2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)
Pune, India. Oct 17 - 19, 2024

D-DNS: A Decentralized Domain Name System on the Blockchain: Implementation and Assessment

2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) | 979-8-3503-5434-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICBDS61829.2024.10837028

[1]Usha Divakarla,
N M A M Institute of Technology,
Nitte, Karkala, Karnataka
ushachavali@gmail.com,

[2]K Chandrasekaran
National Insttitute of Technology
Karnakata, Surathkal
kch@nitk.edu.in

Abstract—**Cache poisoning and DDoS attacks are just two of the many ways that the Domain Name System (DNS), an essential part of the Internet infrastructure, can be attacked. Countermeasures have been suggested, although they are not without restrictions. This article introduces D-DNS, a domain name system built on blockchain technology that can offer effective and safe DNS services. D-DNS solves two issues with current blockchain-based DNS systems: the inefficient query handling and the computationally demanding Proof-of-Work (PoW) protocol. D-DNS accomplishes this by putting in place a domain index and a Proof-of-Stake (PoS) consensus mechanism. To evaluate the security of D-DNS versus legacy DNS in terms of attack success rate, attack cost, and attack surface, a new quantitative comparison is presented.. According to experimental results, the attack surface of D-DNS is substantially less than that of legacy DNS, the attack cost is a million times higher, and the chance of a successful attack on D-DNS is 1% of a successful attack on legacy DNS. When D-DNS query performance is compared to the most advanced commercial DNS implementations, it is demonstrated to achieve equivalent or even reduced query latency.**

Keywords— DNS, blockchain, security, efficiency, PoS, attack surface

I. INTRODUCTION

IP addresses are unique identifiers for resources on the Internet, but domain names are easier to remember for users. The Domain Name System (DNS) provides a mapping service between domain names and IP addresses. However, existing DNS has weaknesses that attackers, such as poor verification methods and single points of failure can exploit.Cache poisoning attacks and DDoS attacks are two common threats to DNS security. Cache poisoning occurs when attackers inject false DNS records into a recursive resolver's cache, leading to clients being directed to a phishing website when they visit the affected domain. DDoS attacks target critical name servers, causing disruptions to sub-domains and reducing the availability of the entire DNS. These attacks have impacted large organisations such as Bandesco and Dyn. Various countermeasures have been proposed to address these vulnerabilities, such as using DNSSEC and raising the entropy of query packets to improve verification, and keeping additional resource records in the cache to mitigate DDoS attacks. However, these solutions have limitations and are not foolproof.

To address these challenges, a blockchain-based decentralised DNS, known as D-DNS, is proposed. D-DNS blockchain's tamper-proof storage and peer-to-peer network to provide a secure and efficient DNS service. It overcomes the limitations of existing blockchain-based DNS systems by implementing a Proof-of-Stake (PoS) consensus protocol and a domain index. A comparison between D-DNS and legacy DNS shows that the probability of a successful attack on D-DNS is significantly lower, the attack cost is higher, and the attack surface is smaller. Additionally, D-DNS achieves similar or lower query latency compared to commercial DNS implementations. Despite the advantages of blockchain-based DNS, challenges remain in its implementation. The centralised Certificate Authority used in traditional TLS security is susceptible to single-point failure and illegal certificate issuance, making T-DNS security uncertain. D-DNS faces challenges in building a secure and efficient blockchain-based DNS system beyond just storing resource records. The proposed solution offers a new perspective for future DNS development.

In this work, we describe a secure and effective domain name system based on blockchain technology: D-DNS. D-DNS employs an index to speed up blockchain searches and stores DNS records as transactions in order to provide effective name service. With D-DNS, users can interact directly with D-DNS name servers and the technology is backwards compatible with the previous DNS system, including recursive resolvers.

This work's remaining sections are organized as follows: The histories of blockchain technology and conventional DNS are covered in Part II. Part III includes detailed D-DNS design information as well as a discussion of the approach for bridging the old DNS and D-DNS gaps. The results of experiments pertaining to D-DNS security and functionality are presented in Section IV. In part V, we finally wrap up the work.

II. LITERATURE SURVEY

In this section, we will present information on previous research and activities focused on improving the security and efficiency of existing DNS systems, as well as initiatives aimed at creating domain name systems using blockchain technology

A. Security and Performance

A number of tactics have been put out to prevent cache poisoning attacks. For instance, Dagon et al. proposed combining capital and lowercase characters in a query packet's domain name to make it more challenging for adversaries to figure out the right combination [7]. Perdisci et al. employed wildcard domain names, such as example: com, in a similar manner to hinder attackers from effectively guessing domain names [8]. By using this method, a recursive resolver can recognize valid answer packets by appending random strings to the requested domain name. Furthermore, a user tracking technique was presented by Klein et al. [18] that permits tracking of user activity even when the user is using privacy mode across various browsers.

