

ABSTRAK

Pemungutan suara merupakan bagian terpenting dalam sistem demokrasi yang menuntut transparansi dan keadilan, namun sistem konvensional masih memiliki kelemahan seperti potensi kecurangan dan keterbatasan verifikasi hasil. Penelitian ini bertujuan merancang dan mengimplementasikan sistem *e-voting* berbasis *blockchain* menggunakan *Hyperledger Besu* dengan arsitektur berlapis yang terdiri dari layer user, aplikasi, *smart contract* dan *blockchain*. Sistem dilengkapi mekanisme keamanan seperti enkripsi *ElGamal* untuk menjaga kerahasiaan suara, *blind signature* untuk memastikan keabsahan tanpa membuka isi pilihan, serta *one-time token* untuk mencegah *double voting*. Hasil implementasi menunjukkan bahwa sistem mampu mengelola seluruh proses mulai dari autentikasi pengguna, pemrosesan surat suara, hingga penyimpanan, dan verifikasi data secara terdistribusi di jaringan *blockchain*. *Smart contract* berhasil mengatur status *voting* dan menerapkan prinsip satu pemilih satu suara, sementara konsensus QBFT memastikan validitas dan finalitas transaksi. Selain itu, fitur verifikasi suara memungkinkan pengguna memastikan suaranya telah tercatat tanpa menunjukkan isi pilihan, sehingga menjaga keseimbangan antara transparansi dan kerahasiaan. Berdasarkan pengujian, sistem ini memenuhi prinsip LUBER JURDIL (Langsung, Umum, Bebas, Rahasia, Jujur, dan Adil), sehingga berpotensi menjadi solusi alternatif dalam penyelenggaraan pemilu yang lebih aman, transparan, dan terpercaya.

Kata kunci: *e-voting, Hyperledger Besu, Blind Signature, one-time token, QBFT*

ABSTRACT

Voting is a crucial component of democratic systems that requires transparency, security, and fairness. However, conventional voting systems still face challenges such as potential fraud and limited verifiability. This study aims to design and implement a blockchain-based e-voting system using Hyperledger Besu with a layered architecture consisting of the user, application, smart contract, and blockchain layers. The system incorporates security mechanisms such as ElGamal encryption to protect vote confidentiality, blind signatures to ensure vote authenticity without revealing its content and one-time token to prevent double voting. The implementation results show that the system successfully manages the entire voting process, from user authentication, and ballot processing to secure storage and verification on the blockchain. Smart contracts effectively control voting status, and enforce the one-voter-one-vote principle, while the QBFT consensus mechanism ensures transaction validity and finality. Additionally, the vote verification feature allows users to confirm that their votes have been recorded without disclosing their choices, maintaining a balance between transparency and privacy. Based on the testing results, the system satisfies the principles of LUBER JURDIL (Langsung, Umum, Bebas, Rahasia, Jujur dan Adil), indicating its potential as a secure, transparent, and trustworthy alternative for modern electronic voting systems.

Keywords: e-voting, Hyperledger Besu, Blind Signature, one-time token, QBFT