Grenze International Journal of Engineering and Technology, June Issue

Lightning Sidebridge: Decentralized RPC Load Balancer

Mayuri Kulkarni[1], Dr. Makarand Shahade[2], Deep Mahajan[3], Bhavesh Nikam[4], Rushikesh Badgujar[5] and Piyush Sharma[6]
[1-6]SVKM's Institute of Technology, Department of Computer Engineering, Dhule, India
Email: mayuridkulkarni@gmail.com, {manu1509.shahade, deepmahajan827, er.bhaveshnikam, rishinaitik1234, sharmapiyush.8378}@gmail.com

***Abstract*— The Decentralized Technology 'Blockchain' has some point Centralization in terms of Remote Procedure Call Mechanism. Relying on centralized RPC (Remote Procedure Call) is risky and running a node can be expensive, time consuming and more complex making it extremely inaccessible for most of the users. Web3 companies must spend huge expenses on maintaining their infrastructure and fault-tolerant operation. The Lightning Sidebridge is Based on the core Infrastructure of Blockchain & Decentralized RPC Load Balancing. Lightning Sidebridge (Load Balancer) is a decentralized RPC Gateway service that provides more secure and reliable access to the blockchain. Lightning Sidebridge is a decentralized network of nodes that are responsible for validating transactions and blocks. The network is secured using a various Consensus mechanism such as Proof of Stake and reputation systems. Lightning Sidebridge is designed to distribute requests across a network of Decentralized RPC nodes to avoid failure and errors. The system (Load Balancer) sits between Decentralized applications and Blockchain RPC Layer. It is designed to distribute the requests amongst a cluster of public RPC nodes. The Proposed system can reroute specific requests to another active RPC endpoint automatically if node that is currently in use goes down. Implemented nodes are hardened and secured for various attacks and continuously monitored for security vulnerabilities. as Current RPC Network is Centralized, the Proposed system is more focused on Decentralized RPC Gateway and enabling potential of decentralized node validation services in fortifying blockchain accessibility and security.**

***Index Terms*— Decentralized RPC, Decentralized Load Balancing, Proof of Work with Reputation system, Blockchain, DApps.**

I. INTRODUCTION

Web-based applications are widely used applications in day-to-day life. Due to this web technology needs to take preventive measures and needs to provide secured platform in online environment. Hence recent development in the web technology introduces the blockchain technology support hence it provides various blockchain features in web3 by integrating some services in it.

Similarly due to security reasons, in digital era blockchain technology is widely accepted by the various applications. These blockchain technology is tamper-proof and immutable [1]. Apart from immutability Markel tree is used to encode the data in secured [2,3]. Distributed node stores data and perform the consensus mechanism

Grenze ID: 01.GIJET.10.2.273

[4]. As the Blockchain network continuously grows, it is important to ensure that the network remains secure and reliable.
Full node with additional Indices consists of the Ethereum Nodes and Solana RPC node used to match the standard security aspects as integrity, availability and privacy. Integrity obtained by offering correct information on blockchains under the security models. This ensures integrity on every blockchain using Flyclient. Availability allows to access information on the blockchain by utilizing group of nodes. Through MetaMask, Infura IP address and Ethereum Wallet addresses are collected to specify confidentiality [5].
RPC services are less decentralized than blockchain networks. In other words, one RPC services to hundred of nodes and to blockchain network ten services to the hundreds of nodes. Hence this could lead to Denial-of-Service attack on DApps [6].