DNSSEC, which creates a trust chain from the root server to authoritative name servers, is another method for boosting security. This enables a recursive resolver to examine a response packet's signatures in order to confirm the query route [19]. Nevertheless, DNSSEC's adoption rate is still low even after it has been suggested for a long time [20]. Only 1% of.com,.net, and.org domains were found to have enabled DNSSEC in a recent survey. This phenomenon can be attributed to a number of factors, including the difficulty of implementing DNSSEC, additional costs, and political considerations (such as hostility from some countries toward the nation where the root servers are located) [8]. In an analysis of 2.1 million DNSSEC keys, Shulman et al.[8] investigated the cryptographic security of DNSSEC-signed domains. They discovered that 35% of the keys are signed with RSA keys that are shared with another domain, and 66% utilize keys that are too short. They came to the conclusion that subpar key creation procedures are the root of this issue. Researchers have suggested T-DNS, which makes use of Transport Layer Security (TLS), as a way to create secure DNS channels. In order to protect against DDoS attacks, Pappas et al. extended the time-to-live (TTL) of DNS records [10]. This ensures that important domains continue to function even in the event that DDoS assaults are launched against their parent domains. Similarly, Ballani et al. suggested storing expired entries in a different "stale cache" that is built within the recursive resolver [9]. Using this method, a recursive resolver can finish the query process by using the records that are stored in the stale cache in the event that it does not receive a response from the authoritative server. Additionally, efforts have been undertaken to assess how well root servers perform in the face of DDoS attacks [4], with some research indicating that large-scale attacks have the ability to overload specific root servers. Furthermore, a DNS-based schema was presented by Alieyan et al[10]. to identify botnets by query and response behaviours. In contrast, Gao et al. proposed several detection and mitigation methods for DDoS attacks.

B. *Blockchain based Name Service*

Numerous initiatives have been made to improve DNS performance via research. For example, Park et al. have proposed CoDNS, a cooperative DNS lookup service, which can be gradually implemented to enhance the current nameservers. Lookup latency has been reduced by 28–82% thanks to this method. Gao et al. have concentrated on offering workable solutions to enhance DNS update performance, which can take a long time. Furthermore, an analytical model has been presented by Alouf et al.[22] for the analysis of expiration-based caching systems in order to identify the best distribution for maximizing hit probability across a network of caches. Another suggestion is ContainerDNS, which maximizes memory and cache management, packet processing, and DNS performance to offer scalable and high-speed DNS for massive container cloud systems.

A blockchain-based naming system called Namecoin was created to establish a namespace. In terms of block size, mining frequency, and scripting mechanism, it is comparable to Bitcoin. Merged mining is used by Namecoin to guarantee data consistency. The majority of registered domains, however, are squatter and unactive, according to an empirical study, which puts the name system at serious risk [16]. The Bitcoin-like technology is also susceptible to mining attacks. Despite the fact that Blockchain-DNS offers a browser-side name resolving solution for Namecoin, Namecoin's inherent issues restrict its use. Another blockchain-based naming and storing solution that was introduced is called Blockstack. Deploying the Blockstack system is facilitated by its quick bootstrapping and cross-chain migration capabilities. Yao et al. have suggested using cloud computing to lessen the blockchain's processing burden and enable low-processing DNS devices to take part in consensus. Lastly, by introducing an Internet of Things (IoT)-based cloud system that offers a safe infrastructure for setting up D-DNS, Stergiou et al. hope to address security and privacy problems. Apart from examining the current blockchain-based DNS server implementations, we also carried out a thorough analysis of roughly ten research articles related to this topic. We were able to determine the drawbacks and restrictions of each of these strategies by this examination. We used a GAP analysis methodology to suggest a novel design and implementation strategy for our DNS system in order to overcome these problems. Through this thorough process, we were able to pinpoint the weaknesses in our current methods and provide a better solution. The following table I highlights some of the weaknesses of the existing models.

