Title	Blockchain-Based Domain Name System
Student name:	George Giamouridis
Supervisor name:	Leonardo Aniello

Aims/research question and Objectives

Web security has been and will always be one of the most important areas of research in computer science. So far, the web-based architecture seems to serve the needs of the users but at the same time the security gaps are constantly increasing. One of the many internet security issues appears in OSI's model (Open Systems Interconnection model) protocols. The present research focuses on the vulnerabilities of the DNS (Domain Name System) protocol and presents a new solution which aims at the safest and most efficient use of this protocol.

The DNS protocol is of the client-server type and is therefore characterized as a centralized protocol. Such a system presents various critical vulnerabilities. Some of the main vulnerabilities which are the main cause of the present research are presented above:

1. **Central point of failure**: As long as DNS relies on a centralized entity, the availability of the service depends exclusively on it. If this central entity goes out of order, then the whole service will be unavailable until the central entity goes up again.
2. **Anonymity limitation**: ISP's (Internet Service Provider) provide their own domain name servers in order to serve their client's requests. Those servers are stetted to be the default servers and thus when someone asks for a domain name the request goes through this server in order to be matched with the appropriate IP address. Therefore, all the user's traffic is monitored by the ISP's as they have fully access to those servers.
3. **Registry control**: ICANN (Internet Corporation for Assigned Names and Numbers) is an American multi-stakeholder group and non-profit organization whose mission to coordinate the DNS. ICANN is the major controller of the Network. It is based on a technical background consisting of thirteen powerful computers, also known as "base servers", located in the US. As a result, only this organization is able to control the DNS and decide its content (website blocking, restrictions etc.)
4. **DNS attacks**: DNS attacks are one of the most popular attacks and are a big chunk of internet security research. Adversaries can exploit DNS's vulnerabilities by creating fake name-IP address pairs and redirecting users to malicious websites. Another crucial vulnerability is DoS attacks where adversaries send large volumes of requests to the servers in a very short period of time and therefore the servers cannot handle all these requests and are stetted out of order.

The present research focuses mainly on solving the following problems by proposing a new solution. The solution we propose is the research of a new DNS protocol which will be based on the blockchain technology. Such a decentralized network will be able to solve the problems of the current protocol and thus contribute to a more secure internet architecture. The main reason for using blockchain technology for such a project is:

- Reducing security gaps
- Improving protocol efficiency
- Equal participation

From time-to-time similar proposals have proposed. However, our proposal is the first research approach aimed at replacing the DNS protocol with a blockchain-based DNS.

Summary of proposed research and analysis methodology

The network we are going to implement is a blockchain network that will have the fundamental functionalities and features of such a network. Although the implementation of the network will start from scratch, many of its features will be based on already existing similar networks. For example, to implement the consensus algorithm, an existing algorithm used in another network will be used. Also, the process of nodes discovering when a new node joins the network will be based on the architecture of Ethereum network discovery (hardcoded boot-nodes). By following this tactic (using existing functionalities in other similar networks) we ensure that the basic functionalities of our network will be functional and secure. Thus, we will be able to focus on the basic functionality we propose which is to subdivide the blockchain network into smaller sub-blockchain networks and search for domain names on them.

The main reason for conducting this research is to create a more efficient and secure protocol. In order to be able to claim that the research was completed successfully, we must present some results that refute the following:

