# Blockchain Name Service

Prof. Suvarna Aranjo[#1], Tushar Adivarekar[#2], Disha Hegde[#3]

[#]*Dept. of Information Technology, Xavier Institute of Engineering, Mumbai - 400016*

[1]suvarnabhoir@gmail.com

[2]tusharadi25@outlook.com

[3]disha.hegde1997@gmail.com

***Abstract*— Blockchain Name Service (BNS), a system that replaces current top-level DNS system, which will offer scalable, secure and robust DNS system. BNS utilizes a domain name ownership system based on Blockchain. BNS removes current DNS vulnerabilities such as DDOS attacks, DNS spoofing and censorship by governments. BNS is reverse compatible with DNS. The system will reduce latency using Interplanetary File System (IPFS) through end to end content delivery.**

***Keywords*— *DNS, Blockchain, IPFS, Distributed, Distributed filesystem, InterPlanetary filesystem***

## I. INTRODUCTION

When everything is connected via Internet, security becomes a major concern. To make the Internet a safer place, we need to fix the broken part of internet. Surfing on Internet and clicking on a page is basically mapping of the IP addresses on server with the name of the website. This work of mapping is done by DNS. DNS translates domain names to IP addresses so browsers can load Internet resources. Blockchain Name Service (BNS), a system that replaces current top-level DNS system, offer scalable, secure and robust DNS system. BNS utilizes a domain name ownership system based on Blockchain. BNS removes current DNS vulnerabilities such as DDOS attacks, DNS spoofing and censorship by governments. BNS provides decentralized authenticated record domain name ownership which is eliminating the need for centralized DNS. BNS is reverse compatible with DNS. The system reduces latency using Interplanetary File System (IPFS) through end to end content delivery.

## II. BACKGROUND AND RELATED WORK

### *A. Using Blockchain to Validate DNS records*

BNS makes use of transaction record mechanism of Bitcoin to record ownership of domain name. Miners are rewarded with the right to claim a domain name instead of rewarding them with cryptocurrency. [1] Each block contains transactions which indicate miner who claim for a new domain name or for transfer of domain ownership. A claim for new domain is validated by a reference to an unclaimed mining reward owned by the claiming user. Each transfer is validated by reference to a previous claim record or transfer record and needs to indicate his ownership by the transferring party. Every domain name in the system can be associated in this way with the new owner's public key. New domains can be claimed and old domains can be transferred between owners.[2]

### *B. Distributed Decentralized Domain Name Service*

It aims only to replace authoritative Top-Level Domain servers currently managed by registrars, where most records are simply a forward to an authoritative DNS server managed by the domain owner, rather than replacing all levels of DNS. This limiting of scope allows us to continue to take advantage of DNS extensions. [3] D3NS has logically discrete components which provide DNS efficient record storage, domain name ownership management and verification, and DNS backwards compatibility, all of which may be modularly replaced or have individual optimizations. D3NS uses a DHT to store DNS records in a distributed fashion and a blockchain to manage domain name ownership. D3NS utilizes public and private key encryption for signing and verifying records. Transactions are grouped together and verified in a block, which are linked together in a chain.[10]

### *C. InterPlanetary File System (IPFS)*

The InterPlanetary File System (IPFS) is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files. In some ways, IPFS is similar to the Web, but IPFS could be seen as a single BitTorrent swarm, exchanging objects within one Git repository. In other words, IPFS provides a high throughput content-addressed block storage model, with content addressed hyperlinks. This forms a generalized Merkle DAG, a data structure upon which one can build versioned file systems, blockchains, and even a Permanent Web. BNS shares zonefiles of DNS using IPFS for quicker response from peers.

### *D. Content Addressing*

All content is uniquely identified by its multi-hash checksum, including links. When being contrasted with content-addressed storage, a typical local or networked storage device is referred to as location-addressed. [12] In a location-addressed storage device, each element of data is stored onto the physical medium, and its location recorded for later use. CAS storage works most efficiently on DNS data which does not change often. In these corporations a large zone files will be stored for as much as a decade, with no changes and infrequent access. CAS is designed to make the searching for a given document content very quick, and provides an assurance that the retrieved DNS record is identical to the one originally stored.

