İSTANBUL UNIVERSITY CERRAHPAŞA

ORIGINAL ARTICLE
Electrica 2025; 25: 1-8

Blockchain Based Ownership and Domain Name System Configuration With Ethereum Rollups

Farhad Asgarov, Fatih Said Duran, Namig Samadov, Şerif Bahtiyar

Department of Computer Engineering, Istanbul Technical University Faculty of Computer and Informatics Engineering, Maslak, Istanbul, Türkiye

Cite this article as: F. Asgarov, F. S. Duran, N. Samadov and Ş. Bahtiyar, "Blockchain based ownership and DNS configuration with ethereum rollups," *Electrica*, 25, 0051, doi: 10.5152/electrica.2025.25005.

WHAT IS ALREADY KNOWN ON THIS TOPIC?

- *Blockchain provides decentralized trust and security.*
- *Cyber attacks on DNS affect the society considerably.*
- *Ethereum is one of the widely used blockchain with advanced properties.*

WHAT THIS STUDY ADDS ON THIS TOPIC?

- *We introduce an innovative use of Ethereum rollups for a DNS registry, providing an affordable and scalable solution for the Internet.*
- *The proposed solution improves the privacy of DNS records.*
- *We evaluate the performance of a domain management on both Ethereum Mainnet and ZKsync.*

Corresponding author:
Şerif Bahtiyar

E-mail:
bahtiyars@itu.edu.tr

Received: March 28, 2025
Revision requested: June 11, 2025
Last revision received: July 30, 2025
Accepted: August 18, 2025
Publication Date: November 21, 2025

DOI: 10.5152/electrica.2025.25005

Content of this journal is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ABSTRACT

Traditional centralized domain name systems (DNS) are vulnerable to security attacks such as DNS spoofing and DNS cache poisoning. Additionally, centralized DNS authorities may impose access restrictions that limit authentication mechanisms; therefore, the centralized nature of the system can significantly impact society. In this research, the limitations of centralized DNS systems are addressed by proposing a new decentralized DNS approach using blockchain rollups. The approach is implemented on an Ethereum rollup using ZKsync. This approach leverages smart contracts to enable secure and cost-effective domain management. Analysis results show that the proposed solution enhances Internet security across all phases of DNS execution that demonstrates the benefits of an immutable and decentralized approach to domain management.

***Index Terms*—**Blockchain, domain name system (DNS), ethereum, rollup, ZKsync

I. INTRODUCTION

A domain name system (DNS) is a crucial component of the internet. It translates user-friendly website names into computer-readable Internet Protocol (IP) addresses. However, the centralized architecture of traditional DNS systems makes them vulnerable to cyberattacks, which may compromise data integrity, availability, and confidentiality. There has been significant research interest in using blockchain technology to address these security challenges. Originally developed for cryptocurrencies, such as Bitcoin, blockchain technology offers a decentralized, immutable, and transparent ledger system, which may help to transform DNS security paradigms.

One of the risks associated with centralized DNS registries is the creation of a single point of failure, which may have catastrophic results for Internet communications. This risk also enables governments and other organizations to filter and manage content for users, such as restricting access to information. Additionally, centralized DNS systems may be exploited for substantial data collection and surveillance, which leads to privacy concerns. Specifically, computing systems are vulnerable to security attacks that may disrupt services, such as DNS spoofing, DNS cache poisoning, and distributed denial of service (DDoS) attacks. Thus, decentralized DNS solutions may reduce the risk of attacks and strengthen Internet security.

In this research, a novel approach that utilizes Ethereum rollup technologies to address challenges of implementing a decentralized DNS registry on Ethereum mainnet is proposed. Key performance limitations on mainnet include access speed and transaction cost, both of which significantly impact the deployment of new contracts to the blockchain. Additionally, modifying deployed contracts incurs substantial performance penalties. This approach improves performance in terms of both speed and cost by leveraging an Ethereum rollup technology called ZKsync. Main contributions of this research are as follows:

- An innovative use of Ethereum rollups is introduced for a DNS registry, providing an affordable and scalable solution for the Internet.
- The proposed solution improves the privacy of DNS records.

- The performance of domain management is evaluated on both Ethereum mainnet and ZKsync.

The rest of the paper is organized as follows. Section II discusses DNS and Ethereum. The next section introduces the decentralized DNS registry on Ethereum rollups. Section IV presents analyses. The final section is dedicated to the conclusion and future work.

II. DOMAIN NAME SYSTEM AND ETHEREUM

The domain name system is a hierarchical, decentralized naming system for computers, services, or any resource connected to the Internet or a private network [1]. It translates domain names, which are human-readable identifiers of resources, into numerical IP addresses required to locate and identify these resources using network protocols. The domain name system operates through a distributed database of resource records organized in a tree-like structure. Top-level domain (TLD) servers, managed by organizations such as International Corporation for Assigned Names and Numbers (ICANN), oversee authoritative DNS records for each domain extension. Domain name system resolution occurs through a recursive process involving queries between client machines, local DNS servers, authoritative DNS servers, and root DNS servers. This structure enables efficient and accurate navigation across the internet.

