Blockchain-based DNS and PKI to solve issues of trust, security and censorship in the context of the IoT

Author: Leon de Klerk[1] , **Supervisor: Miray Ayşen**[1] , **Responsible Professor: Zekeriya Erkin**[1]
Cyber Security Group
Department of Intelligent Systems
[1]Delft University of Technology

Abstract

The domain name system (DNS) and public key infrastructure (PKI) provide the core services for the Internet. The use of these systems requires trust in institutions to provide proper services, which they can fail to provide. Centralized management allows these institutions to perform censorship. Additionally, these legacy systems have seen numerous security issues over the years related to both network security and data security. The rise of the Internet of Things, often resource-constrained devices such as embedded sensors, has leveraged these services. But in doing so has exposed the IoT to the same flaws as the underlying infrastructure. To combat this, both non-blockchain-based and blockchain-based solutions have been proposed, both with their own issues. Non-blockchain-based solutions offer improvements in one dimension, such as trust, but at the cost of security. In comparison, blockchain-based solutions can offer improvements in multiple dimensions simultaneously as has been shown in proposed systems. Blockchain-based solutions deal with their own set of issues: they struggle with the adoption of such a system and lack compatibility with the resource-constrained IoT. To combat the issues of blockchain-based solutions, this paper proposes theoretical improvements on blockchain-based DNS and PKI solutions, building on work done in the field. These improvements address the interoperability with current systems to increase adoptability. Additionally, it offers a system architecture compatible with both the IoT and regular devices by leveraging different types of nodes for the blockchain network based on device constraints and needs.

1 Introduction

The Domain Name System (DNS) [1] and Public Key Infrastructure (PKI)[2] have powered the Internet since the beginning. DNS provides a mapping between domain names and IP addresses, while PKI has a supporting role in the cryptography of the web. However, a new dimension has been added to the Internet in recent history: the Internet of Things (IoT) [3]. The IoT empowers many devices ranging from smart devices in a consumer home to sensors in industrial plants and medical devices. This is achieved while being connected to the Internet and leveraging its core components: DNS and PKI. But over the years, both technologies have experienced a wide range of issues:

- **Trust**: End-users trust governments and institutions to provide the DNS and PKI services, but this makes them dependent [4]. As a result, errors and mistakes made by the service providers, can disrupt services and introduce problems for the end-users while leaving the user powerless to resolve the problems.
- **Security**: DNS is known for its network security issues [5], which cause disruptions and can result in issues for data security. In addition, PKI has problems with physical and hardware security relating to the root private keys [6]. This opens up the potential for unavailability, and incorrect records on critical systems caused by security issues.
- **Internet censorship**: With governments and large institutions having control over these services, they also possess the power to censor these services, resulting in the unavailability of content [7]. A common example of this is the Great Firewall created by the Chinese government [8].

By building on the Internet, the IoT has inevitably inherited these flaws, making the system vulnerable.

With the rise of Bitcoin [9], blockchain technology has seen a large amount of interest and research. By promising high levels of security, a trustless environment, no single point of failure, immutable and auditable data, blockchain technology is a promising technology to mitigate the issues of legacy Internet components.

Related work in this field has focused on both blockchain and non-blockchain solutions. [10] proposed a decentralized version of the DNS before blockchain technology existed to address security issues and the DNS as a single point of failure. Both [11] and [12] provide an overview of existing blockchain solutions for both DNS and PKI. However, none of these works focus on the specific context of the IoT, which adds additional restrictions. Most papers focus on security and a single point of failure, neglecting the points of trust

and internet censorship.

This paper aims to fill in those gaps by providing an overview of the existing solutions and giving theoretical improvements to solve the aforementioned issues regarding trust, security, and censorship with the DNS and PKI, put in the context of the IoT. To achieve this, an overview of the technologies is given, where all four technologies are discussed, and their main advantages and drawbacks are defined. The next step provides an overview of the existing solutions both with and without blockchain technology, their main advantages and drawbacks regarding trust, security, and censorship. Finally, using the advantages and drawbacks of various solutions, the last part provides theoretical improvements for blockchain-based solutions.

This paper is structured in the following manner: Section 2 of this paper gives an overview of the methods used to gather and process sources; Section 3 gives an overview of related work in this field; Section 4 introduces the background of the technologies relevant to this research, as well as how they relate to each other and the issues that currently exist; Section 5 gives an overview of current non-blockchain and blockchain-based solutions, and their main advantages and drawbacks. Section 6 states the key findings from the previous section and proposed improvements for blockchain-based solutions; Section 7 provides all main findings of this paper and proposes recommendations for future work. Section 8 is dedicated to the ethical side of this paper and the reproducibility of the research.

2 Methodology

This literature study is mainly concerned with four different technologies: blockchain, IoT, DNS, and PKI. As a literature study, all methodology relates to searching, reading, and processing various sources. All searches were performed on Google and Google Scholar, with default settings, combined with the TU Delft library extension for access. Within Google Scholar, the following keywords were used to perform searches:

- Technology keywords: DNS, Blockchain, PKI, IoT
- Research dimension keywords: trust, security, censorship

To gain specific information, a combination of these keywords was used, for example, “DNS” and “Security” to find information related to the security of the DNS.

[13] formed the foundation and introduction into the topic of IoT and blockchain. In addition, it gave the first introduction to blockchain-based identity management. [13] together with [11] and [12] introduced a range of topics and specifics into the subject and provided references to specifics. For specific information about technologies, their original proposals were used, Request For Comments for DNS and PKI, and whitepapers for the different blockchain solutions. The proposed improvements build on work from the referenced works in both the background and analysis sections. It combines guidelines and proposals of related work into proposed improvements to mitigate the issues identified in the relevant technologies.

