Blockchain-based DNS: Current Solutions and Challenges to Adoption

George Giamouridis[1], BooJoong Kang[1] and Leonardo Aniello[1]

[1]School of Electronics and Computer Science, University of Southampton, UK

Abstract

The Domain Name System (DNS) is a fundamental component responsible for the translation of domain names into IP addresses. Traditional DNS relies on centralised authorities for domain registration and resolution, raising concerns about censorship, security, and trust. In response to these challenges, blockchain-based DNS (BDNS) solutions have emerged, promising decentralisation, security, and resilience. This paper reviews existing works on BDNS and their potential to transform the domain name landscape. Each BDNS solution is analysed in terms of its objectives, operational mechanisms, supported Top Level Domains (TLD) and limitations. The state of the art of BDNS is discussed to identify the key challenges hindering its widespread adoption, ranging from technical difficulties (scalability, performance, integration with existing infrastructure) to security concerns, and to governance and regulatory considerations.

Keywords

Blockchain, Blockchain DNS, Domain Name System, Decentralisation

1. Introduction

The DNS is a hierarchical, distributed database that enables the resolution of domain names to IP addresses on the Internet. It is implemented through a hierarchy of multiple servers, also known as Name Servers, that work together to resolve domain names.

The traditional DNS architecture suffers from numerous problems. One notable issue is the vulnerability to several cyberattacks, including distributed denial-of-service (DDoS) attacks as well as other attacks such as cache poisoning attacks that can potentially lead to integrity concerns. These vulnerabilities arise primarily due to the centralised nature of the traditional DNS, where a single point of failure can compromise the entire system. Additionally, the traditional DNS lacks transparency and accountability. Indeed, the decision-making processes regarding domain registrations, updates, and resolutions often occur within the closed circles of domain registrars, leaving end-users with limited visibility into how these decisions are made. These weaknesses highlight the urgent need for innovative solutions to strengthen the security, resilience, and trustworthiness of the DNS ecosystem.

In response to these vulnerabilities, several approaches have been proposed. One such solution involves implementing security extensions such as Domain Name System Security Extensions (DNSSEC) [1] to authenticate DNS responses and prevent data tampering. While DNSSEC

g.giamouridis@soton.ac.uk (G. Giamouridis); b.kang@soton.ac.uk (B. Kang); l.aniello@soton.ac.uk (L. Aniello)

DLT2024: 6th Distributed Ledger Technologies Workshop, May, 14-15 2024 - Turin, Italy

strengthens the integrity of DNS data, its adoption remains limited due to complexity and compatibility issues. Another solution relies on the deployment of Content Delivery Networks (CDNs) [2] and Anycast routing [3] to help mitigate the impact of DDoS attacks by distributing DNS queries across multiple servers. However, these solutions primarily focus on addressing specific attack vectors and do not fundamentally address the centralised nature of traditional DNS. Moreover, they often entail increased operational complexity and costs [4], which limits their widespread adoption. As such, while these solutions offer additional improvements to DNS security, they fall short of providing a comprehensive and decentralised approach to address the broader spectrum of DNS security.

Blockchain-based DNS (BDNS) introduces blockchain technology to address the limitations of the traditional DNS architecture. Blockchain is a decentralised and immutable ledger that records transactions across a network of nodes securely and transparently. By applying blockchain principles to DNS, BDNS eliminates the reliance on centralised authorities, thus mitigating the risk of single points of failure and enhancing the system's resilience against cyberattacks. Moreover, BDNS provides a tamper-proof record of domain ownership and associated DNS records, strengthening transparency and accountability in the domain registration process. Through the use of smart contracts and cryptographic techniques, BDNS enables automated and trustless domain management. Furthermore, BDNS offers the potential to address concerns related to censorship and domain ownership conflicts (e.g trademark disputes or expired domains) by providing a decentralised and censorship-resistant infrastructure.

The integration of blockchain technology into the DNS protocol represents a significant advancement in functionality and security. Several alternatives to BDNS have been proposed to date. One novel contribution of this paper is to provide a comprehensive overview of currently active and notable BDNS solutions, explaining their primary objectives, functionalities, and limitations. Additionally, this paper contributes with a unique discussion of the BDNS landscape and the primary factors limiting its potential for widespread adoption.

The rest of the paper is organised as follows. Section 2 introduces the basics of DNS and blockchain. Existing academic works that review the state of the art of BDNS are discussed in Section 3. An extensive analysis of existing BDNS solutions is presented in Section 4. Section 5 identifies the main challenges to the adoption of BDNS. Finally, Section 6 concludes the paper.

2. Background

2.1. The Domain Name System (DNS)

DNS serves as a fundamental component of the Internet infrastructure, translating human-readable domain names into IP addresses, enabling users to access websites and services consistently. Introduced by Paul Mockapetris in 1983, DNS has played a crucial role in simplifying the user experience by replacing numerical IP addresses with easily memorable domain names. DNS operates on a hierarchical and centralised model, where a set of authoritative servers (name servers) manage domain name records for specific zones. DNS data (DNS records) is stored in local databases but is available worldwide. DNS is an application layer protocol that allows computers, hosts, routers, and name servers to communicate and resolve names (translate names

into IP addresses). DNS-lookup is a basic function of the protocol, performed by any machine or service, and results from remote name servers are temporarily stored in local memory to improve performance.

