Journal of Human-centric Science and Technology Innovation
Vol.1, No.3 (2021), pp.57-66
http://dx.doi.org/10.21742/jhsti.2021.1.3.08

The Proposed Model High-performance Grants Low Communication Latency to the Big Size of Data in a Secure and Private System-based on Blockchain with a Software-Defined Network (SDN)

Saad Alshihri[1*] and SooYoung Park[2]

*[1*2]Blockchain and Software Engineering (BaSE) Lab Department of Computer Science, Sogang University, South Korea*
[1]saaad77.sa@gmail.com.com, [2]sypark@sogang.ac.kr*

Abstract

Blockchain technology carries considerable interest from both academia and the financial market through unusual risk on thousands of available cryptocurrencies that make us extremely wondering which one of those is safe and secure to use. This paper suggests the development of Blockchain systems to disclose the significance of scalability. We survey the state-of-the-software-defined network (SDN) also addresses a certain track of Blockchain progress to carry out the useful aspects of the Internet of Things (IoT). In this paper, we present the character of the situation as a necessary decentralized along with algorithm-based consensus point of coordination in our society, showing that centralization is an organization that is not anymore designed to be a politically, private, and secure manner. In this work, we propose a light node-based SDN that significantly improves light Node routing performance. By including additional routing information when a packet passes through the root node for the first time in a light Node communication, when available, without significant overhead. We implement the Openflow protocol and evaluate its performance through extensive simulation. Results show that improves packet reception ratio, round-trip time, and energy usage of light Node communication compared to standard systems. The proposed model is a distributed architecture based on Blockchain technology, that delivers inexpensive, secure, intelligent, and simple access to any type of network infrastructure computing. The proposed model high-performance grants low communication latency to the big size of data in a secure and private system based on Blockchain with a software-defined network (SDN).

Keywords: *Blockchain, SDN, Security, Lightweight node, P2P file system*

1. Introduction

Satoshi Nakamoto proposed Bitcoin as the first cybernetic payment network drew on a decentralized peer-to-peer network [1], unnecessarily need for a trusted third party. Blockchain, one of the technologies leading the 4th industry, is a distributed ledger technology (DLT) that allows all participants to check, record, and store transaction information using a P2P trust network, not a central authority. Blockchain DLT, which is also called the second Internet revolution, is highly likely to be applied as an infrastructure technology for the 4th industry such as artificial intelligence, robotics, quantum computing, Internet of Things, 4D printing, cloud computing, and big data. Blockchain is the core technology of Bitcoin, and Blockchain

Article history:
Received (March 21, 2021), Review Result (April 25, 2021), Accepted (June 5, 2021)

eISSN: 2653-0007 JHSTI

is not only researched for its integration into various fields including finance, economy, logistics but also regarded as capable of changing the ecosystem of the whole industry. Blockchain is a data credit prevention technology based on distributed computing technology where data are stored in small storage called block, prevented from arbitrary modifications, and browsed by anyone [2]. A block consists of a hash with which the block is identified, a header containing block information, and a body containing transaction information. Each block has a head including 6 pieces of information (version, previous block hash, Merkle hash, time, bit, nonce). Among them, the previous block hash refers to the hash value of the block created just before the current block, each block contains the encryption hash, timestamps, and transaction data of the old block, using Merkle tree Hash. Every block has a different hash and nonce [Figure 1].

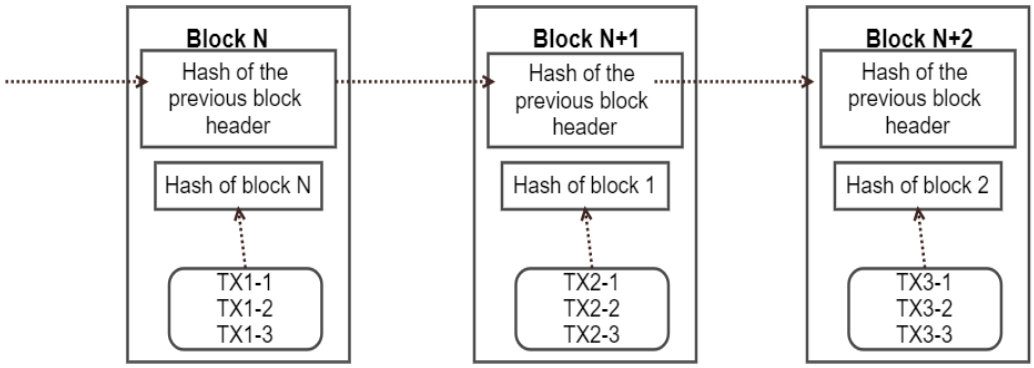

Figure 1. Blockchain is a list of records lists, blocks connected using encryption.

