Challenges with Alternative Name Systems

ICANN Office of the Chief Technology Officer

Alain Durand

OCTO-034
27 April 2022

TABLE OF CONTENTS

This document is part of ICANN’s Office of the Chief Technical Officer (OCTO) document series. Please see the OCTO publication page for a list of documents in the series. If you have questions or suggestions on any of these documents, please send them to octo@icann.org.

Executive Summary

The Domain Name System (DNS) is a component of the system of unique identifiers ICANN helps to coordinate. It is the main naming system for the Internet. It is not the only one. Some naming systems predate the DNS, and others have been recently proposed in the wake of the blockchain approach of decentralized systems.

Proposing a new naming system is one thing. Making sure everybody on the Internet can use it is another. Alternative naming systems face a huge deployment challenge. A number of solutions exist to bridge the DNS to those parallel worlds, but they all come with their own drawbacks.

Furthermore, the lack of name space coordination, either between those alternative naming systems and the DNS, or simply among those alternative naming systems, will result in unworkable name collisions. This could lead to completely separate ecosystems, one for each alternative naming system, which would further fragment the Internet. This is the exact opposite of the vision of “one world, one Internet.”

1 Introduction: Not All Names Are Created Equal

If you are new to the business of domain names, what might you consider when purchasing a name?

A key reason to obtain a brandable domain is that it is easy to remember, pronounce, and spell. We also make assumptions. For example, you might assume that any potential customer anywhere in the world could use the domain name you select to connect with you easily, either by clicking on a link or typing the name into a browser, regardless of which platform the customer is using.

This assumptions holds true when you get a regular DNS domain name. Once the proper DNS records and web servers for that domain name are set up, any user on the Internet can reach you. This is one of the most important advantages of the DNS: domain names can be resolved by anyone, anywhere on the planet, from any platform.

Meanwhile, alternative naming systems have existed for a long while, but have remained marginal. More recently, various blockchains have introduced their own naming systems. Those are often promoted as real alternatives to the DNS.

If you are using a name that is part of such an alternative naming solution, the above assumption no longer holds true. Resolving domain names in an alternative naming system requires a specialized bridge from the DNS world in order for the alternate names to work. What does this mean to the average Internet user? Unless Internet users install specific software or configure certain settings on all of their devices, they will not be able to use these non-DNS names. In this circumstance, an Internet user clicking on a link with an alternate name will see a failure with an error message that the domain cannot be found. Section 3 in this document explores the various techniques that can be used to implement such bridges.

Is there a use case for those alternative naming systems outside of the traditional DNS and what would the interaction with the DNS look like? Section 4 explores this question.

While the governance models of these other systems are varied and do not follow ICANN's multistakeholder model of policy development (and as such do not have the advantage of input from the broader community), it is not a topic that this document seeks to analyze. This document assumes a basic familiarity with the underlying technologies used by those alternative naming systems.

2 A Short Survey of Alternative Naming Systems

There are broadly two kinds of alternative naming systems:

- Those based on the DNS protocol, but using an alternative root
- Those not based on the DNS protocol

As noted throughout this document, there is a large overlap in the issues related to the deployment of either kind of alternative naming systems. What follows is not an exhaustive list of alternative naming systems; rather, it is a list of systems that have either been widely used at some point or are sometimes discussed in technology circles today.

2.1 Alternative DNS Root

People have been experimenting with alternative DNS roots[1] for many years. Alternic[2] was one such effort dating back to 1996, prior to the creation of ICANN. The operation of alternative roots is mostly identical to the operation of the regular DNS; however, the set of top-level domains (TLDs) may or may not be different, and Domain Name System Security Extensions (DNSSEC) may or may not be deployed, using or not using the same cryptography algorithms. ICANN policies do not apply to such systems.

ICANN's perspective on a unique, authoritative root for the DNS can be found in ICP3.[3]

2.2 Historical Non-DNS Based Systems

Non-DNS protocol naming systems have existed for a very long time.