TABLE I. SHORTCOMINGS OF EXISTING RELATED WORKS

Ref Num	Paper Synopsis	Limitations
[12]	The paper introduces RootChain, a blockchain-based architecture designed to address single point of failure, accountability, and transparency concerns in distributed root zone operation inside the Domain Name System (DNS). Using a number of root servers, RootChain enables designated top-level domain (TLD) authority to immediately publish verified data while using smart contracts to log every transaction on the blockchain.	The paper lacks a comprehensive analysis of potential security risks and attacks that could still be relevant in the proposed RootChain architecture, such as smart contract vulnerabilities, 51% attacks, and potential collusion among delegated top-level domain (TLD) authorities.
[13]	In the study, a blockchain-based architecture called RootChain is proposed for distributed root zone operation in the DNS, which is used for managing Internet of Things devices. By strengthening delegated TLD authority and putting smart contracts into place, RootChain seeks to decentralize TLD data publication and enhance accountability and transparency.	The potential limitations of the RootChain architecture include scalability, interoperability, security, governance, and real-world implementation and adoption. Scalability, interoperability with other systems, and security measures are not fully addressed in the paper. Additionally, governance mechanisms and real-world implementation details are not clearly defined.
[14]	In this paper, the decentralized alternative to the conventional Domain Name System (DNS) based on blockchain technology is discussed. It draws attention to the problems and security worries that come with implementing this revolutionary technology. The risks to the blockchain DNS ecosystem—such as browser extensions, blockchain chains (Namecoin and Emercoin), registered domains, and users—are validated	The paper lacks a thorough evaluation of the proposed approach. The authors do not provide a comprehensive analysis of the effectiveness and limitations of their methodology. The evaluation metrics used in the paper may be limited, and the results may not be generalisable to different scenarios or datasets, which weakens the overall robustness of the research.

	empirically by the authors.	
[15]	The blockchain-based domain name system known as B-DNS is presented in the paper as a safe and effective replacement for conventional DNS. To solve the drawbacks of the present blockchain-based DNS, B-DNS uses domain indexing in conjunction with a proof-of-work consensus algorithm. In comparison to old DNS, experimental results demonstrate improved security and query performance.	The paper does not thoroughly discuss the potential weaknesses or limitations of the research. A more comprehensive analysis of the limitations and potential mitigations would provide a more balanced perspective on the results and strengthen the overall validity of the research.
[16]	This study presents a novel approach that makes use of blockchain technology for website verification. In order to prevent URL redirection assaults, the suggested method entails utilizing a smart contract to record the IP address and URL of a reliable website in a blockchain and to perform DNS queries.	The paper does not thoroughly analyze potential limitations and challenges of the proposed mechanism, such as scalability, performance impact, real-world feasibility, and regulatory compliance. The implementation on Ethereum Quorum simulation platform
[17]	The study addresses the flaws and vulnerabilities of current techniques like IP whitelisting and DNS filtering by proposing a revolutionary blockchain-based website verification methodology. The system stores the IP address and URL of a website with permission in a blockchain smart contract that is impervious to manipulation..	The potential shortcomings include a lack of comprehensive analysis of security risks like smart contract vulnerabilities and collusion among permissioned nodes, limited discussion on scalability concerns, regulatory challenges related to data protection and smart contract legality, and platform-specific implementation on Ethereum Quorum, which may hinder interoperability.
[18]	The study suggests a novel blockchain-based technique to decentralize DNS data storage and solve the shortcomings of the existing hierarchical root server architecture. Multiple parallel DNS nodes are established using the planned DecDNS system, which stores important zone file resolution data. According to experimental findings, DecDNS avoids tampering with domain name resolution data, removes single points of failure, and offers regular resolution services.	The paper proposes DecDNS, a new blockchain-based method for decentralising DNS data storage to enhance stability and security. While experimental results show promising outcomes, potential shortcomings include insufficient analysis of security risks, scalability concerns, performance impact, and regulatory challenges.
[19]	The goal of TD-Root, a reliable decentralized DNS root management architecture built on permissioned blockchain, is to use blockchain technology to increase security, resilience, and trustworthiness in order to mitigate the risks and vulnerabilities associated with centralised DNS root management..	The paper lacks in-depth analysis and discussion of potential limitations and challenges of TD-Root. It only validates the system through simulation using Google Cloud, which may not fully reflect real-world performance and security concerns.
[20]	The paper proposes a new approach for detecting malicious behaviour in blockchain transactions by analysing domain names associated with blockchain accounts. The authors leverage the temporal aspects of these domain names and achieve a balanced accuracy of 89.53% in detecting malicious blockchain domain names.	The authors do not provide a thorough overview of existing research and techniques related to threats in decentralised DNS. This omission weakens the paper's contextualisation and may result in a limited understanding of the current state of the field.
[21]	The paper analyses the abuse of blockchain DNS solutions, Namecoin and Emercoin, by malicious actors through longitudinal analysis. The authors use a haircut blacklisting policy and taint analysis on metadata to identify and quantify malicious activities.	The paper has several shortcomings, including the lack of a comprehensive overview of related work, limited evaluation of the proposed methodology, insufficient discussion on ethical considerations, inadequate implementation details, and limited discussion on limitations and generalizability.

