Blockchain-Enabled DNS: Enhancing Security and Mitigating Attacks in Domain Name Systems

Kaushal Shah*
Department of Computer Science and Engineering, School of Technology
Pandit DeenDayal Energy University
Gandhinagar, India
*shah.kaushal.a@gmail.com

Mukti Padhya
School of Cyber Security and Digital Forensics
National Forensic Sciences University
Gandhinagar, India
mukti.padhya@nfsu.ac.in

Sachin Sharma
Department of Computer Science and Engineering, School of Technology
Pandit DeenDayal Energy University
Gandhinagar, India
iamsachin3110@gmail.com

2023 6th International Conference on Signal Processing and Information Security (ICSPIS) | 979-8-3503-2959-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSPIS60075.2023.10343534

Abstract - **The importance of Internet security is increasing as businesses expand through digitalization. Like in the physical world, data transmitted over the Internet must be safeguarded to ensure confidentiality, integrity, and availability. Among the various security threats, Distributed Denial-of-Service (DDoS) attacks are widely recognized as they can potentially compromise all three aspects of data security. Despite several attempts to address these attacks, the traditional Domain Name System (DNS) has struggled to counter them effectively. In this research, we propose the concept of a Blockchain-based DNS as a solution to mitigate DNS-related threats, particularly DDoS attacks. The suggested architecture encompasses all levels of the DNS, including registrars, intermediaries (if any), and clients. By leveraging the decentralized nature of blockchain technology, this approach provides a fundamental defense against DDoS attacks, as it eliminates the vulnerability of a single point of failure. Furthermore, this work explores the appropriate type of blockchain to be used, estimates the cost of implementing such a service, and offers flexibility for organizations to adopt this solution at their discretion.**

Keywords— Information Security, DDOS, Blockchain, DNS

I. Introduction

Web architecture refers to the conceptual structure of the World Wide Web, which facilitates communication between users and the interoperability of different systems and subsystems. It is composed of various components and data formats organized in tiers that form the infrastructure of the internet. The core elements of web architecture include data transmission protocols (TCP/IP, HTTP, HTTPS), representation formats (HTML, CSS, XML), and addressing standards (URI, URL). When a user attempts to visit a website, the process involves recursive Domain Name System (DNS) queries to obtain the website's IP address from different DNS servers [1-3].

The DNS is often considered the backbone of the Internet and plays a crucial role in web interactions [4-6]. Its primary function is to translate human-readable website addresses into logical addresses (IP addresses) so that websites can be located and accessed on the internet. Although the role of DNS may seem simple, its implementation and maintenance on a larger scale to serve the entire internet can be complex.

The initial contact between the client (user's browser) and the website server is established through a 3-Way Handshake, enabling successful data transmission. In some cases, a load balancer or reverse proxy may be positioned before the main servers to manage client requests. A diagrammatic representation of this architecture is shown in the following Fig. 1.

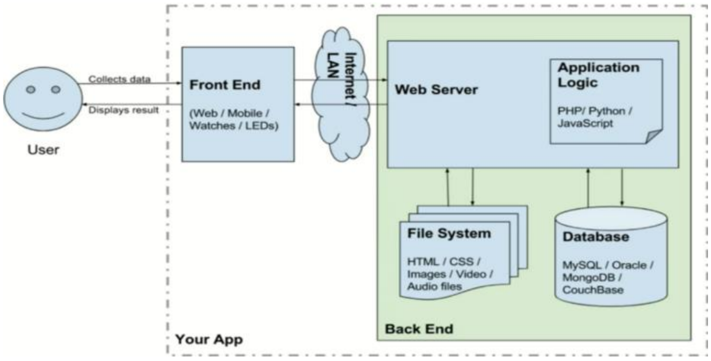

Fig. 1: The existing web architecture

The front end of the web architecture serves as the interface through which the client interacts with the server. The back end encompasses components such as the web server, application logic, file system, and databases. Once the connection is established, the client can request different pages or data from the server. The web server utilizes application logic implemented with a programming language to interact with the file system and database, retrieving the desired response for the client. However, this simplistic architecture may prove inefficient when dealing with high traffic or facing cyber-attacks [7-9].

