A Deeper Grasp of Handshake: A Thorough Analysis of Blockchain-based DNS Records

Katsuki Isobe, Jean-Philippe Eisenbarth, Daishi Kondo, Thibault Cholez, Hideki Tode

A Deeper Grasp of Handshake: A Thorough Analysis of Blockchain-based DNS Records

Katsuki Isobe*, Jean-Philippe Eisenbarth†, Daishi Kondo*, Thibault Cholez‡, and Hideki Tode*
*Graduate School of Informatics, Osaka Metropolitan University, Japan
†SnT, University of Luxembourg, Luxembourg
‡Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France
Email: sb22688c@st.omu.ac.jp, philippe.eisenbarth@uni.lu,
daishi.kondo@omu.ac.jp, thibault.cholez@loria.fr, tode@omu.ac.jp

Abstract—The current domain name system (DNS) relies on specific organizations such as the Internet Corporation for Assigned Names and Numbers for its administration. Therefore, misconfigurations or arbitrary deployments by these organizations may have a negative impact on the Internet. Handshake, which is a blockchain-based DNS service, can offer an alternative and extended system to the current DNS by managing the root zone on the blockchain without relying on specific organizations. This paper addresses the following research question: Can Handshake replace the current DNS in the future? At the time of this writing, this is the first detailed analysis of Handshake, with a particular focus on undesirable activities and security issues observable from the blockchain data. By discussing concerns regarding malicious usage of domain names, such as domain squatting, with the usage cost data, the paper demonstrates that there is a significant possibility of domain name abuse with lower cost in general. Furthermore, by discussing system redundancy as part of the blockchain-based DNS, it shows that there is a likelihood for lower redundancy of authoritative DNS servers. In response to the research question, the paper concludes that Handshake cannot and should not replace the current DNS in the future without resolving these issues through the introduction of security measures for general users.

Index Terms—Blockchain, Domain Name System, Handshake.

I. Introduction

The Domain Name System (DNS) facilitates the conversion between IP addresses and domain names. It is a highly critical service upon which most, if not all, Internet services are dependable. Recently, there have been various opinions questioning its centralized management architecture. The Internet Assigned Numbers Authority, a function of the Internet Corporation for Assigned Names and Numbers (ICANN), oversees the root zone data used for managing top-level domains (TLDs), although various entities, including enterprises, manage DNS servers. Consequently, the ICANN holds authority over the creation of new TLDs and the suspension of existing TLDs. Notably, Ukraine requested the suspension of the .ru domain during the 2022 Russian invasion of Ukraine [1]. Although no suspension decision was made, concerns regarding the potential for arbitrary censorship due to the centralized management of root zone data persist. Furthermore, this centralized approach may introduce misconfigurations or arbitrary actions, which compromises the reliability and security features of DNS, such as DNS Security Extensions (DNSSEC) [2].

Handshake [3] is a blockchain system that can serve as an alternative and extended system to the current DNS by managing the root zone on the blockchain. Launching in 2020, the purpose of Handshake is to create a decentralized and secure DNS infrastructure, and Handshake has unique features that no other blockchain service has, such as providing TLDs mainly for the same purpose as the current DNS. On this system, users can register and own new Handshake TLDs by participating in auctions using cryptocurrency transactions (TXs), akin to the smart contract mechanism of Ethereum [4]. There are minimal restrictions on registrable TLDs, except for length (up to 63 characters) and special symbol usage, such as periods. However, all existing DNS TLDs and several popular second-level domains (SLDs) are reserved for their original owners to prevent conflicts with the current DNS [5]. Owners can register reserved names on Handshake through a specific TX procedure, called Claim [6]. Additionally, domains have expiration dates to prevent them from being locked due to owner inactivity.

While it is important to consider the impact of unique features, there has been limited research [7] investigating the possible misuses of Handshake, and the practical utilization of Handshake remains unclear due to its novelty. We pose the following research question: Can Handshake replace the current DNS in the future? To answer this question, we conduct the first detailed and comprehensive analysis of Handshake, utilizing Handshake blockchain data and discussing concerns regarding malicious domain name usage, including domain squatting. Furthermore, we explore system redundancy and usage costs associated with the blockchain-based DNS. Our experimental results reveal a significant potential for domain name abuse at a lower cost and a likelihood of reduced redundancy in authoritative DNS servers.

Our contributions are as follows:

- Modification of Handshake client to dump all TLD

This work was supported by JSPS KAKENHI Grant Number JP21K17741.

data,
- Discovering a considerable number of TLDs that can be used for domain abuse including domain squatting with lower cost, and
- Discovering lower authoritative DNS server redundancy issue.

The remainder of the paper is structured as follows. Section II elucidates various security concerns surrounding DNS and offers technical insights into Handshake, including client specifications. Section III presents the methodology and results of the experiments analyzing TLDs and their records stored on the Handshake blockchain. Section IV delves into the uncovered issues of Handshake and discusses corresponding countermeasures. Section V explores some other technologies and previous efforts related to the blockchain-based DNS and its challenges. Section VI concludes the paper.

II. Backgrounds

A. Security Concerns of DNS

Domain squatting is an undesirable activity that registers domain names resembling the names of well-known companies or products, typically for malicious or speculative purposes. For example, typo squatting [8], which is a type of domain squatting, is aimed at registering domain names while expecting users to make typographical errors, such as exmaple.com similar to example.com. There is another type of domain squatting called the Internationalized Domain Name (IDN) homograph attack [9]. The IDN homograph attack causes users to visit malicious websites by exploiting Punycode [10], an encoding format to express Unicode characters as ASCII characters, such as Japanese characters. Alphabets with accents and other symbols are also represented in Punycode, such as exàmple.com corresponding to xn–exmple-jta.com in Punycode format. Domain squatting poses risks of personal information leakage and malware execution by leading users to fraudulent websites.

Another concern is the exploitation of DNS name resolution for malware communication. Malicious attackers often leverage domain generation algorithms [11] to prevent targets from detecting command and control communication. Additionally, information leakage by malware presents a significant risk [12].

Regarding the security of DNS management, the significance of redundancy of DNS servers to keep authoritative DNS servers working against Distributed Denial-of-Service (DDoS) attacks, such as a DNS water torture attack, has increased significantly [13]. Maintaining high redundancy of authoritative DNS servers is crucial, even for Handshake domains. This is because authoritative DNS servers manage the subdomain zone data of Handshake TLDs in the same manner as the current DNS, as discussed later.

