Which way to decentralization: A Comparative Study of DNS and ENS

ERIC OSTERWEIL

LIXIA ZHANG

Internet Namespace: the state of affairs

- DNS has been a core supporting component since the dawn of the Internet
- A growing (mis)perception: the DNS namespace is “centrally controlled”
- Several blockchain-based naming systems appeared lately, each claiming to provide “decentralized namespace”
  - One example: Ethereum Name Service (ENS)

Ethereum Name System

- Ethereum is built on using public keys as identifiers (self certifying names, SCN)
- Added ENS to replace keys by (DNS-like) names as the primary identifiers for users

  →Users need semantic names

  - i.e. meaningful to human being
- ENS name resolution:

  name → SCN → on-chain record

DNS, ENS comparison: focus on 3 questions

1. Who are the control parties for name assignments
2. How each of the two systems provide name registration and authentication
3. How each system performs name resolution

- The answers to all the above questions directly relate to how/where the data of each system is stored
  - ENS stores all data on a single crypto chain.

Concepts & Terminology Clarification

- Self-certifying name: using a crypto key as an entity's name
- immutable ledger through cryptographic chaining
- Two different types of immutable ledgers
  1. Identity-based crypto chaining: ***ledger***
     - e.g. Hyper Ledger https://en.wikipedia.org/wiki/Hyperledger
  2. Anonymous crypto chaining: ***blockchain***
     - Use SCNs, hide real user identities

Blockchain 101

- No trusted party; no (relation to real world) identity
- support claimed *decentralization* by 3 pillars:
  - *truth* determined by voting via *proof of work* (or stake, or space)
  - Ensuring *immutability* of truth by chaining all voted records on *a single chain*
    - All things on chain = truth
  - *transparency* by making all chain records public

Q1: who controls the namespace

2 sub-questions:

- Who controls the name assignments under the root node
- Starting from each child name N_C under the root: who controls the name assignments of N_C: the parent node N_P , or N_C itself

The control of root domain

- DNS: everyone at ICANN78 knows
    - Unclear the same is true for everyone else
- ENS:
    - Allocation of TLDs is managed by multisig contract by 7 people
        - yet to be observed in action; up to now ENS has allocated one TLD of .eth
    - Decentralized Autonomous Organization (DAO) of Ethereum users supposedly governs various other aspects of the root domain (to be studied)
        - devils are in the details:
            - users' voting power ≈ their stake in Ethereum
            - due to anonymity, no truth about DAO members (how many, who they are) – out of reach of law enforcement

The control of other domains

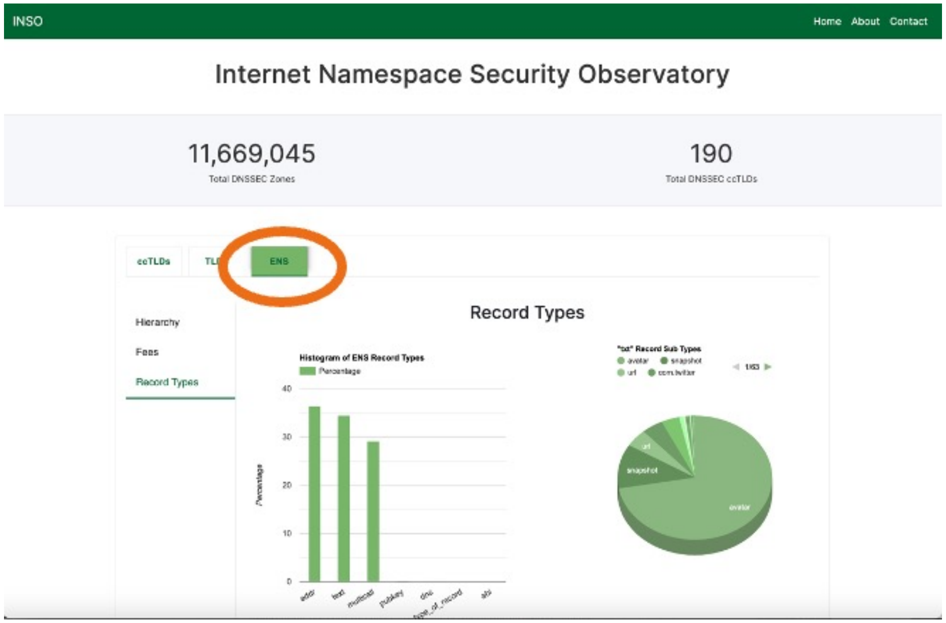
- Observation: name assignment and registration are tied together
- DNS: `example.com` owner makes decision on name assignments/revocations and handles registration (for names directly under it)
- ENS: `example.com` owner makes decision on name assignments/revocations, which has no effect unless/until the corresponding records added to *the Ethereum chain*
    - Taking multiple steps, has a cost

