# Blockchain-Based Domain Name System

UNIVERSITY OF Southampton

**George Giamouridis**

*Supervisor: Leonardo Aniello*

*M.Sc. Computer Science*

## Objectives

The main goal of this project is to prove that the replacement of the classic DNS with a decentralized network can offer the same functionality, and will also provide web users:

- Equal participation
- Anonymity on the web
- Advanced security
- Central authority independence

## Introduction

DNS protocol is one of the most important application layer protocols that translates names into IP addresses and vice versa. Although its presence is extremely crucial and the functionality of the web depends on it, its architecture and the way it works brings to the surface countless problems for web users.

This protocol relies on the C2S architecture and therefore depends on a central authority that is responsible for its management. As it is well known a centralized system presents several vulnerabilities and anonymity issues. In this project, a decentralized approach of the classic DNS is introduced, with the ultimate goal of the complete replacement of the classic DNS model.

## Methodology

This project relies on three basic components which form the core of this research

### *Blockchain Distribution*

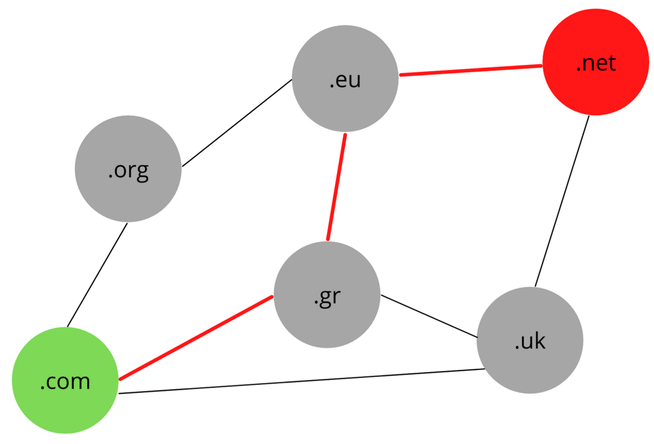
All nodes share a DHT with information about the current network status. When a node joins the network its type is determined according to the DHT.

### *Searching Algorithm*

Requests are propagated to the network trying to reach a node for a response. A searching algorithm is used to discover an appropriate node.

### *Consensus*

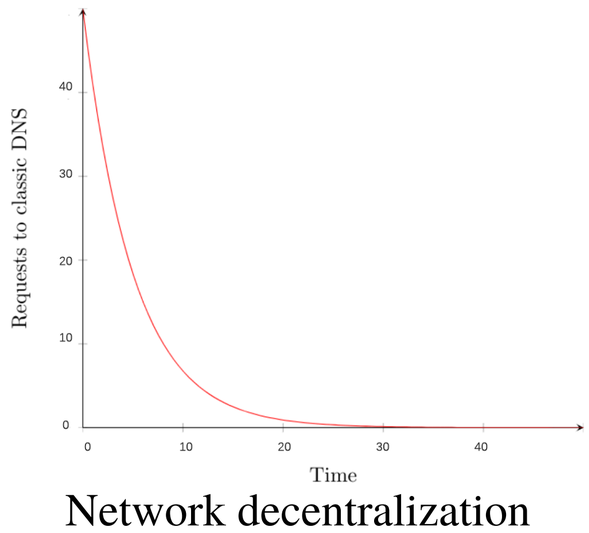
Blockchain consensus is achieved when all nodes agree about new pairs integrations and also their validity (avoiding redirections into fraudulent websites).




Requesting a .net domain

## Results

Network decentralization relies exclusively on the number of users and their activity (requesting new domains).




Network decentralization

Since the blockchains will initially be empty, user's requests will be unable to be granted, and therefore they will be forwarded to the classic DNS.

After a new domain is served by the classic DNS, it is recorded in the blockchain and the ledger is updated.

Therefore, the higher the user activity (more requests to the classic DNS), the faster the network decentralization.

## Important Notice

This project is about a public (permission-less) blockchain that doesn't maintain or issue any cryptocurrency.

Its purpose is to improve an existing protocol by adding new features.

Putting all the above together, usage of this new decentralized network results in:

1. Equal participation. Users have the right to request but at the same time they serve the rest network's requests
2. Anonymity. Encrypted communication channels keep all information anonymous from the ISP
3. Advanced security. Consensus protocol ensures network agreement. All pairs are confirmed by the network
4. Independence. All nodes act on their own, and they don't rely on a central authority (ICANN). Restrictions are eliminated

## Conclusion

This project proves that the replacement of a classic DNS with a blockchain-based DNS, does not negatively affect the basic operation of the protocol, and at the same time can combine equal participation in the network, anonymity, security, and central authority independence.

## Acknowledgments

The idea of a blockchain-based DNS has already proposed by other researchers. Most of these projects aim for specific domain name categories (e.g. only .onion domains). This project is the first approach of including all domain categories in a blockchain network which will operate in the same way as the classic DNS does.