E-ISSN: 2964-6219, P-ISSN: 2964-6200
Volume 5 Number 1 February 2027.
pp: 18-28. DOI: https://doi.org/10.58477/cj.v5i1.514.

Computer Journal

RESEARCH ARTICLE Open Access

Model *Explainable Machine Learning* untuk Deteksi Anomali Transaksi *Blockchain* Bitcoin Menggunakan Analisis SHAP

Muhammad Ibnu Fauzan [1*]

[1*] Program Studi Ilmu Komputer (S2), Fakultas Teknologi Informasi, Universitas Nusa Mandiri, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta, Indonesia.

Correspondence email:
fauzanibnu87@gmail.com.

Article History
Received: 7 September 2026.
Revised: 10 September 2026.
Accepted: 19 October 2026.
Available Online: 5 November 2026
Published: 1 February 2027.

Funding Information
Universitas Nusa Mandiri.

Abstract
The growing volume of Bitcoin transactions requires anomaly detection mechanisms that are both accurate and explainable, as high-performing classifiers often lack decision traceability for auditors and security analysts. This study develops an explainable machine learning approach for Bitcoin transaction anomaly detection by comparing Logistic Regression, Random Forest, and Extreme Gradient Boosting (XGBoost), followed by SHapley Additive exPlanations (SHAP) interpretation on the best model. Using the Elliptic Bitcoin Dataset, preprocessing included feature-label merging, removing unknown labels, binary target conversion, selecting 165 numerical features, MinMaxScaler normalization, and an 80:20 stratified train-test split, retaining 14,253 labeled transactions: 13,380 licit (93.88%) and 873 illicit (6.12%). Evaluation based on accuracy, precision, recall, F1-score, ROC-AUC, confusion matrix, and training time showed that XGBoost achieved the best performance with 0.9961 accuracy, 1.0000 precision, 0.9371 recall, 0.9676 F1-score, and 0.9960 ROC-AUC, yielding 2,676 true negatives, zero false positives, 164 true positives, and 11 false negatives. Transaction-level SHAP analysis revealed how individual feature contributions shifted predictions toward the licit or illicit class, demonstrating that integrating XGBoost and SHAP delivers accurate anomaly detection with transparent decision support for blockchain investigations.

Keywords: Bitcoin; Anomaly Detection; XGBoost; Explainable Artificial Intelligence; SHAP.

Abstrak
Peningkatan volume transaksi Bitcoin menuntut mekanisme deteksi anomali yang akurat sekaligus dapat dijelaskan, mengingat keputusan model klasifikasi berperforma tinggi sering sulit ditelusuri oleh auditor dan analis keamanan. Penelitian ini mengembangkan pendekatan *explainable machine learning* untuk mendeteksi anomali transaksi Bitcoin dengan membandingkan Logistic Regression, Random Forest, dan Extreme Gradient Boosting (XGBoost), serta menginterpretasikan model terbaik menggunakan SHapley Additive exPlanations (SHAP). Melalui tahapan penggabungan fitur dan label pada Elliptic Bitcoin Dataset, penghapusan kelas *unknown*, konversi label biner, pemilihan 165 fitur numerik, normalisasi MinMaxScaler, dan *stratified train-test split* 80:20, diperoleh 14.253 transaksi berlabel yang terdiri atas 13.380 transaksi *licit* (93,88%) dan 873 transaksi *illicit* (6,12%). Evaluasi berdasarkan *accuracy*, *precision*, *recall*, *F1-score*, ROC-AUC, *confusion matrix*, dan waktu pelatihan menunjukkan bahwa XGBoost memberikan kinerja terbaik dengan *accuracy* 0,9961, *precision* 1,0000, *recall* 0,9371, *F1-score* 0,9676, dan ROC-AUC 0,9960, dengan 2.676 prediksi *licit* benar, tanpa *false positive*, 164 transaksi *illicit* terdeteksi benar, dan 11 transaksi *illicit* terlewat. Analisis SHAP pada tingkat transaksi memperlihatkan arah kontribusi fitur menuju kelas *licit* atau *illicit*, yang membuktikan bahwa integrasi XGBoost dan SHAP menghasilkan deteksi anomali berkinerja tinggi sekaligus transparan untuk mendukung investigasi *blockchain*.

Kata Kunci: Bitcoin; Deteksi Anomali; XGBoost; Kecerdasan Buatan; SHAP.

© The Author(s) 2027. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

1. Pendahuluan

Blockchain menyediakan mekanisme pencatatan transaksi terdistribusi yang memungkinkan data disimpan dan diverifikasi tanpa otoritas pusat. Pada ekosistem Bitcoin, transaksi tercatat pada *ledger* publik dan pengguna direpresentasikan melalui identitas pseudonim. Karakteristik ini menciptakan dua konsekuensi sekaligus: riwayat transaksi menyediakan jejak digital yang dapat dimanfaatkan untuk analisis forensik, tetapi pseudonimitas dan kemudahan transfer lintas batas juga rentan disalahgunakan untuk aktivitas pencucian uang, penipuan, *ransomware*, serta pergerakan dana ilegal (Asiri & Somasundaram, 2025; Pocher *et al*., 2023). Seiring dengan peningkatan skala jaringan, identifikasi transaksi mencurigakan secara manual menjadi semakin tidak realistis karena transaksi Bitcoin tidak hanya bertambah dalam jumlah, tetapi juga saling terhubung melalui aliran dana antaralamat dan antartransaksi. Pola ilegal dapat muncul sebagai transaksi tunggal yang tidak wajar, perilaku kontekstual yang menyimpang dari riwayat sebelumnya, maupun rangkaian transaksi kolektif yang secara individual tampak normal tetapi membentuk pola mencurigakan. Kondisi tersebut mendorong penggunaan metode komputasional yang mampu mempelajari pola historis dan menggeneralisasikan pengetahuan tersebut terhadap transaksi baru. Dalam konteks penelitian di Indonesia, pemanfaatan *machine learning* pada aset kripto telah berkembang dari prediksi harga berbasis RNN dan LSTM hingga klasifikasi arah harga dengan Random Forest serta perbandingan berbagai algoritma pada *cryptocurrency* (Hung *et al*., 2023; Julianto, 2022; Khoiri & Wahid, 2024; Rizkilloh & Widiyanesti, 2022). Meskipun fokus studi-studi tersebut bukan pada deteksi transaksi *illicit*, hasilnya menunjukkan bahwa karakteristik data kripto dapat dipelajari menggunakan beragam model *machine learning* untuk mendukung pengembangan analitik keamanan transaksi yang lebih spesifik.