[1] See the following examples for alternative DNS roots, "With Open-root, Open Up the World, Think Big," Open-Root, https://www.open-root.eu/?lang=en,
and "Yeti DNS Project Phase-2: A Live IPv6-only Root DNS Server System Testbed," Yeti DNS Project, https://yeti-dns.org/. (Yeti says it is not providing an alternative name space.)

[2] The Atlernic website, archived at https://web.archive.org/web/19970125144823/http://www.alternic.net/TLDS.html

[3] "ICP-3: A Unique, Authoritative Root for the DNS," https://www.icann.org/resources/pages/unique-authoritative-root-2012-02-25-en.

2.2.1 Host File

Before the DNS even existed, people used a centralized file that listed every host on the Internet. Copies, and copies of copies, were distributed more or less regularly to the various organizations connected to the Internet. This did not scale well. People were updating their local copies without necessarily updating the main sources. As a result, copies were regularly out of sync. This illustrated the difficulties of operating a global system through local control without a strong coordination mechanism.

2.2.2 Organization-level Configuration Systems

Local or organization-level computer configuration systems were commonly deployed in the late 1980's and early 1990's. A good example was Sun Microsystems' NIS/NIS+. Those systems typically included a centralized naming function that worked well within an organization's boundaries, but did not scale to the full Internet. Once organizations' local networks got connected to the Internet, most were replaced by the DNS.

2.3 Current Non DNS-Based Systems

The following is a non-exhaustive, high-level survey of newer alternative naming systems. It should be noted that there is no coordination between the various name spaces of the various alternative naming systems mentioned below.

2.3.1 The Handle System

The Handle System is part of the Digital Object Architecture[4] (DOA). More information about it can be found in the paper, OCTO-002.[5] The DOA has three core components: the identifier/resolution system, the Digital Object Repository system, and the Digital Object Registry system containing metadata about the repository objects. The Handle System is the original name of the identifier/resolution system of the DOA. It poses the same deployment challenges as the other alternative naming systems discussed in this paper.

2.3.2 The Onion System

The Onion system is used by the TOR[6] project. Onion names use the .onion special-use top-level domain defined in RFC7686[7] using a process described in RFC6761 to reserve "special use domain names." As a result, .onion is now included in the IANA Special-Use Domain Name registry.[8]

[4] "Digital Object Interface Protocol SDK For Java," The DONA Foundation, https://www.dona.net.

[5] OCTO-002, "Digital Object Architecture and the Handle System," https://www.icann.org/en/system/files/files/octo-002-14oct19-en.pdf.

[6] "Browse Privately. Explore Freely. Defend yourself against tracking and surveillance. Circumvent censorship.," Tor Project, Inc., https://www.torproject.org.

[7] RFC 7868, "The ".onion" Special-Use Domain Name," https://datatracker.ietf.org/doc/html/rfc7686.

[8] "Special-Use Domain Names," IANA registry, https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xhtml.

2.3.3 Blockchain-based Systems

Several blockchain-based naming systems are in operation, including Namecoin,[9] Ethereum Naming Service[10] (ENS), Unstoppable Domains,[11] and Handshake.[12]

Namecoin is one of the earliest attempts at a blockchain-based naming system. It was an experimental fork of Bitcoin. It uses the .bit TLD. The domain .bit has not been granted the status of "special use domain name" by the Internet Engineering Task Force (IETF).

ENS is based on the Ethereum blockchain technology. It uses the .eth TLD. The IETF has not added .eth to the special use domain name list. As of 28 March 2022, over 800,000[13] domains have reportedly been created on ENS.

Unstoppable Domains is not based directly on Ethereum, it is based on Polygon,[14] an Ethereum scaling platform designed to lower transaction costs. As of 28 March 2022, over 2,100,000[15] domains have reportedly been registered on Unstoppable Domains.

Handshake is using its own coins (HNS) in its own blockchain with code is derived from bcoin,[16] and which is described as an "enterprise-level Bitcoin and Blockchain libraries." As of February 2022, over 3,500,000[17] domains have been reportedly been registered over time in Handshake, and over 115,000 domains are reported to be in use.