3 Related work

With the DNS being a legacy system, alternatives have been proposed before blockchain existed. In [14], an alternative to DNS is proposed that is more suitable for internet objects, possibly complementing the existing infrastructure. [10] proposed a distributed DNS alternative, before the blockchain’s distributed technology existed, it introduces extra servers to maintain copies and eliminate security risks. To remove the need for public static IPs for each device, [15] suggests Unmanaged Internet Architecture (UIA) to provide zero-configuration names for each device.

More recent papers propose and discuss DNS and PKI solutions based on blockchain technology. The first blockchain-based solution was Namecoin [16], based on talks about a hypothetical bitDNS. [17] performs a study on Namecoin, discussing the benefits and flaws of the Namecoin system. [18] introduces a solution based on the Namecoin infrastructure, called Blockstack. Blockstack uses a virtual chain to address issues of upgradability and security present in Namecoin. [19] focuses on the privacy aspect of current PKI solutions and proposes a blockchain-based solution to combat privacy issues, though increased privacy is achievable it does so at the cost of security. [20] performs a study on the current relationship between the DNS and the IoT, identifying the current issues for regular DNS and mDNS. An overview and comparison of various proposed solutions is given in [11] and [12], where the advantages and disadvantages of blockchain-based solutions are discussed. [21] defines general guidelines for reasoning about PKI, and the decentralized web, while also proposing an Ethereum [22] based PKI solution called Ghazal.

4 Background

This section provides the background on the underlying technologies. The first subsection briefly explains what a blockchain is, the basics of the IoT, and how both relate. Section 4.2 gives an overview of both the DNS and PKI technologies, introducing the basic concepts and issues related to these technologies.

4.1 Blockchain and the IoT

To understand how blockchain technology and the internet of things relate to each other. First, a basis of both blockchain and the IoT itself is required. This subsection first introduces both technologies, after which both are combined to show the relationship between the technologies.

4.1.1 Blockchain

Blockchain technology is a new technology that sees active research and development [23]. A blockchain is a distributed ledger shared among a network made up of nodes, with each node being a device. This ledger is a data structure that contains all transactions that occurred on the network. Internally this data structure uses blocks of data: each block contains

a set of transactions and keeps track of the previous block. Together these blocks create a chain where the full history of the ledger is recorded. A transaction on a blockchain is a record containing data. This data can be a financial transaction, as it is with cryptocurrencies, or be another type of data. Blockchain is known for its strong points:

- No need for trust in central authorities
- Immutability of the data
- Auditable
- Security

Each node contains a copy of the complete ledger and therefore can audit every transaction in the ledger's history. The other strong points of the blockchain are achieved with the help of a consensus algorithm: a consensus algorithm is a way to reach a decentralized consensus between the network's nodes, and it is based on strong cryptographic principles [9]. The consensus algorithm ensures that the blockchain is immutable and resistant to faults. In addition, it ensures that it is practically too difficult to tamper with the blockchain, this is achieved by requiring an amount of power in the network to achieve consensus. This power can consist of computational work, as in Proof of Work algorithms, or assets in the network as in Proof of Stake algorithms.

4.1.2 The Internet of Things

The Internet of Things, abbreviated IoT, is an upcoming category of computer devices [3]. The Internet of Things is built on two essential parts: the devices, Things, and the connectivity, the Internet [24]. Things on the Internet of Things are at their core computers but can differ greatly from a regular commercial computer. IoT Things often have one or more of the following characteristics [25]:

- Small: IoT devices can be found in all forms and sizes, but they can be multiple factors smaller than regular computers.
- Embedded: IoT devices are embedded in other items and are normally not visible from the outside. These devices can range from embedded sensors in a chemical plant to the internal controller of a smart fridge.
- Low computing power: Given the size and the location of IoT devices, they do not possess the computing power to process heavy tasks. This gives IoT devices the ability to have a small form factor since they do not require active cooling and have low power consumption.
- Specialized: An IoT device can be specialized for one specific task. A sensor device will only act as a sensor compared to general-purpose computers.
- Real-time: IoT devices, especially sensor devices, can generate large amounts of data, often in real-time. This characteristic is important in high-risk environments, such as chemical plants.
- No Human-Computer interaction: An important aspect that sets an IoT device apart from a general computing device is that it requires little to no human interaction. This ensures that a device can operate on its own without supervision. In addition, this allows devices to be placed in hard-to-reach or remote locations while the data is accessible.

The other aspect of the Internet of Things is connectivity. As is in the name, all IoT devices are connected over the internet. This is characteristic that all IoT devices share to be an IoT device, and this is also what makes other characteristics possible, like placing them in remote locations.

IoT has been deployed in many different contexts, from smart homes to appliances in agriculture, logistics, and the medical field [26]. Nevertheless, although IoT has been in use and is projected to grow to more devices, it also has its own fair share of issues [13; 27; 28]:

- Trust: The specialization of IoT devices makes them limited to their specialization. Nevertheless, the connection of multiple devices over the internet allows for a large interconnected system. To achieve this, IoT generally uses centralized cloud services to accumulate and process all data from a group of devices. This introduces the need for trust in two different places: firstly in the cloud service that the devices connect to, and secondly in the infrastructure that powers the internet, for example, DNS, DHCP, and PKI servers.
- Privacy: IoT devices handle all types of data, but this data contains personal and identifiable data, especially in the context of medical or smart-home devices. This becomes of uttermost importance when dealing with third-party services, as is the case with cloud services. In theory, data can be used for other purposes and possibly sold for advertisement and marketing purposes.
- Security: The computing capabilities on IoT devices leave little room for proper security implementations. Some issues can be attributed to poor implementation and poor configuration. Other devices lack the power and storage to facilitate cryptographic algorithms needed for encryption. Reliance on third-party services and infrastructure only further increases the vulnerability of these devices. In addition to a software approach to security, there is also a hardware side to the story. Physical access to a device can grant a malicious user access to the device's software and, therefore, data.
- Scalability: IoT devices generate a large amount of data, often in real-time. This causes a large load on the underlying internet infrastructure. As well as the ability to process data on a processing service.

