DECLARATION

I declare that this written submission represents my ideas in my own words and where others' Ideas or words have been included, I have adequately cited and referenced the original sources.

I also declare that I have adhered to all the principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.

I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which thus have not been properly cited or from whom proper permission have not been taken when needed.

Tushar Adivarekar (01) _____

Disha Hegde (27) _____

Date: October 15, 2018

Table of Content

List of Tables

List of Figures

Abstract

We are all now connected by the Internet, like neurons in a giant brain. DNS is the heart for accessing anything over the internet. It converts the domain name into IP addresses which the machine can understand. On October 21, 2016, managed DNS provider Dyn suffered a massive DDoS attack. The impact of that attack went far beyond Dyn. Companies such as Amazon, Netflix, Airbnb, Business Insider, Comcast, and many others were effectively "erased" from the Internet for many users.6 The attack exposed the vulnerability of many businesses to service disruption—not due to any issue with their applications, but simply because users were unable to discover them online using the DNS. The reason why users couldn't get to their sites is because these businesses relied only on Dyn to host their authoritative DNS records. When Dyn went down, their entire online presence went down with it.

We present Blockchain Name Service (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. The system will reduce latency using Interplanetary File System (IPFS) through end to end content delivery.

Acknowledgement

I would like to thank Fr (Dr). John Rose S.J. (Director of XIE) for providing us with such an environment so as to achieve goals of our project and supporting us constantly.

I express my sincere gratitude to our Honorable Principal Mr. Dr. Y.D.Venkatesh for encouragement and facilities provided to us.

I would like to place on record our deep sense of gratitude to Prof.Chhaya Narvekar, Head of Deptment Of Information Technology, Xavier Institute of Engineering, Mahim, Mumbai, for her generous guidance help and useful suggestions.

With deep sense of gratitude I acknowledge the guidance of our project guide Asst Prof. Suvarna Aranjo. The time-to-time assistance and encouragement by her has played an important role in the development of our project.

I would also like to thank our entire Information Technology staff who have willingly cooperated with us in resolving our queries and providing us all the required facilities on time.

Tushar Adivarekar _____

Disha Hegde _____

CHAPTER 1

INTRODUCTION

We are all now connected by the Internet, like neurons in a giant brain. As of June 2018, the internet users over the world was 4.2 Billion among 7.6 Billion which is almost 55% of total population, which itself is a big number. Approximately in one minute there will be 219,000 new Facebook posts, 22,800 new tweets, 7,000 apps downloaded, and about $9,000 worth of items sold on Amazon. Now that the Internet is widely available, just one second of global online activity is jam-packed full of events, from communication with others to data storage to entertainment options galore. The amount of data uploaded to the Internet in a single second is a staggering 36,000 gigabytes. Cisco forecasts that monthly Internet data will reach 91.3 exabytes – or 1 billion gigabytes – by the year 2020, pushing the amount of online activity even higher.

All the Internet is relied upon IP address. An IP address serves two principal functions: host or network interface identification and location addressing. Internet Protocol version 4 (IPv4)

defines an IP address as a 32-bit number However, because of the growth of the Internet and the depletion of available IPv4 addresses, a new version of IP (IPv6), using 128 bits for the IP address. When global end-to-end connectivity was envisioned for communications with all Internet hosts, intended that IP addresses be globally unique. Computers can only recognize numbers. Moreover, the human brain can recall words efficiently rather than numbers. This is where the Domain Name System comes into picture.

The Domain Name System, commonly referred to as DNS, is a fundamental component of the Internet. The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. 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. There have been many explorations and attempts to propose a DNS system based on a distributed hash table (DHT). We extend on those papers by implementing a Blockchain backed Domain Name system (DNS) which minimizes latency distance rather than hop distance and implementing a shared record of ownership.

A blockchain is a decentralized, distributed and public digital ledger 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.

1.1 Problem Definition

A chain is no stronger than its weakest link. Internet could also be thought as a fundamentally broken chain thereby making entry point its weakest link. To access any internet resource, we require IP address of that resource which is provided by Domain Name System (DNS). In order to make sure that the data over the internet is secured, it is necessary that the internet must be secure. To make sure that the internet is secured, it is necessary that the DNS should be secure.

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.

The current DNS is accessed by a central DNS resolver. The centralized nature of this system has few shortcomings. If the DNS resolver fails, the entire network comes to a standstill and response time will also be greater.

1.2 Scope of the project

We develop and implement BNS where every machine will act as DNS to itself. BNS will provide decentralized authenticated record domain name ownership which will eliminate the need for certificate authorities. Blockchain will authenticate and do the work of certificate authority without involving any third party. Further, we will eliminate Public key infrastructure's (PKI). BNS is reverse compatible with DNS. This new system will eliminate the central servers as well as organization who maintains them. Replacing current DNS and then changing the world as we know of it today. For the end users BNS will give same interaction like the current centralized DNS system. BNS makes the traditional DNS protocol more secure, robust and scalable. BNS will also contain an interface which will allow the users to obtain new domains or sell their existing domains among the peers present in the network. Everything in BNS system will be decentralize and hence removes the problem of single point of failure from the system.

