Introduction

This is a community pool funding request for a domain name system built on Secret, an approved CCBL project.

Background

Team Digiline started building for Secret Network during the HackAtom 7 Hackathon. We delivered a well developed POC of a 100% on-chain trading card game, Secret DreamScape. We then received community bootstrap funding to turn the POC into a fully functional MVP with playable NFTs, and executed that vision in only two months.

The game received little traction at launch. So with our newly built development experiences we went back to SCRT Labs and pushed for a grant to build a Remix-like editor for Secret Contract development. Our logic suggested that if the dApp user base is small then Secret Network needed more dApps, and the best way to attract more dev teams would be to build a better development experience.

We then received a grant to build Phase 1 of theRemix-like editor and it was delivered on time and on budget. After the Phase 1 launch, we expected to commence a Phase 2 build for the editor which would elevate the development experience further. However, the market took a nose dive and SCRT Labs chose not to fund development of Phase 2 until market conditions improved.

Respecting SCRT Labs risk calculus, we brainstormed what else could be deemed more important than the best developer experience during a bear market. We landed on a DNS built on Secret.

DNS

DNS is a foundational layer of the internet. It was originally designed to be decentralized but due to lack of blockchain technology, it became the hybrid centralized/decentralized system we have today. DNS is like a top layer of the internet and everyone relies on it equally to trust their data is not exploited or used in malicious hacks. Every time you visit a new website, you use DNS, exposing yourself to vulnerabilities and giving away your data. The DNS market which includes Domain Name Registrars and DNS Service providers is a multi billion dollar industry with an increasing CAGR likely due to Premium Domains and an exponentially growing internet. Despite this, the industry hasn't changed much since the early 90s and it has some root problems that have never really been fixed. Instead, the industry has been growing by adding more layers of complexity alongside patchwork and duct tape solutions to the DNS system to attempt to fix the problems.

The core problems with DNS are characterized by the following categories, these are the same problems that any complex centralized system will have:

- Security
- Privacy
- Ownership

The DNS market is ripe for disruption and Secret DNS aims to be the project to do so.

This proposal will discuss the problems with the current DNS system and how Secret DNS aims to solve them at the core level. No more patchwork. No more duct tape. No more layers of complexity. Just a simple, secure, private, and decentralized DNS system.

Overview of the current DNS system

The current DNS system is a hybrid decentralized/centralized system. The centralized system is called the root servers and there are 13 of them located around the world. These root servers are the top of the DNS hierarchy and they are responsible for resolving the top level domain (TLD) names to their authoritative nameservers. The TLD names are the names that end with a dot and a letter. For example, the TLD name for the domain name scrt.network

is .network

. These TLD names are managed by the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a non-profit organization that manages the TLD names and they are the ones that approve new TLD names. No new TLDs can be created without ICANN's approval

. These authoritative nameservers control the domain names for the TLDs that they are responsible for. For example, one of the authoritative nameservers for the .network

TLD is v0n0.nic.network

. The TLD authoritative nameservers are responsible for resolving SLDs, or second level domains to their own authoritative nameservers. For example for scrt.network

the nameservers are penny.ns.cloudflare.com

and darl.ns.cloudflare.com

.

❯ dig +noall +answer scrt.network NS scrt.network. 86347 IN NS penny.ns.cloudflare.com. scrt.network. 86347 IN NS darl.ns.cloudflare.com.

The part of DNS that is currently decentralized is what happens at the domains' nameservers, which are the last level of the DNS hierarchy. These nameservers are responsible for setting the DNS records we're all familiar with, such as A, CNAME, etc.

The Problems

Lack of Privacy and Security

When you query a nameserver for a domain name, the nameserver will return the DNS records for that domain name. Additionally, the WHOIS and the RDAP protocols allow for storing additional information about a domain name. This additional information includes the domain name's owner, the domain name's technical contacts, and the domain name's administrative contacts, along with their physical address, email address, and phone number. This information is stored in a centralized database and is completely public - a massive problem for privacy.

The WHOIS privacy protection services many major registrars offer are just a layer of duct tape. Those privacy protection services store your information in centralized databases, which are accessible by anyone with the resources to do so, including registrar employees, TLD companies, ICANN, and hackers.

Worse yet, there's a more significant problem. DNS queries are not encrypted. Anyone who can see the traffic between you and the nameserver can see the domain name you're querying - meaning that when you navigate to websites with HTTPS, an attacker may know what website you're visiting, with a few exceptions. Numerous issues can still arise even when you inherently trust your DNS Recursive Resolver. For example, security researchers have found ways to intercept DNS queries over the network (Randall, A., Liu, E., Padmanabhan, R., Akiwate, G., Voelker, G. M., Savage, S., & Schulman, A. (2021). Home is where the hijacking is. Proceedings of the 21st ACM Internet Measurement Conference.). This has historically been used as a way to track users across browsers and IP addresses (Klein, A., & Pinkas, B. (2019). DNS Cache-Based User Tracking. Proceedings 2019 Network and Distributed System Security Symposium).

There have been attempts at solving DNS security issues with DNS over HTTPS (DoH) and DNS over TLS (DoT) . The problem with DoH lies in trust. In DoH, DNS queries are sent to a centralized entity (such as Google or CloudFlare). You're now trusting yet another centralized entity to not look at or not store your data. DoT suffers from very much the same problems. DoT is essentially just a different implementation of the same idea as DoH.

We could keep listing issues with DNS for hours here and mention things such as DNS hijacking and DNS cache poisoning, but the above problems are probably enough to illustrate just how insecure the current implementations of DNS are.

