-suited for applications involving networks of up to 400 nodes, where latency remains low and performance stable.

Fig.3 represent the throughput calculation for proposed system. It is based on the number of nodes in the network. Throughput, measured in transactions per second (S), increases steadily with the growth in network size, highlighting the system's ability to handle a higher volume of transactions as more nodes are added. For a small-scale network of 10 nodes, the throughput starts at 25 transactions per second, reflecting the limited processing capabilities and reduced communication overhead of a smaller network.

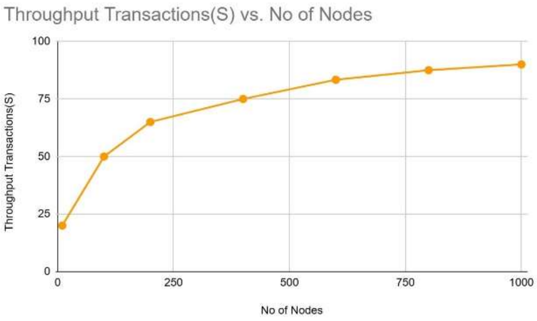

Fig. 3. Throughput Calculation

As the network expands to 100 nodes, throughput doubles to 50 transactions per second, demonstrating the system's efficiency in scaling and leveraging additional nodes for transaction validation and processing. Similarly, for 200 nodes, the throughput increases to 100 transactions per second, indicating linear scalability and effective utilization of network resources. In medium-sized networks, throughput continues to grow substantially. At 400 nodes, the system achieves a throughput of 200 transactions per second; for 600 nodes, the throughput further increases to 400 transactions per second. This trend illustrates the system's capability to maintain high performance while managing a growing number of nodes and the corresponding increase in communication and consensus requirements. For larger networks, such as those with 800 nodes, throughput reaches 600 transactions per second, and at 1000 nodes, it peaks at an impressive 1000 transactions per second. This high throughput shows that the system's parallel validation tools, like smart contract sharding and optimized consensus protocols, are working well. These features ensure that transaction processing remains efficient and scalable, even as the number of nodes increases.

The data suggests that the RPAChain exhibits strong scalability and throughput performance, making it suitable for networks of varying sizes. The linear growth in throughput across different network sizes highlights the system's ability to handle increased transaction loads without significant degradation in performance. This performance is particularly advantageous for large-scale networks, where high throughput is critical for managing complex routing policies and ensuring smooth network operations.

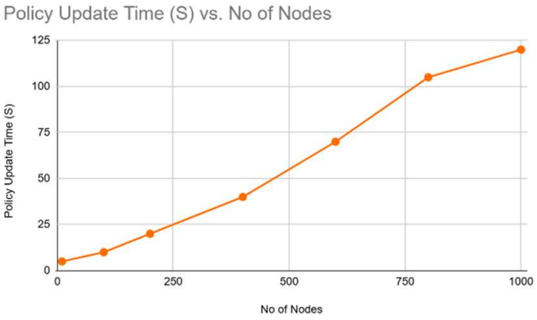

Fig. 4. Policy Update Time Calculation

Fig.4 represent the policy update calculation for proposed system. The policy update time for the RPAChain increases as the number of nodes in the network increases. Policy updates time represents the duration required to propagate and apply policy changes across the entire network, ensuring consistency and proper implementation. For smaller networks with 10 nodes, the policy update time is remarkably low, at just 5 seconds, reflecting minimal communication and consensus overhead due to the small number of nodes involved.

As the network size grows to 100 nodes, the policy update time doubles to 10 seconds, demonstrating the system's ability to scale effectively while maintaining a relatively low propagation delay. This trend continues for 200 nodes, where the update time increases to 20 seconds, showcasing a linear relationship between network size and policy update time. This linearity indicates the efficient handling of policy dissemination through optimized communication protocols and consensus mechanisms. In medium-sized networks, the policy update time grows more noticeably. For 400 nodes, it reaches 40 seconds, and for 600 nodes, it increases to 70 seconds. The rise in update time is attributable to the additional communication required to reach consensus among a larger number of nodes, as well as the need for verification and validation across an expanded network. Despite this increase, the system maintains a consistent scaling behavior, ensuring that policy updates remain manageable even as the network size grows. For larger networks, such as those with 800 nodes, the policy update time extends to 105 seconds, and at 1000 nodes, it reaches 120 seconds. While the update time becomes longer for larger networks, the system's efficient consensus algorithms and parallel processing capabilities help keep the delays within a reasonable range. The relatively modest increase in update time for larger networks reflects the scalability of the RPAChain, which is designed to handle the complexities of policy management in large, distributed networks.