1.3 Existing System

The Domain Name System is pervasive. Collectively, we use it billions of times a day, often without even knowing that it exists. For enterprises, it's their digital identity as well as a critical component of their security architecture. DNS is a fundamental component of the Internet. DNS maps memorable names to the numerical IP addresses used by computers to communicate over IP. Like all technology, though, it is susceptible to threats. Too often, the always-on, ubiquitous nature of DNS lends itself to being overlooked.

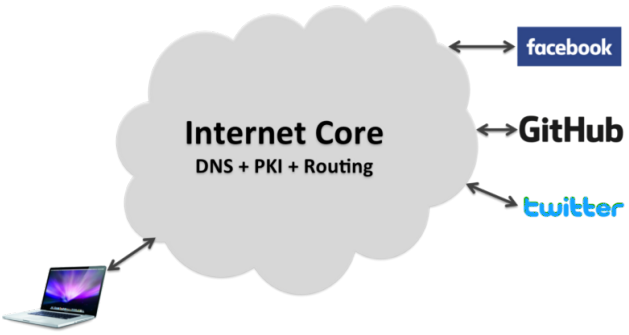

Figure 1.1: Existing System

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. Existing System is fundamentally broken in certain ways such as it is centralized and controlled by few organizations, we blindly trust this organizations. Current system can be censored by the authority, which is not ideology of the internet.

1.4 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. 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

Everytime a request is made for DNS, the nearest peer should process and serve the request made. IPFS does this job. IPFS reduces latency by serving the DNS request in minimal amount of time by processing it from the nearest block possible from where it was queried. All the peers of the blockchain system have the complete list of DNS. When a DNS request is made, it tries to find the required DNS in the nearest of the blocks or zones possible. This zone name is sent at the BNS system which redirects to respective zone and gives the response.

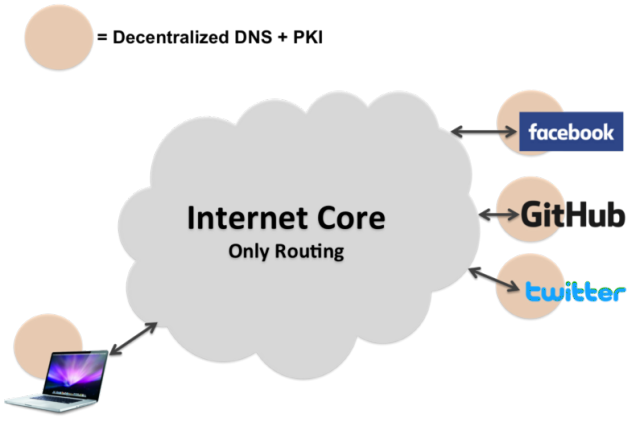

Figure 1.2: Proposed System

CHAPTER 2

REVIEW OF LITERATURE

2.1 Domain Name Service (DNS)

DNS can be thought of as the phone-book 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 host-name 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. 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 re-

cursor 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 host-name back to the DNS Re-cursor (the librarian) that made the initial request.

The mappings are serviced through hierarchically organized, distributed servers that work together to resolve user queries. At the top of the DNS hierarchy are root servers. These are publicly-accessible servers distributed around the globe that provide pointers to top level domain servers (e.g. ".com"), which then provide pointers to second-level domains (e.g. example.com), and so on, until a user's query reaches a server which is authoritative for the domain in which the record exists.The authoritative server provides the record which answers the user's query. A DNS resolver interacts with various tiers of DNS hierarchy, working to resolve queries on behalf of users. When a user's system requests a record of a domain, the resolver will immediately send a response to the user if the resolver has already cached the record. If the resolver does not have the record, it will interact with the DNS infrastructure to retrieve it. While Internet users and even enterprise branch offices may default to their Internet service provider (ISP) to resolve their queries, local ISP providers will likely not offer the same level of service as some popular Public DNS Resolver, such as Google's 8.8.8.8. As a domain name owner, you're responsible for defining where the records that point to your web properties will be stored. Your authoritative records may be self-hosted in your data center, or you may choose to use one or multiple managed DNS providers in place of or in addition to self-hosting. If your brand has any value on the Internet, it's critical that your DNS deployment be scalable and resilient, so that your web or online service presence is always available to your users

