University of Southampton

Faculty of Engineering and Physical Sciences

Cybersecurity Research Group

HyperDom: A Permissionless Blockchain DNS Provider

George Giamouridis

July 2022

Supervisors: Dr. Leonardo Aniello, Dr. BooJoong Kang

First Progression Review

Contents

Chapter 1

Introduction

Domain Name System (DNS) is an application layer protocol that interprets a domain name as an IP address, meaning that it converts a user-friendly domain into a computer-friendly IP address. DNS governance relies solely on a central entity under the name of Internet Corporation for Assigned Names and Numbers (ICANN), responsible for taking decisions regarding its operation and management. Due to its centralized nature, the DNS protocol introduces a series of restrictions as well as potential functional threats related to availability, integrity, and confidentiality.

At the same time, technologies like blockchain radically transform the way technology is organized as it creates the technological possibility for the existence of a decentralised form of trust. This is extremely important, as it can affect traditionally central authorities, transactions and online services. In the same way, blockchain technology can also be used for re-shaping already existing systems in a more functional and secure way.

The blockchain based DNS is one of the several approaches aiming to further improve the functionality, performance, and security of the DNS protocol since blockchain technology is becoming more and more popular nowadays. The main idea behind a blockchain based DNS is to store DNS records in a decentralized public ledger instead of a central database. The network is responsible for maintaining and issuing new domain names, as well as efficiently managing requests by using pieces of automated code called smart contracts.

Traditional DNS is administrated and controlled by a central authority, which is able at any time to make changes and get decisions without permission. For instance, ICANN has approved a process to allow organizations to apply for a Top Level Domain (TLD). Applications and registrations can only be made during an open application window, where companies have time to develop a marketing plan and come up with justification to pay the $185,000 application fee and, if approved, the annual $25,000 fee (1). On the other hand, a blockchain based DNS is managed exclusively by a Peer-to-Peer (P2P) network, meaning that decisions regarding the state of the network are made in a decentralised manner from the whole network (peers) instead of just one certain entity. Any kind of state change depends on aspects like as the consensus algorithm and the number of nodes participating in the network.

Regarding security and decentralization, as traditional DNS is a centralized system, attacks such as Distributed Denial of Service (DDoS) attacks can occur and harm the system. However, in a blockchain based DNS, all records are replicated over all node's local storage. That means that the single point of failure can be prevented, as every node can provide its services no matter the state of the rest network nodes. Furthermore, the way a blockchain stores its records can identify any data manipulation and prevent attacks and unauthorized malicious activities. When the parent block is modified in any way, the parent's hash changes. The parent's changed hash necessitates a change in the "previous block hash" pointer of the child. This in turn causes the child's hash to change, which requires a change in the pointer of the grandchild, which in turn changes the grandchild and so on. This cascade effect ensures that once a block has many generations following it, it cannot be changed without forcing a recalculation of all subsequent blocks. Because such a recalculation would require enormous computation, the existence of a long chain of blocks makes the blockchain's history immutable.

Since traditional DNS introduces a series of issues due to its centralized nature, using blockchain-based DNS can bring considerable enhancements. By taking advantage of the blockchain technology, it would bring several improvements and new functionalities, that would benefit the development of the decentralized web. Today, however, there are still no technologies and applications on which there is unanimous agreement, as they are not yet mature enough to be used on a large scale. Even though many projects and Proof of Concepts (PoC) are under development, improvements in terms of scalability, security, and usability need to be made. Bearing all these in mind, as well as several other research questions that will be clarified later, we propose HyperDom, a fully permissionless blockchain based DNS aiming to providing a secure interconnection between users and the DNS ecosystem in a fully decentralized manner. Our approach is mainly focusing on providing a technical solution to improve the DNS protocol. In this report, we introduce existing blockchain based DNS systems and highlight their research gaps and limitations. We finally present HyperDom, showing how such a blockchain based DNS and its functionalities can provide a solution to the respective problems.

Chapter 2

Literature Review

Several blockchain-based DNS approaches have been proposed with the goal of replacing the traditional DNS model in a more secure and efficient way. The main idea behind all those proposals is the replacement of the centralized DNS ecosystem with a decentralized-blockchain network. After extensive research on this specific field, we have identified all the blockchain-based DNS approaches that have been proposed so far. Below, we present them by introducing their fundamental properties, explaining their limitations and identifying the research gap that has not yet addressed.

