

Strategies For Combating Unauthorized Blockchain Name Use

By **Andrea Calvaruso and Matthew Luzadder** (March 16, 2022, 3:43 PM EDT)

Just when you thought you had a handle on domain name enforcement for your clients, blockchain technology has given rise to new domain names, which bring novel and complex challenges.

There are currently millions of blockchain domain names, with extensions such as .crypto and .eth. Some mimic brand or celebrity names and are being offered for sale for the cryptocurrency equivalent of \$100,000 and much more.

Basic Background Regarding Blockchain Domain Names

What is a blockchain domain name?

A blockchain domain name is similar to a traditional domain name in some ways, but there are significant differences. Unlike a traditional domain name — like www.kelleydrye.com — that is linked to the corresponding website internet protocol address by a domain name system server, a blockchain domain name — like kelleydrye.eth — links to an address on a blockchain via a nonfungible token provided by a blockchain domain name service.

The blockchain address linked to the blockchain domain name is not a website IP address, but a specific crypto wallet that may store crypto and NFTs. The owner of the crypto wallet linked to the blockchain domain name may take additional steps to point the blockchain domain name to a website.

A blockchain domain name service creates NFTs to link blockchain domains to a blockchain address because the text string kelleydrye.eth is not recognized by a blockchain. Blockchain identifiers are a long string of alphanumeric characters — such as `0x9b8c19500a8631c1f755bb365bDE398384E4f2Fa` — that are not as user-friendly as a domain name.

Currently, the two most prolific blockchain domain naming services are Unstoppable Domains, offering domains like .crypto, .nft, .bitcoin, and Ethereum Name Service offering .eth domains.[1]

From an enforcement perspective, one critical difference between traditional domain names and blockchain domain names is that blockchain domain names are outside of the Internet Corporation for Assigned Names and Numbers, or ICANN, traditional DNS system.



Andrea Calvaruso



Matthew Luzadder

Therefore, these domain names are not subject to any DNS-related rules that are in place to protect brand owners, such as ICANN's Uniform Domain-Name Dispute-Resolution Policy or other dispute resolution proceedings, and requirements regarding the maintenance of accurate domain ownership information.

Another critical aspect of blockchain domain names is that the naming entity that distributes the domain does not retain the ability to transfer ownership or control of the domain after the initial sale.

How are blockchain domain names used?

At the moment, there appear to be three main uses for blockchain domain names.

First, blockchain domain names may be used as an alias or nickname for a crypto wallet address to allow transfer of cryptocurrency without use of the entire unwieldy string of alphanumeric characters that constitutes a crypto wallet address. For example, Kelley Drye might simply ask a client to pay kelleydrye.eth instead of listing the crypto wallet address.

Second, blockchain domain names may be used as a universal username for applications that allow for log-ins via a crypto address, such as the way someone may use their email address as a username across different internet platforms.

Third, blockchain domain names may be used as an address for websites. We expect that they will be typically used to connect to websites on a decentralized internet system, where website files are loaded onto a peer-to-peer network for storing and sharing data in a distributed file system.

The chief feature of a decentralized network is that a website cannot be censored or regulated. While this is big benefit for the advancement of freedom of expression in many places, it is also attractive to those seeking to infringe intellectual property.

Enforcement Is Difficult

Given the anonymous, decentralized and unregulated nature of the blockchain community, there are currently few remedies available to stop third parties from owning and using blockchain domain names that reflect another party's trademarks or names.

First, no blockchain domain naming companies currently offer a way for rights owners to object to third-party registration or ownership of infringing blockchain domains. In other words, once a domain naming service has distributed a blockchain domain name to a third party, a rights owner has no recourse to complain to the naming service.

As noted above, these organizations are not governed by ICANN and do not provide for any dispute resolution proceedings.

Some domain naming companies have taken steps to reserve domain names that include names and marks that the organizations have deemed to be well known.

For example, Unstoppable Domains has reserved domain names reflecting words it deems to be "closely associated with well known entities, products, or individuals," according to its protected brands policy,

so that the rightful owner may purchase the domain name itself. This sunrise period has been extended indefinitely.

Similarly, Handshake has reserved for purchase by brand owners the top 100,000 Alexa-ranked websites. In addition, Handshake has offered limited time sunrise periods where trademark owners may pre-reserve certain domain names that are not on this Alexa-ranked list.

Unfortunately, these systems are dependent upon the name services' own determination of which words warrant protection. So far, there appears to be no method via which a rights owner may request that its name or mark be protected from use in a blockchain domain name via a reserved list or otherwise.

While a rights owner may attempt to be the first to mint and purchase blockchain domain names that reflect its marks or names, it would be costly and virtually impossible to register all such domains and related variations — for example, kelleydrye.eth, kelleydryelaw.eth, etc.