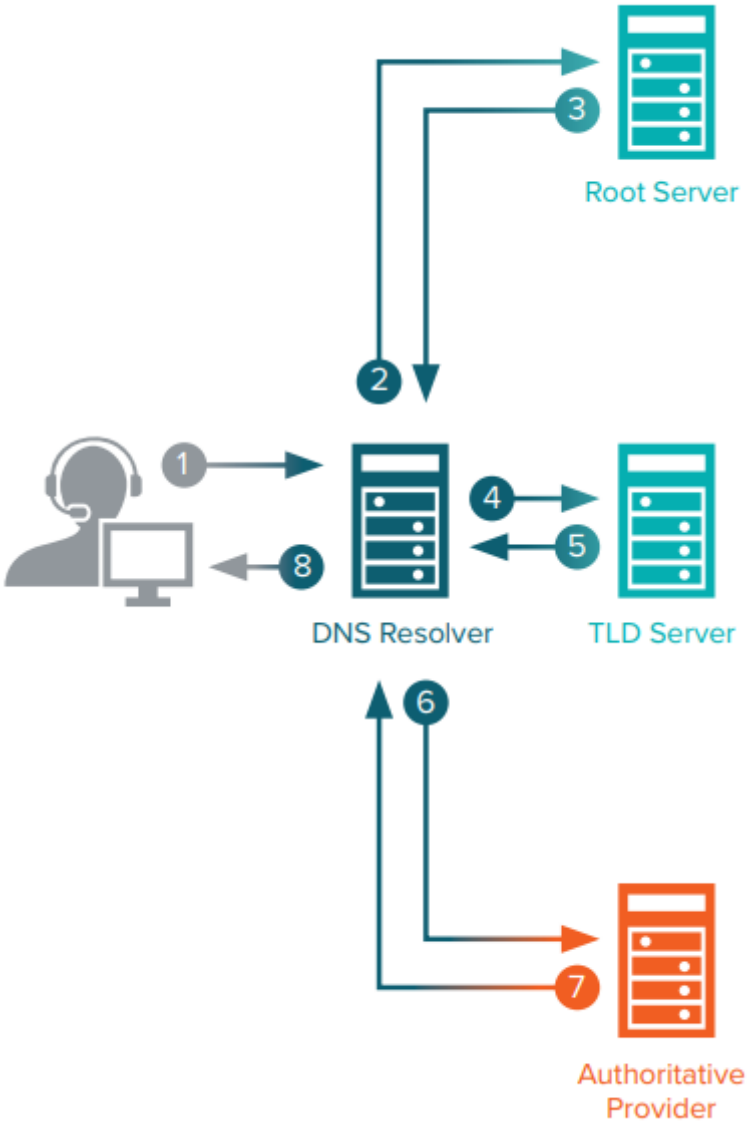

Figure 2.1: Domain name resolution relies on different infrastructures working together

.

2.2 Bitcoin: A Peer-to-Peer Electronic Cash System

Blockchain is a chain of blocks which contains information. The information is broken down and stored in different block which are arranged in chronological order. Each block contains data or information, hash and hash of previous block. Each new block is connected with the previous block with the help of the hash value of previous block. If the information inside a block changes then the hash value of the block will also change. This will make the further blocks invalid. But this mechanism alone cannot provide complete security as computers these days can generate hash values very quickly within second. So blockchain along with hash values and its distributed nature has proof of work mechanism to give security. The proof of work is a mechanism by which the process of creating blocks is slowed down. It requires the new block to solve some cryptographic puzzles to be solved and this solution is shared to all the peers on network. All the members in this peer to peer network verifies this proof of work and if everything is fine and the block is not tampered, it is added to the chain. Also the information can be updated inside of the blocks. Updation again follows the same procedure as of the new block and the timestamp of this new block will be that of recent one. The timestamps can ensure that nobody can backdate and tamper anything or claim some facts to be false after updation because everything is recorded as in a ledger. Any transaction over the internet needs a trusted third party to validate it and build trust. But blockchain provides this security by validating it over a distributed peer to peer network thus eliminating the need of an intermediary. Anything over a blockchain in itself is a valid proof of legitimacy and hence does not need a third party for verification.

2.3 Distributed Decentralized Domain Name Service

The Domain Name System, commonly referred to as DNS [1] [2], is a fundamental component of the Internet. DNS maps memorable names to the numerical IP addresses used by computers to communicate over IP. DNS has security threats and can be influenced by local governments. DNS queries proceed recursively through the DNS hierarchy, beginning with a query to a root server, which then yields a record for a server for the requested top-level domain. This server then directs the request to another DNS server responsible for the domain under that, which yields an answer or another DNS server, which is queried in the same manner. One of the key concepts of the DNS architecture is that no matter which servers end up being queried, a user can expect to receive a record consistent with what the rest of the DNS system will serve for that particular request. We propose a DHT structure which allows for minimum latency optimization. Our system 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 and as places responsibility of managing the network with those who have an incentive for its continued functioning. 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. [3] Transactions are grouped together and verified in a block, which are linked together in a chain. Each block in the chain is a series of transactions published during the time it takes to generate that block. The process of authenticating these transactions and generating a new block is called mining. When a block is mined, it is transmitted to the network and each transaction in it is validated by each peer. The network will then work on mining the next block. Rather than rewarding miners with currency, the reward and incentive for mining is a record that allots the miner the right to claim a domain name. The shared record of the blockchain allows any participant in the mining network to act as a trusted third party to clients. This way, trust is not centralized at a single point of failure. Internally, members of the DHT are also members of the blockchain network and thus all records pushed to the DHT and retrieved records can be confirmed as

legitimate before transmission to the end user. This limits the viability of replay or injection-based attacks. Joining the network is a straightforward process. A new node first learns the location of at least one member of the network to join. The joining node then choses a location in the hash space either at random or based on a problem formulation (for example, based on geographic location or latency information). After choosing a location, the joining node sends a join message to its own location via the known node. The message is forwarded to the current owner of that location who can be considered the "parent" node. The parent node immediately replies with a maintenance message containing its full peer list. This message is sent to the joining node, who then uses this to begin defining the space it is responsible for. The joining node's initial peers are a subset of the parent and the parent's peers. The parent adds the new node to its own peer list and removes all his peers occluded by the new node. Then regular maintenance propagates the new node's information and repairs the overlay topology.