Pendekatan *machine learning* terawasi (*supervised learning*) menyediakan kerangka yang sesuai untuk tugas tersebut dengan mempelajari hubungan antara fitur transaksi dan label kelas sehingga transaksi baru dapat dipetakan ke kategori *licit* atau *illicit*. Dalam ranah ini, Elliptic Bitcoin Dataset telah menjadi salah satu *benchmark* penting untuk penelitian *anti-money laundering* (AML) karena menyediakan graf transaksi Bitcoin berlabel yang dapat dianalisis baik melalui fitur tabular maupun struktur graf (Alarab & Prakoonwit, 2023; Asiri & Somasundaram, 2025). Perkembangan riset deteksi transaksi mencurigakan pada dataset dan ekosistem serupa juga bergerak ke arah pemanfaatan relasi graf, dimensi temporal, serta forensik keuangan. Alarab dan Prakoonwit (2023) mengeksplorasi pemodelan temporal berbasis graf, sedangkan Pocher *et al*. (2023) menempatkan *machine learning-based forensics* dalam kerangka AML/*Combating the Financing of Terrorism* (CFT) untuk mendeteksi transaksi *cryptocurrency* yang anomali. Selanjutnya, Hasan *et al*. (2024) menggabungkan *tree-based classifiers*, penanganan ketidakseimbangan kelas, dan SHAP untuk deteksi anomali transaksi Bitcoin, sementara Liang *et al*. (2025) mengembangkan pendekatan *data-driven* yang fleksibel untuk AML pada jaringan Bitcoin. Arah penelitian tersebut menunjukkan bahwa pemodelan yang semakin kompleks dapat memperkaya informasi relasional, tetapi pada saat yang sama memperbesar kebutuhan terhadap penanganan ketimpangan kelas (*class imbalance*) mengingat dominasi kelas *licit*, sekaligus menuntut kejelasan interpretasi keputusan model agar evaluasi tidak hanya bertumpu pada *accuracy*.

Meskipun model yang kompleks mampu meningkatkan akurasi, performa prediktif tidak selalu sejalan dengan kemudahan interpretasi. Algoritma seperti Random Forest dan XGBoost dapat menangkap relasi nonlinier serta interaksi banyak fitur, tetapi keputusan akhirnya merupakan agregasi dari sejumlah pohon keputusan sehingga sulit ditelusuri secara intuitif. Keterbatasan ini berdampak langsung pada domain finansial dan keamanan karena prediksi anomali dapat berimplikasi pada investigasi lanjutan, pembatasan transaksi, atau proses audit. Oleh sebab itu, *Explainable Artificial Intelligence* (XAI) dikembangkan untuk menjembatani kebutuhan antara performa dan transparansi, terutama ketika model prediktif digunakan pada pengambilan keputusan berisiko tinggi (Ali *et al*., 2023), sebagaimana tercermin pula pada berbagai penelitian nasional yang menerapkan LIME maupun SHAP untuk meningkatkan keterlacakan model klasifikasi dan prediksi (Iffadah *et al*., 2025; Kurniyanto & Hartoyo, 2023; Sari *et al*., 2024; Sibagariang, 2025; Syamkalla *et al*., 2024). Salah satu pendekatan XAI yang banyak digunakan adalah SHapley Additive exPlanations (SHAP), yang memandang setiap fitur sebagai kontributor terhadap keluaran model dan menghasilkan nilai atribusi yang menunjukkan arah serta besar pengaruh fitur terhadap keputusan prediksi. Kerangka *explainability* ini dapat diterapkan pada tingkat global untuk memahami pola kepentingan fitur secara keseluruhan maupun pada tingkat lokal untuk menjelaskan alasan prediksi pada satu observasi tertentu (Ali *et al*., 2023), sehingga sangat relevan dalam *fraud detection* pada data transaksi *cryptocurrency* yang tidak seimbang guna menghubungkan keluaran model dengan kebutuhan analis dan pemangku kepentingan (Ertam, 2025; Yin *et al*., 2024; Zhou *et al*., 2023).

Permasalahan yang diangkat dalam penelitian ini berada pada persilangan tiga kebutuhan utama, yaitu akurasi deteksi, kemampuan menangani ketidakseimbangan kelas, dan interpretabilitas. Dataset transaksi ilegal pada umumnya bersifat tidak seimbang karena jumlah kejadian *illicit* jauh lebih sedikit dibandingkan transaksi *licit*, sehingga nilai *accuracy* yang tinggi belum tentu mencerminkan kemampuan model yang memadai dalam mengenali kelas minoritas. Oleh karena itu, evaluasi kinerja model perlu mempertimbangkan *precision*, *recall*, *F1-score*, ROC-AUC, serta distribusi kesalahan pada *confusion matrix*. Dalam konteks operasional, *recall* sangat penting karena *false negative* berarti transaksi anomali lolos tanpa terdeteksi, sedangkan *precision* berkaitan langsung dengan proporsi *alert* yang benar-benar relevan bagi analis.

Berdasarkan permasalahan dan perkembangan riset tersebut, penelitian ini membandingkan tiga algoritma klasifikasi tabular yang mewakili karakteristik berbeda—yaitu Logistic Regression sebagai *baseline* linear, Random Forest sebagai *ensemble* berbasis *bagging*, dan XGBoost sebagai *ensemble* berbasis *boosting*—pada dataset dan skema evaluasi yang sama, kemudian menerapkan SHAP pada model terbaik untuk menjelaskan dasar prediksi pada tingkat transaksi. XGBoost disertakan sebagai kandidat utama karena pendekatan *boosting* berbasis pohon mampu memodelkan hubungan nonlinier dan terbukti kompetitif dalam berbagai tugas klasifikasi serta deteksi *fraud* pada data terstruktur (Khoiri & Wahid, 2024; Prayoga & Voutama, 2024). Pendekatan terpadu ini dirancang agar analisis tidak hanya berfokus pada pencapaian *accuracy*, tetapi juga menguji kualitas deteksi kelas *illicit* melalui *precision*, *recall*, *F1-score*, dan ROC-AUC, sekaligus menyediakan jalur interpretasi pascaprediksi. Kontribusi penelitian ini terletak pada penyusunan *pipeline* yang mengintegrasikan evaluasi komparatif dan *explainability* dalam satu alur kerja guna mendukung proses *screening* serta investigasi transaksi Bitcoin, sejalan dengan arah kajian mutakhir di bidang deteksi *fraud* berbasis XAI sebagaimana dirangkum pada Tabel 1 (Ertam, 2025; Feng *et al*., 2024; Prayoga & Voutama, 2024; Yin *et al*., 2024).

