JCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Decentralization of DNS using Blockchain: A Survey

Aabid Hussain Ganai[1*] , Mir Aman Sheheryar[2]

[1,2]Dept. of Information Technology, School Of Engineering, Central University Of Kashmir, Srinagar, India

Corresponding Author: aabid.09t@gmail.com, Tel.: +91 9622702526

DOI: https://doi.org/10.26438/ijcse/v7i6.11621168 | Available online at: www.ijcseonline.org

Accepted: 22/Jun/2019, Published: 30/Jun/2019

***Abstract*—** the present DNS is a distributed network which helps in finding the IP addresses. The ICANN or the Internet Corporation for Assigned Names and Numbers lays the regulation for the functioning of DNS. It gives approval for the TLD or the Top Level Domain names like .com. It is the authority that accredit the registrars like the GoDaddy to sell the rights of using the domain name. The current DNS system is hierarchical. This system's root servers represents a high-value attack vector. Since the entire system is centralized even the slightest failure at a single point can take down the whole internet. With a DNS of the Blockchain, it will be based on the decentralized system, and thus, it may not hamper the redirection process. Furthermore, Blockchain based DNS may counter the censure and also avoid the problem of cache poisoning or DNS spoofing. It is true that Blockchain-based DNS inherits the benefits of decentralization. Unlike the current DNS system which is governed and is controlled by organizations, Blockchain-based DNS does not have any authorities. Every node in the server is equal. Only the owners can make changes in the current records. It is difficult for the authorities to make any changes in the domain name records. The current DNS system is prone to attach and hacking, but this is not the case with Blockchain based DNS. Blockchain based DNS will host or store DNS records on blockchain in the form of blocks which means that every block will store domain name and its corresponding IP address (name, value pair).

***Keywords*—**DNS,DNSSEC,blockchain,Bitcoin,Namecoin,Blockstack.

I. INTRODUCTION

Domain name system (DNS) is responsible for the resolution of the global domain name [1], and the root server is commissioned by the Internet Corporation for Assigned Names and Numbers (ICANN) to operate 13 specialized agencies in only a few countries [2]. Domain name services is a distributed database where IP addresses are mapped to domain names, giving people easier access to the Internet. It has been a core service of the Internet, since the first domain name was registered in 1985 .The current DNS system is a centralized where the generation and distribution of domain name is entirely depended on ICANN [3]. The process of domain name transaction is cumbersome and inefficient. In addition, the current DNS system often faces security threats, such as DDos. Most recently, in October, 2016, DDoS attacked the servers of Dyn [4], a company that controls much of the Internet's DNS infrastructure, bringing down websites including Twitter, Netflix, Reddit, CNN and many other in the US and Europe. This attack is roughly twice as powerful as any similar attack on record, which makes it the largest of its kind in history. Other than DDoS which attacks DNS servers, there are several security vulnerabilities oriented from the flaws in the DNS protocol such as DNS cache poisoning and man in the middle attack which also threaten the security of DNS.

The domain name system security extensions (DNSSEC) drafted by IETF tried to replace the DNS for enhancing the security [5]. DNSSEC aims to address these issues by adding security to DNS protocol while maintaining backward compatibility. DNSSEC was designed to provide DNS client's origin authenticated information and to prevent DNS data from being forged or manipulated, which makes it an effective weapon against attacks such as DNS cache poisoning. Basically, in a DNSSEC deployed zone, the DNS answers clients received are digitally signed. By checking the digital signature, clients are able to know whether the data contained in the answers is altered. Although DNSSEC guarantees the authentication and integrity of DNS data, it does not provide confidentiality of data, which means all DNSSEC data are not encrypted and visible to everyone. Another negative effect of DNSSEC is that the signing and verification of DNS data introduce additional overhead to the servers and network, thereby impacting the performance of DNS servers and making them more vulnerable to DDoS attacks. The complexity and difficulties of DNSSEC deployment also hinder the adoption.