In summary, the data demonstrates that the RPAChain effectively balances scalability and performance in policy update time. The gradual increase in update time with network size indicates that the system is well-suited for dynamic, large-scale environments where policy updates need to be propagated efficiently and consistently across multiple nodes. This feature makes sure that the RPAChain can stay in sync and follow new rules without any major delays, even in networks with a lot of nodes.

Latency stays low in smaller networks because there is less communication overhead and consensus processes are simpler. For networks with fewer than 500 nodes, the system handles updates quickly, thanks to techniques like sharding and parallel processing. But as the network grows beyond 1000 nodes, latency starts to rise because of more communication and synchronization needs across nodes. However, blockchain's partitioning mechanisms keep latency manageable even in these larger networks, even though they are more complicated. Fig.5 represent the latency calculation for proposed system.

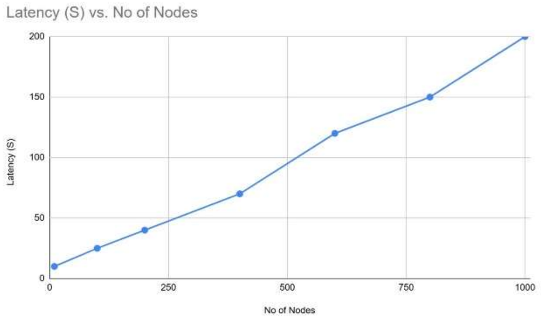

Fig. 5. Latency Calculation

When you look at throughput, smaller networks have the highest transaction rates because there is less communication between nodes, which means that routing updates can be validated and stored more quickly. In larger networks with over 1000 nodes, throughput gradually decreases due to the overhead introduced by consensus mechanisms and increased validation complexity. Still, adding smart contract-based sharding helps keep throughput moderate by letting transactions be validated in parallel. This makes sure that the system can work well in environments with changing routing rules. The system demonstrates impressive scalability, with near-linear performance improvements observed in networks with up to 500 nodes. Sharding achieves this scalability by assigning specific tasks to subsets of nodes, thereby reducing the overall processing load. However, as the number of nodes exceeds 1000, the system experiences diminishing returns in scalability. This is attributed to the growing complexity of inter-node communication and consensus overhead, which can slow down performance in larger networks. When it comes to availability, the system works really well for small to medium-sized networks. It stays almost 100% available thanks to the distributed nature of blockchain and fault-tolerant consensus mechanisms. For enormous networks exceeding 1000 nodes, availability may experience slight degradation due to the risk of network partitioning and higher resource demands. However, even in such cases, the system's decentralized architecture ensures that critical functions remain operational.

Another strong point of the system is that it can handle up to one-third of bad or malicious nodes thanks to its PBFT-inspired consensus mechanism. This ensures the integrity of routing updates and policies, even in scenarios involving adversarial activities. However, for larger networks, the increased overhead required to validate against malicious nodes can impact overall performance slightly. Nevertheless, the robust fault-tolerant design maintains the reliability of the system across all scales. Security remains robust throughout, as the blockchain's immutability and cryptographic features ensure the authenticity and integrity of routing information. By leveraging smart contracts, the system automates policy enforcement and minimizes the risk of manual errors or malicious interference. These features also protect against common BGP vulnerabilities, such as route hijacking and prefix manipulation. Policy updates efficiency is another critical aspect of the system. For smaller networks, updates are near real-time, taking only a few seconds to validate and propagate. In larger networks, the time required for policy updates increases due to communication and consensus overhead, with updates taking a few minutes in extreme cases. Even so, the system’s automation reduces the burden of manual configuration, making it far more efficient than traditional methods. Finally, smaller systems, where parallel validation ensures quick and reliable decision-making, have high consensus efficiency. For larger networks, while consensus remains secure, efficiency decreases due to the increased number of participants in the consensus process. However, advanced techniques like sharding and hierarchical consensus help mitigate these challenges, maintaining acceptable levels of performance.