### *E. Peer Discovery*

While discovering all peers in the BNS network, flask server adds source code to the IPFS network and generating hash value of the source code. if user tampers the source code then that user will not able to connect the BNS network. Then using IPFS dht findprovs, IPFS finds all the peers who are having same source code. After getting all BNS users IPFS id, BNS finds all the active users at that movement.

```
def register_nodes():
    res = api.add('app.py')
    h = res['Hash']
    os.system("ipfs dht findprovs "+h+"> peers")
    time.sleep(10)
    lis = []
    with open("peers", "r") as f:
        _ = f.readline()
        for line in f:
            line.rstrip("\n")
            li = api.dht_findpeer(line[:-1])
            li = li['Responses'][0]['Addrs']
            for ele in li:
                if ele.split("/")[1] == "ip4":
                    a = ele.split("/")[2]
                    try:
                        response = request.get(f'http://{a}:5000/chain', timeout=1)
                        if response.status_code == 200:
                            if a != "127.0.0.1": lis.append(a)
                    except: print("", end="")
```

## III. EXPERIMENTAL METHOD

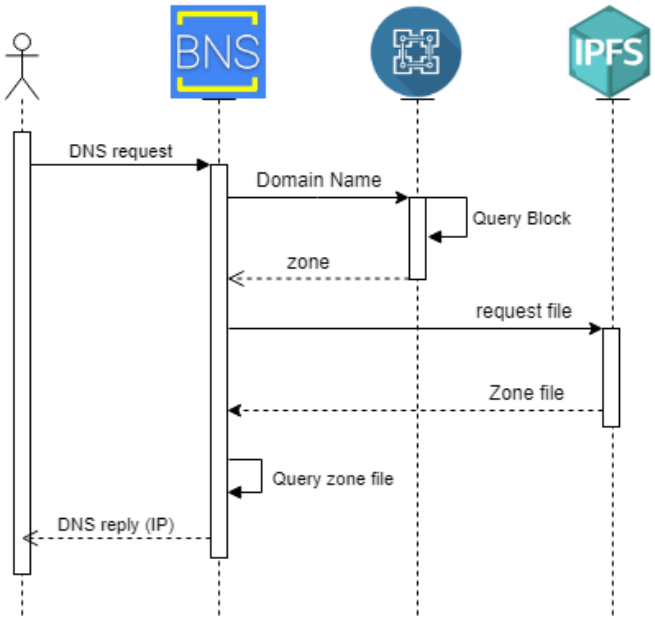


Fig. 1. Query sequence diagram

User Enters the domain name as a DNS query from nslookup command or browser which then sent to BNS flask server, Flask server queries the domain name in blockchain and responds back with the zone file hash value. If someone tampers the zone file then hash value is changed, user will not get the tampered zone file. BNS software request the zone file to IPFS network using content addressing. IPFS network retrieves the zone file based on Qm hash provided.

BNS flask server then gives zone file to DNS server hosted on local machine which serves to the query sent by browser or Nslookup command.

## IV. RESULTS

The following experimental results have been identified as per our testing on the sample data. These tests have been carried out using 3 different DNS servers, Google public DNS, Cloudflare DNS, and BNS.

TABLE I
EXPERIMENTAL RESPONSE TIME

| Server | IP address | Response time (sec) |
|---|---|---|
| Google Public DNS | 8.8.8.8 | 0.2515 |
| Cloudflare DNS | 1.1.1.1 | 0.2606 |
| BNS | 127.0.0.1<br>Localhost | 0.0653 |

```
C:\>nslookup www.google.com 127.0.0.1
Server:  1.0.0.127.in-addr.arpa
Address:  127.0.0.1

Name:    www.google.com
Addresses:  216.58.196.78
64.233.185.100
64.233.185.138
64.233.185.139
64.233.185.102
```

