Abstract

In modern day network browsing behavior, Domain Name System (DNS) plays a huge role. DNS provides the service for mapping a domain name to the underlying IP address. The DNS is a distributed and hierarchical system, where root servers control the top level assignments, and detailed mapping information are provided by name servers lower down in the hierarchy. This conventional system has many advantages, including its scalability and reachability. However, the root servers and the lower level name servers are usually controlled by governmental institutions or for-profit organizations. This has led to many concerns of the system, such as censoring and commercial takeovers. In this project, we attempt to explore the possibility of migrating the DNS onto a block chain based implementation, where the DNS system can be truly democratized.

1 Introduction

Domain name systems (DNS) are the primary way we establish the mapping between a domain name and the IP address of the host. Since the introduction of the system back in 1987 (RFC1034 & RFC1035), this system has dominated the way we use Internet. Nowadays, people never refer to a website by its IP address, a domain name is always used instead. Finding a good domain name is also a big part of running a business. Having a catchy domain is key to customer recall and retention, and legal disputes over popular domain names are coming to public attention more and more often.

However, the domain name system was never designed to be democratized. With the hierarchical design, whoever controls the root servers of the DNS will therefore have control over which version of the mappings is used for query the IP of a domain. In order to make sure that this mapping is consistent throughout the world, root servers are largely controlled by semi-governmental institutions such as ICANN. ICANN then delegate Top Level Domains (TLDs) to registries, and registrars make profit by serving individuals who are interested in registering for a domain name. This multi-level middleman structure is a big obstacle for coming up with new TLDs, and some registrar dramatically overcharges for popular domain names. Moreover, this gives the possibility for a party to seize control over the entire system.
This inevitable flaw in design gave rise to internet censorship methods such as DNS blocking, where by forcing you to use a specific name server, controlling the mapping maintained by that name server is sufficient to completely control your access to the Internet through domain names.

This is an ideal use case for block chain technology. If block chains can guarantee the consistency of multiple copies of a ledger, then adapting this property to the field of domain name systems seems like a low hanging fruit. Instead of starting each DNS resolution query with root servers, we could design a resolution mechanism that obtains the mapping from the chain, which we know will be consistent and highly available. (The chances of not being able to reach any node in the chain is low)

There are prior attempts in adapting the DNS to a block chain based implementation. In this research, we will review the flaws and vulnerabilities of the existing attempts, and propose a new system that addresses a subset of the issues with these attempts.

2 Proposed Structure

The project can be broken up into two phases.

2.1 Phase 1

During phase 1, I will perform a review of the existing attempts of adopting block chain technology onto the domain name system. An analysis on the pros and cons of the existing attempts will be made.

2.2 Phase 2

We then focus on decomposing these implementations into the fundamental functional blocks. For each functional block, we assess the risk of that block being the flawed due to program logic error or limitations of the implementation platform. Then we attempt to isolate that block into an individual piece of software, which may require a re-implementation to strip out unnecessary parts. We then explore ways to improve this specific component of the system.

3 Deliverables

At the end of term, I will provide the following:

- A written report that details the research and organization from the first part of the project, i.e. a review on the current state of the art implementations of block chain backed DNS, and an analysis of the pros and cons of each implementation.
• A written report that details the components that are commonly observed in these implementations and the role of these components. The report will also include at least one isolated piece of the component which can be tested on its own.

4 Time line

The project time line will be organized in two-week blocks.

• Week of Sep 24 - Oct 5
  – Studying existing literature on block chain and its application on DNS.

• Week of Oct 8 - Oct 19
  – Familiarize with Solidity, which is necessary for understanding Ethereum based implementations.

• Week of Oct 22 - Nov 2
  – Compare the existing implementations and make analysis on their advantages and flaws.

• Week of Nov 5 - Nov 16
  – Decompose the existing systems into common patterns of functional blocks. Isolate one piece of the blocks to further investigate.

• Week of Nov 19 - Nov 30
  – Continue work from previous week, explore ways to further improve that specific block of the system.

• Week of Dec 3 - Dec 14
  – Work on write-up and set future goals.

5 Calibration

I intend to meet with Professor Piskac weekly to update her on my progress and adjust the time line and goals of the project as we see fit.