Domain name systems are subject to numerous security threats arising from technical vulnerabilities and malicious activities, including malware attacks. To mitigate these threats, DNS Security Extensions (DNSSEC) were proposed in 1997 [2] to authenticate DNS records and enhance overall security. Additional measures, such as intrusion detection systems and firewalls, are also used to monitor and protect the DNS infrastructure against attacks.

Although DNSSEC ensures the authenticity of DNS responses, it does not provide confidentiality, as responses are authenticated without encryption. Additionally, the process of signing and verifying digital signatures introduces delays in query responses, thereby affecting user satisfaction. Furthermore, challenges related to the implementation and management of DNSSEC remain significant. Large-scale DNS measurements and experiences with domain purchases from major registrars reveal operational challenges and inconsistencies in registrar policies that hinder DNSSEC adoption [3]. Moreover, the complexities of deploying DNSSEC with third-party DNS operators, such as Cloudflare, underscore the need for improved mechanisms to streamline deployment processes and enhance overall security within the DNS ecosystem.

The integration of blockchain technology with DNS has received significant attention in recent years to address several critical shortcomings of the current DNS infrastructure [4, 5]. Blockchain offers inherent properties such as decentralization, immutability, and transparency, which may enhance security, reliability, and trust within the DNS ecosystem. Leveraging blockchain for domain name registration and resolution reduces reliance on centralized authorities, helping to mitigate risks of single points of failure, manipulations, or censorship.

Smart contracts deployed on blockchain networks enable automated and verifiable domain registrations, ownership transfers, and resolution processes, streamlining administrative procedures while ensuring data integrity. In addition, blockchain-based DNS solutions offer improved resistance to DNS spoofing, cache poisoning, and other malicious activities, fostering a more resilient and trustworthy internet infrastructure [6, 7]. For example, a secure, decentralized, and human-readable naming system is based on Zooko's Triangle [8], emphasizing the importance of decentralization in promoting resilience and censorship resistance.

Blockchain-based DNS initiatives assert that such systems fulfill the criteria of Zooko's Triangle. Namecoin is one of the earliest examples of a blockchain-based DNS [4]. It operates on a blockchain with additional functionality that is specifically designed for DNS applications. In the Namecoin network, domain names are stored on the blockchain alongside transactions that allow users to register and manage domain names without relying on a central authority. This is achieved by associating domain names with cryptographic keys, which enables users to prove ownership and securely manage their domains. However, Kalodner et al. [9] identified scalability and usability challenges in Namecoin, while authors in [7] highlighted limitations such as inadequate support and low adoption, which result in insufficient computing power.

Blockstack is a decentralized DNS system [10] that operates on the Bitcoin blockchain to enable a user-controlled domain registration and management. Scalability remains a key challenge for Blockstack due to inherent limitations in the transaction throughput and the block size on Bitcoin's public blockchain. Similarly, Handshake is a decentralized naming protocol that establishes a censorship-resistant, blockchain-based DNS infrastructure intended to replace traditional DNS and certificate authorities [11]. However, a major obstacle for Handshake is interoperability in the case of broader adoption, which presents a significant challenge for the traditional hierarchical DNS.

Security enhancements and attack mitigation strategies in a blockchain-based DNS have attracted significant attention from the research community. Yıldız et al. [12] propose a trust-based DNS system to prevent eclipse attacks on blockchain networks. B-DNS introduces a proof-of-stake consensus protocol and a four-layer architecture to mitigate DDoS attacks while reducing computational overhead. Additionally, it improves query efficiency compared to both traditional DNS and other blockchain-based DNS solutions.

Ethereum name service (ENS) [5] functions as an open system that accommodates a diverse array of records. It primarily serves to associate domain names with blockchain addresses and decentralized websites. Ethereum name service enables users to register and manage domain names ending with ".eth." It operates through a hierarchical structure, with TLDs that are managed by ENS registry contracts on the Ethereum blockchain. However, instances of domain name squatting, malicious decentralized websites, and scam addresses within ENS records highlight ongoing security challenges [13]. Additionally, [14] explores mechanisms involving squatting, elliptic curve cryptography, and first-price sealed-bid auctions. The model incorporates smart contract functionality to prevent unauthorized modifications and ensure fair insurance pricing aligned with market values. A significant challenge in ENS remains that of high and unpredictable gas fees during periods of network congestion, which may make operations such as domain registration, updates, and transfers prohibitively expensive.

Unstoppable domains [15] is an Ethereum-based name service that provides user-controlled, censorship-resistant domain names. Like ENS, it is affected by high gas fees during periods of network

congestion. BlockZone [16] is another Ethereum-based DNS storage system that employs a practical byzantine fault tolerance consensus algorithm and smart contracts. This system outperforms DNSSEC and PoW-based alternatives in terms of parsing, authentication, and network efficiency. These studies demonstrate that blockchain-based DNS solutions have the potential to enhance the security and privacy of DNS infrastructure. On the other hand, they are not yet fully mature. In this research, the state of the art is extended in decentralized DNS registries using blockchain technology.

