BAB I PENDAHULUAN

1.1 Latar Belakang

Dalam beberapa tahun terakhir, ekosistem cryptocurrency mengalami perkembangan yang sangat pesat seiring dengan meningkatnya adopsi teknologi blockchain dan minat masyarakat terhadap aset digital. Cryptocurrency tidak hanya digunakan sebagai instrumen investasi, tetapi juga mulai dimanfaatkan dalam berbagai aktivitas ekonomi digital. Namun, pertumbuhan tersebut juga diikuti dengan meningkatnya berbagai bentuk kejahatan siber dan penipuan digital yang menargetkan investor kripto. Modus penipuan yang sering terjadi antara lain rug pull, phishing wallet, penerbitan token palsu, hingga manipulasi informasi proyek melalui dokumen whitepaper yang tidak valid atau menyesatkan.

Berdasarkan laporan Federal Bureau of Investigation melalui Internet Crime Complaint Center (IC3) tahun 2024, kerugian akibat penipuan investasi berbasis cryptocurrency mencapai lebih dari 6,5 miliar dolar AS dan menjadi salah satu kategori kejahatan siber dengan tingkat kerugian terbesar. Selain itu, laporan Chainalysis dalam Crypto Crime Report 2024 juga menunjukkan bahwa aktivitas penipuan berbasis aset kripto masih terus meningkat dan menyebabkan kerugian hingga miliaran dolar AS setiap tahunnya. Kondisi tersebut diperkuat oleh penelitian yang dilakukan oleh Josh Kamps dan Bennett Kleinberg yang menjelaskan bahwa manipulasi informasi pada proyek cryptocurrency sering dimanfaatkan dalam skema pump-and-dump untuk menarik perhatian investor dan memengaruhi keputusan investasi korban. Selain itu, penelitian mengenai implementasi tanda tangan digital oleh Yusmaniar Lubis, Ibnu Rusydi, dan Ananda Hadi Elyas menjelaskan bahwa dokumen digital sangat rentan terhadap manipulasi dan pemalsuan apabila tidak dilengkapi dengan mekanisme autentikasi yang memadai. Penelitian tersebut menerapkan tanda tangan digital untuk menjaga integritas dan keaslian dokumen. Hasil penelitian menunjukkan bahwa penerapan tanda tangan digital mampu membantu proses verifikasi dokumen dan mengurangi risiko pemalsuan informasi. Hal ini menunjukkan bahwa keaslian dan keamanan informasi dalam proyek cryptocurrency menjadi aspek yang sangat penting, terutama karena masih banyak investor yang mengalami kesulitan dalam membedakan proyek asli dan proyek palsu.

Whitepaper sebagai dokumen utama yang menjelaskan konsep, tujuan, teknologi, serta mekanisme suatu proyek kripto sering dimanfaatkan oleh pelaku kejahatan untuk membangun

kepercayaan palsu. Dalam praktiknya, penipuan berbasis whitepaper umumnya dilakukan melalui beberapa tahapan. Pertama, pelaku membuat dokumen whitepaper yang terlihat profesional dengan meniru struktur proyek yang kredibel, bahkan dalam beberapa kasus menyalin sebagian isi dari proyek yang sudah ada. Kedua, pelaku memodifikasi informasi penting seperti roadmap, tokenomics, serta identitas tim pengembang untuk menciptakan kesan legitimasi. Ketiga, whitepaper tersebut disebarkan melalui website, media sosial, atau platform komunitas kripto untuk menarik minat investor. Setelah dana terkumpul, pelaku kemudian melakukan rug pull dengan menarik seluruh likuiditas atau meninggalkan proyek tanpa kejelasan. Kondisi ini menunjukkan bahwa whitepaper sering dijadikan alat utama dalam membangun kepercayaan semu terhadap proyek palsu.

Salah satu sumber utama dari permasalahan tersebut adalah sulitnya melakukan verifikasi keaslian proyek kripto secara cepat, aman, dan transparan. Banyak proyek belum menyediakan mekanisme teknis yang mampu menjamin bahwa whitepaper, smart contract, maupun identitas tim pengembang benar-benar otentik dan tidak mengalami perubahan. Di sisi lain, sebagian besar investor masih mengandalkan tampilan visual dan isi dokumen tanpa adanya proses verifikasi kriptografis. Celah inilah yang kemudian dimanfaatkan oleh pihak tidak bertanggung jawab untuk menyebarkan proyek palsu dan melakukan penipuan terhadap investor.