5.5 Comparative Analysis

A detailed assessment of RPAChain will happen through a comparison with alternative blockchain-based inter-domain routing solutions such as ROAchain [1], BGPcoin [13] and RouteChain [4].

5.5.1. Scalability

Blockchain-based systems need scalability capabilities to process networks with growing nodes since this feature determines their ability to expand. Fig. 6 show the Scalability level comparison between existing and proposed model. RPAChain operates with a permissioned blockchain system that employs PBFT/Raft consensus mechanisms which enables it to handle 1000 Autonomous Systems (ASes) at optimal speed. The Proof-of-Work mechanism in ROAchain results in decreased scalability because its computational costs are very high. BGPcoin operates with Proof-of-Stake (PoS) but its scalability is moderate because network stakeholders with larger stakes acquire elevated power throughout the system. The PBFT consensus protocol enables RouteChain to scale effectively in networks with up to medium size yet the system requires excessive network traffic when dealing with high AS numbers. The scalability of RPAChain reaches 85% while ROAchain operates at 55% and BGPcoin runs at 65% followed by RouteChain at 60%. RPAChain demonstrates maximum scalability by processing big networks through its efficient system which outperforms PoW and PoS-based solutions in terms of time responses. Fig.6 represent the policy update calculation for proposed system

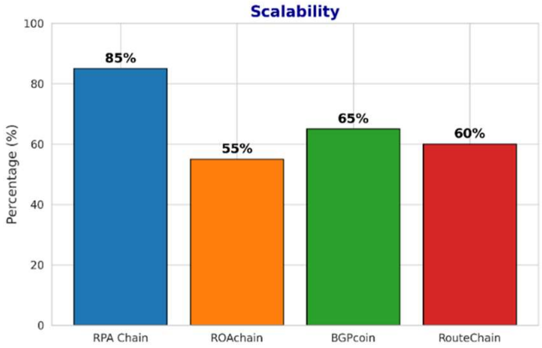

Fig. 6. Scalability

5.5.2. Security

The prioritization of security becomes crucial in inter-domain routing because BGP hijacking together with prefix leaks and route manipulation threat the network's security. Fig. 7 show the Security level comparison between existing and proposed model. The system delivers maximum security because it uses blockchain-immutable elements with automated security policies implemented through smart contracts. The system stops harmful route propagation at the same time it maintains tamper-proof policy management standards. ROAchain primarily verifies route origins through its secure approach yet provides limited protection against hijacking while allowing unauthorized policy modifications. The security features of BGPcoin fall between basic and strong since its Proof-of-Stake system remains vulnerable to Sybil attacks. The security features within RouteChain are limited since the system validates route announcement instead of actively enforcing dynamic security policies. Among four BGP security projects RPAChain stands out with a security percentage of 98% while ROAchain receives 75% and BGPcoin obtains 80% security and RouteChain settles for 70%. By combining blockchain technology and smart contracts RPAChain provides maximum security protection for BGP hijacking prevention and unauthorized policy modification.