DNS Structure. Figure 1 highlights the hierarchical structure of DNS [5], representing the various levels of domain names within its architecture. At the top of the DNS hierarchy, there is the root domain, represented by a dot ("."). Below the root domain, there are top-level domains (TLDS), such as generic TLDs (.com, .org) and country-code TLDs (.us, .uk). Further down the hierarchy, there are second-level domains (SLDs) and subdomains provide additional specificity to individual addresses. DNS records, including essential types like A (address), AAAA (IPv6 address), MX (mail exchange), and CNAME (canonical name) [6], store information associated with domain names. Authoritative name servers, distributed across the internet, play a crucial role in storing and managing these DNS records for specific domains or zones. Resolver servers, operated by internet service providers or end-users, interact with authoritative servers to retrieve the necessary DNS information, thereby facilitating the seamless resolution of domain names to their corresponding IP addresses.

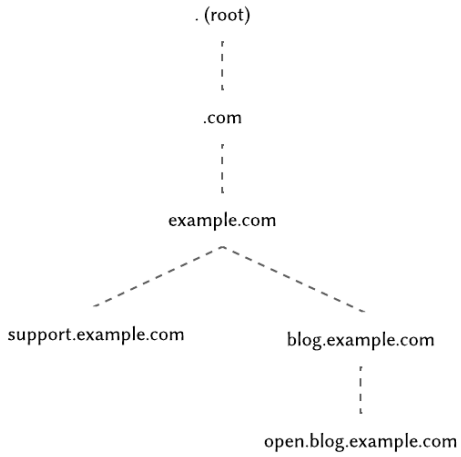

Figure 1: The hierarchical structure of DNS

DNS Governance DNS governance involves a multifaceted framework that defines the policies, protocols, and management of the DNS. The Internet Corporation for Assigned Names and Numbers (ICANN) plays a central role in managing the global coordination of the DNS. ICANN manages the assignment of unique identifiers, such as domain names and IP addresses, ensuring their coherent and organised distribution [7]. Within the ICANN structure, various supporting organisations and advisory committees contribute to policy development, addressing technical, operational, and ethical aspects of DNS management. Additionally, the Internet Assigned Numbers Authority (IANA) is responsible for the allocation and assignment of various DNS parameters and protocol identifiers. DNS governance is characterised by a multi-stakeholder

model, involving input from governments, industry stakeholders, technical experts, and the broader Internet community. This collaborative approach aims to strike a balance between maintaining the stability and security of the DNS while encouraging inclusivity and transparency in decision-making processes.

The DNS Protocol. DNS operates on a client-server model and employs a hierarchical and distributed protocol to simplify the translation of domain names into IP addresses [8]. When a stub resolver (integrated into the end user's device) requests a domain name in a web browser or any other application, a DNS query is initiated. The process begins with the stub resolver contacting a local DNS resolver as shown in Figure 2, typically provided by an Internet Service Provider (ISP). If the resolver possesses the requested information in its cache, it returns the corresponding IP address directly to the user's device, expediting the resolution process.

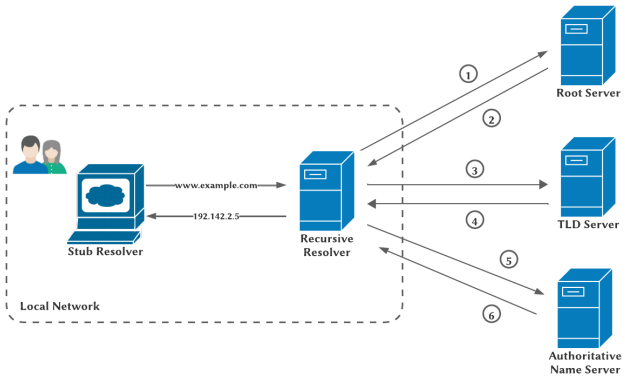

Figure 2: The DNS protocol

If the requested domain name is not found in the local cache or the cache entry has expired, the resolver acts recursively. It queries root DNS servers to determine the authoritative DNS server responsible for the TLD of the requested domain name (e.g., ".com", ".org"). After receiving a response from the root DNS server specifying appropriate the TLD server, the resolver queries the TLD server for information about the domain name's authoritative name server. Once the resolver receives a response from the TLD server with the IP address of the authoritative DNS server, it queries the authoritative DNS server for the IP address of the domain name's authoritative name server.

Once the authoritative name server provides the IP address, the recursive resolver caches this information to optimise subsequent queries for the same domain. The IP address is then relayed to the user's device, enabling it to establish a connection with the desired web server.

Domain Name Registration. Domain name registration involves the process through which individuals or entities acquire the rights to use a specific domain name within the DNS. This process is demonstrated in Figure 3 where registries, under the oversight of the IANA and administered by ICANN, are responsible for managing TLDs such as '.com' and '.net'. Their primary function involves the maintenance of records about domain ownership, attributing individual domains to respective registrants, whether they be individuals or organisations. This hierarchical structure defines the distribution of responsibilities within the DNS, ensuring the

orderly management of Internet resources.

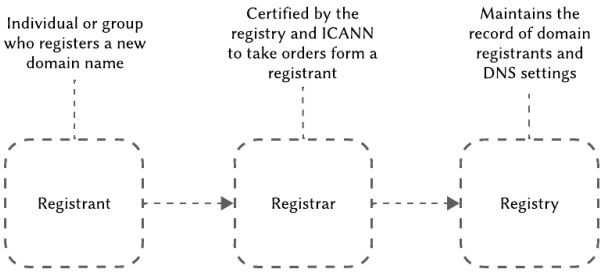

Figure 3: The domain name registration process

Registrars, act as intermediaries between end-users (registrants) and registries, and are responsible for performing transactions related to domain registrations. For instance, when a registrar wants to sell a TLD to another end-user, it is required to inform the corresponding registry (e.g. VeriSign for '.com' domains). Subsequently, the registrar incurs a fee payable to the registry, a cost that is typically embedded within the price charged to the end-user.

