Blockchain Name Service

A system that replaces current top-level DNS system and certificate authorities.

Tushar Dnyandev Adivarekar
Dept. of Information Technology,
Xavier Institute of Engineering,
Mumbai - 400016
tusharadi25@outlook.com

Disha Hegde
Dept. of Information Technology,
Xavier Institute of Engineering,
Mumbai - 400016
disha.hegde1997@gmail.com

Prof. Suvarna Bhoir
Dept. of Information Technology,
Xavier Institute of Engineering,
Mumbai - 400016
suvarnabhoir@gmail.com

***Abstract* — We present BNS, a system that replaces current top-level DNS system and certificate authorities, 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 provides decentralized authenticated record domain name ownership which will eliminate the need for certificate authorities. BNS is reverse compatible with DNS.**

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

I. Introduction (*Heading 1*)

We are all now connected by the Internet, like neurons in a giant brain. 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. This is where our system, Blockchain Name Service (BNS) comes into picture. Internet is relied upon IP address. The Domain Name System, commonly referred to as DNS, is a fundamental component of the Internet. DNS translates domain names to IP addresses so browsers can load Internet resources.

Recently there have been leaks concerning the classified information explaining NSA's spying capabilities raising questions about the security of SSL and TLS as well as the level of trust users place in certificate authorities. These types of threats to DNS, along with security concerns, were not considered when designing the protocol, but DNS is too widely used and too integrated with the Internet as a whole to be replaced. Current DNS are maintained by private organizations, governments and Internet Service Provider (ISP) which cannot be trusted directly. We need to establish trust between these organizations and internet users. The current DNS system is also vulnerable to attacks such as DNS spoofing, DDoS attacks, Cache poisoning and DNS amplification which needs to be overcome to have a reliable and trustworthy DNS. Internet is made by people for people. In some cases, DNS has to undergo censorship by the government authorities which violates the right to internet access, also known as the right to broadband or freedom to connect. These types of threats to DNS, were not considered when designing the protocol, along with security concerns. Using Blockchain we will establish a Distributed Domain Name Ownership.

II. Domain Name System (DNS)

DNS can be thought of as the phonebook of internet. Every device which is connected to internet has a unique IP address example [121.164.64.46] The IP addresses cannot be memorized by humans. DNS server eliminates this need of memorizing IP addresses by converting IP addresses into memorable domain names. DNS resolution converts a hostname such as www.examp.com into IP addresses such as 192.168.1.12 which can be understood by the computers. Each device gets its own IP address on the Internet, which is necessary to find a particular appropriate Internet device-like street address is used to find a particular home.

A. *Working of DNS*

There are four DNS servers involved in loading a webpage i.e there are four stages in which a DNS works.

- **DNS recursor** - The DNS recursor receives queries from client machine. Typically, the recursor is then responsible for making additional requests in order to satisfy the client's DNS query.
- **Root name server** - The root server is the first step in resolving human readable host names into IP addresses. Typically, it serves as a reference to other more specific locations.
- **TLD nameserver** - The top level domain server (TLD) is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is "com").
- **Authoritative nameserver** - The authoritative nameserver is the last stop in the nameserver query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor (the librarian) that made the initial request. Explained in Fig 1.

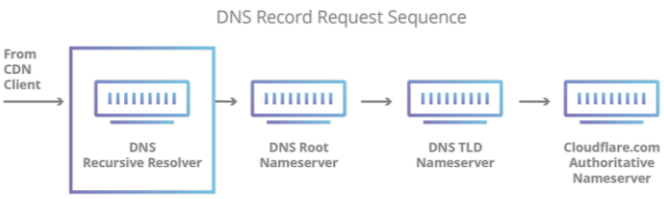

Fig. 1. DNS Record Request Sequence

B. *DNS Attacks*

- **DNS spoofing**

DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer . explained in Fig 2.

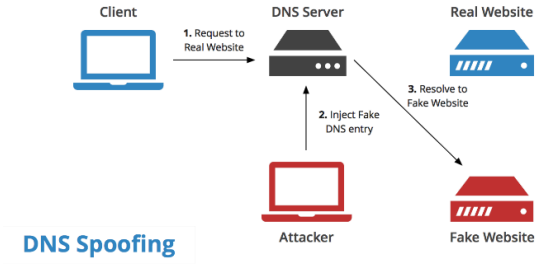

Fig. 2. DNS spoofing attack

- **DDoS attacks**

The attack vectors used to perform DDoS attack include recursive DNS query mechanism or DNS Waterfall Torture or authoritative DNS exhaustion attack as explained in Fig 3. recursive DNS resolver receives the DNS query from the bot to resolve a 12-digit pseudo random host from the domain of the authoritative resolver. It is ensured that the recursive DNS resolver fails to resolve the DNS record of random host, so that the query gets forwarded to the authoritative resolver. This mechanism removes the protection of caching layer from authoritative DNS resolvers. The aim of this attack vector is to forward exceptionally large amount of DNS queries to the authoritative DNS resolver and exhaust the capacity of authoritative DNS resolver to resolve queries.

