IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 14, 2020, accepted June 18, 2020, date of publication June 24, 2020, date of current version July 8, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3004727

Unravelling Ariadne's Thread: Exploring the Threats of Decentralised DNS

CONSTANTINOS PATSAKIS[1,2], (Member, IEEE), FRAN CASINO[1], (Member, IEEE), NIKOLAOS LYKOUSAS[1], AND VASILIOS KATOS[3], (Member, IEEE)

[1]Department of Informatics, University of Piraeus, 185 34 Pireas, Greece
[2]Information Management Systems Institute, Athena Research Center, 151 25 Marousi, Greece
[3]Department of Computing and Informatics, Bournemouth University, Poole BH12 5BB, U.K.

Corresponding author: Constantinos Patsakis (kpatsak@unipi.gr)

This work was supported by the European Commission under the Horizon 2020 Programme (H2020), as part of the projects CyberSec4Europe (Grant Agreement no. 830929), LOCARD (Grant Agreement no. 832735) and ECHO (Grant Agreement no 830943). The content of this article does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

ABSTRACT The current landscape of the core Internet technologies shows considerable centralisation with the big tech companies controlling the vast majority of traffic and services. This situation has sparked a wide range of decentralisation initiatives with blockchain technology being among the most prominent and successful innovations. At the same time, over the past years there have been considerable attempts to address the security and privacy issues affecting the Domain Name System (DNS). To this end, it is claimed that Blockchain-based DNS may solve many of the limitations of traditional DNS. However, such an alternative comes with its own security concerns and issues, as any introduction and adoption of a new technology typically does - let alone a disruptive one. In this work we present the emerging threat landscape of blockchain-based DNS and we empirically validate the threats with real-world data. Specifically, we explore a part of the blockchain DNS ecosystem in terms of the browser extensions using such technologies, the chain itself (Namecoin and Emercoin), the domains, and users who have been registered in these platforms. Our findings reveal several potential domain extortion attempts and possible phishing schemes. Finally, we suggest countermeasures to address the identified threats, and we identify emerging research themes.

INDEX TERMS Blockchain, blockchain forensics, cybercrime, DNS, malware.

I. INTRODUCTION

One could argue that there is a periodic paradigm bounce between centralisation and decentralisation in computer science. A representative example is the transition from mainframes with dummy terminals to personal computers or the shift from centralised local storage to the cloud. Although the Internet was in principle designed to be distributed and decentralised by nature, in reality, the control is placed onto a relatively limited number of stakeholders and the quest for further decentralisation is becoming an imminent need. Such requirement manifests in many ways, see for example the case of net neutrality, or the concept of crowdsourcing which attempts to address efficiency and sustainability issues. As such, in recent years, we are witnessing an increasing demand and creation of decentralised services.

A noteworthy example of decentralisation is the blockchain technology, which is being widely deployed in various and diverse fields [1]. In different forms, the decentralisation wave is gradually reaching traditional centralised services, such as DNS. DNS is a distributed database with a centralised data governance model, primarily controlled by The Internet Corporation for Assigned Names and Numbers (ICANN). In this regard, ICANN manages the top-level domains (TLDs) and the operation of root name servers. In practice, in order for a client to contact a host of a particular domain name, it first issues a query to a DNS server to obtain the host's IP address. For efficiency the DNS server may maintain a copy of this information in its cache, depending on how often this domain is requested. In the case where the DNS server does not hold the information requested, the query is propagated to the root name server. Next, the root name server will find the servers for the corresponding TLD and then forward the query to the corresponding authoritative name server, which would return the requested IP.

The associate editor coordinating the review of this manuscript and approving it for publication was Kuo-Hui Yeh.

While DNS is currently one of the oldest yet critical Internet application-level protocols, it has several drawbacks that mandate its replacement. For instance, DNS does not support cryptographic primitives by default. Although DNS supports security extensions through DNSSEC, these are not widely used. As a result, any query and response can be intercepted by anyone on the same network, exposing this service to numerous threats, primarily through man-in-the-middle type of attacks. Indicatively, there can be confidentiality and privacy violations through passive eavesdropping, as well as integrity breaches since anyone on the same network, may inject a response of an intercepted query. Moreover, totalitarian regimes can exploit DNS to censor unwanted web pages and services. Furthermore, in the past years the DNS servers have been both attack targets - see for example DNS poisoning attacks - as well as components of an attack vector, as they have been used in amplification denial of service attacks.

Motivation: The issues above have driven the research community to seek alternative solutions to DNS. Some initiatives include DNS over HTTPS [2] and DNS over TLS [3] and [4] while others are looking into solutions to provide alternatives to ICANN's centralisation paradigm. One of the most promising decentralised solutions is blockchain DNS which has already been adopted by several chains such as Ethereum, Namecoin and Emercoin. Despite being in their infancy, blockchain domains have attracted the interest of several prominent stakeholders. A notable example is Alibaba, who recently filed a patent for a blockchain-based domain name management system.[1] A brief overview of blockchain DNS together with some degree of scepticism is presented in [5]. To date, blockchain DNS is already being exploited by cybercriminals.[2] Therefore, we argue that there is a need to explore threat models related to novel blockchain solutions,[3] as well as decentralised file storage systems [6]. The decentralisation of services may undoubtedly provide a plethora of possibilities in terms of privacy, security and democratisation. Nevertheless, substantial changes in the backbone of well-established services and infrastructures may come at a high cost. Adversaries are expected to opportunistically take advantage of such changes by exploiting the lack of knowledge, experience and maturity of the users and deployments, as well as the inherent flaws that exist in the early stages of a new technology. At the same time, the use of encrypted and covert communications adds another layer of difficulty to detect infected systems [7], for instance, in the case of botnets. Therefore, it is imperative to raise awareness on the opportunities as well as the emerging security threats. This paper aims to fill this research gap by providing an overview of the current state of the art and practice (Section II), a detailed presentation of the emerging threats and how they could be amplified (Section III). Further to merely speculating future threats, we perform an investigation and analysis of the currently available blockchain DNS ecosystem and illustrate the presence of risks. To this end, in Section IV, we showcase the results of an in-depth analysis of Namecoin, Emercoin and Blockchain DNS. Our findings show that there are ongoing domain extortion activities and indicate that possible phishing campaigns have already been deployed. It should be noted that the threats discussed and the conclusions drawn from the statistical analysis could be extended to other Blockchain DNS systems. Finally, some remarks and findings are further discussed, along with possible countermeasures in Section V.

To the best of our knowledge, the previous work in this field was limited to the research by Kaodner *et al.* [8] back in 2011 who analysed the Namecoin domain. The authors studied an early version of the Namecoin domain; however, they identified issues such as domain squatting which was an anticipated threat. In our work, the analysis is considerably extended by providing a detailed study of Namecoin and Emercoin data in terms of domains, addresses and their corresponding timelines. We perform an analysis and empirical evaluation of the current state of practice in real-world blockchain DNS systems. Moreover, we identify extortion schemes, pricing schemes and discuss both domain squatting and typo squatting. The recent high rate of domain registrations and the observation that particular parties registered a considerable number of domains - some in the order of thousands - indicate that blockchain DNS in its current state may not constitute a safe and secure ecosystem. As such, the broader adoption of such solutions, despite their attractive features, should be approached with scepticism.

II. BACKGROUND

A. BLOCKCHAIN-BASED DNS

Decentralised systems were in principle used to improve the robustness and availability of domain name resolution tasks as well as enabling the feature of bypassing censorship campaigns and tampering, as discussed in [9]–[14]. Some of the research initiatives in this area focused on developing specific TLDs, such as in the Dot-P2P project (with the .p2p TLD) [15]. In this regard, although the idea of using P2P networks to perform distributed domain name resolution was interesting, their performance entailed several drawbacks [16]. Nevertheless, only up until recently, the adoption of distributed DNS is progressively gaining ground [5], mainly due to the inherent features of blockchain technology, such as immutability, verifiability, and trust. These features, when introduced to registrar systems, can enable functional and real-world scale distributed DNS systems. According to Scopus, Web of Science and Google Scholar, a set of approaches, some of which are fully functional, have appeared in the literature since 2016. In what follows, we describe and analyse the main features of the most relevant and adopted solutions. The work presented by Hari *et al.* [17] is one of the first works that

[1] https://domainnamewire.com/2019/08/15/alibaba-files-blockchain-domain-name-patent-application/

[2] https://www.digitalshadows.com/blog-and-research/how-cybercriminals-are-using-blockchain-dns-from-the-market-to-the-bazar/

[3] https://en.bitcoinwiki.org/wiki/Blockchain_Projects_List

propose the use of blockchain to develop a DNS infrastructure. The authors discuss the benefits of such a system over the main threats and drawbacks of traditional models such as compromised hosts, spoofing, trust management, and its heavy dependence on PKIs. Benshoof *et al.* [18] proposed a system named D^3NS, which uses a distributed hash table and a domain name ownership implementation based on the Bitcoin blockchain. They aim to replace the top-level DNS and certificate authorities, offering increased scalability, security and robustness. Liu *et al.* [19] proposed a blockchain-based decentralisation DNS resolution method with distributed data storage to mitigate single points of failure and domain name resolution data tampering. Gourley and Tewari [20] proposed the use of blockchain to enhance the certificate validation procedure to create an improved DNS security extension, providing the same benefits with DNSSEC while overcoming its main drawbacks. Similarly, in an attempt to reduce the level of trust in certificate authorities, Guan *et al.* [21] presented AuthLedger, a blockchain-based system that provides efficient and secure domain name authentication. BlockZone, of Wang *et al.* [22], uses a replicated network of nodes to offer efficient name resolution through an improved Practical Byzantine Fault Tolerance (PBFT) consensus mechanism.