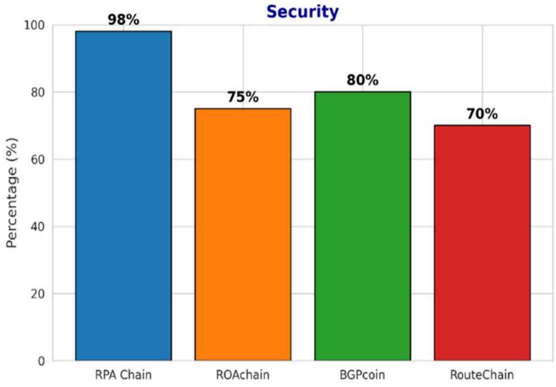

Fig. 7. Security

5.5.3. Performance

Real-time performance of blockchain-based routing systems measures two core functions: update processing speed and policy implementation speed. RPAChain delivers an efficient system performance through its adoption of advanced consensus mechanism (PBFT/Raft) which minimizes blockchain transaction latency. Real-time policies updates occur without significant performance degradation using this system. Performance problems exist in ROAchain due to its Proof of Work (PoW) structure that causes extended transaction verification periods. BGPcoin makes use of proof of stake but maintains delays during policy enforcement procedures due to its dependency on validators. The network operation of RouteChain becomes inefficient when handling extensive deployments that use PBFT. The performance score of RPAChain reaches 92% while ROAchain stands at 68% and BGPcoin at 72% and RouteChain scores 65%. The proposed system provides superior performance making it efficient for prompt policy verification and speedy enforcement beyond conventional PoW and PoS-based solutions. Fig. 8 show the Performance level comparison between existing and proposed model.

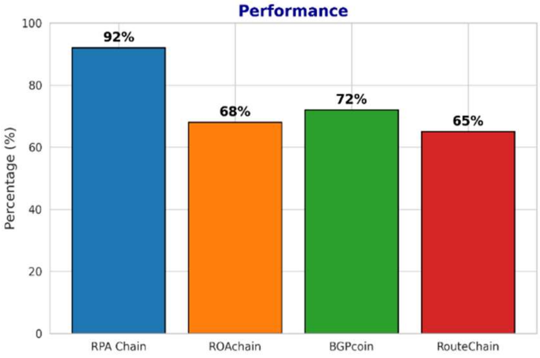

Fig. 8. Performance

5.5.4. Latency

The measurement of latency indicates how long it takes to validate routes while executing security policies. Fig. 9 show the Latency comparison between existing and proposed model. A shorter time period constitutes better performance since it accelerates inter-domain routing response times. The performance of RPAChain beats other systems since it takes 20 seconds for each transaction while the other systems require 50 seconds for ROAchain and 45 seconds for BGPcoin and 48 seconds for RouteChain. The optimized consensus mechanism in RPAChain achieves faster blockchain processing so it delivers improved performance. ROAchain suffers from PoW-related delays because of its mechanism but BGPcoin requires multiple confirmations through its PoS model which leads to slower policy validation process. PBFT adoption in RouteChain produces latency fluctuations because of the excessive network communication that takes place between nodes. Our system operates with the quickest time response which leads to faster policy execution together with routing decisions.

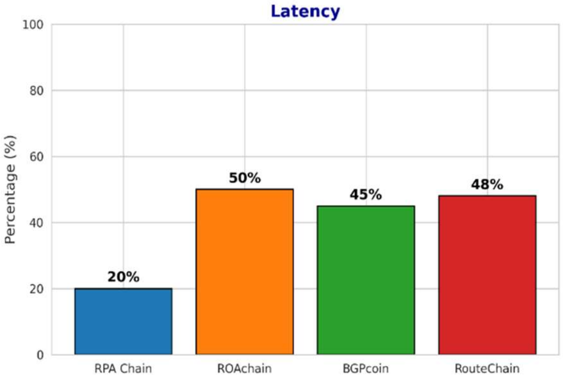

Fig. 9. Latency

5.5.5. Throughput

Throughput serves as a major performance measurement which describes the rate at which transactions together with routing updates are processed in a single second. Fig. 10 show the Throughput comparison between existing and proposed model. As a result, RPAChain outperforms all other networks with a throughput of 1000 transactions per second (TPS) whereas ROAchain operates at 600 TPS, BGPcoin at 700 TPS and RouteChain at 650 TPS. ROAchain operates at a reduced throughput speed because the Proof-of-Work algorithm demands excessive computational effort. The Protocol of Agreement consensus mechanism provides BGPcoin better performance than ROAchain yet causes scalability issues when queues of transactions need validation. The PBFT requirements create communication complexity that leads RouteChain to maintain efficiency when working with medium-sized networks yet incurs problems when handling large transaction volumes. Local Speed of RPAChain reaches 95% because it combines optimized consensus mechanisms and smart contract automation. RPAChain demonstrates the highest data processing capabilities which render it excellent for fast and extensive inter-domain routing systems.

