7-2024

Exploring the market impact of Web3 identity imitation in Ethereum Name Service

Ping Fan KE
Singapore Management University, pfke@smu.edu.sg

Yi Meng LAU
Singapore Management University, ymlau@smu.edu.sg

July 2024

Exploring the Market Impact of Web3 Identity Imitation in Ethereum Name Service

Ping Fan Ke
Singapore Management University, pfke@smu.edu.sg

Yi Meng Lau
Singapore Management University, ymlau@smu.edu.sg

Exploring the Market Impact of Web3 Identity Imitation in Ethereum Name Service

Short Paper

Ping Fan Ke
Singapore Management University
80 Stamford Road Singapore 178902
pfke@smu.edu.sg

Yi Meng Lau
Singapore Management University
90 Stamford Road Singapore 178903
ymlau@smu.edu.sg

Abstract

Digital identities are paramount in today's digital landscape. However, in the Web3 ecosystem, the absence of a central governing body leaves digital identities, such as domain names, vulnerable to cybersquatting and identity imitation. This study examines the market impact of identity imitation in the Web3 ecosystem. By scrutinizing trading activities within Web3 domain names from Ethereum Name Service (ENS) and its imitator, "Ether Name Service," we found that the presence of a newly imitating domain name increases the subsequent resale value of the authentic domain name. Additionally, we find a positive correlation between the resale value of the imitating domain name and the authentic domain name. These findings highlight the complex interplay between trust, reputation, and popularity in the Web3 domain name market and yield valuable insights for stakeholders grappling with digital identity challenges amid the Web3 era.

Keywords: digital identity, Web3, domain name, Ethereum Name Service, cybersquatting

Introduction

In today's digital society, digital identities play a vital role across diverse domains, from business transactions to social interactions. A desirable digital identity incorporates several key attributes: a unique identifier for precise identification, pseudonymity to safeguard privacy, traceability to deter unlawful activities, and credentials to establish trust (Laurent et al., 2015). With the scarcity of unique identifiers in mind, organizations increasingly recognize the importance of cultivating a distinctive and memorable online presence through their digital identities (Lindenthal, 2014). Therefore, domain names from established service providers like .com or .net often come with higher price tags, indicating the domain name owner's established status (Salvador & Nogueira, 2011). In this context, domain names have emerged as pivotal tools for shaping branding strategies and gaining a competitive edge (Tang et al., 2014).

However, the ease of replicating digital goods has facilitated the emergence of the copycat phenomenon (Wang et al., 2018) in the digital identity marketplaces, especially when established entities are willing to pay significant sums for matching domain names (Tang et al., 2014). These imitators, known as cybersquatters in the digital identity context, register or occupy digital identities belonging to others for malicious purposes. For instance, they may register domain names containing celebrity names or well-known trademarks with the intent to demand exorbitant prices (Anschell & Lucas, 2003). They also create variations of reputable names to confuse the public and the target audience of organizations (Gatsik, 2001). In a notable 1995 case, Dennis Toppen registered domain names reflecting a well-known trademark, Panavision, such as "panavision.com" and "panaflex.com". Subsequently, Toppen offered to sell the domain name "panavision.com" to Panavision International (Richtel, 1998) before legal action was taken by Panavision, which ruled in favor of the company (Anschell and Lucas, 2003).

The rapid growth of Web3 and decentralized applications (dApps) has led to a significant increase in demand for Web3 domain names. In 2022, the Ethereum Name Service saw over 2.8 million domain names

registered (Malwa, 2023), while Unstoppable Domains registered over 3.9 million domain names in 2023 (Unstoppable Domains, 2023). Notable transactions, such as the sales of "samsung.eth" and "starbucks.eth" for approximately $90,000 each, further highlight this demand (Shimron, 2022). Unlike Web2, which benefits from centralized governance through ICANN, Web3 lacks such oversight. This absence has provided an opportunity for cybersquatters to exploit domain names within Web3 platforms (Osborn & Alan, 2023). For instance, an opportunist registered the domain "tot.ether" for 0.02 ETH ($26) and approached the owner of "tot.eth" on Twitter with an offer to repurchase it at 0.09 ETH[1]. Although the owner did not repurchase the imitating domain, this example illustrates the potential influence of counterfeit domains, which could undermine the usability and value of Web3-based digital identities.

