BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah memberikan dampak besar terhadap sistem keuangan global, termasuk sistem pembayaran digital di Indonesia. Menurut laporan Bank Indonesia (2023), terdapat pertumbuhan signifikan sebesar 25,5% dalam transaksi uang elektronik dibandingkan tahun sebelumnya. Fenomena ini menunjukkan bahwa masyarakat Indonesia semakin terbiasa dengan penggunaan dompet digital seperti DANA, OVO, dan GoPay sebagai alat pembayaran sehari-hari [1].

Namun, seiring dengan meningkatnya transaksi digital, muncul pula risiko keamanan yang mengancam kepercayaan publik, seperti pencurian data pribadi, pemalsuan identitas, dan manipulasi transaksi [3]. Kasus kebocoran data pada platform e-commerce besar serta meningkatnya serangan phishing dan social engineering menunjukkan adanya celah yang harus segera ditangani dengan pendekatan teknologi yang tepat [2].

Blockchain sebagai teknologi desentralisasi menjanjikan solusi transparansi dan imutabilitas dalam pencatatan transaksi. Setiap transaksi yang dicatat dalam blockchain tidak dapat diubah dan dapat diverifikasi oleh semua pihak dalam jaringan [4]. Dalam konteks ini, algoritma tanda tangan digital memainkan peran kunci untuk memastikan bahwa transaksi benar-benar dikirim oleh pemilik sah [5].

Salah satu algoritma yang umum digunakan dalam blockchain adalah Elliptic Curve Digital Signature Algorithm (ECDSA). ECDSA menawarkan efisiensi kriptografi tinggi dengan ukuran kunci yang kecil namun tetap aman, menjadikannya sangat cocok untuk sistem yang membutuhkan validasi cepat dan skalabilitas tinggi seperti sistem pembayaran digital [6].

Meskipun banyak digunakan secara global di platform seperti Bitcoin dan Ethereum, kajian mengenai potensi dan tantangan implementasi ECDSA dalam konteks lokal Indonesia masih terbatas. Oleh karena itu, penelitian ini berupaya mengisi celah tersebut dengan pendekatan akademik dan simulasi teknis berbasis Python untuk mendeskripsikan proses kerja sistem pembayaran berbasis blockchain yang menggunakan ECDSA [10].

1.2 Rumusan Masalah

Permasalahan yang akan dibahas dalam penelitian ini adalah bagaimana prinsip kerja algoritma ECDSA dalam sistem blockchain serta mengkaji keunggulan ECDSA dibandingkan algoritma

tanda tangan digital lainnya dan apa saja potensi dan tantangan penerapan ECDSA dalam sistem pembayaran digital di Indonesia

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk Mengkaji prinsip kerja dan mekanisme ECDSA dalam blockchain serta menganalisis keunggulan ECDSA dari aspek keamanan dan efisiensi dan menjelaskan potensi dan tantangan penerapan ECDSA dalam konteks sistem pembayaran digital Indonesia.

1.4 Manfaat Penelitian

Manfaat yang di harapkan dari penelitian ini adalah sebagai berikut :

1. Memberikan pemahaman akademis mengenai algoritma ECDSA dalam sistem blockchain.
2. Menjadi referensi untuk pengembangan sistem pembayaran digital yang lebih aman di Indonesia.
3. Mendukung literatur ilmiah dalam bidang keamanan sistem informasi dan teknologi finansial.

1.5 Batasan Masalah

Penelitian ini bersifat akademis dan tidak mencakup pengujian sistem nyata secara teknis atau performa pada jaringan blockchain publik. Simulasi yang dilakukan bertujuan untuk menjelaskan prinsip kerja ECDSA dan implementasi konseptual dalam skenario sistem pembayaran digital. Fokus terbatas pada proses registrasi, tanda tangan digital, validasi transaksi, dan pencatatan ke blockchain dalam konteks ilustrasi fiktif berbasis Python, tanpa menguji interoperabilitas dengan sistem eksternal seperti Dukcapil atau BI-FAST.