To summarize outcomes of the analyses, systems such as Namecoin, ENS, and Blockstack that have pioneered decentralized DNS solutions have been elaborated, but they contain significant challenges, such as scalability, interoperability, and operational costs. This solution builds upon these foundations by utilizing rollup technology to offer a more scalable, cost-efficient, and adaptable DNS architecture that effectively integrates with the broader blockchain ecosystem. Table I provides a comparative analysis of the most prominent blockchain-based DNS platforms alongside the proposed solution, which highlights key differences in performance, cost, and functionality.

III. DECENTRALIZED DOMAIN NAME SYSTEM REGISTRY ON ETHEREUM ROLLUP

The main challenge in the centralized domain name registration is its reliance on centralized DNS providers, which are responsible for securing domain data and registration information, such as two-factor authentication. However, centralized providers remain vulnerable to various attacks, putting domains at risk. A more effective way to minimize this risk is to migrate to decentralized name services, which are typically built using open-source technologies and undergo thorough security audits.

Ethereum offers a pathway to migrate to a more secure, decentralized name service since it is a modular and programmable blockchain [17]. It is open to everyone for building decentralized applications. The primary requirement is to develop a smart contract using a designated programming language, such as Solidity, and then deploy it to the network. Once deployed, the smart contract code is distributed across Ethereum nodes, making it globally accessible. However, since the network is open to all, scalability has emerged as one of Ethereum's most significant challenges in recent years. This challenge is currently being addressed by introducing an additional layer on top of the main network, known as a rollup. The primary function of rollups is to batch transactions efficiently within this secondary layer and transmit the resulting state changes to the Ethereum mainnet. The architecture of the proposed system is shown in Fig. 1, which illustrates how users interact with a DNS registry contract deployed on an Ethereum rollup called ZKsync. The figure also shows how these changes are synchronized with the main Ethereum network.

Recently, Ethereum rollups have seen substantial advancements, establishing themselves as highly optimized environments for smart contract deployments. Transaction speeds are significantly improved. Moreover, network fees are remarkably low. Ethereum improvement proposal (EIP) 4844 [18], also known as Proto-Danksharding, introduces near-zero fees for simple state changes on Ethereum rollups. The impact of Proto-Danksharding on ZKsync's on-chain costs is illustrated in Fig. 2. EIP-4844 went live on ZKsync on March 13, 2024.

In this research, a decentralized approach is proposed for storing and querying DNS records on ZKsync. A DNS registry smart contract is also designed and deployed on the ZKsync network. Initially, the existing DNS registration process was replicated that allows users to assume ownership of specific domains and manage various record types, including adding, removing, and modifying the records. The smart contract manages ownership records for a domain using any Ethereum wallet, which is identified by a 20-byte hexadecimal address [17]. The subscription mechanism for a domain registration, where an Ethereum wallet can be registered on a domain by paying only the network fee, is beyond the scope of this research.

A. Domain Registration

We utilize the ZKsync network to perform basic operations such as registering a new subdomain, adding a new record, or deleting an existing record. To register a new subdomain, the client application must be connected to the decentralized application that manages domain registrations. This connection is established through any blockchain wallet that has access to the ZKsync Main Network.

B. Adding, Updating, and Deleting a Domain Name System Record

The core part of the domain management begins after the registration process is completed. Capabilities of a domain registry are defined through various record types added by a domain manager. Different DNS record types serve different purposes that allow administrators to manage the domain functionality more effectively. By leveraging these records, administrators can enhance control over the domain performance and services, which increases the overall flexibility and efficiency of domain management.

TABLE I. COMPARISON OF EXISTING DECENTRALIZED DOMAIN NAME SYSTEM PLATFORMS AND PROPOSED ROLLUP-BASED APPROACH

	Namecoin	Blockstack	ENS	ZKsync (Proposed)
Blockchain	Namecoin	Bitcoin	Ethereum layer 1	Ethereum layer 2
Gas cost	Medium	Medium	High	Very low
Speed	Low	Low	Medium	Very high
Sponsored transactions	No	No	No	Yes
Adoption	Very low	Low	Very high	Growing
AA support	No	No	Yes	Yes (native)

AA, account abstraction; ENS, ethereum name service.