III. Methodology

In this section, we provide a detailed design of D-DNS D-DNS's architecture will consist of three layers, which allows for good extensibility. The loosely-coupled relationship between the layers also enables upgrading a layer in the future without affecting the operation of other layers.

We use Quorum as the underlying blockchain technology to implement D-DNS. Using Quorum as the underlying technology, we can create a distributed, consensus-driven database for storing DNS records that is more resilient to attack and more resistant to censorship than a traditional DNS system. Additionally, Quorum's privacy features enable us to implement a permissioned network where only authorised parties can participate in the DNS resolution process. With these features, we can create a D-DNS system that is more secure, scalable, and reliable than existing DNS systems.

The Quorum DNS solution is a unique and innovative approach to solving the trust issue in the traditional DNS system. In the traditional system, the root DNS servers have ultimate control over record authentication. They can potentially change the DNSSEC public key published via the registrar, creating an implicit trust issue. However, in Quorum DNS, the user's wallet public key, tied to their identity on the platform, is used instead of the root DNS servers, eliminating the need for implicit trust. Quorum DNS is built on a fast proof-of-history chain that allows updates to occur within DNS TTL windows, making it possible to update records in 30 seconds instead of 10 minutes. This also solves the eventual consistency and propagation delay issues that have been problematic in the traditional DNS system. Additionally, the distributed properties of past DNS systems as shown in Fig-1 are retained in Quorum DNS because all records are signed using the domain owner's public key, allowing any node to serve up records without users having to trust them implicitly. This ensures that the query results are always signed with a key that can be verified, preventing malicious middleboxes from modifying records. Quorum DNS is not a simple "blockchain" solution but a novel distributed database-style solution that is feasible due to the fast proof-of-history chains used in its design.

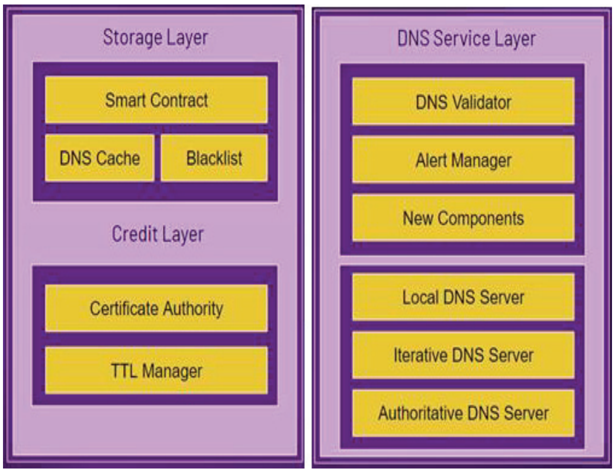

Fig. 1. High-level design of D-DNS

The D-DNS system has a storage layer where DNS records are stored as transactions in a blockchain. To ensure the immutability of the records, a new format called "operation records" will be used, with three types: registration, update, and revocation. Registering a new domain must be done with the corresponding registry, and its information must be signed and encapsulated into a registration record. The update record is used when an IP address changes and needs to be updated in the corresponding registration record. Finally, the revocation record terminates domain ownership, which is automatically done for expired domains. The operation record system is similar to Bitcoin's scripting system, allowing domain ownership and transaction content changes. The blockchain also stores each registry's stake and public keys in the block header, updated every epoch for the PoS consensus protocol. The 3-layer architecture of D-DNS provides good extensibility and allows for future upgrades to a single layer without affecting the others.

The flow of data throughout the system can be summarized with the following diagram as shown in Fig-2

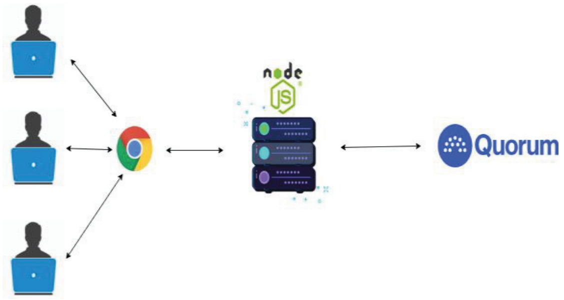

Fig. 2. Data Flow Diagram of D-DNS

The data flows through the stack is as follows

- User makes requests via DNS or HTTP.(runs in-browser) / direct request via DNS or REST API
- Local Node Server - Main JavaScript logic handles CLI commands, DNS queries, and HTTP requests (runs locally)
- Quorum Network API - Calls out via Quorum w3 JSON RPC API to the Quorum network.
- Quorum BPF Rust Program On-Chain - The uploaded BPF Rust program spends your account tokens to run on the Quorum network and perform reads/writes of stored data.

