Blockchain Based DNS and PKI Solutions

Enis Karaarslan and Eylul Adiguzel

Abstract

Domain name systems and certificate authority systems may have security and trust problems in their implementation. This article summarizes how these systems work and what the implementation problems may be. There are blockchain-based decentralized solutions that claim to overcome those problems. We provide a brief explanation on how blockchain systems work, and their strengths are explained. DNS security challenges are given. Blockchain-based DNS solutions are classified and described in detail according to their services. The advantages and feasibility of these implementations are discussed. Last but not least, the possibility of the decentralized Internet is questioned.

Introduction

Internet users rely on the domain name system (DNS) and public key infrastructure (PKI) to connect to a network service, mainly the web. These systems are centralized, but blockchain-based decentralized solutions are also possible.

DNS infrastructure is summarized in Fig. 1. The centralized version is shown on the left side of the figure. The user resolves a domain name to an IP address by asking the configured (local) DNS server. If the local server already knows the address (authoritative server or cached), it will answer directly to the user. Otherwise, the server will ask the DNS root servers and top-level domain (TLD) servers to locate the authoritative server for that domain name. The local DNS server will then ask that server to learn the IP address and then inform the user.

Decentralized DNS usage is shown as the Trust Zone in Fig. 1. The user will ask the decentralized DNS node for the specific domains (.bit, .id, etc.) it serves. This node will answer the user directly, as it keeps all the records for these domains. All blockchain-based DNS nodes are connected to the peer-to-peer (P2P) network and synchronize the records in between.

The anatomy of a web connection is given in Fig. 2. The user initially learns the IP address to connect to the web server. The trustworthiness of the domain name that is used along with this IP address should also be controlled. Digital certificates are used to certify the ownership of a domain name and are also used in the encryption of the web traffic. These certificates are distributed by the certificate authorities (CAs). CA servers issue digital certificates for identification of websites. The authenticity of a public key can be ensured via its digital certificate. Users rely on these signatures to get a secure connection during the HTTPS process, for the confidentiality of the web traffic. HTTPS relies on the SSL/TLS and X.509 technologies for its security. TLS relies on certificates, which are encrypted by X.509 PKI for authentication. Digital certificates keep cryptographic signatures to prove the authenticity, and contain a public key and information.

DNS and PKI run as hierarchical systems and the users trust on their working right. These systems are vulnerable to several attacks, such as denial of service/distributed denial of service (DoS/DDoS) attacks, DNS spoofing, and DNS cache poisoning. The DNS or CA servers can be compromised by attackers or used by governments to intercept the sessions of their citizens. For instance, Comodo CA was attacked, and nine fraudulent SSL certificates to seven web domains (google.com, yahoo.com, skype.com, etc.) were generated in 2011 [1]. The Dutch CA DigiNotar was compromised in 2011, and the attacker gained control of all certificate-issuing servers. The attack is said to have lasted four months, and the attacker probably issued some rogue certificates [2]. Governments, such as the Taiwanese government who intended to block Google's public DNS service recently, may also want to prevent their citizens from reaching some global DNS servers.

There are solutions like DNS certification authority authorization (CAA) and DNSSEC to overcome some of the attacks but there are not enough for the misuse by the governments. Distributed solutions can also be possible as a solution to availability and integrity problems. These systems run on peer-to-peer (P2P) networks. Blockchain technology can be used, which is a new paradigm that aims to eliminate centralized control. Decentralized solutions are possible with these technologies.

In the next section, DNS standards and the blockchain are discussed. DNS security challenges are given in the following section. Then blockchain-based DNS and DPKI implementations and practical experiences are discussed. In the last section, our conclusion is given, and possible future work is discussed.

DNS and PKI Standards

The DNS's working scheme is stable, well known, and described by many requests for comments (RFCs). The Internet name servers store the DNS records for their authorized domain. The root servers keep a record of the authoritative servers. The Internet name servers are configured with the list of the root servers.

Digital Object Identifier:
10.1109/MCOMSTD.2018.1800023

The authors are with Mugla Sitki Kocman University.

