



# Understanding the Collision Risk: Where Blockchain Identifiers Meet the DNS

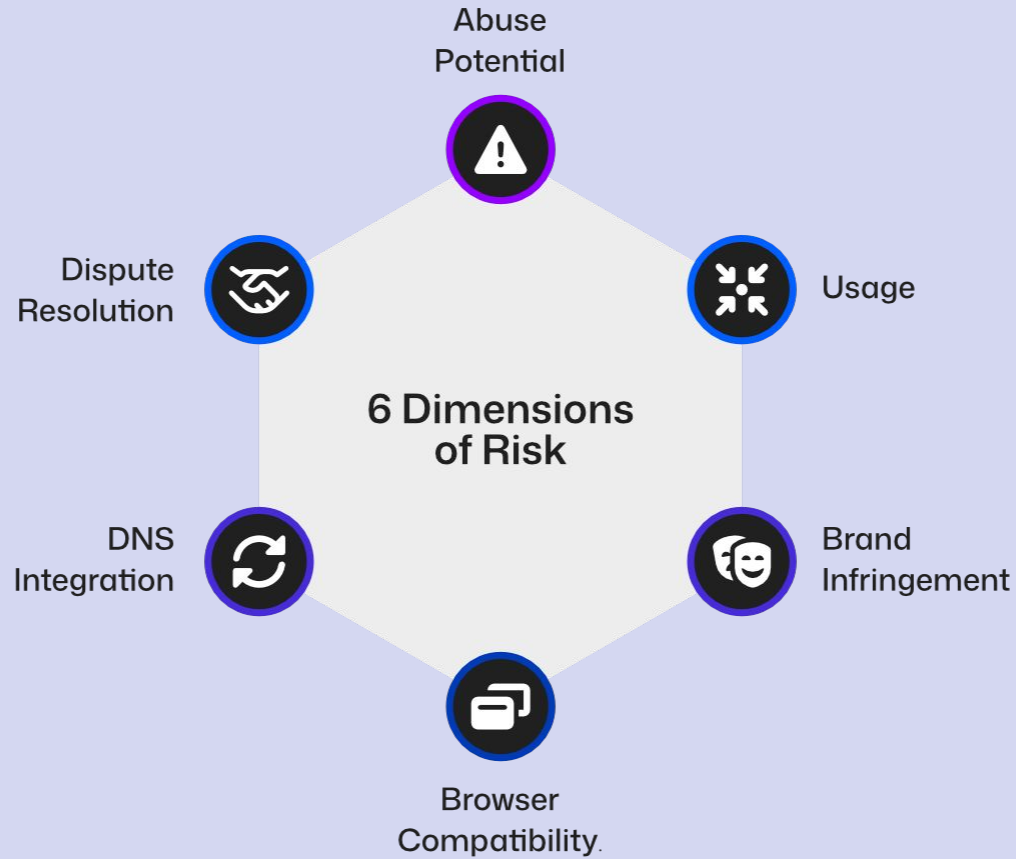
Nathan Alan, Director of Engineering

# Previous Blockchain Research

1. Blockchain and DNS Collisions
2. Blockchain Provider Mapping
3. Risk Analysis

# Risk Analysis Research

- **Not all identifiers pose equal risk** – parked or wallet-mapped domains are less concerning, while active, DNS-like domains carry greater collision potential.
- A **risk assessment framework** was developed to evaluate how these identifiers impact DNS.
- The dataset included **11.3M records** from major blockchain naming providers, focusing on **6.4M second-level records**.
- Threat intelligence used in research from **Global Signal Exchange**.



# Abuse Potential

- Compared 6.4 million blockchain identifiers against Global Signal Exchange (GSE) threat data to assess overlaps with known malicious domains.
- **10.5%** of blockchain identifiers matched domains flagged for abuse, linking them to phishing, malware, or similar threats.
- Over **670,000** identifiers showed confirmed or predictive matches, indicating a notable overlap with malicious DNS activity.



**Abuse  
Potential**

# Brand Infringement

- Around 1% (66,718) contained brand references – mostly keyword matches, some look-alikes, and 207 exact matches.
- Most frequently targeted brands included Audi, Ford, Apple, Tesla, Amazon, and Nike.
- Some providers mitigate this by blocking known trademarks, though anonymity of wallet ownership means even exact matches may not clearly indicate legitimate brand control.



**Brand  
Infringement**

# Dispute Resolution

- Unlike the DNS, blockchain domains lack a unified dispute-resolution process like the UDRP, leaving trademark holders with few remedies for infringement.
- Identified **1,456 blockchain identifiers matching domains previously transferred** through successful UDRP cases in the DNS (e.g., *huaweipay.eth* mirroring *huaweipay.com*).
- Brands most affected by overlapping UDRP cases included Google, Amazon, Lego, Instagram, SAP, Disney, Gucci, Facebook, Ford, and Nike.



**Dispute  
Resolution**

# DNS Integration

- Only 13% of blockchain providers offer native browser support (via Brave or Opera); most rely on extensions, gateways, or custom resolvers for access.
- DNS **integration exists but is inconsistent** – ranging from DNSSEC linking and Cloudflare mapping to self-hosted resolvers and redirect-based gateways that fall short of true DNS interoperability.



**DNS  
Integration**

# Why it Matters

## Understanding the Collision Risks: Where Blockchain Identifiers Meet Domain Names



Carolina Caeiro

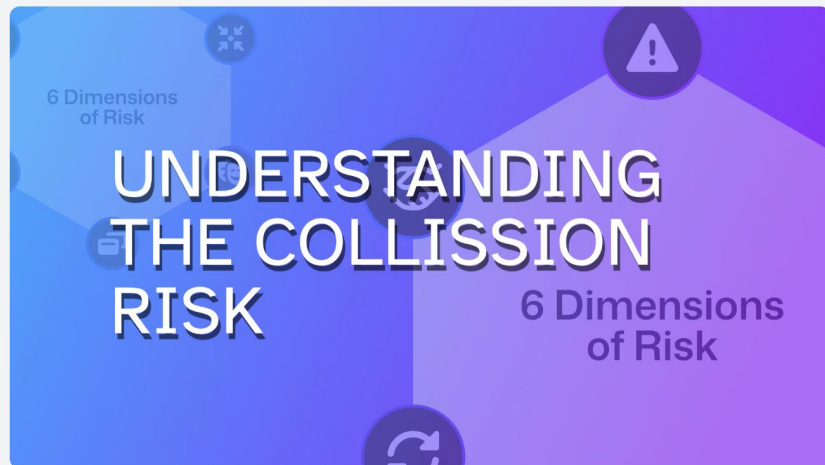


Nathan Alan



Afnic

Published 24 October 2025



Research

#Blockchain