While Namecoin and ENS registrations can be considered second-level domains (SLDs) under their respective TLDs, Handshake and Unstoppable Domains registrations are the equivalent of TLDs.

To put this in perspective, ICANN reported over 163,500,000 domains[18] in the .com zone alone in December 2021. As of 19 April 2022, there are 1,591 TLDs listed in the root zone according to the IANA root zone database.[19]

[9] "Supporting Free Speech," namecoin.org, https://www.namecoin.org.
[10] "Decentralized naming for wallets, websites, & more," ENS DAO, https://ens.domains.
[11] "NFT Domains. No Renewal Fees Ever.," Unstoppable Domains, https://unstoppabledomains.com.
[12] "Decentralized naming and certificate authority: An experimental peer-to-peer root naming system," https://handshake.org.
[13] "Dune," Community Discord, https://dune.xyz/makoto/ens.
[14] "Bringing the world to Ethereum," Polygon, https://polygon.technology.
[15] "NFT Domains. No Renewal Fees Ever.," Unstoppable Domains, https://unstoppabledomains.com.
[16] "Enterprise-level Bitcoin and Blockchain libraries. Built for businesses, miners, wallets, and hobbyists," bcoin.io, Purse, https://bcoin.io..
[17] "Handshake Statistics," Namebase, https://www.namebase.io/stats/#usage.
[18] ".com Monthly Registry Reports," https://www.icann.org/resources/pages/com-2014-03-04-en.
[19] "Root Zone Database," https://www.iana.org/domains/root/db.

3 DNS Replacement or Extension

This section addresses what it would take to use those naming systems as a DNS replacement/extension to provide the usual DNS mappings such as domain name to IP address or mail server lookup. It also includes deployment and scalability considerations.

3.1 New Dedicated Applications

Applications can be built to use any of the available libraries[20,21] adapted to the specific naming service you choose. Those libraries are typically available for commonly used programming languages, such as C, Python, Java, and Golang.

Adapting applications to use a single alternative naming system is relatively straightforward. Adapting it to use multiple alternative naming systems is more complicated and particularly if the names overlap. At a minimum, the application would have to know which alternative naming system to look up for any given domain name or define an order in which the lookups are made. The approach to define an order in which to do those lookups has already been tried in the DNS with search lists. Such an approach is considered non-deterministic and thus problematic.[22]

3.2 Various Bridging Techniques

A number of bridging (or transition) techniques exist to enable early adopters to reach names using alternative naming systems. Those listed below describe the main categories of solutions; there might be others. As seen with IPv6, transition techniques are important and necessary in the initial stage of deployment; they act as a bootstrap mechanism. However, they are not meant to be a permanent solution. In particular, they do not alleviate the use of the DNS. Thus, none of the non-DNS alternative naming systems can act as a pure DNS replacement today. If the IPv4 to IPv6 transition is any indication, a transition to replace the DNS could potentially span multiple decades.

3.2.1 Use a Web Gateway

A special website can be set up to bridge to a specific naming system. For example, a guide[23] to access Handshake names mentions the gateway (http://hns.to) as a bridge to Handshake domains. That guide explains that the gateway can be used as http://hsd.to/welcome.nb to reach the welcome.nb Handshake site. At the time of writing this document, the welcome.nb Handshake domain was not reachable this way.

The advantage of using this method is that it does not require any set up on the client side. The drawback is that those web gateways would have to be maintained over time and must scale

[20] For ENS libraries can be found at https://docs.ens.domains/dapp-developer-guide/ens-libraries.

[21] A Handshake C library can be found at https://github.com/handshake-org/libhns.

[22] SAC064, “SSAC Advisory on DNS ‘Search List’ Processing,” https://www.icann.org/en/system/files/files/sac-064-en.pdf.

[23] “Access Handshake names: walkthroughs for building websites on Handshake names,” Namebase, https://learn.namebase.io/starting-from-zero/how-to-access-handshake-sites

with demand. Gateways also are sources of single point of failure and a potential target for malicious actors.