ICANN (Internet Corporation for Assigned Names and Numbers) is a non-profit organization based in the United States that manages core DNS servers globally [10-12]. As the traditional DNS is facing threats such as Man-In-the-Middle attack, DoS Attack to address such emerging threats to the DNS system, ICANN introduced DNS Security Extensions (DNSSEC). DNSSEC adds an extra layer of security to DNS by incorporating additional records that verify the origin, authenticity, and integrity of data. The implementation of DNSSEC required minor upgrades to the DNS protocol. While DNSSEC offers some protection against Man-in-the-Middle attacks by enabling detection, it falls short as a preventive measure. To effectively utilize DNSSEC, organizations must implement an additional layer to identify and block or drop suspicious requests. The issues and challenges of traditional DNS are discussed below:

979-8-3503-2959-9/23/$31.00 ©2023 IEEE

1. **Man in the middle attack:** The authenticity of a DNS response is uncertain, making it difficult to determine if the response originates from a trusted source or if it has been maliciously altered. Although a basic resolver can rely on IP addresses to assess the legitimacy of a response, attackers can exploit this information using techniques like Man-in-the-Middle attacks. As a result, users may unknowingly be redirected to harmful destinations like phishing websites, highlighting the potential risks associated with this vulnerability.

2. **Denial of service attack:** The global DNS system operates with a limited number of servers responsible for handling all internet traffic. However, if a specific server becomes the target of a Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack [13, 14], serious problems can arise, potentially leading to a complete DNS blackout. In such attacks, the targeted server is overwhelmed by an excessive volume of queries that surpass its capacity to handle, resulting in a backlog of requests. As a consequence, legitimate users are unable to access their desired websites. The impact of these attacks goes beyond significant downtime for commercial organizations; it can also result in permanent hardware damage that requires a longer recovery time than initially expected.

3. **Issues of DNS Security Extension:** DNSSEC fails to effectively combat the significant risk posed by DDoS attacks. Although it can mitigate DNS spoofing risks through its signing policy for requests, DNSSEC lacks a mechanism to discard malicious requests, leading to potential server overload. In fact, DNSSEC inadvertently amplifies the risks associated with DDoS attacks.

Despite numerous attempts to improve traditional DNS, it has remained challenging in effectively countering the aforementioned attacks. As a result, it is imperative to introduce a new framework that can effectively mitigate DNS-related threats, particularly Distributed Denial of Service (DDoS) attacks. In the following section, we will explore the impact and potency of DDoS attacks.

A. Motivation

DDoS (Distributed Denial of Service) attacks pose a significant threat to the stability and security of the internet. These attacks have the potential to disrupt critical online services, causing inconvenience to users and financial losses to organizations. By studying notable cases of DDoS attacks, such as the one experienced by Spamhaus in 2013, we can gain insights into the scale and impact of such attacks. Understanding these incidents can help us recognize the evolving threat landscape and the need for effective mitigation strategies.

In 2013, one of the most notorious DDoS attacks occurred, targeting Spamhaus, a well-known anti-spam organization. This case study examines the details and consequences of the attack, as reported in an article published by The New York Times [15]. The attack, which started in mid-March, initially seemed manageable, with a combined effort successfully mitigating the impact of a 10-11 Gbps attack. However, the situation escalated rapidly, reaching a staggering 120 Gbps by March 22, causing widespread disruption to the internet. The effects of the attack were far-reaching, highlighting the interconnected nature of the internet. Although the attackers failed to take down CloudFlare immediately, they redirected their assault towards CloudFlare's clients. CloudFlare identified the root cause of the attack as Open DNS Resolvers, referring to them as a potential "ticking bomb." This attack was unique in that it was not a direct botnet hit but rather a staged assault.

Unfortunately, DDoS attacks continue to pose a serious threat. In 2016, Dyn, a prominent DNS provider, experienced an attack of 1.5 TBps, originating from the notorious Mirai botnet [16]. Moreover, in 2020, AWS (Amazon Web Services) faced a severe attack of approximately 2.3 TBps, surpassing the scale of the 2013 incident. These examples highlight the persistent and evolving nature of the DDoS threat.

