Decentralization of DNS: Old Problems and New Challenges

Shi Yin
Cyberspace Advanced Technology Research Institute
Guangzhou, China
Cyberspace Security Research Center
Peng Cheng Laboratory
Shenzhen, China
yinshi@e.gzhu.edu.cn

Yu Teng
Zhong Zi Hua Ke Traffic Construction Technology Co. Ltd
Beijing, China
tengyujl@qq.com

Ning Hu†
Cyberspace Advanced Technology Research Institute
Guangzhou, China
Cyberspace Security Research Center
Peng Cheng Laboratory
Shenzhen, China
huning@gzhu.edu.cn

Xu Dong Jia
Cyberspace Advanced Technology
GuangZhou University
Guangzhou, China
Cyberspace Security Research Center
Peng Cheng Laboratory
Shenzhen, China
jiaxudong@e.gzhu.edu.cn

ABSTRACT

The Internet Domain Name System (DNS) provides domain name resolution services for Internet applications and is a vital infrastructure of the Internet. The security of DNS has always been a hot issue in network security research. Traditional research work mainly improves the security protection capabilities of the DNS system by designing security-enhanced protocols. However, frequent DNS security incidents in recent years have shown that simply improving the DNS protocol cannot completely eliminate the security threats faced by the DNS system. Decentralization of DNS is a novel idea to improve the security capability of DNS system. Unlike traditional solutions, DNS decentralization technology is dedicated to changing the architecture of the DNS system and the domain name resolution process. This article analyzes and summarizes representative research work in the past 20 years for DNS decentralization technology, and discusses the development trend of future research.

CCS CONCEPTS

• Network services • Naming and addressing

CIAT 2020, December 4–6, 2020, Guangzhou, China

ACM ISBN 978-1-4503-8782-8/20/10…$15.00
https://doi.org/10.1145/3444370.3444594

KEYWORDS

DNS security, DNS decentralization, P2P, blockchain

1 Introduction

The Domain Name System (DNS) provides domain name resolution services for Internet applications and is an important infrastructure to ensure Internet connectivity. In addition, the domain name system is also used to achieve system load balancing[1], network traffic engineering[2], disaster recovery backup[3], etc. application. With the rapid development of network technology, more and more government, military, and commercial applications are deployed in the Internet environment. As an important infrastructure to ensure the stable operation of the Internet, the reliability, availability, and security of the domain name system have attracted widespread attention from society.

Since the DNS system was proposed, in order to improve its reliability, availability, and security, a large number of research results have emerged. These researches were originally designed to improve the DNS system from the perspective of protocol design and system implementation. Since the beginning of DNS design, 289 RFC documents have been published to improve the design, implementation, and operation of the DNS protocol[4]. Although there are many outstanding works in protocol design and implementation technology[5], DNS still has hidden dangers of centralization in terms of domain name search efficiency and domain name counterfeiting. First of all, DNS mainly adopts recursive and iterative queries, both of which require access to the DNS root server to make it the core node of DNS. Once the DNS root server is attacked, the entire DNS will be greatly affected. In order to improve the query efficiency of domain name resolution, DNS has introduced a caching mechanism. However, the

emergence of cache poisoning attacks makes DNS face new security threats again. In order to resist this attack, DNSSEC[6]was proposed and deployed in about 1372 top-level domain nodes in 90% of the world[7]. Because it relies on a public-key cryptosystem (PKI), it requires a global unified root of trust, which undermines the autonomy of the Internet and presents a risk of unilateral control. In addition, the verification overhead, response time, and bandwidth resources occupied by a large number of digitally signed messages caused by encryption have brought challenges to actual deployment. The TikTok incident further shows that the Internet has national boundaries, and the impact of unilateral control will be more serious. The economic control caused by the disconnection cannot be ignored[8].

Frequent security incidents in recent years[9-13] indicate it is very difficult to completely eliminate the security issues of DNS only by improving the DNS protocol design and system implementation. With the explosive growth of the Internet and the continuous emergence of various new network attack technologies, it is necessary to redesign the DNS system from the perspective of architecture and management mechanisms[14]. The traditional DNS system has a significant centralization feature. This centralization feature has a negative impact on the DNS system's domain name resolution efficiency and domain name authenticity verification. It is also an important cause of hidden dangers in the DNS system. In response to the security threats caused by the centralization of DNS, scholars at home and abroad have put forward many novel ideas in terms of load balancing and data credibility[15-18]. At the same time, it also brings challenges in how to deploy and store on a large scale[19-20]. This article focuses on the technology of DNS decentralization and summarizes the representative research status and development trend of the past 20 years from the three aspects of P2P, blockchain, and alliance.

