Blockchain Naming as Only Partial Decentralization

Paul Hoffman

ICANN DNS Symposium 5
15 November 2022

Overview

- The promise of decentralization
- Decentralization as “differently centralized”
- Alternatives to blockchains for decentralized naming

Internet namespaces

- Namespaces can be almost anything, but tend to be strictly or approximately hierarchical
- International control with unequal hierarchies in identifiers
  - Postal addresses
  - Phone numbers
- One-level of hierarchy for technical identifiers
  - MAC addresses
- DNS names!

Blockchain namespaces

- Probably due to the ubiquity of the DNS, blockchain namespaces are hierarchical, usually with dot-separated names
- Familiarity breeds confusion
- Promises of decentralization may be overblown

Decentralization in namespaces

- Once allocated, the root cannot change the properties of a top-level name
- “Censorship-resistant” in that each name controls its own namespace
- Lack of WHOIS/RDAP equivalents: names are mapped to wallet addresses or cryptographic keys with no link to a real person or organization

Decentralization reality (1)

- All namespaces have a controller who can, if necessary, remove a name
- Here, decentralization means “rarely enforced rules”
- ENS:
  - “The root node is presently owned by a multisig contract, with keys held by trustworthy individuals in the Ethereum community. We expect that this will be hands-off, with the root ownership only used to effect administrative changes, such as the introduction of a new TLD, or to recover from an emergency such as a critical vulnerability in a TLD registrar.”
- This is less centralized than what can happen in the global DNS, but still has centralization features

Decentralization reality (2)

- Blockchain naming is based on crypto currencies: you need some currency to buy names
- But many crypto currencies have very small pools of large holders
- Decentralized money is often managed by venture capitalists and insufficiently vetted code

Decentralization reality (3)

- Mistakes happen, attacks happen
- Mistakes in blockchain currencies and markets are routinely corrected
  - Web3 is going just great
- Attacks on blockchain currencies and markets are routinely corrected
  - Web3 is going just great
- This is less centralized than what can happen in the global DNS, but still has centralization features

Decentralization reality (4)

- Laws happen
- Names are content, some content is banned in some countries, and thus systems that voluntarily and proudly contain those names might be banned as well
  - This has not happened yet (?) to blockchain namespaces, but give it time
- So far, this is less centralized than what is happening in the global DNS, but that is likely due to the much smaller footprint of blockchain naming systems

Decentralization in a DNS namespace

- Start with a real, DNSSEC-signed gTLD
- Require DNSSEC for all SLDs
- Use registrars that allow name privacy
- Create a ledger with lots of people watching it and comparing results
  - Decentralization through active gossip

Relying on watchers and gossip

- There needs to be a mostly-trusted group watching updates to the ledger and comparing them among the group
- Watchers make sure that allocation from the TLD a one-time event that can never change
- Watchers make sure that the TLD zone never has more than one level in it
- If the TLD manager breaks its promises, it will be observed, but what happens next is up to the registrants, just like in blockchain-based name systems

Questions

- ...and comments

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: paul.hoffman@icann.org

@icann

linkedin/company/icann

facebook.com/icannorg

slideshare/icannpresentations

youtube.com/icannnews

soundcloud/icann

flickr.com/icann

instagram.com/icannorg