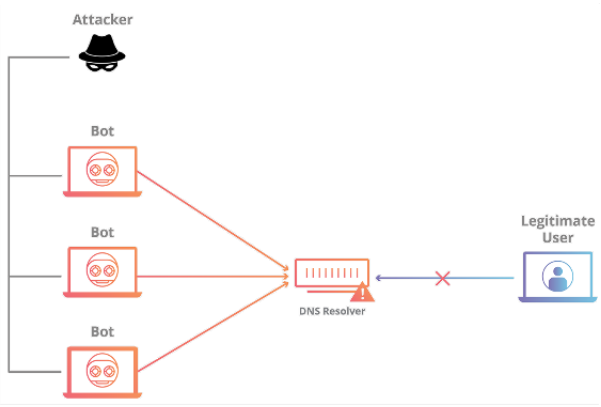

Fig. 3. DDoS Attack

- **DNS amplification Attack**

DNS amplification is an asymmetrical DDoS attack in which the attacker sends out a small look-up query with spoofed target IP, making the spoofed target the recipient of much larger DNS responses. With these attacks, the attacker's goal is to saturate the network by continuously exhausting bandwidth capacity.

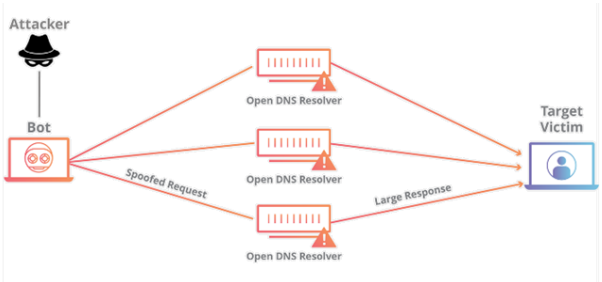

Fig. 4. DNS amplification

- **Censorship**

Blocked domain names are not resolved, or an incorrect IP address is returned via DNS hijacking or other means. This affects all IP-based protocols. A standard feature of most routers, blocking IP addresses is the most primitive and easiest to implement technique. In China, routers are given a blacklist of undesirable IP addresses; the routers will then inspect and drop any packet destined to one of the blocked IPs so that users are unable to establish a connection. The downside of IP blocking is that other innocent websites may also be blocked if they're located at the same IP address or in the same address block.

III. Blockchain

A blockchain is a decentralized, distributed and public digital ledger (explained in Fig 5) that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain.

We use a tool blockchain for maintaining and authenticating our DNS records. Blockchains have their roots in the cryptocurrency Bitcoin, where it is used to authenticate financial transactions and verify account balances. While there have been similar attempts to leverage Bitcoin's mechanisms extend DNS, they have been strictly tied to the concept of currency and not yet academically explored.

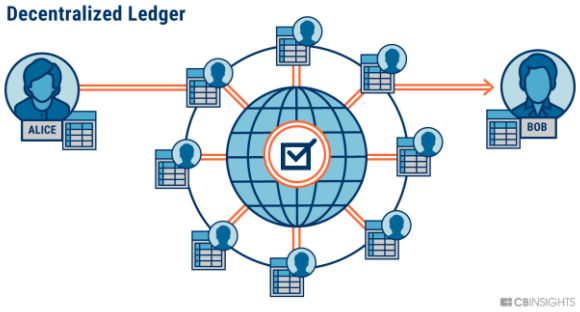

Fig. 5. Decentralized Ledger

A. *Bitcoin*

Bitcoin allows to do online payments without going through any financial organizations. Bitcoin is a pure peer-to-peer version of electronic cash which allows transactions directly between one party to another. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. Bitcoin provides a solution to the double-spending problem using a peer-to-peer network.

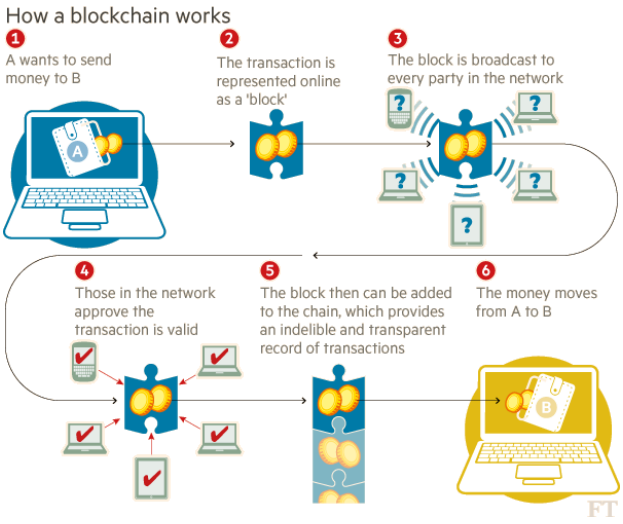

Fig. 6. Working of bitcoin

B. *Using Blockchain to Validate DNS records*

We make 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. Each block contains transactions which indicate miner who claim for a new domain name or for transfer of domain ownership. Claims 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.

