Panning for gold.eth: Understanding and Analyzing ENS Domain Dropcatching

Muhammad Muzammil
Stony Brook University
New York, USA
mmuzammil@cs.stonybrook.edu

Zhengyu Wu
Stony Brook University
New York, USA
zhenwu@cs.stonybrook.edu

Aruna Balasubramanian
Stony Brook University
New York, USA
arunab@cs.stonybrook.edu

Nick Nikiforakis
Stony Brook University
New York, USA
nick@cs.stonybrook.edu

Abstract

Ethereum Name Service (ENS) domains allow users to map human-readable names (such as gold.eth) to their cryptocurrency addresses, simplifying cryptocurrency transactions. Like traditional DNS domains, ENS domains must be periodically renewed. Failure to renew leads to expiration, making them available for others to register (a phenomenon known as dropcatching). This presents a security risk where attackers can register expired domains to leverage the residual trust associated with them and, in the context of ENS, receive transactions intended for their previous owners. In this paper, we conduct the first large-scale study on dropcatching in ENS domains. We curate and analyze a dataset comprising 3.1M ENS domains and 9.7M Ethereum transactions, finding that 241K of these domains were re-registered by new owners after expiration. Our findings indicate a preference for domains linked to high-income wallets in re-registrations. We identify 2,633 transactions that were misdirected to new owners, averaging the equivalent of thousands of US dollars. Lastly, we highlight the lack of countermeasures by digital wallet providers, and suggest straightforward approaches that they can use to minimize financial losses due to ENS dropcatching.

CCS Concepts

• **Security and privacy → Economics of security and privacy**.

Keywords

Cryptocurrency; NFTs; Blockchain; Domains

ACM Reference Format:
Muhammad Muzammil, Zhengyu Wu, Aruna Balasubramanian, and Nick Nikiforakis. 2024. Panning for gold.eth: Understanding and Analyzing ENS Domain Dropcatching. In *Proceedings of the 2024 ACM Internet Measurement Conference (IMC '24), November 4–6, 2024, Madrid, Spain.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3646547.3689009

IMC '24, November 4–6, 2024, Madrid, Spain

ACM ISBN 979-8-4007-0592-2/24/11
https://doi.org/10.1145/3646547.3689009

1 Introduction

The Ethereum Name Service (ENS) [1] functions analogously to the Domain Name System (DNS), providing user-friendly, memorable names that map to cryptocurrency addresses. This simplifies transactions within the cryptocurrency ecosystem by allowing users to utilize easy-to-remember ENS domains instead of lengthy and complex cryptographic addresses. The adoption of ENS domains has expanded significantly, capturing interest from both corporations and public figures. For instance, in 2022, the multi-national sportswear brand Puma adopted the ENS domain `puma.eth` and prominently displayed it as their Twitter/X username [2].

However, ENS domains are susceptible to the same range of attacks as traditional DNS domains, including domain dropcatching. This attack occurs when legitimate domain owners forget to renew their ENS domains on time, allowing attackers to re-register the "dropping" ENS domains either for the purpose of selling them back to the original owner for a profit or potentially intercepting future transactions intended for the original owners. The latter vulnerability (i.e. where the funds sent to `alice.eth` do not go where the sender intended them to, but to whoever re-registered the expired domain) is of particular concern in the ENS context, as successful attacks can result in immediate and irreversible financial losses. Furthermore, even benign, non-malicious re-registrations of dropped domain names can still result in the new owner of a domain receiving funds intended for the previous owner. Prior research has acknowledged this danger of expired domain names in the context of ENS but did not empirically study this phenomenon and the extent to which these attacks are already happening [3].

In this paper, we present the first large-scale study investigating ENS domain expirations and re-registrations. Our study identifies characteristics of ENS domains that make them good candidates for re-registrations (i.e. why are some expired domains more likely to be re-registered than others) and reports on the results of a detailed transaction analysis to quantify incidents of financial loss.

To perform this study, we have compiled the most comprehensive dataset of ENS domain data to date (3.1M names), identifying 241K domains that were re-registered by a new owner following expiration. We find that domains with larger amounts of income directed toward their previous wallet addresses are significantly more likely to be targeted for re-registration. Additionally, our analysis reveals 2,633 transactions that potentially represent cases

of financial loss due to these re-registrations, with an average of 4,700 USD mistakenly sent to the new domain owners.

Availability. To encourage further research in this area, we are making our dataset of ENS domains and code to crawl ENS registration data and Ethereum transactions publicly available [4].

2 Background and Motivation

2.1 Ethereum Name Service (ENS)

In the ENS ecosystem, "domains" are non-fungible tokens (NFTs) owned by users, granting them full control over the domain's use and its associated records. Ownership persists until the domain expires or the owner willingly transfers it. To maintain ownership, users must renew their domain registration before it expires, with the option to extend for multiple years in advance. If a domain is not renewed by its expiration date, it becomes available for others to register after a 90-day grace period (the owner has this time to renew their registration before they lose control of it). To re-register an expired domain, users have to pay an additional temporary premium along with the base price of the domain. The temporary premium starts at a 100M USD at the time of writing, and exponentially decays to 0 USD over 21 days (also known as a "Dutch Auction"). We note that decaying premium is unique to ENS (i.e. there is no equivalent mechanism for dropping domains in DNS [5]) temporarily favoring the users who are willing to invest the most resources to purchase a domain name vs. the users who are the fastest to act upon a domain's expiration.

