Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 2, February : 2023

# An Assessment of a Reliable Block Chain-based T 2 DNS Prototype Domain Name System

**G N Beena Bethel,** Professor, CSE Dept, GRIET
**Prasanthi Gottumukkala** Assistant Professor, IT Dept., GRIET
E-Mail: beenabethel@gmail.com, prasanthi.g946@gmail.com

**Abstract**
We developed a third-party DNS service called T 2 DNS. T 2 DNS offers proof of client trustworthiness, shields clients from server and channel attacks, works according to the existing Internet architecture, and adds finite overhead when responding to client DNS requests. T 2 DNS powers its service proxy with Intel SGX and protects client confidentiality with a hybrid protocol that combines encryption and obfuscation. We effectively overcome the following challenges: scaling the initialization process, minimizing the obfuscation overhead, and optimizing useful system parameters. We create a T 2 DNS prototype, and testing shows that it scalable to a large number of clients, is fully functional, and has a reasonable overhead as compared to other solutions.
**Index Terms:** Ethereum, smart contracts, DNS security, block chains.

## Introduction

The internet has undoubtedly been important in the modern era. After the corona virus (COVID-19) epidemic in the spring of 2020[9], 34% of Austrians and 53% of Americans said they worn the Internet frequently than usual. Seventy percent of CIOs surveyed globally in March stated they presently work from home. Furthermore, about 30% of respondents said they intended to work remotely full-time. Thanks to the Internet, workers may work from home, and students in an outbreak-affected area can learn remotely. Cybercriminals launch attacks using a range of methods, such as malware, denial of service attacks, phishing, and more. Phishing is the most prevalent kind of these attacks. whereby cybercriminals assume the identity of trustworthy websites in order to deceive users into disclosing private information such as usernames, passwords, and credit card details. claims that a new phishing website opens every twenty seconds and that 74% of phishing websites use the HTTPs protocol to convey their content.. Customers were notified by VeriSign that two digital certificates were inadvertently issued to a someone pretending to be a Microsoft official. This gave the fraudster the ability to trick them into visiting a website that contained malicious software. A new method was used to report visitors to a domain that the attacker had compromised[8]. When the victims are asked to download something, two malware versions and a "security certificate update" are downloaded in order to steal the data from their PC.

Federated block chain, sometimes referred to as consortium block chain, is a kind of block chain technology that requires registration and is exclusive to specific organizations or groups. The block chain of Consortium is password-protected. This suggests that the read and compose rights belong exclusively to the collaboration members which are actively involved. The consortium block chain consists of two nodes: one node handles client and node communication, whereas the other node performs cryptographic operations to handle private transaction management. Because proof of work (PoW) is not necessary in permission networks, consortium block chains provide a range of consensus techniques. The public is allowed to consult and transact, but prior a transaction can be validated or a smart contract is generated, the consortium must provide its consent. As a result, the consortium block chain's services are only accessible to authorized nodes and users. Permissioned users and other individuals can both carry out transactions and smart contract implementation.

P2P: Peer-to-peer networks do not have a dedicated server; instead, each computer acts as either a client and a server. This is a good networking choice when there are 10 or fewer people nearby as they are next to each other. Peer-to-peer networks have the potential to be security nightmares since users are going to be ones issuing privileges for shared resources.

**Client/Server:** This type of network services many users by using dedicated machines or servers. Clients need to log in to be able to access the server(s), run programs, or download files. Permissions and security might be managed by one or more administrators, keeping those mentioned computer novices from messing via things they ought not to be. In addition, this type of network provides a multitude of other features that come pre-installed by the network operating system (NOS), reduces network traffic, and makes convenient backup services available.

**Centralized:** "Dumb terminals" are clients in this client/server architecture, that's most commonly utilized in UNIX systems. Because of this, the client may not possess a floppy drive. While it's a CDROM or a hard disk, all applications and computations are carried out on the server or servers. This requires an extremely expensive and speedy server, as you may imagine. Security on this kind of network is very high, while an NT server configured correctly can achieve a comparable level of security.