Establishment of a New Domain

Under the current DNS system, a new domain name is purchased from a company registered with the Internet Corporation for Assigned Names and Numbers (ICANN). That company adds the domain name and a record provided by the owner to the TLD servers. The owner or management company then maintains a name server to answer DNS requests for the purchased domain. In D3NS, new domain names are instead awarded as part of the blockchain mining process or purchased from a previous owner, then transferred to the new owner. These assignments and transfers are both recorded in the blockchain.

Updating Records for a Domain

A domain name record in the current DNS system is used to indicate a record on your own Name Server or to configure the record held by the TLD server that contains the address record. Using D3NS, all records must be signed using their owner's private key and confirmed with the public key. A properly configured D3NS server should not accept any DNS records which have not been signed by their owner or accept a record with an older version number. To push a new DNS record for a domain, the owner must create the record set for the domain and then sign and submit it to a node on the DHT. The DHT will forward the record to the responsible party and store it after confirming its validation. The new record will begin to be broadcast to clients after old records begin to expire.

2.4 IPFS - Content Addressed, Versioned, P2P File System

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.

IPFS is a distributed file system which synthesizes successful ideas from previous peer-to-peer systems, including DHTs, BitTorrent, Git, and SFS. The contribution of IPFS is simplifying, evolving, and connecting proven techniques into a single cohesive system, greater than the sum of its parts. IPFS presents a new platform for writing and deploying applications, and a new system for distributing and versioning large data. IPFS could even evolve the web itself. IPFS is peer-to-peer; no nodes are privileged. IPFS nodes store IPFS objects in local storage. Nodes connect to each other and transfer objects. These objects represent files and other data structures. The IPFS Protocol is divided into a stack of sub-protocols responsible for different functionality:

1. Identities - manage node identity generation and verification.

2. Network - manages connections to other peers, uses various underlying network protocols Configurable.

3. Routing - maintains information to locate specific peers and objects. Responds to both local and remote queries. Defaults to a DHT, but is swappable.

4. Exchange - a novel block exchange protocol (Bit Swap) that governs efficient block distribution. Modelled as a market, weakly incentivizes data replication. Trade Strategies swappable.

5. Objects - a Merkle DAG of content-addressed immutable objects with links. Used to

represent arbitrary data structures.

6. Files - versioned file system hierarchy inspired by Git.

7. Naming - A self-certifying mutable name system.

These subsystems are not independent; they are integrated and leverage blended properties. However, it is useful to describe them separately, building the protocol stack from the bottom up. Notation: data structures and functions below are specified in Go syntax.

2.5 PKI and Digital Certification Infrastructure

Public Key Infrastructure is an infrastructure that uses digital certificates as an authentication mechanism and is designed to manage those certificates and their associated keys.Public Key Encryption is also known as asymmetric encryption. It is more secure than secret key encryption (also known as symmetric) encryption. In Public Key Encryption, two related keys, one public and one private, work together. With one used for encryption and the other used for decrypting. In this model, the public key – as the name would suggest – is publicly available to anyone who wants to begin encrypted communication with the holder of the private key. The private key is never shared.

The problem that PKI solves stems from the difficulty of verifying that a public key is actually owned by the person or entity that claims it. Hence the use of digital certificates and PKI. In this scenario, a trusted third-party certificate authority validates the identity of the person or organization it is issuing the key pair too. From there, via the use of the accompanying digital certificate that is issued, anyone can verify the identity of the key-holder.

A digital certificate / PKI Certificate contains information about the key-holder, the public key, an expiration date and the signature of the Certificate Authority that issued it. Unfortunately, managing digital CA certificates can be a challenge, so Public Key Infrastructure was created to help provide a framework for issuance, renewal, and revocation of these digital certificates.

Public Key Infrastructures are not universal – it's not as if there's a single PKI that governs all digital certificates. Rather, a PKI can be built for a single organization and implemented only on that organization's network or it can be a much larger commercial PKI that governs certificates issued to internet users.

Regardless, all PKIs feature the following four components:

- **A Certification Authority to issue certificates** – A trusted CA is the only entity that can issue trusted digital certificates. This is extremely important because while PKI manages more of the encryption side of these certificates, authentication is vital to understanding which entities own what keys. Without a trusted CA, anyone can issue their own keys, authentication goes out the window and chaos ensues.

- **Policies that govern the PKI** – PKI is largely about governance and management of digital CA certificates. In order to achieve both, a set of rules or guidelines must be in place to ensure things go smoothly. For smaller PKIs, these guidelines or often determined in-house by an IT admin or someone knowledgeable. For larger commercial PKIs, they're determined by a collective of browsers and certificate authorities called the CA/B Forum.

- **The Digital Certificates themselves** – It's kind of tough to manage a group of digital certificates that don't exist. In order for a PKI to work and exist properly, it needs to have digital certificates, otherwise—what's the point?

