Hierarchical Model for Consuming Proof-of-Work Complexity in Blockchain Networks

Shashi Raj Pandey, Sabah Suhail, Yan Kyaw Tun and Choong Seon Hong*
Department of Computer Science and Engineering, Kyung Hee University
Email: {shashiraj, sabah, ykyawtun7, cshong}@khu.ac.kr

Abstract

Blockchain network possess severe challenge in scalability of ledger due to the frequency of transactions and the availability of the resources with peer nodes in the network. The availability of interconnected heterogeneous and lightweight resource-constrained nodes and the rampant growth of IoT with ability to generate transactions experience the need for a framework to accommodate them in the blockchain having resource extensive PoW solutions. In this paper, we proposed a hierarchical model to mitigate this problem of resource scarcity for the blockchain network by introducing a three layered theoretical framework with edge computing infrastructure. The qualitative analysis shows the proposed framework can enable reduction in blockchain weight and integration of heterogeneous nodes in the network.

1. Introduction

Blockchain networks, considered as a virtual overlay peer-to-peer (P2P) network is a type of decentralized and distributed network architecture where each independent nodes participating in the network acts as both suppliers and consumers of resources. It was first introduced as bitcoin’s public ledger in 2009 by Nakamoto [1]. Basically, the blockchain consists of a set of individual blocks, where each block is a record of the most recent transactions and contains hash of the previous block. The nodes in the blockchain network share a common database amongst themselves with the records of transactions. They have a tract of the network transactions and validate them with a decentralized consensus approach called mining process that involves in appending blocks with new transaction records in a chronological fashion to the blockchain. It follows a complicated cryptographic hashing problem as proof-of-work. Hashing algorithm is used to validate a block proof-of-work. Specifically, bitcoin uses hashcash proof-of-work function, SHA-256 [2] that is harder to decrypt through sheer luck or brute force. Thus, the process is resource-intensive and difficult. In Fig. 1 we see the difficulty in mining process over the time [3].

Public blockchain improves transparency during the transfer of monetary information of trading between peers. A miner solves the complex mathematical puzzle to validate and append new information in the network which ensures security of the transactions done. On the other hand, permissionless blockchain networks, also called private blockchain are considered as an evolving trading platform which only allows a certain number of trusted participants to exchange transaction and require significantly less energy to run. However, the challenge on scalability is yet to be tackled efficiently with a
In this paper we proposed a three layered hierarchical model with the Edge Computing Provider (ECP) that avails necessary computing and caching space for the blockchain network to the miners, and other resource-constrained nodes who aims to access the network. Thus, a successful integration of lightweight nodes in the blockchain network can be done. This architecture can eliminated the burden of PoW for the miners where the workload is adopted by ECP with some gas imposed.

2. Blockchain Network with ECP

Figure 2 shows the basic blockchain network where we introduce miners interacting with the ECP platform via a network interface. The block generation rate is considered as a poisson process with parameter \( \lambda \). The solution of PoW i.e., nonce reflects the successful mining process in the blockchain network. Basically, for the header \( h \) and data block \( D \), the size of block is defined as \( (h+D) \), and the corresponding success in mining is characterized as \( P_{\text{success}} = \lambda e^{-\lambda} \). Thus, the contention process while solving more complex puzzle to win the mining game will be increasing as the number of blocks in the network increases.

For the ease of complex PoW solutions, the miners can interact with the ECP to avail its computing resources. Further, the resourced constrained nodes and IoT devices can be integrated with the blockchain network such that they don’t need to store or mine the blocks. Instead, they associate themselves with the ECP which facilitates secure resource management solutions for them. For this purpose, a single smart contract assignment is deployed including all the defined policies [4].

3. Proposed Framework

Figure 3 illustrates the proposed framework which can enable integration of heterogeneous and lightweight nodes to access information in blockchain network. Some of the nodes can participate as a miner and instantiate new transactions in the network. For this purpose, they can coordinate with the edge computing infrastructure (ECP).

The propose model consists of three layers. The first layer is the participating nodes which are possible miners or the resource-constrained nodes (e.g., wireless sensors network) that are connected to the blockchain network. They have resources to be managed by some policies defined in the smart contract of the blockchain framework [4]. The second layer-the communication interface comprises of multiple access points and wireless links that interconnects miners with the edge computing infrastructure. Additionally, it also facilitates to build permissionless blockchain networks for business purposes. The third layer provides computing and caching facility to the blockchain which are the resources to be accessed by the miners upon economic interaction. The miners can purchase these resources to
earn themselves with mining reward.

The proposed model can provide following benefits. (a) The proposed hierarchical model can mitigate the complexity in solving the resource-extensive PoW solutions for the lightweight nodes. (b) The model allows flexible integration of heterogeneous devices in the blockchain networks. (c) Further, it provides an efficient trading platform to bind policies and manage IoT infrastructure. (d) In addition, it enables to resolve scalability issues by promising resources to the miners and involving in consensus process. The ECP also provides the necessary storage facility for the lightweight nodes to access the blockchain network.

![Figure 3 An illustration of the proposed framework](image_url)

4. Summary

The growth in interconnected heterogeneous nodes and Internet of Things expect a flexible architecture for effective resource management and a secure transfer of transactions generated in between. Blockchain technologies have emerged as a promising medium for value exchanges and are envisioned to accommodate these assets trading. In this paper, we explored the issue of scalability in distributed ledger and proposed a hierarchical model to integrate resource-constrained nodes in the blockchain network. We introduced ECP as a governing entity for handling complex PoW solutions for the miners and storing the network information for the lightweight nodes. The interaction instantiated with some incentive values or gas effectively characterized the miner’s participations for possible solutions in the consensus process. In the future, we aim to provide an optimization framework to address the scalability issues in blockchain network while integrating large scale IoT nodes.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2015-00557, Resilient/Fault-Tolerant Autonomic Networking Based on Physicality, Relationship and Service Semantic of IoT Devices) *Dr. CS Hong is the corresponding author

REFERENCES