Note: this approach is not new, it was used to bridge to the DOA-handle[24] world. For example, to reach the xxxxx handle, use this URL https://doi.org/xxxxx.

3.2.2 Use a Dedicated Browser

If an application is based on a browser or a browser library, an alternative solution is to use a specific browser that has been compiled to use the naming service of choice. For example, the Opera[25] browser can access ENS domains. The Beacon[26] browser can natively access the Handshake domains. And Unstoppable Domains has developed its own browser[27] based on Chromium.[28] The Brave[29] browser has announced a collaboration with Unstoppable Domains.

3.2.3 Use a Plug-in or Extension to an Existing Browser

Plug-ins, or extensions, can be added to many existing web browsers. For example, the “bob extension”[30] enables access to Handshake domains directly though the Chrome browser search bar. The “Resolve”[31] add-on enables access for the Firefox browser, and the ENS Gateway[32] does the same for ENS in Chrome.

Using such extensions avoids the necessity to modify and recompile web browsers. However, it creates a new dependency on a third-party piece of software that may or may not be regularly updated, and that may or may not have security issues of its own. An example to illustrate this point is a DOA Handle System plug-in that was developed for the Firefox browser several years ago. Unfortunately, it was developed against an API that Firefox has now deprecated, and as a result, it no longer works.[33]

[24] “Digital Object Interface Protocol SDK For Java,” The DONA Foundation, https://www.dona.net.

[25] “Opera Crypto Browser,” Opera, https://www.opera.com/fr/crypto/next.

[26] “Beacon Web Browser,” Impervious Inc., https://impervious.com/beacon.

[27] “The Decentralized Web Is Here,” Unstoppable Domains, https://unstoppabledomains.com/browser.

[28] “The Chromium Projects,” https://www.chromium.org/.

[29] “Unstoppable Domains and Brave to Provide Millions of Users Access to the Decentralized Web,” Brave, 13 May 2021, https://brave.com/unstoppable-domains/.

[30] “Bob Extension,” Chrome web store, Kyokan, LLC., https://chrome.google.com/webstore/detail/bob-extension/ogcmjchbmdichlfelhmceldndgmgpcem.

[31] “Resolve by Codecrafting :Resolve Handshake domains + DNS TXT metadata records. Metadata records support Skynet, redirects, QR codes, and more,” Firefox add-ons page for Resolve, Codecrafting, https://addons.mozilla.org/en-US/firefox/addon/resolvr/?src=search.

[32] “ENS Gateway: .Eth Domain Browser for Ethereum,” Chrome web store, ensgateway.com, https://chrome.google.com/webstore/detail/ens-gateway-eth-domain-br/jkaiofboahfpipgijdgdmbdldlgcipgo?hl=en.

[33] OCTO-002, “Digital Object Architecture and the Handle System,” https://www.icann.org/en/system/files/files/octo-002-14oct19-en.pdf.

3.2.4 3.2.4 Run a Local Resolver that Bridges to the Other World

Instead of modifying every application running on a host, an alternative approach is to let software use the regular DNS but intercept the DNS queries in the host itself. For that, the host needs to run a modified local DNS resolver to bridge the naming system of choice. An example[34] of this can be found for the Handshake system with a container running a modified version of ISC's BIND[35] DNS resolver.

3.2.5 Point to a Recursive Resolver that Acts as the Bridge

The local resolver approach can be generalized. Instead of running one such resolver per host, one could run a centralized resolver implementing such a bridge to the alternative naming system and then ask users to point their stub resolver there. This might be a simpler approach for large managed networks.

As of the date this document was published, there is at least one public DNS resolver advertised as a bridge for Handshake (with the addresses 103.196.38.38, 103.196.38.39 and 103.196.38.40) that appears to work.

3.3 Deployment Considerations

3.3.1 Deployment as a Single User

A tech-savvy user can deploy any of the above solutions for any given alternative naming system on their own device; however, most Internet users would have difficulty deploying most of these solutions.

Furthermore, such configuration may or may not be available for all devices where names are used, such as Internet of Things (IoT) devices. Also worth noting, such configurations become much more complicated when multiple (and possible conflicting) alternative naming systems need bridging. Section 5 of this document explores those specific challenges.