2.2 Motivation

Traditionally, after the expiration of DNS domains, attackers are known to re-register them immediately and then host malicious content on them, capitalizing on the residual trust of the domain [5–8]. We argue that in terms of ENS domains, the stakes are even higher due to the nature of blockchain and cryptocurrency transactions. Unlike DNS domains where the primary risk of expired domain names is closely tied to the purpose of the original domain name (and therefore may or may not lead to a high-impact vulnerability), the re-registration of ENS domains can directly lead to financial losses. When attackers register an ENS domain that was formerly used in financial transactions, they do not need to host any content; they simply wait for transactions. Due to the immutable nature of blockchain transactions, any funds inadvertently sent to the re-registered domain based on its previous ownership are immediately and irreversibly lost to the attacker.

We argue that domain re-registrations in ENS can be harmful even when they are done without mal-intent. In DNS, re-registered domains with benign intentions may still attract traffic; however, users are typically not harmed as they can often discern from visible webpage characteristics that the domain's ownership has changed. In contrast, ENS domain re-registrations, even with benign intent, carry inherent risks. This is because transaction-initiating users — barring assistance from their cryptocurrency wallets — have no ability to immediately identify that the ENS domain that they are about to send funds to has switched hands.

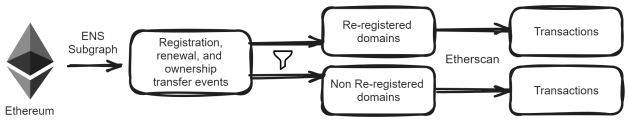

Figure 1: A schematic representation of our data collection, illustrating the integration of third-party APIs.

3 Data Collection

In this section, we describe our data sources and an overview of the data collected for this study (illustrated in Figure 1).

3.1 Registrations, Renewals, and Transfers

Previous research has highlighted the inherent difficulties in extracting a comprehensive dataset of ENS domains from the Ethereum blockchain [3, 9]. This complexity primarily stems from the manner in which ENS domains are stored: rather than being recorded in a human-readable format, they are stored on the blockchain in the form of their keccak-256 hash values. When clients wish to resolve a domain name, they first obtain that hash and then call the appropriate ENS smart contract with the hashed ENS domain as a parameter. While this makes ENS smart contracts more efficient because they can use fixed-length strings, it complicates the process of comprehensively identifying all domains that have been registered. As a result, prior work had to rely on secondary sources and brute-forcing dictionary words into hashes in order to build as complete a list of ENS names as possible [3].

To query ENS data from the Ethereum blockchain, we take advantage of a relatively recent development in the space of blockchains and utilize the ENS subgraph [10], a GraphQL endpoint built atop The Graph protocol [11]. This subgraph is managed by the ENS team itself, which ensures data correctness and completeness. This approach enables the efficient retrieval of information regarding ENS domain names, encompassing ownership details, resolver addresses, and associated records. We queried the ENS subgraph and successfully collected registration data for 3,103,000 ENS domains (and 846,752 subdomains), including registration, renewal, and ownership transfer events. This dataset includes new ownership records, expiration dates, block numbers, and transaction IDs corresponding to these events. However, due to API limitations, 34K ENS names remained unrecoverable, resulting in a data recovery rate of 99.9%. This methodology offers a straightforward, comprehensive, and efficient means of data acquisition compared to direct extraction from the Ethereum blockchain, a process that, as Xia et al. highlighted, faces significant challenges in ensuring data completeness as they were able to collect only 90.1% of all ENS domains [3].

3.2 Ethereum Transactions

The public nature of prominent blockchains enables third-party entities to index their data, subsequently offering access via blockchain explorers like Etherscan [12]. To crawl transaction data within the Ethereum blockchain [13], we leverage the Etherscan API, submitting Ethereum addresses (of ENS domain owners) to procure data on associated incoming and outgoing transactions. This data includes sender and receiver addresses, the amount of ETH transferred, transaction IDs, and timestamps. We manage to

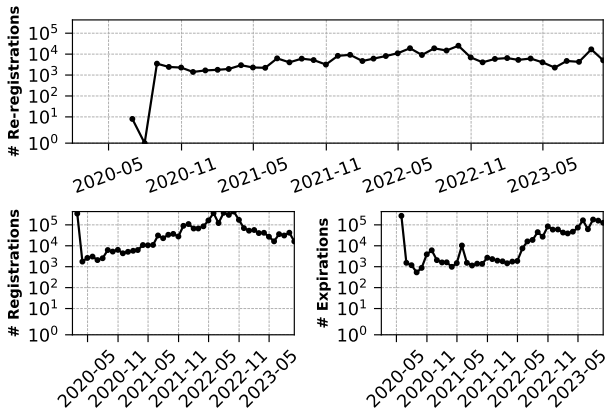

Figure 2: Total registrations, expirations, and re-registration events in ENS along the years 2020 to 2023

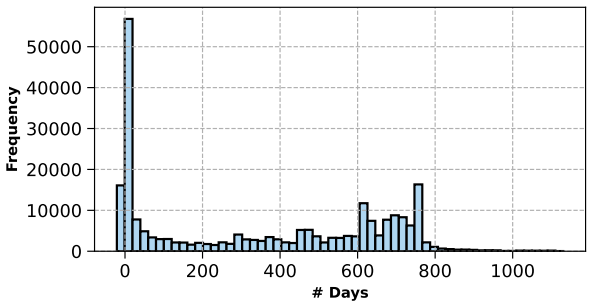

Figure 3: Time (in days) between ENS name expiration and re-registration by a different owner

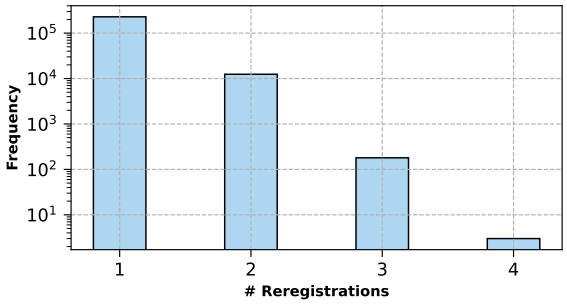

Figure 4: Frequency of the number of times a single domain has been re-registered by a different owner after it expired