This makes that while IoT devices have a useful purpose, there are problems that need to be considered. These problems require solving to ensure that the IoT services can be used securely, reliably, and trusted.

4.1.3 Blockchain and the IoT

If put together, IoT and blockchain technology seem to complement each other. Where IoT lacks in term of security and trust, blockchain technology excels [23]. For this specific reason, a combination of both technologies has gained attention in the last years [13]. However, putting blockchain and IoT together is not as straightforward as possible and introduces

new challenges. For example, both technologies can have issues with scalability: to support the amount of data coming from IoT devices, a blockchain should have a higher transaction throughput than Bitcoin and Ethereum [29]. In addition to that, IoT devices can lack both storage capacity and computing power. To be part of a blockchain, a device needs to be able to run a consensus algorithm. Especially algorithms like Proof of Work are known for their high demands on processing power [30]. Therefore, scalability and computational power pose important problems to integrating blockchain and IoT.

4.2 DNS and PKI: The Internet

The Internet is a complex system that, over the years, gradually grew, from having few components to a wide variety of architectural components [31]. Two of those components are DNS and PKI, this section gives an overview of both technologies, their uses, problems, and finally, their relation to the IoT.

4.2.1 Domain Name System

The DNS is a component of the Internet that manages the mapping of domain names to IP addresses [1]. The DNS was designed to generify and simplify the process of identifying hosts to be ready for the growth of the Internet. The DNS is designed in a decentralized hierarchical manner, where root servers point to domain-specific sub-servers. To perform a DNS domain look-up, a device will contact the root server, which will point to the specific domain server, this can continue until the device reaches the DNS server responsible for hosting the record of the domain. DNS is one of the older components of the Internet, and over the years, it has seen multiple extensions and changes [32]. One important extension of the DNS is the introduction of DNSSEC, which introduces security measures into the DNS [33; 34; 35].

With more than half of the world's population being online, the DNS handles large amounts of traffic [36]. However, despite the heavy usage, the DNS is also known for its flaws:

- Trust: Though the DNS is architecturally decentralized, it does require trust in a set of centralized root servers [1]. The design does allow for the possibility to add local or private DNS servers, but that does not change the need for root servers for non-local records.
- Security: The original DNS did not include security features [1], but with the introduction of DNSSEC, the DNS protocol added digital signatures based on the public key cryptography [37]. However, despite the formalization of DNSSEC, the deployment of DNSSEC is lackluster, as found by Chung *et al.* [38]. In addition, the DNS is a high-profile target for denial-of-service attacks and vulnerable to a wide range of attacks [5].
- Point of failure: As mentioned, DNS servers are high-profile targets for cyber attacks. These attacks can lead to the unavailability of a DNS server or group of servers. In addition, a disrupted or offline DNS server can provide incorrect address mapping. To combat this, the DNS and DNSSEC standards introduced zoning, which tries to resolve unavailability issues, but is still vulnerable to incorrect records.
- Internet censorship: Top-level domain and root domain servers are hosted by countries and large organizations. In over 60 countries, DNS level censoring is applied, where DNS records are altered or removed [7]. Internet censorship introduces issues for human rights organizations and human rights and is against the principles of a free Internet [39].

To mitigate these issues, DNS has seen a large number of patches since the first proposed implementation [40]. Unfortunately, as with the roll-out of the initial DNSSEC protocol, adoption is slow and leaves much to be desired. The discovery of new vulnerabilities will only make this problem larger. In addition, issues of trust and censorship cannot be resolved with new extensions to the DNS, as they come from the fundamental architecture of the system.

4.2.2 Public Key Infrastructure

To secure content and connections on the web, public-key cryptography is used. But the public keys are not guaranteed to have come from the owning entity. To solve this problem, public key infrastructure (PKI) was introduced [2]. PKI verifies the identity associated with a public key and stores this data in a digital signature. PKI is structured hierarchically, with root certificate authorities on top. Each following certificate authority can be verified by going up the chain to the root authorities. Root authorities have self-signed certificates and are included in most browsers and operating systems as a trusted root [41]. In practice, PKI is used to secure the web, it verifies the foundations TLS is built on and enables secure connections for the DNSSEC. PKI is therefore of importance to important components of the Internet and acts as supporting infrastructure.

In its existence, PKI has seen three main points of criticism [42; 6]:

- Trust: PKI works with a chain of trust, this means that an entity can go up the verification chain. But root certificates of CAs are self-signed, meaning that there is no upper authority. CAs and their certificates are trusted because entities within the Internet, such as the browser and operating system vendors, decided to. This introduces a need for trust, which is not quantifiable. This also means that once the root authorities are compromised, the chains fall apart. This results in a system with a single point of failure.
- Security: The PKI is a complex and expansive system, this also introduces multiple points of attack. The standard does take compromises into account by allowing certificates to expire and be revoked. In practice, not all breaches are detected immediately and can result in a delay between the breach and revokal [43]. In addition to software attacks, physical attacks are also possible. The private keys for root certificates and CAs are stored on physical locations. A breach of those private keys would mean a revokal of root certificates and be disruptive to the ecosystem. [42] summarizes the security of the PKI: "Security is a chain; it's only as strong as the weakest

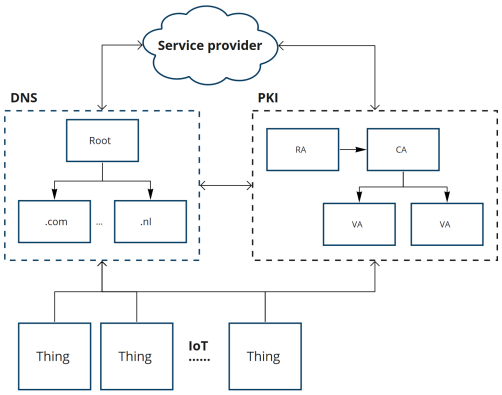

Figure 1: Simplified overview of current network architecture

link. The security of any CA-based system is based on many links and they're not all cryptographic".