2.1 Namecoin

Namecoin is the first ever blockchain-based DNS proposal. The main purpose of Namecoin is to create an alternate DNS-like system that replaces DNS root servers with a blockchain for mapping domain names to DNS records (2) by offering a general name-value (name-IP) resolving system. The blockchain is implemented as a Bitcoin fork with multiple modifications and functionalities, and uses the .bit top-level domain for naming and resolving hosts in the network. Namecoin is a completely functional blockchain-based DNS providing the ability of registering, renewing and transferring domain names. However, the .bit namespace is not yet recognized as an official namespace from the traditional DNS, and therefore users who want to resolve .bit domains must install an additional resolving software. Furthermore, new users face many significant hurdles in registering a domain name as they are required to download, verify, and store the entire blockchain. Users must also remember to update names every 250 days as the domain name will be revoked and will not be reachable any more, until a new owner found. Namecoin also suffers in terms of its blockchain security. The amount of computational power under the control of a single mining pool is more than the rest of the network, and that can lead to a 51% attack. In late 2014 a single mining pool consistently had more than 51% of the compute power while recently, another mining pool called F2Pool controlled up to 75% of compute power in a particular week (3). Finally. in terms of network reliability and throughput, transactions with large number of data fields can cause severe performance problems and trigger network latency problems. That's because Namecoin shares many protocol properties with Bitcoin, including a 10-minute block construction and a 1 MB bandwidth limit on block size.

2.2 Blockstack

Blockstack (3) is the first blockchain-based DNS operating directly on the top of the Bitcoin blockchain, offering a decentralized DNS, Public Key Infrastructure (PKI) and storage system. The main Blockstack's goal is to improve Namecoin's issues that mentioned above, and therefore it shares the same functionalities with it. However, Blockstack is a multi-layer blockchain. As long as it is built on the top of the Bitcoin blockchain, large data storage is limited. Thus, Blockstack uses a separate chain to store data and the Bitcoin layer is only used for achieving consensus within the network. Blockstack faces a crucial issue regarding the transaction's throughput. Bitcoin currently supports between 3 and 7 transactions per second with a 1 MB block size. In terms of operations like registration and domain name modification, when scaling to millions of users, as opposed to thousands, even 8 MB blocks will not suffice and the community needs to look into performing registrations across multiple chains and novel methods for packing multiple name operations in a single transaction. Furthermore, a high volume of small transactions with transaction amounts that are too low for miners to package in a block, can cause an extremely high number of unconfirmed transactions on the network and end up paying 2-3 times higher transaction fees.

2.3 DNSLedger

DNSLedger (4) is not a stand-alone blockchain, rather it is an approach that aims to improve the functionality of already existing blockchain-based DNS systems such as Namecoin and Blockstack. It is a hierarchical multichain structure in which domain name management and resolution are performed in a decentralized way. The blockchain is separated into two different chains. The Root chain, which acts similarly to the current DNS root servers and multiple TLD chains. Nodes are distributed into the chains according to the TLD requirements. For example, nodes in the .cn chain can only provide .cn domain names. Domain names in DNSLeder are split in two parts and stored separately. The label part which is responsible for describing the ownership of the domain is stored in the blockchain, while the domain name data for resolution, is stored in a non-blockchain mold database and the operation of domain name resolution is mainly handled with it. The database is only allowed to be written and modified by the blockchain of DNSLedger. As mentioned before, DNSLedger is not a complete blockchain, but an improved implementation of Namecoin and Blockstack. Thus, issues like a low number of nodes in the network possibly leading to 51% attacks. However, the main limitation DNSLedger faces is that storage is based on a non-blockchain database managed by the DNSLedger blockchain, meaning that a central point of failure is responsible for storing data.