**Describe a DNS server.** The phone book of the Internet is the Domain Name System (DNS). DNS determines the right IP address for websites when users type domain names like "google.com" or "nytimes.com" into web browsers[6]. To obtain website content, browsers utilize these addresses to get in touch with origin servers or CDN edge servers.

DNS servers, which are computers that exclusively respond to DNS queries, enable all of this.

**Explain the role of a server**. A program or instrument created specifically to offer services to other programs, sometimes referred to as "clients," is called a server. DNS clients, which come with the majority of contemporary desktop and mobile operating systems, allow web browsers to establish connections with DNS servers. More details can be found in the Client-Server Model.

When someone requests DNS, how do DNS servers reply?

Describe the function of a waiter. A program or instrument created specifically to offer services to other programs, sometimes referred to as "clients," is called a server. DNS clients, which come with the majority of contemporary desktop and mobile operating systems, allow web browsers to establish connections with DNS servers. More details can be found in the Client-Server Model.

When someone requests DNS, how do DNS servers reply?

Recursive resolvers, root name servers, TLD name servers, and authoritative name servers collaborate to send an IP address to the client in a normal DNS query without the need for caching. A server that receives a query from a DNS client and then communicates with other DNS servers to ascertain the proper response is known as the DNS recursor, also often called the DNS resolver.

The resolver actually adopts the role of a client upon receiving the request from the client and looks up the correct IP address using the other three types of DNS servers.

The resolver makes a query to the root name server first. At the root server, human-readable domain names are first resolved, or turned, into IP addresses. The resolver receives the address of a TLD DNS server (such as.com or.net) that has the data for its domains from the root server. The resolver then sends a query to the TLD server. The official name server IP address for the domain is returned by the TLD server. The IP address of the origin server is what the recursor will reply with when it makes contact with the authoritative name server.

Finally, the resolver will provide the client with the IP address of the origin server. The origin server will reply to the client's query with website data that the web browser can understand and display by using this IP address.

Describe the procedure for DNS caching.

Recursive resolvers can use cached data in addition to the method described above to respond to DNS queries. The resolver will keep the correct IP address for a certain website in its cache for a predetermined period of time after obtaining it. In lieu of doing the usual DNS lookup procedure, the resolver can reply to any additional clients requesting that domain name during this time by using the cached IP address. Once the caching time restriction has passed, the resolver must obtain the IP address once more in order to add a new item to its cache. This time restriction is expressly specified in each site's DNS records and is referred to as the time-to-live (TTL). The TTL is typically 24 to 48 hours. Because web servers occasionally change their IP addresses, resolvers are unable to always serve the same IP address from the cache; for this reason, a TTL is necessary.

**What happens if there is a DNS server outage?**

There are several reasons why DNS servers could go down, including technical issues, hacking, and power outages. Outages of DNS servers could have a big impact on the history of the Internet. Fortunately, DNS comes with a lot of redundancy. For instance, most ISPs provide their customers with backup recursive resolvers, and the root DNS servers and TLD name servers are publicly accessible. (Single users can also utilize publicly accessible DNS resolvers, such 1.1.1.1 from Cloud flare.) The majority of well-known websites also use numerous instances of their reliable name servers.

Some users may encounter delays because backup servers are handling a large volume of queries in the event of a serious DNS server outage; nonetheless, most of the Internet would need to be inaccessible in the event of an extremely big DNS outage. This really occur in 2016, while DNS provider Dyn was the target of one of the worst DDoS assaults ever. Cloud Flare's Managed DNS Service provides protection for DNS servers[4] against attacks and other common reasons for server failure thanks to its integrated DNS security. **DNS filtering**

Our DNS filtering uses blacklists to prohibit fastidious websites or IP addresses that are known to be harmful. However, by utilizing a dissimilar DNS or addition entry to the host server, DNS filtering is easily circumvented. We adjusted to leverage the benefits of the new block chain technology's quick development in order to provide a secure DNS system..

