Introduction to Blockchain Name System Technologies

ICANN Office of the Chief Technology Officer

Paul Hoffman
OCTO-039
17 October 2024

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.

This document supports ICANN's strategic goal to improve the assessment of, and responsiveness to, new technologies that impact the security, stability, and resiliency of the Internet's unique identifier systems through greater engagement with relevant parties. It is part of ICANN's strategic objective to evolve the unique identifier systems in coordination and collaboration with relevant parties to continue to serve the needs of the global Internet user base.

1 Introduction

This document explains the technologies for many of the blockchain name systems currently proposed in the blockchain ecosystem. The primary purpose of this document is to help the ICANN community understand current and proposed blockchain name systems. It is primarily written for people familiar with the Domain Name System (DNS), interested in modern alternative name systems, and who have already read OCTO-040, "Introduction to Blockchain Technologies," which describes many of the foundational ideas covered in this document.

The technologies described here are based on what is known about recent and current blockchain name systems. This document does not state which technical features are used by specific blockchain name systems because those systems change features over time. Thus, the technologies described are general, and only by investigating specific systems can you determine which systems use which technologies.

The terminology used in this document often does not match the terminology used in the blockchain ecosystem. "Introduction to Blockchain Technologies" defines blockchain-specific terminology. When that document uses terms different than are common in the blockchain ecosystems, it lists the similar terms from that ecosystem. DNS-specific terminology is defined in RFC 9499, "DNS Terminology."

This is the first published version of this document. The author expects to publish a second version approximately six months after the first, to include corrections and additions that were received after the first version was published. This second edition will likely be longer, but will contain the same neutral tone. Please send all comments and questions about this document to octo@icann.org.

2 Features of Blockchain Name Systems

A blockchain name system is a name system that has some visible similarities to the global DNS but that is somehow associated with a blockchain. Some existing and proposed features for various blockchain name systems are:

- Resolution of names in the blockchain name system returns an account identifier or other data that is related to blockchains.
- Activities associated with a name in the blockchain name system are permanently stored on the blockchain so that people can always view the entire history of the name.
- Purchase and update of names in the blockchain name system are paid for by blockchain coins instead of traditional currency.
- Alternative top-level domains (called *alt-tlds* in this document) in blockchain name systems can be strings that are not delegated as top-level domains (TLDs) in the global DNS.
- Blockchain name systems can coordinate with the global DNS by using alt-tlds that match the TLDs that are already delegated in the global DNS.

Each of these features are described in more detail below.

Many blockchain name systems have ideas in common with the global DNS. Two of the most important ones are listed here.

2.1 Resolution

Resolution from the client's perspective means sending a request that contains a name and a desired type of data, and receiving an answer for that name that has the requested type of data (or receiving an error). A system that offers name resolution is called a *resolver*. From the resolver's perspective, resolution means receiving a request that contains a name and a desired type of data, and returning an answer for that name that has the requested type of data, or returning an error. Types of errors typical for resolvers to return include "that name does not exist", "that name exists but there is no data of that type associated with the name", "you are not allowed to ask this resolver for that information", "something bad happened as I was trying to return data", and so on.

In the global DNS, requests and responses use the DNS protocol. Resolution in blockchain name systems is not standardized. For many blockchain name systems, there are web APIs (application programming interfaces) and systems that serve data from a copy of the blockchain's database. For others, there are bespoke protocols for querying the databases. Blockchain name systems often have browser plugins for users who want to resolve names directly from their browser.

2.2 Display Format for Names

Because of the ubiquity of the global DNS, people are most familiar with domain names looking like "www.example.com," where the highest level of the name hierarchy is the last label, and the labels are separated by periods. Blockchain name systems can choose how to display their names, although typically they choose to display them in the same way as they are in the global DNS. Some blockchains, in order to not conflict with the global DNS, use a different character (such as "$") between the labels.

3 Resolution to Account Identifiers

The most common resolution query in the global DNS is for the Internet Protocol (IP) address data types. There are dozens of other variations of data types that can be associated with a domain name in the global DNS.