To evaluate the potential market impact of cybersquatters or identity imitators within the Web3 ecosystem, we investigate trading activities involving two types of top-level domain names: ".eth" domains offered by the Ethereum Name Service (ENS) and ".ether" domains provided by Ether Name Service. This analysis aims to provide initial insights into how the market value of the original identity is affected by the imitated one and user behavior towards digital identity sources in Web3. The findings hold practical significance for individuals and organizations considering the adoption of digital identities in the Web3 environment. Moreover, they offer valuable insights for market stakeholders interested in providing identity and brand image protection services. Additionally, this research may aid governing and regulatory authorities in establishing surveillance mechanisms for digital products (Butticè et al., 2020).

Background

In this study, we investigate two Web3 domain name service providers: Ethereum Name Service (ENS), an early player in the Web3 domain name industry, and Ether Name Service, a newer rival. ENS is notable for being one of the pioneering Web3 domain name service providers with a large user base. In contrast, Ether Name Service competes directly with ENS by offering domain names that closely resemble those provided by ENS. Web3 domain names differ from traditional Web2 domain names, which are centrally managed by ICANN and typically linked to specific IP addresses. In contrast, Web3 domain names operate on decentralized blockchains using smart contracts and are usually associated with specific wallet addresses. While the pricing of traditional Web2 domains is determined by the domain name registrar, Web3 domain prices are governed by the smart contract logic defined by the service provider.

Ethereum Name Service (ENS)

Launched in May 2017 on the Ethereum blockchain, Ethereum Name Service (ENS) provides Web3 domain name services with names ending in ".eth". It streamlines the usability of dApps by simplifying the conversion of human-readable names to wallet addresses and other metadata, facilitating innovative applications like censorship-resistant messaging. As an early leader in decentralized domain name systems on Ethereum, ENS is widely embraced by the Ethereum community. Originally minted as ERC-721 assets, ENS domain names can be converted by their owner into ERC-1155 format with the name wrapper function introduced in April 2023, allowing the creation of separate subdomain tokens. Tokenization enables direct ownership transfers or resale on marketplaces like OpenSea. ENS adopts a unique pricing model based on domain name length, with fees ranging from $640 for 3-letter domains to $5 for 5 letters or more, alongside an annual fee requirement. As of February 21, 2024, ENS has registered 2.14 million domains, held by over 800,000 unique users, with a cumulative trading volume of 88,213 ETH on OpenSea.

Ether Name Service

Established on the Ethereum blockchain in October 2022, Ether Name Service offers a novel approach to Web3 identity solutions. Unlike ENS, Ether Name Service requires only a one-time payment of 0.02 ETH for ownership, eliminating recurring fees. The service includes a unique referral program with commissions aimed at building the community. It also pioneered the ability to mint non-fungible tokens (NFTs) for each subdomain upon its launch in 2022, providing owners with an avenue for additional revenue. Following suit, ENS adopted this feature in April 2023. Moreover, the adaptable metadata offered by Ether Name Service empowers users to provide descriptions of themselves or link with social media profiles such as

[1] https://twitter.com/DragonStonk/status/1580803505001857024

Instagram and TikTok. As of February 21, 2024, Ether Name Service has registered around 17 thousand domain names, with around 5.2 thousand unique users, and a total transactional volume of 243 ETH.

Literature Review

Digital Identity and Non-Fungible Token (NFT)

ENS and Ether Name services serve as digital identity solutions for individuals and organizations within Web3 ecosystems, and the digital identities provided from these solutions are represented as Non-Fungible Tokens (NFTs) through smart contracts. Digital identities are essential for entities engaged in online transactions, yet authentication processes over open networks are vulnerable to impersonation and attacks (Grassi et al., 2017). While traditionally associated with individuals, companies are now compelled to innovate digitally to maintain a competitive online presence within their ecosystem (Obwegeser and Bauer, 2016). Research suggests that blockchain solutions can extend digital identity concepts for businesses beyond mere Internet visibility (Balastegui-García et al., 2022). By leveraging blockchain's desirable attributes such as enhanced security, trust, and transparency (Faber et al., 2019), organizations can strengthen their Web3 digital identity implementations to meet evolving requirements and transition away from centralized verification approaches used in current architectures (Goodell and Aste, 2019).