Adding a name to Ethereum chain: steps & cost

- Reserve a name:
  - Send commitment request ($)
  - Send registration request ($)
    - In addition: .eth registrar charge $5/year per name; shorter names cost more
- Set “resolver” contract ($)
  - Can contain Ethereum identifier, other blockchains identifier, IPFS pointers, etc. (adding new types costs $)
  - Can use default public resolver contract (limitation)
  - Miners check new contracts, bid on the addition to the chain
    - rich miners likely to win, get richer, increase future chance
  - Modification to existing records: set new contract ($)

Preliminary measurements

- Will be discussed in Wednesday's DNSSEC and Security Workshop
  - ~3.7% of “Text” types in ENS point to email addresses
  - ~4.7% point to URLs (DNS-based)
  - ~4.5% point to twitter.com
  - ~5.3% point to domains in .com, .org, .xyz, .me, ...



Internet Namespace Security Observatory

11,669,045
Total DNSSEC Zones

190
Total DNSSEC ccTLDs

Q2: Name authentication

- DNS: through DNSSEC
  - Retrieving DNSSEC info via the same process as name resolution
- ENS: on chain record = authenticated data

Q3: Name resolution

- DNS: lightweight look up of *distributed database*, heavy use of caching
- ENS: name → SCN → on-chain record
  - 2 options: run a full node oneself (costly if doable at all), or pay for a lookup service ($, choice of most users)
  - Steps:
    - Hash the ENS name to get the domain's *master contract* from the chain
    - The master contract points to a *registrar contract* (responsible for the record of name-identifier mapping)
    - Use the Ethereum identifier to find on-chain record

More digging needed to fully understand all the operations...

Next step: validate the following Hypothesis

- Networking needs a unified *semantic* namespace
  - Blockchain systems adding DNS-like names
    - sugar-coating over their SCN operations
- Blockchains operate with anonymous keys in absence of trust, thus cannot lead to decentralization
  - Anonymity → proof by resources → rich gets richer → concentration of power
  - No trust → single chain → need centralized servers to perform expensive lookup

Expected Outcome

- Document a comparison of
  - ICANN’s formulation and decision making process
  - ENS DAO’s formulation and decision making process
- Similarly, document DNS’ vs. ENS’ name registration and authentication processes
- Finally, document an analyses of resolution process in the two systems

Focusing on Security, Scalability, and Resiliency of the solutions, and consequent implications on (de)centralization.

https://inso.gmu.edu/docs/Blockchain_Naming___DNS.pdf

Departing words (I): why semantic namespace

- Human society operates on trust
- Human society is protected by laws
- Both trust and laws require unique identifiers in a semantic namespace
    - Which is the Domain Name System we have today

Departing words (II): which way to decentralization

- Blockchain-based designs do not lead to a decentralized naming system
  - Due to economy of scale, proof by resources leads to centralization
  - Due to absence of trust → replicated single chain, unscalability leads to centralization
- As a distributed database, DNS is a completely decentralized name system, with democratic root governance to assure name uniqueness, that blockchains claimed to achieve
- Decentralizing the Internet: enabling direct user-to-user communications to run apps without reliance on clouds
  - Offer users cloud-independent identities (e.g. DNS names)
  - Together with cloud-independent security solutions.