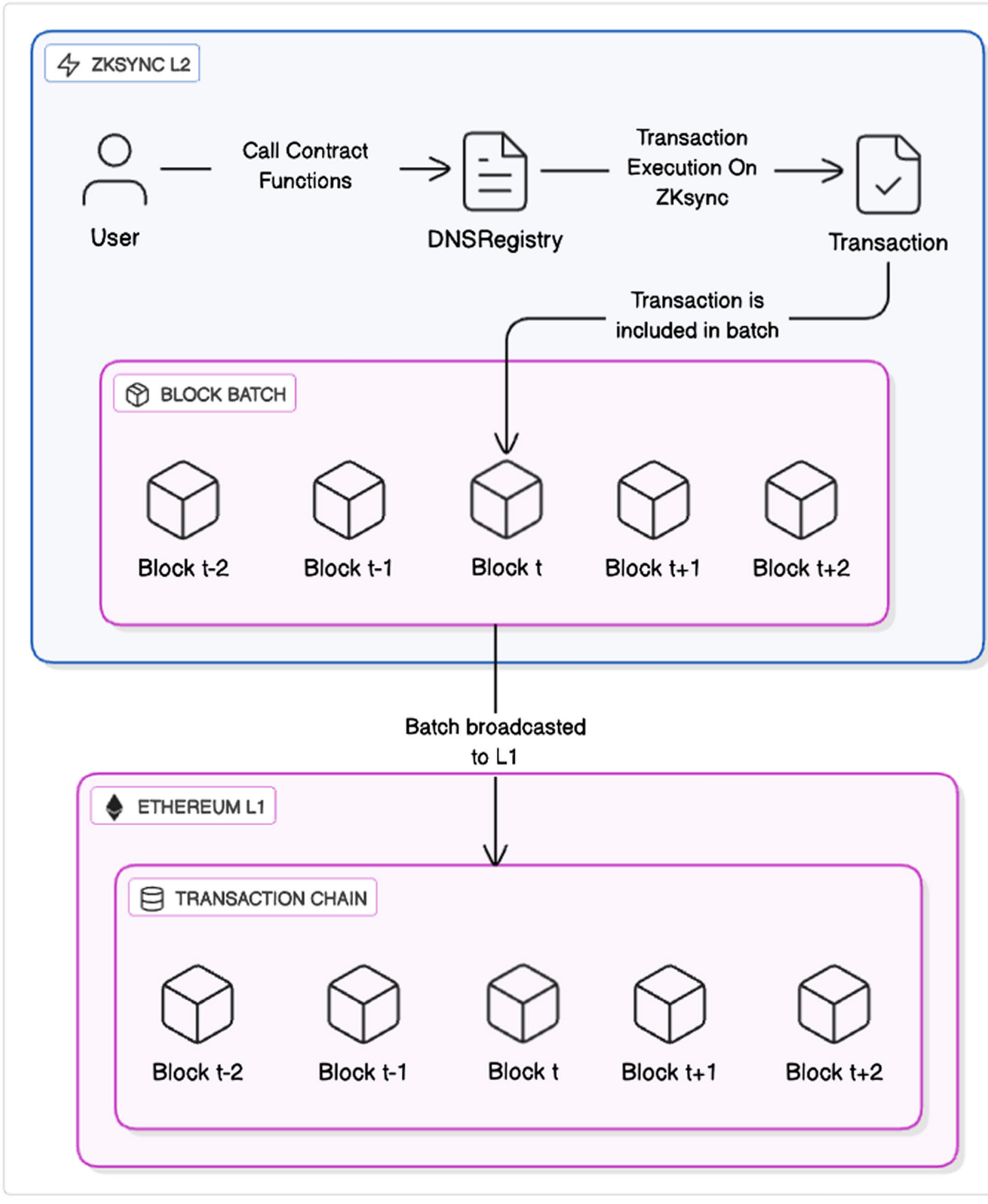


Fig. 1. Architecture of the proposed domain name system registry using ZKsync rollups. User interactions are executed on Layer 2 and they are settled on the Ethereum mainnet.

C. Querying Domain Name System Records

Once a domain is registered, specific records can be added to the network. These records are queried using a smart contract. Querying a record is a straightforward process that is executed through a contract call, which is a globally accessible read operation.

D. Data Structures

We utilize Solidity to define the DNS registry contract interface and necessary data storage structures. This setup facilitates a decentralized DNS management in the proposed approach. Key components of the data model include:

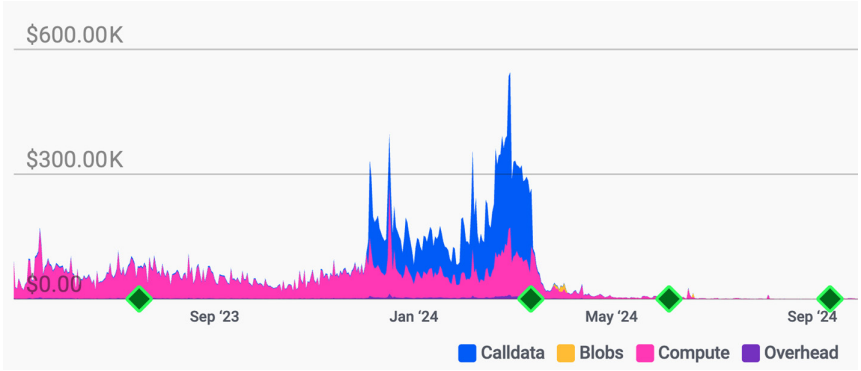


Fig. 2. On-chain transaction cost components on ZKsync before and after EIP-4844. The update on March 13th significantly reduced calldata and compute fees [19].

