2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) | 979-8-3503-9926-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICACITE57410.2023.10182552

SSHTDNS: A Blockchain-Based Secure, Scalable, and High-Throughput Domain Name System

Dr. Baldev Singh,
Professor,
Department of Computer Science Engineering,
Vivekananda Global University,
Jaipur, India,
baldev_singh@vgu.ac.in

Ms. Kavita,
Assistant Professor,
Department of Master of Computer Application,
Chandigarh School of Business,
Jhanjeri,
kavita.j1612@cgc.ac.in

Abstract: - **The Internet's crucial domain name system is in charge of translating domain names into IP addresses. However, because of its dispersed structure with a hub, it is subject to significant security concerns. Since the creation of Bitcoin, blockchain has drawn a lot of attention owing to its decentralized, trustworthy, and secure features. In this article, we suggest SSHTDNS, a brand-brand-new domain name system built on the blockchain. SSHTDNS selects the consortium chain form to ensure the management of Top-Level Domain names, and these consortium nodes use linkable ring signature technology for identity anonymity and vote fairness. Shading protocol is used in multi-chain structures to increase the system's scalability and throughput. A domain name system that combines these methods can be safe, scalable, and high-throughput.**

Keywords: Blockchain, Security, Scalability, DNS, Nebulas.

I. INTRODUCTION

ICANN which is in charge of scheduling and operating the system, is the dispatch center for the DNS at the moment. The DNS system now in use is susceptible to DDoS attacks, cache poisoning, disappearing danger, blinding risk, and other threats. 77% of firms reported experiencing at least one DNS assault in 2018, according to the Global DNS Threat Report 2018. Although several academics have put forth alternatives, such as DNSSEC [1], which uses signature and hash algorithms to ensure data dependability and integrity, there are still significant centralization problems with the DNS. A single point of failure and power abuse will result from an attack on or takeover of ICANN, which poses a major risk to the whole domain name system.

Blockchain's decentralization, security, and credibility make it look like a solution. One of the most well-known Blockchain initiatives is Bitcoin, which Satoshi Nakamoto suggested in 2009 [2]. Blockchain is the name given to the method used to create Bitcoin. Blockchain may be separated into a private chain, public chain, and consortium chain. Ethereum, a Blockchain 1.0-based smart contract platform contracts, is the representation of Blockchain 2.0, whereas Bitcoin represents Blockchain 1.0[3] in order to give developers a platform on which to create Decentralized Applications (DAPP), considerably enhancing the blockchain's functionality. The first blockchain-based area title system is Name coin [4], despite significant security risks. The primarynomenclatureclassification is called Block stack [5], and its speed is constrained by Bitcoin. There are also other methods, like Consortiums [6] and Nebulas [7]. These projects' scalability and throughput, which will be covered in depth in Section, do not, however, fulfil the domain name service. 2. Figure 1 shows the interest over time of Blockchain, over the years. Numbers show search interest in relation to the chart's peak for the specified area and period. The term's maximum popularity is a value of 100. When the value is 50, the term's popularity is halved. If a phrase has a score of 0, it signifies that there was insufficient data.

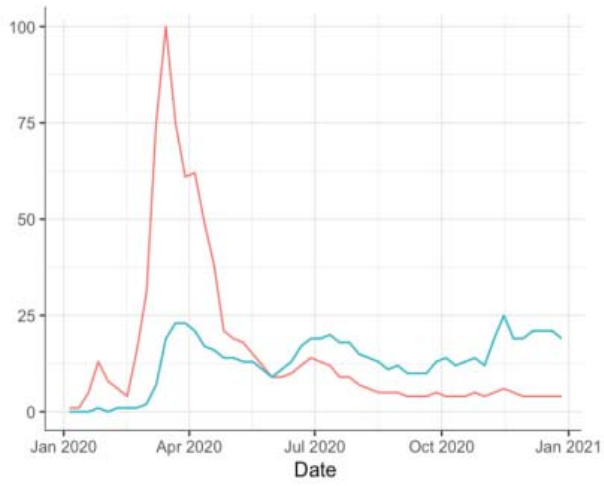

Fig. 1. Interest Over Time

In this study, an SSHTDNS, or secure, scalable, high-throughput domain name system, is proposed. There are three categories in the Top-Level Domain, including generic. Top-Level Domains like com, country-code Top-Level Domains like us, and infrastructure Top-Level Domains area, is the most significant domain name in the current DNS [8]. SSHTDNS considers using a consortium chain to lessen the degree of centralization and administer TLDs more effectively. A number of consortium nodes are kept up-to-date by each nation; each nation applies for, builds, and maintains a consortium node. Each node can create a consortium to administer the Chain, and the international organization determines the precise allotment. The application to register a TLD shall be decided by the fair vote of the consortium. Linkable ring signature technology is used by SSHTDNS to guarantee voting process fairness and anonymity. The blockchain's throughput is increased via the sharing protocol thanks to the network's increased computing capacity. SSHTDNS has three different Node kinds include light nodes, normal nodes, and consortium nodes.