Some work focused on IoT systems, and their communication protocols have also been proposed. For example, Duan *et al.* [23] presented DNSLedger, a hierarchical multi-chain structure in which domain name management and resolution are performed in a decentralised way. The authors claim that their system could enhance IoT-related communication technologies due to its efficiency. BlockONS, proposed by Yoon *et al.* [24], is a system that aims to overcome classical problems related to DNS resolution, namely DNS cache poisoning, spoofing, and local DNS cracking. The authors propose a robust and scalable object name service appropriate for an IoT ecosystem. ConsortiumDNS was introduced by Wang *et al.* [25] as a system based on a three-layer architecture composed by consortium blockchain, a consensus mechanism and external storage. The authors claim that their approach increases the efficiency of the overall system, compared to other well-known approaches such as Namecoin or Blockstack. Finally, a number of patented designs of Blockchain-based DNS systems is found in [26], [27].

Currently, there are several relevant and widely adopted blockchain DNS projects. Handshake[4] is one of the most widely supported technologies, which aims to offer an alternative to existing certificate authorities. Therefore, Handshake aims to replace the root zone file and the DNS name resolution and registration services worldwide. The Ethereum name service (ENS)[5] uses smart contracts to manage the `.eth` registrar by means of bids and recently added the support for `.onion` addresses. Namecoin[6] is a cryptocurrency based on Bitcoin, with additional features such as decentralised name system management, mainly for the `.bit` domain. It was the first project to provide an approach to address Zooko's triangle since the system is secure, decentralised and human-meaningful. Nevertheless, contrary to well-established blockchains like Bitcoin, Namecoin's main drawback is its insufficient computing power, which makes it more vulnerable to the 51% attack. Practically, if an adversary manages to get a slight majority of the computing power, they may rewrite the whole chain. Blockstack [28] is a well-known blockchain-based naming and storage system that overcomes the main drawbacks of Namecoin. Blockstack's architecture separates control and data planes, enabling seamless integration with the underlying blockchain. EmerDNS[7] is a system for decentralised domain names supporting a full range of DNS records. EmerDNS operates under the "DNS" service abbreviation in the Emercoin NVS. Nebulis[8] is a globally distributed directory that relies on the Ethereum ecosystem and smart contracts to store, update, and resolve domain records. Moreover, Nebulis proposes the use of off-chain storage (i.e. IPFS) as a replacement for HTTP. OpenNIC[9] deserves a special mention since it is a hybrid approach in which a group of peers manages namespace registration, yet the name resolving task is fully decentralised. OpenNIC provides DNS namespace and resolution over a set of domains, including those maintained by blockchain solutions such as EmerDNS and New Nations.[10] Moreover, OpenNIC resolvers have recently added access to domains administered by ICANN. In addition to namespace registrar, users can also create their own TLD on request. It should also be noted that OpenNIC has recently voted to drop support for `.bit` after rampant abuse from malware operators. It is worth mentioning that this decision was taken after a voting process by the OpenNIC members. Table 1 summarises the main features of the most relevant Blockchain-DNS systems.

TABLE 1. Technical characteristics of the most relevant DNS systems. Although Blockstack is blockchain agnostic, it is mainly used with Bitcoin blockchain.

Method	Pedigree Platform	Registrar and Resolution Management	TLD Examples
ICANN	Network of Servers and resolvers	Centralised	`.com` `.net` `.org`
OpenNIC	Decentralised Servers	Hybrid	`.bbs` `.pirate` `.libre`
ENS	Ethereum	Decentralised	`.eth` `.onion`
Handshake	Bitcoin	Decentralised	unrestricted
Blockstack	Blockchain agnostic	Decentralised	`.id` `.podcast` `.helloworld`
Emercoin	Bitcoin	Decentralised	`.coin` `.bazar` `.emc`
Namecoin	Bitcoin and Peercoin	Decentralised	`.bit`

[4] https://handshake.org/

[5] https://ens.domains/

[6] https://www.namecoin.org/

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

[8] https://www.nebulis.io/

[9] https://www.opennic.org/

[10] http://www.new-nations.net/

Internet users can reach the TLDs offered by Namecoin, OpenNIC, New Nations, and EmerDNS (e.g. `.bit`, `.coin`, `.emc`, `.lib` and `.bazar`) through various browser extensions such as `peername`, `blockchain-DNS` and `friGate` [29]. The process is outlined in Figure 1.

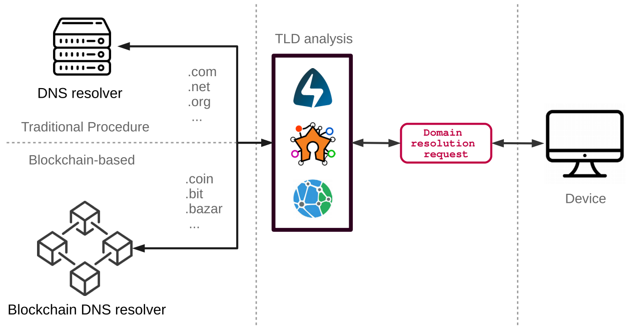

FIGURE 1. Workflow of the browser extensions procedure to enable resolution of EmerDNS, Namecoin, New Nations and OpenNIC domains. The extension inspects the TLD of the requested domain and directs the query to the corresponding DNS system.

B. DOMAIN NAME FRAUD

Apart from the protocol weaknesses DNS carries, there are also several attacks on the underlying processes. For instance, when a business registers its name on a specific TLD, an adversary may opportunistically register the same name to another TLD. This attack is known as *domain squatting*. ICANN, being the central authority of the main TLDs, has the capability to alleviate from such attacks. Another attack stems from the failure of timely renewal of a domain name once its registration has lapsed. An adversary may use automated systems to buy the domain name preemptively. This is referred to as *dropcatching*.

Another attack vector emerges from the typos that people usually make when typing. In this regard, an adversary may register a domain that looks like a known domain, but with a small typo. This is usually called *typosquatting*. A particular case of typosquatting is the exploitation of linguistic collisions. In this attack, the adversary tries to exploit the fact that a typo in a word may result in a word in another language. Therefore, since the search engines correct such errors in the search results, a malicious domain may appear as a legitimate result of a query for the target domain, poisoning the search results. In *bitsquatting*, the adversary tries to exploit the possible network errors that may introduce some noise in the response of a DNS server. In this sense, since there is only one bit of difference between the registered and the target domain, the smallest hardware error could trigger the attack. *Homograph* attacks attempt to exploit the visual resemblance of one domain with another, registering, e.g. punycodes for target domain names so that the IDN looks similar to it in the browser. In *soundsquatting*, the adversary registers domains that sound similar to the target domain. In *combosquatting* the adversary tries to trick a user into trusting a domain because it looks like the original, yet has some additional words appended or prepended. The latter is something that many legitimate sites may do as well for publicity, so the user is accustomed to trusting them. Similarly, in *AbbrevSquatting* the adversary registers a possible abbreviation of a domain name. Since mobile devices have limited space to illustrate information, an adversary may embed a trusted domain name in the second-level domain names. This tactic is known as *levelsquatting*. In Table 2, we provide a categorisation of the related work in terms of attacks and scope (traditional DNS and distributed DNS). Table 3 illustrates most of these attacks with examples.

TABLE 2. Overview of domain attacks related works.

	DNS	Distributed DNS
[30]–[35]	Typosquatting	
[36], [37]	Bitsquatting	
[38]	Combosquatting	
[39]	Soundsquatting	
[40]	Abbrevsquatting	
[41]–[43]	Homograph	
[44]	Levelsquatting	
[45]	Dropcatching	
[46]	Linguistic-collision	
[47]	Domain squatting	
[8]		Domain squatting
This work		Domain & typo squatting

TABLE 3. Examples of types of domain fraud.