According to a report by Cisco in March 2020, the number of DDoS attacks is projected to double by 2023 compared to 2018, with the total count already reaching a massive 7.9 million in 2018 [17]. The compelling data from Cisco's analysis underscores the criticality of implementing robust defense mechanisms and proactive strategies to combat the escalating threat of DDoS attacks. With this research, we aim to introduce the concept of a Blockchain-based DNS as a potential solution to mitigate DNS-related threats, specifically focusing on DDoS attacks.

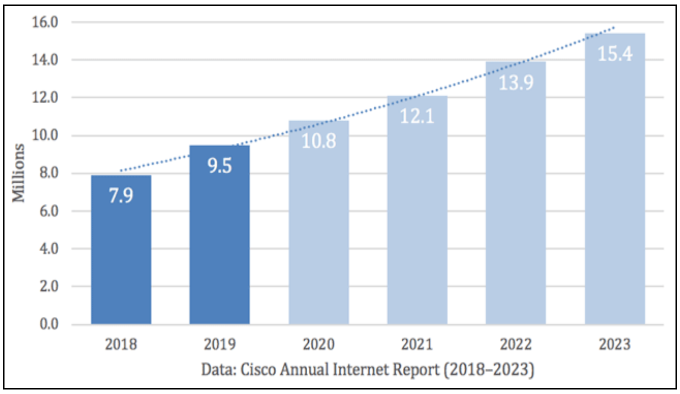

Fig. 2: Cisco Internet Report

Blockchain technology, known for its decentralized nature, offers a fundamental defense against DDoS attacks by eliminating the vulnerability of a single point of failure. Traditional DNS systems often rely on centralized servers, making them susceptible to targeted attacks. In contrast, a Blockchain-based DNS distributes the control and authority across multiple nodes in a network, making it resilient against DDoS attacks that attempt to overwhelm a single server or network segment. By utilizing blockchain, each transaction or update in the DNS record can be securely recorded and verified across the distributed network of nodes. This ensures the integrity of the DNS data and mitigates the risk of malicious tampering or unauthorized modifications. Additionally, the consensus mechanism inherent in blockchain technology provides an added layer of security, as changes to the DNS record require majority agreement from the participating nodes.

In summary, employing a Blockchain-based DNS framework offers a promising approach to mitigate DDoS attacks and enhance the overall security and resilience of DNS systems. Its decentralized nature and robust security mechanisms contribute to a more reliable and resilient infrastructure, reducing the impact and potential success of DDoS attacks on DNS services.

B. Our Contribution

Our research paper makes several key contributions in the field of mitigating DDoS attacks and improving the security and resilience of DNS systems. These contributions can be summarized as follows:

1. **Proposal of a Blockchain-based DNS Framework:** We introduce a novel Three-Tier architecture that utilizes blockchain technology to address the challenges posed by DDoS attacks in DNS systems. This framework covers all levels of the DNS, including registrars, intermediaries (if any), and clients, ensuring comprehensive protection against attacks.
2. **Mitigation of DDoS Attacks**: The proposed architecture leverages the decentralized nature of blockchain to provide core defense against DDoS attacks. By eliminating the reliance on a single point of failure, the architecture enhances the overall security and resilience of DNS systems, reducing the impact and potential success of DDoS attacks.
3. **Exploration of Attack Mitigation:** We discuss various types of attacks viz., NXDOMAIN, DNS Amplification, Cache poisoning etc. can be potentially mitigated using the blockchain-based DNS architecture. By providing an overview of the attack landscape, we highlight the effectiveness and versatility of our proposed solution in countering these threats.
4. **Cost Estimation:** In our research, we provide a price estimation that aligns closely with the yearly Standard plan for services like GoDaddy, taking into account the current rates. This information helps stakeholders assess the feasibility and economic viability of implementing the proposed architecture.
5. **Experimental Validation:** We demonstrate the successful achievement of the identified objectives through an experimental setup. By implementing and testing the proposed blockchain-based DNS framework, we validate its effectiveness in mitigating DDoS attacks and improving the overall security of DNS systems.

