GeoENS: Blockchain-based Infrastructure for Service Discovery at the Edge

James Choncholas
Georgia Institute of Technology
jchoncholas3@gatech.edu

Ketan Bhardwaj
Georgia Institute of Technology
ketanbj@gatech.edu

Ada Gavrilovska
Georgia Institute of Technology
ada@cc.gatech.edu

The Domain Name System (DNS), a standard way of looking up IP addresses of internet services, has served the Internet ecosystem well. However with the advent of edge computing it falls short of some *must-have* functional properties as well as *good-to-have* desirable properties. The *must-have*s include fine-grained geographic localization and discovery of edge services. The *good-to-have*s include doing so in a timely manner with low overhead costs measured in storage and bandwidth as well as user privacy preservation.

To illustrate the need for DNS infrastructure purpose built for multi-access edge computing, consider the following example. Suppose a computer vision service which assists autonomous vehicles is running on hardware at the base station of every cell tower in the United States. In traditional DNS infrastructure, this service would have a CNAME record pointing to an authoritative nameserver which would use GeoIP services [4] to direct users to the closest instance of the edge application. To provide location-specific query resolution, DNS relies on a distributed tier of nameservers, each resolving queries to local/nearby service provider instances. Unfortunately, current support for geo-localization operates in coarse geographic granularity due to the fact that query localization is based on third-party services with variable accuracy. This is due to the limited ability of GeoIP services to localize users by IP address [5]. The course granularity at which GeoIP services operate are unacceptable for edge applications which demand ultra low latency between end users and the edge.

Motivated by these gaps, this work explores the opportunities of a new blockchain-based DNS service which integrates native support for fine grained geographic split horizon DNS and invalidation-based cache management. The resulting system – GeoENS – represents an edge enabled service discovery mechanism that maintains backwards compatibility with DNS. Fine-granularity geographic split horizon is required for users to locate nearest service providers while intelligent cache management keeps the process fast. More technically, GeoENS includes the end user's location with their DNS query and allows end users to perform DNS lookups by geographic bounding box. To accomplish this, GeoENS is built with smart contracts on the popular decentralized, blockchain-based DNS system ENS (Ethereum Name Service.) Using the blockchain allows greater flexibility in which servers can act as recursive resolver in the traditional DNS system while simultaneously addressing issues of privacy and record authenticity that have plagued DNS infrastructure for years [1–3]. Overall, this work makes the following research contributions:

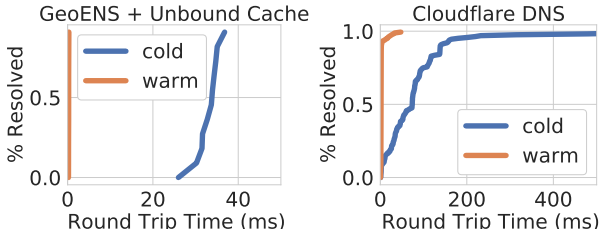

Figure 1: Tests measured 5 queries, every 125 minutes, for twelve total runs. The first query of the five was considered cold. DNS record TTL was set to 1 hour to ensure recursive resolver cache flushes between measurements.

- The feasibility and design challenges in developing a DNS-like system for edge computing using a privacy preserving, decentralized, replicated ledger.
- Geo-localization for blockchain-based service discovery.
- Preliminary results shown in Figure 1 demonstrate GeoENS can improve cold query lookup time by roughly 50% on average, trading performance for storage and idle bandwidth usage.
- A discussion outlining open technical challenges for building a practically deployable solution.
- An open source implementation of GeoENS[1] and a standard proposed as an Ethereum Improvement Protocol EIP2390[2].

[1] https://github.com/ensdomains/resolvers/pull/35
[2] https://github.com/ethereum/EIPs/pull/2390

References

[1] Derek Atkins and Rob Austein. Threat analysis of the domain name system (dns). Technical report, RFC 3833, August, 2004.

[2] Collin Jackson, Adam Barth, Andrew Bortz, Weidong Shao, and Dan Boneh. Protecting browsers from dns rebinding attacks. *ACM Transactions on the Web (TWEB)*, 3(1):2, 2009.

[3] Amit Klein. Bind 9 dns cache poisoning. *Report, Trusteer, Ltd*, 3, 2007.

[4] MaxMind. Geoip2 databases and services. https://www.maxmind.com/en/geoip2-services-and-databases, 2020.

[5] Yuval Shavitt and Noa Zilberman. A geolocation databases study. *IEEE Journal on Selected Areas in Communications*, 29(10):2044–2056, 2011.