The organization of this article is as follows. Section 2 summarizes DNS security threats and examples of attacks against the vulnerability of DNS centralization characteristics, lists various DNS decentralized security enhancement solutions, and compares and analyzes them. Section 3 proposes hot spots and prospects for DNS security research work. The last section, we made a brief summary.

2 Analysis of DNS decentralization scheme

Although DNS is physically deployed in a distributed manner, the DNS root server's resolution and verification of domain names show significant centralization characteristics, which may cause some security problems. Table 1 summarizes the security threats and specific examples of attacks caused by the centralized characteristics of DNS.

Table 1: DNS Security Threats and Attack Instances

Attack method	Attack instance	Cause
Single point of failure	DDoS attacks on DNS root servers in February 2007 and November 2015[9].	The number of root servers is small, and DNS cannot work normally after being attacked.
Unilateral control	In 2003,the United States stopped the domain name resolution of Iraq[10]. In April 2004,the United States blocked".ly"and caused Libya to disappear on the Internet for three days[11].	The root server determines whether the domain name can be resolved or whether it exists.
Domain spoofing	In January 2014,the mainland top-level domain was redirected to the US IP address[12].	The domain name server in the tree structure cannot verify the domain name and can accept addresses forged by attackers.
DNS hijacking	In April 2019,Cisco said that the sea turtle attack had invaded 13 different countries,eavesdropping and hijacking the entire country top-level domain (ccTLD) information[13].	The domain name server in the tree structure cannot verify the domain name.

To try to solve the problems of security, efficiency, and management brought about by the centralization of DNS, some scholars proposed to design a decentralized DNS system[18][21-22]. After DNS is decentralized, each server node is equal, and the DNS resolution process is no longer limited to the root server, which can improve the unilateral control risk brought by the DNS root server in the management plane; enhance the DNS resolution process in the data plane Robustness of attacks such as cache poisoning and domain spoofing; reduce the impact of single point of failure and DoS attacks on the DNS server in the control plane, and achieve progressive deployment.

The current design for decentralized DNS mainly includes the following directions from the technical and theoretical aspects:

2.1 Decentralization based on P2P Network

P2P networks have typical decentralization and autonomy characteristics, all resources can be shared between nodes. Since all nodes are equal to each other, there is no single point of failure[23]. Therefore, the DNS data plane can be constructed based on the P2P network to realize the storage and retrieval of domain names. The P2P-based decentralization scheme is mainly as follows.

2.1.1 Data synchronization

The name service based on data synchronization is mainly to establish consistency between the target data in the root zone and the data stored in a specific server. The literature[24] proposed a

SINTRA architecture[25], which kept state synchronization between the authoritative name servers in the region and can resist Byzantine attacks; the literature[26] formed a peer-to-peer network with the DNS servers of thousands of ISPs around the world and pushed the NS records of DNS to thousands of name servers around the world. Both of the above implement a distributed DNS logical root node, avoid single points of failure, resist DoS attacks, and be compatible with DNSSEC. However, the read operation of the former for remote computing on data synchronization takes about hundreds of milliseconds, and the write operation takes more than 1 to 20 seconds. The latter does not solve the problem of data transmission efficiency in which the NS record of each domain exceeds 100 bytes.

2.1.2 Data positioning

The point-to-point name service based on data positioning mainly hashes the content identifier to determine which covering node needs to save the main copy of the content, and caches at the intermediate forwarding node to enhance fault tolerance and load balancing properties. Distributed hash table[27] uses a hash table to realize the storage of key values and data, and all nodes can effectively retrieve the key values. This type of research mainly includes: DDNS[15], Overlook[16], CoDoNS[17], P-DONAS[18], and hybrid solutions, etc.