- Domain name system record storage: A mapping is used to associate domain names with their corresponding records. Each record contains a data field that stores the content of the DNS entry and an existing flag, which indicates whether the record is active.
- Domain ownership management: Another mapping structure maintains ownership information, linking each domain to its registered owner's address.

By structuring data in this way, the implementation ensures efficient domain resolution and ownership verification while it maintains decentralized control over DNS records.

E. Events

Events are broadcast to the blockchain network to record state updates and track the history of public changes. They serve as an efficient mechanism for logging and retrieving important actions in the DNS management process. Key events in the implementation include:

- Domain registration: When a new domain is registered, an event logs the domain name and its owner's address.
- Domain name system record management: Several events facilitate the tracking of record modifications.
- Record addition: Logs the creation of a new DNS record, including the domain name, a record type, and associated data.
- Record update: Captures updates to existing DNS records that provide details about the modified record type and its new content.
- Record deletion: Logs the removal of a DNS record, which specifies the affected domain and record type.

By incorporating these events, the system ensures transparent and verifiable DNS operations while it enables efficient tracking of domain-related activities.

IV. ANALYSES

We analyzed the cost, speed, and security of the proposed approach to highlight its contributions.

A. Cost Analysis

Due to Ethereum's persistently high transaction costs on Layer 1 (L1), the blockchain community is actively exploring scalable alternatives. As illustrated in Fig. 3, the average transaction cost on the Ethereum mainnet was $2.70 during the period from June 2024 to June 2025. [20].

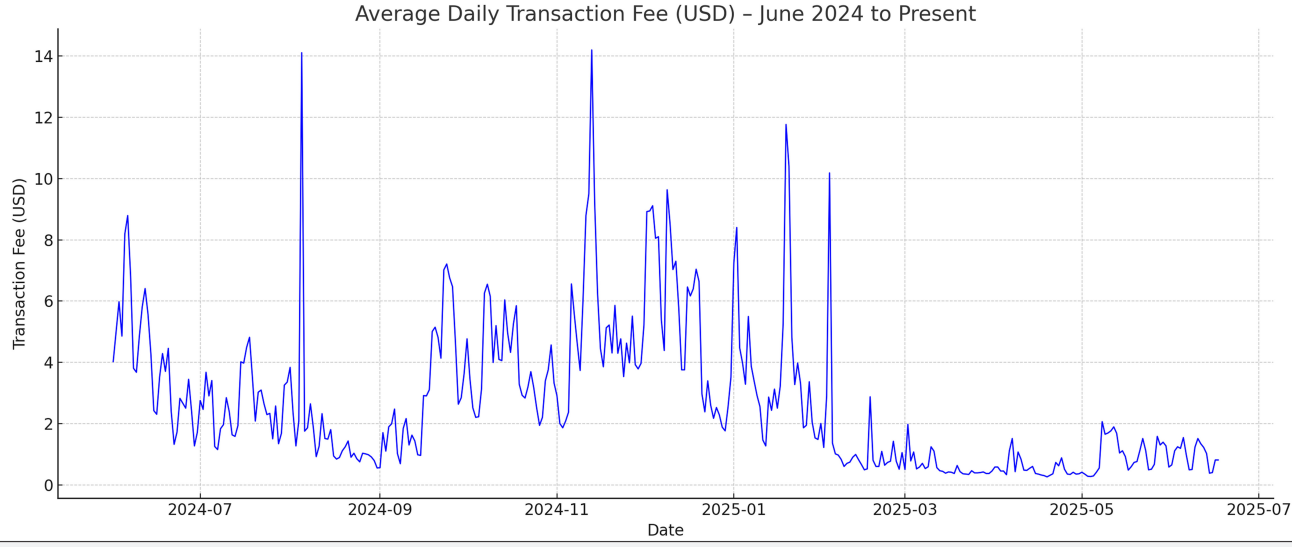


Fig. 3. Average transaction costs (USD) on Ethereum mainnet. Higher Layer 1 fees motivate the use of rollups for scalable domain name system operations.

Rollups provide a large decrease in fees for Ethereum users. Owing to improved data compression and the absence of containing signatures, Optimism and Arbitrum offer rates that are three to eight times lower than the base layer. On the other hand, zero-knowledge (ZK) rollups offer even larger cost savings with fees that are 40 to 100 times lower than the base layer. ZKsync is one of the pioneers of ZK rollups, which is why it is preferred in this solution. In general, the cost optimization on ZKsync can be modeled in (1):

$$C_{tx} = \frac{F_{rollup}}{N} \tag{1}$$

where, C_{tx} is the cost per transaction on ZKsync. F_{rollup} is the total gas fee for the rollup batch, and N is the number of transactions in the batch. The difference between the proposed solution and Ethereum mainnet is computed in (2).

$$R = \frac{C_{mainnet} - C_{tx}}{C_{mainnet}} \times 100 \tag{2}$$

where, $C_{mainnet}$ is the cost per transaction on Ethereum mainnet and R is the cost reduction as a percentage.