The popularity of tokenizing digital assets lies in their ability to represent assets digitally, simplifying transfers and investments (Kölbel et al., 2022). NFTs, appreciated for their unique attributes as indivisible digital assets built on decentralized technology, can verify ownership, originality, and authenticity, enabling authentication as digital identities for both digital and physical items through smart contracts (Hasan et al., 2023). For example, Hideyoshi Moriya demonstrated a proof-of-concept application by using a digital wallet with an ENS NFT to prove their identity and unlock the front door of their house (Web3 Domains, 2023). The decentralized nature of blockchain empowers communities to create their own self-sovereign identities, leading to the emergence of new buzzwords like "Web5" and "Soulbound Tokens" within the industry to describe platforms and applications that utilize these identities (Smethurst, 2023).

As the value of NFTs continues to surge, they face challenges akin to luxury products or artworks, notably susceptibility to counterfeiting (Zimmermann et al., 2023). This challenge leads to difficulties in discerning genuine items, causing economic uncertainty about their true value. While digital copies can be easily duplicated, studies have shown that tokenized pieces maintain unique value due to their exclusivity and scarcity (Galassi et al., 2022). High-performing organizations, in particular, attract imitators seeking to produce counterfeits (Wang et al., 2018), resulting in a rise in counterfeit numbers with increased recognition and success. However, the growing presence of counterfeits does not diminish the demand for authentic products, as customers continue to value their quality, originality, and exclusivity (Nia and Zaichkowsky, 2000). On the other hand, the suggestion of using metadata stored within smart contracts, alongside transparent transaction histories, can streamline NFT verification for all network participants, thereby diminishing the risk of counterfeiting (Popescu, 2021). Still, the imitation of Web3 domain names could present a challenge, prompting our study to assess the potential impact of such imitation.

Domain Names and Cybersquatting

Domain names act as identifiers for individuals or organizations on the Internet. Previous research has investigated domain name sales, revealing how buyer preferences can be influenced by alternative top-level domains (TLDs) and speculative tendencies in the Web2 market (Halvorson et al., 2015). With the emergence of Web3, similar speculative behaviors may arise (Wang et al., 2022). Additionally, factors such as domain length, character composition, and TLD scarcity exert influence on prices in the secondary market, attracting investors (Farahmand, 2017). Moreover, studies indicate that domain name investors in Web3 marketplaces exhibit heightened engagement in auction activities, albeit with a lower number of unique investors compared to the traditional Web2 marketplaces (Ke et al., 2023).

Cybersquatting emerged in the mid-1990s alongside the rapid expansion and commercialization of domain names, often driven by profit-seeking or malicious intent (Anschell & Lucas, 2003). Perpetrators register domain names resembling trademarks or popular brands to either sell them at inflated prices or deceive users into believing they are dealing with legitimate entities (Gatsik, 2001). This undermines brand integrity, poses cybersecurity risks, and disrupts the online domain ecosystem.

By the end of April 2023, there were 1,548,207 unique registrants for blockchain domain names across all providers out of 6,450,309 registered blockchain domain names (Osborn and Alan, 2023). Moreover, many registrants are observed to be registering domain names across multiple providers, with some acquiring multiple domain names featuring popular trademarks and brands. The use of special characters such as spaces, symbols, and emojis further suggests the potential for abuse (Deacon, 2023).

In Web2, ICANN manages the technical aspects of the Domain Name System (DNS) and oversees online disputes, regulating them with various dispute resolution methods (Gatsik, 2001). However, in Web3, which is decentralized, there is no central authority governing these matters. As suggested by Cole (2023), brands can safeguard their identity by registering their name, logo, and relevant intellectual property as trademarks. This legal protection grants them the authority to take legal action against those who misuse their brand. Additionally, the use of monitoring tools, educating customers, and securing social media handles across all platforms using the brand's name may be helpful in further protecting their brands.

Research Model

Our research aims to evaluate the potential market impact of cybersquatting in the Web3 ecosystem, particularly focusing on how identity imitation affects the value of Web3 domain names. On one hand, the presence of imitating domain names may diminish the value of authentic ones, as the widespread use of similar keywords across various digital identities could lead to confusion, especially if names appear identical. This may diminish the credibility of domain names featuring common keywords, consequently lowering their value. Previous research suggests that digital technology companies have experienced reduced profits due to counterfeit goods (Butticè et al., 2020). Therefore, we hypothesize:

H1a: The resale value of a Web3 domain name from an established service provider decreases following the creation of an identical one from an imitating competitor.