The registration process often involves choosing the desired registration period which usually ranges from 1 to 10 years [9], agreeing to terms and conditions, and providing accurate contact information for administrative, technical, and billing purposes. Domain registration is subject to periodic renewal to maintain ownership rights. The hierarchical structure of DNS, including the distinction between registrars and registries, ensures a distributed and organised approach to managing the vast array of domain names on the Internet. This system enables users worldwide to access websites and services efficiently through the DNS.

2.2. Blockchain

Blockchain technology refers to a decentralised, digital ledger that records transactions across a network of computers. It operates as a global public ledger, in which participants (called nodes) can determine the ownership of assets without the need for a central authority or intermediary to validate transactions. The public ledger, which is replicated across all nodes in the network, is trusted as the official record. The blockchain is constructed independently by all nodes in the network, rather than a single entity. As a result, each node in the network can independently validate the data communicated through the network and create a duplicate of the same public ledger, ensuring a secure and transparent system.

Transactions and Blocks. A transaction serves as the fundamental unit of data exchange within the network, representing the transfer of value or information from one participant to another, cryptographically signed by the sender for authentication. Once initiated, transactions undergo validation and verification by network nodes before being grouped into blocks. Each block contains a *header* with metadata uniquely identifying the block. Each block also maintains a reference to its preceding block by including the hash value of the previous block in its header, forming a sequential chain of blocks. This linkage ensures the integrity and immutability of the

transaction history, with any attempt to tamper with the data in a block requiring alteration of subsequent blocks, thus providing a secure and transparent ledger of transactions within the blockchain network.

Distributed Ledger. The blockchain is a distributed ledger that uses a linked list of blocks containing a chronological record of transactions. Each node within the blockchain network maintains a copy of the data associated with the blockchain. The accumulation of blocks results in the concept of a *height*, which refers to the distance from the genesis block, and the *top* block, referring to the most recently added block in the chain.

Consensus. Consensus is a method employed by the participants of a Blockchain network to reach agreement on the current state of the public ledger, which maintains a record of all transactions [10]. The blockchain network attains reliability through the use of consensus algorithms, which also establish trust among unidentified peers. Essentially, the consensus is a protocol that ensures that each block added to the blockchain is valid, meaning that it represents the singular version of reality that the network's nodes have concurred upon.

Smart Contracts. A smart contract [11] is a self-executing (actions are executed when predefined conditions are met) digital agreement programmed to automatically enforce the terms and conditions of a contract once predefined conditions are met. Unlike traditional contracts that necessitate intermediaries and manual enforcement mechanisms, smart contracts use blockchain technology to ensure trustless, transparent, and tamper-proof transactions. By relying on cryptographic principles and consensus algorithms, smart contracts ensure the integrity and security of contractual obligations without the need for centralised oversight.

Crypto Wallets. A crypto wallet is a digital tool that allows users to securely store, send, and receive digital currencies. Functioning similarly to a traditional wallet for physical cash, a crypto wallet manages the private keys necessary for accessing and managing one's cryptocurrency holdings on a blockchain network. These wallets are usually applications installed on mobile phones or physical devices specifically designed for cryptocurrency storage.

3. Related Work

A few attempts have been made in the literature to survey existing research on BDNS. Weihong et al. [12] investigate the effectiveness of blockchain technology in addressing security vulnerabilities in the traditional DNS. Through a review and analysis of two core BDNS systems, namely Namecoin and Blockstack, the study evaluates their ability to provide decentralised, secure, and user-friendly naming systems. This work focuses on these two BDNS solutions only and does not discuss the limitations in the wider state of the art.

The work by Bansal and Sethumadhavan [13] examines the security issues within the DNS and the solutions proposed to mitigate them. It seeks to identify threats within the DNS ecosystem, particularly concerning government-operated root servers susceptible to censorship, data tracking, privatisation, and commercialisation. This work also discusses some BDNS projects, but it does not identify their limitations nor elaborate on BDNS adoption.

In their work, Patsakis et al. [14] provide a background on existing BDNS alternatives that covers a wide array of existing projects, including Dot-P2P, Handshake, ENS, Namecoin, Blockstack, EmerDNS, Nebulis, and OpenNIC. These are analysed in terms of their architecture,

features, and potential applications. Besides this literature review, which also includes projects that are no longer active, the focus of this work is primarily on the threats inherently associated with decentralised DNS architectures and the possible countermeasures; it does not discuss the limitations of each BDNS solution.

Contrarily to the above-mentioned works, this paper systematically discusses goals, operational mechanisms and limitations of the main active BDNS systems as well as relevant academic works. Furthermore, it includes a unique analysis of the challenges to overcome to foster the widespread adoption of BDNS.

4. Blockchain-based DNS Solutions

The application of blockchain technology within the DNS has been recognised as one of the proposed mechanisms for improving security within the DNS protocol and mitigating instances of censorship. In this survey, we focus on exploring the landscape of BDNS and the advancements made in this field. In conducting this research on blockchain DNS solutions, our criteria for selecting existing works emphasised relevance, publication quality, impact and popularity. We prioritised works directly addressing BDNS solutions, published in reputable academic journals or conference proceedings, and demonstrating innovative approaches or significant contributions to the field. Furthermore, we emphasised including works that are currently active within the research community, alongside those that have gained widespread recognition and citation. Through this approach, we aimed to present a comprehensive overview of both active and influential research in the field of blockchain DNS, providing a clear understanding of the current state and future directions. In this section, we present these approaches, highlighting their key characteristics, identifying limitations, as well as areas of research that remain to be explored. We extensively analyse each solution separately, and in Table 1 we summarise the main features of the discussed BDNS approaches.