Tabel 1. Ringkasan kajian terkait dan posisi penelitian

Studi	Fokus/Pendekatan	Relevansi
Asiri & Somasundaram (2025)	Deteksi fraud Bitcoin pada Elliptic; komparasi model klasik dan GCN	Memperkuat penggunaan Elliptic untuk klasifikasi licit-illicit
Alarab & Prakoonwit (2023)	Pemodelan temporal berbasis graf pada transaksi Bitcoin	Menunjukkan nilai informasi temporal dan relasional
Pocher *et al*. (2023)	Deteksi transaksi cryptocurrency anomali dalam konteks AML/CFT	Menguatkan penggunaan machine learning untuk forensik transaksi
Yin *et al*. (2024)	Fraud cryptocurrency pada data tidak seimbang dengan interpretasi	Menghubungkan class imbalance dan explainability
Ertam (2025)	Fraud blockchain dengan explainable AI	Memperlihatkan relevansi XAI pada deteksi fraud blockchain
Penelitian ini	Komparasi Logistic Regression, Random Forest, XGBoost + SHAP	Menyeimbangkan performa, deteksi kelas illicit, dan interpretabilitas

2. Metode

Penelitian ini menggunakan desain eksperimen kuantitatif dengan pendekatan *supervised learning*. Seluruh model menerima masukan berupa fitur numerik transaksi dan menghasilkan keluaran berlabel biner, yaitu 0 untuk transaksi *licit* (normal) dan 1 untuk transaksi *illicit* (anomali). Alur eksperimen secara berurutan meliputi penggabungan data fitur dan kelas, pembersihan label *unknown*, konversi target biner, pemilihan fitur numerik, normalisasi skala fitur, serta pembagian data pelatihan dan pengujian (*train-test split*). Tiga algoritma klasifikasi kemudian dilatih pada subset pelatihan dan dievaluasi pada subset pengujian menggunakan skema metrik yang sama untuk menentukan model terbaik, yang selanjutnya dianalisis probabilitas prediksi serta kontribusi fiturnya menggunakan SHAP guna menjelaskan keputusan klasifikasi pada transaksi *licit* dan *illicit* dalam satu *pipeline* yang konsisten. Seluruh tahapan implementasi dilakukan menggunakan bahasa pemrograman Python dengan dukungan pustaka Pandas, NumPy, Scikit-learn, XGBoost, SHAP, Matplotlib, dan Seaborn. Sumber data yang digunakan adalah Elliptic Bitcoin Dataset, yang merepresentasikan transaksi Bitcoin sebagai simpul (*node*) pada graf transaksi dan aliran pembayaran antarsimpul sebagai sisi (*edge*). Secara keseluruhan, dataset ini menyediakan label *licit*, *illicit*, dan *unknown* beserta 166 atribut pada setiap *node*, dengan total sekitar 203.769

node dan 234.355 *edge* pada graf Elliptic (Asiri & Somasundaram, 2025). Tahap *preprocessing* dimulai dengan menggabungkan berkas *elliptic_txs_features.csv* dan *elliptic_txs_classes.csv* berdasarkan atribut *txId* menggunakan operasi *inner join*, dilanjutkan dengan menghapus seluruh observasi berlabel *unknown* karena tidak dapat digunakan dalam klasifikasi terawasi. Label asli 1 dipetakan menjadi 1 (*illicit*/anomali) dan label asli 2 dipetakan menjadi 0 (*licit*/normal), sedangkan atribut *txId*, *class*, *label*, dan *time_step* dikeluarkan dari variabel prediktor sehingga tersisa 165 fitur numerik anonim dari 14.253 transaksi yang memiliki label pasti [cek data: pastikan apakah 14.253 transaksi ini berasal dari subset tertentu pada Elliptic Dataset]. Selanjutnya, seluruh 165 fitur numerik tersebut dinormalisasi menggunakan MinMaxScaler ke dalam rentang 0 sampai 1, kemudian dibagi menjadi 80% data pelatihan (11.402 transaksi) dan 20% data pengujian (2.851 transaksi) melalui teknik *stratified sampling* dengan parameter *random_state* = 42 agar proporsi kelas *licit* dan *illicit* pada kedua subset tetap sebanding. Rincian karakteristik dataset setelah tahap *preprocessing* disajikan pada Tabel 2.

Tabel 2. Karakteristik dataset setelah preprocessing

Karakteristik	Nilai
Jumlah transaksi berlabel	14.253 transaksi
Jumlah fitur prediktor	165 fitur numerik anonim
Kelas licit/normal (0)	13.380 transaksi (93,88%)
Kelas illicit/anomali (1)	873 transaksi (6,12%)
Data pelatihan	11.402 transaksi (80%)
Data pengujian	2.851 transaksi (20%)

2.1 Algoritma Klasifikasi

Logistic Regression digunakan sebagai model *baseline* karena memiliki struktur linear dan relatif mudah diinterpretasikan dalam mengestimasi probabilitas kelas melalui fungsi logistik. Pada eksperimen ini, parameter *max_iter* ditetapkan sebesar 1.000 untuk memberikan ruang konvergensi pada proses optimasi dan *random_state* = 42 digunakan untuk menjaga reprodusibilitas. Mengingat model linear sensitif terhadap perbedaan skala antarfitur, tahap normalisasi diterapkan sebelum proses pelatihan dilakukan. Sebagai pembanding nonlinier pertama, Random Forest digunakan untuk mewakili model *ensemble* berbasis *bagging*. Algoritma ini membangun sejumlah pohon keputusan (*decision tree*) pada subset data dan fitur secara acak, kemudian menggabungkan hasil prediksi antarpohon untuk menghasilkan keputusan akhir. Pendekatan *tree-based ensemble* ini banyak diterapkan pada deteksi anomali Bitcoin karena mampu menangani hubungan nonlinier serta data berdimensi tinggi (Asiri & Somasundaram, 2025; Hasan *et al.*, 2024). Konfigurasi Random Forest yang digunakan terdiri atas 200 pohon (*n_estimators* = 200), kedalaman maksimum 20 (*max_depth* = 20), *random_state* = 42, serta pemanfaatan seluruh *core* pemrosesan yang tersedia melalui *n_jobs* = -1. Selanjutnya, XGBoost diterapkan sebagai model *ensemble* berbasis *gradient boosting*. Berbeda dengan Random Forest yang membangun pohon-pohon keputusan secara relatif independen, mekanisme *boosting* membangun model secara berurutan sehingga *learner* berikutnya berfokus memperbaiki residual kesalahan prediksi dari model sebelumnya. Pendekatan XGBoost telah terbukti memberikan hasil yang kompetitif pada berbagai tugas klasifikasi data terstruktur dan deteksi *fraud* (Khoiri & Wahid, 2024; Prayoga & Voutama, 2024). Konfigurasi eksperimen untuk XGBoost menggunakan *n_estimators* = 200, *max_depth* = 10, *learning_rate* = 0,1, *random_state* = 42, *eval_metric* = *logloss*, dan *n_jobs* = -1, sebagaimana dirangkum bersama kedua model lainnya pada Tabel 3.