DDNS used DHash (a peer-to-peer distributed hash table based on Chord)[28] for storage and retrieval of DNS records. It used Chord's fault tolerance and load balancing properties to replace the root server's centralized management mode of domain names. DNS records were backed up and stored to achieve peer-to-peer search. The time complexity of the DDNS query is O(logN). The search results of each block were cached along the search path. DHash will automatically transfer data with the increase of servers and select a fixed number (usually six) copies of the stored data in a pseudo-random manner, only if it fails at the same time, data loss occurs; the literature[29] combined the Chord P2P protocol[30] and the round-robin mechanism to weaken the impact of high-level domain name server denial of service on low-level domain name server. The two solutions provide alternative paths for domain name queries through the two parallel paths of the existing root/TLD DNS and P2P systems. How to motivate individual users to run peer-to-peer servers to provide domain name services and reduce query latency are also issues that need to be considered.

Overlook is an extensible name service built on Pastry. Requests for domain name lookup and update are routed to the nodes of the relevant directory through Pastry, and replication is used to update the data to reduce network congestion. In addition to the node-to-node message transfer structure, Beehive[31] can also be used to place copies of the requested data along the path they came from, reducing the cycle of searching. CoDoNS transfers the query to other normal resolvers to reduce the delay caused by local resolver failure. CoDoNS is compatible with traditional DNS and relies on globally distributed servers, which must be contributed to form a globally shared DNS cache.

HDNS[32] proposed a hybrid DNS system that combined DNS hierarchical tree and Chord flat structure. Each root node of the internal zone was assigned a unique identifier and was mapped to a public zone node equal to the identifier of the following root node. Query the domain name by searching for the corresponding identifier. HDNS lookup efficiency is higher than Chord-based DNS, but lower than traditional DNS. As the original DNS tree structure is maintained, it is still unable to resist risks such as unilateral control.

P-DONAS organized the access nodes (AN) of the ISP's access network into a fault-tolerant and scalable Kademlia-based DHT (called Kad). Each AN acted as a DNS server, storing part of all DNS data. DNS requests sent to AN were responded to through P2P lookups while maintaining compatibility with traditional DNS. Due to the good flexibility and scalability of the Kad network, P-DONAS can share the available memory and computing resources of AN without additional costs. As the number of nodes increases, it improves performance and avoids DNS single points of failure. Compared with Chord-based DNS, when the lookup performance reaches O(log2b N) and b = 6.98, Kad-based DNS is more efficient than Chord.

2.1.3 Summary

P2P-based decentralized solutions can achieve load balancing and are compatible with traditional DNS, but have the following limitations:

- Low performance: The query request is processed multiple times on the high-latency network, and the parsing efficiency is significantly reduced[33]. In addition to improving the response time of the system through replication, the cache replacement strategy also has a significant impact.
- Fault tolerance and free-riding: In P2P, there are data loss, forgery, and update. Only when the algorithm is robust enough can normal recovery or data synchronization. Free-riding is a different type of failure mode that requires bypassing or neutralizing uncooperative nodes. How to motivate users to join the peer-to-peer network also requires thinking.
- Incentive: The lack of user incentive mechanism makes it difficult to promote on a large scale.

2.2 Decentralization based on blockchain

Blockchain technology is a new application mode of distributed data storage, point-to-point transmission, consensus mechanism, encryption algorithm and other technologies. Utilizing the characteristics of blockchain decentralization, non-tampering, traceability, time series data, collective maintenance, and security and high credibility[34],it can minimize the user's dependence on third parties, such as DNS root servers or root certificates issuing agency; At the same time, associating domain names with currencies can solve the incentive problem in P2P networks. Therefore, building a programmable currency system is a new research idea of DNS decentralization.

The current DNS decentralized solutions based on blockchain technology are mainly as follows:

2.2.1 Solutions based on public blockchain

The main innovation of the DNS decentralized system based on the public chain is to adopt the idea of universal control, use

domain names and assets as tradable resources, and use the public chain as a currency publishing platform. The more representative schemes include: Namecoin[35] based on Bitcoin branch, Blockstack[21] based on Namecoin improvement, ENS[36] based on Ethereum, etc.

Namecoin replaced the DNS root server with a blockchain that maps domain names to DNS records. Namecoin used digital signatures to record all transactions between users to prevent tampering of logs, and used a virtual ".bit" top-level domain name, but it has not been officially registered in the existing DNS system, and is incompatible with the existing DNS system.51% Example attacks[37],domain name cybersquatting[38] and other issues. Although Namecoin has security, performance and scalability challenges, the blockchain provides an important basic framework for building secure and decentralized services. The cost of tampering with the blockchain increases with user adoption, and nowadays, it would take hundreds of millions of dollars to attack a large blockchain like Bitcoin.