- Conceptual: The PKI also brings up identification and legal issues. Identification issues relate to the fact that certificates establish a link between a key and an entity but do not provide hard links between the digital and physical entities. Legal issues come from repudiation, where the question arises if the owner of a key is responsible for what happens with the key, even if a third party gained access.

Public key infrastructure has allowed the Internet to become more secure by enabling TLS and DNSSEC. But despite those efforts receives criticism for its flaws in trust, security, and concept. Furthermore, as with DNS, PKI is a legacy system used by a large part of the Internet, therefore proposing alternative solutions also introduces issues with adoption.

4.2.3 DNS and PKI with the IoT

To connect to service providers, IoT makes use of the DNS and PKI infrastructure. The DNS is used to look up the service's domain, while the PKI is used to support the security protocols DNSSEC and TLS. The reliance on DNS and PKI means that IoT also inherits the flaws of those systems. This results in an IoT that is based on trust, insecure, and vulnerable to censorship. DNS-related security issues are nothing new to the IoT. A recent example, as of 2021, is the set of "NAME:WRECK" security vulnerabilities in the DNS implementation of 100m+ IoT devices [44]. This vulnerability makes devices potentially vulnerable to denial-of-service attacks and remote code execution. A simplified architectural overview of the DNS, PKI, and IoT is given in Fig. 1.

5 Analysis

To solve the issues of trust, security, and censorship, multiple solutions exist. Generally, these can be divided into two groups: non-blockchain solutions and blockchain solutions. Non-blockchain solutions focus on a subset of issues and can therefore only solve a subset of the issues present. Blockchain solutions offer the potential to solve all of the issues, but do also introduce new issues. This section first introduces and discusses non-blockchain solutions; afterward, several blockchain-based solutions are discussed.

5.1 Non-blockchain solutions

Non-blockchain-based solutions try to solve issues of the DNS and PKI using conventional, pre-blockchain methods. Some examples of this are local recursive DNS, secured distributed DNS, and mDNS.

5.1.1 Local recursive DNS

A local recursive DNS[45] is an improvement over the centralized DNS services from Google [46] and Cloudflare [47]. A local recursive DNS instance processes the DNS requests from devices, if the record is available, it is returned, if not, the server will perform a recursive search from the root DNS nodes[1]. This reduces the need for trust in large DNS services but does not fully eliminate trust since the recursive look-up is reliant on external servers. The server's security is moved from the centralized server to the local server, in itself, the security of the DNS server will not change [48]. The potential for censorship can be reduced since, with decentralization, the influence of the centralized server is reduced. However, individual servers in the look-up process can still impose censorship on the service.

5.1.2 Secure Distributed DNS

The Secure Distributed DNS proposed in [10] is the closest a solution could come to the blockchain without using blockchain. It ensures a decentralized, fault-tolerant system up to fault tolerance of one-third. The solution proposed increases fault tolerance and security compared to the conventional DNS, but does not address the issues of trust and censorship. The solution does not reduce the need for authoritative servers and therefore does not reduce the issues of trust and censorship. The addition of extra servers to reach a fault-tolerant network introduces extra latency for the end-user. An important issue this solution addresses is the issue of adoption. The proposed solution is compatible with the current DNS systems, removing the need to change and upgrade user devices. The adoption of alternative systems is discussed later in this section.

5.1.3 mDNS

Multicast DNS or mDNS is a small-scale variant for DNS, it is intended for deployment on a local scale [49]. Multicast DNS works without a centralized server infrastructure, instead, all devices are addressed directly. The requesting device sends a multicast over the network to all other devices, the addressed device then responds with another multicast to all devices on the network. The mDNS systems are defined to work with .local domain names and cannot process regular top-level domains. Multicast DNS improves on censorship compared to regular DNS by removing the centralized servers. MDNS removes the need for trust in centralized servers but operates under the assumption of cooperative devices [49]. This need for trust together with other issues such as cache poisoning [50], Make the mDNS insecure. Additionally, the high amount of traffic can impose problems on the underlying network architecture and requires too much computing power for some IoT devices [51].

5.2 Blockchain-based solutions

In comparison to the aforementioned solutions, the discussed blockchain-based solutions show similar benefits and drawbacks. Though their implementation differs, they are all based on blockchain technology and provide the benefits of that technology. Blockchain-based solutions increase the network security of the DNS and PKI due to their distributed nature [11]. This reduces the potential for attacks like (D)DoS to target a specific server or group of servers, increasing the overall security and, therefore, availability of the network. Additionally, the immutability of a blockchain removes the potential for DNS-specific attacks like cache poisoning. This is achieved by the need for consensus on the whole network. The immutability of the data and the distributed nodes reduce the power of an institution on the network. This reduces the need for trust in a single authority to provide the proper service and reduces the ability of an institution to impose censorship. Instead of altering one server, it requires the altering party to have enough participation in the blockchain network to research consensus on their own. This means that blockchain-based DNS and PKI can address the issues of trust, security and censorship simultaneously, compared to current and non-blockchain-based solutions. Though blockchain-based solutions have these common characteristics, individual solutions differ. In this paper, four different solutions are mentioned and analyzed: Namecoin, Blockstack, Ethereum Name Services (ENS), and EmerDNS.