2471-2825/18/$25.00 © 2018 IEEE

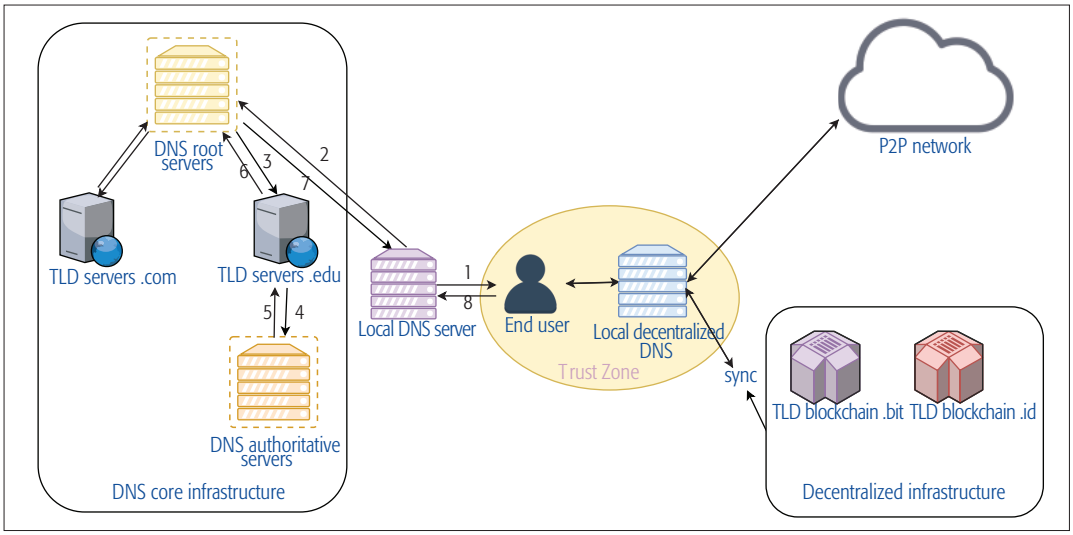

FIGURE 1. Centralized vs. decentralized DNS infrastructure.

The preferred DNS server (the resolver) usually keeps a cache of the previously asked records. If it does not know the answer to the query, it starts the resolution process with a query to one of the root servers. The root servers respond with a referral to the authoritative servers in the hierarchy. The resolver asks the referred servers iteratively until an authoritative answer is received. This iterative approach is described in RFC 1034 [3].

The DNS namespace works in a hierarchical manner because of the design of the DNS. RFC 2826 [4] states the importance of a single and globally unique root and warns that inconsistencies may occur at the instance of different roots. This also requires a unique naming authority.

There are other DNS mechanisms, which are also called alternative DNS, that run their own DNSs. The blockchain-based DNSs do not operate in a hierarchical manner. The nodes of the network are connected to the P2P network, and each keeps all of the records. The blockchain-based ones are:

- Blockstack: provides top-level domain (.id)
- Emercoin: provides top-level domain (.coin, .emc, .lib, .bazar)
- Ethereum Name Services (.eth)
- Namecoin: provides top-level domain (.bit)

The use of cryptography is needed for the confidentiality of the data transferred in the network. Both sides of the communication need cryptographic keys. Asymmetric (public) key cryptography was developed to solve the key distribution problem of the symmetric encryption. Public key infrastructure (PKI) provides authentication and public key distribution with asymmetric encryption. The system maintains a database of identity and public key pairs. There are two main approaches to serve this purpose: centralized PKI and decentralized PKI.

Centralized PKI is the X.509 standard, which has been used for PKI since 1988. HTTPS uses TLS/SSL based on X.509 certificates. The X.509 certificate is formed of a public key and the identity. It is mostly signed by a CA to be trusted. X.509 also defines certificate revocation lists (CRLs), which are used to provide a trust chain [5]. The CA is the foundation for delivering and managing digital certificates for the network of

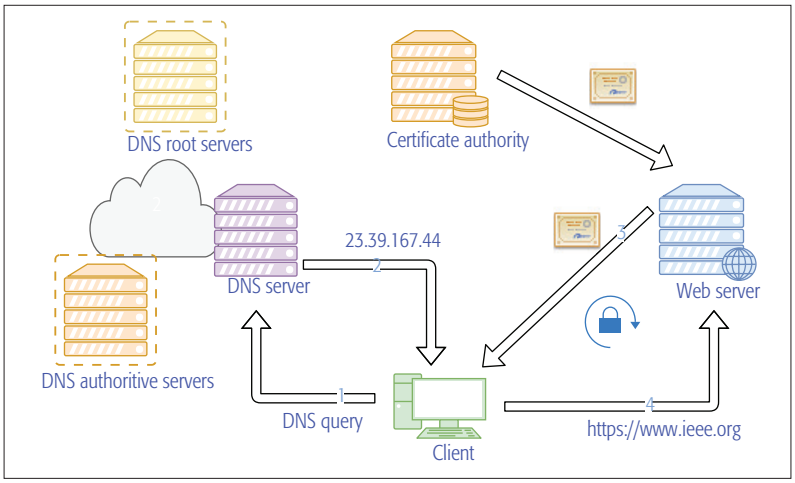

FIGURE 2. Anatomy of a web connection.