The average cost of registering, updating, and modifying entries in the DNS registry is presented in Table II. Following the Proto-Danksharding update [18], the network fees required to perform specific operations on the DNSRegistry contract have dropped to approximately $0.01 per action. The combined cost of registering a new subdomain, adding the necessary DNS records, and modifying them costs roughly $0.06 per user.

B. Speed Analysis

The average execution speed of DNSRegistry function calls highlights the advantages of the ZKsync rollup solution compared to Ethereum mainnet as shown in Table III. While the Ethereum mainnet produces one block every 12 seconds, ZKsync generates one block per second. This makes ZKsync approximately 12 times faster than the Ethereum mainnet for executing write functions. In this solution, the throughput efficiency of ZKsync is modeled in (3).

TABLE II. AVERAGE COST OF CALLING STATE CHANGER FUNCTIONS FROM DOMAIN NAME SYSTEM REGISTRY CONTRACT

Method	ZKsync Cost	Mainnet Cost
Registration of each new domain	$0.03	$6.00
Addition of each new record	$0.02	$4.00
Modification of single record	$0.01	$3.00

TABLE III. AVERAGE REQUIRED TIME FOR CALLING DOMAIN NAME SYSTEM REGISTRY CONTRACT FUNCTIONS

Method	ZKsync Cost	Mainnet Cost
Registration of each subdomain	1 second	12 seconds
Addition of each new record	1 second	12 seconds
Modification of single record	1 second	12 seconds
Querying a record	0.3 seconds	1 second

$$T_{effective} = T_{rollup} \times N \tag{3}$$

- $T_{effectice}$: Total transactions per second processed by the rollup.
- T_{rollup}: Total transactions per second of the rollup layer.
- N: Average number of transactions in a batch.

Throughput improvement compared to Ethereum mainnet (ΔT) is calculated with (4):

$$\Delta T = T_{effective} - T_{mainnet} \tag{4}$$

Although response times are influenced by factors such as connection speed, geographic location, and overall network activity, an average of one second per transaction was observed. For example, adding a new record typically takes around one second. In contrast, view functions, which are used for reading the blockchain state, are significantly faster, with an average read time of approximately 300 milliseconds. These performance results support the viability of implementing a decentralized DNS registry using rollup technology instead of relying on the Ethereum mainnet.

C. Access Control

A decentralized domain registration process eliminates the need for a central authority at all stages. Every operation related to a domain registration and record management is executed through blockchain wallets. An access control mechanism for managing domain records is essential and must be carefully designed. While incorporating a multi-signature structure offers the highest level of security, a single signature is generally sufficient for individual users. Accordingly, the smart contract implements a single signature check before executing operations. The contract ensures that only the domain owner can perform state-changing actions. This is enforced by using modifiers in the Solidity programming language, specifically the onlyOwner modifier, which restricts the transaction execution to the contract owner.

D. Security

Security is a core motivation behind the proposed decentralized DNS system, particularly due to the known vulnerabilities in traditional DNS infrastructure. In this research, we present common attacks that use vulnerabilities, and how this system mitigates them using blockchain and ZK rollups is explained.

- Domain name system spoofing and cache poisoning: In traditional DNS, attackers can forge responses or poison caches to redirect users to malicious sites. In this system, DNS records are stored on-chain, and they are verified by ZK rollups, which generate cryptographic proofs to confirm that only valid updates are accepted. This circumstance prevents forged entries from being processed, securing DNS responses at the protocol level.
- Unauthorized modifications: Centralized name servers can be breached or misused to alter domain records. This system uses smart contracts with strict ownership checks that are enforced through blockchain wallets. Zero-knowledge rollups ensure that only transactions with valid proofs are posted on-chain. Even if a rollup operator is compromised, unauthorized modifications cannot pass verification.
- Censorship and data control: Traditional DNS providers can be influenced by governments or corporations to block domain access. By decentralizing the DNS management on a public blockchain, reliance on any single authority is eliminated. Zero-knowledge rollups allow efficient and secure state updates that preserve openness while maintaining data correctness.

- Distributed denial of service attacks: Centralized DNS servers are frequent targets of denial of service attacks that can disrupt access. This architecture avoids reliance on any single point of failure. Since domain queries are simple read operations on the blockchain and rollup state, they are highly resistant to traffic-based attacks and do not expose a centralized endpoint.

The DNS configuration stored on the blockchain cannot be altered without access to the private key of the blockchain wallet that holds domain ownership. Due to the decentralized nature of the domain registration process, there is no need to trust centralized authorities. Properly designing modular DNS registry contracts and deploying them on Ethereum rollups significantly reduces operational costs.