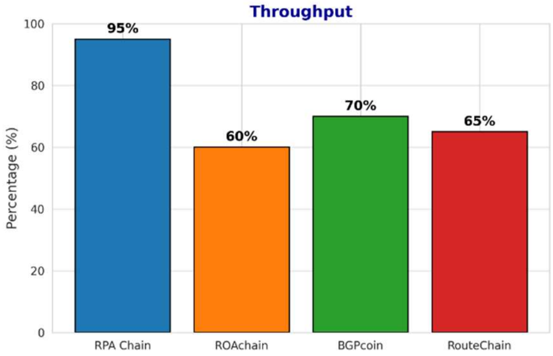

Fig. 10. Throughput

RPAChain demonstrates superior features compared to existing systems in every evaluated parameter because it delivers maximum security and automation along with speed which enables complete autonomous routing policy management while maintaining minimal threat risks. The inter-domain routing performance reaches its highest levels of efficiency (1000 TPS) and speed (20s latency) through RPAChain. RPAChain operates with energy efficiency by combining low overhead costs with exceptional security standards that PoW-based systems lack. While ROAchain and BGPcoin offer moderate solutions, RPAChain outperforms them in scalability, automation, and real-world applicability. RPAChain exists as the most efficient blockchain-based routing approach because it delivers advanced automation together with maximum security alongside unparalleled efficiency in routing management.

6. Conclusion:

The RPAChain framework proposes a critical transformation to inter-domain routing through blockchain integration with smart contracts for advancing routing policy management quality by increasing security and automatic process execution while providing enhanced visibility. RPAChain integrates blockchain characteristics with automated policy management through smart contracts to resolve BGP-based weaknesses including security vulnerabilities and manual configuration and policy inconsistency. RPAChain creates substantial benefits for the efficiency and trustworthiness of data transmission between Autonomous Systems (ASes) while maintaining secure operations. Through its implementation the system defends against BGP hijacking and implements policy compliance and facilitates automated routing stabilization along with fast performance and high data transfer speed. RPAChain outperforms the blockchain solutions ROAchain, BGPcoin and RouteChain by providing better scalability and security enforcement and more efficient consensus operation thus becoming a robust choice for next-generation inter-domain routing. The research recognizes two main obstacles that blockchain introduces through its computational overhead requirements and interoperability issues for effortless integration with existing BGP systems. The following work should concentrate on developing efficient consensus frameworks together with lowering transaction delays and boosting cross-chain functionality to improve blockchain routing automation capabilities. RPAChain presents a future-proof standard for secure automated multivendor routing since it delivers a resilient platform which matches the progressive needs of contemporary network foundations that involve 5G and IoT-based and cloud computing systems. Global networks will experience modernization through secure adaptations due to the advancing nature of blockchain technology which depends on efficient routing policy automation systems.

REFERENCES

[1] Yan, Z.; Lee, J.-H. BGPChain: Constructing a secure, smart, and agile routing infrastructure based on blockchain". The Korean Institute of Communications and Information Sciences

(KICS). ICT Express, Vol.7, Issue: 3, September 2021, pp.376–379, doi: 10.1016/j.icte.2020.12.005

[2] Lu, H.; Tang, Y.; Sun, Y. DRRS-BC: Decentralized routing registration system based on blockchain. IEEE/CAA J. Autom. Sin. Vol.8, Issue 12, December 2021, pp. 1868–1876, doi: 10.1109/JAS.2021.1004204

[3] Paillisse, J.; Manrique, J.; Bonet, G.; Rodriguez-Natal, A.; Maino, F.; Cabellos, A. Decentralized trust in the inter-domain routing infrastructure. IEEE Access 2019, 7, pp: 166896–166905, doi:. 10.1109/ACCESS.2019.2954096

[4] Saad, M.; Anwar, A.; Ahmad, A.; Alasmary, H.; Yuksel, M.; Mohaisen, A. RouteChain: Towards blockchain-based secure and efficient BGP routing. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp.210–218, doi: 10.1109/BLOC.2019.8751229

[5] M. F. Galmés, R. Coll Aumatell, A. Cabellos-Aparicio, S. Ren, X. Wei and B. Liu, "Preventing Route Leaks using a Decentralized Approach: An Experimental Evaluation," 2020 IEEE 28th International Conference on Network Protocols (ICNP), 2020, pp. 1-6, doi: 10.1109/ICNP49622.2020.9259367.

