

Abstrak

Belakangan ini, penempatan kendaraan di area parkir menjadi masalah. Sistem parkir cerdas diusulkan untuk mengatasi masalah tersebut. Sebagian besar sistem parkir pintar memiliki sistem terpusat, di mana jenis sistem tersebut berisiko mengalami kegagalan satu titik yang dapat memengaruhi keseluruhan sistem. Untuk mengatasi kelemahan sistem terpusat, mekanisme paling populer yang diajukan peneliti adalah blockchain. Jika tidak ada mekanisme yang diterapkan pada blockchain untuk memverifikasi keaslian setiap transaksi, maka sistem tidak aman terhadap serangan peniruan identitas. Studi ini menggabungkan mekanisme blockchain dengan tanda tangan digital berbasis Ring Learning With Errors (RLWE) untuk mengamankan skema terhadap peniruan identitas dan serangan pengeluaran ganda. RLWE pertama kali diusulkan oleh Lyubashevsky et al. Skema ini merupakan pengembangan dari skema sebelumnya Learning with Error atau LWE.

Kata Kunci: Sistem Parkir Cerdas; Blockchain; Tanda Tangan Digital; Ring LWE;