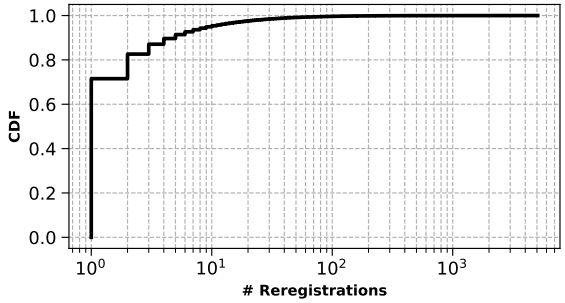

Figure 5: Number of times a unique address re-registered an expired ENS domain

collect transactions for all Ethereum addresses that are relevant to our study, extracting a total of 9,725,874 transactions.

4 Analysis

We utilize registration data for each ENS domain to determine the frequency of registrations attributed to distinct owners. Specifically, we identify domains that have been registered by two or more unique entities. Our dataset comprises a total of 241,283 ENS domains that have undergone at least one cycle of registration, expiration, and re-registration (colloquially known as "dropcatching" in the traditional DNS world [5]).

In this section, we present a detailed analysis of these domains, focusing on patterns and implications of re-registration behaviors. Given that our dataset encompasses registration events of 99% of all ENS domains, it is highly unlikely that a significant number of re-registration events have evaded this analysis.

4.1 Re-registration Overview

Figure 2 illustrates the trends in registrations, expirations, and re-registrations of ENS domains from February 2020 to September 2023. Notably, both registrations and expirations exhibit significant spikes in early 2020. This pattern can be attributed to a critical bug identified in the ENS smart contracts in 2020 [14], prompting a transition from an auction-based system to a new contract framework that supports timed registration and expiration. Under the new system, domain owners were mandated to renew their registrations by May 2020. Failure to comply resulted in the expiration of these domains, thus making them available for new registrations. This event catalyzed a surge in expirations and provided a unique opportunity for users to acquire previously unavailable domains and potentially capture transactions directed to former owners. The data indicates a rising trend in registrations until the end of 2022, followed by a decline. Concurrently, there was a sharp increase in expirations. However, the rate of re-registrations remained relatively consistent throughout the observed period, with the peak monthly re-registrations reaching 25,193.

Figure 3 displays the interval, measured in days, between the expiration of an ENS domain and its re-registration by a different owner. We identify new ownership by searching for domains that are held by new wallets post-expiration vs. pre-expiration. Figure 4 depicts the distribution of the frequencies at which ENS domains have been re-registered, where 12,614 ENS domains have been registered more than twice. Together, these figures indicate a high demand for certain ENS domains; notably, 56,792 domains were re-registered shortly after their temporary premium periods concluded, with 20,014 domains being re-registered on the very day the premium ended. Interestingly, 16,092 domains attracted re-registrations at a premium price pointing to users who were willing to pay significantly more than the standard price to obtain expired ENS domains.

The data reveals that several users have acquired multiple domains following their expiration. Figure 5 presents the CDF of

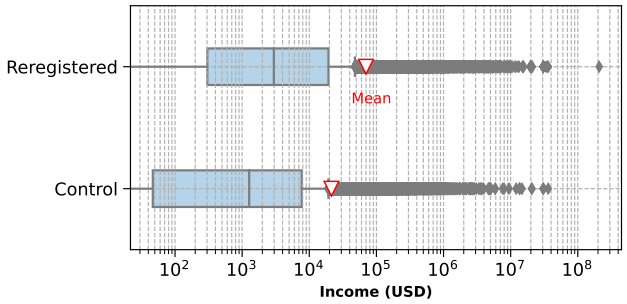

Figure 6: Income in USD received by previous owners of re-registered and control domains.

Feature	Re-registered	Control
`average_income_USD`	69,980	21,400
`average_num_unique_senders`	8	7
`average_num_transactions`	25	24
`average_length`	8	10
`contains_digit`	12,751 (2.3%)	65,432 (27.1%)
`is_numeric`	33,482 (13.9%)	32,534 (13.48%)
`contains_dictionary_word`	108,913 (45.1%)	89,444 (37.1%)
`is_dictionary_word`	17,955 (7.4%)	2,238 (0.93%)
`contains_brand_name`	1,352 (0.6%)	993 (0.41%)
`contains_adult_word`	1,635 (0.7%)	1,998 (0.8%)
`contains_hyphen`	6,753 (2.8%)	14,764 (6.12%)
`contains_underscore`	514 (0.2%)	5,275 (2.19%)

Table 1: Comparison of lexical and transactional features of re-registered/non re-registered domains

the number of re-registrations by unique owners, showing that a subset of users have engaged in the re-registration of a large number of expired domains, which may indicate potential speculative or opportunistic behaviors. Overall, the owners of 19,763 Ethereum addresses have engaged in the re-registration of more than one expired ENS domain. The three addresses most active in such behaviors have re-registered 5,070, 3,165, and 2,421 domains, respectively.