Blockstack proposed a Bitcoin-based on-chain retrieval/off-chain storage DNS implementation scheme to improve the security and scalability of Namecoin. The control plane included a blockchain layer and a virtual chain layer. The former stored the order of operations and reached a consensus on the write order, and the latter defined new operations above it and encoded them as additional metadata in valid transactions, constructing a state machine to store the global state and update the state of the blockchain block; the data plane included the routing layer and the data storage layer, which separated data discovery and storage. The nodes formed a DHT-based peer-to-peer network storage area file, and support variable and immutable storage at the same time, the user can use the key to verify the integrity of the data.

There are also some derivative systems based on Bitcoin that also support name resolution services. Such as ENS[36] based on Ethereum, EMCDNS[39] based on Peername[40],etc.

ENS is an extensible naming system based on the Ethereum blockchain. Domain names (such as "gzhu.eth") are mapped to machine-readable identifiers to represent Ethereum addresses. Top-level domain names (such as ".eth") are registered by the smart contract of the service provider owns, and the distribution of any sub-domain under this domain is completely controlled by the domain owner. Ethereum will maintain a node list (Node Table) similar to Bitcoin and use the Kademlia algorithm to quickly locate the target node with a time complexity of O(log(n)).

EMCDNS used the SHA-256 encryption algorithm, which was originally a hybrid product of Namecoin and Peercoin, using the second-generation equity proof algorithm[41], which can run without mining, making it resistant to 51% attacks.

The literature[42-44] all generated a unique hash of the original data and stored it in the blockchain to prevent cache poisoning. In literature[22], the root server used a consensus algorithm to maintain a consistent root zone file and introduced a trust value and penalty mechanism to eliminate the risks of cache poisoning and trust in the current centralized DNS architecture, and the throughput exceeded 30 transactions per second, which could ensure that domain name operations are completed within 50 seconds.

The blockchains of Ethereum, Bitcoin and Emercoin all have similar structures, but the difference lies in the way data is injected into the blockchain. For example, when designing Bitcoin and other top encrypted digital currencies, the main function considered is "remittance", while Ethereum integrates each smart protocol that uses its additional functions and services into its blockchain itself.

2.2.2 Solutions based on alliance blockchchain

Both Namecoin and Blockstack try to combine domain name services with public chains, hoping to achieve complete decentralization. However, Bitcoin generates 1MB blocks in an average of 10 minutes and the existing management and security problems, which leads to its security and performance defects[37]. The consortium chain adopts partial decentralization, allowing several organizations to participate in the management of the blockchain. Literature[19] proposed a domain name service based on the alliance chain to eliminate a single central node. To deal with the storage challenge of the blockchain, a three-tier architecture was used to separate the data and operation of domain name transactions. The domain name operation was recorded on the blockchain. Data was stored in external storage. It built indexes for transactions to speed up domain name resolution and combined the gossip protocol to synchronize blocks between different nodes, but its throughput was less than 10 transactions per second, and a more effective consensus mechanism was required. Literature[20] is a consortium blockchain that includes a root chain and a TLD chain. It used signatures to ensure the validity and non-tampering of node information and used a hierarchical multi-chain architecture to achieve decentralization of domain name management and resolution.

2.2.3 Summary

Based on blockchain DNS has the characteristics of decentralization and anti-censorship[38], it also has the following limitations:

- Performance and scalability: Blockchain nodes are in the same state and are not controlled by a central party, but a single record is about kilobytes[45],which cannot tolerate large amounts of data, the delay of changing records is affected by factors such as blockchain data dissemination, about 10 to 40 minutes[46].
- The efficiency of the consensus algorithm: The inefficient consensus algorithm is not suitable for real-time update and maintenance of DNS data. It is necessary to design an algorithm with high consensus efficiency and strong consistency.
- Incompatible with existing DNS: The client must install a plug-in to access the domain name system, which is difficult to deploy on a large scale.
- Security:51% attacks actually have 25% of the computing power will threaten system security[47].
- Data storage: It is difficult for users to store all the data of the blockchain. Although SNV[48] provides a server that can

record all, it needs to solve the security problem of data communication.

