# ABSTRACT

Saat ini penggunaan internet dalam kehidupan sehari-hari semakin meningkat sehingga pertukaran data sering dilakukan. Terutama dalam kasus transaksi bisnis, keamanan komunikasi data (seperti untuk transaksi perbankan, kontrak) diperlukan. Sony, dkk. [1] mengusulkan metode untuk mengamankan kontrak dengan menggunakan ECDSA untuk menandatangani kontrak berbasis blockchain. Namun, metode yang diusulkan oleh Sony membutuhkan kompleksitas waktu yang tinggi dan tidak tahan terhadap serangan komputer kuantum. Oleh karena itu, penelitian ini mengusulkan metode untuk mengurangi kompleksitas waktu dan juga tahan terhadap serangan komputer kuantum. Untuk mengatasi serangan kuantum dan mengurangi kompleksitas waktu penandatanganan digital berbasis blockchain, McElliece Cryptosystem dan tanda tangan digital berbasis Niederreiter diusulkan untuk menandatangani kontrak. Karena tanda tangan berbasis McElliece Cryptosystem dan Niederreiter menggunakan perkalian scalar, maka waktu pemrosesan kurang dari ECDSA. Berdasarkan hasil percobaan, terbukti bahwa waktu eksekusi untuk proses penandatanganan menggunakan metode yang diusulkan dapat mencapai hingga 51,1% lebih rendah dari pada waktu eksekusi penandatanganan metode yang diusulkan oleh Sony, dan untuk proses verifikasi hingga 77,8% kurang dari waktu eksekusi verifikasi metode yang diusulkan oleh Sony. Juga terbukti bahwa metode yang diusulkan tahan terhadap serangan kuantum.

**Kata Kunci**: McElliece Cryptosystem, Niederreiter, Tandatangan Digital, Blockchain