4.2 Re-sale Market

In addition to speculative dropcatching, re-registrations of ENS domains may also be motivated by intentions to resell at a higher price. To explore this aspect, we investigated the listings and sales of re-registered domains on OpenSea [15], the largest NFT marketplace [16]. Using the OpenSea API [17], we tracked the events associated with re-registered domains listed for sale. Our findings indicate that only 19,987 (8%) of re-registered domains were ever listed on OpenSea by their new owners, and of these, 12,130 were successfully sold. This data suggests that name hoarding does not appear to be the predominant motive behind the re-registration of ENS domains. It is, nevertheless, important to acknowledge that regardless of benign or malicious intent, ENS names are being re-registered for various purposes and can always receive transactions that were meant for the previous domain owners. For example, the domain `gno.eth` was re-registered for 12K USD by an address that has a high volume of transactions with the "Gnosis: Active Treasury Management" smart contract (labeled by Etherscan). This smart contract is related to the Gnosis chain [18] (an Ethereum side-chain) and transactions can only be approved towards this smart contract if a certain percentage of owners approve them [19], suggesting that the `gno.eth` domain was acquired by Gnosis developers. Before this registration, `gno.eth` used to belong to another user who had registered it for the equivalent of 735 USD. That former user had never transacted with a Gnosis smart contract but had transacted with multiple other different addresses which might still mistakenly send transactions through the repurposed `gno.eth` domain.

4.3 Re-registered Domain Characteristics

When an ENS domain expires, it can be attractive for re-registration due to its potential perceived value. In this section, we explore the attributes that contribute to the valuation of ENS domains, focusing on lexical and transactional features (listed in Table 1), and compare these attributes with those of domains that expired but were not re-registered. Regarding the lexical features, we draw inspiration from the work of Miramirkhani et al. who investigated traditional domain dropcatching in 2018 [5] and sought to identify which features make some expired DNS domains more likely to be re-registered than others.

We hypothesize that lexical attributes influence the value of ENS domains for re-registration. For example, domains such as `abc.eth` and `000.eth`, characterized by their concise three-letter format, typically sell for high prices in the six-figures range [20]. The owners of these domains are recognized as members of the "3 Letters Club" [21], highlighting the market for short and memorable names. The transactional features of an ENS domain can also play a role in its value for re-registration, including the number of transactions, the number of unique sender addresses, and the total amount of ETH transacted to the previous owner's address linked to the domain.

To systematically evaluate the significance of these features, we conduct a comparative analysis using an equally-sized control group of 241,283 domains randomly sampled from the 1.17M domains that expired and were *not* re-registered by a different owner. We collect the same set of features for this control group. For categorical features, we employ proportion tests, while for numerical features, we utilize t-tests to compare the mean values between the re-registered domains and the control group and determine a feature to be statistically significant if the p-value was less than 0.05.

Our results, shown in Table 1, suggest that domains that are easy to recall, transactionally active, and financially lucrative are generally preferred for re-registration. All considered features are statistically significant in distinguishing between domains that are re-registered and those that are not. *Income* is the most notable feature, referring to the total USD value transacted through the domain before its expiration (converted from ETH using the adjusted closing price on the day of each Ethereum transaction [22]). The income differences between the two groups are depicted in Figure 6, showing a clear preference for higher-income domains in the re-registration process.

4.4 Financial Losses

In this section, we describe our methodology for quantifying the success of attackers in terms of receiving unintended transactions in their wallets from re-registered ENS domains.

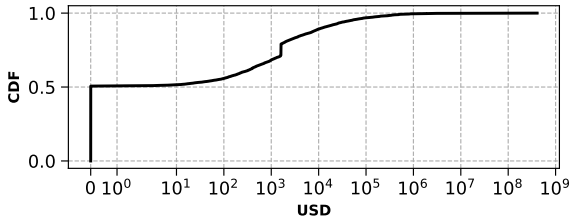

Figure 7: Amount of hijackable USD sent to the corresponding wallet address of an expired ENS domain.

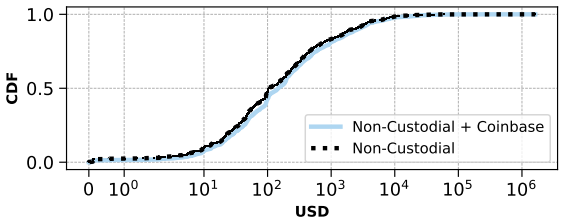

Figure 8: Amounts transacted (in USD) to a_2 by a common sender c.

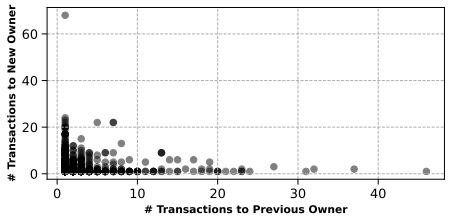

Figure 9: Number of transactions sent by a common sender c to the previous owner a_1 as compared to the new owner a_2 where c is either a Coinbase or non-custodial address.

According to the ENS documentation [23], domains that were registered after ENS contract migration continue to resolve to the addresses set by previous owners even after expiration. This design decision is a clear departure from the behavior of DNS domain names (which stop resolving when they expire) which effectively hides problems by keeping ENS domains functional until it is too late. That is, an expired ENS domain remains functional (its owner is receiving transactions sent by other users) until the new owner registers the domain name and overwrites its resolution address. Without any warning (such as resolution failures) that domain name suddenly starts resolving to a new address that will now receive all transactions intended for the previous owner of that domain.

We attempt to resolve expired domains on popular ENS-supporting wallets (Appendix B), finding that none of these wallets display a warning that the domain name has expired but continue to resolve the domain to the corresponding address. This means that attackers can in fact register expired ENS domains and hijack transactions that these domains might still be receiving. Figure 7 illustrates the amount of hijackable funds that were sent to the corresponding wallet addresses of the expired domains before they were re-registered (i.e. could have been redirected by attackers, had they registered the domain names before their real owners re-registered them).