B. Handshake Specifications

1) Handshake Client Specifications: The source code of the original Handshake client is forked from the Bitcoin client implementation, called bcoin [14]. Therefore, the Handshake blockchain is an independent blockchain with features, such as the consensus algorithm, similar to Bitcoin. For example, Handshake uses a proof-of-work consensus algorithm, unspent TX output and segregate witness TXs, which is used in Bitcoin. There are two types of Handshake client: full and light clients. A full client functions as a full blockchain node by storing all blockchain data. The primary full-client implementation is known as hsd [15]. In contrast, a light client operates as a simplified payment verification node, storing only blockchain headers. Additionally, there exists a specific type of light client designed solely for name resolution, consuming fewer machine resources, such as hnsd [16].

2) Name Resolution of Handshake Domains: The Handshake blockchain only manages the root zone data for Handshake TLDs[1], and running authoritative DNS servers is necessary for the TLDs and their subdomains, similar to the current DNS, as illustrated in Fig. 1[2]. Handshake TLDs are much more free and diverse than the current DNS TLDs. Typically, the current DNS SLDs become TLDs in Handshake.

Both the full and light clients can perform name resolution for Handshake domains[3]. The middle part of Fig. 1 depicts the full client's behavior for the name resolution of a Handshake domain. The web browser first sends a query (a.hns) to the full client. The full client then stores all blockchain data. Therefore, it omits querying root zone data of hns to the root servers. The full client can then perform name resolution procedures in the same manner as the recursive DNS server because the full client contains an embedded DNS resolver program. Finally, the full client returns the desired data to the web browser.

The bottom part of Fig. 1 depicts the light client's behavior for the name resolution of a Handshake domain. The web browser first sends a query (a.hns) to the light client. The light client then asks a peer for the root zone data of the Handshake domain because the light client does not store all the blockchain data. Both GETPROOF and PROOF messages are defined in the clients. The light client can verify PROOF messages containing the root zone data of hns by using stored blockchain header data. After obtaining the root zone data of hns, the light client conducts standard name resolution procedures using the embedded DNS resolver program. This domain can also

[1]TLDs and popular SLDs in the current DNS are reserved and claimable as Handshake TLDs, as mentioned earlier. Those claimed in the past can be found at https://web.archive.org/web/20230926222612/https://handshake.wtf/.

[2]Both the domains and IP addresses depicted are purely for illustrative purposes and are not related to existing data.

[3]Handshake clients have a fallback feature to resolve domain names in the current DNS in the case of failing name resolution of Handshake domains.

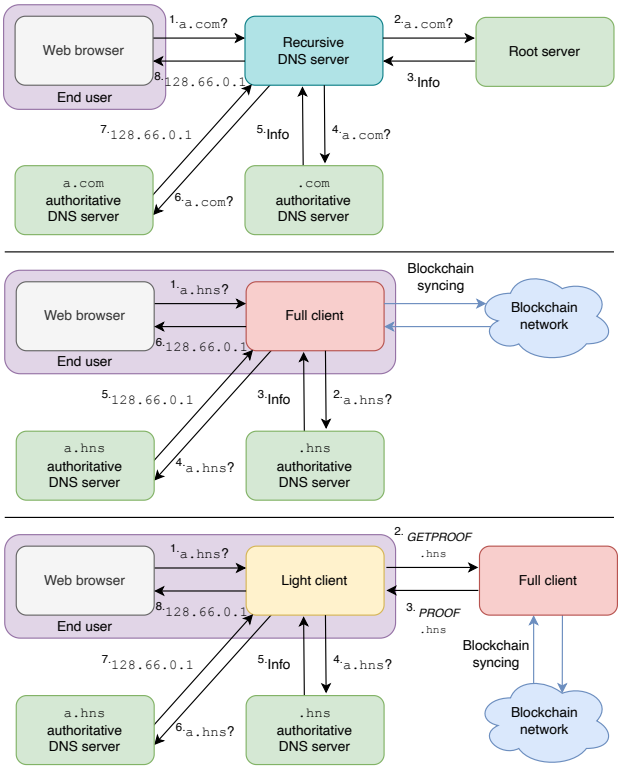

Fig. 1. Name resolution in the current DNS (top) and name resolution of Handshake domain with full client (middle) and light client (bottom)

TABLE I
Resource record types in Handshake blockchain

Record type	Corresponding DNS RRs	Content
DS	DS	Hash of DNSKEY
NS	NS	Authoritative DNS server name
GLUE4	NS & A	Glue record for IPv4
GLUE6	NS & AAAA	Glue record for IPv6
SYNTH4	NS & A	Glue record for IPv4 (shortened)
SYNTH6	NS & AAAA	Glue record for IPv6 (shortened)
TXT	TXT	Text

be resolved using third party services, such as HDNS [17], as the recursive DNS server of the current DNS. However, this is only recommended for experimental use because users are required to trust these third parties.

TABLE I presents the resource record (RR) [18] types for the root zone data in the Handshake blockchain. Note that this RR is different from the current DNS RR and is only used to store the root zone data in the blockchain. DS record is used for the same purpose (DNSSEC) as the DS record in the current DNS. The owner of a Handshake TLD can set up DNSSEC by configuring the appropriate DS records. A primary use case for DNSSEC in Handshake is DNS-based Authentication of Named Entities [19],

TABLE II
Covenant type and purpose

Covenant	Purpose
NONE	To send coin
CLAIM	To claim name
OPEN	To open auction
BID	To send auction bid
REVEAL	To reveal bid value
REDEEM	To redeem bid value
REGISTER	To register name
UPDATE	To update name data
RENEW	To renew name
TRANSFER	To transfer name
FINALIZE	To finish transfer
REVOKE	To revoke ownership

TABLE III
State type and meaning

State	Meaning
OPENING	Period until BIDDING
BIDDING	Period for bidding
REVEAL	Period for revealing
CLOSED	Auction closed
REVOKED	Name revoked
LOCKED	Name locked
TRANSFER	Name in transfer

to secure Transport Layer Security connections without relying on certificate authorities. Similarly, NS and TXT records are also used for the same purpose as these records in the current DNS. However, Handshake introduces some original record types. GLUE4 and GLUE6 records are used as the glue records, indicating the locations of authoritative DNS servers, corresponding with NS and A or NS and AAAA in the current DNS, respectively. SYNTH4 and SYNTH6 records are shortened versions of GLUE4 and GLUE6 records to reduce blockchain data size, respectively.

3) Auction System for Handshake Domains: We clarify below the auction procedure for Handshake TLDs. The registration of Handshake TLDs is managed by Covenant [20], an original function of the Handshake client akin to Ethereum's smart contract. All Handshake TXs contain both input and output Covenant types, with input and output flows corresponding to Covenant transitions. TABLE II lists the types of Covenant, while TABLE III outlines the types of Handshake TLD State, which indicates the status of Handshake TLDs related to the auctions and the ownership transfers. Handshake uses the Vickery auction system [21]. A Vickery auction is a sealed bid auction that the highest bidder pays the second-highest bid value after revealing bid values. To implement this sealed bid auction system on Handshake, bidders send TXs whose output Covenant is BID with an actual bid value and blind value[4]. The bidder does not pay[5] if only one bidder is present at the auction.