4.1. Namecoin

Namecoin [15] (launched in 2011) is one of the pioneering BDNS projects. Its primary objective is to decentralise domain registration and create a secure and censorship-resistant system. Namecoin extends the traditional DNS to provide users with increased privacy and control over their domain names. By using a blockchain network, Namecoin seeks to eliminate central points of control, making it resistant to censorship and domain seizures.

Mechanism. Namecoin based on the Bitcoin codebase [16], functions as a unique cryptocurrency with a primary focus on providing a decentralised DNS. Operating independently, Namecoin manages the *.bit* TLD within its blockchain. The blockchain stores key-value pairs where keys represent domain names, and values include various data like IP addresses and public keys. Users interact with the system through specialised software called *wallet* such as Namecoin Core [1] or Electrum-NMC [2], enabling them to register domains, update DNS records, and transfer ownership. These operations involve creating transactions on the Namecoin blockchain,

[1] https://www.namecoin.org/download/

[2] https://www.namecoin.org/docs/electrum-nmc/

ensuring censorship resistance and tamper-proof domain records.
Challenges. Namecoin was the first BDNS to offer security and decentralisation. However, its primary limitation stems from inadequate support and adoption, leading to insufficient computing power. This makes Namecoin more vulnerable to 51% attacks compared to other analogous systems [17]. Also, Namecoin's low fees do not discourage domain squatters, making it easy for people to hoard names without much cost. Unlike systems incorporating auctions or algorithmic pricing to align name costs with their market value, Namecoin lacks such mechanisms. This absence increases the risk of domain squatting, undermining the equitable distribution and effective utilisation of domain names within the Namecoin ecosystem [15].

4.2. Blockstack

Blockstack [18], is a blockchain network that includes a decentralised DNS called Blockstack Name System (BNS). The primary objective of Blockstack is to create a user-centric internet where individuals have greater control over their digital identities and data. Specifically, Blockstack aims to decentralise domain registration, providing users with ownership and control over their domain names. By utilising blockchain technology, Blockstack aims to enhance security, privacy, and user autonomy, enabling a more transparent and equitable internet ecosystem.
Mechanism. Blockstack DNS operates on the Bitcoin blockchain. Unlike traditional DNS, Blockstack DNS supports custom TLDs like *.id*, *.podcast* and *.helloworld* created by users within its independent blockchain. Information such as domain registrations, ownership details, and decentralised identity data is securely stored in the blockchain. Users interact with Blockstack DNS through the Blockstack Browser [3], a user-friendly application deployed across various platforms. This browser simplifies domain registration, DNS record updates, and ownership transfers through blockchain transactions. DNS lookups for Blockstack DNS domains are executed through the Blockstack Browser or compatible software, querying the blockchain to retrieve decentralised identity and associated data for a specific domain.
Challenges. Scalability is a fundamental concern to many blockchain solutions, and as Blockstack's user base and transaction volume increase, maintaining efficiency and speed on its blockchain may become a formidable challenge. Blockstack DNS operates on the Bitcoin blockchain, which has limitations in terms of transaction throughput and block size. As the number of domain registrations and updates increases, the blockchain may become congested, leading to delays in processing DNS transactions and higher transaction fees. Additionally, the reliance on a public blockchain like Bitcoin could pose scalability challenges as the network grows, potentially impacting the performance and responsiveness of the Blockstack DNS system.

4.3. Ethereum Name Service (ENS)

Ethereum Name Service (ENS) [19] is a decentralised DNS built on the Ethereum blockchain [20]. Its primary objective is to simplify and enhance the user experience in interacting with blockchain addresses. ENS allows users to register and manage domain names ending in *.eth* in a decentralised manner. The primary goal is to replace complex and hard to remember crypto

[3] https://browser.blockstack.org

addresses with human-readable names, making the broader adoption of blockchain technology easier and faster. ENS aims to provide users with a secure, user-friendly, and decentralised naming infrastructure on the Ethereum network.

Mechanism. ENS operates on the Ethereum blockchain to provide a decentralised domain registration and management system. Managing the *.eth* TLD, ENS is not compatible with traditional DNS. Critical data such as domain registrations, and ownership details are securely stored on the Ethereum blockchain. To interact with ENS, users deploy Ethereum wallet software, like MetaMask [4], which integrates seamlessly with ENS features. Users can perform various actions such as registering, updating DNS records, transferring domain ownership, and conducting DNS lookups via their Ethereum wallets. This method ensures a decentralized and secure approach to managing Ethereum-based domain names. It's worth noting that while some operations like ENS lookups may suggest a transactional process with associated costs, they actually function as read operations and do not require any transactions or fees.

Challenges. A significant challenge for ENS is the gas fees during network congestion that can potentially impact the system's operations, particularly for users attempting to register, update, or transfer domain names. During periods of high network congestion on the Ethereum blockchain, gas fees can increase dramatically as users compete to have their transactions processed by miners. This can make ENS operations prohibitively expensive for users, especially for those with limited resources or smaller transactions. Additionally, the unpredictability of gas fees during network congestion can introduce uncertainty for users, making it challenging to plan and budget for ENS transactions effectively. This uncertainty may result in delays or hesitancy in executing critical actions, such as renewing domain registrations or updating DNS records, which could disrupt the normal operation of decentralised applications (dApps) and services relying on ENS.

