BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan dan integritas data memainkan peran krusial dalam era kemajuan teknologi digital, terutama dalam pengelolaan sertifikat digital yang menuntut keberadaan sistem yang tidak hanya aman tetapi juga dapat dipertanggungjawabkan. Sertifikat digital sebagai dokumen elektronik berfungsi sebagai penyimpan informasi identitas pemiliknya (Lorien & Wellem, 2021). Penelitian ini bertujuan untuk mengembangkan aplikasi verifikasi dan validasi sertifikat digital berbasis *blockchain*.

Kebijakan *Work from Home (WFH)* menyebabkan penandatanganan manual pada dokumen menjadi lebih sulit karena para pihak terlibat berada di lokasi yang berbeda. Hambatan ini muncul karena ketidakmungkinan pertemuan langsung untuk proses tanda tangan yang memunculkan kebutuhan akan solusi alternatif yang lebih praktis. Sebagai hasilnya, *digital signature* (tanda tangan digital) menjadi salah satu opsi solusi alternatif. Selain itu, meskipun *digital signature* memberikan solusi bagi penandatanganan jarak jauh, terdapat permasalahan terkait keaslian dokumen yang sudah ditandatangani. Saat ini, tidak ada jaminan yang menyakinkan terkait keaslian dan integritas dokumen yang menggunakan *digital signature* serta risiko pemalsuan atau manipulasi data yang dapat merugikan kepercayaan pengguna terhadap validitas dokumen digital (Yuniati & Sidiq, 2020).

Upaya untuk menghadapi hambatan terkait keamanan dan integritas dokumen yaitu dengan memanfaatkan teknologi *blockchain* serta tambahan algoritma *hash*. Blockchain merupakan teknologi penyimpanan data terdesentralisasi dan terdistribusi yang menggunakan kriptografi untuk mencatat transaksi dalam blok-blok yang saling terhubung secara aman (Zheng et al., 2017). *Blockchain* sebagai infrastruktur terdesentralisasi menawarkan lingkungan yang aman dan dapat diverifikasi, terutama dalam konteks manajemen dan

keamanan sertifikat digital. Algoritma hash adalah sebuah fungsi matematis yang mengonversi input data (pesan) menjadi serangkaian panjang tetap dari nilai hash, yang merupakan representasi unik dari input tersebut (Santoso et al., 2019). Penekanan pada penggunaan *digital signature* dengan memanfaatkan algoritma *hash* dan penerapan jaringan *blockchain* dapat meningkatkan keamanan untuk data yang tersimpan didalamnya.

Terdapat beberapa algoritma *hash* yang biasa digunakan dalam jaringan *blockchain*, yaitu *SHA-256, Keccak256, Blake2,* dan lain-lain. Hasil analisis perbandingan kinerja fungsi hash pada platform komputasi yang berbeda dan dengan parameter input yang berbeda, *Keccak256* menjadi salah algoritma *hash* yang memiliki kinerja yang relatif cepat (Kuznetsov et al., 2021). Penjelasan ini menciptakan dasar yang lebih kuat untuk memahami bagaimana penggunaan *blockchain* dan *digital signature* dapat mengatasi masalah keamanan dan integritas terhadap sertifikat digital.

Penelitian (Danil Muis et al., 2021) menyoroti isu pemalsuan ijazah/transkrip dalam pendidikan dan mencatat upaya Lembaga Layanan Pendidikan Tinggi dengan mengembangkan Sistem Verifikasi Ijazah Secara Online (SIVIL) dan Penomoran Ijazah Nasional (PIN). Meskipun ada langkah-langkah tersebut, sistem yang ada masih rentan terhadap serangan *SQLInjection* karena penggunaan penyimpanan terpusat. Hasil dari penelitian ini mengusulkan solusi dengan menerapkan penyimpanan terdistribusi menggunakan *InterPlanetary File System (IPFS)* untuk data dan *smart contract blockchain* untuk *hash* file ijazah/transkrip.

Penelitian (Shidqi, 2023) membahas penggunaan teknologi *blockchain* dan kriptografi dalam pembangunan *prototype* sistem pemilihan suara *e-voting* yang berfokus pada aspek keamanan. Sistem *e-voting* yang dibangun dalam penelitian ini mengutamakan transparansi, anonimitas, keandalan, kelayakan, dan verifikasi. Hasil penelitian menunjukkan bahwa penelitian ini berhasil merancang dan mengembangkan sebuah *prototype* sistem pemilihan suara *e-voting* yang

bertumpu pada keamanan dengan menggunakan teknologi *blockchain* dan kriptografi.