Fig. 2 illustrates an example of auction procedures. In this scenario, someone sends a TX whose output Covenant is OPEN for a Handshake TLD. After the TX is accepted in the blockchain, OPENING period begins. Any BID TXs cannot be accepted in the blockchain during this period. Following OPENING period ends within 36 blocks, BIDDING period begins. Here, we consider two bidders in the auction. The first and the second bidders send TX

[4]The sum of actual bid and blind value is called Lockup. The Lockup with zero bid value and non-zero blind value is accepted, and only bidders know the actual bid value until they reveal it using Reveal Covenant.

[5]Strictly speaking, a single bidder pays only TX fees.

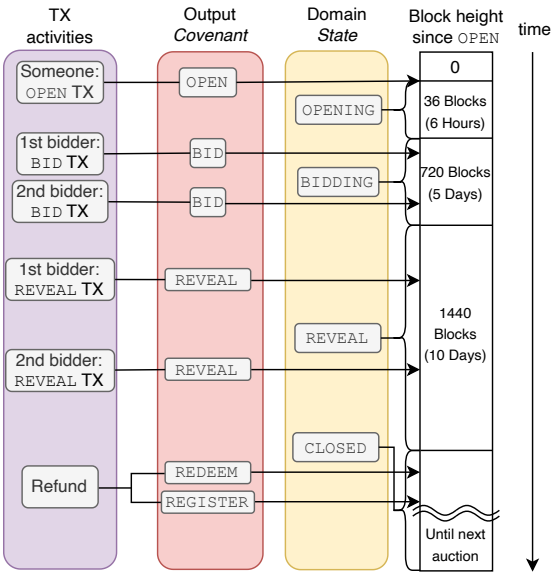

Fig. 2. Handshake TLD auction procedure

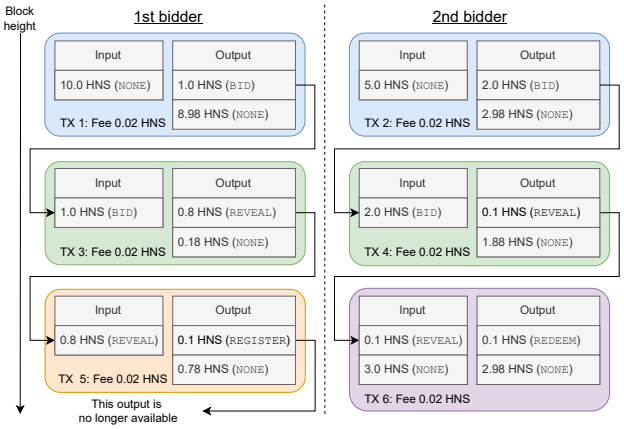

Fig. 3. TX flow in Handshake TLD auction

TABLE IV
Counts of Handshake TLDs per state

State	TLDs
OPENING	127
BIDDING	3,464
REVEAL	29,017
CLOSED	11,754,193
REVOKED	416
LOCKED	29
TRANSFER	0
Total	11,787,246

1 and TX 2, respectively (Fig. 3). Lockup values are 1.0 HNS[6] and 2.0 HNS. After BIDDING period ends, both bidders must send REVEAL TXs (TX 3 and TX 4) by letting outputs of BID TXs be inputs of TXs (Fig. 3). The actual bid values are 0.8 HNS and 0.1 HNS. Everyone can see the actual bid values and blind values are returned at this time. Once REVEAL period concludes, the auction ends, and the highest bidder pays the second-highest bid value. Any excess funds are returned through REGISTER and REDEEM TXs (TX 5 and TX 6) by letting the outputs of REVEAL TXs be inputs of TXs. As a result, the first bidder wins the Handshake TLD by paying 0.1 HNS, and no one can use the 0.1 HNS output anymore, namely, the output is burned. Please note that each TX requires a TX fee (0.02 in this case), and TLD ownership expires unless the owner submits a RENEW TX before the expiration limit (approximately two years).

III. Experiments

A. Methodology

We obtained Handshake blockchain data up to a height of 180,000 as of July 7th, 2023 UTC [22] for analysis by running hsd as a full client on our local machine. To address an issue related to the dumping of Handshake TLD data [23], we modified hsd[7]. Then, we prepared multiple Docker containers running the modified hsd and copied the blockchain data to each container for the experiment, as described below. At this time, the size of blockchain is more than 80 GB.

Fig. 4 depicts the experimental procedure. Here, we explain the procedure used to obtain RRs for each Handshake TLD. In the first step, we executed a specific API command to obtain all TLD data using the function of hsd. In the second step, we ran a script including a specific API command to extract RRs of each TLD. To reduce the experimental time, we created uniquely separated TLD lists from all TLD data and deployed multiple containers to extract multiple RRs in parallel. Following the merging of data, we analyzed the data using the scripts to obtain the results. We obtained the results other than Handshake TLD RRs using the same method. In the subsequent section, we present the results from three perspectives: TLD, TLD record, and auction analyses.

B. Results

1) TLD Analysis: First, TABLE IV illustrates the counts of Handshake TLDs appearing in the blockchain per State. A majority of the TLDs are in the CLOSED period, which indicates at least that the initial auction has concluded. Additionally, we obtained the total count of appeared Handshake TLDs, 11,787,246 which is approximately 8,000 times higher than the count of current DNS TLDs, equaling 1,470 [24]. The reason for this difference is that even random characters can be used for a TLD in Handshake. In other words, Handshake has an open and anti-censorship nature regarding TLD characters while the new TLD registration of the current DNS requires established meaning from common sense. We will discuss

[6]The primary unit of Handshake coin is HNS.

[7]The source code of the modified hsd used in our experiment will be available at https://github.com/k1s0b3/brains-2024.