2.3 Decentralization based on National Alliance

The main research idea of the scheme based on the root server alliance is that different countries or different top servers can reduce the impact of unilateral control through alliances and enjoy the same control rights. The challenges faced by this approach include the design of the national root alliance architecture, the control of the root alliance system, and the synchronization of the root alliance with the main root server.

The literature[49 - 50] believes that the alliance of different countries or top-level servers can weaken the centralized dependence on the root server. The former used blockchain to achieve a distributed consensus on root zone data to ensure the consistency of root zone data, while the latter maintained a single-root tree logical structure and built a multi-root tree analysis structure, which is compatible and expandable. But the challenges faced include the design, control, and synchronization with the main root server of the national root alliance architecture.

3 Comprehensive analysis

Table 2 compares the decentralized schemes of DNS. It can be found that the early schemes tend to maintain the root server more robustly to resist risks such as single points of failure, or use a scheme similar to the literature[51] to make nodes become peers. It also directly accesses shared resources, flattening the DNS structure.

The emergence of blockchain technology provides a new direction for the study of DNS decentralization. For example, the literature[52] used blockchain technology in P2P networks to eliminate risks such as centralized control. At present, most DNS decentralized security protection solutions are based on the improvement of Bitcoin's blockchain, ethereum or alliance chain, how to efficiently design consensus algorithms to achieve safe and rapid domain name resolution, verification and update, how to make blockchain technology compatible with existing DNS and be gradually deployed. These are issues that need to be considered in the future.

Table 2: Analysis and comparison of DNS security enhancement solutions

Enhanced-technology	Schemes	Compared					
		Anti-unilateral-control	Anti-single point of failure	Compatible with traditional DNS	Anti-DoS attack	Anti-cache poisoning	Low latency
P2P	Literature [24]	×	√	√	√	√	×
	Literature [26]	×	√	√	√	√	×
	DDNS	√	×	×	√	√	×
	Literature [29]	√	×	×	√	×	×
	Overlook	×	√	√	×	×	√
	CoDoNS	×	√	√	√	√	part
	HDNS	×	×	√	√	√	part
	P-DONAS	√	√	√	√	√	part
Block-chain	Namecoin	√	√	×	√	√	×
	Blockstack	√	√	×	√	√	×
	ENS	√	√	×	√	√	×
	Peername	√	√	×	√	√	×
	EMCDNS	√	√	×	√	√	×
	Literature [42-44]	√	√	×	×	√	√
	TD-Root[22]	√	√	×	√	√	√
	Literature [19]	√	×	×	√	√	×
	Literature [20]	√	√	×	√	√	×
National-League	Literature [49-50]	√	√	×	√	√	×

4 Conclusion

This article analyzes representative research work in the past 20 years.P2P technology achieves decentralization by flattening the tree structure of DNS. While achieving load balancing, it also brings high-latency performance problems and lacks sufficient incentive mechanisms. Blockchain technology can realize decentralized storage and credible resolution of domain names and enhance incentives by binding digital currencies, but it is not compatible with traditional DNS. The idea of the DNS alliance is still in its infancy due to political and economic factors. It can be seen that there are still many challenging issues in the decentralization of DNS, which require further research and exploration.

ACKNOWLEDGMENTS

Thank the equipment support of Guangzhou University and the support of National Natural Science Fund of China.