Output of nslookup command

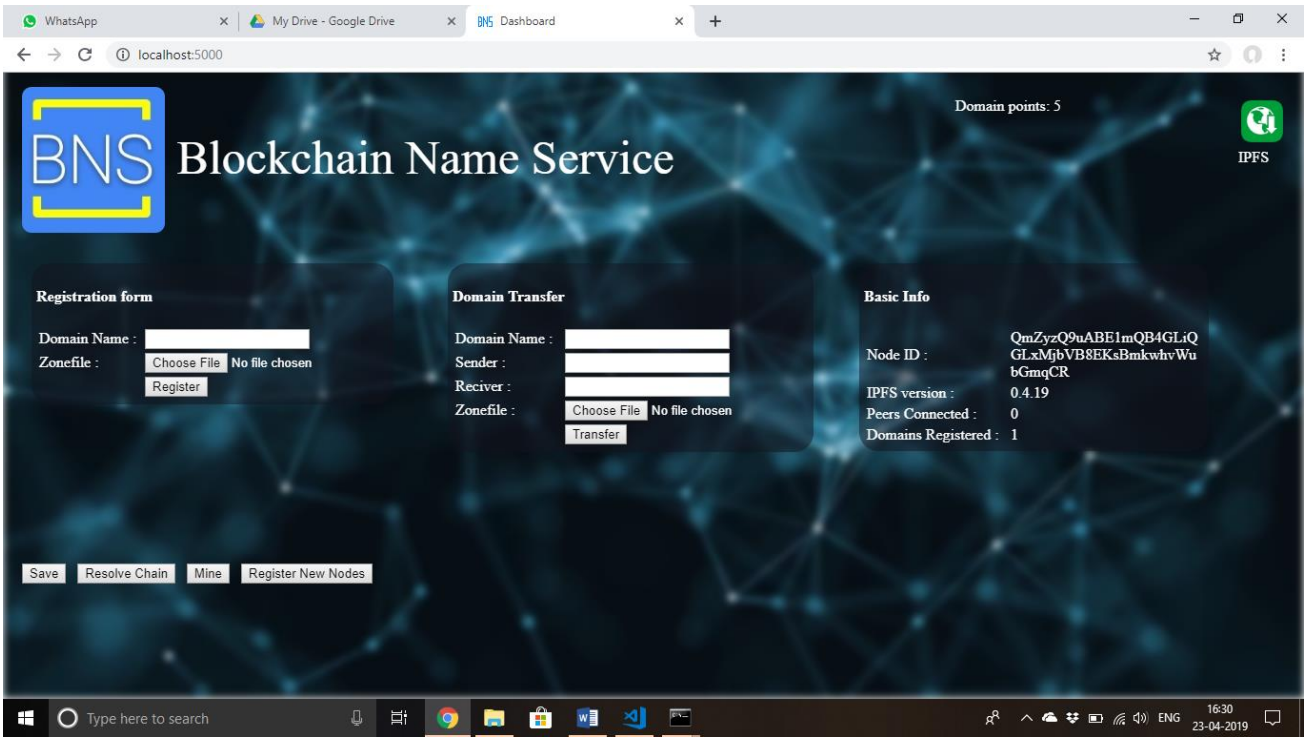


Fig. 2 Dashboard

Dashboard will help users to manage (buy and transfer domain names) and check the information of the BNS node.

## V. Conclusions

User is able to query DNS gateway which was a member of the IPFS and mining network. If the queried domain had a record stored in the IPFS and an owner established in the blockchain, the server would reply with the stored DNS records. Otherwise the server would reply with a DNS failure.

Using all of these components together will allow us to create a system with the following features:

a) Scalability - More number of users using BNS will increase the number of BNS nodes, which will eventually increase the strength of blockchain network.
b) Robustness - The IPFS and Blockchain are both robust to failures and attacks.
c) Extensibility - The DNS reverse compatibility allows any DNS extension to be utilized, if dynamic resolution is required a name server record can be stored in the IPFS to point to a user's specialized DNS servers
d) Decentralization - Both the IPFS and Blockchain can operate without the support of any controlling organization, this offers security against corruption and abuse. We encourage criticism, revision, and adoption of this new system

## Acknowledgment

We would like to thank our department of Information Technology and Prof. Suvarna Aranjo of Xavier institute of engineering for providing us the opportunity to work on the blockchain technology and helping us with its research work and Implementation.

## References

[1] Chul-Jin Park, Seong-Jin Ahn, Jin-Wook Chung, "The improvement for integrity between DHCP and DNS", High Performance Computing on the Information Superhighway, pp. 511-516, 1997
[2] P.Mockapetris, "Rfc 1035: Domain names: implementation and specification (november 1987)," http://www.ietf.org/ rfc/ rfc1035.txt, 2004.
[3] M. Wander, C. Boelmann, L. Schwittmann, and T. Weis, "Measurement of globally visible dns injection,"
[4] M. Lemley, D. Levine, and D. Post, "Don't break the internet," Stanford Law Review Online, vol. 64, p. 34, 2011
[5] S. Crocker, D. Dagon, D. Kaminsky, D. D. McPherson, and P. Vixie, "Security and other technical concerns raised by the dns filtering requirements in the protect ip bill," White Paper, 2011
[6] V. Ramasubramanian and E. G. Sirer, "The design and implementation of a next generation name service for the internet," ACM SIGCOMM Computer Communication Review, vol. 34, no. 4, pp. 331– 342, 2004.
[7] Blockchain: Blueprint for a new economy, M Swan – 2015
[8] " Blockchain Technology" https://www.cbinsights.com/research/what-is-blockchain-technology/
[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Consulted, vol. 1, p. 2012, 2008.
[10] Brendan Benshoof, Andrew Rosen, Robert W. Harrison "Distributed Decentralized Domain Name Service," 2016 IEEE.
[11] L. Smith, "Stop online piracy act," US Government.[Links], 2011.
[12] IPFS - Content Addressed, Versioned, P2P File System Juan Benet, 2014
[13] M. Bedford Taylor, "Bitcoin and the age of bespoke silicon," in Compilers, Architecture and Synthesis for Embedded Systems (CASES), 2013 International Conference on, pp. 1–10, 2013.