BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam beberapa tahun terakhir, perkembangan teknologi *blockchain* dan aset kripto menunjukkan peningkatan signifikan dan menjadi salah satu inovasi yang berpengaruh dalam ekosistem keuangan digital. *Bitcoin* sebagai aset kripto pertama memperkenalkan mekanisme transaksi *peer-to-peer* yang memanfaatkan tanda tangan digital dan pencatatan transaksi berbasis rantai blok untuk mencegah *double spending* [1]. Karakteristik tersebut menjadikan *blockchain* relevan sebagai teknologi pencatatan yang sulit dimanipulasi dan dapat diverifikasi secara publik.

Meskipun demikian, penggunaan aset kripto memiliki tantangan mendasar pada aspek keamanan, khususnya pengelolaan kunci privat (*private key*). Secara konseptual, kepemilikan aset kripto ditentukan oleh kemampuan pengguna untuk membuktikan otorisasi melalui tanda tangan kriptografis atas transaksi, sehingga kompromi atau kehilangan *private key* berpotensi menyebabkan kehilangan akses aset secara permanen [1]. Oleh karena itu, praktik pengamanan kunci privat dan proses otorisasi transaksi menjadi fokus penting dalam pengembangan sistem yang mengelola aset kripto.

Salah satu pendekatan yang umum digunakan untuk meningkatkan keamanan operasional adalah *custodian*, yaitu layanan yang menyediakan mekanisme penyimpanan dan pengelolaan aset digital dengan memusatkan pengendalian operasional pada sistem yang diaudit dan dikontrol. Dalam konteks implementasi teknis, peningkatan keamanan juga dapat dilakukan melalui penggunaan *multisignature* (*multisig*) yang mensyaratkan lebih dari satu tanda tangan untuk mengotorisasi transaksi, sehingga mengurangi risiko apabila satu kunci privat terekspos [2]. Standarisasi transaksi yang mendukung skrip kompleks (termasuk *multisig*) pada ekosistem *Bitcoin* juga ditopang oleh mekanisme *Pay-to-Script-Hash* (*P2SH*) [3].

Selain tantangan pengamanan kunci privat, sistem aplikasi modern yang memproses data finansial juga menghadapi risiko pada lapisan penyimpanan data. Pada banyak aplikasi, informasi sensitif seperti nilai transaksi, biaya, atau status persetujuan dapat tersimpan di basis data terpusat. Apabila terjadi kompromi akses basis data, data tersebut berpotensi dimanipulasi pada level

aplikasi tanpa kontrol kriptografis *end-to-end*. Oleh karena itu, dibutuhkan pendekatan yang meminimalkan penyimpanan data finansial sensitif di basis data dan memaksimalkan mekanisme verifikasi kriptografis. Pada implementasi berbasis *Bitcoin*, sebagian data kritikal dapat direkonsiliasi melalui pencatatan transaksi di *blockchain* yang sifatnya dapat diverifikasi secara publik [1].

Dalam pengelolaan kunci dan alamat, sistem juga memerlukan metode yang terstandarisasi agar aman serta mudah dikelola. Standar *Hierarchical Deterministic Wallet* (*HD Wallet*) menjelaskan mekanisme turunan kunci dan alamat secara hirarkis sehingga sistem dapat menghasilkan banyak alamat dari satu *seed* utama [4]. Untuk mempermudah pengelolaan *seed* oleh manusia, standar *mnemonic* menyediakan representasi kata-kata yang dapat dikonversi menjadi *seed* biner untuk kebutuhan *HD Wallet* [5].

Pada proses pembuatan dan penandatanganan transaksi, sistem *custodian* memerlukan mekanisme yang mendukung kolaborasi penandatangan tanpa membocorkan kunci privat. Format *Partially Signed Bitcoin Transaction* (*PSBT*) didefinisikan sebagai standar pertukaran data transaksi yang memungkinkan beberapa pihak menandatangani transaksi secara bertahap [6]. Untuk kebutuhan pengujian yang aman tanpa melibatkan aset *Bitcoin* sebenarnya, jaringan *Bitcoin* menyediakan *Testnet* sebagai jaringan alternatif untuk eksperimen dan validasi fungsionalitas [7].