In conclusion, our research contributes a comprehensive and innovative approach to mitigating DDoS attacks in DNS systems through the utilization of a Blockchain-based DNS framework. Our findings provide valuable insights into the benefits of blockchain technology and its potential to enhance the security, resilience, and economic viability of DNS infrastructure.

C. Outline of The Paper

The rest of the paper is organized as follows: First, we review some background knowledge and related work in Section 2. The overview of the proposed scheme, framework, and the system model are defined in Section 3. The empirical analysis is made in Section 4. Conclusion and future extensions are provided in Section 5. References are at the end.

II. Related work

Since the speculations of blockchain based DNS system began, there have been some review papers that highlighted the potential of such a system. The authors in a paper titled “A brief review of blockchain-based DNS systems” [7] provided a detailed background regarding the existence of DNS and explored some alternatives such as Namecoin [8] and blockstacks [9]. In a similar work titled “Ethereum Name Service: The Good, the Bad, and the Ugly” [10] authors described the potential dangers in Ethereum platform itself along with the risks of vulnerable smart contracts and how attackers were abusing the ENS. Agostinho, Bruno Machado introduced an interesting idea of WDNS [11] of associating Ethereum wallets with a name. For example, some wallet with address say 0xffff2fffdff5ffcf would be associated with a name xyz@domain. Karaarslan, Enis, and Eylul Adiguzel in their work [12] introduced an architecture to control the signing in blockchain based DNS system.

In a work titled “B-DNS: A secure and efficient DNS based on the blockchain technology” [13] the authors introduced a stable system for establishing a blockchain based DNS in detail. They later compared the performance particularly with PowerDNS. An interesting idea was put together as BlockZone [14], which included the intended consensus algorithm particularly for the setup.

III. Proposed Work

To comprehensively address the traditional DNS associated challenges, we suggest a 3-Tier architecture, depicted in the Fig. 3. The details of Tier Architecture are discussed below:

1. **Tier-1** consists of a consortium blockchain that authorizes the addition of records while allowing public access for lookups. It's important to note that adding records to this tier necessitates the payment of a fixed fee according to the blockchain policy. The implementation of the consensus algorithm remains unaffected.

2. **Tier-2** is an optional tier that offers organizations additional flexibility at the organizational level. Organizations can regulate the websites that can be accessed and those that are restricted. One recommended approach is to maintain a list of permitted websites. This can be accomplished by establishing an intermediate consortium blockchain network between the client and the top level. Moreover, this approach brings an additional advantage. In a production environment, instead of modifying something like the "/etc/hosts" file on the server, changes can be implemented directly on this intermediate blockchain.

3. **Tier-3** is where the end user is situated within the system. Once a successful lookup occurs, the corresponding record can be stored as a "cache" on a local blockchain. It is crucial to update the stored data periodically. A similar concept was employed in the work referenced as [18]. In a local setup, this blockchain would serve as an additional security layer where all users within a specific section share access to the consortium DNS maintained by a network administrator.

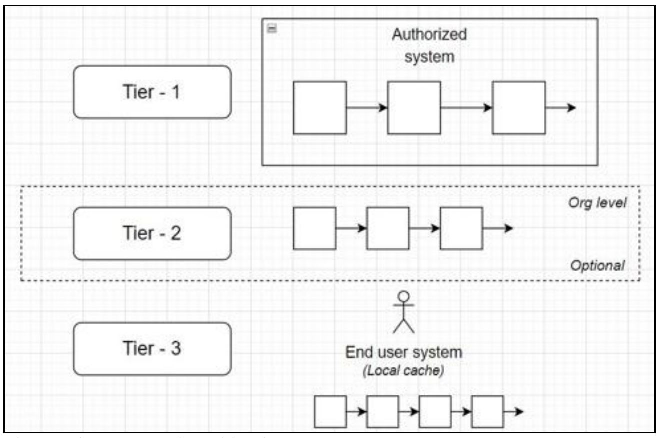

Fig. 3: The Proposed Architechture

A. Smart Contrct Design

A smart contract is comparable to an algorithmic program that operates on the blockchain and is responsible for executing predefined tasks while ensuring policy enforcement. The implementation of the smart contract for Tier-1 is quite extensive and somewhat intricate. It serves two crucial roles: adding records and performing record lookups. There exist various types of DNS records associated with a domain, and each of them should be considered and implemented as necessary.