H2a: The resale value of a Web3 domain name from an established service provider decreases after the resale of an identical one from an imitating competitor.

On the other hand, the presence of a domain name on an imitating platform may enhance its value on the genuine platform due to increased popularity. While counterfeited goods are generally perceived as harmful to authentic goods, studies indicate that over 70% of consumers believe the brand value of genuine goods is not diminished by the widespread availability of counterfeits (Nia & Zaichkowsky, 2000). Additionally, detrimental effects mainly apply to high-quality, nondeceptive copycats capable of substituting the genuine product, particularly in mobile app contexts (Wang et al., 2018). Therefore, we also hypothesize:

H1b: The resale value of a Web3 domain name from an established service provider increases following the creation of an identical one from an imitating competitor.

H2b: The resale value of a Web3 domain name from an established service provider increases after the resale of an identical one from an imitating competitor.

The intrinsic value of a domain name may manifest in its resale value, even on an imitating platform. If the resale of the imitating domain diminishes the resale value of the authentic one, it implies potential substitution between the two, and a higher resale value of the imitating domain could further decrease the value of the genuine one. Conversely, if the resale value of the imitating domain enhances the resale value of the authentic one, a popularity effect may complement both domains, and a higher resale value of the imitating domain could consequently elevate the value of the genuine one. Therefore, we hypothesize:

H3: The resale value of a Web3 domain name from an imitating platform positively moderates the resale effect applied to the original Web3 domain name from an established service provider.

To evaluate our hypotheses, we collected trading data from OpenSea for Ethereum Name Service (ENS) and Ether Name Service spanning from January 1st, 2022, to December 31st, 2023. In addition, we gathered daily closing prices of Ethereum as a control variable. The sample period includes 337,360 ENS resale transactions occurring on various dates. Instead of aggregating transactions to achieve a balanced panel dataset, we introduced a year-month fixed effect in the econometric model. During this period, 17,080 Ether Name Service domains were minted, with 3,335 of them being resold at least once. The minting and the first resale events of Ether Name Service domains will be used as the treatment variable for the corresponding ENS domain, which allows us to conduct a staggered difference-in-difference analysis. For

instance, suppose the imitating domain "vitalik.ether" was minted on May 11th, 2023 and first resold on May 21st, 2023, while the ENS domain "vitalik.eth" was resold on May 1st, May 15th, and May 31st, 2023. In this case, the treatment variable "After minting of imitating domain" will be zero for the resale record on May 1st, and one for those on May 15th and May 31st, whereas the treatment variable "After first resale of imitating domain" will be zero for the resale record on May 1st and May 15th, and one for that on May 31st.

Table 1 presents the summary statistics of the dataset used in this study. The average resale price for ENS is $448, compared to just $80 for Ether Name Service. This disparity may stem from platform heterogeneity, such as service tenure, registration costs, and support from other Web3 platforms. For example, MetaMask supports domain name resolution for ENS but not for Ether Name Service, significantly impacting domain name usability. Additionally, Ether Name Service imposes a restriction on domain names, limiting them to 1 to 20 alphanumeric characters, hyphens, and underscores, whereas ENS does not have such limitations. To accommodate this constraint, we also analyze subsamples that adhere to these criteria as a robustness test in our subsequent analysis.

Table 1. Summary Statistics

Variable	N	Mean	Std. Dev.	Min	Max
1. ENS domain resale price (in USD)	337360	447.9672	2702.864	0	360998.3
2. After minting of imitating domain	337360	0.009761	0.098315	0	1
3. After first resale of imitating domain	337360	0.002834	0.053158	0	1
4. First resale price of imitating domain	337360	0.55542	21.57883	0	5474.87
5. Ethereum price (in USD)	337360	1698.041	538.3677	995.2526	3835.396
6. Second-level domain name length	337360	7.721019	12.17703	1	4419
7. Digit-only domain name	337360	0.439931	0.496379	0	1
8. Letter-only domain name	337360	0.238804	0.426354	0	1

Analysis Results

For our econometric analysis, we initially apply log transformation to the continuous variables in our dataset to address the right-skewed data. In Table 2, Column 1 presents the baseline model with only control variables, including Ethereum price, domain name length, and character composition of the domain name (Farahmand, 2017). The negative and significant coefficient of domain name length suggests that longer domain names tend to decrease the resale price, consistent with typical domain name pricing schemes.