Tabel 3. Parameter model yang digunakan

Model	Parameter utama	Nilai
Logistic Regression	max_iter; random_state	1000; 42
Random Forest	n_estimators; max_depth; random_state; n_jobs	200; 20; 42; -1
XGBoost	n_estimators; max_depth; learning_rate; random_state; eval_metric; n_jobs	200; 10; 0,1; 42; logloss; -1

2.2 Evaluasi Model

Performa ketiga model diukur menggunakan *accuracy*, *precision*, *recall*, *F1-score*, ROC-AUC, *confusion matrix*, dan waktu pelatihan. Meskipun *accuracy* menunjukkan proporsi seluruh prediksi yang benar, metrik ini tidak memadai apabila digunakan secara tunggal pada dataset yang tidak seimbang. Oleh sebab itu, *precision* digunakan untuk menilai ketepatan *alert* anomali yang dihasilkan, *recall* untuk mengukur kemampuan model dalam menemukan transaksi *illicit* yang sesungguhnya, dan *F1-score* untuk merangkum keseimbangan antara *precision* dan *recall* dalam satu nilai harmonis. Selain itu, ROC-AUC digunakan untuk mengukur kemampuan diskriminasi model dalam membedakan kedua kelas pada berbagai nilai ambang (*threshold*), di mana nilai yang

mendekati 1 menunjukkan kapasitas pemisahan kelas yang semakin baik. Dengan mendefinisikan *True Positive* (TP) sebagai transaksi *illicit* yang diprediksi *illicit*, *True Negative* (TN) sebagai transaksi *licit* yang diprediksi *licit*, *False Positive* (FP) sebagai transaksi *licit* yang keliru diprediksi *illicit*, dan *False Negative* (FN) sebagai transaksi *illicit* yang keliru diprediksi *licit*, keempat metrik evaluasi utama tersebut dirumuskan pada Persamaan (1) hingga Persamaan (4):

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \quad (1)$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (2)$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \quad (3)$$

$$\text{F1} - \text{score} = \frac{2\times(\text{Precision}\times\text{Recall})}{\text{Precision+Recall}} \quad (4)$$

2.3 Interpretasi Model dengan SHAP

Setelah algoritma dengan performa evaluasi terbaik ditentukan, tahap interpretabilitas dilakukan menggunakan metode SHAP untuk menelusuri kontribusi setiap fitur terhadap hasil prediksi. Secara matematis, prediksi model direpresentasikan sebagai fungsi penjelasan aditif sebagaimana ditunjukkan pada Persamaan (5):

$$f(x) = \emptyset 0 + \sum_{i=1}^{M} \emptyset i \quad (5)$$

dengan $\emptyset 0$ menyatakan nilai dasar (*base value*) dari keluaran model dan $\emptyset i$ menyatakan nilai atribusi atau kontribusi fitur ke-i dari keseluruhan fitur. Nilai SHAP positif berfungsi mendorong keluaran model menuju kelas target yang dijelaskan (*illicit*), sedangkan nilai negatif menurunkan kecenderungan tersebut menuju kelas sebaliknya (*licit*). Untuk model berbasis pohon keputusan, algoritma TreeExplainer digunakan karena mampu memanfaatkan struktur internal pohon guna menghitung nilai atribusi secara lebih efisien. Secara konseptual, analisis interpretabilitas ini mencakup tingkat global untuk memahami pola kontribusi fitur secara keseluruhan dan tingkat lokal untuk menjelaskan dasar prediksi pada satu transaksi spesifik. Visualisasi pada tingkat lokal disajikan menggunakan *force plot* karena dapat memperlihatkan *base value*, arah serta besaran kontribusi tiap fitur, dan skor akhir prediksi secara simultan, sehingga membantu analis menilai alasan suatu transaksi memperoleh skor anomali tinggi tanpa semata-mata bergantung pada keluaran *black-box*.

2.4 Validitas Eksperimen dan Reprodusibilitas

Untuk menjaga validitas internal eksperimen, perbandingan ketiga model dilakukan pada subset pelatihan dan pengujian yang identik sehingga perbedaan capaian metrik secara langsung mencerminkan karakteristik algoritma pada skenario data yang sama. Penerapan *stratified sampling* menjamin kesebandingan proporsi kelas pada kedua subset, sedangkan penetapan nilai *random_state* yang konsisten meningkatkan reprodusibilitas pada proses pembagian data maupun pelatihan model. Di samping itu, eksperimen ini mempertahankan konfigurasi parameter yang telah ditetapkan tanpa melakukan pencarian *hyperparameter* secara ekstensif, sehingga hasil pengujian diperlakukan sebagai evaluasi komparatif pada konfigurasi yang diuji, bukan sebagai batas performa maksimum dari masing-masing algoritma. Mengingat ke-165 fitur prediktor dalam dataset bersifat anonim, nilai SHAP berperan dalam menjelaskan arah dan besar kontribusi *feature_i* secara matematis terhadap prediksi model, namun belum dapat diterjemahkan secara langsung menjadi indikator bisnis atau forensik spesifik tanpa dukungan metadata fitur asli.

3. Hasil dan Pembahasan

3.1 Hasil

Proses *preprocessing* terhadap Elliptic Bitcoin Dataset menghasilkan representasi numerik yang konsisten untuk ketiga model klasifikasi sebagaimana dirangkum pada Tabel 4. Penggabungan data berdasarkan atribut *txId* memastikan kesesuaian antara fitur dan label pada setiap observasi, sedangkan penghapusan label *unknown* mengeliminasi target yang tidak pasti sehingga menyisakan 14.253 transaksi

berlabel untuk pembelajaran terawasi. Dari jumlah tersebut, sebanyak 13.380 transaksi (93,88%) termasuk dalam kelas *licit* (normal) dan hanya 873 transaksi (6,12%) yang termasuk dalam kelas *illicit* (anomali). Rasio ini memperlihatkan kondisi ketimpangan kelas (*class imbalance*) yang kuat, di mana dominasi kelas *licit* dapat menyamarkan kelemahan model dalam mendeteksi kelas minoritas apabila evaluasi hanya mengoptimalkan *accuracy*. Oleh karena itu, konversi label biner (0 untuk *licit* dan 1 untuk *illicit*), penyeragaman skala 165 fitur numerik anonim menggunakan MinMaxScaler pada rentang 0–1, serta pembagian data melalui *stratified split* menjadi 11.402 data pelatihan (80%) dan 2.851 data pengujian (20%) dirancang untuk menjaga proporsi kelas sekaligus menempatkan *recall* dan *F1-score* sebagai metrik evaluasi yang sama pentingnya dengan *accuracy*.