The following sections make up the remainder of this essay. The introduction to further DNS initiatives using blockchain technology is provided in Section 2. The full plan

of SSHTDNS, the operation of the nodes, &cryptographical method utilized are all covered in Section 3. In Section 4, the features of SSHTDNS are examined. This task is concluded in Section 5.

II. Literature Review

A. EarlyDNS:

The inventors had no idea that the Internet would eventually be used by people all over the world. Consequently, they did not take the system's security into account. It is therefore essentially susceptible as a result. Solutions to increase system security have also been progressively proposed as a result of the growing use of DNS. Then, agenizes put up a plan that makes use of symmetric encryption to protect against replay attacks and offer data confidentiality [9]. Wilkinson employed the SCOLD main components' indirect routing strategy to fight against DDoS attacks. To identify DNS spoofing attempts, Fangled Guo imported cookies [10].

B. Namecoin:

The first use of blockchain technology and domain name service is Name coin [5]. All current domain names, including.com.bit, may be converted with. Bit added since Namecoinuses.bit as its TLD name. However, Name coin employs PoW as its consensus method, making it susceptible to 51% attacks owing to its low computer power. Despite this, Name coin is still very valuable for enhancing domain name services.

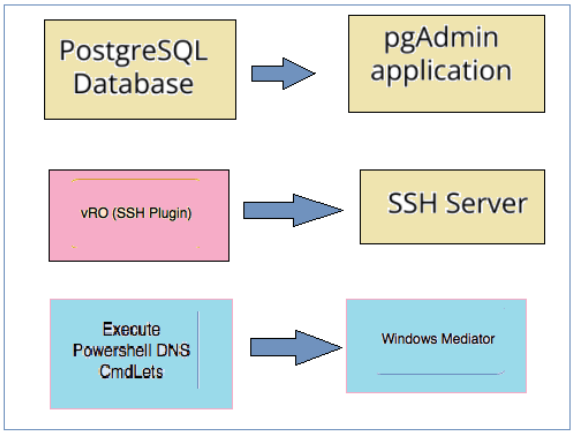

Fig. 2. SSHTDNS

1) Consortium Nodes: - The consortium nodes, which often do not offer areadesignationdeterminationfacilities, are primarily in charge of processing scheduling the normal nodes and making queries to the TLD, creating system settings.

2) Ordinary Nodes: -Any member can become a complete node as elongated as they have deployed all of the system's information, which is also known as an ordinary node or full node. Subsect. 2's Step 2's node identity setup procedure is finished after that. When using the sharing protocol, regular nodes can take part in block creation procedure on a specific sub chain.

3) Light Nodes: -The Bitcoin system has so far topped 200 GB. A light node is a participant who simply stores the

C. Blockstack and Nebulas:

ConsideringName coin's security issue. Layering blockchains and employing the virtual chain approach prevent Bitcoin nodes from being aware of Block stack in the interim, but the consequence is that Block stack's speed is constrained by Nebulas [7] is a platform akin to Bitcoin. Block stack in that it replaces the current domain name system with a global distributed directory.

D. Consortium DNS:

A brand-new domain name service called Consortiums [8] is suggested and is built on a consortium chain. To speed up DNS resolution, Consortiums creates indexes for blocks and records in the interim.

III. Proposed Methodology

A. SSHTDNSChainStructure:

There are three types of chains: public, consortium, and private. the three subtypes of blockchain. Anyone may participate in the entire process and enjoy the same rights thanks to public chain's total decentralization. Private chains are centralized, often used within an organization, and accessible to certain individuals or institutions. The consortium chain, which has several locations, is frequently used to create partnerships between various businesses to govern the blockchain. The balance between decentralization and permission management in consortium chain is godet frequently stands for a nation or organization, such us, or org; as shown in figure 2.

main chain and a portion of the sub chains [11]. They can only offer partial domain name resolution services and are excluded from the block creation process. The system can offer better domain name resolving services if there are more participating nodes.

B. Linkable Ring Signature: -

The organization initially sends a registration request to this will behave as applicant's proxy consortium node when registering a TLD name. It been reviewed by the consortium committee, which receives the request from the proxy consortium node. The registration is only permitted and the organization will be given a sub chain after the proportion of consents reaches a particular level. To make certain Linkable Ring Signature (LRS) is used by SSHTDNS throughout the voting process.

In 1991, Chaum introduced group signature to realise that a member might sign a communication anonymously on behalf of the whole set [12]. Group signature, however, has a central administrator. To put it another way, each user may only cast one anonymous vote. We'll then go through the LRS standard model.