To test Hypotheses 1 and 2, we introduce treatment dummy variables into the econometric model. The results in Columns 2 and 3 of Table 2 show positive and significant coefficients for both the treatment dummies, supporting Hypotheses 1b and 2b. Specifically, the minting of an imitating domain increases the subsequent ENS domain resale price by an average of 5279.6%, while the first resale of an imitating domain increases the subsequent ENS domain resale price by an average of 3743.6%.

To test Hypothesis 3, we included both the after first resale dummy and the first resale price of the imitating domain variable, along with their interaction term, in the model. The results are displayed in Column 4 of Table 2. Surprisingly, the interaction term is statistically insignificant, failing to support Hypothesis 3. However, the positive and significant coefficient of the first resale price of the imitating domain suggests a strong link to the ENS domain's resale price, regardless of timing. This could imply an intrinsic value associated with the name, reflected in both domains' resale prices.

We extended our analysis by incorporating a comprehensive model that includes variables from previous iterations. In Column 5 of Table 2, we observed that the coefficient of the after first resale dummy became statistically insignificant, which suggests the post-resale effect is primarily driven by the post-mint effect. Additionally, we conducted a series of robustness tests to address potential selection bias issues, and the results are presented in Table 3. Initially, we noted that the treatment of Ether Name Service domain minting could not be applied to ENS domains containing forbidden characters or exceeding 20 characters.

To mitigate this bias, we reanalyzed the full model using a subsample comprising only domain names that met these criteria. Despite a reduction in sample size to 271,077, the results remained consistent.

Table 2. Main Regression Results

	(1)	(2)	(3)	(4)	(5)
DV: ENS resale price	Baseline	After Mint	After Resale	Resale Value	Full Model
After minting of imitating domain		3.9852*** (0.2252)			4.0508*** (0.1757)
After first resale of imitating domain			3.6490*** (0.4917)	2.5405* (1.3093)	-1.3251 (0.1284)
First resale price of imitating domain				0.1463*** (0.0275)	0.1469*** (0.0273)
After first resale × First resale price				-0.6314 (0.4697)	-0.6317 (0.4969)
Ethereum price	0.1510 (0.6068)	0.1427 (0.6231)	0.1462 (0.4916)	0.1348 (0.6169)	0.1314 (0.6285)
Second-level domain name length	-1.2343*** (0.1439)	-1.1329*** (0.1355)	-1.2019*** (0.1406)	-1.1778*** (0.1418)	-1.1089*** (0.1355)
Digit-only domain name	-0.0455 (0.1135)	-0.0615 (0.1092)	-0.0488 (0.1122)	-0.0726 (0.1116)	-0.0854 (0.1084)
Letter-only domain name	-0.3541*** (0.0752)	-0.3269*** (0.0736)	-0.3434*** (0.0744)	-0.3336*** (0.0754)	-0.3171*** (0.0745)
Year-month fixed effect	Yes	Yes	Yes	Yes	Yes
Observations	337360	337360	337360	337360	337360
Adjusted R-squared	0.1783	0.2003	0.1839	0.1932	0.2097

*Robust standard errors clustered at year-month are in paratheses. *** p<0.01, ** p<0.05, * p<0.*10

We further refined our analysis by examining a more constrained subsample, comprising domain names present in both the ENS and Ether Name Service datasets. This resulted in a reduced sample size of 3,161, with consistent outcomes. To address potential bias stemming from multiple trades involving the same domain, we applied fractional regression weights equal to the inverse of the number of trades from each domain in the sample. While the overall results remained consistent, we observed the negative coefficient for the post-resale effect became statistically significant (β=-3.2698, $p<0.01$), further indicating a significantly weakened influence after controlling for the post-mint effect. Finally, we controlled for seller and buyer fixed effects, finding consistent results across all specifications.

Discussion and Conclusion

This study explores identity imitation dynamics in the Web3 landscape, analyzing domain name resale records from Ethereum Name Service (ENS) and Ether Name Service. Consistent with previous research on traditional DNS domain names (Farahmand, 2017), our findings indicate that longer ENS domain names generally have lower resale prices, possibly due to the ENS pricing model or reduced usability. Using an econometric model with staggered difference-in-difference estimation, we observe that registering an imitating domain from Ether Name Service drives up the resale value of the authentic domain name from ENS. Similarly, a comparable effect is observed for the initial resale of an imitating domain from Ether Name Service on the resale value of the corresponding ENS domain name, however, this effect becomes insignificant after controlling for the post-mint effect. Moreover, we find a positive association between the resale value of the imitating domain and that of the authentic domain. Our research contributes to the existing literature on Web3 digital identity and counterfeit in digital goods. Furthermore, it provides

valuable insights for market stakeholders and regulators aiming to grasp the price co-movement of these Web3 digital identities, which is useful in shaping investment decisions and market monitoring strategies.