4.4. Handshake

Handshake [5] is a decentralised, permissionless naming protocol with a core objective of revolutionising the traditional DNS. Its primary goal is to create an alternative to existing Certificate Authorities and naming systems by establishing a decentralised and censorship-resistant DNS infrastructure. Handshake seeks to democratise domain ownership, providing users with increased control over their digital identities and mitigating issues related to centralised control and censorship in the current DNS landscape.

Mechanism. Handshake naming protocol has its own dedicated blockchain, distinct from traditional DNS. Introducing various custom TLDs such as *.hs*, Handshake operates independently of traditional DNS, allowing users to create and manage domains on its blockchain. The blockchain stores ownership details, utilising a decentralised and secure system for tamper-resistant records. Interactions with Handshake occur through specialised wallet software like Namebase [6], enabling users to participate in blind auctions using HNS tokens for domain registration. DNS record updates, domain ownership transfers, and DNS lookups are executed through trans-

[4] https://metamask.io/

[5] https://hsd-dev.org/files/handshake.txt

[6] https://www.namebase.io/

actions on the Handshake blockchain, providing a decentralised and secure environment for managing and trading Handshake domain names.

Challenges. The main challenge of the Handshake DNS lies in achieving interoperability with the traditional DNS infrastructure. While Handshake offers a decentralised naming system, integrating it seamlessly with existing DNS servers and resolvers poses complexities. One key challenge is ensuring compatibility between Handshake's decentralised model and the hierarchical structure of the traditional DNS. This involves developing protocols and standards that allow Handshake names to be resolved by conventional DNS servers and browsers without compromising security or performance.

4.5. Unstoppable Domains

Unstoppable Domains [21] is a project with the primary objective of using blockchain technology to provide users with censorship-resistant and truly decentralised domain names. The project aims to replace traditional domain extensions with blockchain-based extensions, allowing users to have full control and ownership of their domain names without the risk of censorship or domain seizures. Unstoppable Domains seeks to allow individuals to use their domain names to receive cryptocurrency payments, host decentralised websites, and manage their digital identities in a secure and privacy-focused manner.

Mechanism. Unstoppable Domains operates on various blockchain networks, including Ethereum and Zilliqa [7]. Managing unique blockchain-based TLDs like *.crypto* and *.zil*, Unstoppable Domains operates independently from traditional DNS. Vital domain information, including ownership records, is stored on the Ethereum blockchain, ensuring immutability and resistance to censorship. Users interact with Unstoppable Domains through compatible wallets like MetaMask, while DNS lookups for these domains are made through decentralised resolution protocols. These protocols involve querying the Ethereum blockchain or other smart contracts that contain the domain name records. The registration process involves a one-time fee and submitting a transaction on the Ethereum blockchain to associate the chosen domain with the user's Ethereum address, providing a secure and transparent domain ownership experience.

Challenges. Similarly to ENS, the main challenge faced by Unstoppable Domains is the potential volatility of gas fees on the Ethereum blockchain. During periods of high network congestion or elevated gas prices, such as significant network activity, the cost of gas fees can increase significantly. For instance, findings in [22] saw that registering a new name through the Unstoppable Domains service incurred approximately $80 in gas fees during a period of elevated fees. In contrast, the actual cost of the name itself was $10. This challenge of unpredictable and potentially high gas fees during network congestion can deter users from utilising Unstoppable Domains and other Ethereum-based services, particularly for smaller transactions or users with limited resources. It introduces uncertainty and unpredictability into the registration process, making it challenging for users to budget effectively and plan for domain acquisitions.

[7] https://www.zilliqa.com/

4.6. B-DNS

B-DNS [23] is a BDNS designed to address vulnerabilities present in the traditional DNS, such as cache poisoning and DDoS attacks. By implementing a Proof-of-Stake (PoS) consensus protocol and an index of domains, B-DNS aims to overcome the limitations of current BDNS solutions, particularly the computation-heavy PoW protocol and inefficient query mechanisms. The paper compares the security of B-DNS and legacy DNS, assessing factors like attack success rate, cost, and attack surface. Experimental results demonstrate that B-DNS significantly enhances security, reducing the probability of successful attacks and increasing attack costs by orders of magnitude compared to traditional DNS.

Mechanism. B-DNS is designed with a four-layer architecture. At the *Data Layer*, DNS records are stored as immutable transactions in the blockchain, utilising operation records for registration, update, and revocation functionalities. Inspired by Bitcoin's scripting system, these records enable dynamic domain ownership changes and content updates. The *Index Layer* offers search speed by maintaining an index tree mapping domain names to IP addresses, with bloom filters facilitating fast revocation checks. In the *Consensus Layer*, a PoS consensus protocol ensures the consistency of DNS records, with block generators selected based on stake proportional probabilities. Finally, the *Network Layer* is responsible for the communication between B-DNS name servers, recursive resolvers, and end-users, enabling direct querying of DNS records from the blockchain and ensuring compatibility with the traditional DNS systems.

Challenges. Mitigating DDoS attacks in B-DNS presents a notable challenge despite the detection of fewer vulnerabilities compared to traditional DNS. In particular, the security analysis that was performed saw that while in traditional DNS 24 vulnerabilities that can lead to DDoS attacks were detected, in B-DNS only 12 vulnerabilities were detected. However, it is essential to recognise that this improvement does not necessarily indicate that B-DNS effectively prevents DDoS attacks. Instead, B-DNS architecture may render it more resilient to such attacks, making it more challenging for attackers to exploit vulnerabilities and disrupt domain resolution processes. Nonetheless, the potential for DDoS attacks to disrupt B-DNS operations remains a concern, highlighting the need for continued research and development to increase the system's defenses against such threats.