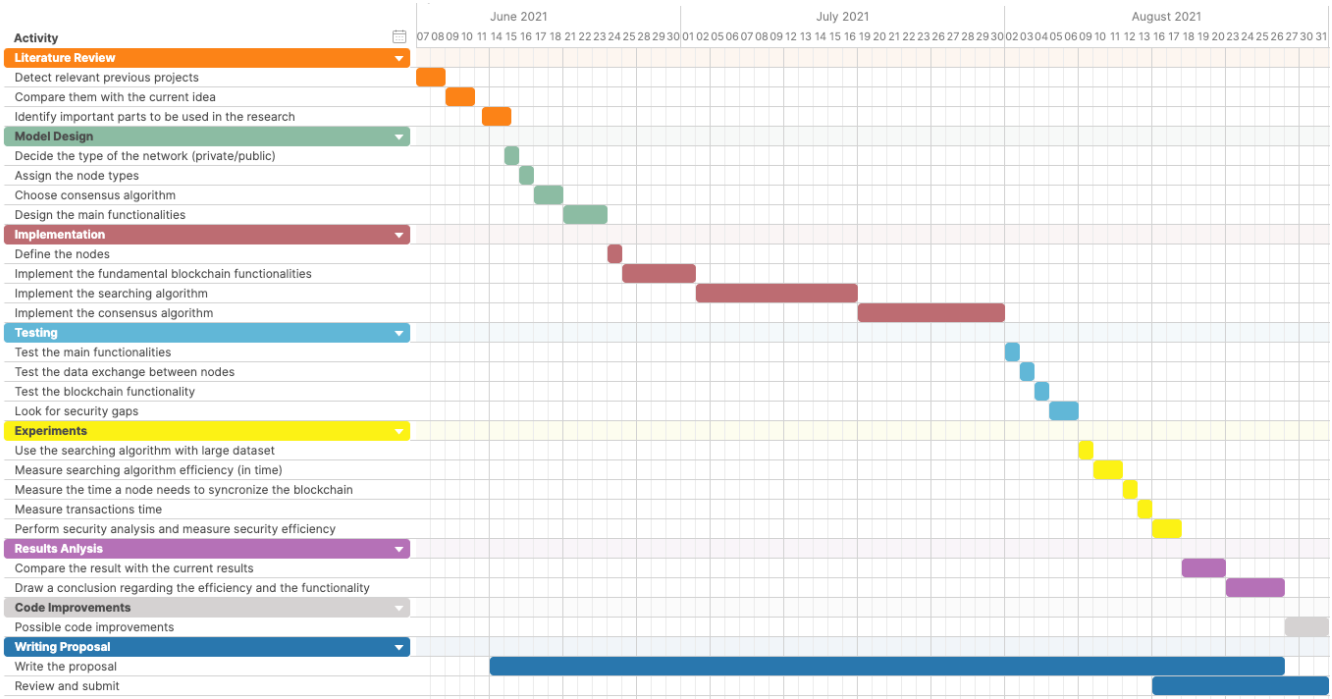
- Protocol efficiency over time
- Protocol efficiency in terms of security and anonymity

Efficiency measurement
The efficiency of the protocol in terms of time is one of the main challenges of this research. Its main function is to search for domain names in different sub-blockchains. Thus, we will be able to characterize the protocol as efficient if and only if the users' requests are served in a time efficient period. In order to be able to calculate whether our model is behaving efficiently in terms of time, we need to perform a series of real-time experiments to draw a conclusion. For this experiment we will use the search algorithm that we will implement in combination with a large amount of data to see how it works even in the worst cases. Then we will enter the same data in the current algorithm, and finally we will compare the results.

Security measurement
Security is the key feature we want to achieve in this research. As mentioned in the introduction, attacks on the DNS vary, making the protocol vulnerable. In our research we propose the use of a consensus algorithm in order to prevent and mitigate any possible attack. In order to be able to claim that our protocol meets the security criteria we need to make sure that possible attacks that may occur in the existing protocol are impossible to occur in our model. To achieve this goal, we will conduct a series of security analysis which will include penetration testing in the protocol. The results we will receive will confirm whether our protocol is finally secure or not.

Implementation methodology
In order to be able to present everything we propose we must have a basic model which will perform the basic functions. Therefore, we will implement a replica of the protocol which will be able to perform all the basic functions we have mentioned. This network will be implemented locally, and random data will be used for research purposes. When we manage to complete the implementation of the code of the basic functions, we will use real devices, and we will experiment with them again in a local network.

Research plan – Gantt chart or Pert chart



Ethical Statement and Data Management Plan

The network we are proposing is a blockchain network. These networks are known to handle sensitive personal data such as transactions, addresses and keys. A blockchain network is designed to store and manage data securely and anonymously. As in all networks, so in ours we must ensure that user data will be stored securely, and their transactions will be executed transparently. For this reason, we will choose a strong encryption algorithm such as SHA256 in order to be able to encrypt user data and store it securely in the blockchain.

Transactions
As mentioned before, transactions should be carried out safely and transparently. Transactions As in blockchain networks are stored in the public ledger and are accessible and visible to anyone. This results in the immediate identification of a user and thus the violation of his anonymity. In order to be able to avoid such incidents we will use transaction anonymization techniques as in the Monero blockchain network. This will ensure that transactions will remain anonymous, and users will not be able to be identified.

Keys and addresses
Addresses and keys are still an instantaneous piece of data that we need to make sure is stored and managed securely. In order to be able to secure this data we need to create a secure wallet for users. This wallet will be able to securely store and encrypt users' keys and addresses

The great advantage of using a blockchain network is that it does not require users to provide their personal data to use it. The network gives users some unique keys which represent them and at the same time maintain their anonymity. Thus, we will not have to direct deal with the user's personal data and decide the way we will handle them.