Table 3. Robustness Tests

	(1)	(2)	(3)	(4)	(5)
DV: ENS resale price	Ether NS Pattern	Match Domain	Weighted Regression	Seller Fixed Effect	Buyer Fixed Effect
After minting of imitating domain	3.4833*** (0.1766)	1.5546*** (0.5578)	4.7136*** (0.1543)	1.4852*** (0.1161)	1.4194*** (0.1144)
After first resale of imitating domain	-0.6914 (1.4962)	1.0509* (0.5362)	-3.2698*** (0.6729)	-0.1761 (0.8500)	-0.8568 (0.7234)
First resale price of imitating domain	0.1286*** (0.0251)	0.3462*** (0.0693)	0.1743*** (0.0256)	0.0641*** (0.0112)	0.0798*** (0.0128)
After first resale × First resale price	-0.7751 (0.5514)	-0.3849** (0.1756)	0.0527 (0.1552)	-0.4087 (0.3170)	-0.2569 (0.2792)
Ethereum price	0.8731*** (0.2715)	0.7018 (0.7783)	0.0779 (0.6812)	0.6368 (0.5322)	0.4568 (0.3549)
Second-level domain name length	-0.2573*** (0.2308)	1.6261 (1.4642)	-0.8995*** (0.1345)	-0.4887*** (0.0535)	-0.6511*** (0.0674)
Digit-only domain name	0.6339*** (0.0911)	1.4789*** (0.4537)	-0.2260** (0.1044)	0.0876 (0.0642)	-0.1026 (0.0689)
Letter-only domain name	0.7185*** (0.1337)	-0.8163 (1.0886)	-0.1120 (0.0702)	-0.0616 (0.0483)	-0.2220*** (0.0348)
Year-month fixed effect	Yes	Yes	Yes	Yes	Yes
Seller fixed effect	No	No	No	Yes	No
Buyer fixed effect	No	No	No	No	Yes
Observations	271077	3161	337264	337360	337360
Adjusted R-squared	0.2956	0.4982	0.2027	0.7417	0.7388

*Robust standard errors clustered at year-month are in paratheses. *** p<0.01, ** p<0.05, * p<0.10*

The positive results observed in Hypotheses 1b and 2b can be attributed to factors such as popularity and trust. Previous studies on copycat mobile apps have indicated that the presence of an imitating app may enhance awareness of the authentic app, subsequently influencing demand for the authentic version. This effect hinges on the extent to which the imitating app can function as a substitute based on its quality and level of deception (Wang et al., 2018). Our findings reveal a complementary relationship between the presence of imitating domain and the increased resale value of the genuine domain, akin to the relationship observed between presence of low-quality, deceptive copycats and the increased demand for the original mobile app. This implies that Ether Name Service may be perceived as a low-quality, deceptive counterfeit when compared to ENS. First, the registration cost of Ether Name Service was abruptly reduced from 0.02 ETH to 0.01 ETH just five days after its initial release, suggesting potential low demand and an unsustainable project. Second, the developer team has launched similar Web3 digital identity services on other blockchains such as Base and Polygon, utilizing identical webpage templates with recurring typographical errors. Third, despite aspirations to integrate Web3 digital identities across multiple blockchains, the developer team has not pursued collaborations with other dApps to provide support and name resolution services, consequently diminishing the usability and quality of the service. Therefore, it is plausible that the imitator domain from Ether Name Service did not undermine the trust or reputation of the ENS domain name. Instead, the exposure of such names likely bolstered the popularity of certain names within the community, consequently increasing the resale prices of the ENS domain names.

