

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era digital saat ini, kredibilitas dokumen akademik semakin rentan terhadap praktik pemalsuan yang terorganisir, seperti yang terlihat pada kasus sindikat ijazah palsu di Universitas Negeri Semarang (UNNES) yang melibatkan jaringan pemasaran dan pencetakan ilegal [1]. Fenomena ini diperparah oleh ketergantungan pada sistem verifikasi konvensional yang bersifat manual, padat karya, dan sangat bergantung pada inspeksi fisik yang rentan terhadap kesalahan manusia (*human error*) [2]. Padahal, penggunaan teknologi kriptografi melalui nilai hash unik (SHA-256) sebagai identitas digital dapat memberikan akurasi hingga 100% dalam mendeteksi manipulasi dokumen [2]. Tanpa mekanisme validasi yang cepat dan independen, kepercayaan publik terhadap legalitas kualifikasi profesional akan terus tergerus oleh kecanggihan teknik duplikasi fisik [3].

Sistem verifikasi saat ini sebagian besar masih bergantung pada otoritas pusat (*Identity Provider*) yang memiliki kelemahan kritis berupa *Single Point of Failure* (SPOF), di mana kegagalan pada satu titik utama dapat melumpuhkan seluruh layanan [3]. Risiko ini terbukti nyata dalam serangan *ransomware* LockBit 3.0 Brain Cipher terhadap Pusat Data Nasional Sementara (PDNS) 2 di Surabaya pada Juni 2024, yang diawali dengan penonaktifan paksa fitur keamanan Windows Defender [4]. Insiden tersebut mengakibatkan lumpuhnya 282 layanan instansi pemerintah karena minimnya cadangan data hanya sekitar 2% data yang tercadangkan di *Cold Storage* Batam sehingga proses pemulihan menjadi tidak mungkin dilakukan secara instan [4]. Ketergantungan penuh pada server tunggal ini menciptakan hambatan birokrasi dan risiko keamanan yang sangat tinggi bagi data sensitif pengguna [2], [3].

Sebagai solusi alternatif, teknologi *blockchain* menawarkan buku besar terdistribusi yang bersifat *immutable* (tidak dapat diubah) dan transparan untuk menjamin integritas data tanpa bergantung pada pihak tunggal [3], [5]. Dengan

mengintegrasikan *InterPlanetary File System* (IPFS), dokumen akademik tidak disimpan langsung di *blockchain* yang mahal, melainkan dibagi menjadi fragmen terdesentralisasi yang memiliki *Content Identification* (CID) unik [5]. Lebih lanjut, konsep *Soulbound Token* (SBT) memperkenalkan identitas digital yang *non-transferable* (tidak dapat dipindahtangankan), yang sangat ideal untuk merepresentasikan kredensial akademik dan reputasi seseorang dalam ekosistem *Decentralized Society* (DeSoc) [6]. SBT memungkinkan institusi untuk memberikan atestasi permanen yang mencerminkan hubungan sosial dan komitmen nyata, bukan sekadar aset finansial yang dapat diperjualbelikan [6].

Hingga saat ini, belum banyak sistem atau aplikasi praktis yang mengimplementasikan *Blockchain* dan *Soulbound Token* untuk menyelesaikan permasalahan-permasalahan yang telah disebutkan. Oleh karena itu, penelitian ini mengusulkan pengembangan Velipe, sebuah sistem verifikasi dokumen yang memanfaatkan jaringan *Base Sepolia Layer 2* untuk mengatasi keterbatasan skalabilitas *blockchain* utama. Penggunaan *Layer 2* sangat krusial karena mampu meningkatkan kapasitas transaksi dari 15–30 *Transactions per Second* (TPS) menjadi 1000–4000 TPS, sehingga menekan biaya operasional secara signifikan [3]. Velipe menerapkan modifikasi standar *ERC-721* menjadi SBT untuk ijazah guna memastikan permanensi identitas, sementara penyimpanan *hash* dokumen secara *off-chain* tetap menjaga privasi pengguna [3], [6]. Dengan optimalisasi infrastruktur ini, sistem diharapkan memiliki skalabilitas tinggi (*high throughput*) dalam menangani lonjakan permintaan verifikasi secara bersamaan, memberikan solusi verifikasi yang tidak hanya aman secara kriptografi tetapi juga efisien untuk penggunaan skala besar [2].

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka dapat ditarik rumusan masalah sebagai berikut:

1. Bagaimana merancang dan membangun arsitektur sistem verifikasi dokumen digital berbasis *Blockchain* dan IPFS yang mampu mendeteksi perubahan data (*tamper-evident*) dan mendukung verifikasi independen?

2. Bagaimana mengimplementasikan *Smart Contract Hybrid ERC-721* untuk membedakan dokumen yang bersifat permanen (*Soulbound*) dan dokumen yang dapat dipindahtangankan, serta mencegah duplikasi dan pemindahtanganan tidak sah?