A new transaction t consists of: Award domain D to user U with proof reference P and signature S
The transaction set T is the set of all transactions considered valid
if P is not marked used **then**
  if owner indicated in P matches signature S **then**
    if D matches domain referenced in P **then**
      Mark P as used
      Consider t valid
    else
      if P is a mining reward **then**
        P is an unclaimed mining reward
        if D is not yet claimed **then**
          Mark P as used
          Mark D as claimed
          Consider t valid
        end if
      end if
    end if
  end if
end if

Fig. 7. Blockchain Transaction validation

C. *Using a Blockchain to Replace Certificate Authority*

The mining network allows any participant to act as trusted third party to clients as the records of blockchain are shared. This ensures that trust is not centralized at a single point of failure. The members of blockchain network can confirm records to be legitimate before transmission to the end users. This method limits the viability of replay or injection-based attacks.

IV. 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. IPFS combines a distributed hash table, an incentivized block exchange, and a self-certifying namespace. IPFS has no single point of failure, and nodes do not need to trust each other.

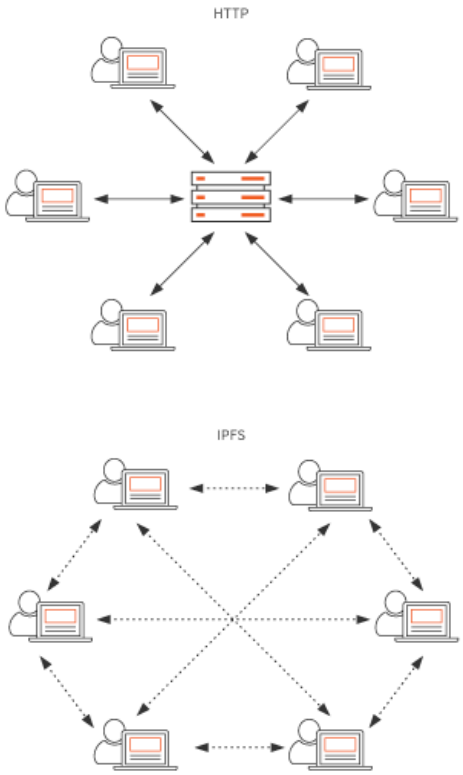

Fig. 8. Treditional HTTP vs IPFS

A. *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. In a location-addressed storage device, each element of data is

stored onto the physical medium, and its location recorded for later use. The storage device often keeps a list, or directory, of these locations. When a future request is made for a particular item, the request includes only the location (for example, path and file names) of the data. The storage device can then use this information to locate the data on the physical medium, and retrieve it. When new information is written into a location-addressed device, it is simply stored in some available free space, without regard to its content. The information at a given location can usually be altered or completely overwritten without any special action on the part of the storage device.

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. In addition, since data is stored into a CAS system by what it contains, there is never a situation where more than one copy of an identical zone file exists in storage. By definition, two identical zone files have the same content address, and so point to the same storage location.

V. PROPOSED SYSTEM

A Domain name system which looks same for end user but internally it works in totally different way. BNS will be a completely decentralized Domain Name Service operating over a Blockchain. BNS does not replace the DNS protocol, but rather adds robustness to the architecture as a whole. Internally, BNS signs all DNS records using public/private keys, providing additional security internal to the DNS system. We show BNS allows for new authentication methods and a means of decentralized proof of ownership.

A user would query the computer we set up as a 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.

Because this system is intended to be reverse compatible with the existing DNS protocol, we serve the data provided by the IPFS after it has been authenticated by the blockchain to other DNS clients. DNS nodes incorporated into the BNS system will not request data from other DNS servers and will only exchange data via IPFS.

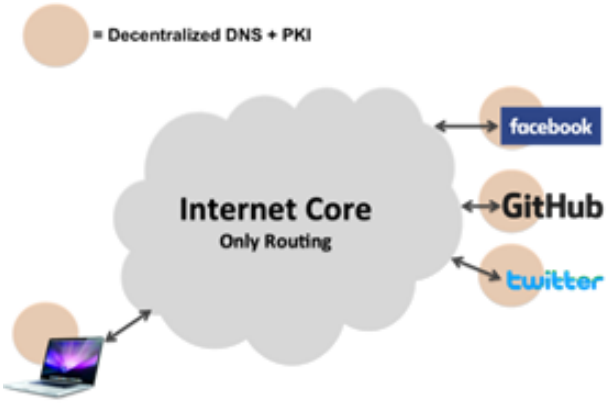

Fig. 9. Proposed system

VI. SECURITY

In BNS system, since no one is controlling it censorship can not be applied on BNS. Blockchain cannot be tampered and user will have a private key sign all record which is very safe and even supercomputers can't crack it easily. Beauty of blockchain lies inside its distributed nature and CryptographyAuthors and Affiliations

A. *Privacy*

Since it is distributed no one can track your internet activity based on DNS record. Blockchain network does not require any information about user. User data is safe.

B. *Benefits*

a) Robustness: The IPFS and Blockchain are both robust to failures and attacks.

b) 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.

VII. CONCLUSION

A user would query the computer we set up as a 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 Bhoir of Xavier institute of engineering for providing us the opportunity to work on the blockchain technology and helping us with its research work.

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil.

Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.