II. Literature Survey

A cryptocurrency wallet operates independently from the blockchain; it translates interface actions into code, which is then dispatched to a node. This code is executed and eventually incorporated into the blockchain. Ethereum is open and distributed virtual computers called Ethereum Virtual Machines (EVM). EVM is responsible for the programs called smart contract. EVM architectures verifies the EVM byte code which is not understood by the developers and users hence EVM architecture before EVM 1.5 are obsolete later EVM which introduced function calls and EVM 2.0 used on WebAssembly. EVM uses addresses to account state. The account states consist of code, storage (machine to machine word), nonce (ever-increasing machine word) and balance (fees paid to run EVM) [7].
When contract calls an account the gas amount might decrease. Gas consumption during contract calls is nondeterministic change which shorten proof goals during brute-force proving symbolic execution. Symbolic states grow rapidly which represents the remaining gas through long sequence of subtractions [7]. However, if the RPC (Remote Procedure Call) nodes, chosen by wallets and various applications, stop responding or decline requests, these applications cease to function.
Mempool in Ethereum is buffer storing the unconfirmed transactions and controls the mining and transaction propagation in downstream services. DETER attacker disables the remote Ethereum node and deny mining and propagation delay in transactions. Also reduce or zero Ether cost incur due to DETER attack on Ethereum clients [8].
Mempool is essential buffer stores the unconfirmed transactions until they are not included by miners in blockchain.By disabling Mempool services affects the revenue generation for the miners in running client.This exploits the real Ethereum clients for admission control and DOS attack at low Ether cost.Through this zero Ether cost cancelled and victimize the normal transactions[8].
DETER attack for four Ethereum clients in a local environment with 100% success rate except parity with 75.6% at zero cost[8].
Due to the substantial cost of hosting an RPC node, which amounts to at least $1,000 per month, developers of decentralized applications (DApps) frequently resort to public RPC nodes. These public RPC nodes are typically hosted by centralized entities such as Google Cloud, Amazon Web Services, and Hetzner. Notably, in the case of Hetzner, a major network provider for Solana, a recent ban on Solana nodes led to more than 22% of Solana's nodes becoming inaccessible.
Consequently, DApps relying on these RPC nodes experienced crashes. This incident with Hetzner underscores the risk of relying solely on one RPC provided by a centrally hosted service. To mitigate the potential for failure, DApp developers can create scripts, modules, or standalone apps designed to automatically switch to an alternative spare RPC endpoint when issues arise. However, if the backup RPC endpoint also fails, developers find themselves without a reliable solution. This enables wide range of services that will be provided to small cases, developers, web3 businesses, investors. Each node is required to stake a certain amount of tokens. This ensures that the nodes are invested in the security and success of the network. the staked amount by node decides its voting power in the network.
The existing Decentralized RPC systems has issue of Unpredictable budget due to volatility of tokens therefore staking constant currency plays crucial role in this. It also Solves the problem of single point of failure by eliminating Centralized RPC as a service.
In proposed system Lightning Sidebridge is a Decentralized Load Balancer that tries to eliminate centralise RPC mechanism. It is discussed in details in the proposed Methodology Section.

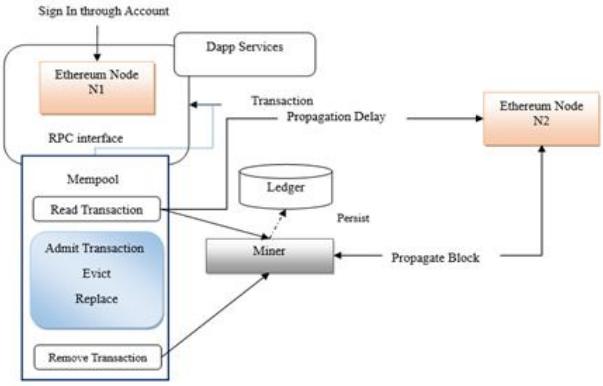

Figure 1. Ethereum Node Architecture

III. PROPOSED SYSTEM

Lightning Sidebridge also uses reputation systems to detect and prevent malicious and un-necessary behaviour on the network. The Proposed System also uses a reputation system to track the performance of each node. Nodes with a good reputation has more Chances to be selected to validate transactions and blocks, and Nodes with a bad reputation has less Chances to be selected. The bad performed Nodes can be Removed. To address this challenge, the concept of a Decentralized Load Balancer has been introduced. Its purpose is to offer a solution to this problem, ensuring continuous operation even if primary and backup RPC endpoints face disruptions.
In the market, other solutions typically fall into one of three categories:

1 .Decentralized Load Balancers with Volatile Token Payments:

These solutions require payments in tokens from volatile projects. While they offer decentralization, the reliance on such tokens can introduce an element of uncertainty.

2. Centralized Yet Accessible Load Balancers:

These solutions provide a single access point to an RPC node, making them more vulnerable in the event of attacks. it compromise's reliability.

3. DIY Load Balancers:

Creating a load balancer in-house is a complex and very costly. It involves assembling a team and setting up all the necessary infrastructure to host the solution.
The Lightning Sidebridge is designed to Outperform Best among these categories.

