

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil implementasi dan serangkaian pengujian sistem Velipe yang telah dipaparkan pada Bab IV, kesimpulan dari penelitian ini dapat menjawab tujuan penelitian yang telah ditetapkan pada Bab I:

1. Tujuan 1 (Arsitektur, Tamper-Resistance, & Verifikasi Independen)

Sistem verifikasi dokumen digital berbasis *blockchain* dan IPFS telah berhasil dirancang dan dibangun menggunakan arsitektur tiga lapisan (*Client*, *Storage* dan *Blockchain Layer*). Penggunaan algoritma *SHA-256* sebagai sidik jari digital terbukti mutlak mampu mencegah manipulasi data (*tamper-resistance*), di mana perubahan sekecil satu bit pun pada berkas PDF akan memicu penolakan validasi (*avalanche effect*). Selain itu, sistem ini sukses mendukung proses verifikasi independen oleh pihak ketiga; karena seluruh hash dokumen tercatat secara *on-chain* di jaringan *Base Sepolia*, publik dapat memvalidasi keaslian dokumen langsung melalui *BaseScan Explorer* tanpa harus bergantung pada portal web Velipe (*vendor-lock free*).

2. Tujuan 2 (Smart Contract Hybrid, SBT, & Pencegahan Duplikasi)

Implementasi *Smart Contract Hybrid ERC-721* telah berhasil membedakan perlakuan dua jenis dokumen secara dinamis di dalam satu *smart contract*. Dokumen identitas akademik dikunci sebagai SBT yang *non-transferable* untuk mencegah pemindahtanganan yang tidak sah, sementara aset digital umum dicetak sebagai NFT standar yang bersifat *transferable*. Sistem juga terbukti efektif mencegah terjadinya duplikasi (*re-mint*) dokumen melalui validasi fungsi pemetaan *hashToToken* secara *on-chain*. Lebih lanjut, pemisahan otoritas antara *Verified Issuer* dan pengguna publik berhasil dikelola secara otomatis menggunakan

IssuerRegistry, meminimalisir intervensi manual dalam penerbitan dokumen resmi.

5.2 Saran

Berdasarkan keterbatasan yang ditemukan selama proses penelitian dan implementasi sistem Velipe, terdapat beberapa rekomendasi konstruktif yang dapat dijadikan landasan untuk pengembangan dan penelitian di masa mendatang:

1. Transisi ke Lingkungan Produksi dan Pengujian Skalabilitas (*Stress Testing*)

Pengujian sistem dalam penelitian ini masih berskala terbatas pada lingkungan simulasi (*Base Sepolia Testnet*). Penelitian selanjutnya disarankan untuk melakukan *deployment* pada jaringan utama (*Base Mainnet*) yang sesungguhnya. Selain itu, perlu dilakukan pengujian beban (*stress testing*) dengan volume transaksi yang masif untuk memvalidasi tingkat skalabilitas dan keandalan sistem dalam skenario produksi nyata.

2. Desentralisasi Penuh pada Lapisan Tata Kelola (*Governance*)

Mekanisme pengelolaan *Verified Issuer* saat ini masih bergantung pada satu entitas terpusat, yaitu *Admin* pemegang *Contract Owner*. Guna meminimalisir risiko sentralisasi, pengembangan sistem ke depan direkomendasikan untuk mengadopsi mekanisme *Decentralized Autonomous Organization* (DAO). Penggunaan *multi-signature wallet* atau pemungutan suara berbasis *on-chain* dapat diimplementasikan agar keputusan registrasi institusi dikelola secara transparan dan terdesentralisasi.

3. Peningkatan Kemandirian Infrastruktur Penyimpanan *Metadata*

Sistem saat ini memanfaatkan layanan *gateway* IPFS pihak ketiga (Pinata) untuk mempertahankan persistensi *metadata* dokumen. Agar ketersediaan data tidak bergantung secara sepihak pada layanan

komersial, penelitian berikutnya disarankan untuk mengintegrasikan protokol penyimpanan permanen yang lebih tangguh (seperti *Filecoin* atau *Arweave*), atau dengan membangun infrastruktur *node* IPFS mandiri secara *self-hosted*.

4. Pengembangan Portofolio Digital Terintegrasi bagi Penerima Dokumen

Antarmuka sistem saat ini difokuskan pada kemudahan penerbitan (*issuer*) dan verifikasi (*verifier*). Untuk meningkatkan nilai tambah aplikasi (*user experience*), disarankan penambahan fitur *dashboard* atau dompet portofolio khusus bagi penerima dokumen. Fitur ini akan memungkinkan pemilik ijazah atau sertifikat untuk melihat, mengelola, serta membagikan bukti kredensial akademik mereka secara langsung melalui platform Velipe.

5. Audit Keamanan Smart Contract secara Ekstensif

Meskipun pengujian dalam penelitian ini telah memvalidasi fungsionalitas logika *hybrid* dan resistensi duplikasi, aspek keamanan belum mencakup seluruh spektrum kerentanan blockchain. Sebelum sistem ini diimplementasikan secara komersial, sangat disarankan untuk melakukan audit keamanan *smart contract* yang lebih komprehensif, mencakup mitigasi terhadap serangan kompleks seperti *reentrancy attack*, *front-running*, dan celah eksploitasi lainnya melalui metode audit otomatis maupun lembaga audit pihak ketiga