ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20220427051644
Original scientific paper

A Decentralized Lightweight Blockchain Nodes Architecture Based on a Secure OpenFlow Protocol Controller Channel

Saad ALSHIHRI*, Sooyong PARK

Abstract: The Blockchain technology raises many concerns because all transactions must be verified by every node in the Blockchain network. Because of this the spread of Blockchain technology in all sectors has been very slow. This paper introduces Blockchain nodes and the difference between nodes and then our approach light node control node based on SDN that has a more secure routing mechanism than only light nodes or networks without full nodes and light nodes. In peer to peer networks nodes connect and disconnect all the time and some of these nodes are malicious and will cost the network security and scalability. We applied a technique that uses route packet information by making a table of the IP address with OpenFlow. We calculate our approach flow measurement performance using large scale simulations. The result showed that by using an IP table we can control the nodes connections and make more scalable, secure ones without the need of full nodes working all the time. The proposed model is a distributed architecture based on Blockchain and OpenFlow protocol technology that provides a low-cost, secure, intelligent, and simple approach in all types of computer network infrastructure.

Keywords: blockchain; lightweight node; openflow; P2P; security;

1 INTRODUCTION

Blockchain is a decentralized digital ledger technology (DLT) [1] that stores data on tiny memory structures called blocks that prevent arbitrary changes and allow anyone to explore it. Satoshi Nakamoto [2] introduced Bitcoin as the first digital payment transaction network based on a distributed peer-to-peer (P2P) network [2]. A reliable third party was unnecessary. Blockchain, the leading technology in the fourth sector, is a DLT that allows all participants to view and store transaction information according to trusted P2P networks instead of central organisations.

DLT is considered the second Internet rival and is probably useful for four-seater infrastructure technologies such as quantum computing artificial intelligence, robotics, cloud computing, the Internet of Things, and Big Data. Blockchain has the potential to change the ecosystem of the entire industry and integrate it into various fields such as finance, business, and logistics. A block contains internal information and transaction information about the block, called the block ID hash. Each block has an internal box containing elements of information on versions, previous block hash, Merkle hash, timestamp, and transaction data. The previous block hash represents the link between the hash of the previous block and current one, and each block encodes the hash of the previous block, timestamp, and transaction information using a Merkle tree hash. Each block is associated with a different nonce (Fig. 1).

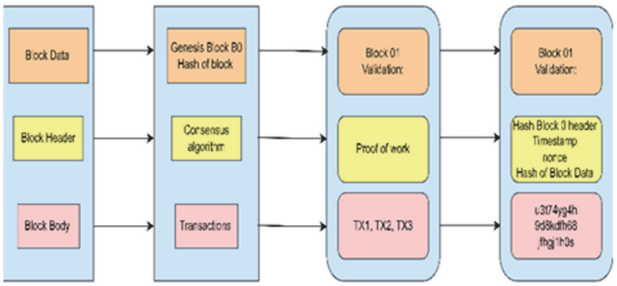

Figure 1 Blockchain records list, blocks connected using encryption

Blockchain is generally being a breakthrough in decentralized distributed computing, so we could assume Blockchain has advantages such as the ability to authenticate, record, and store transaction information, and it distributes big data in a very efficient way. Blockchain is gradually being introduced in decentralized distributed computing, so we could assume that it carries out all transactions that have been verified on all P2P networks to date. It also contains a distributed digital ledger that prevents any alteration or falsification of the entire ledger on the nodes of the P2P network. The threat of this new technology lies in the exchange of pre-programmed transactions that open up the networks and allow participants to use cryptographic algorithms that are verified and registered by the network nodes without the need for mutual understanding and trust [3]. If a small number of nodes are not steady or malicious, the network can use a procedure called proof-of-work to correctly verify and protect the transactions ledger from suspect or malicious parties' nodes and precludes interference or individual control.

Disabling a selected node involved in the maintenance of the Blockchain changes its authority and influence [4]. This can be exploited by attackers who can inject inactive transactions data into the Blockchain. It is expected that Blockchain will continue to proliferate if the intent is to use a tamper-resistant distributed ledger for transactions [2] [16]. Blockchain, which was originally conceived as a decentralized, distributed ledger of transactions for cryptocurrency such as Bitcoin, is still evolving but needs to be further developed and refined.

In this paper we will explain the difference between Blockchain full node and light node, light node architecture and how light node could be more powerful when we apply our approach to network nodes between the full node and the lightning network light node. We implanted simulations tools which allow us to monitor the network and evaluate our approach results.

2 BACKGROUD AND LIMITATION

Lightning network (LN), the off-chain second layer solution to Bitcoin on-chain [3]. In lightning network second layer nodes do not download all transaction

information, therefore the security will be reduced so we develop an SDN technology trying to make the network more secure by adapting openflow with a lightning node IP table that in this section we briefly introduce. Software defined networking (SDN) has been markedly discussed in the network sector, data centres, and enterprises as one of the most advanced and promising technologies for the implementation and realisation of network virtualisation [5]. SDN is a modern network technology that enables a centralised, programmable distribution of the abstraction of the data and control planes, and enables network operators to directly manage and control virtualized networks without the need for extensive hardware processing [6]. It is evident that SDN technology separates the control and data planes so that the control plane is directly programmable and can be managed by a centralised distribution, while the data plane is simplified, and hardware that is not specially designed is sufficient.