The implementation of Tier-2 depends on the specific requirements of the organization. On the other hand, Tier-3 is once again a consortium implementation, but with the authority of a section administrator to make specific changes. However, all the records retrieved from any of the above tiers should be recorded on this blockchain setup.
Furthermore, an auto-updating mechanism is implemented to ensure that the records are regularly updated after a certain period of time. The figure provides a general overview of the working process. In this case, the smart contract was written in Solidity, and an online IDE called Remix was utilized for compilation and other related purposes.

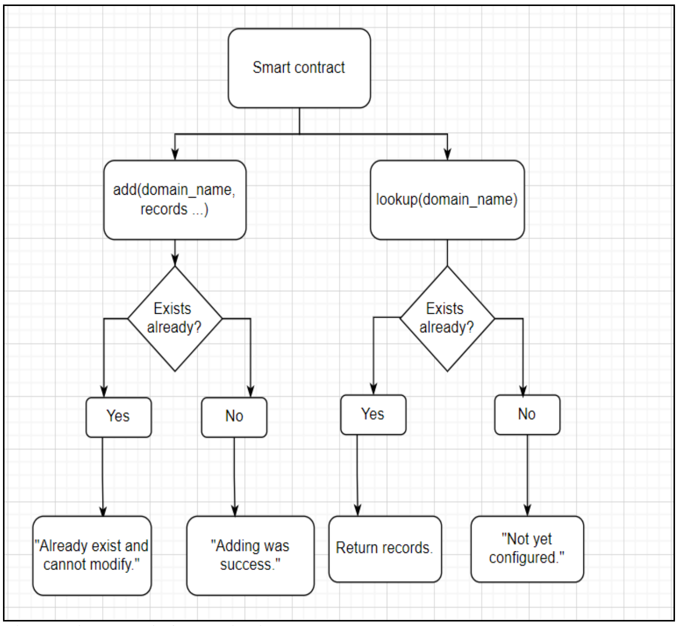

Fig. 4: FlowGraph for Designing Smart Contract

B. Deploying and connection

The interface developed in section 3.2 requires integration with a smart contract deployed on the test net, specifically on the Rinkeby network. To establish the connection between these two components, the web interface and the smart contract, we will utilize Web3. Web3 is a recent trend that aims to incorporate blockchain features, such as decentralization, at its core.
To establish a successful connection, we need the following components:

1. The address of the deployed smart contract.
2. The Application Binary Interface (ABI) code, which is generated as bytecode for the Ethereum runtime.
3. Functions that enable active interaction with the defined functions within the smart contract.

The Fig. 5 provides a general overview of the workflow involved in achieving this integration.

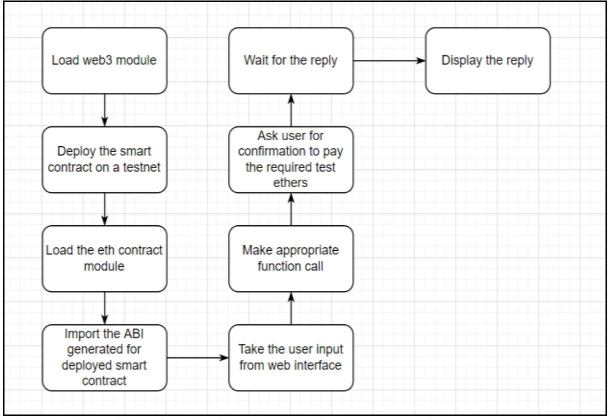
Load web3 module
Deploy the smart contract on a testnet
Load the eth contract module
Import the ABI generated for deployed smart contract
Take the user input from web interface
Make appropriate function call
Ask user for confirmation to pay the required test ethers
Wait for the reply
Display the reply

Fig. 5: Flowchart for deployment and connection between components

IV. Results and Analysis

In this section, we provide details regarding the experimental setup used for evaluation purposes. We also delve into the discussion of the results obtained from performance and cost analyses. Furthermore, we conduct a comprehensive comparison between the security aspects of a blockchain-based DNS solution and traditional DNS.