We further conducted a post-hoc analysis to investigate potential user-specific behaviors within the scope of our research. An intriguing discovery emerged: only one wallet address acquired domain names sharing the same second-level domain, specifically "jacques.eth" and "jacques.ether," within our sample. While it is customary for companies to secure the same name across various TLDs to mitigate cybersquatting risks in the Web2 landscape — exemplified by Microsoft's ownership of domains like "microsoft.com," "microsoft.net," "microsoft.co," and "microsoft.network" — such practice appeared to be less prevalent than anticipated in our current context, potentially attributable to the modest sample size or the use of multiple different wallet addresses by the same user. Future research endeavors could broaden their scope to encompass multiple Web3 domain name service providers within a blockchain or even extend across different blockchains. By doing so, researchers could ascertain whether users actively participate in safeguarding their digital identities and brands by registering or acquiring their names across multiple platforms. This expanded analysis would offer valuable insights into user behavior regarding digital identity management and brand protection strategies in the evolving Web3 landscape.

Another promising avenue for future research could explore the relationship between Web2 and Web3 domain names concerning digital identity protection. Previous studies have revealed vulnerabilities in Web3 domain names, with 3.7% of ENS domain names susceptible to name hijacking, including entities resembling popular Web2 platforms like "youtube.eth" and "taobao.eth" (Xia et al., 2022). Additionally, insights from prior research indicate that Web3 domain name investors are typically more active but constitute a niche group (Ke et al., 2023). By investigating brand-related domain names, researchers can gain a deeper understanding of how traditional organizations transition into the Web3 domain name and digital identity landscape. Such studies would offer valuable insights into the strategies employed by entities to protect their digital identities across different web environments.

Acknowledgments

This research was supported by the Singapore Ministry of Education (MOE) Academic Research Fund (AcRF) Tier 1 grant.

References

Anschell, J. H., & Lucas, J. J. (2003). What's in a name: dealing with cybersquatting. *Entertainment and The Sports Lawyer, 21*(1), 3-10.

Balastegui-García, G., Sabau, E. M. S., Payá, A. S., & Mora, H. (2022). Corporate Digital Identity Based on Blockchain. In *The International Research & Innovation Forum* (pp. 645-655). Cham: Springer International Publishing.

Butticè, V., Caviggioli, F., Franzoni, C., Scellato, G., Stryszowski, P., & Thumm, N. (2020). Counterfeiting in digital technologies: An empirical analysis of the economic performance and innovative activities of affected companies. *Research Policy, 49*(5), 103959.

Cole, B. (2023). *The brand protection blueprint for small businesses.* Forbes. https://www.forbes.com/sites/byroncole/2023/07/28/defending-your-brand-7-ways-to-combat-brand-hijacking/

Deacon, A. (2023). *Brand names in Blockchain Domains: New frontier for brand owners*. DNS Research Federation. https://dnsrf.org/blog/brand-names-in-blockchain-domains---new-frontier-for-brand-owners/

Faber, B., Michelet, G., Weidmann, N., Mukkamala, R. R., & Vatrapu, R. (2019). BPDIMS: A blockchain-based personal data and identity management system. In *The 52nd Hawaii International Conference on System Sciences (HICSS)*.

Farahmand, F. (2017). The importance of human information processing: a behavioral economics model for predicting domain name choice. *Computer, 50*(9), 67-74.

Galassi, A., Spagnoletti, P., & Federici, T. (2022). The Immutability of Artwork in the Age of Digital Reproduction: NFT from the insiders' perspective. In *ITAIS 2022 Proceedings*. 10.

Gatsik, J. H. (2001). Cybersquatting: identity theft in disguise. *Suffolk University Law Review, 35*(2), 277-302.

Goodell, G., & Aste, T. (2019). A decentralized digital identity architecture. *Frontiers in Blockchain, 2*, 17.

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital identity guidelines*. NIST special publication, 800, 63-3.

Halvorson, T., Der, M. F., Foster, I., Savage, S., Saul, L. K., & Voelker, G. M. (2015, October). From. academy to. zone: An analysis of the new tld land rush. In *Proceedings of the 2015 Internet Measurement Conference* (pp. 381-394).

Hasan, H. R., Madine, M., Yaqoob, I., Salah, K., Jayaraman, R., & Boscovic, D. (2023). Using NFTs for ownership management of digital twins and for proof of delivery of their physical assets. *Future Generation Computer Systems, 146*, 1-17.

Ke, P. F., Lau, Y. M., & Hanley, D. V. (2023). Is Web3 Better Than Web2 for Investors? Evidence from Domain Name Auctions. In *Pacific Asia Conference on Information Systems (PACIS) 2023*.

