# ABSTRAK

Jaringan Oportunistik adalah sebuah jaringan yang dapat berjalan meskipun tidak terdapat infrastruktur pendukung. Pada Jaringan Oportunistik pesan dikirimkan dengan metode *Store-Carry-Forward*, dimana node membawa pesan dan menitipkan pesan terus tersebut kepada node lain hingga mencapai tujuan. Untuk menghargai node yang berhasil meneruskan pesan maka diberikanlah hadiah berupa insentif. Proses pemberian insentif tersebut memunculkan masalah baru yaitu kemunculan node yang saling bersekongkol untuk melakukan penipuan supaya mendapatkan insentif (*misbehaving node*) dengan cara menitipkan tanda tangan melalui node lain pada pesan transaksi agar node tersebut ikut mendapatkan insentif meskipun tidak terlibat dalam proses meneruskan pesan. Hal itu terjadi karena sebagian besar skema insentif masih mengandalkan otoritas terpusat sehingga mengakibatkan hanya ada satu pihak yang bertugas untuk mengambil keputusan dalam verifikasi dan validasi transaksi pemberian insentif tersebut mudah untuk ditipu oleh *misbehaving node*.

Maka dari itu pada penelitian kali ini penulis mengusulkan skema *Asymmetric Cryptography* untuk memverifikasi pembagian insentif berbasis Blockchain dalam mengatasi *Misbehaving Node* secara terdistribusi dibandingkan dengan sistem tanpa proses verifikasi dengan mempertimbangkan berapa rata-rata waktu yang diperlukan untuk mengirimkan pesan, persentase jumlah pesan terkirim, jumlah node yang dilewati oleh pesan, persentase Insentif yang didapat oleh Misbehaving Node dibandingkan dengan jumlah total insentif.

Kata Kunci : Asymmetric Cryptography, Proof of Authority, Blockchain.

## ABSTRACT

Opportunistic Network is a network that can run even though there is no supporting infrastructure. In an opportunistic network, messages are sent using the Store-Carry-Forward method, where nodes carry messages and leave the message directly to other nodes until they reach their destination. To reward the node that successfully forwards the message, a reward is given in the form of an incentive. The process of providing incentives raises a new problem, namely the emergence of nodes that conspire with each other to commit fraud in order to get incentives (misbehaving nodes) by entrusting their signatures through other nodes in the transaction message so that these nodes also get incentives even though they are not involved in the process of forwarding messages. This is because most of the incentive schemes still rely on a centralized authority, resulting in only one party in charge of making decisions in the verification and validation of transactions that provide incentives, which are easy to be deceived by misbehaving nodes.

Therefore, in this study the author proposes an Asymmetric Cryptography scheme to verify the distribution of Blockchain-based incentives in overcoming Misbehaving Nodes in a distributed manner compared to a system without a verification process by considering the average time required to send messages, the percentage of the number of messages sent, the number of nodes. through which the message passes, the percentage of Incentives earned by the Misbehaving Node compared to the total number of incentives.

Keywords: Asymmetric Cryptography, Proof of Authority, Blockchain.