Attack	Benign	Malicious
Domain squatting	facebook.com	facebook.new
Typosquatting	facebook.com	facebok.com
Bitsquatting	facebook.com	fccebook.com
Combosquatting	facebook.com	yourfacebook.com
Soundsquatting	facebook.com	phacebook.com
Abbrevsquatting	fb.com	fbk.com
Homograph	facebook.com	facebook.com
Levelsquatting	facebook.com	facebook.com.maldom.com
Linguistic-collision	adobe.com	idobe.com

C. DISTRIBUTED PLATFORMS AND C2

Nowadays, advanced and sophisticated malware campaigns continuously emerge, and some are already employing the services offered by decentralised technologies such as blockchain and distributed file storage (DFS). In the case of botnets, the use of technologies such as DFS systems prevents the generation of *non-existent* domain errors (`NXDomain` responses), which is a well-known Indicator of Compromise (IoC) type for malware using domain generation algorithms. In this regard, Patsakis *et al.* [6] extended the definition of domain generation algorithms (i.e. a family of pseudo-random domain name generators to which an infected host can dynamically identify the location of its C2 server) into a more generic framework, namely Resource Identifier Generation Algorithms (RIGA). Moreover, the authors showed how DFS like IPFS could enhance malware campaigns due to their attractive features such as immutability, efficiency and negligible costs. Botnet C2 management through Blockchain systems is also a noteworthy threat as proposed by Ali *et al.* [48] and used in the case of the Cerber ransomware, analysed in by Pletnick *et al.* [49]. In this case, the malware retrieves the C2 address from the transaction information of the bitcoin blockchain. A more recent threat is the use of encrypted and covert communication channels such as in the case of DNSSec, DNS over HTTPS (DoH) and DNS over TLS (DoT). Although these technologies hinder the possibility of using NXDomain information leaks to detect suspicious behaviour, Patsakis *et al.* showed that even in such case some patterns might emerge [7], which can be used to identify and classify Domain Generation Algorithm (DGA) families accurately. Regarding the recently developed Blockchain-DNS systems, there are emerging uses of these for cybercriminal activities such as the setup of illicit market places.[11]

TABLE 4. Main characteristics of blockchain DNSs.

Property	Description
Trust	Verifiable and robust consensus mechanisms
Decentralisation	The network is completely distributed with no central entities
Availability	The availability of the network depends on multiple peers and not on a single entity.
Censorship-resistant	Access to information and domain name resolution are not subject to borders or bans
Robustness	Resilient to attacks that affect centralised DNS systems such as MiM, spoofing, cache poisoning, cracking.
Unlimited Resources	A high number of simultaneous users sharing their assets.
Namespace Freedom	Registration of new SLDs and TLDs
Automated Management	Auctions to register domain names, fast and transparent ownership control

III. THE DECENTRALISED DNS THREAT

A blockchain-based DNS solution offers the features and benefits as summarised in Table 4. In this regard, one could argue that the traditional DNS seems to be outdated, compared to the novel blockchain DNSs. In any case, the traditional DNS proved its worth in terms of reliability and scalability from the early 80s until today with modest adjustments. However, blockchain-based DNSs are not short of introducing new and emerging threats, giving opportunities for the development of novel attack vectors [50]–[53]. In the following sections, we present and analyse the most well-known threats as well as identify novel ones. We also discuss their potential impact on sociotechnical systems. Figure 2 is an overview of the emerging threats surrounding the blockchain DNS.

A. MALWARE

Malware actors are among the prime beneficiaries of blockchain-based DNS services. This enabling technology provides the capability to register a substantial number of domains with low entropy. Currently, malware authors use DGAs to generate domain names (i.e. algorithmically generated domains or AGDs); however, since most short and meaningful domain names are not available, they resorted to the use of long and random-looking domain names. Upon infecting a host, a bot that uses a DGA issues many Non-Existent Domain (`NXDomain`) requests to resolve the C2 server. The surge of DNS queries and corresponding `NXDomain` answers can be analysed, potentially providing attribution by singling out the underlying DGA.

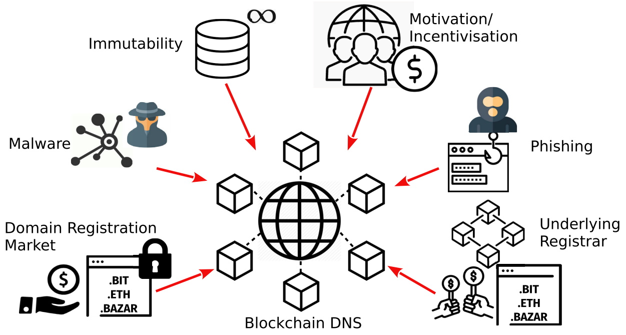

FIGURE 2. An overview of main threats of blockchain DNSs.

With the use of blockchain-based DNS systems, the conventional `NXDomain` requests will not be issued (see next section), hence hindering the detection mechanisms. Moreover, by using domain names with lower entropy, many filtering and machine learning approaches are rendered useless.

Even more, the use of blockchain-based DNSs introduces further challenges for malware analysts. When performing static analysis on the reverse-engineered code, the analyst and the tools that they use must have knowledge on the new domains and who maintains them as the function calls can considerably differ. Traditional filters for domain names will fail to reveal calls to a `.bit` domain for instance, as the resolution mechanism, is completely different. In fact, the use of the blockhain DNS from various botnets[12] to connect to the C2 servers has reportedly created more issues in the analysis, attribution, and takedown. As reported by deteque,[13] more than 100 domains registered in blockchain DNS registrars were used by C2 servers in 2018 implying that their use is actively being exploited by cybercriminals. In light of the above, OpenNIC has recently decided[14] to drop support for `.bit` domains.

In addition, it should be noted that requests to agreeably benign domains, e.g. google.com, may resolve to IP addresses not owned by the domain. The same of course applies for case sensitive domains, e.g. GoOgle.com, or the use of spaces, e.g. google.com. While Handshake, for instance, may have already taken some precautionary measures for the highly visited domain names, this does not prevent the use of existing domain names with less visibility in being exploited to serve

[11] https://www.digitalshadows.com/blog-and-research/how-cybercriminals-are-using-blockchain-dns-from-the-market-to-the-bazar/

[12] https://blog.netlab.360.com/threat-alert-a-new-worm-fbot-cleaning-adbminer-is-using-a-blockchain-based-dns-en/ https://www.microsoft.com/security/blog/2018/03/07/behavior-monitoring-combined-with-machine-learning-spoils-a-massive-dofoil-coin-mining-campaign/

[13] https://www.deteque.com/news/abused-top-level-domains-2018/

[14] https://wiki.opennic.org/votings/drop_namecoin

malware. Unfortunately, these DNS servers register and may resolve domains which are case sensitive, indicating another form of phishing and domain squatting that could be used in the near future. It should be noted that an adversary could still perform fast fluxing and change the IP addresses that are used whenever deemed necessary by simply performing a transaction in the chain. From a digital forensics perspective however the whole history and timeline of the fast-flux will be preserved due to the immutability feature of the blockchain. Finally, it should be noted that blockchain-based schemes often provide strong privacy guarantees, preventing law enforcement agencies from tracking the perpetrators, providing them with the perfect cover-up for their operations.

B. UNDERLYING REGISTRAR MECHANISM

The main approach for registering domains in blockchain DNSs is to perform bids or auctions, replacing the first-request, first-served concept followed in traditional, centralised DNS. However, by exploiting vulnerabilities in the underlying bid system, an attacker may obtain control of domains as recently observed with the `apple.eth` domain grab .[15] Moreover, most blockchain DNS systems such as Emercoin allow the registration of case sensitive domains, which is not possible in traditional systems. The latter, if paired with some other unrestricted practices such as the use of spaces, non UTF-8 or ASCII characters, may lead to an explosion of the (alternative) domain namespace where legitimate domains may not be easily distinguishable. Such a situation is likely to raise trust issues towards the DNS service in general. Note that the attack mentioned above could be prevented and reverted in traditional DNS, but not in blockchain DNSs. As such, the registration processes and implementation of the underlying smart contracts will need to be extensively studied.

In essence, an uncontrolled and fully decentralised DNS type of service may lead to having *parallel* Internets. Note that each blockchain DNS system enables the registration of arbitrary sets of TLDs, which may overlap with existing ones. Therefore, the same domain would resolve to different IPs, depending on the blockchain DNS system used. For instance, even if not used, the domain google.com is registered in Emercoin in block 252362.[16] This opens a whole new avenue of possibilities, in which users can have access to a myriad of contents without restriction. Yet, in many instances, they could be owned by a malicious entity. The latter problem, as discussed in the following sections, is exacerbated by other properties such as immutability.