- **Apps that are written to use the PKI** – This last one may seem abstract, it's really not. This just means any application that is PKI aware and uses the PKI to facilitate an encrypted connection. Take some of the larger commercial PKIs, this would mean web browser, email clients, etc...

2.6 Development of Certificate Authority services for web applications

A certificate authority (CA) is a trusted entity that issues digital certificates. Certificate authorities are a critical part of the internet's public key infrastructure (PKI) because they issue the Secure Sockets Layer (SSL) certificates that web browsers use to authenticate content sent from web servers. If the CAs from PKI are removed you essentially have a large, unverified group of digital CA certificates, many of which are likely viable but some of which could also be used maliciously given that there's no way to verify ownership of them. An entity or person who needs a digital certificate can request one from a certificate authority; once the certificate authority verifies the applicant's identity, it generates a digital certificate for the applicant and digitally signs that certificate with the certificate authority's private key. The digital certificate can then be authenticated (for example, by a web browser) using the certificate authority's public key. The Registration Authority collects and authenticates digital certificate requests, and then submits those requests to the certificate authority, which then issues the certificate to be passed through the RA to the applicant. If it's simply a Domain Validation certificate, the CA just checks ownership over the domain and then, once this is satisfied, issues the certificate.

2.7 Dyn DDOS Cyberattack

On October 21, 2016, managed DNS provider Dyn suffered a massive DDoS attack. The impact of that attack went far beyond Dyn. Companies such as Amazon, Netflix, Airbnb, Business Insider, Comcast, and many others were effectively "erased" from the Internet for many users. The attack exposed the vulnerability of many businesses to service disruption—not due to any issue with their applications, but simply because users were unable to discover them online using the DNS. The reason why users couldn't get to their sites is because these businesses relied only on Dyn to host their authoritative DNS records. When Dyn went down, their entire online presence went down with it. This attack overturned a large portion of the internet in the United States and Europe and affected plenty of services. The source of the attack was the Mirai botnet. According to DYN, Mirai is a piece of malware which infects and exploits the vulnerable network devices on the Internet. The sources from Dyn reported that the service provider experienced a Distributed Denial of Service (DDoS attack). Mitigating DDoS attacks was common to the Network Operations Center (NOC) team of Dyn. However, the NOC team could identify that this attack was unusual and bizarre. In the first attack a huge inclination in the bandwidth consumption was witnessed at various locations of Dyn DNS infrastructure, which imitated a situation like that of a DDoS attack. The Engineering and Operations team of Dyn implemented few mitigation protocols but the attack began to target the US-East region. This abrupt large volume of data was originated from various source IP addresses and were destined for destination port 53, where the data packets were composed of TCP and UDP packets. In second Unlike the previous attempt, this attack was targeting almost all the available Managed Infrastructures of Dyn around the globe. Though the second attempt consisted of same set of attack vectors and protocols used during the first attack, it still managed to disrupt the functionalities of the service provider despite the deployed incident response mechanism of Recursive DNS resolver and Authoritative DNS resolver. A recursive DNS resolver receives the DNS query from the bottom 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.

2.8 Google Fraudulent Certificate

Google says that someone was caught trying to use an unauthorized digital certificate issued in its name in an attempt to impersonate Google.com for a man-in-the-middle attack. Google revealed in a blog post Thursday that its Chrome web browser detected the certificate being used late on the evening of Dec. 24 and immediately blocked it. The unauthorized certificate was created after a Trusted Root certificate authority in Turkey, Turktrust, issued intermediate Certificate Authority certificates to two entities last year that should not have received them. Turktrust told Google that it issued the two CA certificates by mistake, inadvertently giving the two entities certificate authority status. With CA status, the two entities could then generate digital certificates, like a trusted certificate authority, for any domain. These digital certificates could then be misused to intercept traffic intended for that domain in order to steal log-in credentials or read communication.

The unauthorized Google.com certificate was generated under the *.EGO.GOV.TR certificate authority and was being used to man-in-the-middle traffic on the *.EGO.GOV.TR network. Google's spokesman said the unauthorized Google certificate was created sometime in early December, fourteen months after Turktrust issued the CA certificate to *.EGO.GOV.TR.

The google.com certificate, a so-called wild-card certificate, would have allowed whoever was using it to intercept and read any communication that passed from users on the *.EGO.GOV.TR network to any google.com domain, including encrypted Gmail traffic. Google engineers have updated Chrome's revocation list to block any other unauthorized certificates that might have been issued by the two companies. Google also notified Microsoft and Mozilla so that they could update their browsers to block certificates from these companies. This is at least the third time that a fraudulent certificate for Google has been issued. In 2011, a hacker was able to trick a certificate authority in Europe, Comodo Group, into issuing him fraudulent certificates for domains belonging to Google, Microsoft and Yahoo.

A couple of months later, intruders broke into the network of Dutch certificate authority DigiNotar and were able to issue themselves more than 200 fraudulent certificates, including one for Google.