5.2.1 Namecoin

Namecoin is the first blockchain-based solution that offers an alternative to the existing DNS infrastructure [16]. Namecoin is based on the Bitcoin framework and provides the option to create decentralized namespaces, of which the DNS is one. Namecoin provides the ability to create domain names with the .bit extension. In [17] multiple problems with the Namecoin system were identified. A major issue with the Namecoin system is the lack of participation on the network, this resulted in one party having over 51% of the network's power. This breaks the Namecoin system and makes it possible to alter and censor records on the system. In addition, Namecoin only offers the additional .bit domain extension and does not support standard extensions. In the context of the IoT, Namecoin is not feasible since it uses Proof of Work. This is a type of consensus that requires too much computational power for the IoT.

5.2.2 Blockstack

The Blockcstack framework [18], builds on the foundation of Namecoin and tries to address numerous issues of the Namecoin ecosystem. Blockstack introduces a model that builds on a virtual chain, a layer in between the blockchain and the users, to provide a DNS and PKI solution. This virtual chain is agnostic to the blockchain underneath and allows for cross-chain migrations. By moving to Bitcoin instead of Namecoin, Blockstack mitigates the security issues related to Namecoin but does experience transaction scalability issues related to Bitcoin. The ability to migrate to different blockchains reduces problems related to forking and protocol upgrades and allows Blockstack to move away from a Proof of Work protocol later.

5.2.3 Ethereum Name Services

Ethereum Name Services offers naming services [52] based on the Ethereum blockchain [22]. ENS allows for Ethereum domain names with the .eth extensions, in addition, it provides support for some regular top-level domain extensions. The registration of regular top-level domains will automatically synchronize with the ENS, providing access to regular domains on the blockchain. To achieve this, ENS uses the ENS root, which is managed by a group of up to 7 individuals from different foundations. This takes away from the full decentralization Ethereum offers by default. In addition, Ethereum uses Proof of Work and experiences high network latency and transaction fees [53], making it unsuitable for most IoT devices due to the computational power. However, this is set to be resolved with the migration to Ethereum 2.0 [54].

5.2.4 EmerDNS

EmerDNS is similar to Ethereum Name Services but builds on Emercoin instead of Ethereum [55]. It is part of the EmerNVS identity management suite, which provides both DNS and PKI services. Emercoin uses a hybrid approach between Proof of Work, merge-mined with Bitcoin, and Proof of Stake. Similar to ENS, EmerDNS provides the option to use blockchain-only domain extensions such as .coin, .emc, .lib, .bazar or can be used to set up a local DNS server. EmerDNS does not provide services to synchronize between regular TLDs and blockchain-based TLDs.

5.2.5 Issues

The problems of these blockchain-based solutions can roughly be summarized into two problems. Firstly they are too computationally heavy to be used in the context of the IoT, this is especially true for Namecoin. Blockstack could theoretically move to another chain, Ethereum should eventually move on to ETH 2.0 with Proof of Stake. From these four examples, only EmerDNS provides an option other than Proof of Work by default. The second problem with these solutions is interoperability with the current system. Only ENS provides limited support for regular TLDs but still requires extensions to provide this to regular users. Browser extensions such as PeerName [56] and Blockchain-DNS [57] provide seamless integration of regular DNS and blockchain-based DNS for the end-users. Alternative DNS network solutions that run a regular DNS that ICANN does not regulate, such as OpenNIC [58], support blockchain-based TLDs but do not use alternative technologies such as blockchain. In addition, there are other issues related to specific blockchains, such as high fees and block processing times in both Bitcoin and Ethereum.

6 Discussion

Both blockchain-based and non-blockchain-based solutions can help resolve issues with the current infrastructure. Though non-blockchain-based solutions can offer improvements on one aspect, such as trust, they will do so at the cost of another, such as security. Blockchain-based solutions can provide improvement simultaneously on trust, security, and censorship compared to the current infrastructure.

Though proposed blockchain-based solutions offer improvements, they do so at the cost of new disadvantages. Most importantly, lack of integration with current systems and incompatibility with the IoT ecosystem in terms of computational power. This section proposes points of improvements future blockchain-based DNS solutions should incorporate to mitigate the problems current blockchain-based solutions have.

6.1 Functionalities

To accommodate migration from the current ecosystem, it is required that a blockchain-based solution offers the same amount of functionalities. This means that all types of record features in the DNS system should also be compatible with the blockchain system. A comparable system in functionality also helps with adopting a system since there is no loss of functionality. Registration of an entry could follow a similar pattern to that used in Namecoin, where registration is first announced and only after 12 or more blocks the actual registration is performed [16]. This reduces the chance of block propagation resulting in a registration collision. In addition, functionalities to alter, transfer and delete a registration are provided. With the current DNS, registrations can expire and are not always reregistered by mistake. This allows third parties to take over ownership of important domain names. To prevent this problem, blockchain-based registrations are permanent.

6.2 Integration and Adoption

As seen in the case of Namecoin, a lack of adoption can cause significant problems for the functionality and security of a blockchain. An important aspect of adoption is the integration with existing services. A solution that does not address the current existing ecosystem will fail to gain adoption since it would make almost all of the Internet incompatible. Therefore a blockchain-based solution should offer compatibility with existing services, as is done partially in the ENS ecosystem. A system where existing TLDs can synchronize with the blockchain ecosystem means that the DNS infrastructure can migrate away from the current solution. This would provide a lower entry bar for users registering a new domain into the blockchain ecosystem. However, this means that the current issues will keep existing as long as the migration is not complete. In addition, a blockchain-based solution would benefit by using a commonly used blockchain in terms of adoption. This would reduce the potential of having too few users on the network to protect against common blockchain attacks such as the 51% attack.