C. DOMAIN REGISTRATION MARKET

In the least sinister scenario, we consider the case of one registering the domain name of an existing, legitimate webpage. Since the blockchain TLDs are not known to the vast majority of people, it is expected that some will rush to opportunistically buy such names requesting a good payment in exchange for the name. As presented in more detail in the empirical evaluation, this practice is already taking place. Block 160356 of Emercoin[17] illustrates such requests were the fees range from $600 to $20,000.

The problem is an extension of domain backordering as in this instance we are not dealing with expired domains, but with new TLDs. The existence of ICANN and intermediates, e.g. registrars, allows in many cases the arbitration or even the shutdown or handing over of a domain name. However, blockchain systems do not support such remediation mechanisms. In fact, at the time of writing, one can register a name for an arbitrary amount of time in Emercoin. For instance, there are many domain names in Emercoin which are registered for thousands of years, e.g. there are domains registered up to 5014 and 12012 in blocks 200590 and 380209, respectively.[18]

D. PHISHING

Phishing is a fraudulent practice which targets an audience to obtain valuable personal information by using impersonation of entities, persons and more techniques. According to the *State of the Phish 2019* by Proofpoint [54], the number of compromised accounts by these attacks varied from 38% to 65% from 2017 to 2018. This type of attack leverages socially engineering methods to trick users into performing activities that will benefit the attacker in some way, usually financially [55]. Email is the most popular avenue for a phishing attack, with more than 90% of successful cyber-attacks/security breaches being initiated from a spoofed email [56]. In fact, the automated capabilities of this attack, coupled with the incapacity of users to identify a phishing attack [57] may render the threat even more effective. There are many factors which augment this threat and most relate to the human. For instance, the timing of the attack, the authoritative writing, as well as the exploitation of common practices in an organisation, may significantly encourage the user into accepting the email as legitimate. Furthermore, the use of spoofed or compromised email accounts further complicates the situation.

In the context of blockchain DNSs, the above issues can be exacerbated. The users are accustomed to visiting specific web pages and sending emails to particular accounts. If these accounts are pointing to a similar address, e.g. changing the TLD, many users are highly likely to be tricked. The use of puny codes for phishing or the use of different TLDs can become an effective ingredient of an attack vector. With the introduction of blockchain DNSs, an adversary has far more options as there is a wide range of domains that are becoming available at a minimum cost. Practically, this means that not only the phishing sites may have a similar domain name with

[15] https://www.coindesk.com/ethereum-name-service-auction-exploited-to-grab-apple-domain-and-it-cant-be-undone

[16] https://explorer.Emercoin.com/block/252362

[17] https://explorer.emercoin.com/block/160358

[18] https://explorer.emercoin.com/block/200590 and https://explorer.emercoin.com/block/380209

legitimate ones, but with the use of, e.g. a Let's Encrypt[19] certificate, the fraudulent web pages may have valid and trusted HTTPS support. Therefore, the phishing page may have all the distinctive elements, from the UI, the HTTPS support and the valid domain name, making it very difficult for a common user to distinguish the original from the phishing page.

E. LACK OF MOTIVATION

Motivation under the blockchain DNS paradigm is clearly related to the features offered by such a system, including censorship resistance as one of the main attractions. Nevertheless, these desirable features come at a cost, since decentralised systems rely completely on their nodes and their participation [58]. Therefore, keeping the user's interest in blockchain DNSs is critical.

Unarguably, blockchain's adoption in a myriad of scenarios is a reality [1]. Nevertheless, not all blockchain-based projects succeed. In this regard, according to Deadcoins[20] there are approximately 1000 dead cryptocurrencies and more than 660 attempts to promote fraudulent cryptocurrencies. Interestingly enough, as of 2018, ICO scams have already raised more than 1 billion dollars.[21] Despite the existence of some awareness campaigns such as HoweyCoin,[22] the lack of a specific and interoperable framework to pursue such deviant behaviour enables the persistence of these practices. In the case of blockchain, this may hinder the creation of new projects as well as the persistence of well-known and established ones. One of the main problems that could arise is an unbalanced/unstable computational power, which could compromise the underlying consensus mechanisms and trigger, for instance, a 51% attack. Note that this attack may be applied regardless of the number of users that use a blockchain DNS solution, as the attack is targeted towards the nodes that store the blockchain which, depending on the rewards they have, their participation may decrease over time. The latter may allow an adversary to control the blockchain and compromise its integrity without having to exploit any software vulnerability of the system.

F. IMMUTABILITY

The immutability property of blockchains, although standing as one of the main beneficial features, may also be abused for malicious purposes. Well-known blockchains such as Bitcoin Satoshi Vision (BSV)[23] and Bitcoin Blockchain have suffered from serving as an illegal data storage that cannot be deleted [59], [60]. The lack of verifiable deletion mechanisms enables DFS systems such as IPFS and IndImm[24] to host and disseminate illegal content [6]. Therefore, neither contents nor domain names are subject to a take-down mechanism. Moreover, strategies as blacklisting domains are unpractical if the number of domains is high.

From a legal perspective, the GDPR does not consider the immutable nature of blockchains and DFS. In this sense, novel decentralised technologies implement features that are not aligned with current regulations and their requirements, which prevents the possibility to apply requests such as the right to be forgotten [61], [62]. Thus, the aforementioned facts make the combination of blockchain DNS and DFS systems a fertile playground for building malicious ventures. For instance, at the time of writing, Emercoin supports I2P (Invisible Internet Project) links; well-known for their anonymity, however, given the continuous rise of IPFS and other DFS solutions, blockchain DNS systems may support IPFS in the near future. The support of a permanent and distributed storage such IPFS, combined with blockchain DNS, can allow the creation of a permanent link that cannot be taken down. It should be noted that there are already initiatives towards such direction, e.g. Unstoppable Domains.[25] Evidently, the combination of both would be ideal for the distribution of infringing content that would become permanently available for everyone who has access to the link.

IV. ANALYSIS OF REAL-WORLD DATA

To assess the extent and risk of these threats, we conducted an analysis of real-world data. In the first set of experiments, we used the BDNS extension[26] and in the second one we used the Namecoin[27] and the Emercoin[28] blockchain platforms. We argue that the most critical domain names are the top ones as captured in the Alexa domain global ranking system[29] since they handle most of the user traffic. Therefore, if an adversary would like to take over a domain, a domain in the Alexa top 1,000 domains would offer them the highest impact. In addition we constructed a dataset merging the top 1 million Alexa domains[30] with the Cisco Umbrella 1 Million[31] dataset.

In what follows, we will refer to *A1K* as the dataset of the second-level domain (SLD) names of the Alexa top 1,000 domains collected and as *TOP1m* as the SLDs of the merge of the Alexa and Umbrella top 1 million datasets at the time of writing. The intuition behind having two distinct datasets is that *A1K* is small and can be used for exhaustive search without abusing the service provider's resources, while the *TOP1m* allows for a more extensive analysis that can be performed offline.

A. USING THE BDNS EXTENSION

BDNS is an open-source extension for Chrome and Firefox. The goal of the extension is to resolve .bit, .lib, .emc, .coin,

[19] https://letsencrypt.org

[20] https://deadcoins.com/

[21] https://www.ccn.com/ico-scams-have-raised-more-than-1-billion-report-claims/

[22] https://www.howeycoins.com/index.html

[23] https://bitcoinsv.io/

[24] https://en.cryptonomist.ch/2019/07/29/indimm-ripple-blockchain/

[25] https://unstoppabledomains.com

[26] https://blockchain-dns.info

[27] https://www.namecoin.org/

[28] https://emercoin.com/

[29] https://www.alexa.com/topsites

[30] http://s3.amazonaws.com/alexa-static/top-1m.csv.zip

[31] https://umbrella.cisco.com/blog/cisco-umbrella-1-million

.bazar and OpenNIC domains.[32] The extension monitors the requests of the browser for domains. If the domain falls within the supported TLDs, it uses a RESTful interface to resolve the IP.

Based on this concept, we created a crawler which sends queries using this REST interface and tries to resolve A1K domains with any of these TLDs. The search showed that 464 domains out of the potential 25,000 web pages (i.e. generated from the combination of A1K with the different TLDs) were registered. These 464 web pages were mapped to 465 IPs, as one of the DNS records mapped a domain to two IPs. Interestingly, 21 of these IPs were private and 444 public. The latter were actually 55 unique addresses, one of which was used to resolve 220 of these web pages, and 81 belong to another IP address, signifying a high concentration. In terms of countries, these domains resolve to 15 countries, as illustrated in Table 5.

TABLE 5. Distribution by country.