Quorum Blockchain - Quorum provides the data storage layer to hold the records.

Our proposed D-DNS system uses the blockchain technology to provide domain name services to both resolvers and end-users. To enable different types of communication with different entities, D-DNS has three network interfaces. The name servers in D-DNS use different types of messages, such as inv, getblock, getdata, and getmerklepath messages, for data transmission. The communication between name servers is peer-to-peer, which makes the D-DNS network decentralized and secure. This decentralization makes D-DNS a more reliable and robust domain name resolution system.

D-DNS functions as an authoritative name server at the D-DNS 'Name servers to Recursive resolvers' interface, retrieving the desired DNS record from the blockchain that is stored in response to DNS queries. This indicates that customers can seamlessly switch to the D-DNS system because it is compatible with legacy DNS. Clients can add their IP addresses to their resolv.conf file to enable direct communication with D-DNS name servers. A complete node such as the D-DNS name server may easily retrieve the necessary DNS record from the blockchain. However, in the event that it is a light node, it must determine whether the desired DNS entries are kept locally and, if not, it must query a full node in order to obtain the necessary information.. This ensures that even light nodes can access the required DNS records in a timely and efficient manner.A full node stores a complete copy of the blockchain, while a light node only stores a portion of the blockchain or relies on other nodes to access the complete blockchain.

Finally, at the 'D-DNS Name servers to the Users' interface, the query process for D-DNS name servers is different from legacy DNS, as D-DNS name servers are structured peer-to-peer. A full node can respond to the client directly by fetching the required DNS record from the blockchain. However, if the D-DNS name server is a light node, it needs to redirect the query to a full node if the requested DNS record is not stored locally. This approach ensures that the D-DNS system is both efficient and resilient, providing a more reliable and decentralized domain name resolution system. Our contribution to the network layer of D-DNS involves leveraging the benefits of blockchain technology to create a decentralized and secure domain name resolution system. By using a peer-to-peer communication model between D-DNS name servers and implementing an efficient query process for both full nodes and light nodes, we can ensure that the D-DNS system is both efficient and resilient. The use of a blockchain-based system also ensures that D-DNS is more secure and reliable, providing a more robust domain name resolution system for both resolvers and end-users.

The proposed method for integrating a blockchain-based DNS system with the existing DNS service layer involves creating a new layer between the client and the DNS resolver that acts as a bridge to the blockchain-based system. This is achieved through the use of a proxy server that intercepts DNS requests from clients and forwards them to the appropriate DNS resolver. The proxy server then queries a Quorum blockchain, which is a permissioned variant of Ethereum, to retrieve the corresponding IP address for the requested domain name. The Quorum blockchain is used to provide a secure, decentralized, and permissioned layer for managing domain name resolution.

To ensure the security and reliability of the system, the Quorum blockchain uses a combination of Raft consensus and PoS coin flipping consensus. The Raft consensus algorithm ensures that all nodes in the system agree on a common state, while the PoS coin flipping consensus mechanism provides a fair and unbiased way to influence the outcome of consensus. By leveraging the benefits of blockchain technology, such as decentralization, immutability, and transparency, the proposed method provides a more secure and reliable domain name resolution system.

The proposed contribution to the DNS service layer involves utilizing the existing DNS infrastructure as a layer of indirection between the client and the blockchain-based DNS system. This approach allows for the integration of a secure and decentralized layer for managing domain name resolution without disrupting the current DNS architecture. By using a Quorum blockchain with Raft consensus mechanisms, we can ensure the security, reliability, and fairness of the system while still retaining the benefits of the existing DNS service layer.

IV. Research analysis

A. *DNS Spoofing*

DNS spoofing, also known as DNS cache poisoning or DNS hijacking, is an attack where an attacker intercepts DNS queries and returns false information to the DNS resolver. This attack aims to redirect the victim to a malicious website, steal sensitive information or carry out other types of attacks. In a blockchain-based DNS server, the decentralised nature of the network makes it more difficult for attackers to compromise a significant number of nodes to carry out a successful DNS spoofing attack. However, it is not impossible, as attackers can still target individual nodes or use social engineering tactics to trick users into connecting to a malicious node.

Cryptographic techniques such as digital signatures can be used to verify the authenticity of DNS records to prevent DNS spoofing in a blockchain-based DNS server. This means that the DNS resolver can verify that the DNS record received from a node on the network is genuine and has not been tampered with. This can be achieved through public key cryptography, where the nodes on the network have their public and private keys.