6.3 Technical Features

Out of the mentioned solutions, only EmerDNS provided an alternative to the Proof of Work consensus algorithms by allowing Proof of Stake [55]. As stated in [59], currently, none of the consensus algorithms can sufficiently address blockchain issues for the IoT. Therefore a solution is to change the type of devices that run the blockchain nodes. The recommended restriction on the type of consensus algorithm is not to use Proof of Work. Even if a device can run a Proof of Work blockchain, this is a waste of computational power and energy compared to alternatives [30]. As for the different

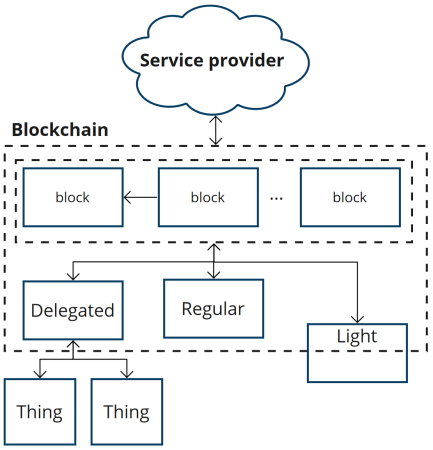

Figure 2: Example architecture containing delegated, regular and light nodes

type of devices, this paper proposes the following three types of nodes:

- Regular nodes: Regular nodes are devices that are capable of running and storing a blockchain. Since the DNS and PKI are concerned with both the IoT and the Internet in general, a blockchain solution should not only support IoT. Within this category of devices fall classic computers such as desktop PCs and servers, but also larger IoT devices with sufficient computational power. These nodes can benefit from blockchain technology fully and provide the lowest latency of the three types. A local index can be built to more efficiently search the blockchain to speed up the record look-up.
- Delegated nodes: Delegated nodes are useful for devices that are too resource-constrained to run a blockchain, within this category fall most IoT devices. A delegated node is a device capable of running the blockchain for other devices. For example, this could be a server representing a group of sensors in an assembly line. The devices dependent on this delegated node interact with this node and do not directly address the blockchain. However, a delegated node does offer reduced improvements in trust and availability by introducing a local point of failure.
- Light nodes: Light nodes are devices that run the blockchain but do not store the full blockchain, as is done with Ethereum in [60]. This type of node provides a middle-ground between delegated and regular nodes. It offers improved trust over delegated nodes but for a smaller range of devices. Compared to regular nodes, it introduces extra latency because of the need to connect to a regular node on the network. A light node can perform management on a registered name or provide additional trust when additional latency is not a problem.

An overview of this structure is given in Fig. 2, and in the long term, it should replace all existing DNS and PKI infrastructure, but at the start, it would use a hybrid environment with both solutions, for increased adoption. The differ-

ent types of nodes can address a large range of devices while providing the benefits of a blockchain-based system over the current systems.

7 Conclusions and Future Work

The current DNS and PKI infrastructure is not sufficient enough to accommodate proper services. As a result, trust in companies, institutions, and governments to provide these services has been compromised on multiple occasions. Their power over the centralized system has allowed them to impose censorship on users. In addition, security issues have led to unavailability and a loss of data integrity, while mitigations have failed to address this properly. The Internet of Things has inherited these same issues by leveraging the services provided.

To address these issues, both non-blockchain-based and blockchain-based have been proposed. Non-blockchain-based solutions can address some of the issues present but do so at the cost of others. On the other hand, blockchain-based solutions can offer improved trust, network, and data security and reduce censorship possibilities. But currently proposed solutions have issues related to adoption due to the lack of interoperability with current systems, and computational power makes them infeasible for the IoT. The proposed theoretical improvements of this paper aim to provide a solution to the problems of blockchain-based solutions. The issue of adoption is addressed by synchronizing current systems with a new blockchain-based system and leveraging an existing blockchain ecosystem.

The problem of computational power with the IoT is addressed by differentiating between three types of nodes: Regular nodes that run the full blockchain on devices that provide enough computational power; Delegated nodes which can run the full blockchain on a dedicated blockchain node to represent a group of devices incapable of running a blockchain, this is done at the cost of trust; Light nodes which can run the blockchain but do not need to store the full blockchain, which can achieve improved trust over delegated nodes at the cost of extra latency.

With these improvements, blockchain-based DNS and PKI solutions can address current issues with blockchain-based solutions, especially in the context of the IoT. Though, multiple points of interest and potential research questions remain:

- This paper only proposes theoretical improvements over existing solutions in this field. Future research could focus on implementing these improvements in a proof of concept or an actual system. This would also open up a way to gain quantifiable analytical data to make further claims about the performance of such a system.
- An important aspect of the DNS and PKI system that is not addressed in this paper is privacy. Privacy in this context relates to the profiling of both users and devices based on the requests they make. Future research could evaluate and possibly improve the privacy aspect of a proposed system.
- Though improvements are suggested to increase the adoption of a new system, the proposed additional hardware would require changes on an end-user side. This means that users would need to change from a current system to a new system. Therefore a less technical but important aspect of a new system would be user willingness to migrate from existing services.
- To accommodate the synchronization of proposed and legacy systems, current operators are required to cooperate. However, this cooperation would require operators to change or end their DNS and PKI-related services, posing problems to adoption. A problem like this is already apparent in current systems, where the roll-out of DNSSEC has been slow at the cost of end-user security.

