Hierarchical Block Verification in Blockchain and Cluster-based Content-Centric Networks

Kamrul Hasan and Seong Ho Jeong
Hankuk University of Foreign Studies
kamrul@hufs.ac.kr, shjeong@hufs.ac.kr

클러스터 기반 블록체인 콘텐츠 중심 네트워크의 계층적 블록 검증

하산 캄룰, 정성호
한국외국어대학교 정보통신공학과

Abstract

This paper introduces a new hierarchical block verification approach, combining the robustness of blockchain technology with the efficiency of cluster-based content-centric networks (CCCN). The proposed architecture employs a hierarchical mechanism for validating blocks, enhancing security and trust in the network. Through the fusion of blockchain and cluster-based techniques, the system aims to address challenges related to content-centric networks (CCN), offering a better solution for hierarchical block verification. The study explores the intricacies of this hybrid approach, its implications for CCN, and its potential contributions to advancing the security and reliability of distributed systems.

Ⅰ. Introduction

The fusion of blockchain and CCCN may enhance the efficiency of the block verification methods [1]. This paper explores "Hierarchical Block Verification," leveraging the decentralized nature of blockchain and strategic clustering in CCCN. Navigating modern information systems and understanding this verification process within both blockchain and CCCN is crucial. Through an examination of its architecture, this paper illuminates the transformative potential of Hierarchical Block Verification at the intersection of blockchain and CCCN.

Ⅱ. Method

Figure 1 illustrates a cluster-based block verification architecture. The yellow nodes denote area leaders, defined by a cluster head selection mechanism, while other nodes function as area members. Double-circled yellow nodes represent zone leaders. Each cluster corresponds to an area, and the network comprises N areas, collectively forming a zone. The network further encompasses M zones. Area leaders within each area establish connections with neighboring area leaders, and zone leaders similarly connect with their counterparts in neighboring zones. Communication enables the verification of proposed blocks by a blockchain user, contingent on the security level assigned to the block.

The CCCN meticulously categorizes proposed blocks according to their content type, assigning distinct security levels for effective management. Verification procedures align with these security classifications: low-level blocks undergo scrutiny within the confines of the area, mid-level blocks within the broader zone, and high-level blocks within both the zone and the vigilant oversight of the neighboring zone leader. The zone leader's dual responsibility involves not only monitoring but also strategically constraining nodes afflicted by security issues, thereby fortifying the overall security stature of the verification process and upholding network safety consistently across diverse areas and zones.

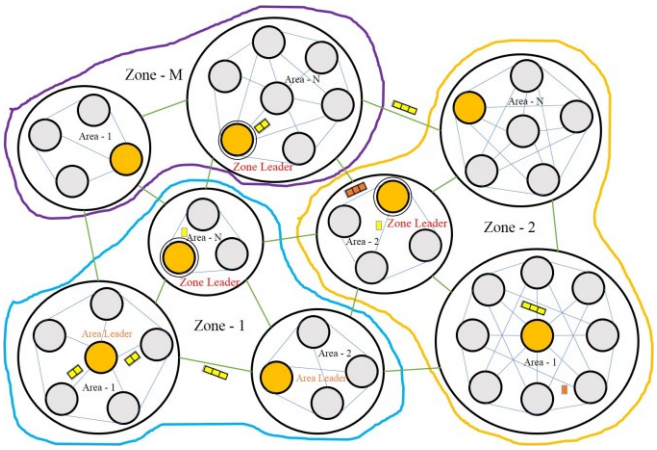

Figure 1: A cluster-based block verification architecture

Ⅲ. Conclusion

In this paper, we introduce an architecture for hierarchical block verification, integrating CCCN and blockchain. The verification of blocks occurs in areas or zones based on three distinct security levels assigned to each individual block.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2021-0-00484).

REFERENCES

[1] Xiao, Y., Zhang, N., Lou, W. and Hou, Y.T., 2020. A survey of distributed consensus protocols for blockchain networks. IEEE Communications Surveys & Tutorials, 22(2), pp.1432-1465.