Penelitian (Gayathiri et al., 2020) bertujuan untuk mengatasi kesulitan mahasiswa dalam menjaga sertifikat pendidikan yang telah didigitalisasi di institusi pendidikan, khususnya sertifikat SSLC, HSC, dan akademis. Verifikasi dan validasi sertifikat oleh organisasi dan institusi dianggap sebagai tugas yang sulit. Solusi yang diusulkan melibatkan penyimpanan sertifikat dalam sistem *blockchain*, mengonversi sertifikat kertas menjadi bentuk digital dengan algoritma kriptografi, dan menyediakan validasi melalui aplikasi seluler. Penelitian ini bertujuan meningkatkan keamanan dan efisiensi proses validasi sertifikat digital dengan menerapkan teknologi *blockchain*. Hasil dari penelitian ini menyoroti kontribusi *blockchain* dalam mengurangi pemalsuan sertifikat dengan memanfaatkan sifat tak terbantahkan, serta memudahkan manajemen sertifikat digital bagi individu dengan aplikasi yang memberikan jaminan atas akurasi dan keamanan informasi.

Penelitian (Frikha et al., 2021) mengusulkan pendekatan baru berbasis arsitektur *hybrid HW/SW (Hardware/Software)* untuk meningkatkan kinerja aplikasi *Internet of Things (IoT)* dengan menggunakan teknologi *blockchain*. Penelitian ini bertujuan untuk mengatasi beberapa tantangan yang dihadapi dalam aplikasi blockchain *IoT*, seperti konsumsi daya dan waktu eksekusi. Hasil yang dicapai dari penelitian ini mencakup pengembangan arsitektur *hybrid HW/SW* yang didesain untuk konsensus *PoW (Proof of Work)* serta validasi implementasinya menggunakan *blockchain Ethereum* dengan *Keccak256* dan kit pengembangan *Field-Programmable Gate Array (FPGA) ZedBoard*. Implementasi ini berhasil menunjukkan peningkatan signifikan dalam waktu eksekusi dan pengurangan konsumsi daya dibandingkan dengan penggunaan *Nvidia Maxwell GPUs.*

Hasil dari penelitian sebelumnya, dapat ditegaskan bahwa keamanan dan integritas dokumen memiliki peranan yang sangat penting. Menurut penelitian sebelumnya, penggunaan *digital signature* dan jaringan *blockchain* terbukti

efektif dalam meningkatkan keamanan dan integritas dokumen digital. Implementasi algoritma hash *Keccak256* juga menunjukan peningkatan dalam waktu eksekusi yang relatif cepat. Penerapan *digital signature* dan algoritma hash *Keccak256* kedalam jaringan *blockchain* pada sertifikat digital akan menjadi fokus utama pada penelitian ini. Tujuan utama dari penelitian ini adalah untuk meningkatkan keamanan serta mempertahankan integritas sertifikat digital.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, rumusan masalah pada penelitian ini adalah:

1. Bagaimana merancang arsitektur sistem untuk verifikasi dan validasi sertifikat digital menggunakan teknologi *blockchain*?
2. Bagaimana mengimplementasikan *digital signature* dan algoritma *hash Keccak256* kedalam jaringan *blockchain* sehingga dapat meningkatkan keamanan dan integritas sertifikat digital?

1.3 Batasan Masalah

Penelitian ini terdapat beberapa batasan yang menjadi fokus untuk mempersempit ruang lingkup dan mengarahkan perhatian pada aspek-aspek tertentu, maka batasan masalah dalam penelitian ini yaitu sebagai berikut:

1. Arsitektur sistem ini bersifat *web-based* dan terfokus pada sertifikat digital dengan format pdf.
2. Metode kriptografis yang digunakan pada penelitian ini untuk memberikan otentikasi dan integritas yaitu *digital signature*.
3. Algoritma hash yang digunakan pada penelitian ini yaitu *Keccak256.*
4. Metode pengembangan sistem yang diterapkan pada penelitian ini adalah *Rapid Application Development (RAD).*
5. Pengembangan sistem pada penelitian ini memanfaatkan teknologi *MySQL* sebagai database, *ReactJS* sebagai *frontend*, *Laravel* sebagai *backend*, dan *Web3js* sebagai penghubung ke jaringan *Ethereum.*

6. Dompet digital yang dipergunakan untuk menyimpan *cryptocurrency Ether* adalah *Metamask Extension* pada peramban *Chrome*.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai pada penelitian ini adalah sebagai berikut:

1. Merancang arsitektur sistem untuk verifikasi dan validasi sertifikat digital menggunakan teknologi *blockchain*.
2. Mengimplementasikan *digital signature* dan algoritma hash *Keccak256* kedalam jaringan *blockchain* sehingga dapat meningkatkan keamanan dan integritas sertifikat digital.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah peningkatan pengetahuan dan pemahaman mahasiswa terkait metode dan teori yang digunakan dalam penelitian ini. Selain itu, diharapkan hasil penelitian ini memberikan referensi untuk penelitian selanjutnya yang tertarik untuk menyelidiki aspek-aspek terkait teknologi *blockchain* khususnya pada bidang *digital signature*.