Blocks are verified using the connection to an earlier block in the way that the hash includes the previous hash. while maintaining the advantages of Blockchain - verifying, recording, and storing transaction information in the Blockchain- and distributing large data very effectively. The Blockchain is widely recognized as a major advance in distributed computing, we can determine the Blockchain contains all the transactions up till now verified in a peer-to-peer network. It contains a constant distributed digital ledger resistant to change or damage and carried out all the ledgers in peer-to-peer nodes of the networks. The intimidating about this new technology is that the network is open and participants do not need to know or trust each other to send and receive transactions that are preprogrammed to be verified and recorded by the nodes of the network via cryptographic algorithms, without human involvement, central control or middleman [2]. If small numbers of nodes are not conscientious or malicious, the network is proficient to accurately verify the transactions and defend the ledger from any untrusted nodes or malicious by using an arithmetic process known as proof-of-work that makes human interfering or administration needless. In addition to synchronization issues that arise upon reconnecting, disabling selected nodes that take part in maintaining the Blockchain results in a shift of power or influence over it [3]. The latter can be exploited by adversaries to force invalid data or transactions into the Blockchain. Blockchain is contemplated tamperproof distributed transaction ledgers in the first place designed as the distributed transaction ledger for cryptocurrency BitCoin [1][17]. The intention of using Blockchains has expanded and is expected to expand increasingly, but still needs more development and improvement.

2. Software-defined networking

Software-defined networking (SDN) technologies are emerging and intensively discussed including mobile, data centers, enterprise networks, etc. as one of the most promising technologies to introduce and realize network virtualization [4]. SDN is the latest networking technology that allows the distribution of centralized programmable control plane and data plan abstraction, where control and data planes are separated, so that network operators or service providers manage and control straight their virtualized resources and networks without acknowledging comprehensive hardware computers [5]. To provide such as system it's clear that SDN technology control and data planes are separated which grants control to be directly programmable and manageable in a distribution centralized method and data plane to be intangible and simplified rather than specially designed hardware not so efficient.

3. Software-defined networking-based blockchain

Combining Distributed Ledger Technology and SDN provides a new opportunity to closely integrate control provisioning in the Blockchain with the network through programmable interfaces and automation [6]. With Blockchain development, the existing Blockchain faces some significant challenges, including guaranteed performance, reliability implementation of hardware (e.g., intrusion detection systems or firewalls), linked difficulty to the strategy administration and topology dependence, and the security and privacy protection [7]. More programmable, more flexible, and more secure Blockchain infrastructure is needed. As a new networking paradigm, SDN is the key technology that can improve Blockchain manageability, scalability, controllability, and dynamism. SDN can provide a current, powerful network architecture that changes traditional Bitcoin backbones into a prosperous service delivery high-level system [6]. Moreover, the SDN-based framework, which supports a service-level model for Blockchain and can exploit multiple options for implementing virtual networks on the underlying physical network [Figure 2], where node confirming the transaction bottom layer. The data layer distributes the transaction. The control layer manages the flow of traffic between networks and the application layer was developed by individual users using Blockchain. Then they increase the practicability of OpenFlow [5] protocol to produce monitoring mechanisms tool, forwarding plane, stabilize the load, and power reduction.