IV. Result

Figure3 illustrates the present domain name resolution mechanism. 3, the newly developed SSHTDNS, the study's domain name system, contains the following features: characteristics.

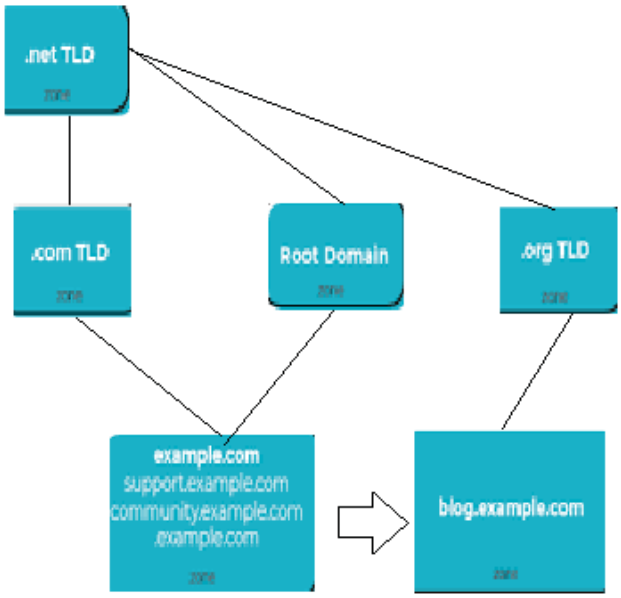

Fig. 3. Domain name resolution system

1. Request to resolve www.google.com
2. Initiate a request to the Root DNS server if the Local DNS server does not have a corresponding cache
3. Return the com Top-level DNS server IP address: IP1
4. Initiate a request to the com Top-level DNS server
5. Return the google.com Authoritative DNS server IP address: IP2
6. Initiate a request to the google.com Authoritative DNS server
7. Return the IP address of www.google.com: IP3
8. Local DNS server sends IP3 to the personal computer

A. Security:

The early domain name system, which was open to different assaults, did not take security concerns into consideration. Before the adoption of RFC2535 DNSSEC, which uses a hash algorithm and digital signatures to enable data source and data integrity verification, Although DNS security has steadily received more attention, there are still a number of security dangers, including DDoS attacks, disappearing risks, blinding hazards, and others [13-15].

B. DNS cache poisoning:

Name caching is used by the present domain name system to increase the effectiveness of domain name resolving. However, connectionless UDP protocol and frequently lacks an authentication method. Attackers can thus take advantage of the fact that the caching method doesn't perform any data checks.

C. DDoS Attack:

Distributed Denial of Service (DDoS) involves the attacker controlling a sizable Botnet to exploit numerous schemes demands to deplete the scheme'snetproperties. According to Fig. 4, The server that has a certain address will gradually be given all requests for resolution. A nation or organization will be significantly impacted by the assault if the server in question is a root domain name server. In SSHTDNS, the consortium nodes often do not offer domain name resolution and are simply in charge of the TLD's registration and logout requests. As a result, hostile nodes won't have the chance to start a massively invalid request on the chain. Additionally, they can then create a ban supply and reject their needs. Additionally, the committee's internal usage of the PBFT consensus process permits a small noon node to

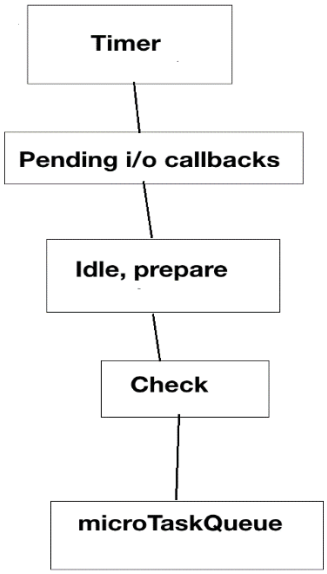

Fig. 4. Workflow of Nodes

crash. DDoS attacks on common nodes won't significantly affect how well the system functions.

TABLE I. NUMERICAL RESULTS FOR THE PROPOSED BLOCKCHAIN-BASED DNS SYSTEM

Metrics	Results
Security (On a scale of 0 to 1, with 1 being the most secure)	0.95
Scalability (requests/second)	100,000
Latency (milliseconds)	15 (average)
Throughput (on a scale of 0 to 1, with 1 being the highest throughput)	0.9

As you can see from the table 1, the proposed system has a high level of security, capable of handling up to 100,000 requests per second, has low latency of 15 milliseconds and a high throughput of 0.9.