One of SDN technologies which we are using in our approach is OpenFlow protocol, a programmable network control separating packet control and forwarding functions.

Implemented in software by installing the control and data plane on a general purpose node the user can freely implement a specific service or application optimization protocol.

3 RELATED WORK

Light node off chain networks operate in a permissionless environment and should be resistant to threats. In the current off chain architecture, for example, no fees are charged if a payment fails, lost payments require network resources. An attacker could use this weakness to perform a security attack. Layer-two protocols improve on layer-one protocols. Light node protocols will not save transactions in a globally distributed open database that can be reviewed. However, several vulnerabilities in LN security have been uncovered [20]. Payment security might be damaged due to short channels. In this article, we focus on security issues, which are a major concern in off-chain solutions. It indicates that light node security will damage the network's reliability and performance. In this research, we emphasize on security issues, which are a major concern in off-chain solutions. We show that security of light nodes would impact the network's performance and node communication, resulting in a less scalable system [25]. Due to its peer-to-peer network design, as r random node connection implies malicious node and failures node that lead to security threats nodes [24].

4 SYSTEM MODEL

4.1 Blockchain Nodes

There are three main types of nodes: archive, full, and light. A full node contains a historical copy of all created blocks. Light nodes download only the block headers in order to reduce storage capacity. A full node operates as a server in a distributed network. Their main tasks are to maintain agreement and verify transactions between different nodes. Furthermore, voting on proposals takes place across all nodes and is more secure when decisions are made in the network. If more than 51% of the votes are against a proposal, it is not considered further. In some cases, when the community cannot agree on certain changes [11], a "hard fork" occurs, resulting in two chains. A hard fork is a specific node created when we begin taking blocks from a Genesis block and reach a certain threshold.

Archive nodes, usually mistakenly called full nodes, are servers where all Blockchain data are stored [12], and whose main tasks are to continue to maintain consistency and verify blocks. The biggest difference between full nodes and archive nodes is their disk capacities. Full nodes store the latest blocks; for example, an Ethereum archive node stores all data from genesis block and requires a storage space of more than 4 TB, while an Ethereum full node requires more than 200 GB. However, like Bitcoin full nodes, the block size is more than 330 GB [16]. Light nodes, another type of Blockchain nodes, come from Simple Payment Verification (SPV) that has been described in the original Bitcoin whitepaper [2, 3]. The SPV node does not store the entire Blockchain or monitor all transactions in the system. It only accepts a part of transactions filtered by the entire connected nodes, and requests specific data without revealing any information about the transactions associated with the node. By tracing the data requested by the SPV node, a third party in the network can link transactions to users, creating a threat to privacy and security. Since this type of node only provides the necessary information, it depends on the entire node to communicate with the Blockchain [13]. To avoid storing concatenated copies, only the heads of the blocks are distributed for processing. Although the operation of SPV nodes is not very resource-intensive, it is clear that there are security issues. Tab. 1 gives an overview of the differences between the nodes [14, 15].

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

4.2 Nodes Architecture

SPV is the method described in Satoshi Nakamoto's paper. SPV allows light nodes to verify the existence of transactions in the Bitcoin Blockchain without having to download the entire Blockchain. An SPV node only needs to download the necessary blockheads in order to verify that the blockheads refer to the same transactions. The SPV client requests an inclusion certificate to confirm that the transaction is included in the block. A Merkle tree is used to merge the efficiency of a tree with the advantages of hash encryption [2].

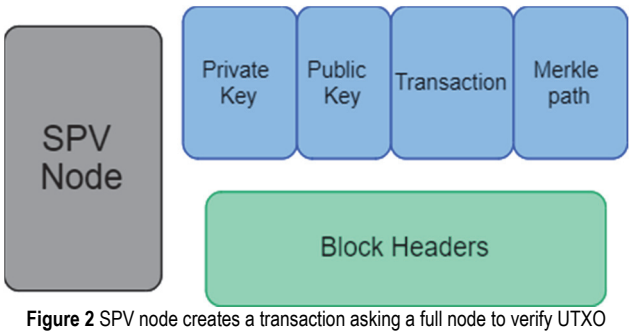

Figure 2 SPV node creates a transaction asking a full node to verify UTXO

A structure is created by combining all transactions and linking them to hashes until only one hash remains - the Merkle root. This creates a tree with two nodes: the parent node and child node. All block transaction information contains a Merkle root. The Merkle root allows each node in the network to verify individual transactions without having to download and verify the entire blocks. The Merkle tree allows each node in the network to verify any transaction without having to verify and download the entire blocks data. If one copy of a block in the Blockchain network has the same Merkle root with a few different entries, this would result in completely different transactions.

