


Chapter 2

Decentralization Principles of Blockchain and BC Tokenization (NFTs) in the Era of Smart Cities

Usman Khalil

 <https://orcid.org/0000-0001-8550-1557>

Universiti Brunei Darussalam, Brunei

Owais Ahmed Malik

 <https://orcid.org/0000-0002-4888-5448>

Universiti Brunei Darussalam, Brunei

ABSTRACT

This chapter delves into the fundamental concepts of distributed and non-distributed systems, laying the groundwork for understanding the intricacies of blockchain technology. A comprehensive overview of public, private, and hybrid blockchain networks is provided, highlighting their unique characteristics and applications. The chapter explores the concept of blockchain tokenization, with a particular focus on non-fungible tokens (NFTs) and their potential to revolutionize security, authentication, and asset digitization. A critical analysis of the challenges and future directions of blockchain technology is presented, followed by an examination of existing NFT-based CPS authentication mechanisms and gaps within the Web2 & Web3 architectures. The chapter concludes with a comparative literature review of NFT-enabled solutions for the cyber-physical environment, highlighting their strengths and weaknesses.

DOI: 10.4018/979-8-3693-8876-1.ch002

INTRODUCTION

This chapter delves into the fundamental concepts of distributed and non-distributed systems, laying the groundwork for understanding the intricacies of blockchain technology. A comprehensive overview of public, private, and hybrid blockchain networks is provided, highlighting their unique characteristics and applications. The chapter explores the concept of blockchain tokenization, with a particular focus on non-fungible tokens (NFTs) and their potential to revolutionize security, authentication, and asset digitization. A critical analysis of the challenges and future directions of blockchain technology is presented, followed by an examination of existing NFT-based CPS authentication mechanisms and gaps within the Web2 & Web3 architectures. The chapter concludes with a comparative literature review of NFT-enabled solutions for the cyber-physical environment, highlighting their strengths and weaknesses.

DISTRIBUTED AND NON-DISTRIBUTED SYSTEMS

The internet inherently poses security risks. Among the myriad services and APIs, certain users are often motivated to breach the layers of established security measures. Jacob Ideskog believes that the “IoT is going to hit us hard if we’re not doing anything about it” (Sandoval 2017). Leading this, many mechanisms based on centralized Web2 architectures have been developed and deployed however scope for robust security mechanisms continues. In a non-distributed (or centralized authorization system) the resources are also shared over the interconnected network but the decisions are centrally controlled by a miner machine such as a server in case of client-server computing exhibiting Web2 design. Here any service that needs the authorization to carry out a specific task gets routed to the central server which approves in case all the decision keys meet the criteria or else disapproves in case or vice versa. The concept gained popularity and most of the systems all over the world implemented the centralized/non-distributed system mechanisms as a safety precaution as every request has to be approved every time by the server to stop illegitimate use of the system until Web3 architectures were introduced (Lampson et al. 1991, 1992).

On the other hand, a distributed system (also known as a non-centralized system) consists of hosts that are interconnected by a network. The hosts here refer to the computers in an interconnected computer network. These hosts communicate with each other and other resources in the network such as files and printers with the help of network services provided by servers. These resources are shared over the interconnected network and can be used by distributed authorization systems

22 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/decentralization-principles-of-blockchain-and-bc-tokenization-nfts-in-the-era-of-smart-cities/386799

Related Content

Discovering Periodicity in Network Flows for Security Monitoring

Neminath Hubballiand Deepanshu Goyal (2016). *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security* (pp. 180-199).

www.irma-international.org/chapter/discovering-periodicity-in-network-flows-for-security-monitoring/153076

Quantum Computing for Cybersecurity: A Comparative Study of Classical and Quantum Techniques

Mohammad Alauthman, Ammar Almomani, Ahmad Al-Qerem, Mohammad A. Al Khaldy, Amjad Aldweesh, Ali Younis Al Maqousiand Mouhammd Alkasassbeh (2024). *Innovations in Modern Cryptography* (pp. 75-100).

www.irma-international.org/chapter/quantum-computing-for-cybersecurity/354036

A Novel Survey on Blockchain for Internet of Things

Jay Kumar Jainand Varsha Jain (2020). *Transforming Businesses With Bitcoin Mining and Blockchain Applications* (pp. 68-90).

www.irma-international.org/chapter/a-novel-survey-on-blockchain-for-internet-of-things/238359

Fundamentals of Quantum Computing, Quantum Supremacy, and Quantum Machine Learning

Kamaljit I. Lakhtariaand Vrunda Gadesha (2021). *Limitations and Future Applications of Quantum Cryptography* (pp. 21-46).

www.irma-international.org/chapter/fundamentals-of-quantum-computing-quantum-supremacy-and-quantum-machine-learning/272363

Pixel Value Differencing Steganography

(2019). *Advanced Digital Image Steganography Using LSB, PVD, and EMD: Emerging Research and Opportunities* (pp. 43-74).

www.irma-international.org/chapter/pixel-value-differencing-steganography/230057