users. The user identity first has to pass through a registration process in the CA servers. The user's identity has to be verified, a distinguished name (DN) is assigned, and their public keys are recorded along with their DN. The records also include an expiration date, as well as an indication of the key's purpose (encrypting data or verifying a signature). The task of the CA is to sign the public keys with the CA's private keys and submit them to the third parties. The public key of the CA is well known and trusted. The user shares the public key with the CA, and the CA checks the user's identity and then signs the public key. After this process, the user will use the CA signed public key during the communication. The other party of the communication can check if the public key is properly signed by the CA.

Decentralized PKI (DPKI) is a decentralized trust model that provides integrity and security. It is an alternative to the centralized trust model of the PKI, which generally depends on a CA. This is also called P2P certification, and is often referred to as the web of trust. The web of trust is a concept that is used in pretty good privacy (PGP) and alike systems to establish the authenticity of the connection between a public key and its owner.

Blockchain technology is not feasible for all problems. It is appropriate to use this technology for a solution in environments, where it is necessary to provide trust between multiple parties and share data [10]. There is a potential for using it in identity management, transaction records, documentation of resources, food traceability, voting systems and similar record management activities.

DNS/CA based attacks/challenges	Legacy solutions	Blockchain-based solutions
DDoS attacks against DNS/CA servers	Difficulty: hard. Increased number of servers, DDoS mechanisms ...	Immune Service: availability
Server damage caused by ransomware/ destroyware derived cyber attack, shutdown of the DNS/CA servers by the authorities or disasters	None. User has to change the DNS address manually to overcome.	Immune Service: availability
Altering specific DNS/CA records on the server	Difficulty: moderate. Server and DNS security measures and monitoring process, which depend on the capabilities of the system admin or the security professional	Immune Service: integrity
Attack on the client to alter the DNS address during session	Difficulty: moderate. End-to-end-deployment of DNSSEC protocol to sign the address info	Immune Service: integrity, authentication

Table 1. DNS/CA challenges and security solutions.

Users can nominate others as trustworthy by signing their public keys.

Legacy DNS implementations do not specify the associated CA servers, but a new paradigm aims to change that. DNS records can be configured to specify the CA servers, which are authorized to issue certificates for that domain. This is specified in RFC 6844, which is currently an Internet Engineering Task Force (IETF) Proposed Standard [6]. The CA authorization (CAA) DNS resource record is proposed to enable additional controls by a public CA. According to the current Qualys report [7], the usage of CAA records is only 3.4 percent among the 150,000 most popular websites.

DNS and CA Security Challenges

There can be serious security problems in the DNS and CA implementations which are given in Table 1. These attacks are against the following security services:

- Availability: The DNS and CA servers are targets of DDOS attacks and physical shutdown conditions. Users will have problems getting service during such cases.
- Integrity and authentication: DNS and CA records can be altered. Fortunately, security measures like DNS CAA and DNSSEC are usable for DNS attacks. Changing the CA records is harder to detect by users. The certificate only shows that it is obtained from a CA, but it does not show whether the certificate is legitimate or not. The attacker might obtain a similar name from another CA. The user can be directed to the attacker's website, which is called the man in the middle (MITM) attack.

As can be seen in Table 1, blockchain-based solutions are immune to most attacks because of the following characteristics:

- The records are immutable. Records can only be changed with the consensus of all of the nodes.
- All the nodes have the full database. The database should be consistent.
- The strength of the infrastructure will be higher as the number of nodes increase.