B. *DNS Cache Poisoning*

DNS cache poisoning, also known as DNS spoofing, is a type of attack where an attacker sends false DNS responses to a DNS resolver. This attack aims to corrupt the DNS cache with bogus records, which can then be used to redirect users to malicious sites or carry out other types of attacks. In a blockchain-based DNS server, DNS cache poisoning can be mitigated using techniques such as cryptographic verification, similar to those used to prevent DNS spoofing. Additionally decentralized nature of the network can help prevent DNS cache poisoning by making it more difficult for an attacker to target a single point of failure.Another technique that can prevent DNS cache poisoning is using TTL (Time to Live) values in DNS records. These values determine how long a DNS record should be cached by a DNS resolver before it is refreshed. By setting lower TTL values, the DNS records are refreshed more frequently, which can help prevent the DNS cache from being poisoned with bogus records.

C. *Distributed Denial of Service (DDoS) Attacks*

Distributed Denial of Service (DDoS) attacks are a type of attack where an attacker overwhelms a server with traffic, making it unavailable to legitimate users. This is achieved by flooding the server with high traffic from multiple sources, often using a botnet of compromised devices. In a blockchain-based DNS server, DDoS attacks can be mitigated by the decentralized nature of the network. Since the DNS records are distributed across multiple nodes, it is more difficult for an attacker to target a single point of failure. This means that even if some nodes on the network are compromised, the rest of the nodes can continue to function normally, reducing the impact of the DDoS attack. Additionally, using a consensus algorithm such as proof-of-work or proof-of-stake can further enhance the security of the blockchain-based DNS server against DDoS attacks. The consensus algorithm ensures that the network validates any changes to the DNS records, making it more difficult for an attacker to carry out a successful DDoS attack. Other techniques that can be used to prevent DDoS attacks include rate limiting, where incoming traffic is limited to a certain threshold, and firewalls or intrusion detection systems to detect and block malicious traffic.

D. *Performance Evaluation*

To begin with, we used a custom-built implementation of D-DNS that was designed to run on a private blockchain network. We chose to use a private blockchain network because it allows us to have full control over the network and easily simulate different scenarios. We set up a network of nodes that are responsible for maintaining the blockchain and resolving DNS queries. Each node has a copy of the blockchain and participates in the consensus protocol to validate transactions and maintain the integrity of the system. We used a combination of Python scripts and tools to simulate DNS queries and record the latency and CDF data. For the latency vs. time graph, we set up a script that sends a large number of DNS queries to both the legacy DNS and D-DNS systems simultaneously and records the time it takes for each query to return a response. We then plotted the data points on a graph to visualize the latency trends over time. For the CDF vs. latency graph as shown in Fig-3, we used a similar approach but with a larger number of queries. We recorded the response times for each query and calculated the CDF based on the distribution of the response times. We then plotted the CDF vs. latency data for both the legacy DNS and D-DNS systems to compare their performance.

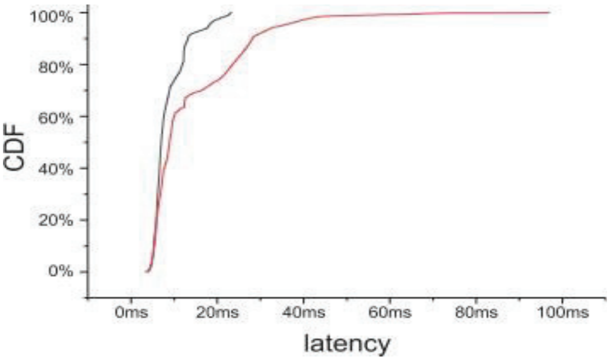

Fig. 3. CDF vs Latency of legacy DNS and Decentralised DNS

The graph titled "CDF vs Latency of legacy DNS and D-DNS" compares the cumulative distribution function (CDF) of latency for legacy DNS and decentralized DNS. Latency refers to the time it takes for a DNS query to receive a response. The CDF shows the probability that the latency will be less than or equal to a certain value. The graph shows that D-DNS has a lower latency than legacy DNS for most of the range of values. This means that decentralized DNS is generally faster at responding to DNS queries than legacy DNS. However, there are still some cases where legacy DNS has lower latency than decentralized DNS. Overall, the graph suggests that D-DNS can provide faster DNS resolution times than legacy DNS