REFERENCES

[1] [Online]. Available: https://patents.google.com/patent/US8756340B2/en
[2] P. Kanuparthy, W. Matthews, and C. Dovrolis. DNS-based ingress load balancing: An experimental evaluation. CoRR, abs/1205.0820, 2012.
[3] Pete Tenerillo, “Why DNS Based Global Server Load Balancing(GSLB) Doesn't Work”, Nov. 3, 2004, XP002586093, URL: http:// www.tenereillo.com/GSLBPageOfShame.htm.
[4] RFC Research. [Online]. Available: https://www.rfc-editor.org/search/rfc_search_detail.php?title=DNS&pubstatus%5B%5D=Any&pub_date_type=any
[5] Cricket Liu, Paul Albitz. DNS and BIND - help for system administrators: covers BIND 9.3 (5. ed.). O'Reilly 2006, ISBN 978-0-596-10057-5, pp. I-XIX, 1-616.
[6] O. Kolkman and R. Gieben. DNSSEC Operational Practices. RFC 4641, Sept 2006.
[7] DNSSEC Deployment Report. [Online]. http://rick.eng.br/dnssecstat/
[8] [Online]. https://www.sohu.com/a/419756712_313745
[9] Yuan P P, Wang C Q. Research on DNS security threats and countermeasures[J].Cyberspace Security, 2018, 9(5): 1-.
[10] Kim G, von Arx & Gregory R. Hagen, Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control, 9 Rich. J.L. & Tech. 4 (2002)
[11] IANA Report on the Redelegation of the .ly Top Level Domain. [Online]. Available:http://www.iana.org/reports/2005/ly-report-05aug2005.pdf
[12] [Online]. Available:https://zh.wikipedia.org/wiki/2014%E5%B9%B4%E4%B8%AD%E5%9B%BD%E5%A4%A7%E9%99%86%E7%BD%91%E7%BB%9C%E5%BC%82%E5%B8%B8%E4%BA%8B%E4%BB%B6
[13] Avi Kak, “Lecture 17: DNS and the DNS Cache Poisoning Attack,” Purdue University, March 2013.
[14] Wang W T, Hu N, Liu B, Liu X, Li S D. A review of DNS security protection technology research. Journal of Software, 2020, 31(7): 2205-2220.
[15] R. Cox, A. Muthitacharoen, and R. T. Morris. Serving dns using a peer-to-peer lookup service. In Proc. 1st Intl. Workshop on Peerto-Peer Systems (IPTPS 2002), pages 155-165,2002.
[16] M. Theimer and M. B. Jones. Overlook: Scalable Name Service on an Overlay Network. In Proceedings of the 22nd International Conference on Distributed Computing Systems (ICDCS). IEEE Computer Society, July 2002.
[17] Venugopalan Ramasubramanian, Emin Gun Sirer,“The design and implementation of a next generation name service for the internet”, SIGCOMM’04, Aug. 30–Sept. 3, 2004, Portland, Oregon, USA.
[18] Peter Danielis, Vlado Altmann, Jan Skodzik, Tim Wegner, Achim Koerner, and Dirk Timmermann. 2015. P-DONAS: A P2P-Based Domain Name System in Access Networks. Acm Transactions on Internet Technology, 2015,15 (3) :11
[19] X. Wang, K. Li, H. Li, Y. Li, and Z. Liang. 2017. ConsortiumDNS: A Distributed Domain Name Service Based on Consortium Chain. In 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS). 617–620.
[20] X. Duan, Z. Yan, G. Geng, and B. Yan. Dnsledger: Decentralized and distributed name resolution for ubiquitous iot. In 2018 IEEE International Conference on Consumer Electronics, ICCE 2018, volume 2018-January, pages 1–3, 2018.
[21] ALI M, NELSON J, SHEA R, et al. Blockstack:a global naming and storage system secured by block chains. 2016 USENIX Annual Technical Conference (USENIX ATC 16). 2016:181-194.
[22] G. He, W. Su, S. Gao, J. Yue TD-Root: a trustworthy decentralized DNS root management architecture based on permissioned blockchain Future Gener Comput Syst, 102 (2020), pp. 912-924
[23] A. Oram, editor. Peer-to-Peer: Harnessing the Power of Disruptive Technologies. O’Reilly & Associates, March 2001.
[24] C. Cachin and A. Samar. Secure distributed DNS. In Dependable Systems and Networks (DSN), July 2004.
[25] C. Cachin and J. A. Poritz, “Secure intrusion-tolerant replication on the Internet,” in Proc. Intl. Conference on Dependable Systems and Networks (DSN-2002), pp. 167–176, June 2002.
[26] M. Handley and A. Greenhalgh, “The Case for Pushing DNS,” in Proc. of Hotnets-IV, 2005.
[27] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker. A Scalable Content-Addressable Network. In Proceedings of SIGCOMM,2001.
[28] Frank Dabek, M. Frans Kaashoek, David Karger, Robert Morris, and Ion Stoica. Wide-area cooperative storage with CFS. In Proceedings of the 18th ACM Symposium on Operating Systems Principles (SOSP ’01), Chateau Lake Louise, Banff, Canada, October 2001.
[29] 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.
[30] I. Stoica, R. Morris, D. Liben-Nowell, D.R. Karger, M.F. Kaashoek, F. Dabek, H. Balakrishnan, “Chord: a scalable peer-to-peer lookup protocol for Internet applications,” IEEE/ACM Transactions on Networking, vol. 11, no. 1, pp. 17-32, Feb 2003.
[31] Venugopalan Ramasubramanian and Emin Gün Sirer. “Beehive: O(1) Lookup Performance for Power-Law Query Distributions in Peer-to-Peer Overlays”. In: 1st Symposium on Networked Systems Design and Implementation (NSDI 2004). San Francisco, USA, Mar. 2004, pp. 99–112.
[32] Y. Song and K. Koyanagi. Study on a hybrid P2P based DNS. IEEE International Conference on Computer Science and Automation Engineering, Shanghai, 2011, pp.152-155.
[33] Liu Y. Common Problems Analysis and Solutions on P2P Network Technology[J]. Computer Cd Software & Applications, 2012.
[34] Yuan Y,Wang F Y. Blockchain:The state of the art and future trends[J].Acta Automatica Sinica,2016,42(4):481-494(in Chinese).
[35] Namecoin. [Online]. Available:https://namecoin.info.
[36] Ethereum Name Service, "Introduction: Ethereum Name Service," ens.domains.[Online]. Available: https://docs.ens.domains.
[37] J. A. Kroll, I. C. Davey, and E. W. Felten. The economics of bitcoin mining, or bitcoin in the presence of adversaries. In WEIS 2013.
[38] C. Patsakis et al. “Unravelling ariadne’s thread: Exploring the threats of decentralised dns,” IEEE Access, p. to appear, 2020.
[39] EMCDNS. [Online]. Available: https://emercoin.com/.
[40] PeerName. [Online].Available:https://peername.com/.
[41] A. Jain, ‘‘Proof of stake with casper the friendly finality gadget protocol for fair validation consensus in ethereum,’’ Int. J. Sci. Res. Comput. Sci., Eng. Inf. Technol., to be published.
[42] T. Jin, X. Zhang, Y. Liu, and K. Lei, “BlockDND: A bitcoin blockchain decentralized system over named data networking,” in 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, Italy, Jul. 2017, pp. 75–80.
[43] J. Liu, B. Li, L. Chen, M. Hou, F. Xiang, and P. Wang, “A data storage method based on blockchain for decentralization DNS,” in In proceeding of the Third IEEE International Conference on Data Science in Cyberspacem, DSC, 2018, pp. 189–196.
[44] W. Yoon, I. Choi, and D. Kim. BlockONS: Blockchain based Object Name Service. In ICBC 2019 - IEEE International Conference on Blockchain and Cryptocurrency, pages 219–226, 2019.
[45] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Tech report, 2009. https://bitcoin.org/bitcoin.pdf.
[46] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In