**Literature Review**

Its qualities have also been the subject of numerous studies that attempt to offer a secure DNS solution. Hari et al. proposed the first piece of work, which constructed the DNS infrastructure mostly utilizing PKI. A distributed autonomous domain name service (DNS) system based on a distributed hash table and utilizing the ownership structure of websites was presented by Benshoof et al. also proposed a DNS resolution technique that reduces data tampering and single points of failure related to domain name resolution by using decentralization [3]. A DNS Cache Resources Trusted Sharing Model is also available—also referred to as DNS [5,]—was put out. They claimed that the methodology might make DNS resolution results more legitimate. To solve the low efficiency problem faced by the collaboration, they proposed a stochastic distributed decentralized storage strategy in the interim.

According to [1], an additional phishing website appears every 20 seconds, and according to [2], the HTTPS protocol powers 74% of phishing websites. Microsoft alerted customers in [3] to the fact that VeriSign had mistakenly granted two digital certificates to an individual posing as an employee of Microsoft, providing the dishonest party with the means to lure users into visiting a website that was infected with malware. [4] revealed a novel method wherein users accessing a domain that has been hacked through the attacker view a screen depicted in Fig. 1. Two malware versions are downloaded in order to steal the victim's computer information, and victims are advised to apply a "security certificate update." Due to the certificate authority authorization (CAA) problem, Let's Encrypt, the biggest and most well-known free certificate authority, claims to have revoked 3 million TLS certificates at the beginning of 2020 [5]. Various techniques have been suggested to

ensure the reliability of IP addresses, such as DNS filtering, IP whitelisting, and more. Users can visit these domains by using a list of trusted IP addresses that are created using IP whitelisting. However, it can be quite labor-intensive to have an up-to-date whitelist of IP addresses, and unplanned changes to IP addresses can result in downtime. DNS filtering, on the other hand, uses blacklists to prevent access to a certain website or IP address that is known to be dangerous. Nevertheless, changing the DNS or adding entries to the host file are simple ways to get around DNS filtering. Many researchers have attempted to use the capabilities of the rapidly developing blockchain technology to build a secure DNS solution. The first study is put forth by Hari et al. [6], who created a DNS infrastructure that mostly relies on PKI.

Benshoof et al. [7] introduced a method known as distributed decentralized domain name service (D3NS). It is built on a distributed hash table and uses an ownership structure for domain names modeled after the Bitcoin blockchain. Liu et al. [8] presented a DNS resolution method in 2018 that lowers the possibility of tampering with domain name resolution data and single points of failure by utilizing the decentralized nature of blockchain technology. Yu et al. [9] also suggested a DNS Cache Resources Trusted Sharing Model, or DNSTSM. They claimed that the model might improve the accuracy of DNS resolution results. To address the issue of low efficiency in the consortium blockchain, they developed a decentralized storage method with stochastic distribution in the interim.

**Proposed Model**

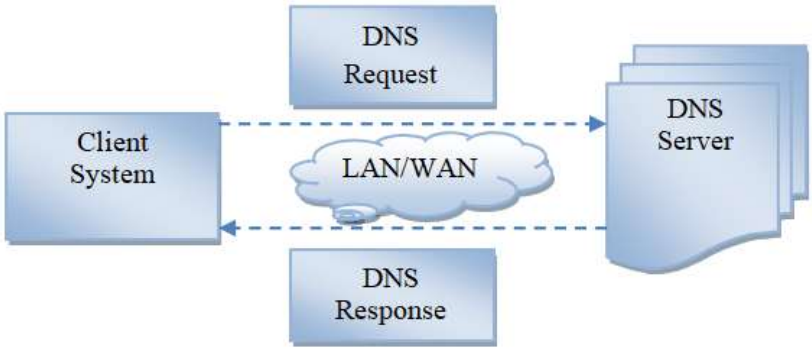
The system's conceptual architecture. Each industry and company comes together to construct a consortium block chain. Since they have been uploaded to blocks in a chain, no one is able to modify their Internet protocol (IP) or universal resource locator (URL). prior to life form permitted to join the collective block chain, a fresh person or organization must first be investigate and authorized by the grouping. If their personal/organizational data is accurate, their website and URL content is right, and their URLs make sense, They are permitted to become a member of the consortium and initiate a smart contract to perform a transaction that uploads their IP address and URL to a block. A hostile hacker is unable to pass authentication because there is not enough actual, valid company data.