4.7. Blockzone

BlockZone [24] is a BDNS storage aimed at addressing the centralisation issues of the traditional DNS architecture and management. BlockZone uses blockchain by treating DNS name servers as nodes within the network, each storing record information for the entire network. By using a Practical Byzantine Fault Tolerance (PBFT) consensus algorithm tailored for DNS, BlockZone ensures consensus and data consistency while offering advantages such as fast consensus and low network traffic. BlockZone achieves significantly higher parsing and authentication efficiency compared to DNSSEC, with the improved consensus algorithm exhibiting a substantial increase in efficiency over PoW-based alternatives.

Mechanism. BlockZone operates by using smart contracts on the Ethereum blockchain to manage DNS resource records, hierarchical relationships, and historical updates. Four types of smart contracts - Consensus Contract (CC), Relationship Contract (RC), Ownership Contract

(OC), and History Record Contract (HC) - are utilised for this process. When adding a new node (name server) to the system, registration involves submitting an application to the blockchain network, undergoing confirmation by the consensus contract, and creating relationship contracts if approved. Data updates are managed by synchronising resource records in the external InterPlanetary File System (IPFS) [8] system and sending information to the service contract, which records updated domain name information and generates historical contracts. Data retrieval involves end users initiating query requests, trusted servers querying the blockchain's service contract, and verifying the integrity of retrieved information. A consensus algorithm, a variant of PBFT, integrates communication and verification processes among participating nodes, enhancing efficiency and reducing network overhead.

Challenges. While BlockZone demonstrates notable improvements in parser throughput, authentication efficiency, and distribution of query requests, several limitations exist within the system. Firstly, the centralised structure of the root servers presents a potential single point of failure risk, particularly evident when cache misses occur, leading to frequent query requests directed to them. This centralised architecture contrasts with BlockZone's non-central design philosophy, potentially undermining the system's reliability and resilience. Additionally, while BlockZone utilises the PBFT consensus algorithm to ensure efficient transaction processing, the rapid increase in blockchain length due to frequent updates poses a challenge in terms of storage overhead. As the number of server nodes increases (for the needs of new domain storage), so does the overall storage load on the blockchain. Thus, while BlockZone offers significant improvements in authentication efficiency, challenges persist in managing the storage overhead and maintaining system reliability in the face of potential centralisation risks.

4.8. Other BDNS Proposals

The reviewed BDNS solutions are among the most active and relevant research efforts to date in the implementation of a BDNS. While alternative concepts have been proposed, the insufficient maturity of their research currently limits us from gathering sufficient information on them. Considering the current availability of materials and resources, we present a brief overview of some of these additional concepts, with the expectation of further research in the future.

EmerDNS [9] operates on the Emercoin blockchain [25] to store domain name records. Users can register domain names using the Emercoin cryptocurrency (EMC). The decentralised nature of the Emercoin blockchain ensures that domain ownership records are transparent, secure, and resistant to tampering or censorship. EmerDNS also incorporates Name-Value Storage (NVS) [26], a feature within the Emercoin blockchain, to store additional information related to domain names. However, EmerDNS competes with established domain registrars and traditional DNS systems, making it challenging to convince service providers to adopt its vision.

AuthLedger [27] is a blockchain-based approach for domain name authentication that uses the Ethereum blockchain to provide a decentralised alternative to traditional Certificate Authorities (CAs). The primary objective of AuthLedger is to reduce reliance on CAs by implementing a decentralised version of the CA system. However, it should be noted that AuthLedger is solely

[8] https://ipfs.tech//

[9] https://emercoin.com/en/documentation/blockchain-services/emerdns/emerdns-introduction/

Table 1
Objectives, mechanisms, supported TLDs and limitations of reviewed BDNS systems.

BDNS Name	Objectives	Mechanisms	Supported TLD	Limitations
Namecoin	Decentralised domain registration, censorship resistance	Bitcoin blockchain, Blockchain-based registration,	.bit	Insufficient computing power, integration, scalability, regulatory scrutiny
Handshake	Decentralised naming protocol, alternative to Certificate Authorities	Handshake blockchain, Blockchain-based auction system	.hs	Usability, integration, competition with existing DNS, regulatory scrutiny
Blockstack	Decentralised internet, user control over data	Bitcoin blockchain	.id .podcast .helloworld	Usability, integration, scalability, regulatory considerations
ENS	Simplify interaction with Ethereum, human-readable smart contract addresses	Ethereum blockchain	.eth	Usability, integration, name resolution speed, regulatory considerations
Unstoppable Domains	Censorship-resistant domains, user-controlled	Ethereum and Zilliqa blockchains,	.crypto .zil	High gas fees, integration, industry acceptance, regulatory considerations
B-DNS	Prevent cache poisoning and DDoS attacks	Agnostic blockchain, 4-layer architecture	Agnostic	Vulnerable to DDoS attacks
Blockzone	Address centralisation issues of traditional DNS architecture and management	Ethereum blockchain	Agnostic	Single point of failure risk, storage overhead

an authentication scheme, and does not allow for the purchase of individual domain names.

DNSLedger [28] is not a standalone blockchain, but rather an enhancement to existing BDNS systems such as Namecoin and Blockstack. It is organised in a hierarchical multichain structure in which domain name management and resolution are performed in a decentralised manner. DNSLedger can also be applied in IoT devices to strengthen their security and enhance their

efficiency by offering a robust distributed name management system.

BlockONS [29] is a permissioned blockchain built on the Hyperledger [10] blockchain. It aims to address traditional security concerns related to DNS resolution, such as DNS cache poisoning and is primarily used for Internet of Things devices.