Blockchain technology was first introduced by Satoshi Nakamoto in 2008 as the foundation of Bitcoin [6]. A blockchain is a distributed database that is used to maintain a continuously growing list of records, called blocks. Each block contains a timestamp and a link to a previous block. A blockchain is typically managed by a peer-to peer network collectively adhering to a protocol for validating new blocks. By design, blockchains are inherently resistant to modification of the data. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network. Blockchains can be divided into fully public blockchain, fully private blockchain and consortium blockchain with different read and write permissions. Blockchain was also adopted by some applications in smart contract, notarization security, digital assets, file storage and other fields, such as Ethereum and HyperLedger [7][8].

Namecoin first made an attempt to combine domain name service and blockchain, and builds a new blockchain with POW protocol, but faces serious security problems [9]. Blockstack absorbs a lot of lessons from Namecoin and migrates domain name service to the Bitcoin blockchain in order to improve security of the system [10].

In this paper, several blockchain- based DNS alternative systems are reviewed and compared. Meanwhile, their merits and potential limitations are also discussed and analyzed.

II. Related Work

In order to have clear cut, unbiased, complete and broader prospective many sources have been explored. The Literature Review has been carried out according to the guidelines proposed by Kitchenham [14]. The extensive Literature review has been carried out in the following databases:

1. ACM digital Library
2. IEEE xplore
3. Science Direct
4. Wiley online Library
5. Springer

The reason behind exploring these databases is their rich library of journals with high impact factors. The review also takes into account conference proceedings.

The search term was ‘Decentralization of DNS using blockchain’. The search was filtered to include the papers and conferences of previous 10 years. This was done to limit the scope of research to the present trends instead of exploring unverified and undeveloped techniques.

In the domestic research field, relevant research scholars have done the following work:

(Zhu Guoku et al.) [19] In year 2017 proposed a system which Aim at the problem of DNS single point failure and resolution data storage, they design a decentralization resolution data storage model, and implement the blockchain-based decentralization domain name resolution data storage system, and build multiple parallel decentralization DNS nodes. Based on this model, a distributed algorithm was designed to achieve the decentralization and consistency of the domain name server.

(Yuan Yong et al.) [20] In year 2016 made a detailed introduction to the ecology of Bitcoin by studying the composition of the blockchain, and studied the principles of blockchain, smart contract, and existing security issues. The centralized management of domain name servers brings cyber security threats to the country.

(Zhao He et al.) [21] In year 2015 presented a research article in which they used blockchain to protect the sampling data. Their research results show that the blockchain can effectively improve the data security protection. This method realizes decentralization domain name management, eliminates the restriction on the number of root servers, enables different organizations to enjoy the same domain name management rights, and solves the data synchronization problem.

(Wang Jiye et al) [22] In year 2017 proposed a blockchain-based data security sharing network system research to resolve problems such as restricted access to centralized deployment, no unique identification, being easily stolen, or falsifying hidden dangers.

In foreign research fields, relevant research scholars have done the following work:

(Swan M) [23] In year 2015 presented a research paper in which he studies the application of blockchain. Research shows that blockchain is beneficial to applications in artificial intelligence and human enhancement.

(Kraft D) [24] In year 2016 proposed a Poisson process model based on time intensity changes. This model is used when the hash value is different, the prediction block discovery time is deduced, and the research applied to Bitcoin is analyzed, and the stability of the update block difficulty guarantee time is analyzed.

(Zyskind G et al) [25] In year 2015 studied the trust mechanism based on Bitcoin and applied it to the field of trusted computing.

(Kypriotaki K et al) [26] In year 2015 studied the digital currency with Bitcoin's similar functional class, using blockchain technology to ensure the correctness of transactions and operations.

(Kosba et al) [27] In year 2016 proposed a decentralization smart contract system to indirectly store blockchain transaction data to effectively protect user privacy.

(Haferkorn M et al) [28] In year 2014 proposed Namecoin which is a DNS system that uses a blockchain and uses a “bit” top-level domain name. A user can apply for a second-level domain name under the domain name without authorization and without third-party control.