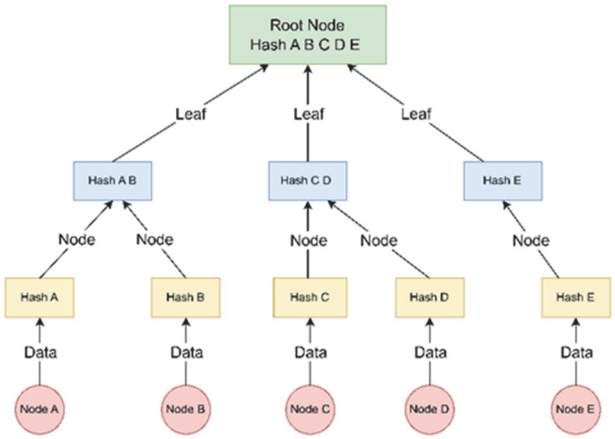

Figure 3 The Merkle tree data structure

Blockchain contains very different Merkle roots because of its hashing properties. Therefore, there is no need for the amount of information required; an important aspect of the Merkle tree is that people who only know the top hash of the Merkle tree can learn whether a transaction is part of the tree and has been included in the Blockchain transactions. Fig. 5 is structured to represent millions of transactions in only 20 hashes and a block size of less than 1 GB. However, the Merkle tree certificate for such a transaction is still less than 1 KB. SPV authentication does not seem to be a big problem.

The problem is needing to download the entire Blockchain after running the node. However, when using SPV certificates, you only need to know the Merkle root of each block in order to authenticate the transaction.

Only 80 bytes of transactions information need to be stored in all nodes unlike Blockchain full node. "SPV nodes" [17, 18] provide better security as they do not rely on a single server. If a virtual currency attack in Bitcoin SPV is 31% successful, an attacker can mislead customers who rely on SPV. We propose adopting the open flow protocol to avoid damaging the underlying security of the entire system network.

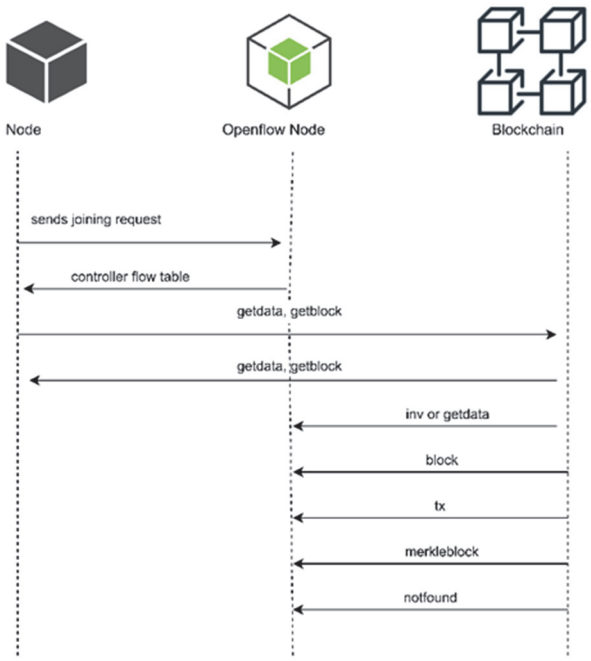

Figure 4 Blockchain- distributed transaction node joints

4.3 Lightweight Blockchain Structure

The combination of using decentralized distributed ledger technology and SDN delivers an advanced way to build up and control the distribution of nodes in a Blockchain network through programmable interfaces [7]. As SDN develops, existing Blockchain networks face many important challenges including assured performance, reliable hardware implementations such as intrusion detection systems or firewalls, difficult management strategies, network topology vulnerabilities, security, and privacy [8]. Additional programmable, flexible, and secure Blockchain infrastructure is required as a new network model SDN is a key technology that will enhance the scalability, manageability, controllability, and activity of Blockchain. SDN can deliver a modern, high-performance network facility that will transform Bitcoin's backbone networks into a thriving, high-level service delivery network system [8]. Moreover, an SDN-based framework can support a service-level model for Blockchain and provide various resources to deploying virtual networks at the top of a basic physical network (Fig. 5) where a node performs transactions on a lower layer. The data layer distributed transactions. The control layer controls traffic between the network and application layer, which is generated by each user applying Blockchain. This increases the likelihood that [10] when creating a control mechanism tool, the routing layer stabilizes the load and reduces energy consumption.

Fig. 4 summarises the node forwarding method where a p2p node initiates a transaction, and then OpenFlow node returns a response with the block header in the light nodes. OpenFlow node initiates a transaction by adding a p2p node to the root of the block which contains the Merkle tree, timestamp, nonce, and transactions of the previous blocks.