[6] Jin, J. BGP Route Leak Prevention Based on BGPsec. In Proceedings of the 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 27–30 August 2018; pp. 1–6, doi: 10.1109/VTCFall.2018.8690840

[7] Chen, D.; Ba, Y.; Qiu, H.; Zhu, J.;Wang, Q. ISRchain: Achieving efficient interdomain secure routing with blockchain. Comput. Electr. Eng. 2020, 83, 106584, doi: 10.1016/j.jpdc.2020.04.005

[8] S. Angieri, M. Bagnulo, A. García-Martínez, B. Liu and X. Wei, "InBlock4: Blockchain-based Route Origin Validation," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2020, pp. 291-296, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162879.

[9] Gómez-Arevalillo, Alfonso de la Rocha and Panos Papadimitratos. “Blockchain-based Public Key Infrastructure for Inter-Domain Secure Routing.” (2017).

[10] M. Karakus, E. Guler and S. Uludag, "QoSChain: Provisioning Inter-AS QoS in Software-Defined Networks with Blockchain," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1706-1717, June 2021, doi: 10.1109/TNSM.2021.3060476.

[11] Liu, Y.; Zhang, S.; Zhu, H.;Wan, P.J.; Gao, L.; Zhang, Y.; Tian, Z. A novel routing verification approach based on blockchain for inter-domain routing in smart metropolitan area networks. J. Parallel Distrib. Comput. 2020, 142, 77–89, doi: 10.1016j.jpdc.2020.04.005

[12] J. Jin, "BGP Route Leak Prevention Based on BGPsec," 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), 2018, pp. 1-6, doi: 10.1109/VTCFall.2018.8690840.

[13] M. Sankara Mahalingam, N. Suresh Kumar, R. Kanniga Devi, J. Logeshwaran, A reliable inter-domain routing framework for autonomous systems using hybrid Blockchain, Computers and Electrical Engineering, Volume 123, Part A, 2025, 110031, ISSN 0045-7906,10.1016/j.compeleceng.2024.110031

[14] M. F. Galmés and A. Cabellos-Aparicio, "Decentralised Internet Infrastructure: Securing Inter-Domain Routing (DEMO)," IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2021, pp. 1-2, doi: 10.1109/INFOCOMWKSHPS51825.2021.9484629.

[15] Prashanth Podili, Kotaro Kataoka, TRAQR: Trust aware End-to-End QoS routing in multi-domain SDN using Blockchain, Journal of Network and Computer Applications, Volume 182, 2021, 103055, pp: 1-19, doi: 10.1016/j.jnca.2021.103055.

[16] J. Yue, Y. Qin, S. Gao, W. Su, G. He and N. Liu, "A Privacy-Preserving Route Leak Protection Mechanism Based on Blockchain," 2021 IEEE International Conference on Information Communication and Software Engineering (ICICSE), 2021, pp. 264-269, doi: 10.1109/ICICSE52190.2021.9404125.

[17] Sfirakis, I.; Kotronis, V. Validating IP prefixes and AS-paths with blockchains. arXiv 2019, arXiv:1906.03172, doi: 10.48550/arXiv.1906.03172

[18] Ma, X.; Xu, D.; Dang, H. BGP-LSChain: An Inter-domain Link State Sharing Framework Based on Blockchain. In Proceedings of the 2019 International Conference on Blockchain Technology, Honolulu, HI, USA, 15–18 March 2019; pp. 19–23, doi: 10.1145/3320154.3320157

[19] Guobiao He, Wei Su, Shuai Gao, Member, IEEE, Jiarui Yue, and Sajal K. Das, Fellow, IEEE,

"ROAchain: Securing Route Origin Authorization with Blockchain for Inter-Domain Routing" Published in IEEE Transactions on Network and Service Management, Vol. 18, Issue: 2, June 2021 pp.1690-1705, doi: 10.1109/TNSM.2020.3015557

[20] Xing, Q.; Wang, B.; Wang, X. Bgpcoin: Blockchain-based internet number resource authority and bgp security solution. Symmetry 2018, 10, 408.