E. Comparison of Domain Registration Approaches

The DNS configuration inside the blockchain cannot be changed without accessing the private key of the blockchain wallet, which has the domain ownership. Owing to the decentralized structure of the domain registration process, centralized authorities are not trusted. Properly building modular DNS registry contracts and running them on Ethereum rollups reduces the cost.

Since the blockchain and layer 2 technologies are relatively new, future improvements in the blockchain ecosystem will make them more convenient and beneficial. Even today, the observations have shown promising results with low cost and high speed. The comparison of centralized and decentralized DNS registries is shown in Table IV.

F. Sponsored Transactions

Domain owners should have access to a frictionless interface to enable seamless integration with a decentralized DNS registration system. One of the key advantages of the ZKsync rollup is its support for an account abstraction, which allows user transactions to be sponsored [21]. To enable sponsorship, a gasless paymaster contract must be developed and deployed on the ZKsync network. If the contract is funded and the paymaster logic is correctly configured, network fees can be paid by the contract itself. This functionality is made possible by ZKsync's native support for an AA. Traditionally, externally owned accounts (EOAs), which are wallets controlled by a single private key, do not support sponsored transactions or AA features. However, in ZKsync, EOAs are natively implemented as smart contract wallets. As a result, running a decentralized DNS registry on the ZKsync network enables transaction sponsorship even when the user interacts with a standard EOA. This feature is also expected to become available on other Ethereum rollups through the introduction of EIP-7702 [22].

TABLE IV. OVERALL COMPARISON OF CENTRALIZED AND DECENTRALIZED DOMAIN NAME SYSTEM REGISTRIES

	Centralized DNS Registry	**Decentralized DNS Registry**
Ownership	Centralized authority	Individual peers
Registration costs	Adjusted by centralized authority	Programmable and permissionless
Modification	Free	Network fee
Modification time	Instant	Almost instant
Transfer	Secured by central authority	Peer-to-peer

DNS, domain name system.

V. CONCLUSION AND FUTURE WORK

Deploying the smart contract on Ethereum rollups and ensuring compatibility with existing DNS administration tools are essential for the practical implementation of a decentralized DNS registry. A user-friendly approach that enhances both security and usability is proposed by abstracting the complexity of blockchain transactions and enabling users to manage their domains in a manner similar to conventional systems. Moreover, AA and sponsored transactions in the proposed architecture further improve the user experience of DNS management.

The proposed decentralized DNS registry system can be deployed alongside existing DNS infrastructure in real-world scenarios. By leveraging Ethereum rollups, it is possible to achieve a scalable architecture that is capable of handling an increasing DNS query demand while maintaining low costs and fast transaction speeds. Furthermore, interactions between users and domain administrators can be made seamless. As future work, the smart contract architecture may be further optimized by implementing caching mechanisms and exploring novel consensus models.

Data Availability Statement: The data that support the findings of this study are available on request from the corresponding author.

Peer-review: Externally peer-reviewed.

Author Contributions: Concept – F.A., F.S.D., N.S., Ş.B.; Design – F.A., F.S.D., N.S., Ş.B.; Supervision – Ş.B.; Resources – F.A., F.S.D., N.S.; Materials – F.A., F.S.D., N.S.; Analysis and/or Interpretation – F.A., F.S.D., N.S., Ş.B.; Literature Search – F.A., F.S.D., N.S.; Writing – F.A., F.S.D., N.S., Ş.B.; Critical Review – F.A., F.S.D., N.S., Ş.B.

Declaration of Interests: The authors have no conflicts of interest to declare.

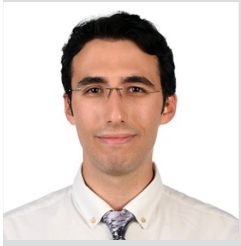
Funding: The authors declare that this study received no financial support.

REFERENCES

1. P. Mockapetris, and K. J. Dunlap, "Development of the domain name system," in *Proc. Symp. Commun*, *Architectures and Protocols*, 1988, pp. 123–133.
2. T. Chung et al., "A longitudinal, end- to-end view of the DNSSEC ecosystem," in *Proc. 26th USENIX Security Symp. (USENIX Security '17)*, 2017, pp. 1307–1322.
3. T. Chung et al., "Understanding the role of registrars in DNSSEC deployment," in *Proc. 2017 Internet Measurement Conf. (IMC)*. New York, NY, USA: ACM, 2017, pp. 369–383. [CrossRef]
4. Namecoin. [Online]. Available: https://www.namecoin.org/. [Accessed: Dec. 26, 2024].
5. *ENS Domains*. [Online]. Available: https://ens.domains/. [Accessed: Dec. 26, 2024].
6. Y. Liu, Y. Zhang, S. Zhu, and C. Chi, "A comparative study of blockchain-based DNS design," in *Proc. 2019 2nd Int. Conf. Blockchain Technol. Appl.* New York, NY, USA: ACM, 2019, pp. 86–92. [CrossRef]
7. G. Giamouridis, B. Kang, and L. Aniello, "Blockchain-based DNS: Current solutions and challenges to adoption," in *Proc. 6th Distrib. Ledger Technol. Workshop*, 2024, (DLT2024).
8. A. Swartz, "Squaring the triangle: Secure, decentralized, human-readable names." [Online]. Available: http://www.aaronsw.com/weblog/squarezooko. [Accessed: Dec. 26, 2024].