2.4 EmerDNS

EmerDNS (5) is a decentralized DNS supporting a full range of DNS records, meaning that the blockchain can handle any kind of TLD. EmerDNS gives domain owners the opportunity to change values, lease times, delete them or transfer ownership to another Emercoin (EMC) address. The main EmerDNS feature is its storage technology called NVS (Name-Value Storage). Data is stored in pairs of names - value on the blockchain. The initial concept was inherited from the Namecoin. However, Emercoin NVS allows not only arbitrarily cast information on the blockchain, but it also let users manage their assets (domain names) using the wallet or API. Technically, EmerDNS can support any DNS zone. However, for seamless integration into a standard DNS tree, and to prevent collisions with existing DNS-zones, it currently recommends creating EmerDNS records only in the zones: .emc, .coin, .lib, .bazar. When mentioning DNS collisions, we are referring to an attempt of resolving a name used in a private name space (e.g. under a non-delegated Top-Level Domain) which results in a query to the public Domain Name System (DNS) (6).

2.5 Ethereum Naming System (ENS)

ENS (7) is the official Ethereum name service. ENS is responsible for mapping human-readable names like ‘alice.eth’ to machine-readable identifiers such as Ethereum addresses, other cryptocurrency addresses, content hashes, and metadata. ENS functionalities are similar to those of the traditional DNS, but their architecture differs a lot. ENS operates on a system of dot-separated hierarchical names, with the owner of a domain having full control over subdomains. Currently, ENS handles only the .eth and .test top-level domains, which are owned by smart contracts called registrars, that specify rules governing the allocation of their subdomains. The ENS registry consists of a single smart contract that maintains a list of all domains and subdomains, and stores critical pieces of information about each. The owner of a domain may be either an external account or a smart contract. A registrar is simply a smart contract that owns a domain and issues subdomains of that domain to users that follow some set of rules defined in the contract. The main issues that ENS faces are security related, such as vulnerabilities due to domain name typo-squatting, fraud addresses and record persistence meaning that when an ENS name expires, the name and its subdomain name's records would be kept in the blockchain, and some ENS wallets could still resolve them to blockchain addresses or other records.

2.6 Handshake

Handshake (8) is an experimental and permissionless naming protocol that uses blockchain technology to create a decentralized root zone, as opposed to a centralized root zone regulated by ICANN. Handshake uses a cryptocurrency called Handshake (HNS) for domain name registration. Whenever users wish to register, transfer or upgrade their domain names, HNS coins are used to perform these functionalities. Domains can be registered through an external provider called Namecheap, which is the only domain registrar offering registration services for handshake domains for the general public. Although Handshake is a promising blockchain-based DNS proposal, its limited accessibility (both from a registration and browser support), sets the current system firmly in control as a limited number of nodes participating in it similarly to other blockchain-based DNSs. Another big concern is the possibility that ICANN releases conflicting TLDs with the current handshake TLDs. If that were to happen, ISP's DNS resolvers would have to choose whether to resolve to the ICANN TLD or the handshake TLD.

2.7 Unstoppable Domains

Unstoppable Domains (9) is a Non-fungible Token (NFT) Ethereum Decentralized Application (DApp) provide users with an easier way (than traditional domain name providers do) to buy their domain, while also acting as a cryptocurrency wallet. This overcomes the initial hurdle of buying a domain with encryption (encrypt personal details like owner identity), making it significantly more user-friendly. In addition, all domains purchased in Unstoppable Domains are for life. This removes the recurring cost of renting a domain and gives the user complete control over how they are used. Unstoppable Domains converts a DApp address into a readable, user-friendly domain name. To achieve this goal, it creates NFT domains that keep data private and provide many additional benefits. Each domain serves as more than just a web address. An Unstoppable Domain's domain name can be used as a place to transfer cryptocurrencies, as a connection to a decentralized web, and even provide a universal username, allowing domain owners to have a single identity online. Unstoppable Domains set just one limitation. Domains can be only purchased for Web 3.0 services, meaning that traditional web cannot access those kinds of domains.

2.8 Other Blockchain DNS Proposals

All the blockchain-based DNS solutions mentioned above are currently the most considerable research attempts for the implementation of a decentralized DNS. Apart from them, other similar ideas have been proposed, but the fact that their research status is not mature yet does not help us collect further information about them. Therefore, according to the availability of our material and resources, we are presenting some of them and hopefully expecting to have more research content in the future.