ConsortiumDNS [30] is based on a three-layer architecture consisting of a consortium blockchain, a consensus mechanism, and external storage. The primary goal of ConsortiumDNS is to address the storage limitations of existing BDNS systems such as Namecoin and Blockstack by implementing a three-layer architecture and external storage. The three-layer architecture separates data records and domain name operation data, with domain name data stored in the storage layer and domain name operation data stored in the underlying blockchain layer.

5. Challenges to BDNS Adoption

The integration of blockchain into DNS is a notable attempt to reform the Internet infrastructure, offering decentralisation, and user empowerment. However, this transformative potential comes with several challenges that must be carefully considered to realise the full benefits of BDNS solutions. In this section, the multifaceted challenges to the adoption and implementation of BDNS are explored. From scalability and performance concerns to regulatory and governance hurdles, each challenge represents a promising research direction to explore further.

Scalability. One of the biggest challenges in BDNS is scalability. Traditional DNS systems handle a vast number of queries daily, and scaling blockchain solutions to accommodate similar or higher loads while maintaining performance is non-trivial. The consensus mechanisms and distributed nature of blockchains often result in slower transaction processing times and limited throughput, hindering their ability to handle DNS queries at scale. For example, in 2007, The CryptoKitties craze clogged the Ethereum network, causing congestion and significantly increasing transaction fees [31]. This incident highlights the scalability limitations of blockchain networks when faced with sudden spikes in transaction volume.

Performance. Performance is closely related to scalability and is another significant challenge for BDNS. The decentralised nature of blockchain networks introduces latency compared to centralised DNS systems, potentially impacting user experience. Improving the performance of blockchain networks through optimisations in consensus algorithms, network infrastructure, and caching mechanisms is essential for wider adoption. Bitcoin's blockchain is well known for its slow transaction processing times and high fees during periods of network congestion [32]. This poor performance has led to usability issues and deterred some users from utilising Bitcoin for everyday transactions.

Security. While blockchain technology offers various security benefits, it also introduces new security challenges for DNS systems. Smart contract vulnerabilities, consensus algorithm weaknesses, and the potential for 51% attacks are among the security threats that BDNS systems must mitigate. Ensuring the integrity of DNS data stored on the blockchain is crucial to prevent unauthorised access or tampering. The decentralized autonomous organization (DAO) hack on the Ethereum blockchain [33] not only resulted in financial losses but also weakened trust in the

[10] https://www.hyperledger.org/

security of smart contracts and DApps built on blockchain platforms. This incident highlighted the importance of robust security measures and thorough code audits in blockchain-based systems.

Governance and regulatory considerations. Regulatory challenges pose significant barriers to the adoption of BDNS. The decentralised nature of blockchain networks complicates regulatory compliance and governance, particularly concerning domain ownership, dispute resolution, and legal liability. Establishing clear regulatory frameworks and standards for BDNS systems is essential to address these challenges and foster trust among stakeholders. Conflicting regulations and lack of clarity have created barriers to entry for startups and innovators in the space.

Usability and adoption. Usability is a critical challenge for BDNS adoption. User-friendly graphical interfaces, integration with existing DNS infrastructure, and compatibility with popular browsers and applications are essential to encourage widespread adoption. Moreover, educating users and DNS administrators about the benefits and complexities of BDNS is necessary to overcome scepticism and resistance to change. Some BDNS solutions suffer from poor user experience and lack of adoption due to complex registration processes, unfamiliar interfaces, and limited support from traditional DNS providers.

Integration with existing infrastructure. Integrating BDNS with existing infrastructure presents technical challenges such as ensuring compatibility with legacy systems and protocols. Interoperability between BDNS solutions and traditional DNS infrastructure is essential for a smooth transition and to minimise disruptions to existing services. Incompatibility issues between BDNS solutions and traditional DNS infrastructure can lead to interoperability challenges and disruptions in service. For example, DNS resolvers may struggle to resolve blockchain domain names or may not support DNSSEC for blockchain domains, creating confusion and inconvenience for users [34].

6. Conclusion

The concept of BDNS seems a promising solution in the attempt of trying to make the Internet more secure and resilient to censorship. The investigation into BDNS solutions reveals a wide range of objectives, mechanisms, and limitations. However, the journey toward widespread adoption of BDNS is not without challenges. Integration challenges with existing Internet infrastructure, scalability concerns, and the need for regulatory landscapes further highlight the complexity of implementing BDNS on a large scale. Additionally, usability remains a common hurdle, as users who adopt traditional DNS may find the transition challenging. Addressing these concerns will be crucial for the success of these transformative technologies.

7. Acknowledgments

This work was partially supported by the UK Research and Innovation (DTP Scholarship under grant EP/T517859/1); and the Academic Centre of Excellence in Cyber Security Research - University of Southampton (EP/R007268/1).

References

[1] ICANN, Dnssec – what is it and why is it important?, ???? URL: https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en.

[2] A. Vakali, G. Pallis, Content delivery networks: Status and trends, IEEE Internet Computing 7 (2003) 68–74.

[3] S. Sarat, V. Pappas, A. Terzis, On the use of anycast in dns, ACM sigmetrics performance evaluation review 33 (2005) 394–395.

[4] M. Müller, T. Chung, A. Mislove, R. van Rijswijk-Deij, Rolling with confidence: Managing the complexity of dnssec operations, IEEE transactions on network and service management 16 (2019) 1199–1211.

[5] J. Postel, Domain name system structure and delegation, Technical Report, 1994.

[6] S. P. Singh, The use of dns resource records, International Journal of Advances in Electrical and Electronics Engineering (IJAEEE, ISSN: 2319-1112) 1 (2012) 230–236.

[7] S. Bechtold, Governance in namespaces, Loy. LAL Rev. 36 (2002) 1239.

