Journal of Informatics Engineering and Software Applications

Money Laundering Detection on the Ethereum Blockchain Using the XGBoost Algorithm

Aldo Amrullah[1], Muhammad Arhami[2]*, Umri Erdiansyah[3]

[123] Jurusan Teknologi Informasi dan Komputer, Politeknik Negeri Lhokseumawe, Kota Lhokseumawe, 24301 INDONESIA
*Penulis Korespondensi : muhammad.arhami@pnl.ac.id

INFORMASI ARTIKEL

Riwayat artikel:
Diajukan pada 10 November 2025
Direvisi pada 26 November 2025
Publikasi pada 20 Desember 2025

Kata kunci:
Kejahatan Finansial
Pencucian Uang
Cryptocurrency
DataverseNL
XGBoost

Keywords:
Financial crime
Money Laundering
Cryptocurrency
DataverseNL
XGBoost

ABSTRAK

Kejahatan finansial berbasis aset crypto semakin kompleks dan menimbulkan tantangan signifikan bagi deteksi dini, terutama dalam praktik pencucian uang. Penelitian ini bertujuan untuk mendeteksi aktivitas pencucian uang pada jaringan Ethereum dengan memanfaatkan sepuluh fitur transaksi terpilih serta menerapkan pendekatan pipeline yang menggabungkan imputasi nilai hilang menggunakan SimpleImputer (strategi mean) dan algoritma Extreme Gradient Boosting (XGBoost) dengan fungsi objektif binary:logistic. Data yang digunakan merupakan data sekunder dari DataverseNL, mencakup 4.681 akun yang terdiri dari 2.179 akun illicit dan 2.502 akun normal. Berdasarkan hasil klasifikasi, distribusi label aktual menunjukkan 53,5% untuk kelas normal dan 46,5% untuk kelas illicit, sedangkan hasil prediksi model menunjukkan 54,2% dan 45,8% secara berurutan. Evaluasi performa menggunakan Confusion Matrix menghasilkan akurasi sebesar 95%, dengan nilai rata-rata precision, recall, dan F1-score masing-masing sebesar 0,95. Hasil tersebut menunjukkan bahwa model memiliki kinerja yang seimbang dan akurat dalam mengklasifikasikan aktivitas transaksi crypto. Secara keseluruhan, sistem pipeline XGBoost terbukti efektif sebagai pendekatan deteksi awal terhadap risiko pencucian uang pada ekosistem cryptocurrency, serta berpotensi dikembangkan lebih lanjut sebagai dasar sistem pemantauan dan kepatuhan (compliance) keuangan digital.

ABSTRACT

Financial crimes involving crypto assets are becoming increasingly complex and pose significant challenges for early detection, particularly in money laundering practices. This study aims to detect money laundering activities on the Ethereum network by leveraging ten selected transaction features and implementing a pipeline approach that combines missing value imputation using SimpleImputer (mean strategy) and the Extreme Gradient Boosting (XGBoost) algorithm with a binary:logistic objective function. The data used was secondary data from DataverseNL, comprising 4,681 accounts, which included 2,179 illicit accounts and 2,502 normal accounts. The classification results show that the actual label distribution was 53.5% for the normal class and 46.5% for the illicit class, while the model's predictions showed 54.2% and 45.8%, respectively. Performance evaluation using a Confusion Matrix yielded an accuracy of 95%, with average precision, recall, and F1-score values of 0.95 each. These results indicate that the model has a balanced and accurate performance in classifying crypto transaction activities. Overall, the XGBoost pipeline system proves to be an effective approach for the early detection of money laundering risks in the cryptocurrency ecosystem and has the potential for further development as a foundation for digital financial monitoring and compliance systems.

1. Pendahuluan

Cryptocurrency merupakan sistem uang elektronik berbasis peer-to-peer yang memungkinkan transfer nilai secara langsung tanpa perantara lembaga keuangan [1], [2]. Sistem ini bersifat terdesentralisasi, tidak memiliki bentuk fisik, dan didukung oleh teknologi blockchain yang menjamin transparansi serta keamanan transaksi [3], [4]. Namun, karakteristik anonim dan global dari cryptocurrency juga menjadikannya sarana potensial dalam praktik pencucian uang lintas negara [3], [5].