AuthLedger (10) is a blockchain-based system built on the Ethereum blockchain that provides efficient and secure domain name authentication as it reduces the level of trust in Certificate Authorities (CAs). The main goal of AuthLedger is to reduce the level of trust in CAs by providing a decentralized CA system. However, AuthLedger is only an authentication scheme, meaning that users cannot buy their own domain names. BlockONS (11) is a permissioned blockchain built on the Hyperledger blockchain. BlockONS is a system that aims to overcome classical security issues related to DNS resolution, namely DNS cache poisoning and spoofing, and is mainly used for IoT devices. ConsortiumDNS (12) is a system based on a three-layer architecture composed by a consortium blockchain, a consensus mechanism and external storage. The main goal of Consortium DNS is to address the storage challenge of already existing blockchain-based DNSs like Namecoin and Blockstack by proposing a three-layer architecture and additional external storage. The three-layer architecture aims to separate data records and domain name operation data that domain name data store in storage layer, while domain name operation data stored in the underlying blockchain layer. Finally, B-DNS (13) is a blockchain-based name system which aims to provide a lighter computational functionality by proposing Proof-of-Stake as the main consensus algorithm, and an efficient way for querying the blockchain.

It is clear that all the above Blockchai-based DNS are in principle intent to improve the robustness, availability, and security of the DNS protocol as well as addressing privacy and censorship concerns. Some of them focus on developing a completely new DNS ecosystem with the goal of fully replacing the traditional DNS, while others propose improvements to the existing protocol. Although the idea of using a decentralized blockchain network to perform decentralised DNS resolution is interesting, and many of the proposals mentioned above introduce some promising solutions, there are still several drawbacks and research questions to be covered. Table 2.8 wraps up the main problems and limitations that existing blockchain-based DNS solutions face, and then in section 3 we extensively analyse the main research problems that led us to propose HyperDom.

DNS Name	Platform	Issues/Limitations
Traditional DNS	Web	Central point of failure Privacy and anonymity issues Censorship concerns
Namecoin	Bitcoin	Additional software required Blockchain security Network reliability and throughput
Blockstack	Bitcoin	Storage limitations High number of unconfirmed transactions
DNSLedger	-	Inefficient number of nodes Non-blockchain storage Blockchain security
EmerDNS	Emercoin	Limited accessibility TLD conflicts with ICANN
ENS	Ethereum	Domain name typo-squatting Domain name renewal Fraud addresses and record persistence
Handshake	-	Limited accessibility TLD conflicts with ICANN
Unstoppable Domains	Ethereum	Only Web 3.0 usage

Table 2.1: Existing blockchain DNS limitations

Chapter 3

Problem Definition

After collecting and putting together all the relevant literature, we tried to identify the principal traditional DNS problems, and how existing blockchain-based DNS solutions approach them. The ideas that have been listed in section 2 are the ones that came closest to the proposal of a solution that would address the main DNS problems. However, there are still lots of limitations and research questions that have not yet been addressed by them. In this section, we present the main DNS research problems arising from the above proposals and explain their limitations that led us to propose our research idea. To start with, it is considered essential to address the main reasons researchers proposed a blockchain-based DNS.

3.1 Privacy and Anonymity

The traditional DNS protocol is a big topic of discussion in terms of privacy and anonymity concerns, as DNS requests are processed by a central entity called Internet Service Provider (ISP). Each ISP maintains a DNS database including DNS records through which DNS request come through in order to decrease DNS traffic and prevent overloading.

When entering the domain name of a host in the browser, a DNS request is created and forwarded to the local DNS cache memory, where the host's IP address is found. The DNS requests will then go to DNS servers owned and operated by their ISP, meaning that internet traffic passes through the ISP's DNS servers, which record all the data (14). Resource requests are recorded in a log, along with the IP address of the customer who requested the address, the date and time of day, and other sundry information. In many countries, these DNS server logs can be subpoenaed by the government, law enforcement agencies, or entertainment industry lawyers to allow them to track activities on the web.

In some countries, the United States included, ISPs can sell these logs to advertisers and other third parties without needing your approval to do so (15). VPNs are widely used for establishing a protected network connection when using public networks by encrypting the internet traffic and disguising the user's online identity. for hiding all internet activity, including the DNS requests. However, VPN providers can see what users are up to and therefore privacy concerns still exist.