In blockchain name systems, the most common result of resolution is a single account identifier (often called a "wallet address" in the blockchain ecosystem). The limit to one identifier originally came from the idea that a blockchain name was associated with a single blockchain account. Some blockchain name systems allow retrieving multiple account identifiers (in some cases, from multiple blockchains) with resolution using nondefault queries.

The WALLET RR type (resource record type) was added to the global DNS in 2024, and some resolver and authoritative software have already adopted this new data type. The registration for the WALLET RR type is shown in the IANA DNS parameters registry, and the type description itself describes how it appears both on the wire and in applications in the global DNS.

Some blockchain name systems have additional data types that are not yet supported by the global DNS. For example, some have data types that hold pointers to documents on the InterPlanetary File System (IPFS), avatars (drawings that represent the account holder), and so on. These types of data might be supported in the future in the global DNS; the process for adding new RR types is described in RFC 6895, "DNS IANA Considerations."

4 Permanent Ledger of Name Activities

A distributed public ledger can keep track of business transactions to help others track changes in ownership of assets such as domain names. Additionally, the ledger can track all visible public changes to the asset. Blockchains are currently the most prominent type of public ledger, but almost any type of trusted public ledger can be used for this type of publication. The ledger needs to support all the relevant types of transactions supported by the name system being tracked.

In the global DNS, delegation information (currently NS records) is published by registries, while registration metadata (such as ownership and contact information) is published by many entities. In generic TLDs and some ccTLDs (country code TLDs), publication responsibility is shared between registries and registrars. In other ccTLDs and infrastructure TLDs such as .arpa, delegation information and registration metadata is controlled by the registries. There are a variety of existing blockchain name systems, and they have different ownership and control systems for their names.

You do not need a blockchain in order to have a distributed public ledger for a name system. Existing blockchains can certainly be used for name system data, but they are not a requirement. Name system data does not need to be in blocks: it can be added one transaction at a time. Nor does that data need interesting rules or programs for the ledger's state machine because a data ledger only needs to keep two tables (the history of transactions and the current value for the processed data).

Choosing a trust model for a public ledger depends on many possibly conflicting factors. The data originates with the registrant, so maybe only the registrant might be trusted to create transactions for the ledger. In much of the global DNS, the registrant always interacts with a registrar who checks the validity of some of the data, so the registrar might be a better creator of transactions. Global DNS registries, and the operators of blockchain name systems, operate and manage the servers that resolvers request some of the data from, and are thus maybe more reliable creators of these transactions.

Further, the parties relying on the ledger would want the ledger to be maintained for the long term. The trust model for them would include who will keep the ledger alive, active, and accurate. Different organizations have very different track records for maintaining such data sources.

5 Payment by Blockchain Coins

In the global DNS, activities like registering a new name and renewing a registration are often paid for using standard national or regional currencies. Many activities, such as updating data

records for existing names or changing contact information, are typically free. Some TLD registries in the global DNS do not require any payments at all for registration.

Different blockchain name systems have different ways to pay for the activities related to name creation and maintenance. Some require payment in a particular blockchain coin, some allow payment by a variety of blockchain coins, and some allow payment by national or regional currencies. Payment by blockchain coins that are mostly anonymous are similar to cash payments in non-blockchain coins.

6 Use of TLDs That Are Not Delegated

Because they are not part of the global DNS, blockchain name systems are able to choose any names they want, without asking the permission of any other organization. ICP-3, “A Unique, Authoritative Root for the DNS,” describes why this is so. "These alternate roots typically substitute insular concerns in place of the community-based processes that govern the management of the authoritative root. Their operators decide to include particular top-level domains in these alternate roots that have not been subjected to the tests of community support and conformance with consensus processes – coordinated by ICANN – that would allow their inclusion in the authoritative root. These decisions of the alternate-root operators have been made without any apparent regard for the fundamental public-interest concern of Internet stability. The widespread use of active domain names in these alternate roots could in fact impair the uniqueness of the authoritative name-resolution mechanism and hence the stability of the DNS."