Ethical aspects

Ethical aspects regarding the consensus protocol
A blockchain network is characterized as a network of peer players who come to a full consensus on the decisions taken. In order for this to happen, blockchain networks use a consensus algorithm. The first blockchain consensus algorithm is called Proof of Work (PoW) and adopted by Satoshi Nakamoto in 2009 to the Bitcoin blockchain. Over time this algorithm has proven as the most capable of filling the security gaps of the network, resulting in its smooth operation. Today, most blockchain networks use the PoW algorithm to achieve network consensus. The name Proof of Work comes in response to a mathematical problem, that network nodes try to solve by using their computing power. The process is known as mining and the nodes on this network are known as miners. The high-power consumption causes the electricity companies to install facilities that generate power using renewable fuels, and this leads to more carbon in the atmosphere. This means that the high energy requirement of POW Bitcoin system encourages the use of renewable energy sources, thereby affecting climate change caused by more carbon emissions. As mentioned above, the mining process to achieve network consensus seems to have a negative impact on the environment. Thus, in our research we will try to complete the implementation of the network using another consensus algorithm (Proof of Stake) which will be more environmentally friendly. This algorithm tends to become as worthy as the PoW and at the same seems to be echo friendly.

Ethical aspects regarding the architecture
As we will mention in the next section, the DNS is based on a private company whose servers are located in four different countries of the world and therefore its operation is based on those servers. This means that these decorators must be active 356 days a year 24 hours a day so that they can serve the requests of the users. This results in continuous energy consumption. On the contrary, the network we propose is a decentralized network which does not depend on any central entity but at the same time can serve the requests of the users. This network does not require energy consumption and is therefore more environmentally friendly.

Commercial aspects

Like all public blockchain networks so ours will keep its own cryptocurrency. Therefore, this project can introduce two different ways in which someone can be benefited from a commercial point of view.

Mining
As we mentioned in the above section our network will start initially using the Proof of work consensus algorithm. The process by which this algorithm works is called mining and the users who participate in it are called miners. Miners use their computing power to extract new blocks and maintain network consensus. In return, they are rewarded with the network cryptocurrency for their contribution to it. Mining is therefore the first commercial way in which users can be benefited from the network.

Financial
Nowadays cryptocurrencies have acquired great value and are a key sector in the field of investment. As mentioned before, our network will maintain its own cryptocurrency. This, users will be able to buy and sell this cryptocurrency and with the right trading techniques to be benefited financially.

Although the original idea of this project is not a commercial product, we can easily, as we have shown before, find solutions from which users can be benefited financially. Also, the inclusion of a cryptocurrency in the market can bring changes in the current financial situation

Legal aspects

As longs as the project will manage user data directly, we will need to make sure it complies with any legal framework related to personal data. Personal data follow the legal structure of the General Data Protection Regulation (GDPR). In our case, there is no third-party entity (company, organization) which must comply with the GDPR. As known, a public blockchain network is a decentralized peer to peer network that is maintained and operated by its own users. So, we have to make sure that even if our network is not relying on a central authority that has to comply with the regulation, it meets all the legal (GDPR) requirements.

Right to access
According to Article 15 of GDPR, data have the right to receive confirmation from the data controller. However, it has been observed that some entities designated as data controllers may not have access to blockchain data. As a result, they may not be able to determine whether the ledger contains real personal data about the subject to whom they refer, a fact which activates the right of access.

Right to alteration/deletion
According to Articles 16 and 17 of GDPR, the data subject has the right to request from the data controller the correction or deletion of inaccurate personal data. In Blockchain networks the modification and deletion are extremely difficult processes so to ensure network integrity and reliability. This is in contrast to the GDPR, as according to it the data must be changed in order to make it possible to delete them.

Right to transition
According to Article 20 of the GDPR, the data subject has the right to receive the personal data concerning him/her and to transfer them to another auditor. The French Data Protection Authority (CNIL) considers that blockchain technology does not create problems in complying with the data transfer requirement. However, Article 20 of the GDPR, emphasizes the interest in ensuring interoperability between different solutions in blockchain networks. It has been emphasized in relation to social media networks that it does not make sense to transfer data from one provider to another. The same concerns raised by shared networks also apply to blockchain networks. Effective enforcement of data transfer is therefore one of the many reasons that should encourage the interoperability of different solutions.