Decentralized RPC Mechanism over Centralized RPC Mechanism:

Using decentralized RPC instead of centralized RPC significantly enhances system performance. The absence of a single point of failure in decentralized mechanisms ensures that even if a node goes offline, it does not disrupt the network. In contrast to a centralized RPC, where the number of nodes is limited and challenging to scale, decentralized RPC allows nodes to be added autonomously without the need for central authority. This approach ensures high scalability, achieved through various methods like peer discovery protocols or decentralized RPC node clusters systems.
Furthermore, decentralized systems offer high security compared to their centralized systems. They mitigate data breaches and anonymous attacks effectively, enhancing overall network safety. Similar to centralized RPC, decentralized RPC deals error handling mechanisms, if an error occurs, a single error message is generated and transmitted to the calling node, streamlining the debugging process. In blockchain environments, consensus mechanisms are used to validate nodes. Decentralized RPC systems also bolster fault tolerance, ensuring robustness and resilience in the face of failures.
Lightning Sidebridge works by distributing requests across a cluster of RPC nodes. Each RPC node in the cluster is responsible for processing a subset of the total requests. When a DApp sends a request to Lightning Sidebridge , Lightning Sidebridge automatically routes the request to one of the RPC node in the cluster. If a node goes down, Lightning Sidebridge will automatically reroute requests to another node in the cluster.

Lightning Sidebridge can also be used to improve the performance of DApps by distributing requests across a cluster of nodes. This can help to reduce latency and improve overall throughput. Lightning Sidebridge also helps to protect DApps from attacks by making it more difficult for attackers to target
a single RPC node. If an attacker tries to target a single RPC node, Lightning Sidebridge will automatically reroute requests to other node in the cluster.
Lightning Sidebridge is building a decentralized RPC gateway. This will allow developers to connect their DApps to a cluster of public RPC nodes without having to worry about managing their own load balancer. This will make it easier for developers to build and deploy decentralized applications on the network.

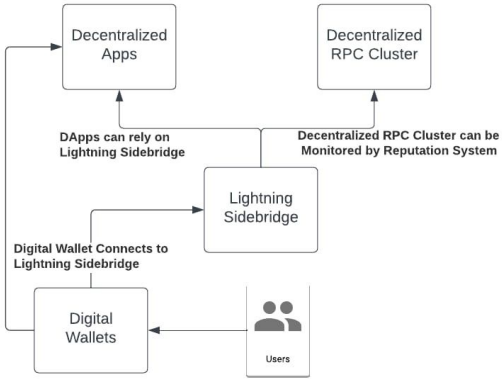

Figure 2. Overview of Lightning Sidebridge Dataflow

Current Developer Options:

Developers currently have several options when it comes to ensuring the consistent operation of the RPC layer.
Decentralized Token-Based Balancer: Developers can opt to pay for a decentralized balancer using project tokens. However, this option comes with the challenge of dealing with the fluctuating prices of these tokens.
Third-Party Centralized Balancers: Another choice is to rely on third-party providers offering centralized balancers. While accessible, this approach includes risks due to centralization.
Self-Developed Balancers: As previously mentioned, developers can also choose to create their own balancer. But, this can be a costly option, requiring a dedicated Developer team and agreements with multiple validators.
The Lightning Sidebridge Solution: The Lightning Sidebridge is an open-source load balancer that effectively distributes requests among several public RPC nodes to create a cluster. Importantly, it has the capability to automatically redirect all requests if the selected node experiences any form of failure. In practical terms, this means that a DApp will remain operational no matter the circumstances, as long as at least one RPC node is active. Additionally, this solution is free to use and straightforward to implement via Docker. Developers have the flexibility to configure it to meet their specific needs.

Various Consensus and Protocols used in Lightning Sidebridge:

*1.Proof of Stake***:** Lightning Sidebridge uses a Proof of Stake consensus mechanism to secure the network. This means that nodes are rewarded for staking their Stable (Non-Volatile) tokens. This helps to ensure that the network is always secure and reliable.
2.Reputation system: Lightning Sidebridge also uses a reputation system to help identify and prevent malicious behaviour on the network. This helps to keep the network honest and fair & Nodes are Judged on the basis of Reputation.
3.Decentralized network: Lightning Sidebridge is a decentralized network, meaning that it is not controlled by any single entity. This makes the network more resistant to censorship and attack.
It works by using a round-robin algorithm to distribute requests across the cluster of RPC nodes. This means that each RPC node will receive an equal number of requests. If an RPC node goes down, Lightning Sidebridge will automatically reroute requests to another node. The Lightning Sidebridge Also Connects 15 Professional Nodes to Public Nodes to Increase the Reliability.