In this document, those names are called alt-tlds, but different blockchain name systems use a variety of synonyms, such as “top-level labels” or “names” or, confusingly, “TLDs.” Some blockchain name systems choose alt-tlds that are not delegated in the global DNS, even though these names may appear as TLDs in the global DNS in the future. Resolution of names in these alt-tlds can work if the chosen names are not yet in the global DNS, if the chosen alt-tld is unique among blockchain name systems, and if the user can determine where to send resolution requests.

There are already many different blockchain name systems, and more will possibly be created in the future. Each blockchain name system can choose which alt-tlds they want to use, which means that multiple blockchain name systems can use the same alt-tld names. The result is that users don’t know which resolvers to use for names that appear in multiple blockchain name systems. Further, multiple blockchain name systems using the same alt-tlds might have different sets of second-level domains (SLDs), so a user might need to query multiple resolvers to find all the possibilities for a particular name. There are some informal agreements between some of the blockchain name systems to not use the same alt-tlds, but those agreements are nonbinding and they are not universal.

There is no agreement among the blockchain name systems about what to do when the alt-tlds they are using appear in the global DNS. This will present technical challenges to users similar to multiple blockchain name systems using the same alt-tlds. The order that a user queries resolvers will have a significant effect on the answers they receive to queries.

Names under TLDs that are not delegated in the global DNS require a different form of resolution than the one already used by everyone using today’s Internet. Different blockchain

name systems use different resolution technologies. Many use web APIs that connect to a centralized database with the data associated with each of the names. Others use bespoke protocols for those connections.

Some blockchain name systems use DNS resolvers that have been modified to also answer queries that are outside the DNS, such as those for names under alt-tlds. In the latter case, those resolvers of course cannot use Domain Name System Security Extensions (DNSSEC) to validate the data before responding to queries because the names based on alt-tlds cannot have DNSSEC signatures that chain to the global DNS's root zone's trust anchor. Instead, the resolver responds to those queries without the Authentic Data (AD) bit set, and users must check for the AD bit when making queries.

7 Coordinated Functionality with the Global DNS

As described above, because they are not part of the global DNS, blockchain name systems are able to choose any names they want, without asking permission of any other organization, including choosing TLDs that are in the global DNS. If a blockchain name system uses alt-tlds that are in use in the global DNS, these name systems can have data related to the names that is the same or different from the data in the global DNS. Having data that is the same causes some problems (such as coordination between the two systems), and having data that is different causes other problems (such as needing to do multiple resolutions to find the desired data).

Some blockchain name systems that also use alt-tlds corresponding to TLDs in use in the global DNS state that they are fully coordinated with the DNS: all data that appears in the blockchain portion of the system is identical to the data that appears in the DNS. This duplication can only be done if the operator of the blockchain name system is also the party hosting the registrant's DNS data, which means that the registrant is not in full control of their name.

Other such blockchain name systems keep some of the data (such as the associated cryptocurrency account identifiers) only in the blockchain portion of the system. These systems can cause technical problems for users because they need to resolve names using multiple resolvers, or to choose a particular resolver that is trustworthy to combine data from all the name systems (but without DNSSEC protection for data in the blockchain portion of the system).

Having different data in each portion of the system can cause problems if the names in the two parts are not controlled by the same entity. For example, if one person owns a domain name in the global DNS and a different person owns that same name in a blockchain name system, there is no logical tie between the data that you get from resolving in the different systems.

There is another significant problem with coordinating a name in a blockchain name system and the global DNS: the names often have different mechanisms for creation, deletion, and transfer. The rules for ownership of a name might be different, so even if a name in the two systems is initially controlled by the same person, that might change during the lifecycle of the name. Another example is that an owner of a name in the global DNS might want to transfer ownership

of that name to someone who is not participating in the blockchain name system, and control of the name becomes divided.

Appendix A Further Reading

OCTO-040, “Introduction to Blockchain Technologies”

RFC 9499, “DNS Terminology”

RFC 6895, “DNS IANA Considerations”

A.1 Documentation for Some Well-Known Blockchain Name Systems

ENS documentation

Unstoppable Domains documentation

Namecoin documentation

Handshake documentation

GNU Name System documentation