Lack of Ownership

Ownership, as most of us understand the term, falls short in traditional DNS. If you were to purchase a domain name such as libertyandprivacyarerights.com

, you'd be expected to pay an annual rent to a centralized for-profit entity, your registrar. The registrar then pays the TLD owner and ICANN, and then they can do whatever they want with the domain name. You don't own the domain name; you only own the right to use it. This is a problem for freedom of speech and freedom of expression. In addition to that, you're not allowed to transfer your domain name to another registrar without the permission of the registrar you're currently using, and even when you do have the permission, i.e. the domain is "unlocked", you're still not allowed to transfer it to another registrar without a 60 day waiting period. A registrar can also charge you a fee to unlock your domain name and transfer it to another registrar.

The Solution

Secret DNS will provide all the features of traditional DNS. Plus, it will fix the existing problems of traditional DNS that all internet users today accept. Thanks to Secret Network, a truly decentralized and community-governed internet can be born.

Secret DNS is a decentralized, permissionless naming protocol in a separate, community-managed DNS root that will allow anyone to register a domain name, set the DNS records for that domain name, and create a TLD without the need for a centralized entity. Secret DNS will be a completely new DNS root managed by the community. The community will vote on the rules that govern the Secret DNS root, the fees charged for domain name registration and possibly renewal, and the

ability to disable domain renewal costs at the TLD level.

Secret DNS aims to prove new ways the internet can be more secure, resilient, and socially beneficial.

Why Secret, and what about ENS and Unstoppable Domains?

1. Ethereum-based DNS has no privacy controls. It would be possible to discover the owner of a domain and track all of their financial transactions.
2. Unstoppable Domains does not offer all of the features of traditional DNS such as all record types and classes. Besides wallet address resolution, Unstoppable Domains only resolves IPFS content. Secret DNS will offer all the same experiences used with traditional DNS.
3. Secret DNS is designed and funded from the ground up to be community owned and governed.

See the table below for a more granular comparison to all other options.

How is Secret DNS different?

Traditional DNS

ENS Domains

Unstoppable Domains

Handshake

Secret DNS

Centralization

Centralized to a very small amount of entities

Technically controlled by a DAO, but not really decentralized

Controlled by the main development team

Completely decentralized

Completely decentralized

Privacy

Very limited and not very trustworthy

Nonexistent: every domain is associated to the eth address of the user registering it

Nonexistent: every domain is associated to the eth address of the user registering it

Limited. Once someone knows you own a particular domain they can quickly find out all the other domains you own.

Verifiably Private

Security

Very low, for the reasons mentioned above

Low, DNS queries can be tracked by the querying node or by MitM attacks

Low, DNS queries can be tracked by the querying node or by MitM attacks

High: DNS queries are entirely private and cannot be tracked (assuming that the resolving happens with hnsd).

Very High: DNS queries are entirely private and cannot be tracked. Queries don’t even need to go to any other server to resolve to an answer.

Ownership

Low

Medium, the owner truly has control over the domain and decides what to do with it, but they still need to renew a domain to not lose control

High, the owner truly has control over the domain and decides what to do with it

High, the owner truly has control over the domain and decides what to do with it

High, the owner truly has control over the domain and decides what to do with it

TLD-Creation

Centralized, long laborious process

Centralized process

Centralized process

Completely decentralized and community controlled.

Completely decentralized and DAO controlled

Domain Creation

Slow, may take up to a day with some registrars

Fast, always takes a few minutes to a few hours

Fast, always takes a few minutes to a few hours

Extremely slow, may take days or weeks to get a domain, depending on how popular it is.

Instantaneous, takes 6 seconds

Censorship and control

Centralized, multiple entities have power to censor

Centralized, but unlikely

Centralized, but unlikely

Not possible without a hard fork

DAO controlled and discouraged for anything but the worst things imaginable

Deliverables, Timelines, and Ask

Contracts

- Root Contract - This contract replaces the traditional DNS root run by the 13 entities mentioned above. It will also manage TLDs and all the records for every domain, replacing every layer of the traditional DNS root as well as the TLD servers and domain nameservers.
- Estimated delivery date: Oct. 20th
- Estimated delivery date: Oct. 20th
- DAO contract - This contract adds the DAO controls so that DNS finally becomes a community managed service, enabling the community to own a foundational layer of the internet.
- Estimated Delivery Date: Oct. 27th
- Estimated Delivery Date: Oct. 27th

Frontend

- A browser extension - will allow user to browse websites on Secret DNS.
- Estimated Delivery Date: November 10th
- Estimated Delivery Date: November 10th
- A basic frontend registrar service - will be built that allows users to purchase domains.

- Estimated Delivery Date: November 10th
- Estimated Delivery Date: November 10th

All contract code will be open sourced at the conclusion of the project. Estimated date of November 10th.

Total ask $40,000. Amount of SCRT asked to be updated in this thread at time of going on-chain.

Funds will be used for product development, testing, design, quality control, and post MVP business development. We have a third and possibly fourth team member ready to join us for this effort if the proposal passes.

Expectations After Community Bootstrapped MVP

The community funds will provide us the development support we need to bootstrap a fully functional MVP. The MVP will need further support to grow and develop into a domain name system that becomes widely adopted. The end goal being native OS and native browser support.

After launch, we will hold an NFT sale. There will be 1337 NFTs each with a unique rarity score. The rarity score will be proportional to the amount of Secret DNS utility tokens (SDNS) that can be claimed by the owner of the respective NFT.