Chapter 14
Global Naming and Storage System Using Blockchain

Chanti S.
Pondicherry University, Pondicherry, India

Taushif Anwar
 https://orcid.org/0000-0002-6937-7258
Pondicherry University, Pondicherry, India

Chithralekha T.
Pondicherry University, Pondicherry, India

V. Uma
 https://orcid.org/0000-0002-7257-7920
Pondicherry University, Pondicherry, India

ABSTRACT

The global naming systems are used to resolve the DNS (domain name system) queries by providing the IP address of a particular domain. Humans are familiar in remembering the text rather than numbers. So the DNS servers help in resolving the human-readable domain names into system understandable IP address. In the current DNS architecture, there are several threats that cost a lot of damage to the organizations. At the earlier stage, DNS protocol lacks security assurance in place. To solve this issue, they introduced DNSSEC (subsequent DNS) as an additional layer of trust on top of DNS by providing authentication. Still, the current DNS servers couldn't address issues such as DoS/DDoS attacks. To address all these issues, blockchain technology offers an innovative method to handle those challenges. The existing naming systems are centralized, which is a major problem in achieving security.. The main aim of this chapter is to provide an overview of blockchain technology and a brief introduction to blockchain-based naming and storage systems.

INTRODUCTION

The Domain Name System (DNS) is introduced in the early days of the internet and mainly used for an academic and military purpose (Wei-hong, Meng, Lin, Jia-gui, & Yang, 2017). DNS is used to translate the human-readable names into the numerical address of the computer. At the early stage, a host file is maintained to store the human-readable name to represent the numerical address of a computer on ARPANET (Wikipedia, n.d.). Maintaining the host files in the long turn becomes much complex and to overcome this, Paul Mockapetris created the Domain Name System in early 1980s.

The DNS lacks in security features because they didn't think that the Internet will become popular and spread globally. Denial of Service Attack (DoS) becomes a major security threat to the DNS (Bisiaux, 2014). To overcome those security issues, DNSSEC is introduced to address the security problems created on DNS (Marrison, 2015). DNSSEC provides the authenticity and integrity of the information in DNS. But, the DNSSEC fails to address the confidentiality of the data because the data is not encrypted and so anyone can see the information and there is a possibility that the manipulation of information is also carried out.

Blockchain is a decentralized peer-to-peer network, in which all the nodes in the network share the same information (Wikipedia, 2019a). It is like a public ledger that is available with all the nodes in the network and so any type of insertion or updation of records can be ubiquitous. Bitcoin is the cryptocurrency used in blockchain for transferring digital money in a peer-to-peer network more securely (Crosby, Pattanayak, Verma, Kalyanaraman, 2016). The blockchain network is fully decentralized and there is no third party in between them (Iansiti & Lakhani, 2017; Pilkington, 2016). In the initial stages, the blockchain is used for the digital transaction using cryptocurrencies. In blockchain, the miner is a peer in the network who mines the set of transaction to create a new block and miners are rewarded for successful creation of a block. Later, the technology behind the blockchain is used for many purposes. Some real-time application of blockchain technologies are: voting system using blockchain, in food industry the blockchain helps end user to see all the stages from the former to the customer, blockchain based land registration process, blockain based DNS and so on (Foroglou & Tsilidou, 2015). Blockchain can be used for global naming and storage system that is fully decentralized and it also maintains the security level as higher (Wang, Wang, Guo, Du, Cheng, & Li, 2019). The blockchain based naming system can address the security issues in the traditional DNS.

A secured naming system is required to protect the privacy of the internet users. The structure of this book chapter is given as follows: Section-1 explains the basic concepts of DNS like how it works, what are the components and parties involved in creating a domain name and so on. Section-2 is about the potential threats systems. (For example, Denial of service attack, Zero-day attack, DNS cache poisoning, DNS hijacking) that current DNS couldn't failed to address. Section-3 provides the alternative solutions that are available to provide a secure internet i.e., blockchain based naming and storage system. Namecoin, Blockstack, Nebulis, Bitforest are the existing blockchain based naming systems. Finally section-4 provides the conclusion of the book chapter.

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/global-naming-and-storage-system-using-blockchain/261982

Related Content

Global Terrorism as a Virus: Pathogenesis of Evildoing
Primavera Fisogni (2021). *International Journal of Cyber Warfare and Terrorism (pp. 58-73).*
www.irma-international.org/article/global-terrorism-as-a-virus/289386

Global Information Infrastructure
Andrew Colarik (2006). *Cyber Terrorism: Political and Economic Implications (pp. 58-81).*
www.irma-international.org/chapter/global-information-infrastructure/7429

A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare
Kenneth J. Boyte (2017). *International Journal of Cyber Warfare and Terrorism (pp. 54-69).*
www.irma-international.org/article/a-comparative-analysis-of-the-cyberattacks-against-estonia-the-united-states-and-ukraine-exemplifying-the-evolution-of-internet-supported-warfare/181793

Anti-Social Factors Influence the Decision Making of Tourists: A Study of Kashmir
Parwaiz Ahmad Najar, Hafizullah Dar, Priya Singhand Ashaq Hussain Najar (2022). *International Journal of Cyber Warfare and Terrorism (pp. 1-14).*
www.irma-international.org/article/anti-social-factors-influence-the-decision-making-of-tourists/315590

In Internet's Way: Radical, Terrorist Islamists on the Free Highway
Raphael Cohen-Almagor (2012). *International Journal of Cyber Warfare and Terrorism (pp. 39-58).*
www.irma-international.org/article/in-internets-way/86075