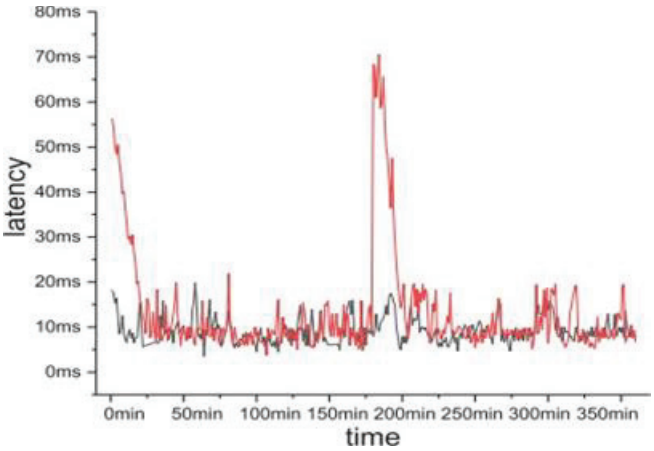

Fig. 4. Latency vs Time graph of legacy DNS and Decentralised DNS

The "Latency vs Time" graph as shown in Fig-4 compares the response time of D-DNS and legacy DNS over time. It shows that D-DNS consistently responds faster to DNS queries than legacy DNS. Additionally, while both D-DNS and legacy DNS experience occasional spikes in latency, D-DNS exhibits less frequent and less severe spikes, indicating greater consistency and reliability in DNS resolution times. This superior performance of D-DNS can lead to improved user experience and better application performance that rely on DNS resolution.

V. Conclusion and Future Work

The proposed D-DNS system provides a secure and efficient solution for domain name resolution. It is compatible with current DNS and can offer better defence against common DNS attacks, including cache poisoning attacks and DDoS attacks. Our research actively explores the construction of the next-generation DNS infrastructure. It provides a potential solution for building domain name systems for a wide area network, local area network, or intranet. In Conclusion, D-DNS represents a significant step forward in the evolution of DNS technology. Overall, our research contributes to the ongoing effort to enhance the security and efficiency of domain name resolution. The proposed D-DNS system offers a promising solution to the challenges faced by traditional DNS systems, and it has the potential to revolutionise how we manage and resolve domain names in the future.

Based on the findings of this research, there are several areas of future work that could be explored. One possible direction is to investigate the performance and scalability of the D-DNS system under various network conditions and loads. This could involve conducting more extensive testing and analysis to evaluate the system's ability to handle large-scale DNS queries and ensure that it remains fast and reliable.

Finally, further research could be conducted to evaluate the security of the D-DNS system and identify potential vulnerabilities or attack vectors. This could involve conducting penetration testing and vulnerability assessments to ensure that the system remains secure in the face of various threats and attacks. Overall, there are many potential avenues for future work in the area of blockchain-based DNS systems, and continued research in this field could lead to important advancements in internet security and privacy.

References

[1] M. A. Aslam, H. Irfan, M. F. Arshad and S. A. W. Gillani, "A Study to Distribute the Data of Blockchain in a DHT-Based System for DNS," 2021 15th International Conference on Open Source Systems and Technologies (ICOSST), Lahore, Pakistan, 2021, pp. 1-6, doi: 10.1109/ICOSST53930.2021.9683861.

[2] Z. Li, S. Gao, Z. Peng, S. Guo, Y. Yang and B. Xiao, "B-DNS: A Secure and Efficient DNS Based on the Blockchain Technology," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1674-1686, 1 April-June 2021, doi: 10.1109/TNSE.2021.3068788.

[3] Z. Yu, D. Xue, J. Fan and C. Guo, "DNSTSM: DNS Cache Resources Trusted Sharing Model Based on Consortium Blockchain," in IEEE Access, vol. 8, pp. 13640-13650, 2020, doi: 10.1109/ACCESS.2020.2966428.

[4] M. Caldeira and M. Correia, "Blockchain Address Transparency with DNS," 2021 IEEE Symposium on Computers and Communications (ISCC), Athens, Greece,2021, pp. 1-7, doi: 10.1109/ISCC53001.2021.9631542.

[5] E. Karaarslan and E. Adiguzel, "Blockchain Based DNS and PKI Solutions," in IEEE Communications Standards Magazine, vol. 2, no. 3, pp. 52-57, SEPTEMBER 2018, doi: 10.1109/MCOMSTD.2018.1800023.

[6] J. Wang, Y. Yu, J. Zhao and H. Yu, "The Blockchain Name System (BNS): Polymorphic Identification Technology for Blockchain Supervision," *2021 4th International Conference on Hot Information-Centric Networking (HotICN)*, Nanjing, China, 2021, pp. 19-25, doi: 10.1109/HotICN53262.2021.9680835.

[7] J. Choncholas, K. Bhardwaj and A. Gavrilovska, "The Performance Argument for Blockchain-based Edge DNS Caching," 2021 IEEE/ACM Symposium on Edge Computing (SEC), San Jose, CA, USA, 2021, pp. 312-318, doi: 10.1145/3453142.3491288.