8 Ethical and Responsible Research

Though this paper does only deal with theoretical concepts, ethical questions are of importance. Two main ethically concerned subjects emerge from the contents of this paper: Internet censorship and the use of blockchain technology. Internet censorship deals with the oppression of people's freedom to look up information on the internet and the repression of freedom of speech by disabling online places to do so [61]. To combat the ability to perform this type of censorship, this paper identifies blockchain technology as a solution to do so by reducing the power of institutions over the services where censorship is performed. But blockchain technology does come with its own ethical dilemmas. Blockchain technology is criticized for its energy consumption, especially when using the Proof of Work consensus algorithm [30]. This paper addresses this issue by recommending against this type of consensus algorithm. A second ethical issue related to blockchain relates to the anonymity of such a framework. This is a point criticized as facilitating a place for illegal activities [62]. Though this paper does not fully address this point, a blockchain-based solution would not facilitate financial transactions but the mapping of names and values.

In addition to the ethical aspects based on the content, responsible research and reproducibility issues are of importance. Though this paper does not contain any analytical data, this still allows for reproducibility. Section 2 provides insight into the applied methodology for this research and discusses search term keywords; Section 3 provides the reference framework of work done by other authors; Section 4 contains the foundation of this paper, providing an extensive overview of the technologies and problems. The analysis section discusses both blockchain and non-blockchain-based solutions evaluating advantages and downsides. The proposed improvements are supported by argumentation and are based on verifiable issues with other solutions. The final section mentions the open questions left to be answered and indicates potential issues with the proposed improvements. All combined give an overview of the path taken from problem statement to proposed improvements, where arguments and references support claims to ensure reproducibility.

References

[1] P. V. Mockapetris, "Rfc1034: Domain names-concepts and facilities," 1987.

[2] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu, "Rfc3647: Internet x. 509 public key infrastructure certificate policy and certification practices framework," 2003.

[3] M. Presser, "The rise of iot–why today," *First Published on January*, vol. 12, p. 2016, 2016.

[4] P. De Filippi, M. Mannan, and W. Reijers, "Blockchain as a confidence machine: The problem of trust challenges of governance," *Technology in Society*, vol. 62, p. 101284, 2020. [Online]. Available: https://dx.doi.org/10.1016/j.techsoc.2020.101284

[5] T. H. Kim and D. Reeves, "A survey of domain name system vulnerabilities and attacks," *Journal of Surveillance, Security and Safety*, vol. 1, no. 1, pp. 34–60, 2020.

[6] D. Cvrcek, "Real-world problems of pki hierarchy," in *Proceedings of the SPI Conference, Brno Czech*. Citeseer, 2001, pp. 39–46.

[7] P. Pearce, B. Jones, F. Li, R. Ensafi, N. Feamster, N. Weaver, and V. Paxson, "Global measurement of {DNS} manipulation," in *26th {USENIX} Security Symposium ({USENIX} Security 17)*, 2017, pp. 307–323.

[8] M. Roberts and M. E. Roberts, *Censored*. Princeton University Press, 2018.

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[10] C. Cachin and A. Samar, "Secure distributed dns," in *International Conference on Dependable Systems and Networks, 2004*, 2004, pp. 423–432.

[11] E. Karaarslan and E. Adiguzel, "Blockchain based dns and pki solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 52–57, 2018.

[12] Faizan and A. Kupcu, "Improving pki, bgp, and dns using blockchain: A systematic review," *arXiv pre-print server*, 2020. [Online]. Available: https://arxiv.org/abs/2001.00747

[13] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019. [Online]. Available: https://ieeexplore.ieee.org/ielx7/9739/8727625/08580364.pdf?tp=&arnumber=8580364&isnumber=8727625&ref=

[14] M. Walfish, H. Balakrishnan, and S. Shenker, "Untangling the web from dns," in *NSDI*, vol. 4, Conference Proceedings, pp. 17–17.

[15] B. Ford, J. Strauss, C. Lesniewski-Laas, S. Rhea, F. Kaashoek, and R. Morris, "Persistent personal names for globally connected mobile devices," in *Proceedings of the 7th symposium on Operating systems design and implementation*, 2006, pp. 233–248.

[16] "Namecoin whitepaper." [Online]. Available: https://www.namecoin.org/resources/whitepaper/

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

[18] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: Design and implementation of a global naming system with blockchains," *Last visited on*, vol. 25, no. 2, 2016.

[19] L. Axon and M. Goldsmith, "Pb-pki: A privacy-aware blockchain-based pki," 2016.

[20] A. Hamzic and I. Olofsson, "Dns and the internet of things: Outlining the challenges faced by dns in the internet of things," 2016.

[21] S. Moosavi, "Rethinking certificate authorities: Understanding and decentralizing domain validation," Thesis, 2018.

[22] V. Buterin, "Ethereum whitepaper." [Online]. Available: https://ethereum.org/en/whitepaper/

[23] H. Treiblmaier, *Toward More Rigorous Blockchain Research: Recommendations for Writing Blockchain Case Studies*, 2018.

[24] O. Mazhelis, E. Luoma, and H. Warma, "Defining an internet-of-things ecosystem," in *Internet of Things, Smart Spaces, and Next Generation Networking*, S. Andreev, S. Balandin, and Y. Koucheryavy, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 1–14.

[25] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the internet of things (iot)," *IEEE Internet Initiative*, vol. 1, no. 1, pp. 1–86, 2015.

[26] I. Lee and K. Lee, "The internet of things (iot): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0007681315000373

[27] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804517301455

[28] P. Goyal, A. K. Sahoo, T. K. Sharma, and P. K. Singh, "Internet of things: Applications, security and privacy: A survey," *Materials Today: Proceedings*, vol. 34, pp. 752–759, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S221478532033385X

[29] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, "Blockchain and scalability," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 2018, pp. 122–128.

[30] A. Fiat, A. Karlin, E. Koutsoupias, and C. Papadimitriou, "Energy equilibria in proof-of-work mining," in *Proceedings of the 2019 ACM Conference on Economics and Computation*, 2019, pp. 489–502.