1.3 Batasan Masalah

1. Sistem dibangun sebagai aplikasi terdesentralisasi berbasis web (dApp), dengan *Next.js* sebagai *framework* antarmuka pengguna.
2. Jaringan *blockchain* yang digunakan adalah *Base Sepolia (testnet)*, sehingga seluruh pengujian bersifat simulatif dan tidak melibatkan aset kripto bernilai nyata.
3. Penyimpanan metadata dokumen dilakukan melalui layanan *gateway* IPFS, dengan *Pinata* digunakan sebagai contoh implementasi.
4. Sistem tidak menyimpan dokumen asli dalam bentuk berkas di *blockchain* maupun IPFS. Sebagai gantinya, sistem menyimpan nilai hash kriptografi (*SHA-256*) dan metadata pendukung, dengan asumsi bahwa perubahan sekecil apa pun pada dokumen akan menghasilkan nilai *hash* yang berbeda.
5. *Soulbound Token* pada penelitian ini diimplementasikan sebagai token *non-transferable*, di mana token tidak dapat dipindahtangankan oleh pemilik. Sebagai pengecualian, penerbit dokumen resmi (*Verified Issuer*) diberikan hak untuk memindahtangankan token kepada alamat dompet lain sebagai mekanisme pemulihan (*recovery*), misalnya dalam kondisi pemilik kehilangan akses terhadap dompet digitalnya. Selain itu, penerbit tetap memiliki kewenangan untuk mencabut (*revoke*) dokumen sebagai mekanisme koreksi atau pembatalan. Mekanisme transfer oleh pihak selain penerbit resmi akan ditolak secara mutlak oleh *smart contract*.
6. Penelitian ini tidak membahas aspek legalitas atau kekuatan hukum dokumen digital yang dihasilkan dan hanya difokuskan pada aspek teknis dan keamanan sistem.
7. Analisis keamanan dalam penelitian ini dibatasi pada pencegahan duplikasi dokumen (*re-mint*) dan pengulangan transaksi (*replay attack*), tanpa mencakup analisis kriptografi lanjutan atau audit keamanan menyeluruh.

8. Sistem diuji dalam skala terbatas dan tidak membahas performa pada penggunaan skala besar atau lingkungan produksi.
9. Validitas otoritas penerbitan dokumen bergantung sepenuhnya pada partisipasi institusi resmi dalam mendaftarkan alamat dompet digital mereka ke dalam kontrak pintar *Issuer Registry*.
10. Untuk dokumen yang diterbitkan secara mandiri oleh pengguna (*self-minting*) atau penerbit yang belum terverifikasi, sistem hanya menjamin integritas data digital (bahwa berkas tidak berubah sejak diunggah) dan tidak memvalidasi kebenaran materiil isi dokumen tersebut.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian adalah menghasilkan aplikasi verifikasi dokumen terdesentralisasi yang mampu:

1. Merancang dan membangun arsitektur sistem verifikasi dokumen digital berbasis *Blockchain* dan *IPFS* yang terbukti mampu mencegah perubahan data (*tamper-resistance*) serta mendukung verifikasi independen oleh pihak ketiga.
2. Mengimplementasikan *Smart Contract Hybrid ERC-721* untuk membedakan perlakuan antara dokumen yang bersifat permanen (*Soulbound*) dan dokumen yang dapat dipindahtangankan, sekaligus mencegah terjadinya duplikasi (*re-mint*) dan pemindahtanganan tidak sah.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik secara teoritis maupun praktis sebagai berikut:

1. **Manfaat Teoritis:** Memberikan kontribusi referensi akademis terkait implementasi *Smart Contract Hybrid ERC-721* dalam sistem verifikasi dokumen digital berbasis *blockchain*, serta pemanfaatan arsitektur penyimpanan terdesentralisasi berbasis *hash* untuk menjaga integritas dokumen.

2. Manfaat Praktis:

- a. **Bagi Institusi Pendidikan:** Menyediakan prototipe sistem penerbitan ijazah digital yang mendukung verifikasi keaslian dan keterlacakan dokumen secara digital.
- b. **Bagi Industri/Perekrut:** Membantu pihak industri atau perekrut dalam melakukan verifikasi keaslian dokumen pendukung pelamar kerja secara mandiri dan terstruktur.
- c. **Bagi Masyarakat:** Memberikan alternatif mekanisme kepemilikan dokumen digital berbasis *blockchain* yang tidak bergantung pada satu server pusat.

1.6 Sistematika Penulisan

Sistematika penulisan dalam laporan skripsi ini disusun sebagai berikut:

BAB I PENDAHULUAN Berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA Memuat studi literatur dari penelitian terdahulu yang relevan serta dasar teori yang digunakan, meliputi *Blockchain*, *Ethereum*, *Smart Contract*, *IPFS*, Standar *ERC-721*, dan *Next.js*.

BAB III METODE PENELITIAN Menjelaskan objek penelitian, alur penelitian (termasuk perancangan sistem dan arsitektur *smart contract*), serta alat dan bahan yang digunakan dalam pengembangan sistem.

BAB IV HASIL DAN PEMBAHASAN Menguraikan hasil implementasi sistem *Velipe*, mulai dari *deployment smart contract*, integrasi antarmuka, hingga pengujian fungsionalitas fitur penerbitan dan verifikasi dokumen.

BAB V PENUTUP Berisi kesimpulan yang diperoleh dari hasil penelitian serta saran untuk pengembangan sistem selanjutnya.