As we will extensively describe in section **??** currently, blockchain-based naming systems can provide anonymous and private DNS querying only to domain names that their TLD is supported by the blockchain (ex. Namecoin can only resolve .bit domain names). That means that DNS requests with unsupported domain names are forwarded back to the traditional DNS or cannot be handled.

3.2 Censorship

The centralized nature of DNS is another problem that brings lots of limitations. DNS is managed and maintained by a central authority called ICANN, which means that decisions about the way it operates are made solely by it. Domain holders are technically domain tenants with limited capabilities managed by an intermediate entity. Whenever a user wishes to purchase a new domain, there are two different central entities involved to complete the buying process. First, the user must request their domain name through a recognized registrar such as Cloudflare, associated with ICANN. Then the registrar must rent the TLD from the registry (also associated with ICANN) and provide the full domain back to the user.

It is clear that ICANN has full control of the DNS ecosystem, meaning that it can approve and reject user requests as well as revoke purchased domain names anytime. On top of that, the domain buying process sets expenses to the user as fees have to be paid when buying a new domain.

Finally, although people often think of buying and owning domain names, the truth is that registries own all their domain names and registrars simply offer the opportunity to reserve those domain names for a limited amount of time. The maximum reservation period for a domain name is ten years. A user can hold onto a domain name for longer than ten years, as registrars usually let them keep renewing their reservation indefinitely (16).

3.3 Data Fragmentation

The fact that blockchain technology is based on cryptography can provide a solution to the censorship problems that have been listed above. Like in all the existing blockchain-based DNS systems, so in ours, dealing with censorship is one of our priorities. As we mention in section 4, the usage of blockchain technology can give a solution to this problem, and this is the main reason we decided to use it in the same way existing blockchain-based DNS do.

However, there is still a common problem all those systems are facing. Limited access to a narrow range of domain names. Current blockchain-based DNS can only support specific TLDs, meaning that users can only buy, and access domain names that their TLDs are supported by them. For example, Namecoin uses the .bit TLD, a fact that force domain names within the Namecoin blockchain to be related with the .bit TLD. In the same way Emercoin can only support the .lib, .coin, .bazar and.emc TLD which means that DNS requests that are not supported from the corresponded blockchain have to be forwarded back to the traditional DNS. As there is no currently any blockchain based DNS supporting this functionality, the respective networks return a NXDOMAIN response back to the web browser.

It is worth noting that technically, some current blockchain DNS systems like EmerDNS and ENS can support any DNS-zone or TLD, meaning that already purchased domain names can be stored in their ledgers (17). However, for seamless integration into a standard DNS tree, and to prevent collisions with existing DNS-zones, they currently support their own zones.

Chapter 4

Research Approach

The several problems mentioned above are the kick-starter of our current research. Apparently, current blockchain-based DNS face more problems, but we have not listed them all as we believe that dealing first with the fundamental ones is our top priority. After identifying the current main research gaps we came up with a concept, we believe it can be a solution to them. We therefore propose HyperDom, a fully autonomous permissionless blockchain operating between users and all current existing DNS systems (both traditional and blockchain-based), responsible for providing a secure interconnection with the DNS ecosystem.

As shown in figure 4.1, the main idea behind HyperDom is the implementation of a blockchain layer that will be able to give users access to all DNS systems in a decentralized manner. A mentioned in section 2, all blockchain-based DNS system use their own protocols and rules, meaning that they are only accessible through their own software. Our goal is to implement an intermediate blockchain layer between users and existing DNS systems and provide efficient, secure and private access to the DNS ecosystem.

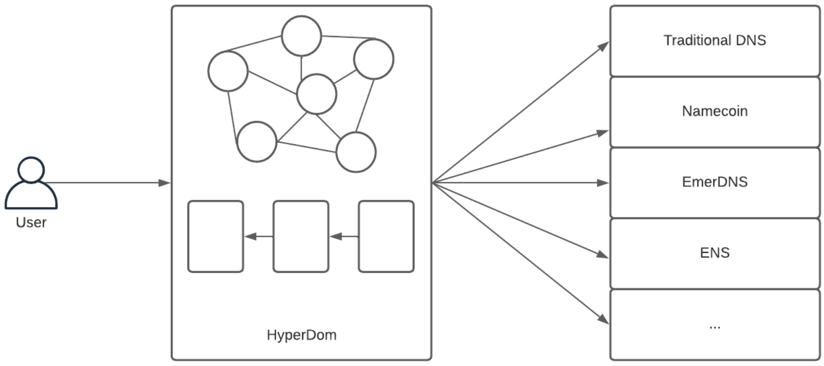

Figure 4.1: HyperDom blockchain logic

Our blockchain does not aim to replace any existing DNS system, but operate alongside them and improve the functionality of the current DNS. Below we explain the main operation of the HyperDom blockchain, and then we present our research approach through which we believe that we can find a solution to the problems mentioned in section 3 by implementing a blockchain such HyperDom.