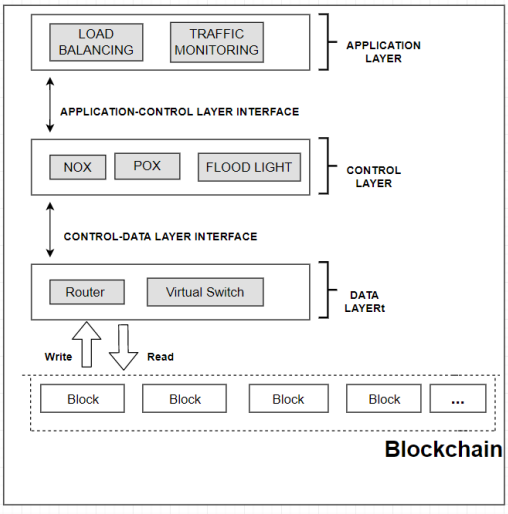

Figure 2. Blockchain Information technology architecture

4. Blockchain nodes

Simply there are three main node types: The Full node, slightly Full node, and the light node. Another term used to describe nodes is a client that provides wallet functionality. The entire block contains a history copy of the Blockchain, including all the blocks generated. All light nodes download only block headers to save your hard drive space. The Full node acts as a server on the distributed network. The main activities include maintaining agreement and verifying transactions between different nodes. Blockchain data are also stored and more secure when making decisions about the network, the Full node is the node that votes for proposals. If more than 51% do not agree with this proposal will ignore it. In some cases, this leads to a Hard fork where the community cannot agree on certain changes, thus creating two chains. The Pruning node is a particular node here is why when you start downloading blocks from the genesis block and reach a set limit, you delete only the oldest blocks and keep only the location of the headers and chains. For example, if you set the size limit to 5000 MB, you store all the latest blocks that fit into that hard drive space, and before you can switch to this state, you must validate the old blocks through the entire Blockchain. pruning nodes are considered Full nodes but We may disagree with that. Archive Nodes are what most people refer to running a Full node. They imagine a server hosting the entire Blockchain data, these key tasks are to maintain agreement and validate blocks. The difference between a Full node and an archive node is the difference in hard drive space, Full node stores the most recent blocks, the Ethereum Archive node requires stores of more than 4TB, and the Ethereume Full node is more than 200 GB. But since the Bitcoin Full and Archive node is the same block size more than 330 GB [12]. Another type of Blockchain node used is a lightweight node or a Simple Payment Verification (SPV) mode. As you've already seen, you're familiar with the definition of a light wallet [1]. Because this type of node provides the necessary information, it relies on the entire node to communicate with the Blockchain [18]. To avoid saving chain copies, only the block headers are distributed for processing. Given the above capabilities, running SPV nodes does not require many resources, but that will be a security question. In the next table, we summarize the differences between nodes [14][15]. In [Figure3], a summary of how node combination was done. First, node1 starts a transaction, and then node2 response back contains block header in light node, node3 starts a transaction by asking node4 to submit root of the block contains Merkle tree, timestamp, nonce, and transactions of previous blocks.

Table 1. Blockchain node types and properties

Types of nodes	Can propose new Block	Send new Transaction	Holds wallet balance Information	Holds complete data history of Blockchain	Holds some data history of Blockchain
Full Nodes	NO	YES	YES	YES	NO
Pruning Nodes	NO	YES	YES	NO	YES
Archive Nodes	NO	YES	YES	YES	NO
Mining Nodes	YES	NO	NO	NO	NO
Light Nodes	NO	YES	YES	NO	YES
SPV Nodes	NO	YES	YES	NO	YES