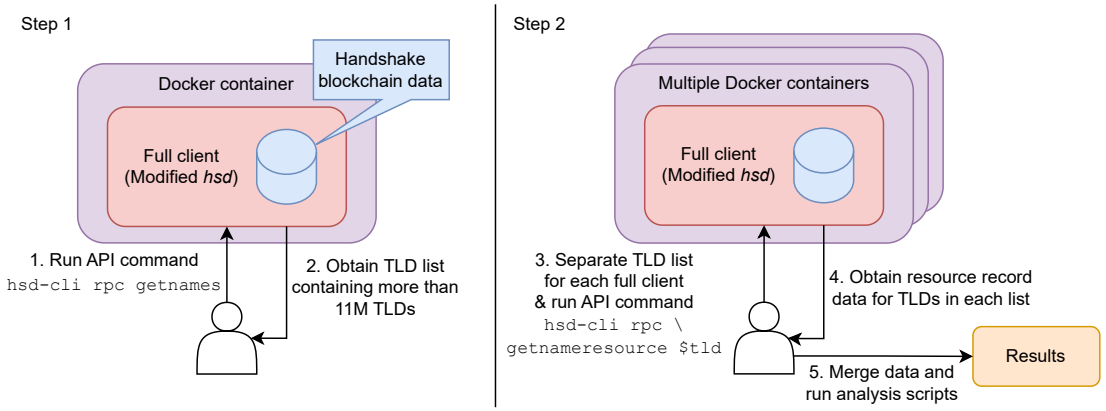

Fig. 4. Experiment procedure

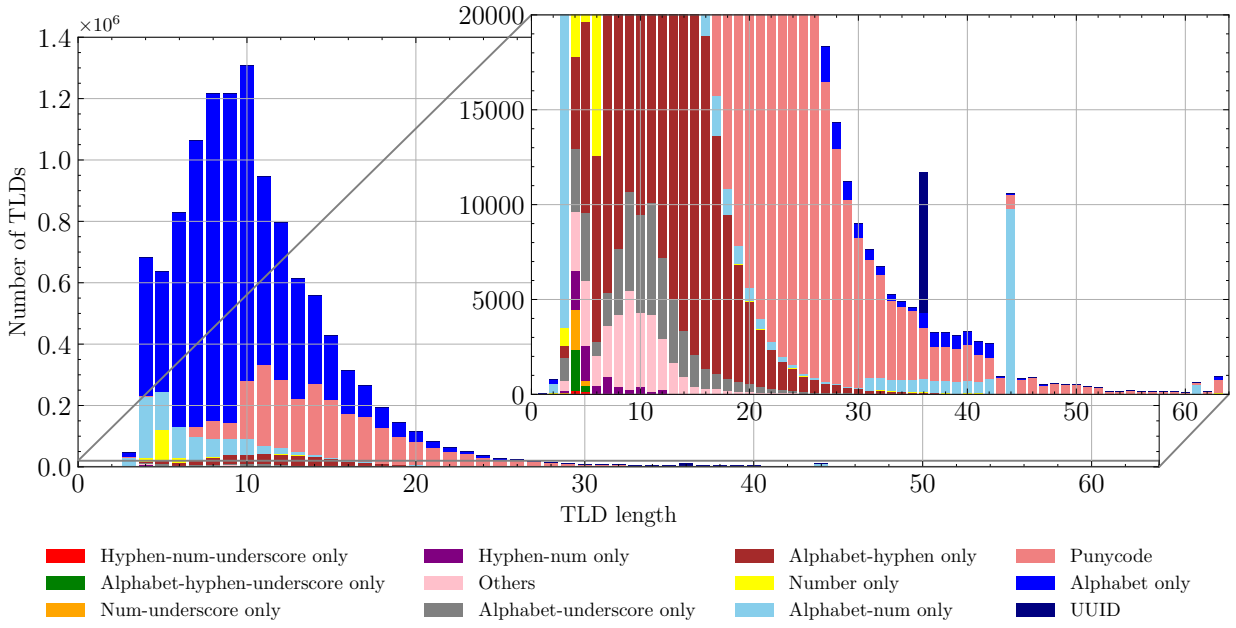

Fig. 5. TLD length and character classification

security concerns such as domain squatting related to the nature of Handshake later.

In view of these differences, we analyzed the characteristics of Handshake TLDs. Fig. 5 illustrates the length and character classification of Handshake TLDs. The x and y-axes represent the length of TLDs and the total count for each classification, respectively. We use the following labels for character classification, hyphen-num-underscore only such as 1_2-3, alphabet-hyphen-underscore only such as a_b-c, num-underscore only such as 1_2_3, hyphen-num only such as 1-2-3, others such as a_1-2, alphabet-underscore only such as ab_c, alphabet-hyphen only such as ab-c, number only such as 123, alphabet-num only such as abc123, Punycode such as xn–gckr3f0f, alphabet only such as abc, and Universally Unique Identifier (UUID) [25] such as 00000000-0000-0000-0000-000000000000. We have the following insights from Fig. 5:

- Alphabet-only TLDs constitute the majority.
- Generally, there is a declining trend beyond 10 characters.
- Numerous number-only TLDs exist within the 3–5 character length range, potentially posing compatibility issues with systems following the current DNS specifications.
- The proportion of Punycode TLDs exhibits a gradual increase, with a total count of 2,300,949.
- A significant number of alphabet-num-only TLDs are observed within the 31–42 character length range, possibly in encrypted or encoded formats.
- The count of hyphen-num-underscore only, hyphen-num only, alphabet-hyphen-underscore only, and num-underscore only TLDs is relatively small.

Additionally, 4 outliers exist:

- 36 length: UUID
- 44 length: Alphabet-num only (Possibility of encrypted, encoded or hash text)
- 61 length: Alphabet-num only (Possibility of encrypted, encoded or hash text)
- 63 length: Punycode (Text separated by underscores likely acquired for fun purposes)

Regarding the possibility of domain squatting on Handshake, two types of attack are considered in this analysis: attacks on legitimate[8] SLDs in the current DNS claimed as TLDs in Handshake, and attacks on legitimate TLDs in the current DNS. In other words, the first attack considers the similarity between Handshake domains, and the second attack exploits the similarity between Handshake domains and domains in the current DNS. We analyzed the Punycode TLDs of Handshake using an open source program, called IDN Homograph Detector [26], written in Python. This program receives a list of Punycode texts, legitimate names, and a dictionary of characters used for replacement as the inputs. The output of the program is Punycode texts, which become the legitimate names with at least one replacement of characters. It should be noted that we do not consider Punycodes that do not satisfy Internationalized Domain Names for Applications 2008 specifications [27] including Punycode usage for Internationalized Domain Names. We created a list of the legitimate names using the TLD list of the current DNS and selecting domain prefixes[9] from the top 1 million entries of the Tranco list [28], a domain popularity ranking dataset.

We used 1,318 unique TLDs[10] and 875,284 unique domain prefixes for our analysis, where the date of Tranco list corresponds to the same date as the blockchain data, namely, July 7th, 2023.

Fig. 6 illustrates the relationship between the popularity ranking of the legitimate names and Handshake Punycode TLDs similar to the legitimate names. Additionally, TABLE V reveals the top-counted Handshake Punycode TLDs similar to the legitimate names and total counts. From Fig. 6 and TABLE V, we find that the frequency concentrates on the specific names such as big tech companies and the counts exceeds 30,000. In particular, the count of navyfederal, which is not a big tech company, but a credit union in the U.S., is not normal. Therefore, we can infer that Handshake has significant concerns regarding domain squatting for specific names, even under the current circumstances. Fig. 7 illustrates the relationship between TLDs in alphabetical order and

[8]We use the word "legitimate" to refer to popular existing names in the current DNS.

