Cluster Computing (2025) 28:208
https://doi.org/10.1007/s10586-024-05026-w

IBF network: enhancing network privacy with IoT, blockchain, and fog computing on different consensus mechanisms

Iraq Ahmad Reshi[1] · Sahil Sholla[1]

Received: 30 April 2024 / Revised: 8 September 2024 / Accepted: 21 December 2024 / Published online: 25 January 2025

Abstract

An amalgamation of blockchain technology and the Internet of Things (IoT) has presented notable concerns regarding scalability, security, and privacy, particularly in IoT contexts with limited resources. Conventional blockchains, including traditional consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS), meet challenges in handling many transactions, meeting energy efficiency standards, and addressing privacy issues in blockchain-based IoT networks. This work presents a new fog-based blockchain paradigm that integrates the benefits of Proof of Authority (PoA) and Delegated Proof of Stake (DPoS) consensus mechanisms and a proxy re-encryption approach to guarantee improved efficiency and system security. The proposed architecture integrates three essential operational algorithms: Fog Node Operation, Blockchain Node Operation, and Privacy Preservation Mechanism. These algorithms manage data processing, ensure secure transactions, and maintain privacy. Fobsim is used to conduct a series of simulations to evaluate the performance of PoA, DPoS, PoW, and PoS. The results indicate that PoA and DPoS provide better transaction speed, energy efficiency, and scalability than conventional consensus. As illustrated in the results, PoA stands out for its deficient energy consumption, making it an ideal fit for IoT applications. This research addresses the pressing concerns of scalability, privacy, and energy efficiency in blockchain-enabled Internet of Things (B-IoT) systems. The results lay the foundation for the future advancement of integrated B-IoT systems that can enable extensive, real-time IoT applications.

Keywords Consensus · Proof of authority · Blockchain based IoT · Fog computing · Proxy re-encryption · Delegated proof of stake

1 Introduction

Today, the Internet of Things (IoT) has become very popular due to the availability of affordable and powerful devices like sensors, radio frequency identifiers (RFIDs), and different communication technologies. This popularity has opened up opportunities for developing home automation systems and industrial applications, including connected drones, connected health, smart farming, wearables, and more. The IoT industry is forecasted to grow from over 15 billion devices in 2015 to more than 75 billion devices by 2025 [1]. According to this forecast, the average number of personal IoT devices per person on the planet will be at least 25 [2]. The data generated by these devices is projected to reach an astonishing 73.1 zettabytes(ZB) [3]. Hence, it is crucial to provide resilient systems that safeguard the confidentiality of users' identities and empower them to manage the disclosure and utilisation of their data. Nevertheless, the swift growth of IoT networks has brought about substantial barriers, especially in data confidentiality, protection, and scalability. Contemporary approaches to guarantee security and privacy in the IoT, such as obfuscation [4], enforcement [5]), and one-time passwords (OTP) [6], largely prioritise the safeguarding data privacy. Nevertheless, these approaches frequently neglect the safeguarding of user privacy and are ineffective in preventing privacy breaches, particularly when data is housed and managed in centralised systems [7]. Furthermore, these centralised systems are susceptible to single

✉ Iraq Ahmad Reshi
rshiraq333@gmail.com

Sahil Sholla
sahilsholla@gmail.com

[1] Department of CSE, Islamic University of Science and Technology, Awantipora, Kashmir, J&K 192122, India