Menurut laporan Chainalysis Crypto Crime Report 2025, sekitar US $ 40 miliar aset crypto telah dicuci melalui alamat ilegal sepanjang tahun 2024 [6]. Sebagian besar transaksi tersebut mengalir melalui layanan decentralized finance (DeFi), mixers, dan dompet pribadi yang sulit dilacak [7], [8]. Fenomena ini menunjukkan bahwa regulasi dan mekanisme penegakan hukum global masih tertinggal dibandingkan dengan kecepatan inovasi teknologi blockchain [9], [10].

Permasalahan utama dalam deteksi pencucian uang pada transaksi cryptocurrency meliputi: (1) pola transaksi yang sangat kompleks dan berlapis-lapis sehingga sulit dilacak, dan (2) ketidakseimbangan serta keterbatasan data transaksi ilegal yang menghambat efektivitas model deteksi berbasis machine learning. Kondisi tersebut menuntut pendekatan cerdas yang mampu mengenali pola anomali dalam data transaksi secara akurat dan efisien.

Beberapa metode machine learning seperti K-Nearest Neighbors (KNN), Random Forest (RF), Support Vector Machines (SVM), dan Isolation Forest telah digunakan untuk mendeteksi aktivitas mencurigakan [11], [12]. Namun, penelitian terdahulu menunjukkan bahwa algoritma Extreme Gradient Boosting (XGBoost) memiliki performa terbaik dalam mendeteksi aktivitas pencucian uang [13], [14]. Studi empiris oleh Siddhesh et al. [8] menunjukkan bahwa XGBoost mencapai akurasi, presisi, dan recall sempurna (1.00), dengan nilai AUC sebesar 0.94, yang melampaui model lain seperti RF (0.89), SVM (0.92), dan KNN (0.90).

Keunggulan utama XGBoost terletak pada kemampuannya dalam menangani dataset besar dan kompleks dengan efisiensi tinggi, serta memprioritaskan fitur yang paling berpengaruh dalam proses klasifikasi [15], [16], [17]. Berdasarkan hal tersebut, penelitian ini berfokus pada implementasi algoritma Extreme Gradient Boosting (XGBoost) untuk mendeteksi aktivitas pencucian uang dalam transaksi cryptocurrency. Model ini diharapkan mampu mengklasifikasikan transaksi ke dalam kategori normal dan illicit, sehingga dapat digunakan sebagai dasar dalam sistem pemantauan keuangan digital untuk memperkuat deteksi dini dan pencegahan kejahatan finansial berbasis aset crypto.

2. Metode

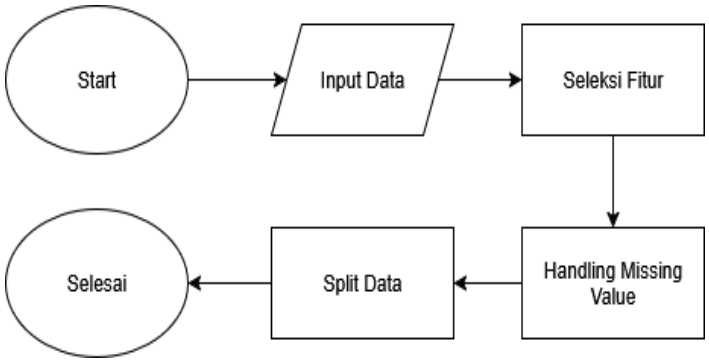
2.1 Data dan Pengumpulan Data

Data yang digunakan dalam penelitian ini merupakan data sekunder yang bersumber dari DataverseNL, yaitu dataset publik yang dikembangkan untuk mendeteksi aktivitas ilegal pada jaringan Ethereum [9]. Dataset ini terdiri atas 4.681 akun Ethereum, yang terbagi menjadi 2.179 akun Illicit (ilegal) dan 2.502 akun Normal (legal).

Masing-masing akun berisi catatan histori transaksi dalam bentuk structured data berformat CSV, yang mencakup berbagai fitur numerik seperti nilai transaksi, frekuensi pengiriman dan penerimaan Ether, serta interval waktu antar transaksi. Data ini dipilih karena merepresentasikan aktivitas keuangan yang nyata di blockchain, sehingga sesuai untuk dijadikan bahan analisis deteksi pencucian uang menggunakan pendekatan machine learning. Proses pengumpulan data dilakukan dengan mengunduh dataset dari repositori DataverseNL secara terbuka, kemudian memeriksa kelengkapan, struktur kolom, dan konsistensi nilai sebelum masuk ke tahap preprocessing.

