BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam beberapa tahun terakhir, perdagangan melalui e-commerce di Indonesia telah berkembang pesat. Transaksi online telah menjadi bagian penting dari perekonomian digital, memudahkan konsumen dan penjual untuk melakukan jual beli tanpa batasan fisik [1]. Namun, di balik kemudahan dan efisiensi yang ditawarkan, terdapat risiko signifikan yang mengintai, yaitu penipuan digital. Berdasarkan riset nasional, ditemukan bahwa 66,6% responden di Indonesia pernah menjadi korban penipuan digital, khususnya dalam jual beli online. Modus penipuan yang sering digunakan termasuk penipuan berkedok hadiah (36,9%), pengiriman tautan atau link berisi malware (33,8%), serta jual beli palsu (29,4%) [2]. Kasus-kasus ini tidak hanya menyebabkan kerugian finansial bagi korban tetapi juga merusak kepercayaan masyarakat terhadap keamanan transaksi digital.

Seiring berkembangnya tren e-commerce, inovasi signifikan lainnya yang muncul adalah penggunaan cryptocurrency sebagai alat transaksi digital [3]. Cryptocurrency menawarkan efisiensi, kecepatan, serta peluang investasi yang menarik. Laporan dari Badan Pengawas Perdagangan Berjangka Komoditi (BAPPEBTI) menunjukkan bahwa nilai transaksi kripto di Indonesia mencapai Rp 211 triliun hingga April 2024, dengan prediksi peningkatan hingga Rp 800 triliun pada akhir tahun tersebut [4] [5]. Namun, penggunaan cryptocurrency dalam transaksi digital juga tidak lepas dari risiko penipuan. Di tingkat global, kerugian akibat penipuan dalam transaksi kripto meningkat dari 2,57 miliar dolar AS pada tahun 2022 menjadi 3,94 miliar dolar AS pada tahun 2023, atau sekitar 53% [6]. Salah satu kasus penipuan yang terjadi adalah kasus penipuan yang menimpa seorang penjual Bitcoin di platform Coinbase, dengan kerugian mencapai Rp 1,1 triliun. Penipuan ini menggunakan metode address poisoning, di mana pelaku mengelabui korban untuk mengirimkan aset kripto ke alamat yang salah melalui taktik phishing. Akibat penipuan ini, korban kehilangan 97% dari asetnya yang tersimpan di platform kripto [6]. Kasus ini terungkap oleh perusahaan keamanan blockchain, CertiK, yang mendeteksi transfer sebesar 69,3 juta dolar AS ke alamat palsu, dan sebagian besar Bitcoin curian kemudian ditukarkan dengan Ethereum. Jenis kasus penipuan berbasis transaksi kripto ini tidak hanya menimbulkan kerugian finansial bagi para

pengguna tetapi juga menimbulkan keraguan terhadap keamanan ekosistem kripto dan teknologi blockchain secara keseluruhan. Lalu, bagaimana cara agar pengguna dapat merasa aman bertransaksi kripto sehingga terhindar dari kasus penipuan tersebut.

Pertanyaan ini menjadi tantangan besar bagi PT Tennet Depository Indonesia, sebuah kustodian aset kripto yang memiliki visi untuk menjadi pilihan utama sebagai penjaga aset kripto yang terpercaya di Indonesia [7]. Sebagai kustodian, Perusahaan ini berkomitmen untuk memberikan perlindungan dan keamanan yang optimal bagi aset digital *client*-nya. Namun, saat ini perusahaan belum memiliki sistem yang memadai untuk memenuhi permintaan *client* yang membutuhkan layanan keamanan ekstra dalam transaksi kripto. Banyak *client* yang meminta agar perusahaan dapat menyediakan sistem atau mekanisme yang dapat menjamin keamanan transaksi mereka akibat banyaknya kasus penipuan yang terjadi dalam transaksi kripto.

Untuk mengatasi masalah ini, salah satu solusi yang paling tepat adalah dengan merancang dan mengimplementasikan sistem *escrow* berbasis *Xcrow*. Sistem ini memungkinkan pihak ketiga yang terpercaya memegang dana dari pembeli sementara sampai syarat tertentu terpenuhi. Syarat tersebut terpenuhin apabila barang atau aset kripto telah diserahkan sesuai kesepakatan bersama [8]. *Escrow* menjamin keamanan transaksi dengan meminimalisir risiko penipuan, baik bagi pembeli maupun penjual. Dengan demikian, PT Tennet Depository Indonesia dapat memenuhi kebutuhan *client* mereka.

1.2 Dasar Teori

Blockchain adalah teknologi yang memungkinkan penyimpanan dan pencatatan transaksi secara terdesentralisasi, aman, dan transparan [9]. Sistem ini bekerja dengan cara mengelompokkan transaksi dalam blok yang kemudian disusun dalam urutan yang saling terhubung sehingga membentuk sebuah rantai. Oleh karena itu, istilah ”blockchain” berasal dari dua kata, yaitu ”block” (blok) dan ”chain” (rantai) yang menggambarkan struktur data yang terdiri dari serangkaian blok yang saling terhubung. Setiap blok berisi data transaksi yang diverifikasi oleh peserta jaringan melalui mekanisme konsensus, seperti Proof of Work (PoW) atau Proof of Stake (PoS). Setiap blok tidak hanya menyimpan informasi transaksi, tetapi juga mencantumkan hash dari blok sebelumnya. Hash adalah hasil dari fungsi kriptografi yang mengubah data menjadi string alfanumerik unik yang berfungsi untuk

memastikan integritas data dalam blok tersebut. Dengan adanya previous hash yang menghubungkan setiap blok, perubahan pada satu blok akan memengaruhi seluruh rantai blok dikarenakan hash yang terhubung akan menjadi tidak valid [9]. Dengan demikian, hal ini membuat data di dalam teknologi blockchain bersifat sangat aman dan tidak mudah diubah.