Blockchain-Based DNS and DPKI

The blockchain system is formed as a P2P network of nodes running the same protocol. Each transaction should be recorded. These records are kept in a chain of blocks called a ledger. The system is durable to tampering by design. The blocks in the ledger are linked and secured using cryptographic hash functions like the SHA algorithm. Each block usually contains transaction data, a timestamp, and a hash, which is a pointer to the previous block. The nodes of the system make a joint decision by using the consensus protocols running on each node. To verify new blocks or change them, all peers have to communicate and agree on it. Proof-of-work (PoW) protocol is used widely, which depends on the mining process. However, different consensus protocols such as proof of stake (PoS) are possible [8].

Blockchain is secure, transparent, and distributed by design. Blockchain systems are widely used for cryptocurrency today. The identity verification (authentication) is mostly done by asymmetric cryptology. The public wallet address is the public key, and the private key is formed by implementing cryptographic functions. These keys are used for the key distribution of the session key, which will be used to encrypt the communication (providing confidentiality) and to sign the transactions (providing integrity and authenticity) [9].

However, blockchain technology is not feasible for all problems. It is appropriate to use this technology for a solution in environments where it is necessary to provide trust between multiple parties and share data [10]. There is potential for using it in identity management, transaction records, documentation of resources, food traceability, voting systems, and similar record management activities.

There can be scalability problems as the system can slow down under heavy traffic. New solutions, such as Lightning and Plasma, are proposed to mitigate the scalability issues. Transactions will not need a consensus process in the Lightning network when the parties of the transaction trust each other. This will speed up the transaction process; also, transactions will not be written on the chain. Some decentralized

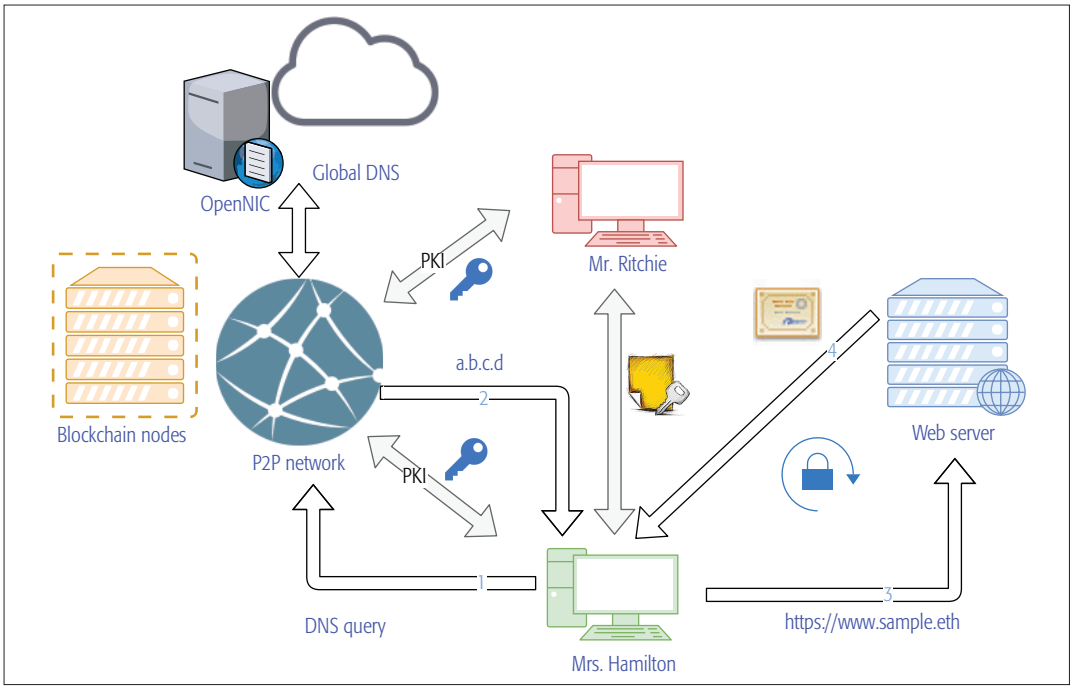

FIGURE 3. Blockchain based DNS and DPKI.

applications (dApps) may generate too many transactions on the blockchain, so solutions like Plasma propose that each dApp operates on its own separate blockchain.

A blockchain-based DNS and DPKI usage scenario is given in Fig. 3. There is no need for a CA, as the public keys are kept in the blockchain as a DPKI infrastructure. These keys will be used for the cryptographic functions between the users, Mrs. Hamilton and Mr. Ritchie. Mrs. Hamilton will obtain the digital identity (public key and personal details) of Mr. Ritchie from the P2P network.