[8] B. Rajendran, G. Palaniappan, D. R, B. B. S and S. S D, "A Universal Domain Name Resolution Service – Need and Challenges - Study on Blockchain Based Naming Services," 2022 IEEE Region 10 Symposium (TENSYMP), Mumbai, India, 2022, pp. 1-6, doi: 10.1109/TENSYMP54529.2022.9864361.

[9] W. -B. Hsieh, J. -S. Leu and J. -I. Takada, "Use chains to block DNS attacks: A trusty blockchain-based domain name system," in Journal of Communications and Networks, vol. 24, no. 3, pp. 347-356, June 2022, doi: 10.23919/JCN.2022.000009.

[10] L. Jin, S. Hao, Y. Huang, H. Wang and C. Cotton, "DNSonChain: Delegating Privacy-Preserved DNS Resolution to Blockchain," 2021 IEEE 29th International Conference on Network Protocols (ICNP), Dallas, TX, USA, 2021, pp. 1-11, doi: 10.1109/ICNP52444.2021.9651951.

[11] C. Patsakis, F. Casino, N. Lykousas and V. Katos, "Unravelling Ariadne's Thread: Exploring the Threats of Decentralised DNS," in IEEE Access, vol. 8, pp. 118559-118571, 2020, doi: 10.1109/ACCESS.2020.3004727

[12] J. Wang, Y. Yu, J. Zhao and H. Yu, "The Blockchain Name System (BNS): Polymorphic Identification Technology for Blockchain Supervision," *2021 4th International Conference on Hot Information-Centric Networking (HotICN)*, Nanjing, China, 2021, pp. 19-25, doi: 10.1109/HotICN53262.2021.9680835.

[13] J. Choncholas, K. Bhardwaj and A. Gavrilovska, "The Performance Argument for Blockchain-based Edge DNS Caching," 2021 IEEE/ACM Symposium on Edge Computing (SEC), San Jose, CA, USA, 2021, pp. 312-318, doi: 10.1145/3453142.3491288.

[14] B. Rajendran, G. Palaniappan, D. R, B. B. S and S. S D, "A Universal Domain Name Resolution Service – Need and Challenges - Study on

Blockchain Based Naming Services," 2022 IEEE Region 10 Symposium (TENSYMP), Mumbai, India, 2022, pp. 1-6, doi: 10.1109/TENSYMP54529.2022.9864361.

[15] W. -B. Hsieh, J. -S. Leu and J. -I. Takada, "Use chains to block DNS attacks: A trusty blockchain-based domain name system," in Journal of Communications and Networks, vol. 24, no. 3, pp. 347-356, June 2022, doi: 10.23919/JCN.2022.000009.

[16] C. Patsakis, F. Casino, N. Lykousas and V. Katos, "Unravelling Ariadne's Thread: Exploring the Threats of Decentralised DNS," in IEEE Access, vol. 8, pp. 118559-118571, 2020, doi: 10.1109/ACCESS.2020.3004727

[17] Y. Li and S. Xu, "Design and Implementation of a Scalable Distributed DNS System," 2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS), Chengdu, China, 2021, pp. 528-535, doi: 10.1109/ICCCS52626.2021.9449106.

[18] X. Yuchi, S. Zhang, Z. Yan, K. Dong, H. Li and Z. Zhang, "A Trusted Notifier Reporting Framework for Incentive DNS Abuse Mitigation Based on Blockchain," 2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Hangzhou, China, 2022, pp. 35-40, doi: 10.1109/CSCWD54268.2022.9776110 Based on Blockchain," 2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Hangzhou, China, 2022, pp. 35-40, doi: 10.1109/CSCWD54268.2022.9776110

[19] Hangzhou, China, 2022, pp. 35-40, doi: 10.1109/CSCWD54268.2022.9776110 Based on Blockchain," 2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Hangzhou, China, 2022, pp. 35-40, doi: 10.1109/CSCWD54268.2022.9776110.

[20] Z. A. E. Houda, A. Hafid and L. Khoukhi, "BrainChain - A Machine learning Approach for protecting Blockchain applications using SDN," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9148808.

[21] A. K. Yıldız, A. Atmaca, A. Ö. Solak, Y. C. Tursun and S. Bahtiyar, "A Trust Based DNS System to Prevent Eclipse Attack on Blockchain Networks," 2022 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 2022, pp. 01-08, doi: 10.1109/SIN56466.2022.9970533.

[22] A. K. Yıldız, A. Atmaca, A. Ö. Solak, Y. C. Tursun and S. Bahtiyar, "A Trust Based DNS System to Prevent Eclipse Attack on Blockchain Networks," 2022 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 2022, pp. 01-08, doi: 10.1109/SIN56466.2022.9970533