To ensure the correctness of the user's website resolution findings, the threat will be segregated from the reliable network.

We safeguard the DNS Entries—that is, the domain name and IP address bindings—in the DNS Server by utilizing block chain technology.

**Contributions**

chains of blocks that are impervious to arbitrary change. Their personal or corporate information is validated. Malicious attackers are unable to pass the authentication due to a lack of officially verified business data. The threat is going to be inaccessible so as to verify the accuracy of the user's domain name resolution results.



Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 2, February : 2023

Figure.1. System projected model

**Module for DNS Security**

Watch out for potentially compromised domain name system (DNS) registry information that can jeopardize external DNS servers that are useful for targeting. This conduct will be difficult to identify because it will be mainly hidden from the target organization's view. The focus of detection efforts may be on related stages of the adversary lifecycle, like command and control.

Be alert for logged DNS registry information that may compromise external DNS servers that may be the target of an attack. This conduct will be difficult to identify because it will be mainly hidden from the target organization's view. The focus of detection efforts may be on related stages of the adversary lifecycle, like command and control**.**

**Module for DNS Servers**

The phone book of the Internet is the Domain Name System (DNS). DNS is in charge of determining the correct IP address for websites when users type domain names like "google.com" or "nytimes.com" into web browsers. To obtain website content, browsers use these addresses to get in touch with origin servers or CDN edge servers. All of this is made possible by DNS servers, which are computers that only reply to DNS inquiries.

**Domain name query module**

To get better query presentation, the entire consortiums force constructs the top-level domain (TLD) block chain. To interact with a smart contract that has been set up on the block in a DApp, a user types in a URL. The smart pact will then drive a DNS request to the TLD block chain. The activities of the user have

Domain name resolution module

**As part of this phase's overall procedure, Internet corporations are included in the construction of the root block chain.**

In reply to a user's demand, a smart contract will submit the first DNS query to the root block chain. The root block chain proceeds the address of the smart convention in the target url block chain. Next, the target smart contract in the url block chain initiates an automatic investigate for the position of the reliable block chain.

**Results & Analysis**

Results an added secure, reliable, and trustworthy DNS resolving service is provided by the suggested mechanism, which integrates participant identification, key management, and the consortium blockchain's consensus process. In this segment, we look at the safety of the suggested program. Figure 2 summarizes the essential components of our proposal and its comparison with previous, well-known designs. The stratification feature emulates the hierarchical distribution of recursive DNS queries to different blockchain-based domains in the current global DNS. Large inquiries would otherwise be routed to recursive servers, increasing network load and resulting in a service bottleneck. This feature avoids this from happening. The comparative result shows that, in addition to the stratification feature, the suggested instrument has enhanced safety than others. The primary advantages are as follows: 1) Reputable providers of domain names the blockchain can assurance the reliability and integrity of data on the network. However, should a malicious applicant upload the information, the phoney before the domain name is recorded, the applicant is verified in our system against the application's supporting paperwork. The on-chain data is controlled by the consortium's consensus. A timestamp (prehash) and the hash of the preceding block are included in the block structure. Any block may only be changed by altering all on-chain data, which is not feasible. If the candidate registers a fresh domain name using the same IP address, the new block will have a recent timestamp that is easy to verify.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 2, February : 2023