[9]In this context, a domain prefix refers to the last subdomain part in the Tranco list. Namely, we exclude the part called effective TLD (eTLD) or public suffix. For example, google is the domain prefix (expected SLD) of google.com and google.co.jp. .co.jp is one of the eTLDs.

[10]Punycode TLDs already existing in the current DNS are excluded to avoid complication in the experiment.

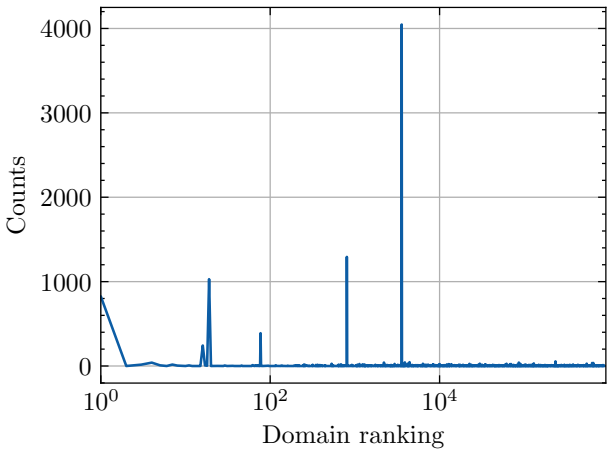

Fig. 6. Handshake Punycode TLD counts similar to the legitimate names (mostly SLDs in the current DNS)

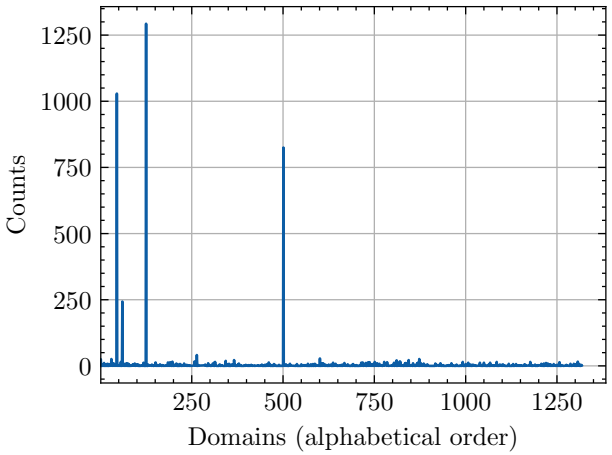

Fig. 7. Handshake Punycode TLD counts similar to TLDs in the current DNS

Handshake Punycode TLDs similar to legitimate TLDs. Please note that there are some overlaps of names with Fig. 6 because some domains such as amazon, apple, bestbuy and google have also their own TLDs in the current DNS.

2) TLD Record Analysis: We analyzed the resource records associated with Handshake TLDs stored on the blockchain. TABLE VI lists the counts of resource records stored on the Handshake blockchain. The total count of RRs is greater than that of existing TLDs because it is possible to save multiple records for one Handshake TLD.

GLUE4, GLUE6, SYNTH4, and SYNTH6 records include IP address data of authoritative DNS servers for TLDs. We extracted unique IP addresses from these records. Fig. 8 displays the frequency ranking of unique IP addresses in Handshake records. The x and y-axes are plotted on a logarithmic scale. The frequency of the top two IP addresses is approximately 9 million, accounting for a majority. Additionally, we found that a company called Namebase [29] owns authoritative DNS servers

TABLE V
The top-counted Handshake Punycode TLDs similar to legitimate names and total counts

Name	Counts	Ranking
navyfederal	4,047	3,571
bestbuy	1,293	804
amazon	1,029	19
google	825	1
paypal	389	77
apple	243	16
...	...	...
Total	31,771	-

TABLE VI
Counts of resource records stored on the Handshake blockchain

Record type	Counts
GLUE4	16,533,886
NS	16,592,649
DS	12,183,482
TXT	88,032
GLUE6	20
SYNTH4	5
SYNTH6	1

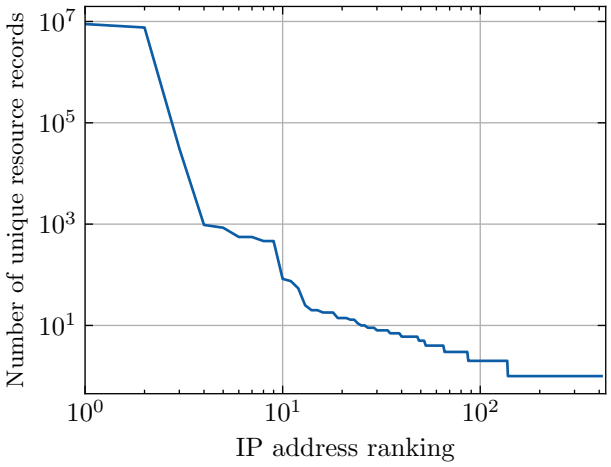

Fig. 8. Unique IP addresses ranking in Handshake records

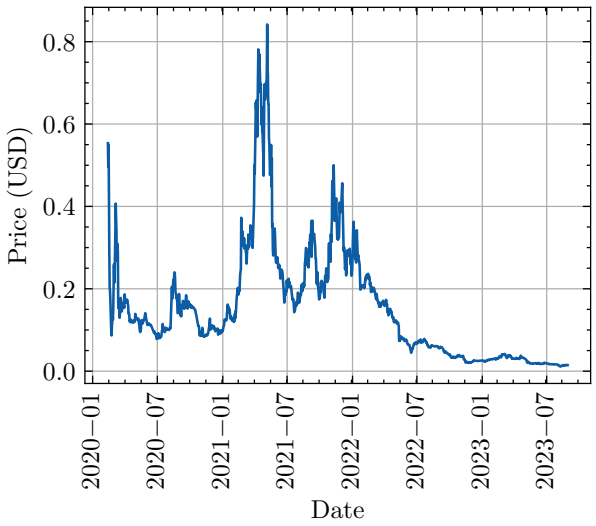

Fig. 9. Handshake coin rate

TABLE VII
Statistics of Handshake TLD cost
(TLDs sold at zero value are excluded for this calculation)

Statistic	HNS	USD
Average	15.33	2.35
90%ile	7.00	1.67
95%ile	20.00	4.27
99%ile	139.99	25.70
Standard deviation	787.98	95.93
Maximum	673,410.00	53,658.34
Total	32,058,714.15	4,907,306.36

associated with these two IP addresses. The Namebase provides a service for automated custodial participation in Handshake TLD auctions and the management of owned Handshake TLDs. Therefore, the concentration of IP addresses in the records stored on blockchain may be because Namebase assigns authoritative DNS servers for owning TLDs in a custodial manner. The concentration of TLD authoritative servers may become the target of DDoS attack, such as DNS water torture attack, and the suspension of name resolution owing to such attack is a critical issue for DNS. Based on the nature of the blockchain peer-to-peer network, it seems that the root zone redundancy is high in Handshake. However, the concentration of TLD authoritative servers may become an issue of server redundancy in reality, as presented in this result. This reminds us the fact that decentralization and distribution are two different concepts. If Handshake root zone is indeed decentralized, TLDs servers are however very poorly distributed. This contradicts the goal of building an infrastructure that is resilient in its entirety.