A. Experimental Setup

To effectively demonstrate the intended mechanism, a web interface is required, which will serve as both Tier-1 for authorized record addition and Tier-3 for record lookup. To fulfill this purpose, any format can be utilized, but in this case, we will utilize a specific format: an input field accompanied by an "Add" button for DNS record addition. For the sake of simplicity, we have used the A record as an example. Similarly, a "lookup" button is included to retrieve records. A straightforward template has been developed using HTML, CSS, and JS. The figure depicts the utilized interface.

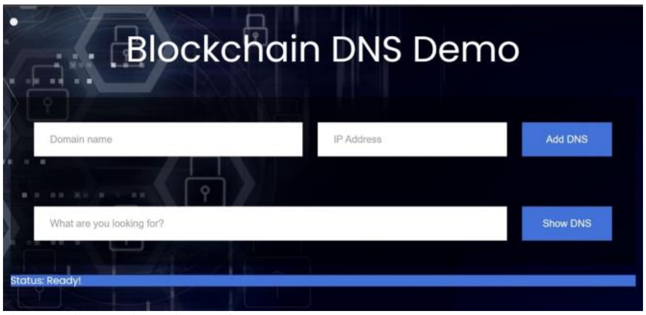

Fig. 6: The Designed Interface

In order to assess the effectiveness of the setup, a straightforward script was developed to initiate concurrent connection requests. As a result, an example DNS server, implemented in Golang, experienced a crash when subjected to approximately 5,000 requests. This experimental setup demonstrated its capability to withstand a simulated "supposed" DDoS attack, particularly during the lookup procedure.

However, when a state-changing DDOS attack was executed on a local blockchain network utilizing ganache, the gas limit appeared to increase, and the attack was automatically halted. Nevertheless, this incident caused a significant slowdown in normal transactions for a temporary period of time.

B. Performance and Cost Analysis

In this section, our focus has been primarily on transaction time, specifically in the context of the Rinkeby test net. Although this is a test environment, it provides a reliable estimate of transaction durations. Gas is a concept in the blockchain ecosystem that represents the fee required for a transaction to be processed. Higher gas fees tend to attract more attention from miners, while transactions with low gas fees may never be executed. In our analysis, we have used Wei as the unit of measurement, which is the smallest denomination of ether [19]. During the testing phase, the gas price for Rinkeby was determined to be 3 Gwei. Using this as the base value, we derived five additional values by dividing and multiplying by 10 and 2: 0.3, 1.5, 3, 6, and 30. The table provided represents the average waiting time for transactions associated with each gas value.

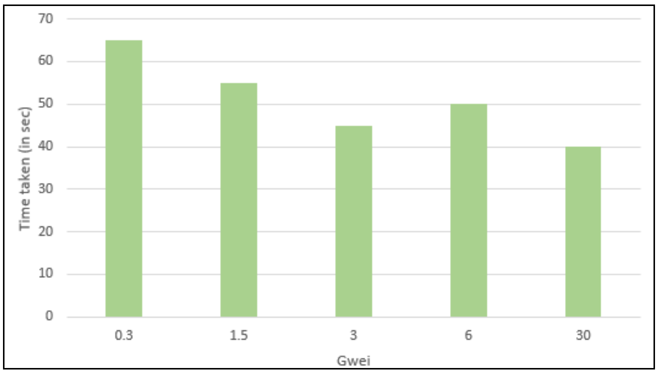

Fig. 7: Average Time Taken for Transactions

The results indicate that a gas value of 30 Gwei had the shortest waiting time, while 0.3 Gwei had the longest. However, it is noteworthy that 6 Gwei offered the best average transaction time, which also appeared to be cost-effective. At the time of testing, considering the current exchange rate [20-23], this gas fee amounted to approximately $15.78. This fee can be considered as the baseline cost to be paid when registering a domain at Tier-1.