Kölbel, T., Lamberty, R., Sterk, F., & Weinhardt, C. (2022). Spotlight on DeFi Centerpieces: Towards an Economic Perspective on Asset Tokenization Services. In *Pacific Asia Conference on Information Systems (PACIS) 2022*.

Laurent, M., Denouël J., Levallois-Barth C., & Waelbroeck P. (2015). Digital Identity. In M. Laurent & S. Bouzefrane (Eds.), *Digital Identity Management,* (pp. 1-45). Elsevier.

Lindenthal, T. (2014). Valuable words: price dynamics of internet domain names. *Journal of the Association for Information Science and Technology, 65*(5), 869–881.

Malwa, S. (2023). *Ethereum Name Service Recorded Over 2.8M Domain Registrations in 2022*. CoinDesk. https://www.coindesk.com/markets/2023/01/04/ethereum-name-service-recorded-over-28m-domain-registrations-in-2022/

Nia, A., & Lynne Zaichkowsky, J. (2000). Do counterfeits devalue the ownership of luxury brands?. *Journal of product & brand management, 9*(7), 485-497.

Obwegeser, N., & Bauer, S. (2016). Digital innovation and the becoming of an organizational identity. In *HCI in Business, Government, and Organizations: eCommerce and Innovation: Third International Conference, HCIBGO 2016* (pp. 556-564). Springer International Publishing.

Osborn, G., & Alan, N. (2023). Web 3 disruption and the domain name system: understanding the trends of blockchain domain names and the policy implications. *Journal of Cyber Policy*, 1-23.

Popescu, A. D. (2021, May). Non-fungible tokens (nft)–innovation beyond the craze. In *5th International Conference on Innovation in Business, Economics and Marketing Research* (Vol. 32).

Richtel, M. (1998). *Speculator in vanity domain names loses to big-name business*. The New York Times. https://archive.nytimes.com/www.nytimes.com/library/tech/98/04/cyber/articles/26domain.html

Salvador, P., & Nogueira, A. (2011). Analysis of the internet domain names re-registration market. *Procedia Computer Science, 3*, 325–335. https://doi.org/10.1016/j.procs.2010.12.056

Shimron, L. (2022). *Amazon.eth, Starbucks.bitcoin, Coke.dao? Crypto Domain Names are the Next Big NFT Craze*. Forbes. https://www.forbes.com/sites/leeorshimron/2022/09/10/amazoneth-starbucksbitcoin-cokedao-crypto-domain-names-are-the-next-big-nft-craze

Smethurst, R. (2023). Digital Identity Wallets and their Semantic Contradictions. *In European Conference on Information Systems (ECIS) 2023*.

Tang, J. H., Hsu, M. C., Hu, T. Y., & Huang, H. H. (2014). A general domain name appraisal model. *Journal of Internet Technology, 15*(3), 427–431. https://doi.org/10.6138/JIT.2014.15.3.1

Unstoppable Domains. (2023). *Unstoppable, the largest provider of Web3 domains, launches 12 new registrar partnerships to expand global access*. Yahoo Finance. https://finance.yahoo.com/news/unstoppable-largest-provider-web3-domains-183000115.html

Wang, Y., Horky, F., Baals, L. J., Lucey, B. M., & Vigne, S. A. (2022). Bubbles all the way down? Detecting and date-stamping bubble behaviours in NFT and DeFi markets. *Journal of Chinese Economic and Business Studies, 20*(4), 415-436.

Wang, Q., Li, B., & Singh, P. V. (2018). Copycats vs. original mobile apps: A machine learning copycat-detection method and empirical analysis. *Information Systems Research, 29*(2), 273-291.

Web3 Domains. (2023). *ENS vs Unstoppable Domains*. https://web3domains.com/ens-vs-unstoppable-domains/

Xia, P., Wang, H., Yu, Z., Liu, X., Luo, X., Xu, G., & Tyson, G. (2022). Challenges in decentralized name management: The case of ens. In *Proceedings of the 22nd ACM Internet Measurement Conference* (pp. 65-82).

Zimmermann, R., Udokwu, C., Kompp, R., Staab, M., Brandtner, P., & Norta, A. (2023). Methods to Authenticate Luxury Products: Identifying Key Features and Most Recognized Deficits. *SN Computer Science, 4*(6), 747.