3) Auction Analysis: We estimated the auction costs of Handshake TLDs in U.S. dollar (USD). We use the historical exchange rate dataset of Handshake coin provided by Coingecko [30]. This dataset comprises the average exchange rate of cryptocurrency exchanges gathered by Coingecko. Fig. 9 reveals the exchange rate between HNS and USD. We obtained the following results below by converting HNS value to USD value using the rate at the end of the auction of each Handshake TLD.

TABLE VII presents the statistics of the auction costs (the actual paid value) for Handshake TLDs. The average, 90%ile, 95%ile and 99%ile of paid value in USD is considerably low. However, the maximum paid values in HNS and USD are remarkable, and we noticed these high price values in the data for .web3 and .b TLDs, respectively. These TLDs can be considered to be acquired for speculation or business in competitive auctions, although we have no clues about .b other than that a single-letter TLD is special because there is no single-letter TLD in the current DNS. Furthermore, the total value indicates the number of coins burned from the blockchain, suggesting a substantial value expended on Handshake TLDs. We excluded TLDs whose paid values are zero from the calculation, as most Handshake TLDs are sold for zero HNS, which would introduce noise into the average calculation.

TABLE VIII shows the auction results of the TLDs in TABLE V in terms of the auction price (i.e., the second highest bid value) and the highest bid value. The average,

TABLE VIII
Statistics of Handshake TLD cost in USD

Name	Avg. sold	Max. sold	Min. sold	Avg. highest bid	Max. highest bid	Min. highest bid
navyfederal	1.90	1,308.45	0.0	11.76	3,157.06	0.0
bestbuy	1.56	257.41	0.0	23.44	11,049.32	0.0
amazon	1.73	312.48	0.0	8.52	365.27	0.0
google	0.98	127.65	0.0	13.16	2,836.41	0.0
paypal	0.77	104.93	0.0	9.60	1,196.11	0.0
apple	2.91	179.20	0.0	12.56	381.04	0.0

max and min values are calculated from the bids for the TLDs that hold the possibility for domain squatting of popular names. As a result, we find that the average auction price is relatively low, allowing malicious actors to perform domain squatting.

IV. Discussion

We discuss the results by focusing on domain squatting, usage cost, and DNS redundancy, according to the countermeasures and new features of Handshake related to the issues.

A. Domain Squatting

We identified a certain risk of domain squatting on Handshake TLDs. In particular, two types of domain squatting against the similarity between Handshake domains, and that between the Handshake domain and the domain in the current DNS. While there are countermeasures in place to protect general users, such as generating a warning against the suspicious domains within web browsers, it is difficult to prevent the use of suspicious domains due to the anti-censorship nature of blockchain technology. There is a possibility that collaboration among Handshake blockchain miners could hinder certain Covenant activities on the blockchain, such as RENEW and UPDATE for existing TLDs, as well as OPEN for non-existing TLDs. However, such collaboration may lead to arbitrary control of the blockchain, which is not conducive to its governance.

Given the risk of domain squatting, it is crucial to pay attention to the soft fork[11] of the Handshake blockchain implemented on February 2, 2024. This soft fork alters the client behavior of specific reserved TLDs on Handshake. In particular, reserved TLDs that have not yet been claimed are partially expired [31], and such TLDs may be acquired by anyone participating in auctions. Given this context, it becomes increasingly important to safeguard general users from DNS abuse, such as domain squatting. Therefore, Handshake should not replace the current DNS without implementing countermeasures against domain squatting.

[11]Soft fork means a backward-compatible change of the client and the blockchain.

B. Usage Cost

In terms of usage cost, particularly the average auction cost, it is worth noting that it is not excessively high. However, making a direct comparison between the cost of Handshake TLDs and that of current DNS TLDs is not straightforward, primarily because current DNS TLDs are not typically sold to general users. Furthermore, owners of Handshake TLDs are required to renew their ownership until expiration, which may be accomplished by sending a RENEW TX with only the TX fee. Consequently, the total cost, including maintenance expenses, tends to be lower for most Handshake TLDs. Moreover, Handshake TLD owners may utilize subdomain registry services to monetize domain registration for subdomains. They can also leverage the secondary marketplace service for Handshake TLDs without auction on the blockchain[12]. Given such an environment that facilitates monetization, there are specific TLDs that are traded at higher prices, potentially for speculative purposes.

C. DNS Redundancy

Handshake TLD records stored on the blockchain reveal that authoritative DNS servers for most TLDs are managed by a single entity, Namebase, which provides the secondary marketplace for Handshake TLDs and automated auctions with custodial wallet services. This concentration raises concerns regarding a single point of failure, highlighting the need for high redundancy through technologies, such as load balancing. Due to this concentration, we opted not to analyze RRs managed by TLD authoritative servers but focused solely on the analysis of root zone RRs stored in the blockchain. Analyzing more than 11 million TLDs in the short term could be construed as a DDoS attack by the TLD authoritative servers.

As for countermeasures, one approach is for owners of Handshake TLDs to manage authoritative DNS servers themselves, which may reduce the dependence on a single management service. In the long term, promoting redundancy necessitates the existence of multiple management services operated by different entities, as managing DNS servers individually requires considerable effort.

[12]Namebase offers both of these services by leveraging custodial management of Handshake TLDs. Additionally, some third-party providers offer similar services, including Namecheap, which is one of the current DNS registrars and is the parent company of Namebase.

However, another countermeasure addresses the issue of lower redundancy through a new technology proposed for Handshake known as decentralized SLD (dSLD) [32]. Various dSLD deployments [33], [34] may be achieved by replacing TLD authoritative servers with smart contracts on platforms like Ethereum or Optimism [35], a layer 2 solution[13] for Ethereum.

V. Related Work

We focus on the emerging technology called blockchain-based DNS or blockchain-based naming services providing a name space similar to the current DNS, and refer to them as blockchain-based DNS for convenience.