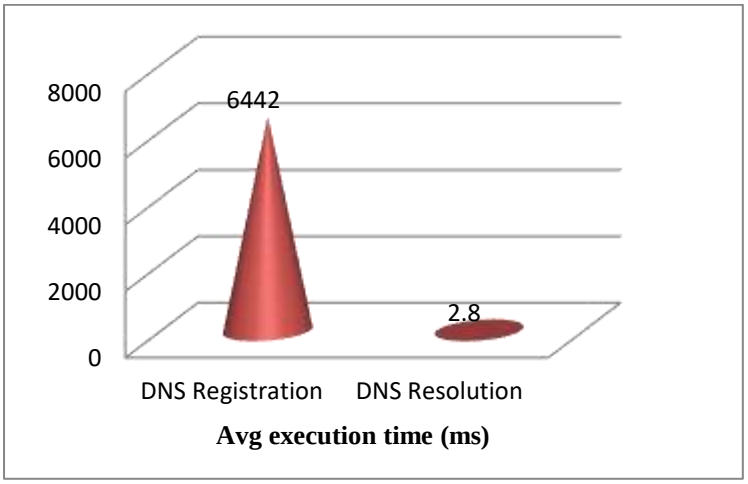



Figure.2. It represents the average execution time

Because the chain's information is made available in an open and secure manner, the proposed DNS may offer dependable service. 2) Have faith in identification via keys. On a blockchain with permission, exchange of messages is limited to authenticated nodes only. Utilizing a recovered signature and the key-based authentication mechanism, sender nodes are confirmed. A set of asymmetric keys generate on the elliptical curve is provided to every user. Every sender uses recoverable to sign messages with the other, allowing the recipient to deduce the sender's public key without the message signature. The haul out public key is compared by the recipient alongside the list of public keys that are associated with other permissioned nodes. The receiver verifies the authenticity of the sender node only if one of the elements matches. If not, the receiver rejects the connection. In order to prevent any one node from making a significant change, Quorum needs a set number of authenticators. Furthermore, for an action to be taken in Quorum, a adequate number of nodes must submit their credentials.

**Conclusion**

After citing previous studies on block chain-based DNS solutions, we present an innovative safe domain name system built around the consortium block chain in this paper. Smart contract-based DNS registration and promise is projected as a dependable method. The provided mechanism uses the Quorum with Raft consensus algorithm to deliver high-quality presentation while ensuring the safety of domain name resolving. The efficiency results among Raft and IBFT are thoroughly examined and contrasted. We consider that the proposed DNS approach can efficiently repel different types of assaults. We will endeavor to effectively incorporate the recommended method into your existing DNS in the future. We will additionally develop a certificate authority that improved Quorum's remote verification for users and authentication of transactions so as to build a more proficient and protected system.

**References**

1. wandera.com, “Mobile Threat Landscape Report,” 2020.
2. apwg.org, “Q4 2019 Phishing Activity Trends Report,” 2021.
3. B. Fonseca, “VeriSign issues false Microsoft digital certificates,” ComputerWorld:Security, Mar. 23, 2001
4. C. Osborne, “Backdoor malware is being spread through fake security certificate alerts,” ZDNet: Security, Mar. 5, 2020.

5. C. Cimpanu, “Let’s Encrypt to revoke 3 million certificates on March 4 due to software bug,” ZDNet: Security, Mar. 4, 2020.
6. A. Har and T. V. Lakshman, “The Internet blockchain: A distributed, tamper-resistant transaction framework for the Internet,” in Proc. ACM HotNets, 2016.
7. B. Benshoof, A. Rosen, A. G. Bourgeois, and R. W. Harriso, “Distributed decentralized domain name service,” in Proc. IEEE IPDPSW, May 2016.
8. J. Liu, B. Li, L. Chen, M. Hou, F. Xiang, and P. Wang, “A data storage method based on blockchain for decentralization DNS,” in Proc. IEEE DSC, Jun. 2018.
9. Z. Yu, D. Xue, J. Fan and C. Guo, “DNSTSM: DNS cache resources trusted sharing model based on consortium Blockchain,” IEEE Access, vol. 8, pp. 13640-13650, 2020.