ABSTRACT

A written contract has several weaknesses, the contract can be lost and damaged, it is not cost effective and one party can commit fraud. The solution for that is to use the smart contract Ethereum. *Smart contract* Ethereum *is a computer protocol that functions to facilitate, verify, or enforce digital negotiations written through the program code. Smart contract works without going through a third party and has a credible transaction process so that it cannot be tracked or changed. But* Blockchain *technology is not suitable for storing large amounts of data and expensive costs, so the author combines* IPFS *technology on* Ethereum Blockchain. *So the* Ethereum Blockchain *only stores the hash of the file, then the hash of this file can be connected to the file on* IPFS *to access it. In this research a web-based* DApp (*Decentralized applications*) *system was built that implemented* IPFS *on the smart contract Ethereum and used the* Network Development Life Cycle (NDLC) *method. The final result of this study is a discussion of data integrity and Quality of Service* (QoS) *communication between* IPFS *nodes on the smart contract Ethereum as a reference for implementation of the company. With the results of the implementation it was found that the data integrity possessed by* IPFS *was very good by fulfilling aspects of information security and having Quality of Service with average throughput values of 56.40 Kbps, 65.80 Kbps, and 66.31 Kbps, for average packet loss values of 1.92 %, 1.57% and 0.85%, while the average value of delay is 24.78 ms, 25.87 ms and 20.17 ms with the average value of the Quality of Service index which is 3 which satisfies the satisfying category based on* THIPON *standards.*

Keywords: Blockchain*, Smart Contract,* Ethereum*,* IPFS*, Node, Data Integrity, Quality of Service* (QoS)*.*