(Satoshi Nakamoto) [6] In year 2008 proposed a system for electronic transactions without relying on trust. He started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, he proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.
(Muneeb ali et al) [29] In year 2017 presented Blockstack as a new decentralized internet secured by blockchains. Blockstack provides a full stack to developers for building decentralized applications including services for identity, discovery, and storage. Blockstack can introduce new functionality without modifying the underlying blockchains and can survive the failure of underlying blockchains. The design of Blockstack is informed by 3 years of production experience from one of the largest blockchain-based production systems to date. Their performance results show that Blockstack can give comparable performance to cloud services on the traditional internet and only introduces a small CPU overhead.

(DR. GAVIN WOOD) [7] In year 2014 presented “Ethereum Project Yellow Paper” in which he explained blockchain paradigm when coupled with cryptographically-secured transactions has demonstrated its utility through a number of projects, with Bitcoin being one of the most notable ones. Each such project can be seen as a simple application on a decentralised, but singleton, compute resource. We can call this paradigm a transactional singleton machine with shared-state. Ethereum implements this paradigm in a generalized manner. Furthermore it provides a plurality of such resources, each with a distinct state and operating code but able to interact through a message-passing framework with others.

(X. Wang et al) [3] in year 2017 proposed ConsortiumDNS, a new distributed domain name service based on consortium chain. They have designed a three-layer architecture and add external storage layer to address the storage challenge of blockchain. The system builds indexes for transactions and blocks to speed up domain name resolution. In addition, a similar Gossip protocol was used to synchronize blocks between different nodes. They have also mentioned in their paper that Blockchain has many advantages in decentralization and security. Combining domain name service and blockchain is an excellent solution. It can make DNS decentralized and more secure. They also proposed their future work to address the problem of low throughput in their system by adopting a more efficient consensus mechanism. Maybe the Byzantine protocol is a choice. Therefore, there is a lot of work to do to make ConsortiumDNS feasible. Their three-layer architecture is shown below.

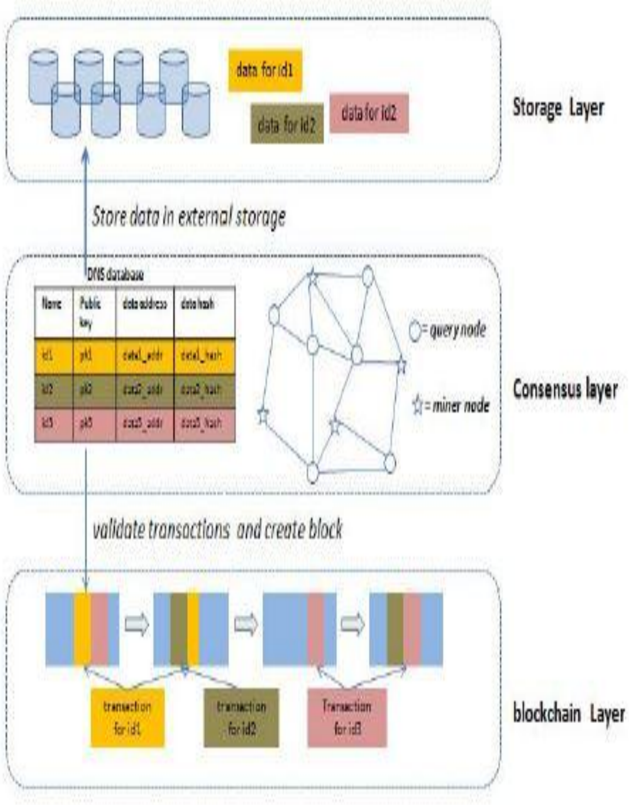

Figure 1: Architecture of ConsortiumDNS [5]

(Li.liu et al) [36] In year 2018 presented a paper in which they are trying to explain the features and effects of Blockchain technology on our business. They said that blockchain can change the way of conducting business. Blockchain technology is a new way of trading based on key technologies such as password security, decentralized coherence, shared public accounts and visibility of its proper controls and permissions. They said that Blockchain can completely change the way our society produces and lives by registering and exchanging assets which are physical and virtual, tangible and intangible. Blockchain technology is not just an application technology for new-generation transactions. It creates trust, responsibility and transparency while simplifying business processes. It will completely change the way Internet transactions and bring about changes to Internet information security technology. The realization and application of any technology will inevitably face some security risks in the development process. However, the unique information storage and sharing method of blockchain technology is expected to bring a revolutionary solution to the unmanaged information security industry.