3.3.2 Deployment in a Closed or Controlled Environment

Any of the above solutions can be deployed in a closed environment. It is a tradeoff between modifying and deploying applications versus managing the configuration of existing devices.

[34] "Handshake-Resolver," Github, https://github.com/james-stevens/handshake-resolver.

[35] "BIND 9: Versatile, classic, complete name server software," Internet Systems Consortium, https://www.isc.org/bind/.

If special purpose applications are being built, embedding a library to the chosen name systems might be the easiest solution. If a large number of regular Internet applications need to be modified, using a URL bridge or a modified recursive resolver might be easier.

In any case, a certain level of expertise is required to deploy any of the above solutions. That expertise must be maintained for the whole lifetime of the chosen alternative naming system.

3.3.3 Deployment on the Internet

Deploying any of the solutions at the device level, as described in section 3.2, is a tall order for a typical Internet user. Most users do not change any of the settings on their devices. A recent ICANN study showed that less than 5% of European Union (EU) consumers of large ISPs were using a public resolver.[36]

Using a URL gateway is an easy-to-deploy solution. However, if the stated goal of the alternative naming system is to replace the DNS, using a URL gateway will not accomplish that goal. More importantly, gateways need to scale with traffic and can become single points of failure or targets of security attacks.

That leaves two avenues to explore: a) specific devices or specific applications that embed code to use the alternative naming solutions or b) relying on large DNS resolvers to do the bridging.

The deployment of specific devices or specific applications is a possibility; however, the fact that only one alternative naming system can be active at a time and the uncertainty as to which one will actually get traction frustrates any significant changes and fragments the Internet: while some people will adopt new systems, the majority of people will wait to see which naming system is the best or most widely accepted.

Public DNS resolvers (or large ISP DNS resolvers) acting as a bridge to alternative naming systems for the benefit of large portions of the Internet would create additional problems. First, not all DNS resolvers will choose to bridge to the same alternative naming system. Second, there might be domain name conflicts between those alternative naming systems, which is discussed further in Section 5. And third, name resolution for those alternative domain names may work in some places but not in others. For example, resolution may work in one public Wi-Fi hotspot but not in another. Worse, a single device configured to use multiple ISPs (e.g., home Wi-Fi and cellular), some providing the bridging, some not, may experience unpredictable failure modes leading to end-user confusion and costly support calls.

We can possibly draw some lessons from deployment of the DOA Handle System over the last decades. Many of the solutions described in section 3.2 have been tried, such as URL bridges, browser plug-in, and relays. Two approaches are still in use today. Native applications compiled with specific libraries are used in controlled environments. URL proxies are also used on the wider Internet. It should be noted that the relatively slow adoption of DOA has not stressed the scalability issues of the URL gateways.

[36] OCTO-032, “DNS Resolvers Used in the EU,” https://www.icann.org/en/system/files/files/octo-032-01mar22-en.pdf.

3.3.4 3.3.4 Concerns about the Plurality of Alternative Naming Systems

A critical deployment issue derives from the plurality of alternative naming systems.

All of the solutions described above work for a single alternative naming system. When a plurality of them is deployed over the Internet, the same number of bridges must be built. This creates an additional challenge, as now a user must know which alternative naming system the domain is registered with to select the correct bridge to reach it.

For example, if purpose-built browsers are used, they can only bridge to one alternative naming system at a time. Some might only bridge to ENS, some to Unstoppable Domains, and some to Handshake. This means a user would have to switch browsers (or at least change the browser configuration) when hopping from a name registered in one system to another name registered elsewhere. It also means that the user must somehow know which name system a particular name they are using is associated with.

An additional deployment concern related to the plurality of alternative domain systems is name collision. This concern is further analyzed in section 5.

4 Non-DNS Use of Naming System

Is there a use case for alternative naming systems outside of acting as a replacement of the traditional functions of the DNS such as name to IP address mapping or mail relay lookup?