2.2 *Preprocessing* Data

Tahap pra-pemrosesan dilakukan untuk memastikan kualitas dan konsistensi data sebelum digunakan dalam proses pelatihan maupun inferensi model XGBoost [20]. Tahapan preprocessing ditunjukkan secara konseptual pada Gambar 1 Rancangan Preprocessing.



Gambar 1. Rancangan Preprocessing

Proses dimulai dengan memuat berkas data berformat .csv ke dalam struktur DataFrame untuk memudahkan manipulasi dan analisis data. Selanjutnya, dilakukan seleksi terhadap sepuluh fitur teratas yang direkomendasikan oleh literatur sebagai variabel prediktor utama dalam mendeteksi aktivitas pencucian uang.

Variabel target diperoleh dari kolom FLAG yang dikonversi ke dalam tipe bilangan bulat, di mana label 0 merepresentasikan akun normal dan label 1 merepresentasikan akun illicit. Karena seluruh fitur bersifat numerik, konversi tipe data dilakukan secara defensif untuk menjaga keseragaman skema dan mencegah inkonsistensi saat pemrosesan.

Langkah berikutnya adalah pemeriksaan keberadaan nilai hilang (missing values) pada setiap fitur. Jika ditemukan nilai kosong, sistem secara otomatis menjalankan proses imputasi menggunakan komponen SimpleImputer dengan strategi mean, sehingga setiap variabel memiliki nilai representatif tanpa kehilangan informasi penting. Apabila data tidak mengandung nilai hilang, tahap imputasi dilewati secara otomatis.

Seluruh proses preprocessing diintegrasikan dalam sebuah pipeline untuk memastikan konsistensi antara tahap pelatihan dan tahap prediksi. Hasil akhir dari tahapan ini berupa matriks fitur dengan sepuluh variabel numerik yang siap digunakan oleh model XGBoost, serta vektor target FLAG bertipe integer. Mekanisme ini menjamin bahwa proses klasifikasi aktivitas pencucian uang pada transaksi cryptocurrency dapat dilakukan secara konsisten, replikatif, dan bebas dari gangguan akibat ketidakteraturan data.

2.3 XGBoost

XGBoost merupakan algoritma machine learning berbasis ensemble learning yang dikembangkan untuk meningkatkan akurasi prediksi melalui pendekatan gradient boosting framework [7], [16]. Algoritma ini membangun model prediktif secara berurutan dengan menggabungkan sejumlah weak decision trees, di mana setiap pohon selanjutnya berfungsi memperbaiki kesalahan dari model sebelumnya [14], [15]. Keunggulan utama XGBoost terletak pada efisiensi komputasi, mekanisme regularization eksplisit, serta kemampuannya dalam menangani imbalanced data dan fitur-fitur tidak relevan [20].

Secara umum, XGBoost meminimalkan fungsi objektif yang terdiri atas dua komponen, yaitu loss function dan fungsi regularisasi kompleksitas pohon. Formulasinya ditunjukkan pada Persamaan (1).

$$obj^{(t)} = \Sigma_{i=1}^{n} \ell(y_i, \hat{y}_i^{(t-1)} + f_t(x_i)) + \Omega(f_t) \quad (1)$$

Keterangan: obj^(t) adalah nilai fungsi tujuan pada iterasi ke–t, ℓ(y_i, ŷ_i) menyatakan fungsi kerugian, ŷ_i^(t-1) adalah prediksi sebelum penambahan pohon ke–t, f_t(x_i) merupakan keluaran pohon ke–t untuk sampel ke–i, dan Ω(f_t) adalah pena0lti kompleksitas pohon (regularisasi).

1. Regularisasi Kompleksitas Pohon

Regularisasi bertujuan mengendalikan kompleksitas model agar tidak terjadi overfitting. Bentuk regularisasi yang digunakan dalam XGBoost dinyatakan pada Persamaan (2).

$$\Omega(f_t) = \gamma T + (\lambda/2) \Sigma_{j=1}^{T} w_j^2 \quad (2)$$

Keterangan: T adalah jumlah daun pada pohon f_t; w_j merupakan bobot atau skor daun ke–j; λ adalah koefisien L2 regularization untuk menekan bobot berlebih; γ merupakan penalti penambahan daun.