(B.Benshoof et al) [37] In year 2016 presented a paper in which they explain how D3NS can overcome the problems faced by current DNS. They also explain in their paper that how D3NS can eliminates the need for certificate authorities .They present D3NS, a system to replace the current top level DNS system and certificate authorities, offering increased scalability, security and robustness. D3NS is based on a distributed hash table (DHT) and utilizes a domain name ownership system based on the Bitcoin blockchain. It addresses previous criticism that a DHT would not suffice as a DNS replacement. D3NS provides solutions to current DNS vulnerabilities such as DDOS attacks, DNS spoofing and censorship by local governments. D3NS eliminates the need for certificate authorities by providing a decentralized authenticated record of domain name ownership. Unlike previous DNS replacement proposals, D3NS is reverse compatible with DNS and allows for incremental implementation within the current system.

(J.Liu et al) [39] In year 2018 published a paper in which they try to explain how a DecDns is compatible with current DNS. They experimentally verified that how a blockchain technology can replace the current DNS. Their main motivation for this model was the challenges and problems faced by current DNS. They said that the technology of blockchain is still in the developing stage. The boundedness of query efficiency and capacity limit the popularization and application of blockchain. The emergence of blockchain provides the foundation for the development of decentralization application. Choosing the appropriate blockchain model is the key to solve the problem. The domain name system is the core service of the Internet. With the continuous development of the Internet, the security problem of the domain name system has become more and more prominent. Aiming at the problem of DNS single point failure and resolution data storage. They designed design a decentralization resolution data storage model, and implement the blockchain-based decentralization domain name resolution data storage system, and build multiple parallel decentralization DNS nodes. In the case of one or more resolution nodes failing, as long as a parallel resolution node works well, DecDNS deployed in a real network environment can implement normal domain name resolution function. Their experimental results show that DecDNS can be compatible with the original system, achieve parallel domain name resolution, solve the problem of domain name autonomy and single point of failure, and meet good performance requirements. So it provides a practicable method for the decentralization of domain name resolution.

III. BLOCKCHAIN BASED DNS ALTERNATIVES

1. Namecoin

Namecoin[9] is the first blockchain-based DNS system. It is a fork of Bitcoin with modifications which allow the blockchain to store name-value data other than transactions. Thus, Namecoin and Bitcoin share the most functionalities and mechanisms. Namecoin was designed as a more general name-value resolving system rather than a substitution of the current DNS system. Namecoin uses the virtual .bit top-level domain name which is not officially registered in current DNS system. This means Namecoin is isolated from the DNS system and users cannot resolve .bit domain names without installing additional resolving software. Namecoin provides complete functionalities for registering, renewing and transferring a domain as traditional DNS does.

2. Blockstack

Blockstack[10] is the first naming system which operates directly on top of the Bitcoin blockchain. Formerly it was Onename and built on top of Namecoin. After a security crisis of Namecoin, the development team decided to migrate the whole system to the Bitcoin blockchain. Therefore, the ability to migrate across different blockchains became one of their design philosophies and the name is also changed to Blockstack which reflects the concept of layered blockchains. Both Namecoin and Blockstack share the similar DNS functionality with one major difference stemming from Blockstack’s distinctive multi-layer blockchains. Namecoin stores name-value pair data on the blockchain. Thus, the maximum length of a domain name is 64 characters. Otherwise the blockchain will grow too fast. On the contrary, Blockstack is built on top of the Bitcoin blockchain which cannot accommodate large data such as name-value pair information. Therefore, a separate logical layer, i.e. virtualchain, on top of the blockchain is proposed to maintain the naming system while the underlying blockchain is only used for achieving consensus on the state of the naming system and the integrity of name-value data records.