[8] H. Gao, V. Yegneswaran, Y. Chen, P. Porras, S. Ghosh, J. Jiang, H. Duan, An empirical reexamination of global dns behavior, in: Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM, 2013, pp. 267–278.

[9] S. Hao, M. Thomas, V. Paxson, N. Feamster, C. Kreibich, C. Grier, S. Hollenbeck, Understanding the domain registration behavior of spammers, in: Proceedings of the 2013 conference on Internet measurement conference, 2013, pp. 63–76.

[10] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, C. Qijun, A review on consensus algorithm of blockchain, in: 2017 IEEE international conference on systems, man, and cybernetics (SMC), IEEE, 2017, pp. 2567–2572.

[11] N. Szabo, Smart contracts: building blocks for digital markets, EXTROPY: The Journal of Transhumanist Thought,(16) 18 (1996) 28.

[12] H. Wei-hong, A. Meng, S. Lin, X. Jia-gui, L. Yang, Review of blockchain-based dns alternatives, 3 (2017) 71–77.

[13] M. K. Bansal, M. Sethumadhavan, Survey on domain name system security problems-dns and blockchain solutions, in: Futuristic Trends in Networks and Computing Technologies: Second International Conference, FTNCT 2019, Chandigarh, India, November 22–23, 2019, Revised Selected Papers 2, Springer, 2020, pp. 634–647.

[14] C. Patsakis, F. Casino, N. Lykousas, V. Katos, Unravelling ariadne's thread: Exploring the threats of decentralised dns, IEEE Access 8 (2020) 118559–118571.

[15] H. A. Kalodner, M. Carlsten, P. M. Ellenbogen, J. Bonneau, A. Narayanan, An empirical study of namecoin and lessons for decentralized namespace design., in: WEIS, volume 1, 2015, pp. 1–23.

[16] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Decentralized business review (2008).

[17] F. Casino, N. Lykousas, V. Katos, C. Patsakis, Unearthing malicious campaigns and actors from the blockchain dns ecosystem, Computer Communications 179 (2021) 217–230.

[18] M. Ali, J. Nelson, R. Shea, M. J. Freedman, Blockstack: A global naming and storage system secured by blockchains, in: 2016 {USENIX} annual technical conference ({USENIX}{ATC}

16), 2016, pp. 181–194.
[19] P. Xia, H. Wang, Z. Yu, X. Liu, X. Luo, G. Xu, Ethereum name service: the good, the bad, and the ugly, arXiv preprint arXiv:2104.05185 (2021).
[20] V. Buterin, et al., Ethereum white paper, GitHub repository 1 (2013) 22–23.
[21] W. Rehman, H. e Zainab, J. Imran, N. Z. Bawany, Nfts: Applications and challenges, in: 2021 22nd International Arab Conference on Information Technology (ACIT), IEEE, 2021, pp. 1–7.
[22] A. Randall, W. Hardaker, G. M. Voelker, S. Savage, A. Schulman, The challenges of blockchain-based naming systems for malware defenders, in: 2022 APWG Symposium on Electronic Crime Research (eCrime), IEEE, 2022, pp. 1–14.
[23] Z. Li, S. Gao, Z. Peng, S. Guo, Y. Yang, B. Xiao, B-dns: A secure and efficient dns based on the blockchain technology, IEEE Transactions on Network Science and Engineering 8 (2021) 1674–1686.
[24] W. Wang, N. Hu, X. Liu, Blockzone: A blockchain-based dns storage and retrieval scheme, in: International Conference on Artificial Intelligence and Security, Springer, 2019, pp. 155–166.
[25] A. Yakubov, W. Shbair, A. Wallbom, D. Sanda, et al., A blockchain-based pki management framework, in: The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018, Tapei, Tawain 23-27 April 2018, 2018.
[26] A. Singla, E. Bertino, Blockchain-based pki solutions for iot, in: 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), IEEE, 2018, pp. 9–15.
[27] Z. Guan, A. Garba, A. Li, Z. Chen, N. Kaaniche, Authledger: A novel blockchain-based domain name authentication scheme., in: ICISSP, 2019, pp. 345–352.
[28] X. Duan, Z. Yan, G. Geng, B. Yan, Dnsledger: Decentralized and distributed name resolution for ubiquitous iot, in: 2018 IEEE International Conference on Consumer Electronics (ICCE), IEEE, 2018, pp. 1–3.
[29] W. Yoon, I. Choi, D. Kim, Blockons: Blockchain based object name service, in: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, 2019, pp. 219–226.
[30] X. Wang, K. Li, H. Li, Y. Li, Z. Liang, Consortiumdns: A distributed domain name service based on consortium chain, in: 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), IEEE, 2017, pp. 617–620.
[31] X.-J. Jiang, X. F. Liu, Cryptokitties transaction network analysis: The rise and fall of the first blockchain game mania, Frontiers in Physics 9 (2021) 57.
[32] T. Klein, H. P. Thu, T. Walther, Bitcoin is not the new gold–a comparison of volatility, correlation, and portfolio performance, International Review of Financial Analysis 59 (2018) 105–116.
[33] M. I. Mehar, C. L. Shier, A. Giambattista, E. Gong, G. Fletcher, R. Sanayhie, H. M. Kim, M. Laskowski, Understanding a revolutionary and flawed grand experiment in blockchain: the dao attack, Journal of Cases on Information Technology (JCIT) 21 (2019) 19–32.

[34] A. Herzberg, H. Shulman, Dnssec: Security and availability challenges, in: 2013 IEEE Conference on Communications and Network Security (CNS), IEEE, 2013, pp. 365–366.