2. Fungsi Kerugian Logistik untuk Klasifikasi Biner

Untuk kasus klasifikasi biner, digunakan fungsi kerugian logistik sebagaimana ditunjukkan pada Persamaan (3), dengan fungsi aktivasi sigmoid pada Persamaan (4).

$$\ell(y_i, \hat{y}_i) = -[y_i \log \sigma(\hat{y}_i) + (1 - y_i) \log (1 - \sigma(\hat{y}_i))] \quad (3)$$

$$\sigma(z) = 1 / (1 + e^{(-z)}) \quad (4)$$

3. Pendekatan Orde Dua (Gradien dan Hessian)

Untuk mempercepat proses optimasi, XGBoost menggunakan pendekatan orde dua dengan menghitung turunan pertama (gradient) dan turunan kedua (hessian) dari fungsi kerugian sebagaimana pada Persamaan (5) dan (6).

$$g_i = \partial \ell / \partial \hat{y}_i = \sigma(\hat{y}_i) - y_i \quad (5)$$

$$h_i = \partial^2 \ell / \partial \hat{y}_i^2 = \sigma (\hat{y} i) (1 - \sigma(\hat{y}_i)) \quad (6)$$

4. Akumulasi dan Optimasi Bobot Daun

Nilai gradien dan hessian dari setiap sampel yang jatuh ke dalam daun ke–j diakumulasikan sebagaimana Persamaan (7), sedangkan bobot optimal tiap daun dihitung menggunakan Persamaan (8).

$$G_j = \Sigma_{i \in I_j} g_i, H_j = \Sigma_{i \in I_j} h_i \quad (7)$$

$$w_j^* = -G_j / (H_j + \lambda) \quad (8)$$

5. Evaluasi Split Menggunakan Gain

Keputusan untuk melakukan split pada cabang kiri (L) dan kanan (R) ditentukan berdasarkan skor gain, yang menunjukkan peningkatan nilai fungsi objektif akibat pemisahan data. Formulasinya ditunjukkan pada Persamaan (9).

$$Gain = 1/2[(G_L^2/(H_L+\lambda) + G_R^2/(H_R+\lambda) - G^2/(H+\lambda))] - \gamma \quad (9)$$

6. Fungsi Pohon dan Pembaruan Prediksi

Hasil akhir model pada iterasi ke–t dinyatakan dalam bentuk fungsi pohon sebagaimana Persamaan (10), dengan pembaruan prediksi yang dilakukan secara aditif sebagaimana Persamaan (11).

$$f_t(x) = w_{q(x)}, \; q: R^m \rightarrow \{1,\ldots,T\} \quad (10)$$

$$\hat{y}_i^{(t)} = \hat{y}_i^{(t-1)} + \eta f_t(x_i), \; p_i = \sigma(\hat{y}_i^{(final)}) \quad (11)$$

2.4 Evaluasi dan Pengujian Model

Evaluasi performa model dilakukan menggunakan pendekatan k-fold cross-validation sebanyak 10-fold untuk memastikan kemampuan generalisasi model terhadap data yang berbeda-beda. Teknik ini membagi dataset menjadi sepuluh subset, di mana sembilan bagian digunakan untuk pelatihan dan satu bagian untuk pengujian secara bergantian hingga seluruh data terliput [21]. Pendekatan ini banyak digunakan pada penelitian klasifikasi biner untuk mengurangi bias estimasi dan memvalidasi konsistensi model terhadap variasi data [22].

Performa model diukur menggunakan Confusion Matrix dan Classification Report yang memuat metrik accuracy, precision, recall, dan F1-score, yang mencerminkan keseimbangan antara prediksi benar dan kesalahan klasifikasi [23]. Evaluasi ini penting untuk memahami sejauh mana model mampu meminimalkan false positives maupun false negatives, terutama pada konteks deteksi aktivitas pencucian uang yang sensitif terhadap kesalahan prediksi.