Several studies have proposed new blockchain-based DNS [37]–[39]. Additionally, several measurement studies have examined blockchain-based DNS that have already been deployed. Kalodner et al. [40] reported the real-world usage and concerns surrounding Namecoin [41] providing domain names with .bit TLD not related to the current DNS. Namecoin domains can be used for the name resolution as DNS. Patsakis et al. [42] highlighted concerns regarding domain squatting in Namecoin and Emercoin [43] through an analysis of domain information in their blockchains. In Emercoin system, name resolution service is made available particularly for specific TLDs such as .coin and .emc not related to the current DNS. In addition, Xia et al. [44] provided domain statistics, such as auction costs and domain squatting concerns for the Ethereum Name Service (ENS) [45]. ENS provides domain names with the .eth TLD also not related to the current DNS. Although it mainly provides the conversion between domain names and Ethereum addresses, the data for the conversion can be extended to other resources. Additionally, concerns regarding malware communication using blockchain-based DNS have been raised. Randall et al. [7] analyzed these concerns, including Handshake record counts. While these security concerns should be addressed appropriately by the operators, performance concerns have also been raised. Our prior work [46] provided insights into the issue of higher name resolution latency on Handshake.

Handshake is currently a community-based project. Several implementations of Handshake blockchain explorers have been developed by community volunteers [47]–[50]. Moreover, live statistical data, including the total number of TLDs, are published by some community members [51]–[53]. However, there is limited research [7] on Handshake analysis using a snapshot of the Handshake blockchain. Furthermore, no prior work has evaluated Handshake TLD characters and domain squatting concerns quantitatively within the Handshake ecosystem. As we mentioned in the introduction, Handshake has unique features such as providing TLDs mainly for the same purpose as the current DNS, unlike other blockchain-based DNS. Therefore, we focus on Handshake and update the data reported in prior work [7]. Our research also includes a quantitative and comprehensive analysis of data that have not yet been reported on Handshake.

[13]A layer 2 is a separate blockchain that extends Ethereum and is used for solving a scaling problem of Ethereum [36]

VI. Conclusion

In this study, we analyzed the domain names and records in the Handshake blockchain as a blockchain-based DNS. Specifically, we conducted an analysis of existing TLDs on Handshake in terms of length and characters. Moreover, we evaluated concerns regarding malicious usage, including domain squatting, and identified a considerable number of Handshake TLDs that can be exploited for domain squatting, obtainable at low cost. Furthermore, we discussed the low redundancy of authoritative TLD servers managed by a single entity. In conclusion, we demonstrated that Handshake cannot and should not replace the current DNS in the future without addressing these issues. This could be achieved by introducing security measures for general users.

Future research will include a detailed analysis of the security risks considering the effects of new Handshake features, such as the modification of TLDs reservation (soft fork) and dSLD management. Additionally, we are considering conducting a more elaborate analysis of TLD similarity, including not only Punycodes but also normal ASCII characters. Furthermore, it is desirable to analyze the blockchain network and name resolution traffic for a deeper understanding of Handshake usage.

References

[1] "Ukraine asks ICANN to revoke Russian domains and shut down DNS root servers | Ars Technica," Accessed: Nov. 7, 2023. [Online]. Available: https://arstechnica.com/tech-policy/2022/03/ukraine-wants-russia-cut-off-from-core-internet-systems-experts-say-its-a-bad-idea/

[2] P. E. Hoffman, "DNS Security Extensions (DNSSEC)," RFC 9364, Feb. 2023, doi: 10.17487/RFC9364.

[3] "Handshake," Accessed: Jun. 26, 2023. [Online]. Available: https://handshake.org/

[4] "Home | ethereum.org," Accessed: Mar. 15, 2024. [Online]. Available: https://ethereum.org/en/

[5] "handshake-org/hs-names: Pre-reserved Handshake Names," Accessed: Jan. 31, 2024. [Online]. Available: https://github.com/handshake-org/hs-names

[6] "Handshake Developer Documentation: How to Claim a Name," Accessed: Jan. 31, 2024. [Online]. Available: https://hsd-dev.org/guides/claims.html

[7] A. Randall, W. Hardaker, G. M. Voelker, S. Savage, and A. Schulman, "The challenges of blockchain-based naming systems for malware defenders," in Proc. 2022 APWG Symposium on Electronic Crime Research (eCrime), 2022, pp. 1–14, doi: 10.1109/eCrime57793.2022.10142131.

[8] P. Agten, W. Joosen, F. Piessens, and N. Nikiforakis, "Seven months' worth of mistakes: A longitudinal study of typosquatting abuse," in Proc. the 22nd Network and Distributed System Security Symposium, 2015, doi: 10.14722/ndss.2015.23058.

[9] H. Suzuki, D. Chiba, Y. Yoneya, T. Mori, and S. Goto, "ShamFinder: An automated framework for detecting IDN homographs," in Proc. the ACM Internet Meas. Conf. (IMC), 2019, pp. 449–462, doi: 10.1145/3355369.3355587.

[10] A. M. Costello, "Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)," RFC 3492, Mar. 2003, doi: 10.17487/RFC3492.

[11] M. Antonakakis, R. Perdisci, Y. Nadji, N. Vasiloglou, S. Abu-Nimeh, W. Lee, and D. Dagon, "From throw-away traffic to bots: Detecting the rise of DGA-based malware," in Proc. the 21st USENIX Security Symposium (USENIX Security 12), Aug. 2012, pp. 491–506.

[12] N. Ishikura, D. Kondo, V. Vassiliades, I. Iordanov, and H. Tode, "DNS tunneling detection by cache-property-aware features," IEEE Trans. Netw. Service Manag., vol. 18, no. 2, pp. 1203–1217, 2021, doi: 10.1109/TNSM.2021.3078428.

[13] K. Hasegawa, D. Kondo, M. Osumi, and H. Tode, "Collaborative defense framework using FQDN-based allowlist filter against DNS water torture attack," IEEE Trans. Netw. Service Manag., vol. 20, no. 4, pp. 3968–3983, 2023, doi: 10.1109/TNSM.2023.3277880.

[14] "bcoin-org/bcoin: Javascript bitcoin library for node.js and browsers," Accessed: Nov. 8, 2023. [Online]. Available: https://github.com/bcoin-org/bcoin

[15] "handshake-org/hsd: Handshake Daemon & Full Node," Accessed: Nov. 7, 2023. [Online]. Available: https://github.com/handshake-org/hsd

[16] "handshake-org/hnsd: Handshake SPV name resolver," Accessed: Nov. 7, 2023. [Online]. Available: https://github.com/handshake-org/hnsd

[17] "HDNS - Handshake DNS," Accessed: Nov. 7, 2023. [Online]. Available: https://www.hdns.io/

[18] "Handshake Developer Documentation: Handshake Resource Record Guide," Accessed: Jan. 19, 2024. [Online]. Available: https://hsd-dev.org/guides/resource-records.html

[19] P. E. Hoffman and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA," RFC 6698, Aug. 2012, doi: 10.17487/RFC6698.