Sebagai solusi, penerapan tanda tangan digital (digital signature) menjadi salah satu pendekatan yang relevan untuk meningkatkan keamanan dokumen proyek cryptocurrency. Dengan menggunakan tanda tangan digital, dokumen dapat ditandatangani menggunakan private key resmi milik pengembang, sehingga pihak lain dapat memverifikasi keaslian dokumen tersebut menggunakan public key yang dipublikasikan. Metode ini tidak hanya mampu menjaga integritas data (data integrity), tetapi juga memberikan autentikasi (authentication) dan non-repudiation terhadap dokumen digital. Menurut Joseph Bonneau dkk. (2015), tanda tangan digital merupakan salah satu komponen fundamental dalam sistem blockchain yang berfungsi untuk memastikan keaslian data dan mencegah manipulasi oleh pihak yang tidak sah.

Salah satu algoritma tanda tangan digital yang paling banyak digunakan dalam ekosistem blockchain adalah Elliptic Curve Digital Signature Algorithm (ECDSA). Algoritma ini digunakan pada jaringan besar seperti Bitcoin dan Ethereum karena mampu memberikan tingkat keamanan tinggi dengan ukuran kunci yang relatif kecil serta efisiensi komputasi yang lebih baik dibandingkan algoritma klasik seperti RSA. Meskipun demikian, ECDSA tetap memiliki beberapa

potensi risiko, terutama apabila nilai acak (nonce) tidak dikelola dengan baik atau terjadi kebocoran informasi melalui serangan side-channel, yang dapat menyebabkan kompromi terhadap private key.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis penerapan algoritma ECDSA sebagai solusi teknis dalam memverifikasi keaslian dokumen whitepaper proyek cryptocurrency. Penelitian ini juga akan mengevaluasi efektivitas proses penandatanganan dan verifikasi terhadap dokumen PDF, serta mengkaji kemampuan metode tersebut dalam mendeteksi adanya manipulasi dokumen. Dengan pendekatan ini, diharapkan penelitian dapat memberikan kontribusi dalam meningkatkan keamanan dokumen digital, membantu investor melakukan verifikasi keaslian proyek kripto, serta mengurangi potensi penipuan berbasis dokumen digital di ekosistem cryptocurrency.

1.2 Rumusan masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah:

a. Bagaimana proses digital *signature* menggunakan algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) dapat diterapkan untuk menjamin keaslian dan integritas dokumen *whitepaper* proyek *cryptocurrency*?
b. Bagaimana implementasi digital *signature* berbasis ECDSA dapat digunakan untuk menjamin keaslian dan integritas dokumen *whitepaper*?
c. Apakah sistem yang dibangun dapat mendeteksi perubahan isi dokumen melalui proses validasi tanda tangan digital?

1.3 Tujuan

Tujuan dari penelitian ini adalah:

a. Menganalisis cara kerja algoritma Elliptic Curve Digital Signature Algorithm (ECDSA) dalam proses penandatanganan dan verifikasi digital dokumen whitepaper.
b. Membangun sistem eksperimental yang mampu menghasilkan tanda tangan digital dari dokumen whitepaper dan memverifikasinya menggunakan ECDSA.
c. Menguji keakuratan sistem dalam mendeteksi keaslian dokumen berdasarkan validitas tanda tangan digital.
d. Menyajikan hasil validasi dokumen dalam bentuk informasi visual dan status keaslian, serta mengevaluasi fungsi sistem secara fungsional.

1.4 Manfaat

Manfaat yang diharapkan dari penelitian ini antara lain:

a. Bagi akademisi: Menjadi referensi ilmiah dalam studi keamanan digital signature dan penerapannya pada verifikasi dokumen berbasis blockchain.
b. Bagi pengembang proyek kripto: Menyediakan acuan teknis dalam penerapan tanda tangan digital yang aman dan dapat diverifikasi untuk whitepaper.
c. Bagi investor dan masyarakat umum: Meningkatkan kesadaran terhadap pentingnya otentikasi dokumen kripto untuk menghindari penipuan dan proyek palsu.
d. Bagi pengembang sistem keamanan dan AI: Memberikan wawasan mengenai penerapan algoritma kriptografi (ECDSA) dalam sistem validasi otomatis berbasis machine learning atau AI.