4.1 Handle System

Although the Handle System could be used to replace the DNS, the most common use of DOA is to access directories of digital objects that have nothing to do with the DNS.

Outside of applications developed specifically to use the Handle System, the URL bridge is the most commonly deployed solution to interface with the Handle System.

4.2 Blockchain-based Naming Systems

Blockchain elements are referred to by a long hexadecimal string. Just like IPv6 addresses, those are hard to remember. Creating human-friendly names that resolve to those strings was deemed an important step for the early adoption of blockchain technologies. Early blockchain developers did not develop DNS extensions for that purpose. They created entirely new alternative naming systems based on the particular blockchain they were working on. The following two sections will highlight some current use cases for those alternative naming systems.

4.2.1 Naming Blockchain-related Elements

Blockchain-based naming systems are often used to name wallets[37,38] and other objects stored in blockchains, such as non-fungible tokens[39] (NFTs).

4.2.2 Naming Objects in "Web3"

Web2 (or Web 2.0) is the web as it is known today. Web3[40] is an idea to make the web completely decentralized, building it on a set of tools like blockchain, blockchain-based naming systems, and a distributed storage solution such as the Interplanetary File System[41] (IPFS), a peer-to-peer hypermedia protocol.

Opinions vary[42] as to whether or not a fully decentralized system is economically viable at a very large scale: over the last few decades, centralization has shoen to be a tool providing very significant economies of scale. For example, it is much less expensive to run an application on a virtual machine (centralized) than on a dedicated piece of hardware (decentralized) in the same datacenter. Similarly, centralizing around cloud solutions has brought reduction in both hardware and software purchases (CAPEX) and operational cost (OPEX).

5 Blockchains and DNS: Collision or Integration?

The ICANN Name Collision Analysis Project[43] (NCAP) has created a definition for a name collision:[44] "Name collision refers to the situation where a name that is defined and used in one namespace also appears in another. Users and applications intending to use a name in one namespace may attempt to use it in a different one, and unexpected behavior may result where the intended use of the name is not the same in both namespaces. The circumstances that lead to a name collision could be accidental or malicious."

The indiscriminate and uncoordinated introduction of new namespaces without a careful review from the larger community may be a cause of ongoing and unavoidable name collisions, making the Internet less stable and less secure.

[37] "Blockchain Wallet," *Investopedia,* 13 January 2022, https://www.investopedia.com/terms/b/blockchain-wallet.asp.

[38] "Decentralised naming for wallets, websites, & more.," ENS DAO, https://ens.domains.

[39] "Non-fungible tokens (NFT)," ethereum.org, https://ethereum.org/en/nft/.

[40] Sam Richards, "WEB2 VS WEB3," Ethereum Docs page, ethereum.org, https://ethereum.org/en/developers/docs/web2-vs-web3/.

[41] "IPFS powers the Distributed Web: A peer-to-peer hypermedia protocol designed to preserve and grow humanity's knowledge by making the web upgradeable, resilient, and more open," InterPlanetary File System, https://ipfs.io.

[42] "My first impressions of web3," moxie.org, https://moxie.org/2022/01/07/web3-first-impressions.html.

[43] Name Collision Analyst Project (NCAP), Mailing list archives, NCAP group page, https://community.icann.org/display/NCAP/NCAP+Discussion+Group.

[44] "Managing the Risks of Top-Level Domain Name Collisions Findings for the Name Collision Analysis Project (NCAP) Study 1," https://www.icann.org/en/system/files/files/ncap-study-1-report-19jun20-en.pdf.

5.1 Name Collisions Between Multiple Blockchains

As seen in section 2.3.3, at least four blockchain-based naming systems are competing today. As a result, when developing an application, one must decide which blockchain-based naming system to use. As there is no namespace coordination mechanism between those alternative naming systems, name collisions must be expected. As such, supporting multiple alternative naming systems within a single application can lead to unpredictable results. Note: this issue is related to the DNS search list issue analyzed in SAC064.[45]

Some may view this absence of alternative name space coordination as an opportunity: if a name is not available in one of the naming systems, just look in another one! This is true on the registration side, yet there is a cost: the domain can only be reliably reached by the client-side applications specifically developed to support this naming system and no others. Users of client-side applications potentially supporting multiple naming systems would first have to be aware of this multiplicity. Then, they would have to specifically instruct the application to use this particular naming system to reach that specific domain. That setting might need to be changed to reach another domain. Similar issues happen on server-side applications, when client-side applications pass names that are only valid in an alternative namespace unsupported by the server. Those issues get compounded when using peer-to-peer applications.