The blockchain-based solutions do not provide the standard domains, so they cannot be thought of as a replacement for the legacy system. They are hosting-specific domains like .bit and .eth. The domain name database is kept in the ledger, and all the nodes of that system have the same database. Blockchain-based solutions have peering agreements with OpenNIC, which aims to be a non-national democratic alternative to the traditional domain registries. OpenNIC provides global DNS namespace and also the blockchain-hosted domains. OpenNIC servers (https://servers.opennicproject.org/) are available for public use. The OpenNIC server works in a centralized way, so the system represents a hybrid model, where decentralized blockchains work along with the centralized solution.

The main blockchain-based solutions are classified in Table 2. Most blockchain-based DNS solutions focus on the name resolution. Ethereum does have an ID management system, but "Ethereum Name Services" does not. Blockstack and DNSchain also provide other services to form a complete solution. The services they provide are presented in the following sections.

Name Resolution

The name resolution service is the basic DNS service. Blockchain-based name services provide the owner of a domain full control over the distribution of subdomains. The legacy DNS system only allows domain names to be rented for a period of time. Users will keep their domain names forever with blockchain technology. The users need to deploy a blockchain-based name resolution registry, implementing a registrar representing a contract that controls a node. DNSResolver should be set as the domain name resolver with the service functions. A user's NS records can be updated with the user's registrar.

Namecoin was the first blockchain-based DNS, which was forked from Bitcoin. Most of the following solutions were derivatives of Namecoin. Namecoin does not seem to be functional [11]. KeyId and NXT are more experimental naming services, which are more theoretical and not very reliable. Blockstack has its own Blockchain Name System. Ethereum Name Service is the most valid and functioning system at the moment.

The decentralized namespace should be carefully designed, and it would be a good idea to have a hybrid model, where there are also centralized services [11]. As these domains are mostly used for web browsing, browser add-ons should be deployed to reach this decentralized namespace.

Identity Management

Identity management enables P2P sharing of personal identities and related information. It provides greater control over personal data and reduces risks. Identity verification and a digital ID can be merged to provide the functionality of a digital watermark. Blockstack, for example, provides a decentralized public key distribution system, and a registry for apps and user identities. The Blockstack application programming interface (API) can handle identity and authentication. Applications can request permissions from the users and then gain read-and-write access to the user resources.

Identity management enables P2P sharing of personal identities and related information. It provides greater control over personal data and reduces risks. Identity verification and a digital ID can be merged to provide the functionality of a digital watermark. Blockstack, for example, provides a decentralized public key distribution system, and registry for apps and user identities.

	Name resolution	Identity management (PKI)	Distributed storage	Distributed applications
Ethereum Name Services	Yes	X	X	X
Namecoin	Yes	Yes	X	X
EmcDNS	Emercoin NVC	Yes. EMCSSH	Yes	Yes
Blockstack	Yes. BNS	Yes	Yes. Gaia	Yes
DNSChain	Yes. Uses Namecoin	Yes. Uses Namecoin	Yes. Customizable	Yes. Uses Blockstack

Table 2. Classification of the blockchain-based solutions.

Distributed Storage

A decentralized cloud storage (DSN) network allows sharing and storage of data without having to trust any third parties. This is significant for privacy, security, and data control. It also reduces the rate of data failures and outages. DSN is different from traditional cloud networks with its client-side encryption, which is more secure against threats. Proof of retrievability ensures the integrity and availability of the data. The main advantage of the DSN is flexibility. Speed and low cost advantages can be reached via proper implementation. The biggest concern about decentralized storage is the storage capacity. Keeping the whole ledger in every single node looks like an illogical solution, especially in Internet of Things (IoT) type lightweight devices. Maintaining the current state of the registered domains and keys is a better idea. There is still need for storage space that is linear with the number of registered domains. It will only require a constant time for checking the integrity of the blockchain whenever a new domain is registered [12].

The Gaia storage system is used by Blockstack. It stores data on behalf of a user after the user logs into the application. Gaia is used to reuse the existing cloud infrastructure, but writes the data in encrypted or signed form [13]. Storj works as a P2P cloud storage network.