C. Comparativve Analysis

The blockchain-based DNS offers enhanced resilience compared to the legacy DNS system, addressing some of its core vulnerabilities. The following TABLE I provides a comparison of the two systems in terms of their ability to address various DNS attacks.

TABLE I. Comparative analysis

Type of Attack	Legacy DNS	Blockchain DNS
DDOS	No	Yes
NXDOMAIN	No	Yes
DNS Amplification	No	Yes
Cache Poisoning	No	Yes

One key reason why DDoS attacks are ineffective against blockchain-based DNS is due to the fundamental property of decentralization inherent in blockchain. Being peer-to-peer in nature, every node in the blockchain is connected and holds the record. This makes it virtually impossible to alter or poison any single node through a Sybil attack. While DDoS attacks are highly impactful when targeting a single centralized target, executing such an attack on a blockchain-based DNS would require an enormous amount of resources and power to bring down the entire network, rendering it impractical.

It's important to note that even if a DDoS attack is carried out by overwhelming the network with information, such as by flooding it with excessive requests to add records, it would not bring down the blockchain network. Instead, the continuous influx of requests would cause the Gas Price to rise, making it increasingly difficult for the attacker to sustain the attack due to the higher computational costs involved in blockchain transactions.

In summary, the decentralized nature of blockchain-based DNS provides robust defense against DDoS attacks, making it significantly more resilient compared to the legacy DNS system.

V. Conclusion and Future work

This research introduces a blockchain-based architecture that aims to mitigate DDoS attacks and leverage other benefits offered by blockchain technology. Furthermore, various types of attacks viz., NXDOMAIN, DNS Amplification, Cache poisoning etc. can potentially be mitigated using this architecture are discussed. The provided price estimation aligns closely with the yearly Standard plan for services like GoDaddy, taking into account the current rates.

As a burgeoning technology, blockchain has the potential to enhance security measures while offering flexibility and robustness. The experimental setup demonstrates the successful achievement of the identified objectives.

To expand on this research, it is possible to address real-life challenges associated with the functioning of the World Wide Web (WWW). An example of such a challenge is the use of reverse proxy to handle incoming requests and distribute them across multiple servers to prevent overloading. This functionality can be implemented at Tier-1 of the proposed architecture. Additionally, it is beneficial to incorporate a signing procedure, particularly at the protocol level like SMTP (Simple Mail Transfer Protocol), to mitigate related attacks. By including this security measure, potential vulnerabilities can be minimized. Furthermore, the inclusion of a maintenance bot, such as crawlers, can enhance the system's efficiency by keeping track of active domains. Implementing this feature at Tier-1 allows for better monitoring and management of the network. Lastly, to cater to the varying needs of customers, it is advisable to make the fee estimation more flexible. This flexibility would enable customization of the fee structure based on individual customer requirements and preferences.

References

[1] Fielding, Roy T.; Taylor, Richard N. “Principled design of the modern Web architecture,” ACM Transactions on Internet Technology, vol. 2(2), pp. 115–150,2002. doi:10.1145/514183.514185.

[2] Muzaki, Rizki Agung, Obrina Candra Briliyant, Maulana Andika Hasditama, and Hamzah Ritchi. "Improving Security of Web-Based Application Using ModSecurity and Reverse Proxy in Web Application Firewall." In 2020 International Workshop on Big Data and Information Security (IWBIS), pp. 85-90. IEEE, 2020. doi:10.1109/IWBIS50925.2020.9255601

[3] Karakostas, Bill. "A DNS architecture for the internet of things: A case study in transport logistics." Procedia Computer Science 19, pp. 594-601, 2013. doi: 10.1016/j.procs.2013.06.079

[4] Liu, Daiping, Shuai Hao, and Haining Wang. "All your dns records point to us: Understanding the security threats of dangling dns records." In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 1414-1425. 2016. doi:10.1145/2976749.2978387

[5] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized business review , 21260, 2008.