4.1 HyperDom Concept

We can think of HyperDom as an ISP, with the main difference that HyperDom is a blockchain network and not a centralized scheme managed by a central authority. A DNS request is originated through the user's web browser and then forwarded to the HyperDom blockchain as shown in figure 4.2. HyperDom maintains its own public ledger, meaning that data (DNS records) are stored in it in a chronological order. Once the DNS request is routed to the blockchain, a smart contract is responsible for handling the request by looking for the associated IP address, which is stored in the ledger, and returning it to the web browser.

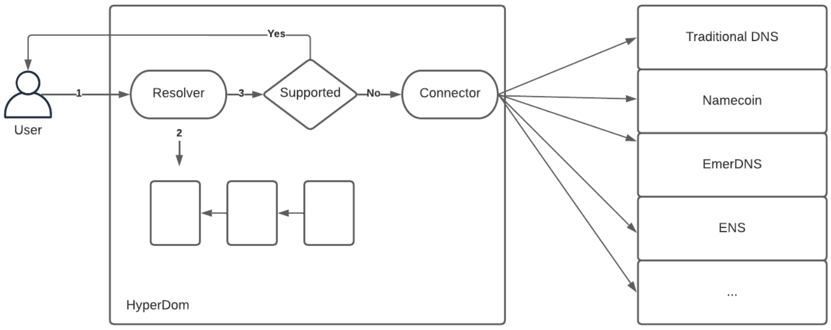

FIGURE 4.2: HyperDom workflow

Although ISP DNS databases store a wide range of DNS records, some requests cannot be handled by them and therefore forwarded to the DNS servers. As HyperDom operates similarly to an ISP, requests that cannot be handled must be forwarded to the corresponding DNS server, either it is the traditional DNS servers or a blockchain-based DNS ledger.

In the next section, we explicitly describe the main functionalities of the HyperDom blockchain and explain how they can give a solution to the problems mention in section 3.

4.2 HyperDom Approach

4.2.1 DNS Request Handling

According to the DNS request lifecycle, ISP's DNS server is the first stop of such a request. As we mentioned in the previous section, that can lead to privacy issues as data can be tracked or collected for commercial purposes. Mitigating unauthorized tracking or even preventing any kind of privacy manipulation is one of our top priorities that lead us to propose HyperDom. In order to be able to guarantee a private DNS system, we believe that replacing a central entity with a decentralized network based on blockchain technology is the first action we have to take.

The nature of blockchain networks gives the ability of anonymous data exchange between all users participating in it. DNS requests are handled by a fully autonomous network, which acts as a decentralized DNS system. HyperDom is responsible for handling DNS requests, as we will explain later. Even if HyperDom blockchain is unable to handle a DNS request, it acts as an anonymization mechanism. Request are anonymized before they are being forwarded to the corresponded DNS system and therefore data remain private.

Furthermore, as data within a blockchain remains anonymous, participants will not be able to take advantage of them for any profitable activities. It is obvious that a central authority such as ISP can bring up a variety of issues related to censorship. By replacing such an entity with a decentralized network like HyperDom we aim to prevent any kind of censorship concerns as requests have no identity within the blockchain and users can interact with any DNS system privately.

4.2.2 Network Availability

Another thing we want to make sure is that HyperDom blockchain remains fully available at any time. As mentioned before, a centralized system is vulnerable to availability issues. We are currently focusing on two factors that can lead to such issues. Central point of failure and insufficient number of nodes.