2.9 Global DNS Performance Benchmark Report

The 2018 Global DNS Performance Report measures the performance of three DNS infrastructures managed DNS providers, public resolvers, and global roots. It's designed to provide data to enterprises and software as a service (SaaS) providers on infrastructure that's critical to digital experience. It provides a point-in-time study of performance that can be used to make provider choices and track changes over time. The report also includes findings on the state of DNS deployment among enterprise and SaaS providers. More Than Two-Thirds of Global Fortune 50 Companies Are Not Ready for the Next Major DNS Attack, According to ThousandEyes DNS Performance Report.

DNS performance can have a noticeable impact on web and application performance, yet it's an aspect of IT infrastructure that's often given limited attention. Use this report as a reference and educational tool for your staff. Below is a summary of recommendations.

Sr No.	Year	Name of paper	Author	Content
1	2007	Understanding DNS	Incognito Software	DNS
2	2008	Bitcoin: A Peer-to-Peer Electronic Cash System	Satoshi Nakamoto	Blockchain
3	2016	Distributed Decentralized Domain Name Service	benshoof	D3NS
4	2012	IPFS - Content Addressed, Versioned, P2P File System	Juan Benet	IPFS
5	2001	PKI and Digital Certification Infrastructure	R. Hunt	PKI
6	2012	Development of Certificate Authority services for web applications	S.P. Al-Janabi, A.K. Obaid	CA
7	2016	Dyn DDOS Cyberattack – a case study	Aishwarya Sreekanth, Prashant Sri	DYN attack
8	2013	Google Fraudulent Certificate	kim-zetter	TurkTrust Issue
9	2018	GLOBAL DNS PERFORMANCE BENCHMARK REPORT	ThousandEyes, Inc.	DNS threats

Table 2.1: Summary of Research

CHAPTER 3

DESCRIPTION

Blockchain Name Service (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. The system will reduce latency using Interplanetary File System (IPFS) through end to end content delivery.