Country	IPs	Country	IPs	Country	IPs
DE	238	CA	5	AT	1
US	146	SG	3	HK	1
CN	20	GB	2	IT	1
FR	12	NL	2	SE	1
RU	9	SC	2	TW	1

Going a step further, we browsed each of the domains. From the 464 domains, 163 did not resolve to a valid server or returned an error on the server-side and 9 to a default welcome landing page of a service, e.g. IIS Server. Then, 80 pages redirected the user to a porn web page (https://iusr.co) which belonged to the same IP address (192.243.100.192). Note that the latter IP served only this web page except for one page that was down. Then, many of the pages resolved to placeholder pages. Three of them resolved to the same IP (161.97.219.84) pointing to ''Computer Rehab domain hosting'', 11 pointed to a parking domain of dotbit.me with the same IP (144.76.12.6). Sixty-seven domains were registered as part of the project New Nations http://www.new-nations.net from a single IP (178.254.31.11). The latter IP also resolved 76 more web pages that were divided into three placeholder web pages (ww1.partenka.net,ww17.cikidot.com, ww38.partenka.net) with 63 in the first one, 3 in the second and 9 in the last one. Notably, from the domains that resolved to the same one listed in A1K (34), almost half of them (16) belonged to porn web sites. The rest 18 of them belonged to 11 web pages, including Wikipedia, Instagram and mega.

B. THE NAMECOIN DATA

Namecoin was the first widely used Blockchain DNS, becoming a reference point for more recent approaches such as Emercoin and Blockstack. This blockchain manages the registrar of the `.bit` TLD through a straightforward procedure, in which users specify the SLD that they wish to register (which will be later appended with a `.bit`), as well as the resolving IP and other secondary parameters. At the time of writing this article, Namecoin has a total of 106,659 active domains (i.e. they have been recently created or periodically renewed by their owners). Nevertheless, despite the restrictions imposed by the registrar procedure and the data structure template to be added in the blockchain as well as the deviant behaviour of some users, we found some relevant statistics that showcase the potential of Namecoin as a platform to impulse illicit activities.

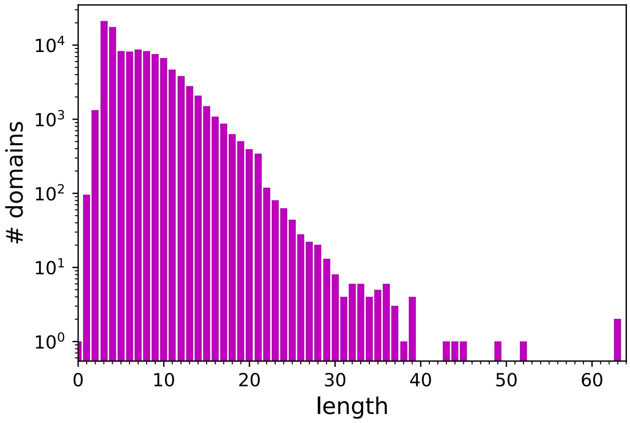

FIGURE 3. Length distribution of domain names registered in Namecoin. Note that values are represented in logarithmic scale.

As a foreseeable tendency, most users opted for registering domains of low length (from the set of domains offered by ICANN, practically all SLDs with length lower than six are already registered or reserved), as described in Figure 3. As already discussed, this hinders procedures such as AGD detection. Clearly, the fact that a domain has to be renewed every certain time at a small cost, a feature which is not implemented in Emercoin, prevents the ownership of domains for long periods if there is no revenue. Nevertheless, this does not seem a constraint for some users, as seen in Table 6. More concretely, more than 87,000 addresses registered at least one domain, yet there are users that own more than 1,000 domains, which often contain the words *sex*, *porn*, *stream*, *hack* as well as other SLDs from well-known brands and companies. Although most of them do not resolve to an IP, this may change in almost real-time with a simple update. Finally, it is worthwhile noting that the intersection of the SLDs of the TOP1m SLDs with the unique SLDs registered in Namecoin is 32,446 and if we count the naming variations (lower/capitals) 32,865, which account for 30,81% of the 106,659 registered domains. Again, using `dnstwist`, we identified 6,299 domains that belong to A1K and whose names have been registered with different typo variations.

C. THE EMERCOIN DATA

Emercoin blockchain is one of the most well-known services for domain registration. In total, the blockchain contains 54,210 records at the time of writing. Interestingly,

[32] https://www.opennic.org/

TABLE 6. Top 10 addresses in Namecoin with most registered domains.

Namecoin address	# domains
MyZTAGS74akZBiqYPKuvD3zGCfL8tGmXpz	1900
N256bGgH4E84P8fcEcLs4m1YCXYZb6nzAm	43
NJ6HHqGu9mmW25XgyGoj7V6hPoCSkQLnQ6	40
MwyGuUCawVzCcCSoNJpWjN1Kcioq7TNM92	17
MzB1bm2QDmqpmAKeaRPev4QxAxTWj1kZRi	7
MwAaZiRFGiVcTfVh2bJsHN5WXTEctocjjY	6
NAfxmnNyNoXTxCXtp3R7TZdy1SVqu885ax	4
N2pF7NKSQG73fUkgq9ZSxsjGAHnRH81P7D	4
MyFUY4gCVGYs7TfNxxuGNaf2k6hqrQEkcy	4
NHtkpFy3yWWYsAwbkEUSr1uwFXX57xded3	3

TABLE 7. Lexical statistics for domain names registered in Emercoin.

Feature	Registered domains
`.com` TLD	44
Punycode (xn–)	1261
Capital letters	316
Whitespace character	35

although the naming requirements of Emercoin specify that only lowercase alphanumeric ASCII characters are allowed, the chain contains case sensitive domains not only for the advertised TLDs but for standard TLDs like `.com`. The distribution of the domains is illustrated in Table 7. In this regard, we observed that most of the addresses registered one or two domains (i.e. more than 43,500 addresses registered at least one domain in Emercoin), while some addresses registered more than 1,000 domains, as showed in Table 8. Many of these records contained an IP, an email address, or a note advertising that the domain is for sale. More concretely, by querying the Emercoin blockchain, we found that up to 617 domains contain the words "for sale" in their *value* field, and in most cases an email to contact. Moreover, when searching for "$" in the *value* field, the search returned more than 100 domains with a specific sale value. Finally, correlating the A1K dataset with the Emercoin chain returned 1,045 domains, which correspond to 328 unique SLDs registered with different TLD variants. The intersection of the SLDs of the TOP1m SLDs with the unique SLDs registered in Emercoin is 12,214 and if we count the naming variations (lower/capitals and different TLDs) 31,587, which is 58.27% of the 54,210 registered domains. Moreover, using `dnstwist`[33] we identified 9,634 domains that belong to A1K and whose names have been registered with different typo variations (typosquatting).

The domain name length distribution is depicted in Figure 4. Notably, most of the domains have lengths below five, with three letters being the most registered domains (as in the case of Namecoin). As previously stated, these SLD are no longer available in ICANN, since they are already registered, and are among the first to be registered once a new TLD appears. Given the high correlation with ICANN domains, it is expected that many of them, if they do not belong to the corresponding ICANN owners, are highly likely to be used for malicious activities such as phishing or cybersquatting.

TABLE 8. Top 10 addresses in Emercoin with most registered domains.

Emercoin address	# domains
ETkxi1X1CeX2QDSWp3CDmuDj7jJZtftfNF	4255
EKzDF4RAHat8tWdQGbvR9zm7PJrHcth7Rm	3068
EUKa9nrsqX8udF8UpfCGLcYQG8cfT98ZvT	707
EQADxQhroZwGnQAyirFtNbwwjoykciFqv3	253
EYBExDLR3aqZunRj6NuyRC9TXt8NHKKXWZ	196
ENnpjY8YQr5rvKNc1TY6kkBwsDZXwmEiY2	150
EWwX61CW9TorzZ7Dy1dmnfKYPxz7dBMGxJ	137
EaQkdxCMPVzMXtTFqYaQxV7wQ1qqLy8aXF	58
ELRNsgvTbV83MyPdD5ACf1xyemLFV7Sued	53
ESCWovPDaX55KCpX3bdkKWqbH4zBEiwNrd	46

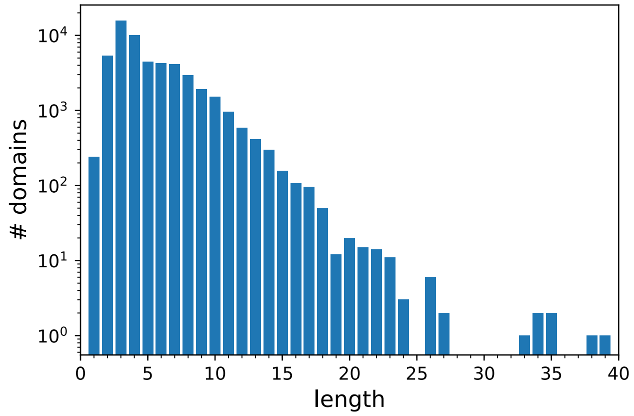

FIGURE 4. Length distribution of domain names registered in Emercoin. Note that values are represented in logarithmic scale.