The term central point of failure refers to the vulnerable nature of a centralized system due to different scenarios that can set it unavailable. Some examples can be malicious activity, infrastructure overload or even system outages due to technical reasons. By replacing a central entity with a blockchain network, we aim to overcome such concerns by taking advantage of the blockchain properties. Blockchain networks are decentralized networks rely on a P2P protocol, meaning that each node maintains a copy of the current network state. All nodes are equally participate and contribute to the network.

Therefore, if a node goes out of order, the rest network is not affected and keep operating normally.

As for the network population, we want to make sure that our blockchain has enough nodes participating and equally contributing. A satisfactory number of nodes ensures the safety of the blockchain, as more nodes can prevent common issues like 51% attacks, which is currently a crucial issue of some blockchain DNS systems (18). Therefore, we propose an implementation on the top of an already existing blockchain such as Ethereum, instead of building our own one from scratch. By doing so we make sure that we take advantage of all the existing Ethereum functionalities (consensus algorithm, P2P rules, etc.) as well as its sufficient number of nodes.

4.2.3 Data Access

In section 3.3 we mentioned that current blockchain-based DNS systems can only give access to a specific range of domain names associated with supported TLDs. That means that unsupported DNS requests cannot be handled by those blockchains as well as forwarded to the traditional DNS. In order to tackle this issue down, and make our blockchain capable to handle any kind of DNS requests without relying on any other DNS system, we propose a storage solution within our own public ledger. The main idea is to gradually cache DNS records from the existing DNS systems into our ledger. By doing so, our network will be able to handle any kind of DNS request, no matter what TLD is associated with them. DNS requests will be handled in a decentralized manner by HyperDom instead of being forwarded to any other existing DNS system.

We also mentioned in section 3 that current blockchain-based DNS systems use their own protocols and rules, and therefore a different setup is required to access them. HyperDom aims to overcome this complex procedure by providing a sufficient interconnection with all the existing DNS systems. As long as DNS records are cached in HyperDom's blockchain, access to them can be archived without any effort.

4.2.4 Network Scalability

In terms of our blockchain architecture, we want to make sure that our network will be fully scalable and available to respond in an efficient way. As Ethereum 2.0 (19) is about to be launched soon, we would like to take advantage of some upgrades that it proposes in order to scale our blockchain. The main property that we would like to apply is the sharding architecture in order to achieve scalability and bring a solution to the storage problem. According to it, sharding splits an entire blockchain network into smaller partitions, known as "shards". Each shard consists of its own data, making it distinctive and independent when compared to other shards. DNS records are stored in different shards according to their top-level domains. In HyperDom shards will be designed according to their content size and can store a specific number of different top-level domains with unlimited number of namespaces associated with them. The size of each DNS namespace differs as more domain names are associated with more popular namespaces. For example, the .com namespace is larger than the .gr namespace. Thus, we must take into consideration this fact and equally distribute the namespaces into the shards.

By using the sharding architecture, we believe that we can find a solution regarding the storage problem. As we will see in the next subsection, our blockchain will handle data from all the existing DNS systems. A noticeable example is the traditional DNS. Currently, according to Verising (20) the size of the traditional DNS's dataset is approximately 90 GB meaning that once the whole DNS is mirrored in our blockchain, each node joining must synchronize 90 GB in their local storage. Instead, by proposing a sharded blockchain, we distribute the data within the shards and significantly decrease the storage requirements.

Chapter 5

Research Management Plan

After we make sure that our proposal fulfils the research gaps that we have previously mentioned, we are planning to start working on the blockchain architecture, so we can start making progress on the actual implementation. At first, a requirement analysis is considered essential in order to understand what tools and techniques we will need to start our implementation.

After identifying the fundamental tools, techniques and requirements that we need, we will start working on the actual blockchain implementation. Table 5.1 shows the tasks that we are going to work on during the next nine months. After that, figure 5.1 presents our time management plan through a Gantt chart.