In practice, supporting multiple uncoordinated namespaces is a very tall order, and the end result might very possibly be completely separate ecosystems, one for each naming system.

5.2 Name Collisions Between a Blockchain-based Naming System and the DNS

Handshake[46] and ENS[47] each have policies to reserve some DNS domains. These initial unilateral reservations should not be confused with any ongoing coordination effort between those blockchain-based naming systems and the DNS. As a result, name collisions with the DNS will necessarily occur.

A naïve view would be to consider that this is not an issue because it is unlikely that those alternative naming systems would be used to perform normal DNS-type resolution. However, applications using those alternative naming systems (for example to resolve blockchain wallet names or NFTs) also use the DNS for their Internet name resolution. It is therefore likely that software defects and misconfigurations will result in names leaking from one system to another, leading to further name collisions and unexpected behaviors.

[45] SAC064, "SSAC Advisory on DNS 'Search List' Processing," https://www.icann.org/en/system/files/files/sac-064-en.pdf.

[46] "Handshake Whitepaper," Namebase, https://www.namebase.io/handshake-whitepaper.

[47] "Announcing the ENS 3–6 Character .Eth Name Reservation Process," "https://medium.com/the-ethereum-name-service/announcing-the-ens-3-6-character-eth-name-reservation-process-7f3cc4d13f65.

5.3 Using DNS as a Naming System for Blockchain Elements

DNS solutions, based on a new[48] DNS resource record (RR) type or a specific use of the URI RR type[49] for Distributed Identifiers (DID), have been proposed to store arbitrary objects. Those solutions could be applied to associate DNS names to wallets, NFTs, and other blockchain objects. As such, a blockchain-based naming system is not necessary to name blockchain-based objects.

DNS-based solutions could be augmented to include a scoping parameter, essentially creating a layer of indirection pointing a DNS domain to a blockchain-based domain while also specifying which blockchain is to be consulted.

6 Conclusion

Even though alternative naming systems can be deployed in controlled, managed environments, deploying them on the Internet at large faces serious challenges.

As we have seen over three decades of IPv6 deployment, transition mechanisms are useful for early adopters, but do not seem to be a viable long-term approach. Similarly, alternative naming system bridging solutions cannot be expected to work flawlessly. Requiring user intervention to install or configure anything is typically a non-starter. Asking resolver operators to bridge the DNS to those alternative naming systems can lead to unpredictable results, user frustration, rising support costs, and in the end, a less secure and stable Internet.

Furthermore, the use of specially built applications to work with alternative naming systems poses significant risks. As seen in Section 5, the creation of new namespaces without any coordination (either among themselves nor with the DNS) will necessarily lead to name collisions, unexpected behaviors, and user frustration. The end result might very well be completely separate ecosystems, one for each naming system, further fragmenting the Internet. It is worth remembering that the vision of a single Internet necessitates a unique system of identifiers, in other words a unique namespace, as discussed in ICP3.[50]

7 Acknowledgment

The author would like to acknowledge the contributions of Paul Muchene and David Huberman from ICANN's Office of the Chief Technology Officer.

[48] "The Decentralized Identifier (DID) in the DNS," draft-mayrhofer-did-dns-05, https://datatracker.ietf.org/doc/html/draft-mayrhofer-did-dns-05.

[49] RFC 7553, "The Uniform Resource Identifier (URI) DNS Resource Record," https://datatracker.ietf.org/doc/html/rfc7553.

[50] "ICP-3: A Unique, Authoritative Root for the DNS," https://www.icann.org/resources/pages/unique-authoritative-root-2012-02-25-en.