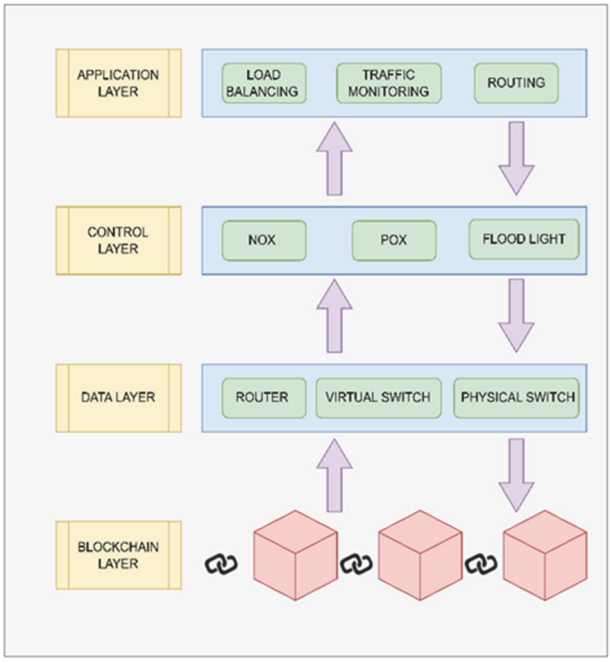

Figure 5 Blockchain Information technology architecture

5 IMPLEMENTATION

SDN features inherently provide a security advantage to any custom technology. Much of the recent research has focused on promoting consensus algorithms to improve the Blockchain system [19, 20]. SDN can verify both transactions and node confirmations, eliminating the need for consensus and greatly improving security. In addition to the computational power of the Blockchain in proof of work (PoW) consensus algorithms [21], miners can also mine blocks without energy-intensive hardware as in PoW, which is a win-win situation for miners and users as a block is only created by storing old blockheads instead of whole blocks. Using Blockchain and SDN for combined protection reduces the complexity of existing distributed protocols and architectures and enables scalability and intelligence in the face of security attacks.

While Blockchain simplifies existing approaches by providing a ready-made decentralized distributed infrastructure for broadcast transactions without the need to create a special index or other allocation mechanisms, SDN optimizes the control and management of data response to attacks. Fig. 6 shows that SDN separates the management layer from the data layer. This improves network visibility through distributed, centralized management in order to detect and fix specific network problems, using Virtual Private Servers (VPS) with light nodes that cost money and are not very secure [22]. Thanks to our free approach and the use of SDN hardware and software support, the risk of hacking resources servers is minimized. In the test we compare flow table based packets with action and other flow table entries allow adding metadata values to packets before sending one packet to another flow table, the meta data value is compared with the meta data value in the next table and continues to the next table until the packet is processed.

Then a set of action buckets to be executed for the incoming flow action bucket contains a set of actions to be executed and parameters consist of entry ID value, group type, and counter action buckets.

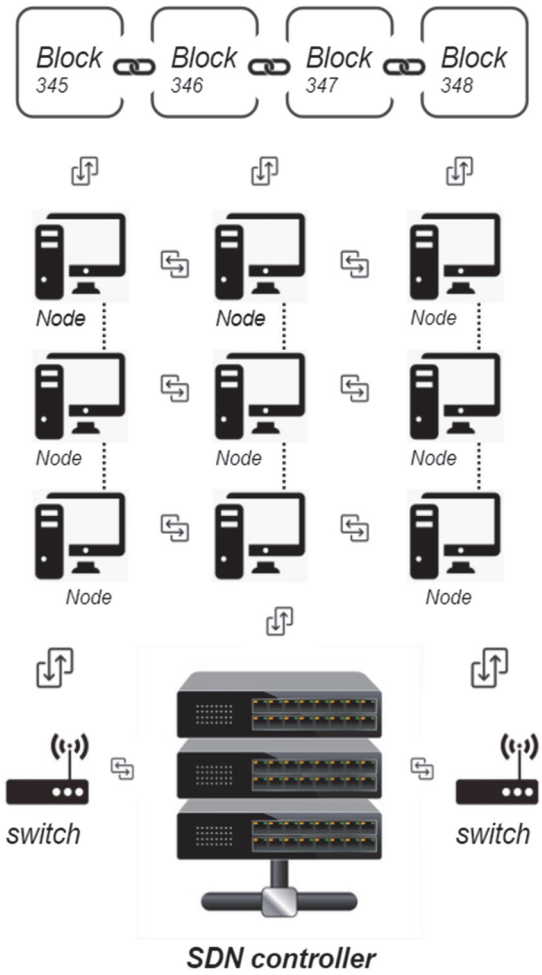

Figure 6 A Blockchain-based architecture for collaborative SDN network

6 SIMULATION EVALUATION

Our simulation was run using the NS3 simulator [23], a simulation environment for network nodes, and malicious node detection using the OpenFlow protocol on Ubuntu with an intel core i5-7500 @3.40 GHz*4 processor, 7.6 GiB of memory, mesa intel HD-Grafik 630 KB GT2 graphics, and a 1.0 TB hard drive. A node attempting to connect to the network registers with a certification authority, and then assigns an OpenFlow IP address. It is managed by an intelligent distributed central controller that uses an OpenFlow-type communication protocol.

The OpenFlow protocol detects untrusted nodes and malicious attempts to connect to other nodes and accepts and authenticates nodes by looking at the authorisation information and assigns the node an SDN ID or IP address. If the node ID or IP does not match any registered information, SDN will detect the malicious node.