3.1 Analysis

3.1.1 Class Diagram

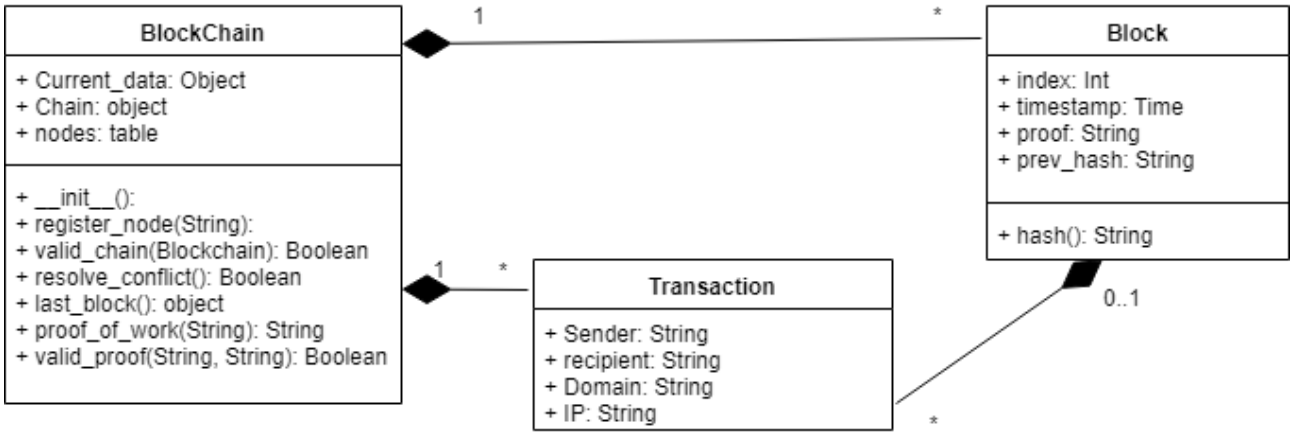

Figure 3.1: Class Diagram of Blockchain Module

3.1.2 Sequence Diagram

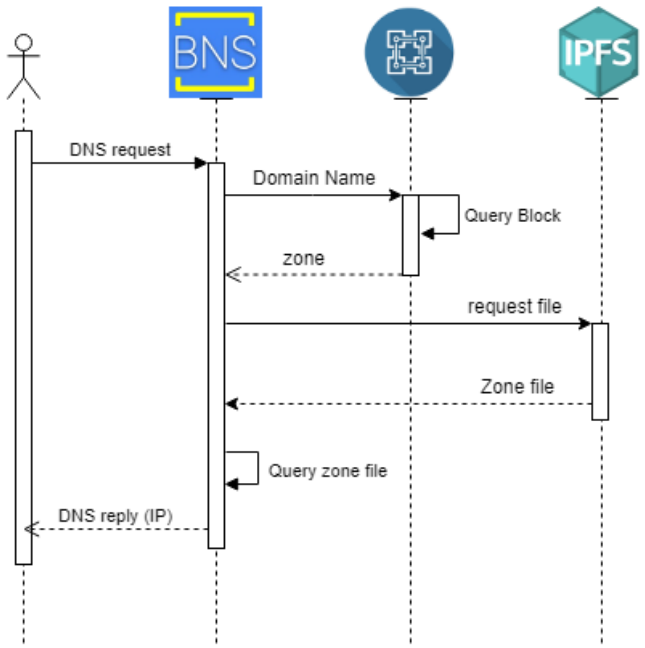

Figure 3.2: Sequence Diagram

3.2 Design

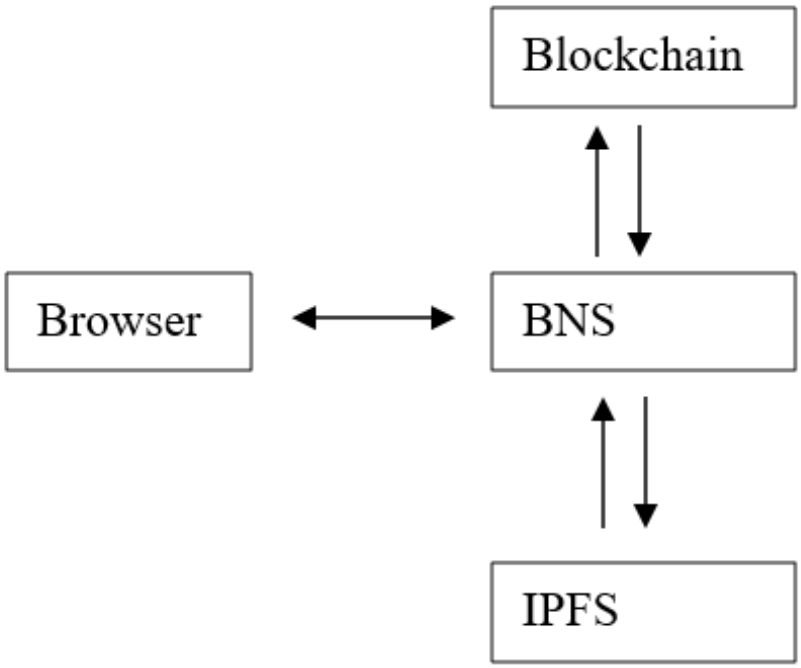

Figure 3.3: Block diagram

When the user will type the name of particular website in browser, the BNS will send request to the block chain which will send the name of zone file. This name will be forwarded to IPFS by BNS. The IPFS will search the zone file from the nearest peers and return the website to browser.

3.3 Implementation Methodology

Since the current dns system is centralized making it vulnerable to various forms of attack we are implementing BNS which will be distributed and making use of blockchain along with IPFS. Blockchain helps us verify and validate all the information and protect it from tampering. Various attacks such as DDoS, DNS spoofing, Cache poisoning and DNS amplification can be avoided by using blockchain technology. Also using blockchain will avoid the need of certificate authority and third party verification. Since blockchain stores all the information in the form of ledger, the information once stored and approved by the peers in network cannot be falsified. Since all the peers have the copy of the entire chain, we need to find a ay for efficient, time saving processing of the request. Everytime a request is made for DNS, the nearest peer should process and serve the request made. IPFS does this job. IPFS reduces latency by serving the DNS request in minimal amount of time by processing it from the nearest block possible from where it was queried. All the peers of the blockchain system have the complete list of DNS. When a DNS request is made, it tries to find the required DNS in the nearest of the blocks or zones possible. This zone name is sent at the BNS system which redirects to respective zone and gives the response. The tracking of zone and response with the help of IPFS makes it faster. Also BNS provides with domain credits to its peers to verify a new block which wishes to enter the systems chain. These domain credits can b used to buy a domain. On selling upon a domain the seller will receive domain credits which he can use to buy another or new domain.

3.3.1 Distributed Consensus Mechanism

A core obstacle within distributed computing and multi-agent systems is the consensus problem. The problem highlights the difficulty that can materialize when distributed processes and systems attempt to reach an agreement on some data value that is needed during computation. Some actors participating in the distributed processes and systems may fail, or may not be reliable, which would result in an unreliable network. Consensus algorithms are mechanisms that are used to achieve agreement on a single data value, and thus obtain reliability in a network that can involve unreliable participants.This agreement, or consensus, is achieved by use of consensus algorithms. Because of the blockchain's distributed nature, there must be a way for these nodes to reach agreement as to the shared state of the blockchain. These algo-

rithms enables network participants to agree on the contents of the blockchain in a distributed and trustless manner. The very first implementation of a distributed and trustless consensus algorithm is Bitcoin's proof-of-work (PoW) algorithm. PoW requires miners to solve complex cryptographic puzzles before they can add a block to the blockchain. In exchange for solving the puzzle, miners are rewarded with domain credits, this is known as a block reward. It is important to note that each block that is added to the blockchain must follow a certain set of consensus rules. Blocks that do not follow these consensus rules will be rejected by network nodes. The combination of the PoW consensus algorithm and the consensus rules produces a reliable network in which agreement as to the shared state of the blockchain can be achieved.