Decentralized Applications

DApps are a concept wherein anyone can publish their apps. Unlike today's apps, it does not need a third party to gain access to the user's information. The app will remain in its original form as the ledger is immutable. This makes DApps unstoppable and resistant to censorship. DApps can be developed for money management, e-voting, governance systems, and more [14]. The main concerns about DApps are [15]:

- The security risks of running anonymous or incomplete code
- Scalability problems
- Resiliency of the application platform

Two DNS DApps examples are Blockstack and DNSChain. Blockstack is a decentralized web application, which is in a modular, layered structure that enables the modules to be configured with different software. The DNSChain system provides simple and secure key distribution; it ensures the security with the MITM-proof RESTful API.

Decentralized Internet

The Internet should be liberated and decentralized in theory. Violation of net neutrality, censorship, privacy problems, and disruption of the services with DOS attacks are some of the problems we face today. The standards are not evolving as fast as they should. DNS records can be censored at some of the DNS servers, which will cause the domains to be unreachable. DNS is managed as a single and globally unique root. Even though it is managed in a so-called democratic way, being a centralized solution can be a problem, especially during DDoS attacks.

Decentralized systems can be a robust alternative, and can especially replace the central systems that need trust. There are several solutions for the decentralized name resolution services. Blockchain systems can also be used as a PKI. Digital certificates and public keys can be stored in the ledger. Such a system will not need central CAs. The cloud can be used for storage back-ends by implementing the trust issues in a decentralized way. Blockstack and Emercoin can be given as candidate implementations of such systems. Cloud security is implemented by proper selection and careful implementation of the cryptographic protocols. The data is written encrypted on the cloud and then signed.

Blockstack proposes a decentralized DNS, PKI, and storage. The authors of Blockstack represent it as "the new Internet, where users don't need to trust remote servers" [13]. The implementation of Blockstack is flexible in such a way that any number of blockchains can be used as communication channels, and any public cloud can be used for storage. Blockstack also provides a full stack to build applications for the developers. The system is formed of three components [13]:

- Blockchain: Virtualchain is used to bind information to public keys and provide trust.
- Peer network: The Atlas network is used to provide a scalable index for global data.
- Storage system: Gaia is used.

The Emercoin system uses EmcDNS, a PKI service called EmerSSH, and storage. EmcDNS is a decentralized domain name service, which supports a full range of DNS records of any kind in name-value format. Emercoin preserves an agreement with the DNS provider OpenNIC. Users can reach the domains that are registered with EmcDNS through the OpenNIC DNS servers. The following can be mentioned as differences from Blockstack:

- Emergate.net: This is an experimental work, which will serve as a public gateway to all EmcDNS zones by using the URL addresses.
- Emercoin wallet: DNS records can easily be retrieved from any Emercoin wallet using the three types of user interface, or by the standard RFC1034 DNS protocol, which is built in on every Emercoin wallet.

Practical Experience

We tried existing tools and applications in our lab. The Blockstack browser is installed on local machines for creating (name.id) and managing the personal profile associated with it. These

identities are then registered on the blockchain. Typical implementations show that this system is used mostly for identity management. Name.id is associated with the user's public key, which is a cryptocurrency wallet address. The profile data is mostly kept in the cloud environments. Social media addresses are also linked to the profiles.

Personal profiles are expected to be used widely when the usage of DApps increases. Blockstack also sponsors an "Ecosystem-Wide, Universal" Dapp Store (https://app.co/) where several apps are listed. They also created a criteria list for DApps such as identity, data encryption, data storage, and software licences.

We installed a Blockstack core as a blockchain node. Blockstack keeps the records as four layers on top of the Bitcoin blockchain. Name queries were tested. Blockstack had 524,876 blocks, and the namespace consisted of 77,706 .id names at the time of our test. New TLD namespaces (.site, .media, .device ... etc.) are said to be coming soon.

```
root@bcrg_testbed:/home/enisk/blockstack#
blockstack consensus
{
   "block_height": 524876,
            "consensus":  "799b9236dc2b7b-
8311ba44f17738ef4b"
}
```

Results and Conclusion

We are facing the violation of net neutrality, censorship, and privacy problems, which threaten the freedom and usability of the Internet. Denial of service attacks cause the disruption of many online services. The standards are not evolving as fast as they should. Decentralized blockchain technologies can be developed as a solution.

Blockchain implementations that give name service and host-specific extensions like .bit and .eth. can also be peered by other services like OpenNIC. The hybrid solutions are not fully decentralized, but they are still important and serve their purpose. The importance of such a solution is that there will not be only a single entity managing the namespace, but also some other alternatives as well. These solutions also work as a distributed public key infrastructure. The existence of many nodes on the P2P network serving the namespace will serve availability during DDoS attacks.