Identifying the precise number of unintended transactions directed towards new owners of ENS domains is not straightforward. Unlike DNS domains, where passive DNS data can reveal resolution frequencies, ENS domains lack such visibility. Transactions via an ENS domain involve a smart contract, known as a resolver, which resolves the domain to its corresponding wallet address before the transaction is executed on the Ethereum blockchain. However, only an address-to-address transaction will be visible on Ethereum, and not the resolution event or the ENS domain that was used. Consequently, one cannot definitively conclude that a given transaction was initiated using an ENS domain vs. by directly pasting the wallet address into the digital wallet and bypassing ENS entirely. We made multiple efforts to acquire resolution data from various digital wallet vendors, but were ultimately unsuccessful due either to the vendors' reluctance to share such data or the unavailability of long-term resolution data.

Given this absence of data, we adopt a conservative approach to identify cases of financial loss using registration history data and raw transactions from our dataset. Our approach aims to minimize false positives in our analysis, by focusing on cases where there is a high probability that funds sent to the new owner of an ENS domain, were in fact intended for a previous owner.

We consider this scenario: address a_1 holds the domain d, which expires and is then re-registered by address a_2. There is a sender c that sent funds to a_1 only while a_1 held d, but only ever sent funds to a_2 when a_2 held d, and never again to a_1. This pattern suggests that c likely used the ENS domain to send funds, unaware of the change in ownership, thus mistakenly sending their funds to a_2 instead of the intended recipient a_1 through the re-registered domain name. While there are additional scenarios where a_2 could have received funds intended for a_1 (such as in the case of a user who had never transacted with a_1 pre-expiration), these are harder to identify by purely using transaction data. As such, in the rest of this section, we focus on the aforementioned scenario to quantify financial losses.

Note that c can either be a custodial or a non-custodial wallet address. Custodial wallets are managed by a third party, such as an exchange or service provider, that holds and controls users' private keys and funds on their behalf. Multiple users can access and utilize the same wallet infrastructure, and hence subsequent transactions by a custodial address c might be sourced by different users even if they share the same address. Contrastingly, non-custodial wallets operate on the principle of individual ownership and control. Each non-custodial wallet is associated with a single user who has exclusive control over their private keys and funds. There are multiple ENS-supporting non-custodial wallets, however, Coinbase is the only exchange that supports ENS resolution at the time of this writing. This gives us the opportunity to filter out the transactions where c is a non-Coinbase custodial address. To do so, we source a list of 558 non-Coinbase custodial addresses from Etherscan and filter out any transactions where they are the sending address. We also collect 25 Coinbase addresses from Etherscan and report our results where c is a Coinbase address.

There are currently 484 domains that have received funds in accordance with our aforementioned scenario through an address

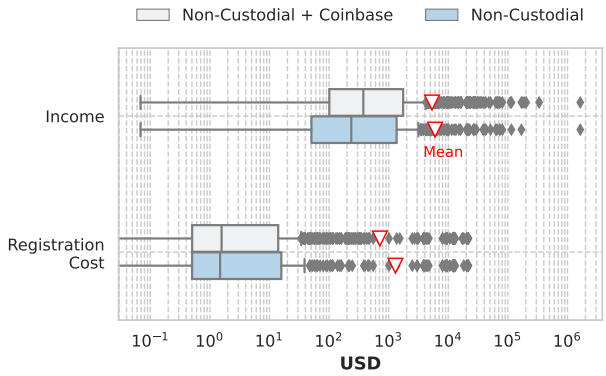

Figure 10: Comparison between the cost of re-registering an expired ENS domain name vs income received from common senders.

c that is a non-custodial address. This number increases to 940 when considering Coinbase addresses for c. Figure 9 displays a scatter plot comparing the number of transactions from c to addresses a_1 and a_2 for both Coinbase and non-custodial addresses c. The same plot in Appendix C considers only non-custodial addresses as c. In both cases, the most commonly observed transaction ratio between a_1 and a_2 is one-to-one, although many-to-many and one-to-many relationships are also prevalent.

Our findings reveal that an average of 1,944 USD was transferred to a_2 addresses by 195 unique non-custodial c addresses, spanning 1,617 transactions. Conversely, an average of 1,877 USD was transferred by 201 unique addresses, encompassing both Coinbase and non-custodial addresses, across 2,633 transactions. Figure 8 illustrates the amounts in USD transferred to a_2 through c addresses.

Figure 10 shows the amounts in USD that attackers spent to re-register expired domains alongside the income they were able to attract towards their wallets from c, showing a clear distinction between the two groups. In total, we find that 91% of addresses that re-registered an expired domain profited from doing so and that the average profit gained from dropcatching an ENS domain is 4,700 USD. Hence, despite applying a conservative methodology for estimating financial losses, we find that attackers are successful in profiting from expired ENS domains.

For example, the domain `profittrailer.eth` underwent registration by two different owners. The initial owner a_1 controlled the domain from February 2020 to January 2021. Subsequently, a_2 acquired it from November 2022 to November 2023. During a_1's period of ownership, an address c initiated 46 transactions to a_1. However, during a_2's ownership, c sent only one transaction to a_2, and ceased transactions to a_1. After a_1's ownership of the domain expired, it continued to resolve to a_1; we observe 10 transactions from c to a_1 in this time-period. Similarly, `spambot.eth` changed hands three times, each to a different owner. a_1 managed the domain from April 2022 to April 2023, and a_2 took over in July 2023, maintaining ownership to date. Address c dispatched 13 transactions to a_1 during this ownership phase, but only a single transaction to a_2 during a_2's control. No transactions occurred in the gap between these registrations. The domain `cryptobuilders.eth` received only one transaction to both a_1 and a_2 from c. Interestingly, both these transactions were of the same value of 1.0 ETH. In all aforementioned examples, c is a non-custodial address.