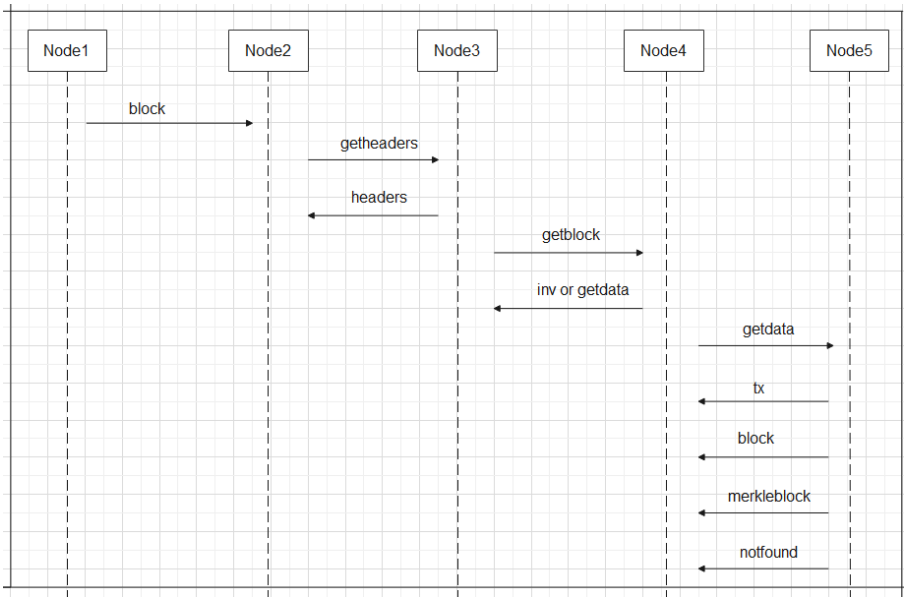

Figure 3. A blockchain- distributed transaction node joints

5. Simple payment verification

The SPV (Simple Payment Verification) is a method outlined in Satoshi Nakamoto's paper. SPV grants light nodes to check if the bitcoin Blockchain contains transactions left out downloading all the Blockchain data. The SPV node only just requires to download block headers that are needed to verify transactions that block headers point to the same transactions, the SPV client requests a certificate of inclusion to verify that the transaction is in the block. Merkle Tree combines tree efficiency with the advantages of encryption hashing. It was invented in the form of a branch of a macule tree [1]. The structure is generated by grouping all the transactions and hashing them together until only one hash, McRoot, remains. This creates a tree with two subordinate nodes on all nodes and can be used to create the parent nodes. The most important thing about McClure Tree is that it allows people who only know McClure Top Hash to see if the transaction is parting of the tree and included in Blockchain. This takes nodes in the path that connect Merkle Root to one of the lowest transactions and allows the original user to reroute to Root in a verifiable way, which allows Hash1 and Hash0 to see if they merged Gen.Erase top hash, meaning Hash1 and Hash0 are legitimate children, apply the same check indication to Hash0–0 and Hash0–1, claim that both are originally part of the block, and finally, L1 is the source of Hash0–0 [Figure 5], very efficient enough to represent millions of transactions and is not that deep only 20 hashes. This is enough to show less than 1GB of block size. However, the Merkle tree certificate for such a transaction remains less than 1KB in size. SPV authentication doesn't seem to be a big problem. Why did you perform the same task beyond all these hops when you could verify bitcoin transactions by running the entire node, the problem is that after running the entire node, you have to download the entire Blockchain but if you use SPV certificates, you only need to know the McRoot of each block to validate the transaction? Therefore, instead of the larger size per block required for all nodes, you only need to store 80 bytes per block. Such a reduction of 90% or more would be completely impossible if validation could be performed within a low-resource device or smart contract, and if we downloaded all the blocks “Figure 4. SPV nodes deliver additional

security than web wallets since they do not need to trust a single server. If a 51% attack on the virtual currency is successful, the attacker can trick clients that rely on SPV authentication and accept all kinds of invalid transactions, such as coins generated in the air. Our approach (proposed) using SDN will prevent this, though a successful 51% attack would raise questions as to how serious a threat it is regarding allowing double-spending, destroying basic security homes, and damaging the entire system.