9. 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. workshop Econ.," *Inf. Secur. (WEIS)*, vol. 1, no. 1, pp. 1–23, 2015.
10. M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains," in *Proc. 2016 USENIX Annu. Tech. Conf. (USENIX ATC)*, 2016.
11. *Handshake, Handshake* Paper. [Online]. Available: https://hsddev.org/files/handshake.txt. [Accessed: Dec. 26, 2024].
12. A. K. Yıldız, A. Atmaca, and O. Solak, Y. C. Tursun, and S. Bahtiyar. "A trust-based DNS system to prevent eclipse attacks on blockchain networks," in *Proc. 2022 15th Int. Conf. Security Inf, Networks (SIN)*, pp. 1–8, 2022.
13. P. Xia et al., "Challenges in decentralized name management: The case of ENS," in *Proc. 22nd ACM Internet Measurement Conf.* New York, NY, USA: ACM, 2022, pp. 65–82. [CrossRef]
14. W.-Y. Lin, K.-Y. Tai, and F. Y.-S. Lin, "A trustable and secure usage-based insurance policy auction mechanism and platform using blockchain and smart contract technologies," *Sensors (Basel)*, vol. 23, no. 14, p. 6482, 2023. [Online]. [CrossRef]
15. W. Rehman, H. e Zainab, J. Imran, and N. Z. Bawany, *"NFTs: Applications and challenges," in Proc. 2021 22nd Int. Arab Conf. Inf. Technol. (ACIT)*, 2021, pp. 1–7.
16. W. Wang, N. Hu, and X. Liu, "Blockzone: A blockchain-based DNS storage and retrieval scheme," in *Proc. Int. Conf. Artif. Intell. Secur.*, X. Sun, Z. Pan, and E. Bertino, Ed. Berlin: Springer, 2019, pp. 155–166. [CrossRef]
17. V. Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform* White Paper, 2014. [Online]. Available: https://ethereum.org/whitepaper. [Accessed: Dec. 26, 2024].
18. V. Buterin et al., "EIP-4844: Shard blob transactions," *Ethereum Improv. Proposals*, no. 4844, Feb. 2022. [Online serial]. Available: https://eips.ethereum.org/EIPS/eip-4844.
19. "L2BEAT, 'zkSync era,' scaling projects," 2024. [Online]. Available: https://l2beat.com/scaling/projects/zksync-eraonchain-costs. [Accessed: Jan. 6, 2025].
20. "Average transaction fee in USD," *Etherscan*. [Online]. Available: https://etherscan.io/chart/avg-txfee-usd. [Accessed: Jan. 06, 2024].
21. K. Chin, K. Emura, and K. Omote, *"An anonymous yet accountable contract wallet system using account abstraction," arXiv Preprint*, 2023. (arXiv:2309.03480).
22. V. Omote, V. Buterin, and A. Dietrichs, and lightclient, "EIP-7702: Set EOA account code [DRAFT]," 2024. [Online serial], *Ethereum Improvement Proposals*, no. 7702. Available: https://eips.ethereum.org/EIPS/eip-7702.

Farhad Asgarov is pursuing a bachelor's degree in Computer Engineering at Istanbul Technical University. He is a blockchain software engineer at Clave, where he works on developing self-custodial smart contract wallets. His research interests primarily focus on account abstraction and Ethereum rollups, contributing to the advancement of scalable and secure blockchain technologies.



Fatih S. Duran obtained a B.S. degree from the Department of Computer Engineering at Istanbul Technical University in 2024. He is currently an M.S. student there. He is currently working as a research assistant at MEF University. He is an active researcher part of the Artificial Intelligence & Robotics Laboratory at ITU. Moreover, he collaborates with BASIRA and SPF Labs for medical data.

Namig Samadov is a master's student in the Department of Accounting, Financial Management, and Control at Bocconi University. He earned a Bachelor's degree in Computer Engineering from Istanbul Technical University in 2024. His current research focuses on blockchain technology, decentralized finance, and algorithmic trading.

Dr. Şerif Bahtiyar is a professor in the Department of Computer Engineering at Istanbul Technical University. He received his BS in Control and Computer Engineering and MS in Computer Engineering degrees both from Istanbul Technical University, respectively, and his PhD degree in Computer Engineering from Boğaziçi University. Dr. Bahtiyar was with MasterCard, TU Berlin in Germany, and the National Research Institute of Electronics and Cryptology. Dr. Bahtiyar is the founder and director of the Cyber Security and Privacy Research Laboratory, SPF LAB, at Istanbul Technical University. His current research includes cyber security and privacy, mobile systems, trust modeling, machine learning, e-health, and financial systems.