2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 17-21, 2015, pages 104–121, 2015.
[47] Ittay Eyal and Emin Gun Sirer. Majority is not enough: Bitcoin mining is vulnerable. In Financial Cryptography, 2014.
[48] Simplified name verification protocol. http://blockstack.org/docs/light-clients
[49] ZHANG Y, XIA C D, FANG B X, et al. An autonomous open root resolution architecture for domain name system in the internet[J]. Journal of Cyber Security, 2017,2 (4)(in Chinese).
[50] Fang Binxing. Discussion on Autonomous Root Domain Name System Based on National Union from "Network Sovereignty". Information Security and Communications Privacy, 2014(12):35-38 (in Chinese with English abstract).
[51] Musiani, F. A Decentralized Domain Name System? User-Controlled Infrastructure as Alternative Internet Governance. Presented at the 8th Media In Transition (MiT8) conference, May 3-5, 2013, Massachusetts Institute of Technology, Cambridge, MA. 2013 Available as draft at http://web.mit.edu/comm-forum/mit8/papers/Musiani_DecentralizedDNS_MiT8Paper.pdf
[52] E. Karaarslan and E. Adiguzel, “Blockchain based dns and pki solutions,” IEEE Communications Standards Magazine, vol. 2, no. 3, pp. 52–57, 2018.