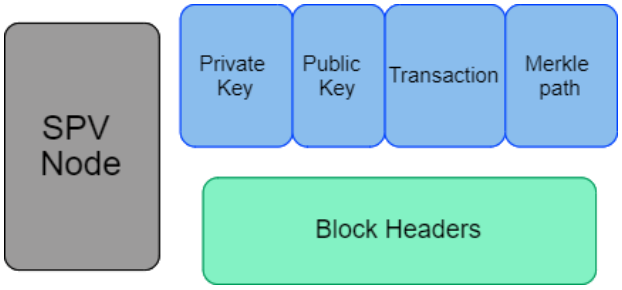

Figure 4. SPV node creates a transaction and asking a full node to verify UTXO

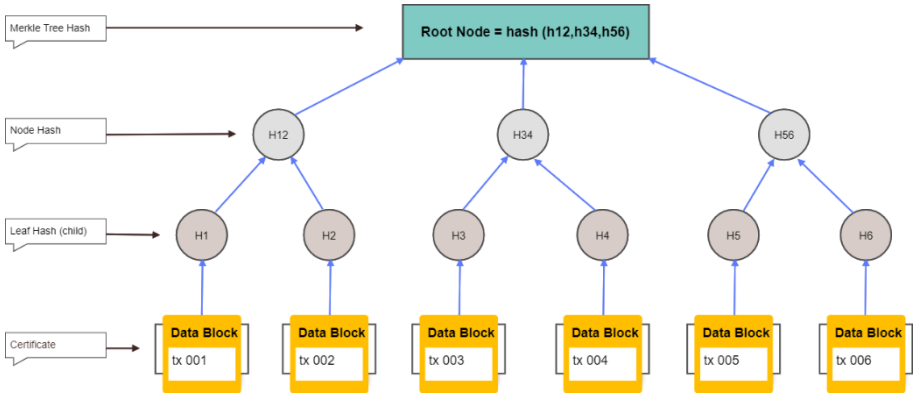

Figure 5. The Merkle tree data structure

6. Type-style and fonts IPFS

InterPlanetary File System (IPFS) is a hypermedia protocol processed with files and IDs, and a distributed file system designed to connect all computing devices through the same file system [2]. IPFS network divides a file into a block and stores the block where content-based hashes function as an address through which files can be approached and downloaded. IPFS can be a solution to the limit of block capacity, an existing limitation of Blockchain DLT. Large file data is distributed and stored on IPFS nodes, and only the hashes of IPFS files are stored on the Blockchain ledger. The file can be accessed and downloaded using the content-based hashes in the Blockchain network [Figure 6]. Process of accessing files stored in IPFS using hash values stored in the Blockchain. IPFS distributes and manages hash tables directly using Distributed Hash Tables (DHT), which can manage nodes with large data sizes by avoiding load concentration [11]. Besides, BitTorrent, a P2P file transfer protocol that distributes and stores files on the Internet, and downloads files from multiple locations at the same time to accelerate the transfer, is a representative technology expanded using DHT [11]. IPFS delivers large files fast and efficiently using the BitSwap protocol, a protocol inspired by BitTorrent, and is achieved by exchanging blocks with peers. In addition, IPFS stores all data on the

network in a Merkle-DAG structure, a combination of Merkle tree and Directed Acyclic Graph (DAG), which permits any node to hold data. Especially, since the Merkle tree is a binary tree where hash functions are used serially, the highest root hash value will change if the data is faked even a little. In IPFS, the content itself serves as an address of the data exchanged in the P2P network, through the Merkle-DAG structure, integrity can be verified with a multi-hash checksum, which can check whether the data has changed. IPFS stores encrypted file hash values, which were obtained by storing large files, in the ledger. The stored large files are read by comparing the hash values stored in the Blockchain to those stored in IPFS. However, the data itself imported from outside the blockchain may contain errors. Therefore, the reliability issue of the possible errors in the data itself, due to various factors such as omission or manipulation of the data, is still a task to be resolved.

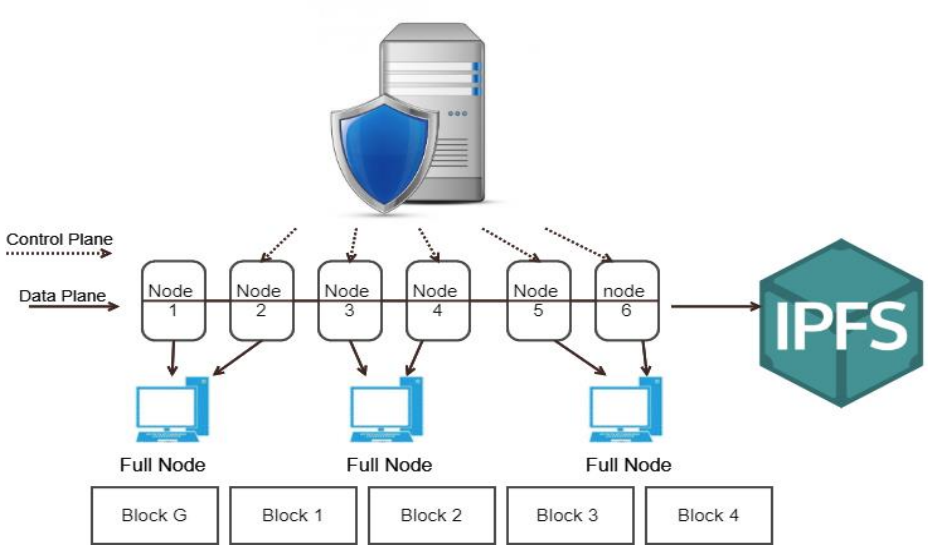

Figure 6. The IPFS- based architecture for collaborative SDN network

7. Security

An SDN capability by nature ensures the security benefit to any adapted technology lately, a numerous of research have aimed to drive Blockchain algorithms consensus to more ameliorate system but these consensus algorithms are solving some specific problems of Blockchain [7][9]. SDN can control nodes transactions as well as confirmations with the purpose that consensus becomes unnecessary and security can be significantly increased. Besides Blockchain computing power in Prof of Work (PoW) consensus algorithms [8] by generating the block so miners only store old block headers instead of full blocks, beside miners receive the prospect for mining blocks without the need of energy waste hardware as a POW so it's a win-win situation for miners and users. Using Blockchain and SDN to provide combined defense reducing the complexity of existing distributed protocols and architectures for manufacturing scalability and security attacks information. While Blockchain simplifies existing approaches with an out-of-the-box distributed infrastructure to broadcast addresses devoid of the require to create a special index or other distribution mechanisms methods, software-defined networks can optimize the management of flows in response to attacks "Figure 7 show that SDN separates those manage layer from the data layer to improve network visibility by distributed centralized control for performing operations in particular network