Tabel 4. Ringkasan hasil preprocessing

Tahapan preprocessing	Hasil
Penggabungan dataset	Berhasil berdasarkan txId
Penghapusan label unknown	14.253 sampel tersisa
Konversi label	0 = licit; 1 = illicit
Pemilihan prediktor	165 fitur numerik anonim
Normalisasi	MinMaxScaler, rentang 0–1
Train-test split	80% train (11.402); 20% test (2.851), stratified

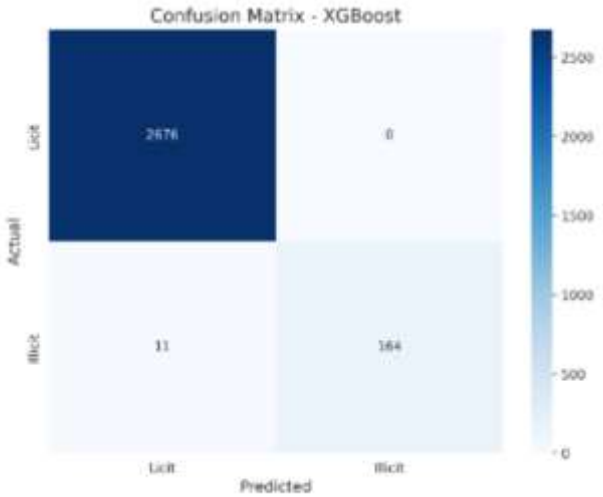
Berdasarkan data hasil *preprocessing* tersebut, pengujian ketiga algoritma klasifikasi menunjukkan peningkatan performa yang konsisten dari model linear menuju model *ensemble* berbasis pohon keputusan. Sebagai *baseline* linear, Logistic Regression memperoleh *accuracy* sebesar 0,9776, *precision* 0,8881, *recall* 0,7257, *F1-score* 0,7987, dan ROC-AUC 0,9658. Capaian *accuracy* yang relatif tinggi tersebut belum diikuti oleh *recall* yang memadai untuk kelas *illicit*, karena nilai *recall* sebesar 72,57% mengindikasikan bahwa sekitar seperempat transaksi anomali masih berpotensi lolos tanpa terdeteksi, yang membuktikan bahwa pola kelas *illicit* tidak sepenuhnya dapat dipisahkan oleh batas keputusan linear. Sebaliknya, penggunaan Random Forest meningkatkan seluruh metrik utama dengan capaian *accuracy* sebesar 0,9912, *precision* 1,0000 (tanpa *false positive* pada nilai ambang yang digunakan), *recall* 0,8571, *F1-score* 0,9231, serta ROC-AUC 0,9941. Perbaikan performa yang signifikan ini mengonfirmasi bahwa interaksi antarfitur pada transaksi Bitcoin bersifat nonlinier dan lebih efektif dimodelkan melalui pendekatan *ensemble decision tree*. Performa tertinggi secara keseluruhan dicapai oleh algoritma XGBoost dengan *accuracy* sebesar 0,9961, *precision* 1,0000, *recall* 0,9371, *F1-score* 0,9676, dan ROC-AUC 0,9960, sebagaimana disajikan pada Tabel 5. Apabila dibandingkan dengan Random Forest, peningkatan *accuracy* pada XGBoost sebesar 0,49 poin persentase memang tampak kecil, tetapi lonjakan *recall* sebesar 8,00 poin persentase dan *F1-score* sebesar 4,45 poin persentase memiliki implikasi praktis yang jauh lebih besar karena berkaitan langsung dengan bertambahnya jumlah transaksi *illicit* yang berhasil teridentifikasi. Lebih lanjut, jika dibandingkan terhadap Logistic Regression, XGBoost mencatatkan peningkatan *recall* hingga 21,14 poin persentase dan *F1-score* sebesar 16,89 poin persentase. Dari perspektif efisiensi komputasi, Logistic Regression merupakan model tercepat dengan waktu pelatihan sekitar 0,8 detik, disusul oleh XGBoost sekitar 2,1 detik dan Random Forest sekitar 4,2 detik pada lingkungan eksperimen yang sama. Dengan demikian, XGBoost tidak hanya menghasilkan *recall* dan *F1-score* tertinggi, tetapi juga membutuhkan waktu pelatihan sekitar separuh dari waktu komputasi Random Forest, sehingga dipilih sebagai model utama untuk analisis lebih lanjut.

Tabel 5. Perbandingan hasil evaluasi model

Metrik	Logistic Regression	Random Forest	XGBoost
Accuracy	0,9776	0,9912	0,9961
Precision	0,8881	1,0000	1,0000
Recall	0,7257	0,8571	0,9371
F1-Score	0,7987	0,9231	0,9676
ROC-AUC	0,9658	0,9941	0,9960
Train time (detik)	~0,8	~4,2	~2,1

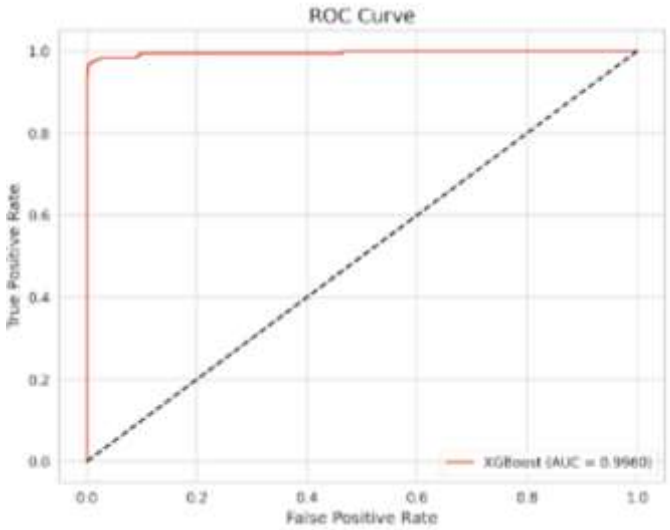
Distribusi ketepatan dan kesalahan prediksi pada model terbaik tersebut dirinci melalui *confusion matrix* XGBoost yang ditampilkan pada Gambar 1. Dari total 2.851 data uji, model berhasil mengklasifikasikan 2.840 transaksi secara tepat, yang terdiri atas 2.676 transaksi normal yang diprediksi benar sebagai kelas *licit* (*true negative*) tanpa satu pun transaksi normal yang keliru diprediksi sebagai *illicit* (*false positive* = 0), serta 164 transaksi anomali yang berhasil dideteksi dengan benar sebagai kelas *illicit* (*true positive*) dan 11 transaksi

anomali yang keliru diprediksi sebagai *licit* (*false negative*). Struktur kesalahan ini sepenuhnya selaras dengan capaian *precision* 1,0000 dan *recall* 0,9371. Ketiadaan *false positive* menunjukkan bahwa seluruh *alert* anomali yang dihasilkan model pada data uji benar-benar berasal dari kelas *illicit*, sehingga dalam skenario operasional karakteristik ini mampu menekan munculnya peringatan palsu dan mengurangi beban investigasi manual. Meskipun demikian, keberadaan 11 *false negative* tetap menjadi risiko yang perlu diperhatikan karena merepresentasikan transaksi ilegal yang lolos dari pemeriksaan lanjutan, sehingga pengembangan model berikutnya perlu tetap diarahkan pada peningkatan *recall* tanpa memicu lonjakan *false positive* secara berlebihan.