Finally, some statistics of the domain registering behaviour over time are depicted in Figure 5, which shows the domains registered from the beginning of the blockchain up to March 2020. Notably, we can see some peaks in its lifetime.

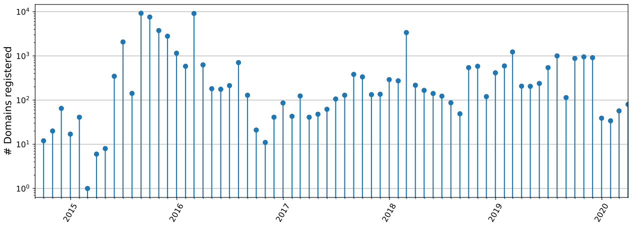

FIGURE 5. Timeline of registered domains in Emercoin. Note that values are represented in logarithmic scale.

The distribution over time of the domains registered with `.com` was also explored. As seen in Figure 6, such practices, although not alarmingly numerous, are still active in 2020. Therefore, the registrar system still allows anybody to register domains with TLDs different than those offered by Emercoin. This situation can enable several of the threats presented earlier, such as the vulnerabilities with the underlying registrar, which in turn may enable malware and phishing campaigns, as well as cybersquatting.

Finally, global statistics for Namecoin and Emercoin were produced. Currently, there are more than 140K domain names registered in both blockchains, but only 5,266 have an IP address associated with them in their registrar blocks.[34]

[33] https://github.com/elceef/dnstwist

[34] https://blockchain-dns.info/explorer/

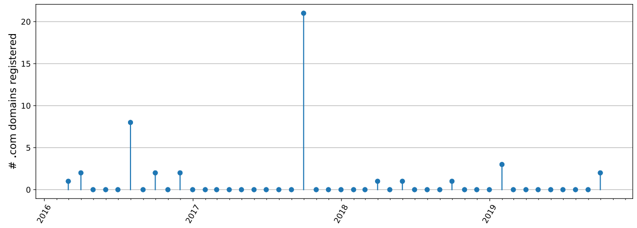

FIGURE 6. Timeline of `.com` domains registered in Emercoin.

Out of these 5,266, we computed the distribution of TLDs (Table 9). We can observe that most of the domains belong to `.coin`, `.bit`, `.lib`, `.bazar`, and `.emc`. Note that some of the other TLDs should not be "available", considering the whitespace character. Next, we explored the distribution of IP addresses controlling these domains, according to the data contained in the blockchain. In this regard, the top 15 IPs used for that purpose are described in Table 10. We observe that *192.243.100.192* is the IP address to which most domains resolve (i.e. a total of 1957 domains).

TABLE 9. Distribution of TLDs resolving to an IP in both Emercoin and Namecoin.

TLD	Number	TLD	Number	TLD	Number
coin	1261	$	1	net	1
bit	1045	oz	1	ln	1
lib	1017		1	in	1
bazar	998	bbs	1	9988	1
emc	861	news	1	kib	1
i2p	19	ua	1	fashion	1
neo	14	luxsocks	1	woshiwo321	1
com	8	mayun	1	name	1
onion	3	years	1	www	1
cn	3	pi	1	cion	1
coin	2	aaatttaaa	1	mec	1
eth	2	io	1	su	1
enc	1	liib	1	biz	1
org	1	linux	1	1010	1

TABLE 10. Top 15 IPs to which domains resolve in both Emercoin and Namecoin.

IPs	Domains	IPs	Domains
192.243.100.192	1957	78.107.255.15	53
144.76.12.6	448	192.241.241.153	45
202.108.22.5	402	202.108.8.82	45
192.227.233.13	340	81.2.247.158	45
178.128.220.134	144	94.242.60.7	37
185.31.209.8	88	185.61.138.167	32
178.32.148.152	67	46.29.251.130	29
92.63.101.1	53		

In order to go a step further and explore whether the information contained in the blockchain is valid from a domain to IP address resolution perspective, we extracted all the domains and IP addresses from Namecoin and Emercoin and attempted to resolve them. Surprisingly, the results indicated that there were only 273 and 471 unique IPs resolving Namecoin and Emercoin domains, respectively. The latter supports the data illustrated in Table 10, where there are multiple domains hosted by only a few IPs. However, there might be cases where domain data have not been properly registered or updated in these chains.

V. DISCUSSION AND COUNTERMEASURES

Arguably, the aforementioned threats seem to portray an obscure future. In what follows, we propose a set of mitigation strategies and mechanisms for each of the identified threats.

As identified, Emercoin registrar allows some theoretically forbidden patterns and characters, including the `.com` TLDs. These practices, although uncommon, are still active, as seen in Figure 6. In the case of Namecoin, the periodic renewal mechanism, as well as the fact of only controlling one TLD, allows a higher degree of control. Yet, both blockchains have similar patterns and user behaviours as analysed in Sections IV-B and IV-C. As such, more robust mechanisms have to be implemented in the future to avoid deviant behaviours. These mechanisms should cover the whole registrar procedure in an end-to-end manner, from the auction systems (e.g. with robust smart contracts and revocation mechanisms, triggered following a condition such as a majority vote) to the proper checking of the data structures stored in the blockchain so that malicious/unexpected information cannot be inserted. Other solutions and functionalities such as forks, which will be later described for the case of the immutability threat, could also be adopted.

In the case of cybersquatting, several strategies have been implemented by systems like Handshake, in which they pre-reserve the top 100k Alexa domains. Other similar policies may be implemented in future decentralised DNS systems as well as a controlled flow of domains being registered, to prevent users from registering arbitrary amounts of domains. Due to the unrestricted nature of Blockchain DNS systems, users may register the most used SLDs and append one of the multiple TLDs offered by the new blockchain DNS registrars. As previously stated, the appearance of blockchain DNS systems which aim to register and resolve all the domain spectrum (both in terms of SLDs and TLDs), may create different versions of the Internet. In this scenario, the challenge of controlling the domain name registration as well as the resolution will require unprecedented security and privacy mechanisms.

The email had always accommodated a noteworthy attack surface due to the lack of security considerations since its inception. The evolution of email security at some point called upon the DNS infrastructure in an attempt to prevent certain types of spam and phishing. Email security policies and protocols such as the Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain Message Authentication Reporting (DMARC) which depend upon DNS can be extended and adapted to force checks on domains and prevent domain spoofing attempts. In addition, the email clients should include scanning and checking functionality to distinguish between the different emerging *parallel* Internets attributed to different blockchain DNS entries. The email servers (and MTAs in general) could enforce tighter policies by requiring properly configured DMARC services. In essence, the email ecosystem could act in this instance as the gatekeeper prior to entering the blockchain DNS controlled realm.

The decentralised nature of blockchain DNS is expected to change and improve the botnets' C2 communication channels by providing more effective Rendez-vous algorithms than the current DGAs. Fewer `NXDomain` responses, covert channels and encrypted communications are expected. Traffic analysis, similar to the one described by [7], is expected to be less effective. This new state of play would require more proactive approaches such as hunting for synthesised IoC type of patterns in the blockchain itself, not only limited in the domain information but also all available metadata. The immutability of the blockchain would allow to continuously and reliably study the botnets' modus operandi and respond with mitigation actions.

The immutability of blockchains requires other approaches to counter malicious records. Although less popular, forks are a well-known mechanism to "delete" data from the blockchain [62]. Nevertheless, forks are used only in exceptional cases and are not considered to be an efficient solution, since they add a prohibitive overhead to the system, especially if the number of deletion requests is high. Other strategies regarding the block consolidation mechanism (the number of blocks created in front of the actual block for it to be considered safe) can also be explored, yet, again, they could hinder the efficiency of the system. In terms of blockchains, technical efforts to circumvent immutability while preserving their inherent security are steadily emerging [62].

Finally, it should be emphasised that for such initiatives to become mainstream and not a tool for cybercrime, they need to build trust in their services. At their current form, it is evident that both Namecoin and Emercoin have already a number of issues as their users face privacy and security challenges. Therefore, moderation solutions must be developed to protect the reputation of the emerging ecosystem. The moderation may prevent poisoning of the chains and removal of malicious records making the users trust the provided services.

VI. CONCLUSION

When a disruptive technology such as blockchain enters the realms of one of the core Internet services such as DNS, it is imperative that the security community invests a significant amount of effort to study and investigate the security implications. The DNS hijacking incident back in 2014 where 300K routers were compromised,[35] albeit having a high impact to businesses, is minuscule compared to the potential damage malicious actors can cause when the blockchain DNS becomes widely accepted. This paper attempted to tessellate the emerging threats and provide insight into the associated risks introduced by moving from a centralised to a fully decentralised DNS. The thorough analysis and evaluation of several open TLD registries such as OpenNIC as well as two well-known blockchain-based DNS systems, namely Emercoin and Namecoin, showcased that the actual solutions are far from being adopted by the users due to several security and reliability issues. Therefore, from a forensic investigation perspective, the use of blockchain is a mixed blessing; on the one hand, some of the evidence will be stored in a forensically sound manner. On the other, the introduction of yet another technology into the Internet backbone will not only increase the complexity leading to a potentially wider attack surface but will also result in significant attribution challenges. Future work will focus on the exploration of other blockchain-based DNS systems and the elaboration of ontologies and security models to overcome the main drawbacks of such systems, with the aim to provide a reliable and sustainable decentralised DNS landscape.