3. Nebulis and more

Another project similar to Blockstack is a platform called Nebulis [30], a global distributed directory which intended to upgrade and replace the existing DNS using blockchain. The difference between the two is that their platform uses IPFS [31] or MaidSafe[32] as a replacement for HTTP and utilizes the Ethereum[28] blockchain for DNS capabilities.
There are other blockchain-based naming systems such as Emercoin[33] and EtherID[34] which may focus on other aspects of a DNS system such as name squatting, pricing policies. These are more of social or economic issues than technical problems. Fundamentally they share the similar underlying technology with Namecoin or Blockstack.

IV. Comparative Analysis

The favorable points of interest and drawbacks of all the above talked strategies are depicted in table 2.

Table 1: Comparative Analysis

S.NO	Approach	Advantages	Disadvantages
01.	Consortium DNS [3]	•distributed domain name service •address the storage challenge of blockchain	•low throughput
02.	Namecoin [9]	•Can be used as a DNS •Created Decentralized DNS	•Low throughput (more lookup time). •Less scalability of blockchain •No DNS caching.
03.	Blockstack [10]	•operates directly on top of the Bitcoin blockchain	•The maximum length of a domain name is 64 characters.
04	D3NS[37]	•Successfully implemented the approach as a DNS server. •Robustness	•Security issues relevant to DNS authentication. •Doesn't implement DNS caching (More lookup time)
05.	DecDns[39]	•compatible with current DNS •achieve parallel domain name resolution	•query efficiency •capacity limit

V. Research questions

The systematic review intends to classify the work related to Blockchain in a field of DNS by proposing the set of questions .The aim of the work is to identify the gaps in existing methodologies and propose an answer to fill the gaps. The questions we wish to answer are as follows:

RQ1: What is the present state of the art?
RQ2: What are the advantages, if any of using Blockchain over traditional methods for DNS?

VI. Answers to Research Questions

RQ1: During the review, it was found the Blockchain has not been explored in detail. In general SPRINGER had the highest number of pertaining to Blockchain.

RQ2: Blockchain has been used in diverse fields and applications. However, the focus of the review was to find the applicability of Blockchain in DNS. Research reveals Blockchain provide a robust way for decentralizing DNS over traditional system .But the applicability of Blockchain in decentralizing DNS is still in infancy and is not explored in detail.

VII. Proposed work

Our proposed work is to develop a blockchain backed DNS, that is decentralised DNS on blockchain. Our work will be to store the DNS entries on blockchain. We will be storing a domain name and its corrosponding IP adress on blockchain.A single block will contain an information about a single domain .These blocks of DNS entries will be linked together by a Hash value of a previos block. We will not be replacing entire DNS system with blockchain but we will be trying to replace the DNS caching concept with blockchain. For this we will develop a web interface. It can be also done using command line. Our proposed work will be as follows:

- Develop a private etherium blockchain network with 3-4 nodes.
- Write smart contracts in solidity language and deploy them on blockchain.
- Use HTTP server to host web application for domain name resolution.
- Develop two smart contracts

A. Registration of DNS

This smart contract will provide an interface to register or store domain name information directly on blockchain.

B. Querying

This samrt contract will be used to retrive or fetch domain adress from blockchain. This will check first if the required domain is stored On blockchain .If so it will fetch it from blockchain. If not then it will retrive it from taditional DNS system and then will strore it on blockchain. Next if same domain is requested then domain resolution will be done from blockchain itself like DNS caching.

VIII. STRUCTURE OF A DNS RECORD IN OUR PROPOSED WORK

A DNS record for a domain will be stored in a structure DNS which stores the IP address or the nameserver (Dip), validity information valid from and valid to, owner address (owner addr), update address (update addr) and two arrays pubsd and privsd for storing the information about registered public and private sub-domains respectively. Structure of a DNS record is shown in table 2.