Task Name	Description
Requirement analysis	Identifying tools, techniques and requirements
Overall architecture	Designing a network overall architecture
Blockchain setup	Setting up a basic blockchain
DNS requests handling	Implementing DNS request handling functionalities
DNS records mirroring	Implementing DNS records mirroring functionalities
Connection with existing DNSs	Setting interconnection with existing DNSs
Testing	Testing current implementation
Scalability improvements	Working on blockchain scalability improvements

Table 5.1: Tasks to be implemented

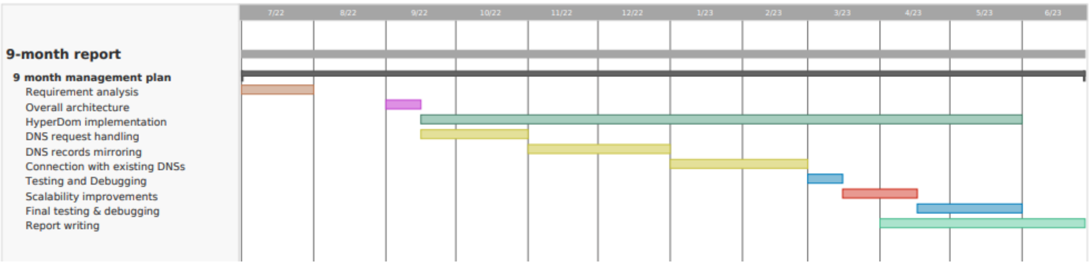

Figure 5.1: Workflow Gantt chart

Bibliography

[1] A. Roselli, “Make your own tld? (i want .bacon),” June 2011. [Online]. Available: https://adrianroselli.com/2011/06/make-your-own-tld-i-want-bacon.html

[2] “Namecoin.” [Online]. Available: https://www.namecoin.org/

[3] M. Ali and J. Nelson, “Blockstack: A global naming and storage system secured by blockchains,” June 2016. [Online]. Available: https://www.usenix.org/system/files/conference/atc16/atc16_paper-ali.pdf

[4] X. Duan and Z. Yan, “Dnsledger: Decentralized and distributed name resolution for ubiquitous iot,” 2018. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8326118

[5] C. PATSAKIS and F. CASINO, “Unravelling ariadne’s thread: Exploring the threats of decentralised dns,” April 2020. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9123760

[6] “Name collision resources information.” [Online]. Available: https://www.icann.org/resources/pages/name-collision-2013-12-06-en

[7] P. XIA and H. WANG, “Ethereum name service: the good, the bad, and the ugly,” April 2021. [Online]. Available: https://arxiv.org/pdf/2104.05185.pdf

[8] H. Community, “Handshake: Decentralized naming and certificate authority,” 2018. [Online]. Available: https://hsd-dev.org/files/handshake.txt

[9] “Unstoppable domains.” [Online]. Available: https://unstoppabledomains.com/developers

[10] A. G. Zhi Guan, “Authledger: A novel blockchain-based domain name authentication scheme,” 2019. [Online]. Available: https://www.scitepress.org/Papers/2019/73668/73668.pdf

[11] D. K. Wondeuk Yoon, Indal Choi, “Blockons: Blockchain based object name service,” July 2019. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8751464

[12] K. L. Xiangui Wang, “Consortiumdns: A distributed domain name service based on consortium chain,” February 2018. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8291986

[13] S. G. Zecheng Li, “B-dns: A secure and efficient dns based on the blockchain technology,” March 2021. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9387163

[14] M. BURGESS, “The uk is secretly testing a controversial web snooping tool,” March 2021. [Online]. Available: https://www.wired.co.uk/article/internet-connection-records-ip-act

[15] M. Klimas, “Can isps sell your data?” December 2021. [Online]. Available: https://surfshark.com/blog/isp-selling-data

[16] Cloudflare, “What is a domain name registrar?” [Online]. Available: https://www.cloudflare.com/en-gb/learning/dns/glossary/what-is-a-domain-name-registrar/

[17] E. Community, “Emerdns documentation.” [Online]. Available: https://emercoin.com/en/documentation/blockchain-services/emerdns/emerdns-introduction/

[18] Y. Liu and Y. Zhang, “A comparative study of blockchain-based dns design,” December 2019. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/3376044.3376057

[19] S. G. Rene Millman and L. J. Kelly, “What is ethereum 2.0? ethereum’s consensus layer and merge explained,” March 2022. [Online]. Available: https://decrypt.co/resources/what-is-ethereum-2-0

[20] J. Spencer, “How many domains are there? – domain name stats for 2022,” 2022. [Online]. Available: https://makeawebsitehub.com/how-many-domains-are-there/#:~:text=How%20Many%20Domain%20Names%20are,marking%20a%201.4%20percent%20increase