PT Mitra Integrasi Digital sebagai perusahaan teknologi yang bergerak dalam pengembangan solusi digital menjadi konteks pelaksanaan kerja magang pada proyek ini [8]. Dalam proyek *Bitcoin Custodian*, sistem dirancang untuk mendukung penyimpanan dan pengiriman *Bitcoin* secara aman, termasuk fitur *multisig*, *HD wallet*, pemantauan saldo, dan kontrol akses berbasis peran. Penerapan *Role-Based Access Control* (*RBAC*) digunakan untuk memastikan bahwa akses pengguna terhadap sumber daya sistem dibatasi sesuai perannya, sejalan dengan konsep *RBAC* yang dibahas dan distandardisasi pada konteks sistem informasi [9].

Pada sisi autentikasi aplikasi *web*, mekanisme token banyak digunakan untuk mengelola sesi secara aman. *JSON Web Token* (*JWT*) merupakan standar token ringkas yang digunakan untuk membawa klaim identitas secara *URL-safe* dan dapat ditandatangani secara kriptografis [10]. Di sisi penyimpanan kredensial, *password* seharusnya tidak disimpan dalam bentuk asli, melainkan menggunakan fungsi *password hashing* yang adaptif terhadap peningkatan daya komputasi; salah satu pendekatan yang dikenal luas adalah *bcrypt* [11]. Selain itu, transmisi data

antara klien dan *server* perlu diamankan menggunakan *TLS*/*HTTPS* untuk menjaga kerahasiaan dan integritas komunikasi [12].

Berdasarkan latar belakang tersebut, pengembangan sistem *Bitcoin Custodian* pada proyek magang ini menjadi relevan karena memadukan prinsip keamanan kriptografi, standar pengelolaan kunci, serta praktik keamanan aplikasi *web* untuk membangun layanan pengelolaan aset kripto yang lebih terstruktur dan dapat dipertanggungjawabkan.

1.2 Maksud dan Tujuan Kerja Magang

Pelaksanaan kerja magang bertujuan untuk menyanggupi salah satu ketentuan akademik pada Program Studi Informatika, Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara. Selain itu, kerja magang memberikan kesempatan bagi mahasiswa untuk memperoleh pengalaman langsung dalam lingkungan kerja profesional serta mengimplementasikan kompetensi pengembangan perangkat lunak pada proyek nyata di industri.

Secara khusus, kerja magang ini dilaksanakan di PT Mitra Integrasi Digital [8] dengan fokus utama pada perancangan dan pengembangan sistem *Bitcoin Custodian*. Tujuan teknis dari pengembangan sistem ini meliputi: membangun mekanisme pengelolaan *wallet* berbasis *HD Wallet* [4, 5], menerapkan transaksi *multisig* untuk memperkuat kontrol otorisasi [2, 3], mendukung alur penandatanganan bertahap melalui *PSBT* [6], serta mengintegrasikan praktik keamanan aplikasi *web* melalui autentikasi token, *hashing password*, dan komunikasi aman [10, 11, 12].

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Pelaksanaan kerja magang di PT Mitra Integrasi Digital berlangsung selama tiga bulan, dimulai pada tanggal 18 Agustus 2025 dan masih berjalan hingga saat ini [8]. Program magang ini diselenggarakan untuk memenuhi ketentuan Universitas Multimedia Nusantara terkait pemenuhan minimal 640 jam kerja. Sistem kerja magang di perusahaan menerapkan mekanisme kontrak yang dibuktikan melalui *letter of acceptance*, sehingga peserta tetap diwajibkan menyelesaikan periode magang sesuai perjanjian.

Selama masa magang, penulis ditempatkan sebagai *Junior Developer* dengan sistem kerja *full work from home* (*WFH*) mengikuti jam operasional

perusahaan dari pukul 09.00 hingga 17.00 WIB. Dalam struktur organisasi, penulis berada di bawah supervisi pembimbing lapangan serta memperoleh arahan terkait aspek keamanan dan arsitektur sistem.

Fokus utama proyek selama magang adalah pengembangan sistem *Bitcoin Custodian* yang mencakup integrasi dengan *Bitcoin Testnet* untuk kebutuhan pengujian [7], implementasi proses transaksi dan penandatanganan, serta penerapan kontrol akses berbasis peran [9]. Seluruh aktivitas pengembangan dilakukan secara iteratif dan terstruktur agar selaras dengan standar kualitas dan praktik industri.