[35] https://www.theregister.co.uk/2014/03/04/team_cymru_ids_300000_compromised_soho_gateways/

REFERENCES

[1] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Inform.*, vol. 36, pp. 55–81, Mar. 2019.

[2] P. Hoffman and P. McManus, *DNS Queries Over HTTPS (DoH)*, document RFC 8484, 2018, p. 21. [Online]. Available: https://tools.ietf.org/html/rfc8484

[3] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, and P. Hoffman, *Specification for DNS Over Transport Layer Security (TLS)*, document RFC 7858, 2016. [Online]. Available: https://tools.ietf.org/html/rfc7858

[4] S. Dickinson, D. Gillmor, and T. Reddy, *Usage Profiles for DNS over TLS and DNS Over DTLS*, document RFC 7841, Internet Engineering Task Force, 2018, vol. 10.

[5] E. Karaarslan and E. Adiguzel, "Blockchain based DNS and PKI solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 3, pp. 52–57, Sep. 2018.

[6] C. Patsakis and F. Casino, "Hydras and IPFS: A decentralised playground for malware," *Int. J. Inf. Secur.*, vol. 18, no. 6, pp. 787–799, Dec. 2019, doi: 10.1007/s10207-019-00443-0.

[7] C. Patsakis, F. Casino, and V. Katos, "Encrypted and covert DNS queries for botnets: Challenges and countermeasures," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101614.

[8] H. A. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau, and A. Narayanan, "An empirical study of namecoin and lessons for decentralized namespace design," in *Proc. WEIS*, 2011.

[9] Z. Liu, E. S.-J. Swildens, and R. D. Day, "Domain name resolution using a distributed DNS network," U.S. Patent 7 725 602 B2, May 25, 2010.

[10] C. Cachin and A. Samar, "Secure distributed DNS," in *Proc. Int. Conf. Dependable Syst. Netw.*, 2004, pp. 423–432.

[11] V. Ramasubramanian and E. G. Sirer, "The design and implementation of a next generation name service for the Internet," in *Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun. (SIGCOMM)*. New York, NY, USA: Association for Computing Machinery, 2004, pp. 331–342.

[12] M. Wachs, M. Schanzenbach, and C. Grothoff, "A censorship-resistant, privacy-enhancing and fully decentralized name system," in *Proc. Int. Conf. Cryptol. Netw. Secur.* Cham, Switzerland: Springer, 2014, pp. 127–142.

[13] Z. Qiang, Z. Zheng, and Y. Shu, "P2PDNS: A free domain name system based on P2P philosophy," in *Proc. Can. Conf. Electr. Comput. Eng.*, 2006, pp. 1817–1820.

[14] M. Abu-Amara, F. Azzedin, F. A. Abdulhameed, A. Mahmoud, and M. H. Sqalli, "Dynamic peer-to-peer (P2P) solution to counter malicious higher domain name system (DNS) nameservers," in *Proc. 24th Can. Conf. Electr. Comput. Engineering(CCECE)*, May 2011, pp. 001014–001018.

[15] D. Storm. (2010). *P2P DNS to Take on ICANN After us Domain Seizures*. [Online]. Available: https://www.computerworld.com/article/2469753/p2p-dns-to-take-on-icann-after-us-domain-seizures.html

[16] R. Sancho and R. Lopes Pereira, "Hybrid peer-to-peer DNS," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2014, pp. 977–981.

[17] A. Hari and T. V. Lakshman, "The Internet blockchain: A distributed, tamper-resistant transaction framework for the Internet," in *Proc. 15th ACM Workshop Hot Topics Netw. (HotNets)*, 2016, pp. 204–210.

[18] B. Benshoof, A. Rosen, A. G. Bourgeois, and R. W. Harrison, "Distributed decentralized domain name service," in *Proc. IEEE Int. Parallel Distrib. Process. Symp. Workshops (IPDPSW)*, May 2016, pp. 1279–1287.

[19] J. Liu, B. Li, L. Chen, M. Hou, F. Xiang, and P. Wang, "A data storage method based on blockchain for decentralization DNS," in *Proc. IEEE 3rd Int. Conf. Data Sci. Cyberspace (DSC)*, Jun. 2018, pp. 189–196.

[20] S. Gourley and H. Tewari, "Blockchain backed DNSSEC," in *Proc. Int. Conf. Bus. Inf. Syst.*, in Lecture Notes in Business Information Processing, vol. 339, 2019, pp. 173–184.

[21] Z. Guan, A. Garba, A. Li, Z. Chen, and N. Kaaniche, "AuthLedger: A novel blockchain-based domain name authentication scheme," in *Proc. 5th Int. Conf. Inf. Syst. Secur. Privacy*, 2019, pp. 345–352.

[22] W. Wang, N. Hu, and X. Liu, "Blockzone: A blockchain-based DNS storage and retrieval scheme," in *Artificial Intelligence and Security*. Cham, Switzerland: Springer, 2019, pp. 155–166.

[23] X. Duan, Z. Yan, G. Geng, and B. Yan, "DNSLedger: Decentralized and distributed name resolution for ubiquitous IoT," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2018, pp. 1–3.

[24] W. Yoon, I. Choi, and D. Kim, "BlockONS: Blockchain based object name service," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 219–226.

[25] X. Wang, K. Li, H. Li, Y. Li, and Z. Liang, "ConsortiumDNS: A distributed domain name service based on consortium chain," in *Proc. IEEE 19th Int. Conf. High Perform. Comput. Commun., IEEE 15th Int. Conf. Smart City, IEEE 3rd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Dec. 2017, pp. 617–620.

[26] H. Li, H. Ma, L. Haopeng, Z. Huang, X. Yang, K. Li, and H. Wang, "Blockchain-based domain name resolution system," U.S. Patent App. 15/768 833, May 30, 2019.

[27] H. Li, X. Wang, Z. Lin, J. Wu, X. Si, K. Li, X. Yang, and H. Wang, "Systems and methods for managing top-level domain names using consortium blockchain," U.S. Patent App. 10/178 069, Oct. 4, 2019.

[28] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains," in *Proc. USENIX Annu. Tech. Conf. (USENIX ATC)*, Denver, CO, USA: USENIX Association, Jun. 2016, pp. 181–194.

[29] Emercoin. (2019). *Emercoin Links & Resources*. [Online]. Available: https://emercoin.com/en/documentation/links-resources

[30] D. B. Gilwit, "The latest cybersquatting trend: Typosquatters, their changing tactics, and how to prevent public deception and trademark infringement," *Wash. UJL Pol'y*, vol. 11, p. 267, Jan. 2003.

[31] B. Edelman, "Large-scale registration of domains with typographical errors," in *Domain Name Typosquatter Still Generating Millions*. Cambridge, MA, USA: Harvard Univ., 2003.

[32] B. Liu, C. Lu, Z. Li, Y. Liu, H. Duan, S. Hao, and Z. Zhang, "A reexamination of internationalized domain names: The good, the bad and the ugly," in *Proc. 48th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2018, pp. 654–665.

[33] P. Agten, W. Joosen, F. Piessens, and N. Nikiforakis, "Seven Months' worth of mistakes: A longitudinal study of typosquatting abuse," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2015, pp. 1–13.

[34] J. Spaulding, S. Upadhyaya, and A. Mohaisen, "The landscape of domain name typosquatting: Techniques and countermeasures," in *Proc. 11th Int. Conf. Availability, Rel. Secur. (ARES)*, Aug. 2016, pp. 284–289.

[35] M. T. Khan, X. Huo, Z. Li, and C. Kanich, "Every second counts: Quantifying the negative externalities of cybercrime via typosquatting," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 135–150.

[36] A. Dinaburg, "Bitsquatting: DNS hijacking without exploitation," *Proc. BlackHat Secur.*, Jul. 2011.

[37] N. Nikiforakis, S. Van Acker, W. Meert, L. Desmet, F. Piessens, and W. Joosen, "Bitsquatting: Exploiting bit-flips for fun, or profit?" in *Proc. 22nd Int. Conf. World Wide Web (WWW)*, 2013, pp. 989–998.

[38] P. Kintis, N. Miramirkhani, C. Lever, Y. Chen, R. Romero-Gómez, N. Pitropakis, N. Nikiforakis, and M. Antonakakis, "Hiding in plain sight: A longitudinal study of combosquatting abuse," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 569–586.