Gambar 1. Confusion matrix XGBoost

Selain evaluasi pada titik potong keputusan tunggal melalui *confusion matrix*, kemampuan diskriminasi model di seluruh rentang nilai ambang diuji menggunakan kurva *Receiver Operating Characteristic* (ROC) pada Gambar 2, yang memperlihatkan bahwa lintasan kurva XGBoost berada sangat dekat dengan sudut kiri atas dengan nilai *Area Under the Curve* (AUC) mencapai 0,9960. Capaian tersebut mengindikasikan kapasitas model yang sangat kuat dan stabil dalam memeringkat probabilitas transaksi *illicit* di atas transaksi *licit* pada berbagai variasi *threshold*. Apabila dibandingkan antarmodel, ketiga algoritma sebenarnya sama-sama menunjukkan kemampuan diskriminasi yang tinggi, yakni 0,9658 pada Logistic Regression, 0,9941 pada Random Forest, dan 0,9960 pada XGBoost. Walaupun selisih ROC-AUC antara Random Forest dan XGBoost hanya terpaut 0,0019, penggabungan metrik ini bersama capaian *recall* serta *F1-score* membuktikan bahwa XGBoost tetap memberikan profil kinerja deteksi yang paling seimbang, serta menegaskan pentingnya pembacaan multimetrik secara simultan pada pengujian dataset yang timpang.



Gambar 2. Kurva ROC XGBoost (AUC = 0,9960)

Selanjutnya, untuk membuka mekanisme pengambilan keputusan di balik prediksi XGBoost, metode SHAP diterapkan pada tingkat observasi individual menggunakan visualisasi *force plot*. Dalam representasi ini, nilai dasar (*base value*) model berfungsi sebagai titik awal sebelum setiap fitur menggeser skor prediksi menuju kelas *licit* (0) atau *illicit* (1), di mana kontribusi bernilai negatif mengurangi kecenderungan menuju kelas *illicit* dan kontribusi bernilai positif meningkatkan kecenderungan tersebut. Pada contoh pengujian transaksi *licit* yang ditunjukkan pada Gambar 3, tampak dominasi fitur-fitur berkontribusi negatif yang secara kolektif mendorong keluaran model menjauh dari kelas anomali, yang menandakan bahwa kombinasi nilai fitur pada observasi tersebut konsisten dengan profil transaksi normal yang dipelajari oleh model. Sebaliknya, pada contoh transaksi *illicit* yang disajikan pada Gambar 4, terdapat sejumlah fitur dengan kontribusi positif yang kuat sehingga mengakumulasi pergeseran skor keluaran model secara tegas menuju kelas 1. Melalui jejak atribusi lokal ini, analis keamanan tidak hanya menerima label akhir secara pasif, tetapi juga dapat membedakan apakah suatu prediksi anomali dipicu oleh satu fitur ekstrem atau oleh kombinasi beberapa fitur moderat saat melakukan triase investigasi. Meskipun visualisasi *force plot* tersebut mampu menyajikan dekomposisi keputusan secara jelas, perlu digarisbawahi bahwa seluruh 165 variabel prediktor pada implementasi dataset ini bersifat anonim, sehingga nilai SHAP hanya menerangkan besaran dan arah dorongan setiap *feature_i* secara matematis terhadap pergeseran prediksi tanpa dapat dipastikan makna semantiknya—seperti jumlah *input*, nilai *output*, atau derajat koneksi jaringan—apabila tidak disertai pemetaan fitur asli.



Gambar 3. SHAP force plot pada transaksi licit (normal)



Gambar 4. SHAP force plot pada transaksi illicit (anomali)

3.2 Pembahasan

Keunggulan performa XGBoost dibandingkan kedua model pembanding dalam eksperimen ini berakar pada kesesuaian mekanisme algoritmanya terhadap karakteristik data yang berdimensi tinggi dan memiliki kelas minoritas yang sangat timpang. Logistic Regression hanya membentuk batas keputusan linear sehingga keterkaitan kompleks antarfitur transaksi tidak dapat ditangkap secara optimal. Di sisi lain, meskipun Random Forest dan XGBoost sama-sama memanfaatkan struktur pohon keputusan yang fleksibel terhadap relasi nonlinier, mekanisme gradient boosting pada XGBoost bekerja memperbaiki residual kesalahan secara sekuensial, sehingga observasi kelas illicit yang sulit diklasifikasikan pada iterasi awal memperoleh bobot perhatian yang lebih besar pada iterasi berikutnya dan menghasilkan peningkatan recall yang nyata. Temuan ini sejalan dengan literatur terdahulu yang menunjukkan efektivitas tree-based ensemble dalam menangani interaksi nonlinier dan ketimpangan kelas pada data transaksi blockchain (Hasan *et al.*, 2024). Kajian mutakhir pada Elliptic Bitcoin Dataset juga mengonfirmasi bahwa model tabular berbasis pohon tetap kompetitif sebagai baseline yang kuat, sementara pemodelan berbasis graf seperti Graph Convolutional Network (GCN) dan temporal GCN menawarkan nilai tambah ketika struktur relasi edge serta dinamika waktu antarpelaku transaksi dimodelkan secara eksplisit dalam kerangka forensik AML/CFT (Alarab & Prakoonwit, 2023; Asiri & Somasundaram, 2025; Pocher *et al.*, 2023).

Dari perspektif operasional, pencapaian precision sempurna (1,0000) oleh XGBoost memiliki implikasi langsung terhadap efisiensi sistem peringatan dini (alert system) karena ketiadaan false positive menghindarkan tim investigator dari beban pemeriksaan kasus normal yang keliru ditandai. Akan tetapi, orientasi yang terlalu berfokus pada precision tetap menyimpan risiko terhadap recall, sebagaimana tercermin dari masih adanya 11 kasus false negative pada hasil pengujian walaupun nilai recall telah mencapai 0,9371. Mengingat dalam sistem anti-fraud dampak kerugian akibat lolosnya transaksi ilegal (false negative) sering kali lebih krusial dibandingkan biaya verifikasi false positive, penentuan nilai ambang (threshold) klasifikasi pada implementasi nyata perlu dikalibrasi sesuai toleransi risiko dan kapasitas audit organisasi. Hal ini sekaligus menjelaskan mengapa capaian ROC-AUC sebesar 0,9960 tidak boleh diinterpretasikan secara terpisah dari matriks kesalahan dan metrik kelas positif; pada dataset dengan prevalensi kelas illicit yang hanya 6,12%, nilai AUC yang mendekati sempurna belum menjamin seluruh transaksi anomali terdeteksi, sehingga penggunaan kurva precision-recall serta average precision pada riset selanjutnya dapat melengkapi evaluasi sensitivitas model terhadap kelas minoritas.

