

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi telah mengalami kemajuan yang sangat pesat di berbagai aspek kehidupan (Yoga Nugraha et al., 2024). Salah satu buah dari kemajuan ini adalah munculnya era digital, yang ditandai dengan kehadiran *cryptocurrency*, yaitu mata uang digital yang berbasis pada teknologi kriptografi (Astoni Nurdin et al., 2020). Terdapat dua *cryptocurrency* besar, yaitu *bitcoin* dan *ethereum* yang mendominasi era mata uang digital (Warsito & Robiyanto, 2020). *Bitcoin* sebagai pelopor telah menarik banyak perhatian dari pelaku pasar (Febri Pramudya Wardani & Audrey Gamaliel Dotulong Tangkudung, 2024). Namun, *Ethereum* membawa dimensi baru dalam perkembangan mata uang *crypto* (Andini Widi Baharani et al., 2024). *Ethereum* juga merupakan salah satu *cryptocurrency* yang populer menurut (Timothy Bastian Sianturi et al., 2023). Berdasarkan data dari Ethereum.Org (2024) *Ethereum* memiliki 4.000+ proyek, 96 juta akun, 53 juta *smart contract*, dan 18 juta transaksi harian. *Ethereum* memiliki jenis mata uang digital yang umum dikenal sebagai *ether* (ETH) (Haruli Dwicaksana & Pujiyono, 2020). *Ether* juga berfungsi sebagai instrumen investasi, dengan tingginya permintaan mendorong kenaikan signifikan pada harga asset (Gunawan & Febrianti, 2023). Sedangkan menurut Rut Arta Pangaribuan et al. (2023), *Ethereum* bukan hanya berperan sebagai instrumen investasi, tetapi bisa juga digunakan untuk pembayaran dan menawarkan fasilitas layanan keuangan, *game*, serta aplikasi.

Menurut Nurul Huda & Risman Hambali (2020), meskipun investasi di *Ethereum* menawarkan kemudahan, terdapat risiko seperti volatilitas harga, penipuan, kejahatan siber, dan risiko teknologi. Dengan sifat desentralisasi dan anonimitas *Ethereum* membuat tidak ada otoritas atau institusi yang bertanggung jawab atas pengelolaan *blockchain*, sehingga sulit mengidentifikasi pihak yang bertanggung jawab dalam kasus penipuan (Hassan et al., 2021). Salah satu bentuk penipuan yang terkenal dalam dunia *Ethereum* adalah skema *Ponzi* (Chen et al., 2019). Antara tahun 2015 hingga 2017, teridentifikasi 191 *ponzi* yang memanfaatkan *smart contract* di *Ethereum*. Hal ini menyebabkan kerugian hingga \$500.000 yang dialami lebih dari 2000 pengguna (Bartoletti et al., 2020).

Untuk mengatasi masalah yang ada, beberapa penelitian telah menerapkan berbagai pengklasifikasi dan metode untuk mendeteksi penipuan di *Ethereum*. Penelitian oleh Farrugia et al. (2020) memanfaatkan algoritma *XGBoost* bersama dengan prosedur validasi silang, berhasil mendeteksi akun berbahaya dalam transaksi *Ethereum* dengan tingkat *accuracy* sebesar 96,3%. Sementara itu, Yuan et al. (2020) mengembangkan model algoritma *support vector machine* (SVM) untuk mengidentifikasi penipuan *phishing* di bursa *Ethereum* dengan tingkat *accuracy* absolut 84,6%. Penelitian terbaru oleh Aziz et al. (2022) menggunakan delapan model algoritma untuk mendeteksi aktivitas penipuan yang berdasarkan pada kelainan dalam data transaksi *Ethereum*. Transaksi yang menyimpang dari norma dianggap sebagai anomali atau mencurigakan. Kemudian diperoleh salah satu algoritma yaitu *Light Gradient Boosting Machine* (LGBM), yang menunjukkan nilai *accuracy* terbesar di bandingkan yang lainnya, yaitu 99,03% (Aziz et al., 2022).