Network nodes in Blockchain operate on virtual hosts using docking containers that provide portability, separations, and light node virtualization. Each container runs a Bitcoin core application. Multiple hosts can create an overlay network using a Docker cluster, which is a machine that can be used for simulation between different physical machines. Therefore, a very large Blockchain network can be evaluated using swarm Docker mode. Under real-world network conditions, our framework uses test tools developed to evaluate the resilience of docking

container applications, ensuring the reliability of the system and its ability to recover from failures. It is also possible to test the network by simulating various real-world elements. Network characteristics, such as delay, bandwidth, and packet loss, were also tested. We used built-in Linux features to manipulate container output traffic at the kernel level. NetEMextension can then be used to change traffic control rules and allow users to specify the network actions, containers, network interfaces, links, and directions (inbound or outbound) to run. In Blockchain Bitcoin limited tests and development environments, any solution tends to undermine the final use of the assessment tests. For example, Bitcoin testnet did not use Internet to respond to the developer. Additionally, cryptocurrency testnet could not imitate Bitcoin improved client application into the source code. Internet development objectives such as mining demand and alternative programs created in the block were included. We modified the testing Bitcoin network client application.

LAN was disconnected from the shared test network, providing global control over the test network. In the test environment to obtain a new Blockchain, we created a new Genesis block by marking Hash and Genesis Hash returns, and modifying the information in the existing Genesis source code. We also removed the DNS channels to protect the nodes in order to keep experimenting with equivalent IP addresses. Network topology and metrics played an important role in module performance. To ensure high flexibility in the network's node structure, the number of nodes and the topology of the Blockchain user must be determined. They are not only connected to each other, but also to some projects. User-specified nodes or connections with delays can also be assigned to specific start and end destinations.

We then performed resource offloading between nodes. Users can specify the number of processors allocated to each node depending on the available CPU power of the host. Mining Bitcoin nodes allows the internal excavator of an in-person client to continuously run clients, Bitcoin to set up a client and create new blocks, and the conditions use the maximum resources allocated to each node by weighing how the important functions of power distribution resources will affect the entire network. Safety and individual nodes control mining in difficult environments based on finite computational capabilities and the measurement of the difficulty and setup of the testnet network:

$$T = Mining\ difficulty \times 2^{32} \,/\, Hi$$

The mining of bitcoins requires a clear understanding of the relationship between the cost of mining and the corresponding income. In this experiment, the miner's income is calculated by multiplying the number of submitted blocks by the fee per block. The hashing power used in mining can be expressed as a percentage of the hashing rate, calculated with the following formula:

$$Hash\,rate\ \% = \frac{Mining\ difficulty}{Hash\ power\left(miners\right)}$$

Bitcoin nodes use gossip protocols to spread Blockchain notifications and data. This is done through the P2P network. The first consensus is that this protocol is vulnerable to network delays, causing Blockchain forks to be inconsistent with the network and raising concerns that network security could be compromised. Delay can affect the equity of the network because there are nodes with faster propagation speeds. Blocks created before delays are unlikely to be committed to the primary chain. Other contentions include area network delays, network fairness, network evaluation, and complex equitable relationships. An experiment was conducted to apply different network delay ranges.

Table 2 Blockchain node Simulation parameters

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

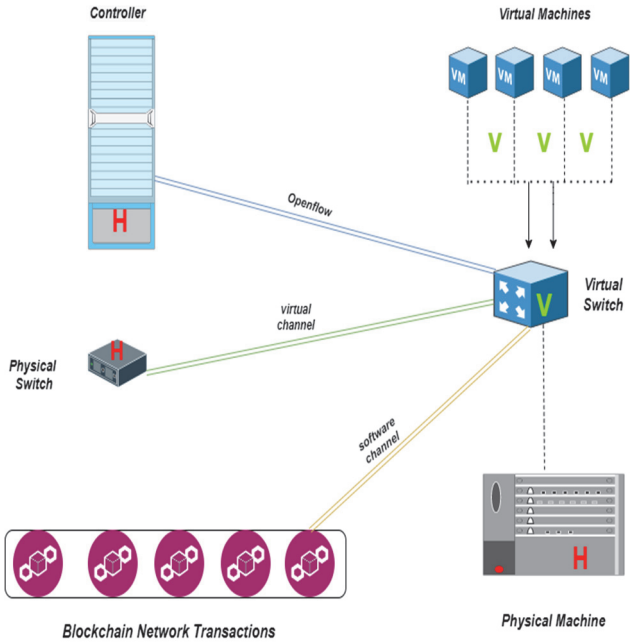

Figure 7 A Blockchain-based architecture for collaborative SDN network

7 RESULTS

Block efficiency improves the spread of relay networks although other mechanisms were conceptualized in the node experiment. Blocks are normally issued 10 times and connect to a node bandwidth network for other relay participants. The phase is then changed to a node percentage transmission network for block propagation medium time measurement. This is the centre value of propagation time. Measurements are made for the following type of node groups: non-member network and relay network nodes. Blockchain sets parameters to the same conditions, and the simulation results with a low percentage special call network ratio are shown in Fig. 8. However, the node threat value shows significant improvement with simulation time. The nodes that participate in propagation network delay time of the transmission cycle can achieve more improvements as the delay increases. Figs. 9, 10, 11, 12, and 13 show the results of the block node network, mining difficulty, and time.