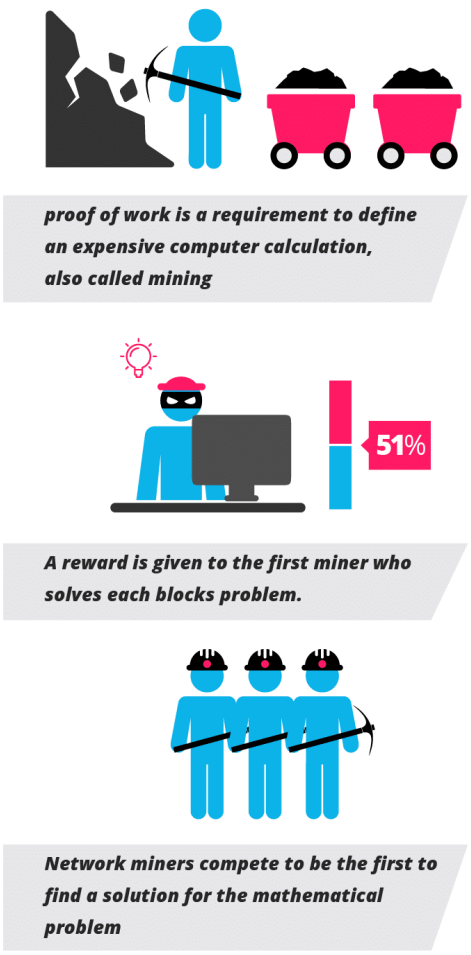

Figure 3.4: Proof of Work

3.4 Details of Hardware & Software

Recommended System Requirements

- **Processors:** Intel® Core™ i5 processor 4300M at 2.60 GHz or 2.59 GHz (1 socket, 2 cores, 2 threads per core), 8 GB of DRAM
- **Disk space:** 2 to 3 GB
- **Operating systems:** Windows 10, macOS, and Linux

Minimum System Requirements

- **Processors:** Intel Atom® processor or Intel® Core™ i3 processor
- **Disk space:** 1 GB
- **Operating systems:** Windows 7 or later, macOS, and Linux
- **Python versions:** 2.7.X, 3.6.X

Software

- **Windows:** Python 3.6.2, PIP
- **IPFS node**

CHAPTER 4

IMPLEMENTATION PLAN

We will approach this project in four major phases. These phases are as follows :

1. BNS software

2. Blockchain module

3. IPFS interface

4. Web interface

4.1 BNS software

This module will be completely written using Python. BNS will be installed in every system. It will be the end point for our system. BNS makes our system backward compatible with

DNS protocol. BNS will communicate with browser via port 53. For the end user DNS will encapsulate all the working of our system and it looks like a traditional DNS for the end users using it. BNS software is the main component of our system through which all other modules coordinate. Since it will be developed in Python which is compatible with all major platforms/OS like Windows, MacOS and Linux making it platform independent and easy to setup.

4.2 Blockchain module

Blockchain module is responsible for providing security, robustness and decentralization to the system. Blockchain will maintain all the work related with ownership and electronic trust. All the blocks in blockchain will be stored in JSON that makes it easy to query upon large data size. Each peer in the network will have one copy of blockchain which will consists of all the blocks present in the chain. Blockchain module will distribute any new block for verification and validation over the entire peer network. Using the distributed consensus approach the block will be added to the chain. Blockchain module will serve to DNS module by providing a distributed ledger.

4.3 IPFS interface

This module will be using IPFS APIs to distribute and retrieve the zone files over the network. It makes use of content addressing to locate the zone files in the nearest peer in the network. It will help reduce the latency of DNS request giving the response much faster which is one of the major concerns of DNS. IPFS module will serve to BNS module by providing it the required zone file. The zone file fetched by IPFS will be processed by BNS and the required web page location(IP address) and other details.

4.4 Web Interface

Web interface will be hosted on all local machines who have BNS software installed. Web interface helps us to manage domain name credits, ownership rights. Using web interface users will buy or sell the domains. It also keeps account of domain credits for every individual user in the network of peers. Web interface will be developed in HTML5, CSS3 and web sockets. Web sockets plays major role in communication between web interface and BNS.

CHAPTER 5

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.

e)Elimination - of a third party or a certificate authority for building trust and validating the information.

REFERENCES

[1] Incognito Software *Understanding DNS (the Domain Name System)* January, 2007

[2] P. Mockapetris. *"Domain names: concepts and facilities(November 1987),"* Standard, 2003.

[3] Satoshi Nakamoto *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008

[4] P. Mockapetris, "Domain names: implementation and specification (November 1987)," http://www.ietf.org/ rfc/ rfc1035.txt, 2004.

[5] Brendan Benshoof, *"Distributed Decentralized Domain Name Service",* Department of Computer Science, Georgia State University.

[6] Juan Benet, *"IPFS - Content Addressed, Versioned, P2P File System"*

[7] R. Hunt, *PKI and Digital Certification Infrastructure*, IEEE conference on networks, Oct 2001.

[8] S.P. Al-Janabi, A.K. Obaid, *"Development of Certificate Authority services for web applications",* International Conference on Future Communication Networks, Apr. 2012.

[9] Aishwarya Sreekanth, Prashant Sri *"Dyn DDOS Cyberattack – a case study"*

[10] Kim Zetter, *"GOOGLE DISCOVERS FRAUDULENT DIGITAL CERTIFICATE ISSUED FOR ITS DOMAIN",* wired.com 2013 https://www.wired.com/2013/01/google-fraudulent-certificate/

[11] ThousandEyes Report, *"GLOBAL DNS PERFORMANCE BENCHMARK REPORT",* 2018 Edition