[20] "Handshake Developer Documentation: Handshake Protocol Summary," Accessed: Mar. 15, 2024. [Online]. Available: https://hsd-dev.org/protocol/summary.html

[21] W. Vickrey, "Counterspeculation, auctions, and competitive sealed tenders," The Journal of Finance, vol. 16, no. 1, pp. 8–37, 1961, doi: 10.2307/2977633.

[22] "Block 180000," Accessed: Jan. 30, 2024. [Online]. Available: https://www.niami.io/block/180000/

[23] "Node RPC getnames Response Exceeds Limit · Issue #447 · handshake-org/hsd," Accessed: Jun. 26, 2023. [Online]. Available: https://github.com/handshake-org/hsd/issues/447

[24] "tlds-alpha-by-domain.txt," Accessed: Jul. 7, 2023. [Online]. Available: https://data.iana.org/TLD/tlds-alpha-by-domain.txt

[25] P. J. Leach, R. Salz, and M. H. Mealling, "A Universally Unique IDentifier (UUID) URN Namespace," RFC 4122, Jul. 2005, doi: 10.17487/RFC4122.

[26] "varrickkoh/IDN-Homograph-Detector: Detect IDN homographs and phishing domains," Accessed: Jan. 27, 2024. [Online]. Available: https://github.com/varrickkoh/IDN-Homograph-Detector

[27] J. C. Klensin, "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework," RFC 5890, Aug. 2010, doi: 10.17487/RFC5890.

[28] V. L. Pochat, T. Van Goethem, S. Tajalizadehkhoob, M. Korczyński, and W. Joosen, "Tranco: A research-oriented top sites ranking hardened against manipulation," in Proc. the 26th Network and Distributed System Security Symposium, 2019, doi: 10.14722/ndss.2019.23386.

[29] "TLD Registry + HNS Exchange for Decentralized Web | Namebase," Accessed: Nov. 7, 2023. [Online]. Available: https://www.namebase.io/

[30] "Handshake Price: HNS Live Price Chart, Market Cap & News Today | CoinGecko," Accessed: Nov. 7, 2023. [Online]. Available: https://www.coingecko.com/en/coins/handshake

[31] "icann lockup soft fork - Add 10k alexa to the soft-fork. by nodech · Pull Request #828 · handshake-org/hsd," Accessed: Mar. 12, 2024. [Online]. Available: https://github.com/handshake-org/hsd/pull/828

[32] "namebasehq/decentralized-slds: Handshake Decentralized SLDs," Accessed: Nov. 7, 2023. [Online]. Available: https://github.com/namebasehq/decentralized-slds

[33] "Impervious Domains," Accessed: Nov. 7, 2023. [Online]. Available: https://impervious.domains/

[34] "HNS.ID," Accessed: Nov. 7, 2023. [Online]. Available: https://hns.id/

[35] "Optimism," Accessed: Mar. 12, 2024. [Online]. Available: https://www.optimism.io/

[36] "Layer 2 | ethereum.org," Accessed: Jul. 29, 2024. [Online]. Available: https://ethereum.org/en/layer-2/

[37] W. Wang, N. Hu, and X. Liu, "BlockZone: A blockchain-based DNS storage and retrieval scheme," in Proc. the 5th International Conference on Artificial Intelligence and Security, 2019, pp. 155–166, doi: 10.1007/978-3-030-24268-8_15.

[38] W. Liu, Y. Zhang, L. Liu, S. Liu, H. Zhang, and B. Fang, "A secure domain name resolution and management architecture based on blockchain," in Proc. 2020 IEEE Symposium on Computers and Communications (ISCC), 2020, pp. 1–7, doi: 10.1109/ISCC50000.2020.9219632.

[39] L. Jin, S. Hao, Y. Huang, H. Wang, and C. Cotton, "DNSonChain: Delegating privacy-preserved DNS resolution to blockchain," in Proc. 2021 IEEE 29th International Conference on Network Protocols (ICNP), 2021, pp. 1–11, doi: 10.1109/ICNP52444.2021.9651951.

[40] H. A. Kalodner, M. Carlsten, P. M. Ellenbogen, J. Bonneau, and A. Narayanan, "An empirical study of namecoin and lessons for decentralized namespace design," in Proc. the 14th Annual Workshop on the Economics of Information Security, 2015, pp. 1–23.

[41] "Namecoin," Accessed: Jun. 26, 2023. [Online]. Available: https://www.namecoin.org/

[42] C. Patsakis, F. Casino, N. Lykousas, and V. Katos, "Unravelling ariadne's thread: Exploring the threats of decentralised DNS," IEEE Access, vol. 8, pp. 118 559–118 571, 2020, doi: 10.1109/ACCESS.2020.3004727.

[43] "Official website of Emercoin blockchain platform." Accessed: Jan. 31, 2024. [Online]. Available: https://emercoin.com/

[44] P. Xia, H. Wang, Z. Yu, X. Liu, X. Luo, G. Xu, and G. Tyson, "Challenges in decentralized name management: the case of ENS," in Proc. the 22nd ACM Internet Meas. Conf. (IMC), 2022, pp. 65–82, doi: 10.1145/3517745.3561469.

[45] "Ethereum Name Service," Accessed: Jun. 26, 2023. [Online]. Available: https://ens.domains/

[46] K. Isobe, D. Kondo, and H. Tode, "A first look at the name resolution latency on handshake," in Proc. the 22nd ACM Internet Meas. Conf. (IMC), 2022, pp. 756–757, doi: 10.1145/3517745.3563024.

[47] "niami.io | Rating Handshake Domains," Accessed: Jan. 29, 2024. [Online]. Available: https://www.niami.io/

[48] "Handshake explorer — 3xpl," Accessed: Jan. 29, 2024. [Online]. Available: https://3xpl.com/handshake

[49] "HNS Explorer," Accessed: Jan. 29, 2024. [Online]. Available: https://e.hnsfans.com/

[50] "Blocks List," Accessed: Jan. 29, 2024. [Online]. Available: https://hnsnetwork.com/

[51] "Statistics - Handshake (HNS) Explorer," Accessed: Jan. 29, 2024. [Online]. Available: https://hns.cymon.de/stats

[52] "Stats | The Shake," Accessed: Jun. 26, 2023. [Online]. Available: https://theshake.xyz/stats

[53] "Stats | Namebase," Accessed: Jan. 29, 2024. [Online]. Available: https://www.namebase.io/stats/