[39] N. Nikiforakis, M. Balduzzi, L. Desmet, F. Piessens, and W. Joosen, "Soundsquatting: Uncovering the use of homophones in domain squatting," in *Proc. Int. Conf. Inf. Secur.* Cham, Switzerland: Springer, 2014, pp. 291–308.

[40] P. Lv, J. Ya, T. Liu, J. Shi, B. Fang, and Z. Gu, "You have more abbreviations than you know: A study of abbrevsquatting abuse," in *Proc. Int. Conf. Comput. Sci.* Cham, Switzerland: Springer, 2018, pp. 221–233.

[41] V. Le Pochat, T. Van Goethem, and W. Joosen, "Funny accents: Exploring genuine interest in internationalized domain names," in *Proc. Int. Conf. Passive Act. Netw. Meas.* Cham, Switzerland: Springer, 2019, pp. 178–194.

[42] D. Chiba, A. A. Hasegawa, T. Koide, Y. Sawabe, S. Goto, and M. Akiyama, "DomainScouter: Understanding the risks of deceptive IDNs," in *Proc. 22nd Int. Symp. Res. Attacks, Intrusions Defenses (RAID)*, 2019, pp. 413–426.

[43] F. Quinkert, T. Lauinger, W. Robertson, E. Kirda, and T. Holz, "It's not what it looks like: Measuring attacks and defensive registrations of homograph domains," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 259–267.

[44] K. Du, H. Yang, Z. Li, H. Duan, S. Hao, B. Liu, Y. Ye, M. Liu, X. Su, G. Liu, Z. Geng, Z. Zhang, and J. Liang, "TL;DR hazard: A comprehensive study of levelsquatting scams," in *Security and Privacy in Communication Networks*, S. Chen, K.-K. R. Choo, X. Fu, W. Lou, and A. Mohaisen, Eds. Cham, Switzerland: Springer, 2019, pp. 3–25.

[45] N. Miramirkhani, T. Barron, M. Ferdman, and N. Nikiforakis, "Panning for gold.Com: Understanding the dynamics of domain dropcatching," in *Proc. World Wide Web Conf. World Wide Web (WWW)*, 2018, pp. 257–266.

[46] M. Joslin, N. Li, S. Hao, M. Xue, and H. Zhu, "Measuring and analyzing search engine poisoning of linguistic collisions," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 1311–1325.

[47] Y. Zeng, T. Zang, Y. Zhang, X. Chen, and Y. Wang, "A comprehensive measurement study of domain-squatting abuse," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[48] S. T. Ali, P. McCorry, P. H.-J. Lee, and F. Hao, "ZombieCoin 2.0: Managing next-generation botnets using bitcoin," *Int. J. Inf. Secur.*, vol. 17, no. 4, pp. 411–422, Aug. 2018.

[49] S. Pletinckx, C. Trap, and C. Doerr, "Malware coordination using the blockchain: An analysis of the cerber ransomware," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, May 2018, pp. 1–9.

[50] R. Amado. (2018). *How Cybercriminals are Using Blockchain DNS: From the Market to the. Bazar*. [Online]. Available: https://www.digitalshadows.com/blog-and-research/how-cybercriminals-are-using-blockchain-dns-from-the-market-to-the-bazar/

[51] J. Sanders. (2019). *Blockchain-Based Unstoppable Domains is a Rehash of a Failed Idea*. [Online]. Available: https://www.techrepublic.com/article/blockchain-based-unstoppable-domains-is-a-rehash-of-a-failed-idea/

[52] F. ul Hassan, A. Ali, S. Latif, J. Qadir, S. Kanhere, J. Singh, and J. Crowcroft, "Blockchain and the future of the Internet: A comprehensive review," 2019, *arXiv:1904.00733*. [Online]. Available: http://arxiv.org/abs/1904.00733

[53] R. Rasmussen and P. Vixie, "Surveying the dns threat landscape," Internet Identity, Tech. Rep., 2013.

[54] Proofpoint. (2019). *2019 State of the Phish Report*. [Online]. Available: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

[55] M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: A literature survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2091–2121, 4th Quart., 2013.

[56] Phishme. (2016). *Enterprise Phishing Susceptibility and Resiliency Report*. [Online]. Available: https://www.infosecurityeurope.com/__novadocuments/351537?v=636276130024130000

[57] C. Iuga, J. R. C. Nurse, and A. Erola, "Baiting the hook: Factors impacting susceptibility to phishing attacks," *Human-centric Comput. Inf. Sci.*, vol. 6, no. 1, p. 8, Dec. 2016.

[58] P. G. Lopez, A. Montresor, and A. Datta, "Please, do not decentralize the Internet with (permissionless) blockchains!" 2019, *arXiv:1904.13093*. [Online]. Available: https://arxiv.org/abs/1904.13093

[59] BBC. (2019). *Child Abuse Images Hidden in Crypto-Currency Blockchain*. [Online]. Available: https://www.bbc.com/news/technology-47130268?ocid=socialflow_twitter

[60] R. Matzutt, J. Hiller, M. Henze, J. H. Ziegeldorf, D. Müllmann, O. Hohlfeld, and K. Wehrle, "A quantitative analysis of the impact of arbitrary blockchain content on bitcoin," in *Proc. 22nd Int. Conf. Financial Cryptogr. Data Secur. (FC)*. Cham, Switzerland: Springer, 2018, pp. 420–438.

[61] E. Politou, E. Alepis, and C. Patsakis, "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions," *J. Cybersecurity*, vol. 4, no. 1, Jan. 2018, Art. no. tyy001.

[62] E. Politou, F. Casino, E. Alepis, and C. Patsakis, "Blockchain mutability: Challenges and proposed solutions," *IEEE Trans. Emerg. Topics Comput.*, early access, Oct. 25, 2019, doi: 10.1109/TETC.2019.2949510.

CONSTANTINOS PATSAKIS (Member, IEEE) received the B.Sc. degree in mathematics from the University of Athens, Greece, the M.Sc. degree in information security from the Royal Holloway, University of London, and the Ph.D. degree in cryptography and malware from the Department of Informatics, University of Piraeus.

He was a Researcher with the UNESCO Chair in Data Privacy, Rovira i Virgili University (URV), Tarragona, Spain, and a Research Fellow with Trinity College, Dublin, Ireland. He is currently an Assistant Professor with the University of Piraeus and an Adjunct Researcher with the Athena Research and Innovation Center. He has authored numerous publications in peer-reviewed international conferences and journals. He has been teaching computer science courses in European universities for more than a decade. He has been working in the industry as a Freelance Developer and a Security Consultant. He has participated in several national (Greek, Spanish, Catalan, and Irish) and European Research and Development projects. His main areas of research include cryptography, security, privacy, data anonymization, and data mining.

FRAN CASINO (Member, IEEE) received the B.Sc. degree in computer science and the M.Sc. degree in computer security and intelligent systems from Rovira i Virgili University, Tarragona, Spain, in 2010 and 2013, respectively, and the Ph.D. degree *(cum laude)* in computer science from Rovira i Virgili University, in 2017, and the best dissertation award. He was a Visiting Researcher with ISCTE-IUL, Lisbon, in 2016. He is currently a Postdoctoral Researcher with the Department of Informatics, Piraeus University, Piraeus, Greece. He has participated in several European-, Spanish- and Catalan-funded research projects. He has authored more than 40 publications in peer-reviewed international conferences and journals. His research interests include pattern recognition, and data management applied to different fields, such as privacy and security protection, recommender systems, smart health, and blockchain.

NIKOLAOS LYKOUSAS received the B.S. degree from the Department of Informatics, University of Piraeus, in 2016, and the master's degree in intelligent interactive systems from Universitat Pompeu Fabra, in 2017, where he was awarded with an academic excellence scholarship for his achievements. He is currently pursuing the Ph.D. degree with the University of Piraeus studying deviant behavior in modern social networks. Since his undergraduate studies, he has participated as a Research Engineer in several EC funded projects and has gained considerable experience in the fields of big data analytics, cybersecurity, digital privacy, and cloud computing.

VASILIOS KATOS (Member, IEEE) is currently a Professor with Bournemouth University. Prior to his current post, he was a Professor of information and communications systems security at the Department of Electrical and Computer Engineering, Democritus University of Thrace, Greece, and a Principal Lecturer at the School of Computing, University of Portsmouth, where he has participated in the development of the interdisciplinary Masters course M.Sc. in Forensic IT. He has worked in the industry as a Security Consultant as an expert witness in information systems security and is NIS Expert for ENISA. He has over 100 publications in reputable scientific journals and international conferences in the area of digital forensics and incident response. He has served as a reviewer on a number of venues, e.g., IEEE Communication Letters. He is an Editorial board member of *Computers & Security*.