

ABSTRACT

Diploma forgery is a serious problem in education, not only harming individuals but also tarnishing the credibility of educational institutions and eroding public trust in academic documents. Blockchain, as a distributed technology that ensures data security, transparency, and integrity, offers a potential solution to this problem. By securely storing diploma data on the blockchain, the authenticity of documents can be verified without the involvement of a third party.

However, the transparent nature of blockchain presents challenges in maintaining the confidentiality of academic data, including students' personal data. To address this, this study proposes the implementation of private smart contracts that restrict access to authorized parties, supported by the Quorum platform with Tessera to ensure privacy at the node level. A distributed application (DApp) was successfully developed based on this approach to facilitate the secure verification and management of diploma data.

Furthermore, this study also evaluates the performance of blockchain networks with Raft consensus in 4-node and 7-node configurations. Test results show that 4 nodes is the minimum usable number, achieving a throughput of 160 transactions per minute and 6–16% CPU usage, while a 7-node configuration yields 60 transactions per minute with 8–12% CPU usage. Thus, this study not only presents a private smart contract-based DApp implementation but also provides an empirical overview of the performance of blockchain networks relevant to managing college diploma data.

Keywords: Blockchain, Private Smart Contract, DApp, Personal Data Protection, Diploma, Quorum

INTISARI

Pemalsuan ijazah merupakan masalah serius dalam dunia pendidikan yang tidak hanya merugikan individu, tetapi juga mencoreng kredibilitas institusi pendidikan dan mengurangi kepercayaan masyarakat terhadap dokumen akademik. *Blockchain*, sebagai teknologi terdistribusi yang menjamin keamanan, transparansi, dan integritas data, menawarkan solusi potensial untuk mengatasi persoalan tersebut. Dengan menyimpan data ijazah secara aman di *blockchain*, keaslian dokumen dapat diverifikasi tanpa keterlibatan pihak ketiga.

Namun, sifat transparan *blockchain* menghadirkan tantangan dalam menjaga kerahasiaan data akademik, termasuk data pribadi mahasiswa. Untuk mengatasi hal tersebut, penelitian ini mengusulkan penerapan *private smart contract* yang membatasi akses hanya bagi pihak berwenang, didukung oleh *platform* Quorum dengan Tessera guna menjamin privasi pada tingkat *node*. Sebuah aplikasi terdistribusi (DApp) berhasil dikembangkan berdasarkan pendekatan ini untuk memfasilitasi verifikasi dan pengelolaan data ijazah secara aman.

Selain itu, penelitian ini juga mengevaluasi performa jaringan *blockchain* dengan konsensus Raft pada konfigurasi 4 *node* dan 7 *node*. Hasil pengujian menunjukkan bahwa 4 *node* merupakan jumlah minimum yang dapat digunakan, dengan capaian *throughput* 160 transaksi per menit dan penggunaan CPU 6–16%, sedangkan konfigurasi 7 *node* menghasilkan 60 transaksi per menit dengan penggunaan CPU 8–12%. Dengan demikian, penelitian ini tidak hanya menghadirkan implementasi DApp berbasis *private smart contract*, tetapi juga memberikan gambaran empiris mengenai kinerja jaringan *blockchain* yang relevan untuk pengelolaan data ijazah perguruan tinggi.

Kata Kunci: Blockchain, Private Smart Contract, DApp, Perlindungan Data Pribadi, Ijazah, Quorum