[31] B. M. Leiner, V. G. Cerf, D. D. Clark, R. E. Kahn, L. Kleinrock, D. C. Lynch, J. Postel, L. G. Roberts, and S. Wolff, "A brief history of the internet," *SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 5, p. 22–31, 2009. [Online]. Available: https://doi.org/10.1145/1629607.1629613

[32] R. RADER, "One history of dns," *Byte. org*, 2006.

[33] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "Dns security introduction and requirements," RFC 4033 (Proposed Standard), Tech. Rep., 2005.

[34] ——, "Resource records for the dns security extensions," RFC 4034 (Proposed Standard), Report, 2005.

[35] ——, "Protocol modifications for the dns security extensions," RFC 4035, March, Tech. Rep., 2005.

[36] M. Meeker and L. Wu, "Internet trends 2018," 2018.

[37] T. Chung, R. van Rijswijk-Deij, B. Chandrasekaran, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, and C. Wilson, "A longitudinal, end-to-end view of the {DNSSEC} ecosystem," in *26th {USENIX} Security Symposium ({USENIX} Security 17)*, 2017, pp. 1307–1322.

[38] ——, "A longitudinal, end-to-end view of the {DNSSEC} ecosystem," in *26th {USENIX} Security Symposium ({USENIX} Security 17)*, 2017, pp. 1307–1322.

[39] P. Brophy and E. Halpin, "Through the net to freedom: information, the internet and human rights," *Journal of Information Science*, vol. 25, no. 5, pp. 351–364, 1999. [Online]. Available: https://doi.org/10.1177/016555159902500502

[40] A. Herzberg and H. Shulman, *Security of Patched DNS*. Springer Berlin Heidelberg, 2012, pp. 271–288. [Online]. Available: https://dx.doi.org/10.1007/978-3-642-33167-1_16

[41] G. Huston, S. Weiler, G. Michaelson, and S. Kent, "Resource public key infrastructure (rpki) trust anchor locator," RFC 6490. Internet Engineering Task Force, Tech. Rep., 2012.

[42] C. Ellison and B. Schneier, "Ten risks of pki: What you're not being told about public key infrastructure," *Comput Secur J*, vol. 16, no. 1, pp. 1–7, 2000.

[43] N. Leavitt, "Internet security under attack: The undermining of digital certificates," *Computer*, vol. 44, no. 12, pp. 17–20, 2011.

[44] D. Santos, S. Dashevskyi, A. Amri, J. Wetels, S. Oberman, and M. Kol, "Name:wreck," Report, 2021. [Online]. Available: https://www.forescout.com/company/resources/namewreck-breaking-and-fixing-dns-implementations/

[45] J. Salmela. Pi-hole - network-wide ad blocking. [Online]. Available: https://pi-hole.net/

[46] Google, "Introduction to google public dns." [Online]. Available: https://developers.google.com/speed/public-dns/docs/intro

[47] ——, "What is 1.1.1.1?" [Online]. Available: https://www.cloudflare.com/learning/dns/what-is-1.1.1.1

[48] A. M. Taib, M. T. Zabri, N. A. M. Radzi, and E. A. Kadir, "Netguard: Securing network environment using integrated openvpn, pi-hole, and ids on raspberry pi," in *Charting the Sustainable Future of ASEAN in Science and Technology*. Springer, 2020, pp. 97–110.

[49] S. Cheshire and M. Krochmal, "Multicast dns," RFC 6762, February, Tech. Rep., 2013.

[50] A. Atlasis, "An attack-in-depth analysis of multicast dns and dns service discovery," *slides presented in*, 2017.

[51] A. Hamzic and I. Olofsson, "Dns and the internet of things: Outlining the challenges faced by dns in the internet of things," 2016.

[52] "Ethereum name services." [Online]. Available: https://docs.ens.domains/

[53] J. E. de Azevedo Sousa, V. Oliveira, J. Valadares, G. Dias Goncalves, S. Moraes Villela, H. Soares Bernardino, and A. Borges Vieira, "An analysis of the fees and pending time correlation in ethereum," *International Journal of Network Management*, vol. 31, no. 3, p. e2113, 2021.

[54] P. Fairley, "Ethereum will cut back its absurd energy use," *IEEE Spectrum*, vol. 56, no. 1, pp. 29–32, 2019. [Online]. Available: https://dx.doi.org/10.1109/MSPEC.2019.8594790

[55] "Emerdns." [Online]. Available: https://emercoin.com/en/emerdns

[56] "Blockchain-based amp; decentralized domains." [Online]. Available: https://peername.com/

[57] "Blockchain-dns." [Online]. Available: https://blockchain-dns.info/

[58] "Opennic project." [Online]. Available: https://www.opennic.org/

[59] M. Salimitari, M. Chatterjee, and Y. P. Fallah, "A survey on consensus methods in blockchain for resource-constrained iot networks," *Internet of Things*, vol. 11, p. 100212, 2020. [Online]. Available: https://dx.doi.org/10.1016/j.iot.2020.100212

[60] E. Reilly, M. Maloney, M. Siegel, and G. Falco, "A smart city iot integrity-first communication protocol via an ethereum blockchain light client," in *Proceedings of the International Workshop on Software Engineering Research and Practices for the Internet of Things (SERP4IoT 2019), Marrakech, Morocco*, 2019, pp. 15–19.

[61] C. S. Leberknight, M. Chiang, H. V. Poor, and F. Wong, "A taxonomy of internet censorship and anti-censorship," in *Fifth International Conference on Fun with Algorithms*, 2010.

[62] S. Foley, J. R. Karlsen, and T. J. Putniņš, "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?" *The Review of Financial Studies*, vol. 32, no. 5, pp. 1798–1853, 04 2019. [Online]. Available: https://doi.org/10.1093/rfs/hhz015