Table 2: Structure of DNS Record in proposed work

Block Header
Domain Name (e,g www.abc.com)
IP Address corresponding to particular domain (e,g 1.2.3.4)
Valid from (Date Of Registration Of domain on blockchain)
Valid to (Date of deletion of domain from blockchain)

IX. CONCLUSION AND FUTURE SCOPE

The technology of blockchain is still in the developing stage. Blockchain has many advantages in decentralization and security. Combining domain name service and blockchain is an excellent solution. It can make DNS decentralized and more secure. Blockchain technology is an unstoppable force that could converge to a storm of computing revolution that would profoundly reshape not only businesses and societies, but also variety of Internet services. In this storm, blockchain-based DNS systems are forerunners of this Internet innovations from whom we can learn lessons. Essentially, blockchain technology is a candidate of great promise for the next generation DNS system in that it inherently possesses the qualities of censorship-resistance, security, and resilience. On the other hand, there still are issues such as 51% attack and last mile problem which have to be addressed by the endeavor of blockchain communities and researchers before blockchain-based DNS can be standardized and deployed in practice.

ACKNOWLEDGMENT

Much significant thanks and profound respect to Mr. Mir Aman Sheheryar for his commendable direction, profitable criticism and steady support all through the term of review.

REFERENCES

[1] Mockpetris P V Domain names-concepts and facilities [J].Std Rfc Usc/information Sciences Institute, 1987, 21(6):513

[2] Mockapetris P. Rfc 1035: domain names implementation And specification [J].RFC-883, USC/Information Sciences Institute, 1987, 19(6):697.

[3] X. Wang, K. Li, H. Li, Y. Li, and Z. Liang, " ConsortiumDNS: A Distributed Domain Name Service Based on Consortium Chain," 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), 2017.

[4] Dyn Statement on 10/21/2016 DDoS attack [EB/OL]. http://dyn.com/ blog/dyn-statement-on-10212016-ddos-attack/.

[5] Ateniese G,Mangard S.A new approach to DNS security(DNSSEC).In: ACM Conf.on Computer and Communications Security.2001.86-95.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[7] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," Ethereum Project Yellow Paper, 2014.

[8] Hyperledger. https://www.hyperledger.org/.

[9] Namecoin. https://namecoin.org/

[10] M. Ali, J. C. Nelson, R. Shea, "Blockstack: A Global Naming and StorageSystem Secured by Blockchains," USENIX Annual Technical Conference. Pp.181-194, 2016. Pp.181-194, 2016.

[11] ATKINS D, AUSTEIN R. RFC3833: Threat Analysis of the Domain Name System (DNS) [J]. Internet Engineering Task Force, 2004, 5(1):108-117.

[12] WILCOX-O'HEARN Z. Names: decentralized, secure, human meaningful: Choose two [EB/OL]. https://web.archive.org/web/20011020191610/http://zooko.com/distnames.html.

[13] DINGLEDINE R, MATHEWSON N, SYVERSON P. Tor: the second-generation onion router [J]. Journal of the Franklin Institute, 2004, 239(2): 135-139.

[14] Kitchenham,B. et al, "systematic literature review in software engineering", Information and Software technology, Elsevier,2008.

[15] ATKINS D, AUSTEIN R. RFC3833: Threat Analysis of the Domain Name System (DNS) [J]. Internet Engineering Task Force, 2004, 5(1):108-117.

[16] WILCOX-O'HEARN Z. Names: decentralized, secure, human meaningful: Choose two [EB/OL]. https://web.archive.org/web/20011020191610/http://zooko.com/distnames.html.

[17] DINGLEDINE R, MATHEWSON N, SYVERSON P. Tor: the second-generation onion router [J]. Journal of the Franklin Institute, 2004, 239(2): 135-139.

[18] Medium. (2019). EthDNS: an Ethereum backend for the Domain Name System - Medium. [Online] Available at: https://medium.com/@jgm.orinoco/ethdns-an-ethereum-backend-for-the-domain-name-system-d52dabd904b3 [Accessed 25 Jun. 2019].

[19] Zhu Guo-ku, Jiang Wen-bao.A Decentralized Domain Name System for the Network [J]. Syberspace Security, 2017(1):14-18.