Selain pada lingkungan *Ethereum*, algoritma yang akan digunakan dalam penelitian ini juga telah berhasil diterapkan di bidang lain. Penelitian oleh Raihan Kemmy Rachmansyah & Ria Astriratma (2023) menggunakan algoritma *Extra Trees* untuk klasifikasi cuaca di Provinsi DKI Jakarta dan memperoleh *accuracy* tertinggi sebesar 79,8%. Selanjutnya, Kurniawan et al. (2024) menerapkan algoritma *Gaussian Naïve Bayes* untuk klasifikasi status gizi pada balita dan menghasilkan *accuracy* sebesar 87,42%. Adapun penelitian oleh Pahlevi et al. (2024) menggunakan algoritma *CatBoost* untuk klasifikasi risiko stunting Pada Balita dan mencatat *accuracy* tinggi sebesar 98,47%.

Berdasarkan penelitian-penelitian sebelumnya, berbagai algoritma *machine learning* telah digunakan untuk mendeteksi penipuan pada transaksi *Ethereum*, dengan *LightGBM* menunjukkan *accuracy* terbaik mencapai 99,03%. Pada penelitian ini akan digunakan *dataset* yang serupa dengan penelitian tersebut, namun akan mengevaluasi algoritma yang berbeda, yaitu *LightGBM*, *Extra Trees*, *Support Vector Machine* (SVM), *Gaussian Naïve Bayes*, dan *CatBoost*. Hal ini dilakukan karena beberapa algoritma tersebut belum digunakan dalam penelitian dengan topik yang sama. Dengan demikian, diharapkan algoritma yang dipilih mampu bersaing atau bahkan melampaui *accuracy LightGBM*.

1.2 Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana cara implementasi dan membandingkan algoritma *LightGBM*, *Extra Trees*, *Support Vector Machine* (SVM), *Gaussian Naïve Bayes* dan *CatBoost* pada *dataset Ethereum* untuk mendeteksi aktivitas penipuan?
2. Bagaimana Hasil Evaluasi algoritma *LightGBM*, *Extra Trees*, *Support Vector Machine* (SVM), *Gaussian Naïve Bayes* serta *CatBoost* dalam mendeteksi penipuan di jaringan *Ethereum*?

1.3 Tujuan Penelitian

Tujuan penelitian dalam penelitian ini adalah sebagai berikut:

1. Mengimplementasikan serta membandingkan algoritma *LightGBM*, *Extra Trees*, *Support Vector Machine* (SVM), *Gaussian Naïve Bayes* dan *CatBoost* pada *dataset Ethereum* untuk mendeteksi aktivitas penipuan.
2. Menganalisis dan mengevaluasi kinerja setiap algoritma dalam mendeteksi aktivitas penipuan di jaringan *Ethereum*, untuk menentukan algoritma yang memiliki performa terbaik.

1.4 Manfaat

Manfaat dalam penelitian adalah sebagai berikut:

1. Bagi Mahasiswa: Penelitian ini memberikan manfaat dalam memahami bagaimana algoritma *machine learning* dapat diterapkan untuk mendeteksi penipuan di jaringan *blockchain Ethereum*. Melalui penelitian ini, mahasiswa berkesempatan untuk mengasah keterampilan analisis data, menerapkan berbagai algoritma, serta mengoptimalkan model *machine learning*, yang akan sangat bermanfaat dalam pengembangan penelitian di masa mendatang.
2. Bagi Universitas: Penelitian ini memperkaya penelitian akademik tentang *blockchain* dan *machine learning*, serta memperkuat reputasi universitas sebagai lembaga yang mendorong inovasi teknologi. Temuan ini juga dapat menjadi referensi berguna bagi mahasiswa lain dalam pengembangan aplikasi *machine learning* berbasis *blockchain*.

3. Bagi Investor: Penelitian ini memberikan wawasan berharga bagi para investor mengenai efektivitas algoritma *machine learning* dalam mendeteksi aktivitas penipuan di jaringan *Ethereum*. Informasi tersebut dapat memberikan bantuan bagi investor dalam mengambil keputusan investasi yang lebih aman serta mendukung pengembangan sistem deteksi penipuan yang lebih handal untuk melindungi aset digital dari tindakan ilegal.