problem detection and solving it, the OpenFlow Protocol capability network controller by providing a programmable and systematize joining in the middle of the data layer and control layer, that will help us to prevent the node from malicious node attack. The issue with using Virtual Private Servers (VPS) with lighting nodes is you have to pay fees and not very secure [18], with our approach no fees and having to maintain SDN hardware and software, so the risk of hacking into servers and stealing your funds are reduced.

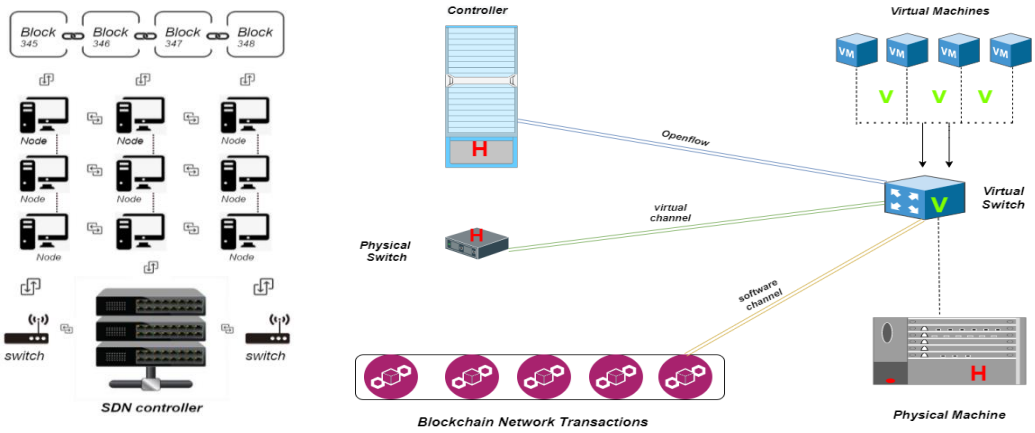

Figure 7. A Blockchain-based architecture for collaborative SDN network

8. Simulation evaluation

The simulation was done using the NS3 simulator [16], which provides a control simulation environment for nodes network and detection of a malicious node using OpenFlow protocol in Ubuntu with processor intel core i5-7500 CPU @3.40GHz*4, a memory of 7.6 GiB, graphics mesa intel HD graphics 630 KBL GT2, and disk capacity of 1.0TB. The node that attempting to join the network registers with the certification authority which is the SDN and then assigns the IP to the OpenFlow protocol. It is managed intelligently centrally and distributed controller using a communication protocol such as OpenFlow. When malicious or untrusted nodes are trying to connect to other nodes, the OpenFlow protocol detects the malicious node by SDN Certificate Authority Reception node and authentication View the information through permissions and assign a node ID or IP to the SDN then SDN and nodes communicate with each other. If the node ID or IP does not match the registered info, SDN will detect the malicious node.

Table 2. Simulation parameters

Parameter	Value
Network weight	100 nodes
Malicious node	10 nodes
Simulation time	100 sec
Traffic type	VM