Jika seseorang mencoba mengubah data dalam satu blok, maka hash dari blok tersebut akan berubah, yang akan merusak hubungan dengan blok-blok berikutnya. Untuk memodifikasi seluruh rantai, seorang penyerang harus mengubah hash di setiap blok dalam jaringan, yang hampir mustahil dilakukan karena blockchain beroperasi dalam jaringan yang terdesentralisasi, di mana data tersimpan di banyak komputer (node) secara bersamaan [9]. Dengan struktur ini, blockchain menjamin transparansi dan keamanan karena setiap transaksi yang tercatat di dalamnya dapat diverifikasi oleh semua anggota jaringan tanpa memerlukan pihak ketiga, serta tidak dapat dimanipulasi setelah dicatat. Oleh karena itu, blockchain menjadi teknologi yang sangat menarik untuk berbagai aplikasi, termasuk cryptocurrency, smart contracts, dan banyak lagi [9].

Dalam sistem blockchain, public key dan private key adalah dua komponen kriptografi yang sangat penting untuk menjaga keamanan transaksi digital [10]. Public key berfungsi sebagai alamat yang digunakan untuk menerima aset digital, mirip dengan nomor rekening bank yang dapat dibagikan kepada siapa saja. Public key ini memungkinkan pihak lain untuk mengirimkan transaksi, namun tidak dapat digunakan untuk mengubah atau mengakses aset yang diterima. Sebaliknya, private key adalah kunci rahasia yang hanya diketahui oleh pemiliknya dan digunakan untuk menandatangani transaksi, memberikan otorisasi untuk memindahkan atau membelanjakan aset yang terkait dengan public key tersebut. Dikarenakan private key memberi kontrol penuh atas aset digital, pengguna perlu menjaga kerahasiaannya. Dengan kata lain, kehilangan private key berarti kehilangan akses ke aset tersebut. Dengan demikian, sistem public key dan private key dalam blockchain menciptakan lapisan keamanan yang memungkinkan transaksi yang aman dan terverifikasi, tanpa perlu bergantung pada pihak ketiga atau otoritas terpusat [10].

Jaringan Polygon adalah salah satu jenis jaringan blockchain yang digunakan dan atau didukung oleh aplikasi ini. Jaringan ini merupakan solusi Layer 2 yang dibangun di atas blockchain utama seperti Ethereum. Selanjutnya, jaringan ini menawarkan biaya transaksi yang lebih rendah berkat penggunaan teknologi sidechains dan Plasma [11]. Dengan sidechains, transaksi diproses di luar jaringan utama Ethereum, mengurangi beban dan kepadatan, serta meningkatkan efisiensi.

Selain itu, Polygon mengadopsi mekanisme konsensus Proof of Stake (PoS) yang lebih hemat energi dan efisien dibandingkan Proof of Work (PoW), sehingga mempercepat proses validasi transaksi dan menurunkan biaya. Polygon juga merupakan public blockchain yang artinya siapa saja bisa bergabung, memverifikasi transaksi, dan mengakses data secara terbuka. Jaringan ini bersifat publik karena jaringan dikelola oleh komunitas tanpa otoritas pusat yang memastikan desentralisasi dan transparansi tinggi. Oleh karena itu, jaringan ini dijadikan sebagai pilihan ideal untuk mengembangkan aplikasi ini. [11].

1.3 Maksud dan Tujuan Kerja Magang

Maksud dari kerja magang ini adalah untuk mendalami tantangan dalam transaksi kripto di sektor *e-commerce* Indonesia, terutama terkait keamanan. Dengan pertumbuhan *cryptocurrency* sebagai alat pembayaran dan investasi, risiko penipuan meningkat. PT Tennet Depository Indonesia berinisiatif mengembangkan sistem *escrow* berbasis *Xcrow* guna meningkatkan keamanan transaksi kripto.

Tujuan magang ini adalah merancang dan mengimplementasikan sistem *escrow* yang dapat melindungi pengguna, meminimalkan risiko penipuan, serta meningkatkan kepercayaan publik terhadap *cryptocurrency*. Selain itu, magang ini bertujuan untuk mengembangkan keterampilan teknis dan analitis, sambil mendukung pertumbuhan industri kripto yang lebih aman dan transparan.

1.4 Waktu dan Prosedur Pelaksanaan Kerja Magang

Kerja magang akan dilaksanakan selama 4 bulan, dimulai dari tanggal 5 Agustus 2024 hingga 5 Desember 2024. Pelaksanaan magang ini akan dilakukan secara *Work From Office (WFO)*. Hari dan jam kerja adalah lima hari dalam seminggu, yaitu setiap Senin hingga Jumat, dari pukul 08:00 hingga 17:00 WIB.