Second, there are many obstacles to bringing a lawsuit to prevent unauthorized ownership or use of blockchain domain names. Anonymity is a big feature of blockchain communities, so it is often impossible to ascertain the identity of a blockchain domain name owner. This presents obvious challenges in determining the proper party, jurisdiction and venue with respect to anti-cybersquatting, infringement or other legal claims.

Legal options to compel an exchange to produce ownership information are limited and costly, particularly because many of these organizations are decentralized entities or not located in the U.S.

In addition, due to the nature of blockchain technology and the ability to hide an individual's identity online, the exchange or marketplace may not even have useful information regarding the ownership of blockchain domain names.

Finally, forensic investigations that attempt to track the identity of a blockchain domain owner from blockchain wallet information and other online activity can be prohibitively expensive, with no guarantee that the investigation will ultimately identify the owner.

The Lanham Act's Anti-Cybersquatting Consumer Protection Act, or ACCPA, provides in rem jurisdiction over domain names themselves in certain circumstances where there is no personal jurisdiction over the defendant who owns the domain name.[2]

However, this is only possible in judicial districts where the registrar or other domain name registry or authority that issued the domain name is located. To the extent that there is an identifiable legal entity associated with blockchain naming companies, most are not located in the U.S. and do not utilize centrally located servers that might give rise to location in one place.

Perhaps more importantly, even if one successfully obtained a court order directing that an infringing blockchain domain be assigned to the genuine rights owner, the major blockchain domain name distributors apparently are not able to transfer ownership of a blockchain domain after the initial distribution.

Currently, there is not a mechanism in place within the blockchain domain protocols to force an owner of a blockchain domain name to transfer ownership of the domain name.

However, practitioners may consider bringing an in rem action under the ACCPA and request that a court order a blockchain naming service like Unstoppable Domains to disable a link from an infringing domain name to a blockchain or burn the NFT,^[3] which would effectively disable the functionality of the domain name.^[4]

Alternative Enforcement Strategies for Practitioners to Consider

Given the limited and costly options currently available to force the assignment or disabling of an infringing blockchain domain name, attorneys should consider alternative strategies for their clients directed at minimizing consumer confusion and devaluing infringing blockchain domain names.

First, utilizing takedown procedures offered by certain NFT marketplaces should be considered to stop the sale of infringing blockchain domain names.

As with traditional cybersquatting, it would appear that the vast majority of unauthorized blockchain domain names containing third-party trademarks or names were minted and purchased for investment purposes — because the owner speculates that some future use or sale of the blockchain domain name will prove valuable.

Many of the major NFT marketplace platforms such as OpenSea, Rarible and Nifty Gateway offer takedown procedures to remove items from the marketplace. These marketplaces are not the exclusive method of selling NFTs, but do provide access to the largest market of potential buyers.

While these takedown procedures will not result in an assignment of ownership of the infringing domain, removing the infringing domain names from sale on these major platforms may serve to drive down the resale value.

Second, practitioners should advise their clients to consider purchasing blockchain domain names that reflect their primary marks or names. As noted above, some naming services have reserved the use of certain words they have determined to be well-known for purchase by a rightful owner, at least for a limited time.

Third, the public should be informed via media campaigns about any official blockchain domain names associated with the client's brand and/or warned against any blockchain domain names that are not associated with the rights owner. This public outreach will help guard against consumer confusion and deception and will also help to devalue the infringing blockchain domain name.

Finally, while the decentralized nature of blockchain communities makes it difficult to implement effective laws and regulations, practitioners may suggest that their clients consider combining resources and lobbying governments and other stakeholders in the internet and blockchain communities to advocate for the creation of protections for brand owners in the blockchain domain name environment.

The potential threat of restricting certain blockchain activity, together with the desire within the blockchain communities to gain legitimacy in the marketplace, might influence blockchain community stakeholders.

KelleyDrye senior associate Kerianne Losier and special counsel Constantine Koutsoubas contributed to this article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] An entity named Handshake is also a leading blockchain-based domain naming system, which attempts to decentralize the DNS by enabling users to register and operate their own top level domains on the Handshake blockchain. For example, rather than distributing the domain name "kelleydrye.eth" such as ENS, Handshake distributes a top level domain that is to the right of the dot such as .kelleydrye.

[2] The ACCPA provides a safe harbor from liability for domain name registrars which will apply in most cases. See 15 U.S.C.A. § 1114(2)(D).

[3] "Burning" an NFT involves transferring ownership of the NFT to a null crypto wallet, so that it is no longer transferable or usable. The ability to burn an NFT without the NFT owner's consent will depend on the particular smart contract underlying the NFT.

[4] This would arguably amount to a cancellation or forfeiture of a domain name permissible under 15 U.S.C. § 1125(d)(2)(D)(i). ("The remedies in an in rem action under this paragraph shall be limited to lose a court order for the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark.").