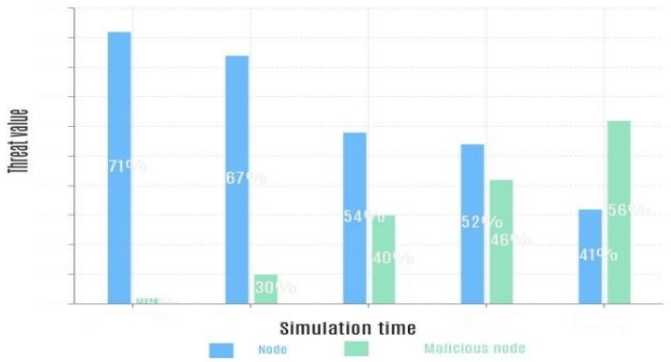

Figure 8. Malicious node detection percentage simulation in the network

9. Conclusions

SDN separates the data plane and control plane, therefore, allows creating simply large-scale and defense from attack network structure. High distribution of SDN provides intelligible detachment among virtual networks grant researching on a real domain, in our proposed security and scalability problems in Blockchain can be solved with a more complicated authentication with the centralized server. In Blockchain and SDN architecture we don't need to be ensured by a Proof of Work (PoW) mechanisms, that, for the generation of a new block requires solving a very complex, and computationally expensive, mathematical puzzle. Blockchain-based SDN is vulnerable to malicious node attacks, which can prevent Blockchain nodes from transmitting or receiving any block information. There is a great need to design appropriate security mechanisms to inspect and control traffic. Because of this problem, our approach establishes the protection of data node attack reduction and obtains control. From now on we will expand our experiment with Bitcoin testnet and compare our work with other models.

Acknowledgments

This work has been financially supported by the information and Communication Technology Promotion Center, funded by the South Korean government (Ministry of Science, Technology, and Information) in 2018 (No. 2021-2017-0-01628, Human resource training of information and communication technology)

References

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” **(2008)**, Available: https://bitcoin.org/bitcoin.pdf

[2] Blockchain as a Service, Available: https://azure.microsoft.com/en-us/solutions/blockchain/

[3] V. Buterin, “On public and private blockchains,” **(2015)**, Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[4] F. Hu, Q. Hao, and K. Bao, “A survey on software-defined network (SDN) and open flow: From concept to implementation,” IEEE Community Surveys Tuts., vol.16, no.4, pp.2181-2206, **(2014)**

[5] OpenFlow Switch Specification version 1.3, Open Networking Foundation, http://www.opennetworking.org/, 2012
[6] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," IEEE Community Surveys Tuts., vol.15, no.4, pp.2046-2069, **(2013)**
[7] NRI: Survey on blockchain technologies and related services. Tech. rep. **(2015)**
[8] D. Kraft, "Difficulty control for blockchain-based consensus systems," Peer-to-Peer Networking and Applications, vol.9, no.2, pp.397-413, **(2016)**
[9] "Floodlight OpenFlow controller," Project Floodlight, **(2017)**, Available: http://www.projectfloodlight.org/floodlight
[10] M. Yu, "Scalable flow-based networking with DIFANE," Proc. ACM SIGCOMM 2010 Conf., pp.351-62, 201
[11] B. Cohen, "Incentives build robustness in BitTorrent," In Workshop on Economics of Peer-to-Peer Systems, vol.6, pp.68-72, 200
[12] Blockchain Charts - Blockchain.com https://www.blockchain.com/charts/blocks-size
[13] Bitcoin Core: Bitcoin, Available: https://bitcoincore.org
[14] Bitcoin.org https://bitcoin.org/en/full-node
[15] Ethereum nodehttps://ethereum.org/en/developers/docs/nodes-and-clients/run-a-node/
[16] NS3 simulator https://www.nsnam.org/docs/tutorial/html/getting-started.html
[17] M. Tran, I. Choi, G. J. Moon, A. V. Vu, and M. S. Kang, "A stealthier partitioning attack against bitcoin peer-to-peer network," 2020 IEEE Symposium on Security and Privacy (SP), pp.894-909, **(2020)**, DOI: 10.1109/SP40000.2020.00027
[18] B. Zhao, Y. Liu, X. Li, J. Li, and J. Zou, "TrustBlock: An adaptive trust evaluation of SDN network nodes based on double-layer blockchain," PLOS ONE, vol.15, no.3, **(2020),** e0228844, DOI: 10.1371/journal.pone.0228844
[19] H. D. Hoang, P. T. Duy, and V. -H. Pham, "A security-enhanced monitoring system for northbound interface in SDN using blockchain," In Proceedings of the Tenth International Symposium on Information and Communication Technology (SoICT 2019), Association for Computing Machinery, New York, NY, USA, pp.197-204, **(2019)**, DOI: 10.1145/3368926.3369709

Authors

Saad Alshihri
Ph.D. Student, Blockchain and Software Engineering Lab, Department of Computer Science and Engineering, Sogang University Seoul, Korea

Prof. Sooyong Park
Sogang University Computer Science & Engineering Professor, Blockchain and Software Engineering Lab., Chairman of Korean, Blockchain Society, Leading Intelligent Blockchain Research Center, Dean of Graduate School of Information and Technology, Sogang University Seoul, Korea