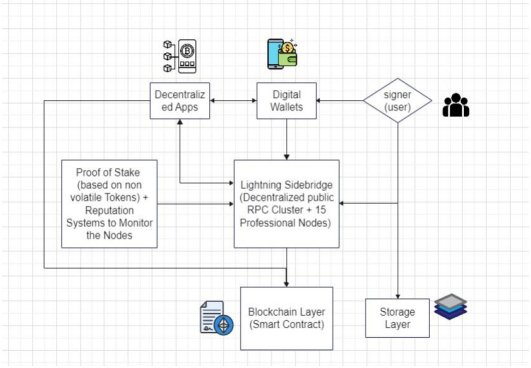

Figure 3. Lightning Sidebridge's Decentralized RPC Gateway In Blockchain Infrastructure

Optimizing Data Structure can allow to Accelerate RPC Layer:
Shred as a Data Structure: A "shred" is a fundamental data structure, often referred to as the smallest unit within a block. These shreds are transmitted across the network in the form of UDP packets, using a method known as Turbine Block Propagation. Shredding is a process that occurs after ledger entries are created.
Shredding serves two essential purposes:
1.Handling Network Limitations: Sending an entire entry as a single UDP packet is impractical due to the constraints of the IPV4 MTU (Maximum Transmission Unit), which is limited to 1500 bytes.
2.Ensuring Reliability: Shreds are erasure coded, providing redundancy to safeguard against packet loss and the deliberate dropping of packets.

Types of Shreds:

Within this context, there are two main types of shreds:
1. *Data Shreds***:** These shreds contain the actual ledger entries.
2. *Coding Shreds***:** Coding shreds are essential to provide redundancy, which protects against both network-related packet loss and malicious attempts to drop packets. The use of coding shreds is particularly critical due to the potential for UDP networks to lose packets. Unlike TCP (Transmission Control Protocol), which retransmits lost packets, UDP does not provide such guarantees.

Shred Data Layout:

Each shred adheres to a specific data layout consisting of three main components:
1. *Common Header:* This section includes information common to all shreds, providing essential details about the shred's origin and purpose.
2. ***Data or Coding Header:*** This header contains information specific to whether the shred is a data shred or a coding shred. It plays a vital role in distinguishing between the two types.
3. *Payload:* The payload encompasses the actual data, whether it's ledger entries (in the case of data shreds) or coding information (for coding shreds).

IV. Decentralized RPC Mechanism In Blockchain:

Decentralized RPC in blockchain networks increases the security by reducing point of failure & limiting attack vectors.
Traditional RPC systems are completely depends on centralized servers, which introduces the possibility of failure & poor security. In contrast, decentralized RPC distributes this communication process across multiple nodes in the blockchain network. This decentralization improves the security architecture of the network in several important aspects.
Firstly, decentralization improves the network's ability to resist attacks. Without a central access point, it will be more difficult for attackers to interfere with or disrupt RPC operations through Denial-of-service attacks or other malicious activities. Even if some nodes processing RPC requests are disrupted or attacked, other unaffected nodes can continue to provide service and maintain the integrity of the network. Second, decentralization reduces the risk of centralization, which is often a concern in blockchain systems. By decentralizing RPC operations across nodes, there is no single control centre, reducing the risk of malicious interference or manipulation. This will reduce the decision making manipulation in network.

Additionally, RPC deployment helps improve privacy and security. Direct communication between nodes means that sensitive information does not have to go through an intermediary; this reduces the possibility of information leakage or permissible errors. Nodes communicate securely and directly, increasing the overall confidentiality and security of the communication process.
In terms of Trust, decentralized RPC is in line with the principle of blockchain technology. Trust is distributed across the network rather than in a single location or server, increasing overall trust and reducing potential trust breaches. And also, decentralized management also increases the robustness and fault tolerance of the network. In a distributed RPC infrastructure, the failure of one or a few nodes will not affect the entire system. The network can offload requests to work tasks, ensure services are not interrupted, and maintain network performance even in difficult conditions.
In summary, decentralized RPC greatly increases the security and unreliability of blockchain networks by reducing vulnerabilities, increasing resilience, improving privacy, and promoting a robust and fault tolerant communication framework. Together, these features will help to create a safe & reliable blockchain ecosystem.

BENEFITS OVER EXISTING SYSTEM:

Reliability: This element is highly important in ensuring that DApps are always running even if some RPC node goes offline.
Performance: A decentralized load balancer enhances the performance of DApps by efficiently distributing requests to a cluster of nodes.
Security: It Protects DApps against potential attacks by creating it more challenging for attackers to pinpoint a single vulnerable RPC node.
Decentralization: This solution contributes to the overall resilience of the network by building a decentralized RPC gateway, thereby reducing its vulnerability to censorship attempts.
Automatic failover: The system is designed to automatically reroute the requests to another nodes if a node becomes unresponsive. This guarantees that DApps stay Functional, even when there is disruptions in the RPC layer.
Health monitoring: This feature continually monitors the health of RPC nodes within the cluster, by removing any nodes that are inactive or Corrupted nodes.
Blacklisting: Developers can use this feature to blacklist specific RPC nodes, a valuable tool for avoiding nodes with known reliability issues or malicious intent.
Whitelisting: This feature is used to whitelist specific RPC nodes, ensuring that DApps exclusively connect to trusted and verified nodes.
Denial of Service Attack Avoidance: Using all this Security Mechanism and Additional Professional Nodes It Can Avoid DoS Attacks.