[20] Yuan Yong, Wang Fei-yue. Blockchain: the state of the art and future trends [J]. Acta Automatica Sinica, 2016, 42(4):481-494

[21] Zhao He, Li Xiaofeng,Zhan Likui,et al. Data integrity protection method for microorganism ampling robots based on blockchain technology[J].Journal of Huazhong University of Science and Technology(Natural Science Edition),2015(S1):216-219.

[22] Wang Jiye, Guo Lingchao,Dong Aiqiang,et al. Bolck Chain Based Data Security Sharing Network Architecture Sesearch[J].Journal of Computer Research and Development ,2017,54(4):742-749.

[23] Swan M. Blockchain Thinking: The Brain as a Decentralized Autonomous Corporation [Commentary][J]. IEEE Technology & Society Magazine, 2015, 34(4):41- 52.

[24] Kraft D. Difficulty control for blockchain-based consensus systems [J]. Peer-to-Peer Networking and Applications, 2016, 9(2):397-413.

[25] Zyskind G, Nathan O, Pentland A'. Decentralizing Privacy: Using Blockchain to Protect Personal Data[C]// IEEE Security and Privacy Workshops. IEEE, 2015:180- 184.

[26] Kypriotaki K, Zamani E, Giaglis G. From Bitcoin to Decentralized Autonomous Corporations[C]// International Conference on Enterprise Information Systems. SCITEPRESS - Science and Technology Publications, Lda, 2015:284-290.

[27] Kosba A, Miller A, Shi E, et al. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts[C]// Security and Privacy. IEEE, 2016:839-858.

[28] Haferkorn M, Diaz J M Q. Seasonality and Interconnectivity Within Cryptocurrencies - An Analysis on the Basis of Bitcoin, Litecoin and Namecoin[M]// Enterprise Applications and Services in the Finance Industry. Springer International Publishing, 2014: 107- 111.

[29] Blockstack: A New Internet for Decentralized Applications Muneeb Ali, Ryan Shea, Jude Nelson Michael J. Freedmany http://blockstack.org Whitepaper Version 1.1 October 12, 2017.

[30] Nebulis[EB/OL].https://www.nebulis.io/.

[31] IPFS (the InterPlanetary File System) [EB/OL]. https://github. Com/ ipfs/ipfs.

[32] IRVINE D. MAIDSAFE.NET: US, EP2118808 [P]. 2009.

[33] Ethereum project [EB/OL]. https://www.ethereum.org/.

[34]Emercoin[EB/OL].http://emercoin.com/DNS_and_Name-Value_Storage.

[35] Ethereum decentralized DNS [EB/OL]. http://etherid.org/.

[36] L. Liu and B. Xu, "Research on information security technology based on blockchain," 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), 2018.

[37] B. Benshoof, A. Rosen, A. G. Bourgeois, and R. W. Harrison, "Distributed Decentralized Domain Name Service," 2016 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), 2016.

[38] K. Kim, Y. You, M. Park, and K. Lee, "DDoS Mitigation: Decentralized CDN Using Private Blockchain," 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), 2018.

[39] J. Liu, B. Li, L. Chen, M. Hou, F. Xiang, and P. Wang, "A Data Storage Method Based on Blockchain for Decentralization DNS," 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), 2018.

Authors Profile

Aabid Hussain Ganai pursed Bechelor of Computer Science and Engineering from Baba Ghulam Shah Badshah University Rajouri, Jammu in 2016. He is presently research scholor of Masters of Technology from Central University OfKashmir, India.

Mir Aman Sheheryar pursed Bachelor of Technology from Islamic University of science and Technology, J&K India in 2014 and Master of Technology with specilization in Networking from Sharda University in year 2016. He has IIRS certfication, CCNA,CCNP and MCSA certificaions.Trained SSCVT driven process.. Currently working as Assistant Professor in Department of Information Technology, Central University of kashmir,India . He has guided various research projects and published research papers in reputed international journals also available online. His main research work focuses on Cyber Forensics, Network Security, Cloud computing, Networking,, IoT,wireless Communication,Mobile Computing and authentication. He has 2 plus year of teaching experience and 1 year of Technical Experience as Network Admin.