5 Related Work

The issue of residual trust in expired domain names is a well-studied and well-recognized problem in traditional DNS with unfortunately no good general-purpose solutions [5–8, 24–40].

Studies have also been conducted on the security concerns revolving blockchain naming services such as ENS [3, 9, 41–54] and digital wallets [55–61]. The most closely related work by Xia et. al [3] systematically studies ENS, describing its growth along with some attacks the domains can be vulnerable to. They describe the fact that since the resolution records of ENS domains are kept even after expiration, and digital wallets can keep resolving these domains to their corresponding wallet addresses, the expiration and re-registration events can easily go unnoticed. In comparison, this paper provides the first ever in-depth and systematic analysis of this phenomenon, where we report on the total number of re-registration events, compare re-registered domains with domains that were expired but not re-registered, and perform careful transaction analysis to report likely cases of financial loss that resulted due to expired ENS domains.

6 Discussion and Conclusion

Countermeasures. In both Coinbase and non-custodial wallets, no warning is shown if users attempt to send funds to recently expired/re-registered domain names (Appendix B). Adopting such warnings is a straightforward countermeasure that we expect would greatly reduce the security impact of expired ENS domains.

Limitations. Given the unavailability of off-chain ENS domain resolution data, we employed a conservative methodology to identify funds potentially misdirected toward re-registered domains. Even though we anticipate that our methodology is most likely to *underestimate* the total financial losses associated with ENS dropcatching, it is possible that some of the transactions we flagged were intentional, i.e., a user c who had sent funds to a_1 *intended* to send a transaction to a_2 who also happened to re-register an expired domain that used to belong to a_1. We hope that wallet providers will eventually share their resolution data with researchers so that follow-up work can more authoritatively quantify accidental ENS transactions.

In this paper, we drew attention to the issue of domain dropcatching in the context of the Ethereum Name Service (ENS) and performed the first empirical study of this phenomenon. We collected the largest dataset of ENS domains to-date and identified 241K cases where an ENS domain changed hands to a new owner post-expiration. Among others, we observed that the income towards the pre-expiration wallet of the domain name was significantly higher in re-registered domains vs. domains that expired but were not re-registered. Finally, through careful and conservative analysis of transaction data, we identified 2,633 (1,617 if only non-custodial senders considered) transactions that appear to have been intended for the previous owners of domain names and yet were sent to new owners because of expired and re-registered ENS domains.

Acknowledgments We thank the anonymous reviewers for their helpful feedback. This work was supported by the Office of Naval Research (ONR) under grant N00014-24-1-2193 as well as by the National Science Foundation (NSF) under grants CNS-2211575, CNS-2126654, CNS-1909356, and CNS-1941617.

References

[1] ENS. Ens, April 2024. https://app.ens.domains/.

[2] Ornella Hernandez. Puma registers ens domain, changes name to puma.eth on twitter, May 2024. https://cointelegraph.com/news/puma-rebrands-to-puma-eth-on-twitter.

[3] Pengcheng Xia, Haoyu Wang, Zhou Yu, Xinyu Liu, Xiapu Luo, Guoai Xu, and Gareth Tyson. Challenges in decentralized name management: the case of ens. In *Proceedings of the 22nd ACM Internet Measurement Conference.*, pages 65–82, 2022.

[4] Pragsec Lab. ens-dropcatching, August 2024. https://github.com/pragseclab/ens-dropcatching.

[5] Najmeh Miramirkhani, Timothy Barron, Michael Ferdman, and Nick Nikiforakis. Panning for gold.com: Understanding the dynamics of domain dropcatching. In *Proceedings of the 2018 World Wide Web Conference*, pages 257–266.

[6] Chaz Lever, Robert Walls, Yacin Nadji, David Dagon, Patrick McDaniel, and Manos Antonakakis. Domain-z: 28 registrations later measuring the exploitation of residual trust in domains. In *2016 IEEE symposium on security and privacy (SP)*, pages 691–706.

[7] Johnny So, Najmeh Miramirkhani, Michael Ferdman, and Nick Nikiforakis. Domains do change their spots: Quantifying potential abuse of residual trust. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 2130–2144.

[8] Tyler Moore and Richard Clayton. The ghosts of banking past: Empirical analysis of closed bank websites. In *International Conference on Financial Cryptography and Data Security*, pages 33–48. Springer, 2014.

[9] Audrey Randall, Wes Hardaker, Geoffrey M Voelker, Stefan Savage, and Aaron Schulman. The challenges of blockchain-based naming systems for malware defenders. In *2022 APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–14.

[10] ENS. Ens subgraph, March 2024. https://docs.ens.domains/web/subgraph.

[11] The Graph. The graph, March 2024. https://thegraph.com/.

[12] Etherscan. Etherscan.io, March 2024. https://etherscan.io/.

[13] Vitalik Buterin et al. Ethereum white paper. *GitHub repository*, 1:22–23, 2013.

[14] Dean Eigenmann. Let's talk ens migration (post-mortem), May 2024. https://medium.com/deaneigenmann/lets-talk-ens-migration-a92d5c21df28.

[15] Opensea. Opensea.io, April 2024. https://opensea.io/.

[16] David Rodeck. Top nft marketplaces of august 2024, August 2024. https://www.forbes.com/advisor/investing/cryptocurrency/best-nft-marketplaces/.

[17] Opensea API. Opensea.io api, April 2024. https://docs.opensea.io/reference/api-overview/.

[18] Gnosis. Gnosis chain, April 2024. https://www.gnosis.io/.