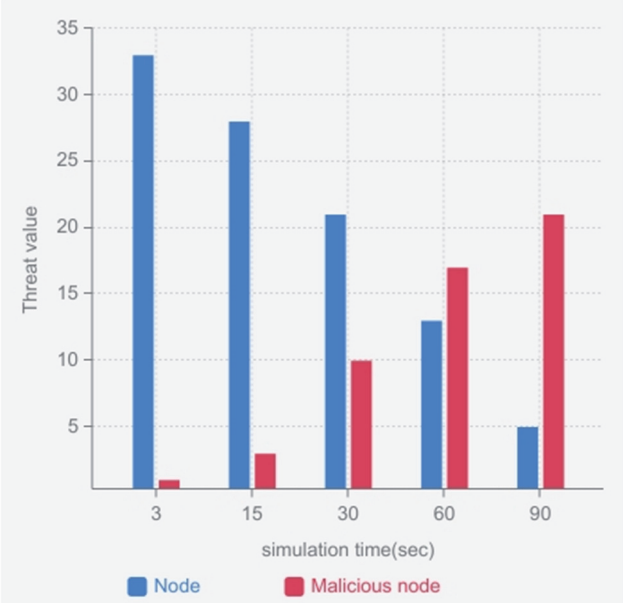

Figure 8 Malicious node block propagation time

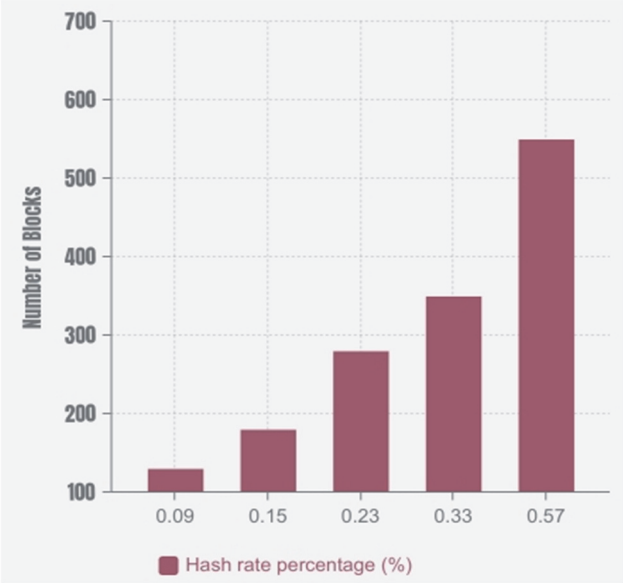

Figure 9 Local test network hash rate and committed blocks

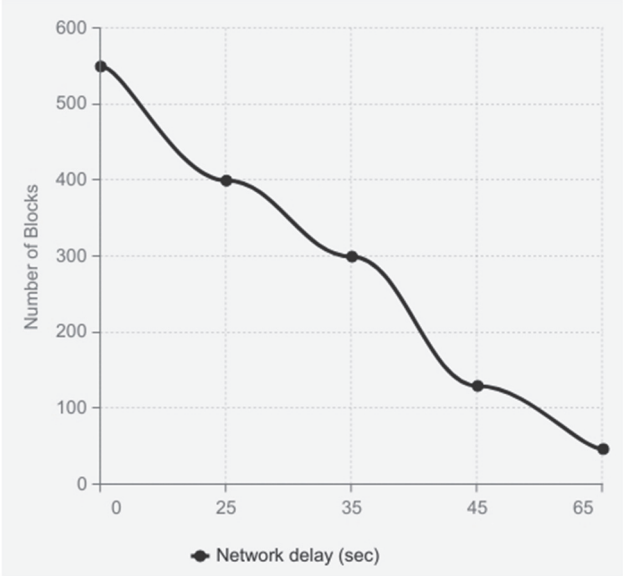

Figure 10 The effect of network delay on the number of blocks forwarded to the main chain