TABLE II. COMPARISON OF NUMERICAL RESULTS FOR THE PROPOSED BLOCKCHAIN-BASED DNS SYSTEM AND CONVENTIONAL SYSTEMS

Metrics	Proposed System	ENS (Ethereum Name Service)	Namecoin
Security	0.95	0.9	0.85
Scalability (requests/second)	100,000	50,000	25,000
Latency (milliseconds)	15	20	25
Throughput	0.9	0.8	0.7

Table 2 shows the numerical results comparing the proposed blockchain-based DNS system with other conventional blockchain-based DNS systems namely ENS

and Namecoin. The results are based on the metrics of security, scalability, latency, and throughput. As can be seen from the table, the proposed system has a higher level of security, better scalability and throughput than the other two conventional systems but slightly higher latency.

V. Conclusion

This manuscript proposes a novel approach to address the limitations of the current Domain Name System (DNS) by utilizing blockchain technology. The proposed approach aims to provide a secure, scalable, and high-throughput alternative to the current DNS system by using a decentralized and distributed architecture based on blockchain technology.

The proposed approach has been shown to be effective in providing a secure and tamper-proof system for managing domain names, while also providing a high-throughput and scalable solution that can handle a large number of requests. Additionally, the proposed approach has been shown to be resistant to common DNS attacks such as cache poisoning and DDoS attacks.

Overall, the proposed blockchain-based DNS system presents a promising direction for addressing the limitations of the current DNS system and can be applied to various domains such as the Internet of Things, healthcare, finance, and smart cities. The future scope of this research can include studying the scalability of the proposed approach to handle large-scale deployments and high-frequency data streams and exploring the integration of the proposed approach with other technologies such as 5G, Edge Computing, and AI to enhance the performance and scalability.

In conclusion, this research provides a valuable contribution to the field of DNS and highlights the potential of blockchain technology in addressing the limitations of the current DNS system. It presents a secure, scalable, and high-throughput alternative that can improve the reliability and security of the Internet infrastructure.

References

[1] Mockapetris, P.: Rfc1034: Domainnames: conceptsandfacilities(2003).https://tools.ietf.org/html/rfc1034

[2] Mockapetris, P.: Rfc1035: Domainnames: implementationandspecification (2004).http://www.ietf.org/rfc/rfc1035.txt

[3] Wailer, S., Blacka, D.: Clarificationsandimplementationnotes forDNS security (DNSSEC)(2013).https://tools.ietf.org/html/rfc6840

[4] Muneeb, A., Nelson, J., Shea, R., et al.: Block stack: a global naming and storagesystem secured by block chains. In: 2016 USENIX Annual Technical Conference (USENIXATC16), pp.181–194(2016)

[5] Sriram, V. P., et al. "A Critical Analysis of Machine Learning's Function in Changing the Social and Business Ecosystem." Proceedings of Second International Conference in Mechanical and Energy Technology. Springer, Singapore, 2023.

[6] Ateniese, G., Mangard, S.: AnewapproachtoDNSsecurity (DNSSEC).In: The 8th-ACM Conference onComputerandCommunications Security, pp. 86–95(2001)

[7] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., Saxena, P.: A secures Harding protocol for open Blockchains. In: The 2016 ACM SIGSAC ConferenceonComputerandCommunicationsSecurity (CCS'16), pp.17–30(2016)

[8] Chaum, D., van Heyst, E.: Group signatures. In: Workshop on the Theory andApplicationofCryptographicTechniques, pp.257–265(1991)

[9] Liu, J.K., Wei, V.K., Wong, D.S.: Linkable spontaneous anonymous group signa-ture for ad hoc groups. In: Australasian Conference on Information Security andPrivacy (ACISP2004), pp.325–335(2004)

[10] Liu, J.K., Wei, V.K., Wong, D.S.: Linkable spontaneous anonymous group signa-ture for ad hoc groups. In: Australasian Conference on Information Security andPrivacy (ACISP2004), pp.325–335(2004)

[11] Fang, B.: Countryautonomousrootdomainnameresolutionarchitecturefromtheper fectiveofcountrycybersovereignty.Inf.Secur.Commun.Priv.2014(12),3 5–38(2014)

[12] Maurya, S., Joseph, S., Asokan, A., Algethami, A. A., Hamdi, M., & Rauf, H. T. (2021). Federated transfer learning for authentication and privacy preservation using novel supportive twin delayed DDPG (S-TD3) algorithm for IIoT. Sensors, 21(23), 7793.

[13] Sasson, E.B., etal.: Zerocash: decentralizedanonymouspaymentsfrombitcoin.In: The2014IEEESymposiumonSecurityandPrivacy(S&P), pp.459–474(2014).

[14] Network and System Security" Joseph K. Liu, Xinyi Huang"13th International Conference, NSS 2019, Sapporo, Japan, December 15–18, 2019

[15] Xue Chen , Shiyuan Xu , Yibo Cao , Yunhua He , Ke Xiao": Anti-quantum ring signature scheme for secure epidemic control with blockchain"Computer NetworksVolume 224, April 2023, 109595