[19] Etherscan. Etherscan: Gnosis active treasury management smart contract, April 2024. https://etherscan.io/address/\0x849d52316331967b6ff1198e5e32a0eb168d039d.

[20] Nicholas Boey. Most expensive crypto domains, May 2024. https://www.coingecko.com/research/publications/most-expensive-crypto-domains.

[21] Vision. Vision.io 3 letters club, April 2024. https://vision.io/category/3-letters.

[22] Yahoo. Ethereum usd (eth-usd), May 2024. https://nz.finance.yahoo.com/quote/ETH-USD/history/.

[23] ENS. Ens faq: What happens if i forget to renew my name, March 2024. https://docs.ens.domains/faq.

[24] Tobias Lauinger, Abdelberi Chaabane, Ahmet Salih Buyukkayhan, Kaan Onarlioglu, and William Robertson. Game of registrars: An empirical analysis of {Post-Expiration} domain name takeovers. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 865–880, 2017.

[25] Tobias Lauinger, Ahmet S Buyukkayhan, Abdelberi Chaabane, William Robertson, and Engin Kirda. From deletion to re-registration in zero seconds: Domain registrar behaviour during the drop. In *Proceedings of the Internet Measurement Conference 2018*, pages 322–328.

[26] Tristan Halvorson, Kirill Levchenko, Stefan Savage, and Geoffrey M Voelker. Xxxtortion? inferring registration intent in the. xxx tld. In *Proceedings of the 23rd international conference on World wide web*, pages 901–912, 2014.

[27] Tristan Halvorson, Janos Szurdi, Gregor Maier, Mark Felegyhazi, Christian Kreibich, Nicholas Weaver, Kirill Levchenko, and Vern Paxson. The biz top-level domain: ten years later. In *Passive and Active Measurement: 13th International Conference, PAM 2012, Vienna, Austria, March 12-14th. Proceedings 13*, pages 221–230. Springer.

[28] Nick Nikiforakis, Luca Invernizzi, Alexandros Kapravelos, Steven Van Acker, Wouter Joosen, Christopher Kruegel, Frank Piessens, and Giovanni Vigna. You are what you include: large-scale evaluation of remote javascript inclusions. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 736–747.

[29] Thomas Vissers, Timothy Barron, Tom Van Goethem, Wouter Joosen, and Nick Nikiforakis. The wolf of name street: Hijacking domains through their nameservers. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 957–970.

[30] Johann Schlamp, Josef Gustafsson, Matthias Wählisch, Thomas C Schmidt, and Georg Carle. The abandoned side of the internet: Hijacking internet resources when domain names expire. In *Traffic Monitoring and Analysis: 7th International Workshop, TMA 2015, Barcelona, Spain, April 21-24, 2015. Proceedings 7*, pages 188–201. Springer.

[31] Tobias Lauinger, Kaan Onarlioglu, Abdelberi Chaabane, William Robertson, and Engin Kirda. Whois lost in translation: (mis) understanding domain name expiration and re-registration. In *Proceedings of the 2016 Internet Measurement Conference*, pages 247–253.

[32] Sourena Maroofi, Maciej Korczyński, Cristian Hesselman, Benoit Ampeau, and Andrzej Duda. Comar: Classification of compromised versus maliciously registered domains. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 607–623.

[33] Timothy Barron, Najmeh Miramirkhani, and Nick Nikiforakis. Now You See It, Now You Don't: A Large-scale Analysis of Early Domain Deletions. In *22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019)*, pages 383–397.

[34] Guannan Liu, Lin Jin, Shuai Hao, Yubao Zhang, Daiping Liu, Angelos Stavrou, and Haining Wang. Dial" n" for nxdomain: The scale, origin, and security implications of dns queries to non-existent domains. In *Proceedings of the 2023 ACM on Internet Measurement Conference*, pages 198–212.

[35] Andrew J Kalafut, Minaxi Gupta, Christopher A Cole, Lei Chen, and Nathan E Myers. An empirical study of orphan dns servers in the internet. In *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, pages 308–314, 2010.

[36] Raffaele Sommese, Mattijs Jonker, Roland van Rijswijk-Deij, Alberto Dainotti, Kimberly C Claffy, and Anna Sperotto. The forgotten side of dns: Orphan and abandoned records. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 538–543.

[37] Shuang Hao, Alex Kantchelian, Brad Miller, Vern Paxson, and Nick Feamster. Predator: proactive recognition and elimination of domain abuse at time-of-registration. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 1568–1579.

[38] Shuang Hao, Matthew Thomas, Vern Paxson, Nick Feamster, Christian Kreibich, Chris Grier, and Scott Hollenbeck. Understanding the domain registration behavior of spammers. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 63–76.

[39] Daiping Liu, Shuai Hao, and Haining Wang. All your dns records point to us: Understanding the security threats of dangling dns records. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1414–1425.

[40] Eihal Alowaisheq, Peng Wang, Sumayah A. Alrwais, Xiaojing Liao, XiaoFeng Wang, Tasneem Alowaisheq, Xianghang Mi, Siyuan Tang, and Baojun Liu. Cracking the wall of confinement: Understanding and analyzing malicious domain take-downs. In *26th Annual Network and Distributed System Security Symposium, NDSS*. The Internet Society, 2019.

[41] Muhammad Muzammil, Zhengyu Wu, Lalith Harisha, Brian Kondracki, and Nick Nikiforakis. Typosquatting 3.0: Characterizing Squatting in Blockchain Naming Systems. In *Proceedings of the Symposium on Electronic Crime Research (eCrime)*, 2024.

[42] Constantinos Patsakis, Fran Casino, Nikolaos Lykousas, and Vasilios Katos. Unravelling ariadne's thread: Exploring the threats of decentralised dns. *IEEE Access*, 8:118559–118571, 2020.