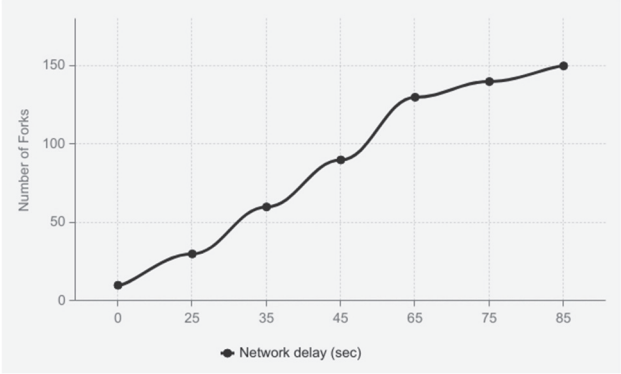

Figure 11 The effect of network delay on the number of forks

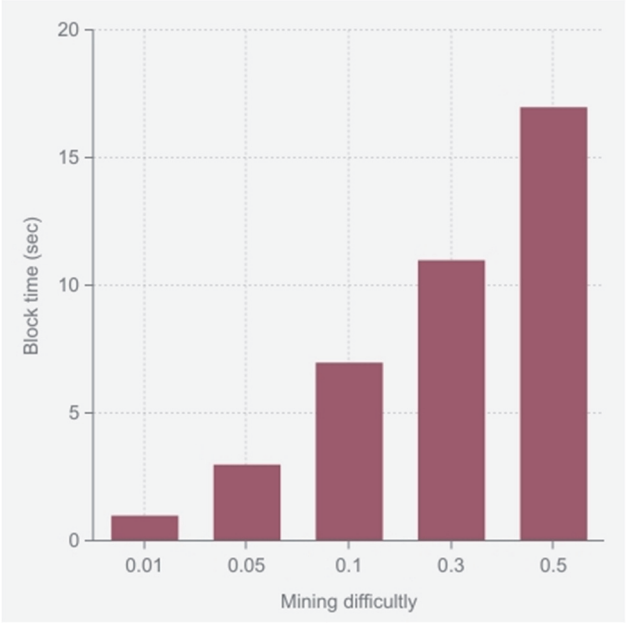

Figure 12 Impact of the incremental relationship between fork frequency and network delay

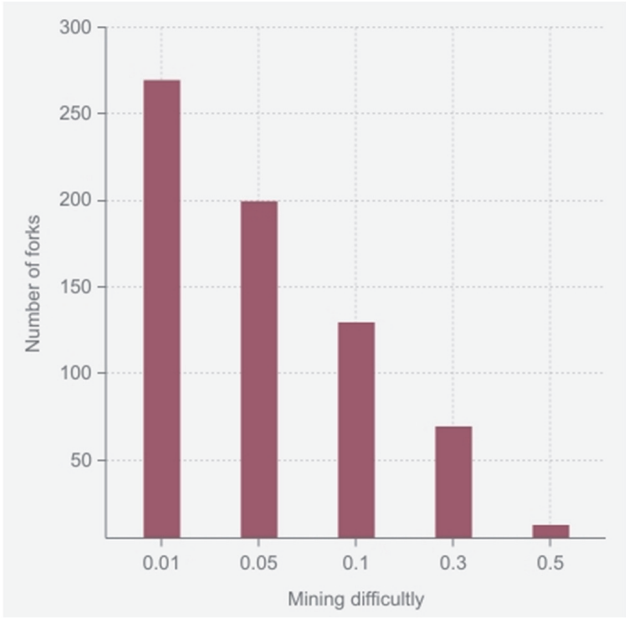

Figure 13 Impact number of forks on mining difficulty

Fig. 14 presents the times between the real network and simulation network. It can be seen that many running times are distributed between 300 ms and 800 ms, which corresponds to the lower bound of the time range, and the

real network has a larger distribution (close to the lowest value) than the simulation network, which has increasing block progressions. This is because the proposed network algorithm can concentrate more nodes on the central part of the network topology, and also appears in the range of about 200 ms to 900 ms, while the concentrated distribution appearsin the range of about 300 ms to 600 ms for the network. The area of the concentrated distribution reflects the propagation time of the blocks generated by nodes far from the centre of the network. In this case, it seems that the proposed algorithm can reduce propagation time.

Figure 14 Block propagation with different network environments

To simulate this case, we set the transaction limit to 1000 transactions for all executions. However, with each execution of the simulation, we adjusted the propagation time limit to include more transactions per block. By increasing the number of transactions per block, we were able to simulate this case in 34 minutes.

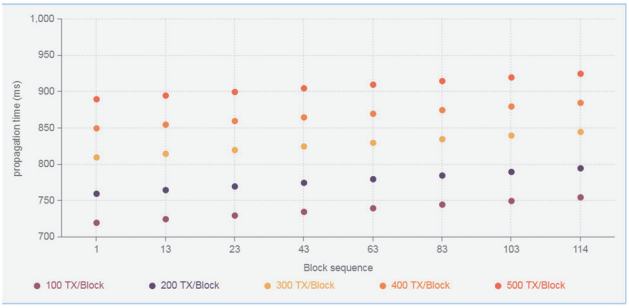

Figure 15 Block propagation for different number of transactions per block using score based on Block delivey

The results (Fig. 15) show that the number of blocks between each execution should increase by 20 KB. This increase corresponds to 100 additional transactions. Furthermore, it can be seen that the propagation time increased by about 15 ms for each execution.

8 CONCLUSIONS

When using a Blockchain and SDN architecture, there is no need for a PoW mechanism that requires solving a very complex and computationally intensive mathematical puzzle to generate a new block. A Blockchain-based SDN is vulnerable to attacks from malicious nodes that can prevent Blockchain nodes from sending or receiving block information. Security mechanisms are designed to monitor and manage traffic.

To solve this problem, our approach introduces a protection that limits attacks on data nodes and controls their reception. We expanded our experience using the Bitcoin test network and compared our work with other models. We also provided a technical description of broadcasting used to reduce data size and radio stations.

The transaction data size could be determined by determining which smaller node duplicate evidence was missing, and using radio waves and compression blocks to reduce data size. The modular architecture of the simulator also enables new features such as configurable security attacks and tag support to be deployed more easily, and failover tests can be performed without significant changes being made to the simulation framework.

Future Work

Find protocol to enable an accurate simulation of a real P2P network. Use more CPU power consumption modelling for certain cryptographic operations. Improve the SDN model by using different protocols. Increase nodes number and use different mining powers. Changing the mining difficulty and hashing power.