Lebih jauh, integrasi analisis SHAP memperluas fungsi model dari sekadar mesin prediktor menjadi perangkat pendukung keputusan (decision support tool). Sebagaimana ditekankan dalam literatur XAI, transparansi model tidak harus dicapai dengan menyederhanakan arsitektur algoritma, melainkan dengan menyediakan mekanisme penelusuran hubungan input–output yang dapat dipahami oleh pengguna (Ali *et al.*, 2023; Zhou *et al.*, 2023). Pemanfaatan SHAP pada penelitian ini bersesuaian dengan tren riset deteksi fraud pada jaringan blockchain dan cryptocurrency yang memadukan pengklasifikasi berkinerja tinggi dengan analisis atribusi fitur guna memperkuat keterlacakan prediksi pada data tidak seimbang (Ertam, 2025; Feng *et al.*, 2024; Yin *et al.*, 2024). Penerapan force plot memberikan nilai praktis karena investigasi forensik umumnya berawal dari pemeriksaan kasus per kasus, di mana analis dapat segera mengidentifikasi variabel pendorong utama saat suatu transaksi ditandai sebagai illicit. Namun, agar pipeline ini siap diterapkan pada lingkungan produksi, nilai atribusi SHAP perlu dihubungkan dengan nama fitur yang memiliki makna domain—seperti nominal transaksi, rasio input–output, umur address, pola interval waktu, atau metrik sentralitas jaringan—sehingga hasil penjelasan tidak hanya mengidentifikasi kode fitur pendorong prediksi, tetapi juga menerangkan perilaku transaksional yang dinilai mencurigakan.

Di samping keterbatasan semantik akibat anonimitas fitur, terdapat beberapa aspek metodologis dalam eksperimen ini yang membuka ruang penyempurnaan pada penelitian mendatang. Pembagian data menggunakan stratified random split mengasumsikan bahwa subset pelatihan dan pengujian berasal dari distribusi yang statis, padahal transaksi blockchain di dunia nyata bersifat dinamis dan modus pencucian uang terus berevolusi lintas waktu; oleh karena itu, skema evaluasi berbasis urutan waktu (time split atau walk-forward validation) perlu diterapkan guna menguji ketahanan generalisasi model terhadap pola anomali baru pada periode selanjutnya. Selain itu, proses normalisasi MinMaxScaler dalam eksperimen ini diterapkan sebelum train-test split, sehingga untuk pipeline produksi yang lebih ketat, parameter scaler sebaiknya di-fit hanya pada data pelatihan sebelum ditransformasikan ke data pengujian guna mencegah kebocoran informasi statistik antarsubset. Dari sisi penanganan class imbalance dan representasi data, penelitian ini masih mempertahankan distribusi alami tanpa rekayasa keseimbangan kelas serta belum mengeksploitasi struktur topologi graf; eksperimen lanjutan dapat menguji pengaturan parameter scale_pos_weight pada XGBoost, teknik oversampling atau undersampling terkontrol (Yin *et al.*, 2024), maupun arsitektur hibrida yang memadukan graph embedding (seperti GCN atau Graph Attention Network) dengan pengklasifikasi XGBoost dan SHAP agar informasi relasional antar-node dapat ditangkap tanpa mengorbankan kemudahan interpretasi (Alarab & Prakoonwit, 2023; Asiri & Somasundaram, 2025).

Secara praktis dan keilmuan, rangkaian temuan ini menegaskan bahwa kombinasi XGBoost dan SHAP mampu berfungsi efektif sebagai lapisan penyaringan awal (initial screening) dalam alur kerja human-in-the-loop. Model bertugas memprioritaskan antrean transaksi berdasarkan estimasi probabilitas illicit pada volume data yang masif, sedangkan SHAP menyertakan dasar atribusi fitur untuk setiap alert yang diterbitkan sebelum auditor menggabungkannya dengan riwayat alamat dan bukti eksternal guna mengambil keputusan akhir yang akuntabel. Dari sisi kontribusi ilmiah, hasil studi ini membuktikan bahwa peningkatan kompleksitas model dari struktur linear (Logistic Regression) ke arsitektur gradient boosting (XGBoost) tidak harus mengorbankan transparansi secara keseluruhan; lonjakan tajam pada kemampuan deteksi kelas illicit dapat berjalan beriringan dengan pemulihan interpretabilitas pascaprediksi melalui SHAP, sehingga menghasilkan titik temu yang proporsional antara ketajaman deteksi dan keterjelasan keputusan pada analitik keamanan transaksi berisiko tinggi.

4. Kesimpulan

Pendekatan *explainable machine learning* pada penelitian ini berhasil diterapkan untuk mendeteksi transaksi anomali pada Elliptic Bitcoin Dataset yang memiliki tingkat ketimpangan kelas tinggi, yakni 13.380 transaksi *licit* (93,88%) dan 873 transaksi *illicit* (6,12%) dari total 14.253 transaksi berlabel dengan 165 fitur numerik anonim. Di antara tiga algoritma yang dievaluasi menggunakan skema multimetrik, XGBoost membuktikan performa secara keseluruhan yang paling unggul dibandingkan Random Forest dan Logistic Regression dengan capaian *accuracy* sebesar 0,9961, *precision* 1,0000, *recall* 0,9371, *F1-score* 0,9676, serta ROC-AUC 0,9960. Evaluasi melalui *confusion matrix* pada data pengujian mengonfirmasi bahwa XGBoost mampu mengidentifikasi 2.676 transaksi *licit* secara tepat (*true negative*) tanpa menghasilkan *false positive*, serta mendeteksi 164 transaksi *illicit* dengan benar (*true positive*) dan hanya menyisakan 11 transaksi *illicit* yang terlewat (*false negative*), sekaligus mencatatkan kombinasi paling seimbang antara ketajaman diskriminasi kelas, sensitivitas deteksi anomali, dan efisiensi waktu pelatihan. Integrasi metode SHAP pada

model XGBoost menambahkan lapisan interpretabilitas pascaprediksi dengan memperlihatkan arah dan besaran kontribusi fitur terhadap keputusan klasifikasi pada tingkat transaksi individual. Visualisasi *force plot* memperjelas bagaimana dominasi kontribusi fitur negatif mendorong skor prediksi menjauh dari kelas anomali pada transaksi *licit*, sedangkan akumulasi kontribusi positif menggeser prediksi secara tegas menuju kelas anomali pada transaksi *illicit*, sehingga menghasilkan model deteksi yang tidak hanya akurat tetapi juga transparan untuk mendukung proses *screening* dan investigasi transaksi *blockchain*. Untuk meningkatkan kesiapan implementasi pada lingkungan operasional, penelitian selanjutnya perlu menitikberatkan pada penerapan skema evaluasi berbasis urutan waktu (*temporal evaluation*), penanganan *class imbalance* secara eksplisit, pemanfaatan struktur relasional graf, validasi lintas dataset eksternal, serta pemetaan fitur anonim ke dalam indikator transaksional yang bermakna agar sistem deteksi yang dihasilkan semakin *robust* dan dapat diaudit secara menyeluruh.