[43] Harry A Kalodner, Miles Carlsten, Paul M Ellenbogen, Joseph Bonneau, and Arvind Narayanan. An empirical study of namecoin and lessons for decentralized namespace design. In *WEIS*, volume 1, pages 1–23, 2015.

[44] Muneeb Ali, Jude Nelson, Ryan Shea, and Michael J Freedman. Blockstack: A global naming and storage system secured by blockchains. In *2016 USENIX annual technical conference (USENIX ATC)*, pages 181–194.

[45] Yuhao Dong, Woojung Kim, and Raouf Boutaba. Bitforest: a portable and efficient blockchain-based naming system. In *2018 14th International Conference on Network and Service Management (CNSM)*, pages 226–232.

[46] Georgia Osborn and Nathan Alan. Web 3 disruption and the domain name system: understanding the trends of blockchain domain names and the policy implications. *Journal of Cyber Policy*, pages 1–23, 2023.

[47] Fran Casino, Nikolaos Lykousas, Vasilios Katos, and Constantinos Patsakis. Unearthing malicious campaigns and actors from the blockchain dns ecosystem. *Computer Communications*, 179:217–230, 2021.

[48] Joshua Theoder, Binusha Shabu Metharath, and Sahel Alouneh. Securing domain name systems with blockchain. In *2023 Fourth International Conference on Intelligent Data Science Technologies and Applications (IDSTA)*, pages 48–53.

[49] Apurva Tamhankar, Sunita Dhavale, Arun Mishra, Balaji Rajendran, and Gopinath Palaniappan. Blockchain based decentralized technology for internet naming systems. In *2023 IEEE 11th Region 10 Humanitarian Technology Conference (R10-HTC)*, pages 1–6.

[50] Daiki Ito, Yuta Takata, Hiroshi Kumagai, and Masaki Kamizono. Investigations of top-level domain name collisions in blockchain naming services. In *Proceedings of the ACM on Web Conference 2024*, pages 2926–2935.

[51] Jintao Huang, Pengcheng Xia, Jiefeng Li, Kai Ma, Gareth Tyson, Xiapu Luo, Lei Wu, Yajin Zhou, Wei Cai, and Haoyu Wang. Unveiling the paradox of nft prosperity. In *Proceedings of the ACM on Web Conference 2024*, pages 167–177, 2024.

[52] Dipanjan Das, Priyanka Bose, Nicola Ruaro, Christopher Kruegel, and Giovanni Vigna. Understanding security issues in the nft ecosystem. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages

667–681, 2022.
[53] Hongzhou Chen and Wei Cai. How information manipulation on social media influences the nft investors' behavior: A case study of goblintown. wtf. *IEEE Transactions on Computational Social Systems*, 2023.
[54] Navin Keizer, Onur Ascigil, Michal Król, Dirk Kutscher, and George Pavlou. A survey on content retrieval on the decentralised web. *ACM Computing Surveys*, 56(8):1–39, 2024.
[55] Christof Ferreira Torres, Fiona Willi, and Shweta Shinde. Is your wallet snitching on you? an analysis on the privacy implications of web3. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 769–786.
[56] Jaakko Pentinsaari. Private key vulnerabilities in browser wallets. 2023.
[57] Kailun Yan, Jilian Zhang, Xiangyu Liu, Wenrui Diao, and Shanqing Guo. Bad apples: Understanding the centralized security risks in decentralized ecosystems. In *Proceedings of the ACM Web Conference 2023*, pages 2274–2283.
[58] Philipp Winter, Anna Harbluk Lorimer, Peter Snyder, and Benjamin Livshits. Security, privacy, and decentralization in web3, 2023.
[59] Kailun Yan, Xiaokuan Zhang, and Wenrui Diao. Stealing trust: Unraveling blind message attacks in web3 authentication. *arXiv preprint arXiv:2406.00523*, 2024.
[60] Panagiotis Chatzigiannis, Konstantinos Chalkias, Aniket Kate, Easwar Vivek Mangipudi, Mohsen Minaei, and Mainack Mondal. Sok: Web3 recovery mechanisms. *Cryptology ePrint Archive*, 2023.
[61] Sihao Hu, Zhen Zhang, Bingqiao Luo, Shengliang Lu, Bingsheng He, and Ling Liu. Bert4eth: A pre-trained transformer for ethereum fraud detection. In *Proceedings of the ACM Web Conference 2023*, pages 2189–2197, 2023.

A Ethics

This paper reports on the analysis on publicly available data from the Ethereum blockchain and the ENS subgraph. We did not interact with any users (benign or malicious) for any of the experiments in this paper. Hence, this paper does not raise any ethical concerns.

B Digital Wallets

Digital Wallet	Date/Version #	Displays Warning
Metamask	11.13.1	No
Coinbase	05/2024	No
Trust Wallet	2.9.2	No
Bitcoin.com	8.22.1	No
Alpha Wallet	3.72	No
Atomic Wallet	1.29.5	No
Rainbow Wallet	1.4.81	No

Table 2: Popular ENS supporting digital wallets (custodial or non-custodial) do not display a warning before a transaction is being sent to an expired/re-registered domain

C Financial Losses

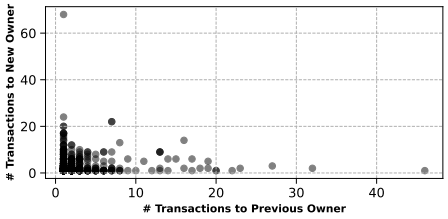

Figure 11: Number of transactions sent by a common sender c to the previous owner a_1 as compared to the new owner a_2 where c is a non-custodial address.