V. CONCLUSION

Lightning Sidebridge presents a complex approach to address significant challenges in the area of decentralized applications and web3 infrastructure. By eliminating centralized RPC, it eliminates the vulnerability associated with single point of failure, by enhancing the system's robustness. Additionally, the integration of Proof of Stake (over stable Tokens) serves as a safeguard against Eclipse Attacks and Double Spending, by boosting the security and reliability of decentralized networks.
Furthermore, our proposed solution reduces the high maintenance and expenses associated with maintaining nodes on Web3 services and also encourages cost effectiveness, broadens accessibility for developers and users by creating the long-term sustainability of decentralized applications.
The Lightning Side-Bridge will help in enhancing the acceleration of decentralized app performance on web3 infrastructure and promise increased user experience and greater potential for adoption of decentralized technologies. This innovative solution offers a feature over existing system to enhance the security, affordability, and performance of decentralized applications, potentially reshaping the web3 ecosystem.

REFERENCES

[1] Sharma, A., Kaur, P. Tamper-proof multitenant data storage using blockchain. Peer-to-Peer Netw. Appl. 16, 431– 449 (2023). https://doi.org/10.1007/s12083-022-01410-8
[2] Chen, Y.-C.; Chou, Y.-P.; Chou, Y.-C. An Image Authentication Scheme Using Merkle Tree Mechanisms. Future Internet 2019, 11, 149. https://doi.org/10.3390/fi11070149

[3] H. Liu, X. Luo, H. Liu and X. Xia, "Merkle Tree: A Fundamental Component of Blockchains," 2021 International Conference on Electronic Information Engineering and Computer Science (EIECS), Changchun, China, 2021, pp. 556-561. https://ieeexplore.ieee.org/abstract/document/9588047/
[4] Ma, Jue. "Blockchain Consensus Mechanism Based on Improved Distributed Consistency and Hash Entropy." Scientific Programming 2021 (2021): 1-9.
[5] Zhongtang Luo, Rohan Murukutla, Aniket Kate, “Last Mile of Blockchains: RPC and Node-as-a-service”, 2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA), 978-1-6654-7408-5/22/$31.00 ©2022 IEEE DOI 10.1109/TPS-ISA56441.2022.00044
[6] Kai Li el at, “As Strong As Its Weakest Link: How to Break Blockchain DApps at RPC Service”, Network and Distributed Systems Security (NDSS) Symposium 2021 21-25 February 2021, Virtual ISBN 1-891562-66-5 https://dx.doi.org/10.14722/ndss.2021.23108
[7] Yoichi Hirai, “Defining the Ethereum Virtual Machine for Interactive Theorem Provers”
[8] Kai Li, Yibo Wang, and Yuzhe Tang. 2021. DETER: Denial of Ethereum Txpool sERvices. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS ’21), November 15– 19, 2021, Virtual Event, Republic of Korea. ACM, New York, NY, USA, 23 pages. https://doi.org/10.1145/3460120.3485369
[9] A Decentralized Remote Procedure Call Transaction Manager by Wanlei zhou (1992)
[10] Load Balancing in Blockchain Networks: A Survey by M. Baldi, S. Bracciali, C. Cavalli, A. Giaretta, and G. Mazzoni
[11] Decentralized Load Balancing for Blockchain Networks by P. Wang, D. He, and M. Li
[12] A Decentralized Load Balancing Algorithm for Blockchain Networks by Y. Li, X. Chen, and M. Zhang
[13] Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform (February 9, 2021) (Updated 2023) Whitepaper Link: https://whitepaper.io/document/718/ethereum-whitepaper
[14] Solana: A new architecture for a high-performance blockchain v0.8.13 (updated 2022) Link: https://whitepaper.io/document/602/solana-whitepaper
[15] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, “Integrated blockchain and edge computing systems: A survey, some research issues and challenges,” IEEE Commun. Surveys Tut., vol. 21, no. 2, pp. 1508–1532, Apr. 20