Acknowledgements

This work has been financially supported by the information and Communication Technology Promotion Center, funded by the South Korea government (Ministry of Science, Technology and Information) in 2018 (No. 2022-2017-0-01628, Human resource training of information and communication technology).

9 REFERENCES

[1] Alshihri, S. & Park, S. Y. (2021). 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). *Journal of Human-centric Science and Technology Innovation*, *1*(3). https://doi.org/10.21742/JHSTI.2021.1.3.08

[2] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[3] Poon, J. & Dryja, T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Retrieved from: https://lightning.network/lightning-network-paper.pdf

[4] Blockchain as a Service. Retrieved from: https://azure.microsoft.com/en-us/solutions/blockchain/

[5] Buterin, V. (2015). On public and private blockchains. Retrieved from: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[6] Hu, F., Hao, Q., & Bao, K. (2014). A survey on software-defined network (SDN) and openflow: From concept to

implementation. *IEEE Communications Surveys & Tutorials*, *16*(4), 2181-2206. https://doi.org/10.1109/COMST.2014.2326417
[7] OpenFlow Switch Specification version 1.3. Open Networking Foundation. Retrieved from: http://www.opennetworking.org/
[8] Wan, J., Li, J., Imran, M., Li, D. et al. (2019). A blockchain-based solution for enhancing security and privacy in smart factory. *IEEE Transactions on Industrial Informatics*, *15*(6), 3652-3660. https://doi.org/10.1109/TII.2019.2894573
[9] Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials*, *15*(4), 2046-2069, 2013. https://doi.org/10.1109/SURV.2013.031413.00127
[10] Guo, H. & Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: Research and Applications*, *3*(2), 100067. https://doi.org/10.1016/j.bcra.2022.100067
[11] Kraft, D. (2016). Difficulty control for blockchain-based consensus systems. *Peer-to-Peer Networking and Applications*, *9*(2), 397-413, 2016. https://doi.org/10.1007/s12083-015-0347-x
[12] Floodlight openflow controller (2017). Project Floodlight. http://www.projectfloodlight.org/floodlightFreitas
[13] Yu, M. (2019). Scalable Flow-Based Networking with DIFANE. *Proceedings of the ACM SIGCOMM 2010 conference*, 351-62. https://doi.org/10.1145/1851275.1851224
[14] Cohen, B. (2003). Incentives build robustness in BitTorrent. *1st Workshop on Economics of Peer-to-Peer systems*, *6*, 68-72.
[15] Wang, C., Shen, J., Lai, J.-F., & Liu, J. (2020). B-TSCA: blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs. *IEEE Transactions on Emerging Topics in Computing*, 1. https://doi.org/10.1109/TETC.2020.2978866
[16] Blockchain Charts - Blockchain.com. Retrieved from: https://www.blockchain.com/charts/blocks-size
[17] Bitcoin Core: Bitcoin. Retrieved from: https://bitcoincore.org
[18] Bitcoin.org. Retrieved from: https://bitcoin.org/en/full-node
[19] Ethereum.org. Retrieved from: https://ethereum.org/en/developers/docs/nodes-and-clients/run-a-node/
[20] Tran, M., Choi, I., Moon, G. J., Vu, A. V., & Kang, M. S. (2020). A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network. *2020 IEEE Symposium on Security and Privacy (SP)*, 894-909. https://doi.org/10.1109/SP40000.2020.00027
[21] Zhao, B., Liu, Y., Li, X., Li, J., & Zou, J. (2020). TrustBlock: An adaptive trust evaluation of SDN network nodes based on double-layer blockchain. *PloS One*, *15*(3), e0228844. https://doi.org/10.1371/journal.pone.0228844
[22] Hoang, H. D., Duy, P. T., & Pham, V.-H. (2019). A Security-Enhanced Monitoring System for Northbound Interface in SDN using Blockchain. *Proceedings of the Tenth International Symposium on Information and Communication Technology (SoICT 2019)*, 197-204. https://doi.org/10.1145/3368926.3369709
[23] NS3 sinulator. Retrieved from: https://www.nsnam.org/docs/tutorial/html/getting-started.html.
[24] Rohrer, E., Malliaris, J., & Tschorsch, F. (2019). Discharged payment channels: Quantifying the lightning network's resilience to topology-based attacks. *Euro S&P Workshops*, 347-356. https://doi.org/10.1109/EuroSPW.2019.00045
[25] Malavolta, G., Moreno-Sanchez, P., Schneidewind, C., Kate, A., & Maffei, M. (2019). Anonymous multi-hop locks for blockchain scalability and interoperability. *26th Annual Network and Distributed System Security Symposium (NDSS).* https://doi.org/10.14722/ndss.2019.23330

Contact information:

Saad ALSHIHRI
(Corresponding author)
Department of Computer Science & Engineering, Sogang University Seoul,
Blockchian & Software Engineering Lab,
04107, Korea
E-mail: Saaad77.sa@gmail.com

Prof. Sooyong PARK
Department of Computer Science & Engineering, Sogang University Seoul,
Blockchian & Software Engineering Lab,
04107, Korea
E-mail: sypark@sogang.ac.kr