Referensi

Alarab, I., & Prakoonwit, S. (2023). Graph-based LSTM for anti-money laundering: Experimenting temporal graph convolutional network with Bitcoin data. *Neural Processing Letters*, *55*(1), 689–707. https://doi.org/10.1007/s11063-022-10904-8

Ali, S., Abuhmed, T., El-Sappagh, S., Muhammad, K., Alonso-Moral, J. M., Confalonieri, R., Guidotti, R., Del Ser, J., Díaz-Rodríguez, N., & Herrera, F. (2023). Explainable Artificial Intelligence (XAI): What we know and what is left to attain trustworthy artificial intelligence. *Information Fusion*, *99*, 101805. https://doi.org/10.1016/j.inffus.2023.101805

Asiri, A., & Somasundaram, K. (2025). Graph convolution network for fraud detection in Bitcoin transactions. *Scientific Reports*, *15*(1), 11076. https://doi.org/10.1038/s41598-025-95672-w

Ertam, F. (2025). Near real-time Ethereum fraud detection using explainable AI in blockchain networks. *Applied Sciences*, *15*(19), 10841. https://doi.org/10.3390/app151910841

Feng, X., Shi, Q., Li, X., Liu, H., & Wang, L. (2024). IDPonzi: An interpretable detection model for identifying smart Ponzi schemes. *Engineering Applications of Artificial Intelligence*, *136*, 108868. https://doi.org/10.1016/j.engappai.2024.108868

Hasan, M., Rahman, M. S., Janicke, H., & Sarker, I. H. (2024). Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis. *Blockchain: Research and Applications*, *5*(3), 100207. https://doi.org/10.1016/j.bcra.2024.100207

Hung, C., Wijaya, J. F., Victor, V., Pardosi, I. A., & Sinaga, F. M. (2023). Prediksi fluktuasi harga Bitcoin dengan menggunakan Random Forest classifier. *Jurnal SIFO Mikroskil*, *24*(2), 95–108. https://doi.org/10.55601/jsm.v24i2.1024

Iffadah, A. S., Trimono, T., & Prasetya, D. A. (2025). SHapley Additive exPlanations interpretation of the XGBoost model in predicting air quality in Jakarta. *Jurnal Riset Informatika*, *7*(3), 119–127. https://doi.org/10.34288/jri.v7i3.366

Julianto, J. (2022). Analisis investasi dalam memprediksi pergerakan harga Bitcoin dengan menggunakan Recurrent Neural Network pada platform Indodax. *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi*, *8*(2), 136–147. https://doi.org/10.24014/rmsi.v8i2.17233

Khoiri, S. A., & Wahid, A. (2024). Analisis kinerja algoritma *machine learning* dalam prediksi harga *cryptocurrency*. *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia)*, *9*(2), 133–141. https://doi.org/10.32528/justindo.v9i2.1965

Kurniyanto, F. P., & Hartoyo, A. (2023). Explainable AI: Identification of writing from famous figures in Indonesia using BERT and Naive Bayes methods. *Jurnal Media Informatika Budidarma*, *7*(1), 160–169. https://doi.org/10.30865/mib.v7i1.5392

Liang, Y., Wu, W., Liang, R., Chen, Y., Lei, K., Zhong, G., Zhang, J., Gan, Q., & Huang, J. (2025). A plug-and-play data-driven approach for anti-money laundering in Bitcoin. *Expert Systems with Applications*, *266*, 126072. https://doi.org/10.1016/j.eswa.2024.126072

Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M. Z., & Ferretti, S. (2023). Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. *Electronic Markets*, *33*(1), 37. https://doi.org/10.1007/s12525-023-00654-3

Prayoga, A. H., & Voutama, A. (2024). Pengembangan aplikasi *bank account fraud detection* dengan menggunakan algoritma XGBoost. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(3), 2916–2922. https://doi.org/10.36040/jati.v8i3.9564

Rizkilloh, M. F., & Widiyanesti, S. (2022). Prediksi harga *cryptocurrency* menggunakan algoritma Long Short Term Memory (LSTM). *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *6*(1), 25–31. https://doi.org/10.29207/resti.v6i1.3630

Sari, A. P., Billy, B., Tsaqif, D. A., Sartono, B., & Firdawanti, A. R. (2024). Classification of drinking water source suitability in West Java using XGBoost and cluster analysis based on SHAP values: Klasifikasi kelayakan sumber air minum di Jawa Barat menggunakan XGBoost dan analisis klasterisasi berdasarkan nilai SHAP. *Indonesian Journal of Statistics and Its Applications*, *8*(2), 202–214. https://doi.org/10.29244/ijsa.v8i2p202-214

Sibagariang, S. (2025). Interpretable machine learning for job placement prediction: A SHAP-based feature analysis. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, *14*(3), 190–198. https://doi.org/10.22146/jnteti.v14i3.20516

Syamkalla, M. T., Khomsah, S., & Nur, Y. S. R. (2024). Implementasi algoritma CatBoost dan SHapley Additive exPlanations (SHAP) dalam memprediksi popularitas *game indie* pada platform Steam. *Jurnal Teknologi Informasi dan Ilmu Komputer*, *11*(4), 777–786. https://doi.org/10.25126/jtiik.1148503

Yin, P., Jiang, W., Ma, Z., & Zhang, L. (2024). Cryptocurrency transaction fraud detection based on imbalanced classification with interpretable analysis. *International Journal of Intelligent Information Technologies (IJIIT)*, *20*(1), 1–21. https://doi.org/10.4018/IJIIT.357696

Zhou, Y., Li, H., Xiao, Z., & Qiu, J. (2023). A user-centered explainable artificial intelligence approach for financial fraud detection. *Finance Research Letters*, *58*, 104309. https://doi.org/10.1016/j.frl.2023.104309