Blockchain-based DNS and PKI implementations are not mature enough yet, but the services they can deliver are promising. There are challenges to be solved, such as scalability and energy consumption. New solutions, including the Lightning network and Plasma, have been proposed for the scalability issues. The blockchain should only be used for keeping records; the data should be kept in the cloud. Most blockchain implementations use PoW consensus protocols and too much electricity resources. However, there are other consensus protocols, such as PoS, which require less resources, and these protocols can be enhanced to reach acceptable security at lower cost. The decentralized Internet is not a dream. Decentralized infrastructure-related research should be more in focus, but there are new working groups like IETF's Decentralized Internet Infrastructure Research Group (DINRG) addressing this subject. This area should be studied in depth, and implementations should be enhanced continuously.

The decentralized Internet is not a dream. Decentralized Infrastructure-related research should be more on the focus, yet there are new working groups like IETF decentralized Internet infrastructure research group (DINRG) on this subject. This area should be studied in depth and implementations should be enhanced continuously.

References

[1] P. Roberts, "Phony SSL Certificates Issued for Google, Yahoo, Skype, Others," Mar. 2011; https://threatpost.com/phony-ssl-certificates-issued-google-yahoo-skype-others-032311/75061/, accessed June 30, 2018.

[2] D. Fisher, "Final Report on DigiNotar Hack Shows Total Compromise of CA Servers," Oct. 2012; https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/, accessed June 30, 2018.

[3] IETF RFC 1034, "Domain Names — Concepts and Facilities," P. Mockapetris, *The Internet Society*; https://tools.ietf.org/html/rfc1034, 1987.

[4] IETF RFC 2826, "IAB Technical Comment on the Unique DNS Root," Internet Architecture Board, Network Working Group; https://www.ietf.org/rfc/rfc2826.txt, 2000.

[5] IETF RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"; https://tools.ietf.org/html/rfc5280, 2008.

[6] IETF RFC 6844, "DNS Certification Authority Authorization (CAA) Resource Record,"; ISSN: 2070-1721, 2013; https://tools.ietf.org/html/rfc6844, 2013.

[7] Qualys SSL Labs, "SSL Pulse"; https://www.ssllabs.com/ssl-pulse/, accessed June 30, 2018.

[8] A. Kiayias *et al.*, "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol," *Annual Int'l. Cryptology Conf.*, Springer, 2017, pp. 357–88.

[9] G. Karame, "On the Security and Scalability of Bitcoin's Blockchain," *Proc. 2016 ACM SIGSAC Conf. Computer and Commun. Security*, 2016, pp. 1861–62.

[10] K. Wüst, and A. Gervais, "Do You Need a Blockchain?," IACR Cryptology ePrint Archive, 2017, p. 375.

[11] H.A. Kalodner *et al.*, "An Empirical Study of Namecoin and Lessons for Decentralized Namespace Design," *WEIS*, 2015.

[12] S. Wilkinson *et al.*, "Storj A Peer-to-Peer Cloud Storage Network," 2014.

[13] M. Ali *et al.*, "Blockstack: A New Decentralized Internet," White Paper, 2017.

[14] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," White Paper, 2014.

[15] A. Castano, "Why I'm Betting on Blockstack to Save the Decentralized Internet," Sept. 2017; https://medium.com/@alidcastano/why-im-betting-on-blockstack-to-save-the-decentralized-internet-56f65a11fec4, accessed June 30, 2018.

Biographies

Enis Karaarslan (enis.karaarslan@mu.edu.tr) is an assistant professor in the Department of Computer Engineering at Mugla Sitki Kocman University. He received his Ph.D. in computer engineering (2008) from Ege University. He was a post-doctoral researcher at EC JRC-IPSC, Italy (2011–2012). He is the head of the MSKU Blockchain Research Group. His research areas are computer networks, security, privacy, and blockchain. He has over 40 papers to his name.

Eylul Adiguzel (eyluladiguzel@posta.mu.edu.tr) is an MSKU Blockchain Research Group member who is eager to learn the fundamentals and technical barriers of this technology. She has worked on using blockchain effectively for e-voting systems for her finishing thesis. She received her B.S. in computer engineering in 2018.