[6] Ariyapperuma, Suranjith, and Chris J. Mitchell. "Security vulnerabilities in DNS and DNSSEC." In The Second International Conference on Availability, Reliability and Security (ARES'07), pp. 335-342. IEEE, 2007. doi:10.1109/ares.2007.139

[7] Shah, Kaushal, et al. "Blockchain-based Pharmaceutical Drug Supply Chain Management System." 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). IEEE, 2022.

[8] Al-Mashhadi, Saif, and Selvakumar Manickam. "A brief review of blockchain-based dns systems." International Journal of Internet Technology and Secured Transactions 10, vol. 4, pp. 420-432, 2020.

[9] Ali, Muneeb, Jude Nelson, Ryan Shea, and Michael J. Freedman. "Blockstack: A global naming and storage system secured by blockchains." In 2016 USENIX annual technical conference (USENIX ATC 16), pp. 181-194. 2016.

[10] Xia, Pengcheng, Haoyu Wang, Zhou Yu, Xinyu Liu, Xiapu Luo, and Guoai Xu. "Ethereum name service: the good, the bad, and the ugly." arXiv preprint arXiv:2104.05185, 2021.

[11] Agostinho, Bruno Machado, Fellipe Bratti Pasini, Fernanda Oliveira Gomes, Alex Sandro Roschildt Pinto, and Mario Antônio Ribeiro Dantas. "An Approach Adopting Ethereum as a Wallet Domain Name System within the Economy of Things Context." In 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC), pp. 176-185. IEEE, 2020.

[12] Shah, Kaushal, et al. "Hireblock: Hyperledger-based Human Resource Recruitment System." 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). IEEE, 2022.

[13] Karaarslan, Enis, and Eylul Adiguzel. "Blockchain based DNS and PKI solutions." IEEE Communications Standards Magazine 2, no. 3, pp. 52-57, 2018.

[14] Li, Zecheng, Shang Gao, Zhe Peng, Songtao Guo, Yuanyuan Yang, and Bin Xiao. "B-DNS: A secure and efficient DNS based on the blockchain technology." IEEE Transactions on Network Science and Engineering 8, no. 2, pp. 1674-1686, 2021.

[15] Shah, Kaushal, et al. "Exploring applications of blockchain technology for Industry 4.0." Materials Today: Proceedings 62 (2022): 7238-7242.

[16] Wang, Wentong, Ning Hu, and Xin Liu. "Blockzone: A blockchain-based dns storage and retrieval scheme." In Artificial Intelligence and Security: 5th International Conference, ICAIS 2019, New York, NY, USA, July 26–28, 2019, Proceedings, Part IV, pp. 155-166. Cham: Springer International Publishing, 2019.

[17] Adrian Taylor, “The 5 most famous DDoS attacks in history”, September 19, 2020, [Online]. Available: https://bdtechtalks.com/2020/09/19/top-5-ddos-attacks-in-history/

[18] Cisco, U. "Cisco annual internet report (2018–2023) white paper." Cisco: San Jose, CA, USA 10, no. 1 (2020): 1-35.

[19] Yu, Zhong, Dong Xue, Jiulun Fan, and Chang Guo. "DNSTSM: DNS cache resources trusted sharing model based on consortium blockchain." IEEE Access, vol. 8, pp. 13640-13650, 2020.

[20] Makadiya, Yogi, Rutvi Virparia, and Kaushal Shah. "IoT Forensics System based on Blockchain." 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2023.

[21] Lathiya, Dhruvil, Naimish Lukhi, and Kaushal Shah. "Blockchain-enabled Dynamic Document Ownership Verification." 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2023.

[22] Dave, Nisarg, et al. "Secured E-voting System Through Blockchain Technology." Intelligent Sustainable Systems: Proceedings of ICISS 2022. Singapore: Springer Nature Singapore, 2022. 247-260.

[23] Shah, Kaushal, et al. "Securing Cookies/Sessions Through Non-fungible Tokens." International Conference on Database Systems for Advanced Applications. Cham: Springer International Publishing, 2022.