Selain itu, Receiver Operating Characteristic (ROC) Curve digunakan untuk mengukur kemampuan model dalam membedakan kelas positif (Illicit) dan negatif (Normal) berdasarkan nilai Area Under Curve (AUC). Nilai AUC yang mendekati 1 menunjukkan bahwa model memiliki kemampuan klasifikasi yang sangat baik dan stabil dalam memisahkan dua kelas [18], [23]. Metode ini telah terbukti menjadi ukuran evaluasi paling konsisten untuk model klasifikasi biner karena tidak bergantung pada ambang batas keputusan.

3. Hasil Dan Pembahasan

3.1 Hasil Pengumpulan Data

Berdasarkan hasil pengumpulan dan pemeriksaan awal, diperoleh 42 fitur yang dapat digunakan dalam mendeteksi aktivitas pencucian uang. Hasil data dapat diliat pada Tabel 1 yang menampilkan beberapa hasil pengempulan data.

Tabel 1. Hasil Pengumpulan Data

Address	FLAG	Time_Diff_between_ first_and_last_(Mins)	total_ether_ received	min_value_ received	.....
0x0020731604c882cf7bf8 c444be97d17b19ea4316	1	4815.43	1.752.978.485	1	.....
0x002bf459dc58584d58 886169ea0e80f3ca95ffaf	1	9622.53	153.378.461	0.586269	.....
0x002f0c8119c16d31034 2d869ca8bf6ace34d9c39	1	321.42	131.882	0.00102	.....
0x0059b14e35dab1b4ee e1e2926c7a5660da66f747	1	73091	3.755.604.606	0.000784	.....
0x00009277775ac7d0d59 eaad8fee3d10ac6c805e8	0	704785.63	5.864.666.748	0	.....
0x0002b44ddb1476db43 c868bd494422ee4c136fed	0	1218216.73	3.085.478.209	0	.....
0x001f99982965a3792077 893ecadc7be0c61d613c	0	329.78	101	44.048.882	.....

Berdasarkan hasil pengumpulan dan pemeriksaan awal, diperoleh 10 fitur utama yang relevan dan paling berpengaruh dalam mendeteksi aktivitas pencucian uang. Tabel 2 menunjukkan fitur-fitur yang akan digunakan pada model.

Tabel 2. Fitur yang digunakan

Fitur	Kelas Normal	Kelas Illicit
Time_Diff_between_first_and_last_(Mins)	Memiliki rentang waktu aktivitas yang panjang; transaksi tersebar dalam periode yang stabil.	Aktivitas cenderung berlangsung dalam waktu singkat; menunjukkan tujuan jangka pendek dan pola cepat tutup akun.
total_ether_balance	Biasanya memiliki saldo Ether yang relatif besar dan stabil.	Saldo cenderung kecil atau fluktuatif; digunakan hanya sementara untuk aktivitas tertentu.
min_value_received	Transaksi masuk memiliki nilai minimum yang lebih besar dan jarang dilakukan berulang.	Nilai transaksi masuk kecil dan dilakukan berulang untuk menyamarkan aliran dana.
min_val_sent	Nilai minimum transaksi keluar lebih besar, menunjukkan aktivitas normal seperti pembayaran rutin.	Nilai minimum transaksi keluar kecil dan sering; strategi untuk menghindari deteksi sistem otomatis.
avg_val_received	Rata-rata nilai transaksi masuk cukup tinggi dan stabil.	Rata-rata transaksi masuk rendah dan acak; digunakan untuk fragmentasi dana (*smurfing*).
Avg_min_between_received_tnx	Waktu antar transaksi masuk relatif lama; tidak menunjukkan intensitas tinggi.	Waktu antar transaksi masuk sangat singkat; menunjukkan aktivitas cepat dan simultan.
Avg_min_between_sent_tnx	Transaksi keluar dilakukan secara teratur dengan jeda waktu yang wajar.	Transaksi keluar sering dilakukan berurutan dan cepat untuk segera memindahkan dana.
Unique_Received_From_Addresses	Menerima transaksi dari jumlah alamat pengirim yang terbatas dan berulang.	Berinteraksi dengan banyak alamat unik untuk menyulitkan pelacakan pola transaksi.
max_value_received	Nilai maksimum transaksi masuk biasanya proporsional terhadap total saldo akun.	Sering memiliki transaksi masuk besar yang tidak biasa sebagai bagian dari pola pencucian uang.
avg_val_sent	Nilai rata-rata transaksi keluar tinggi dan stabil.	Nilai rata-rata transaksi keluar rendah, sering tersebar ke banyak alamat berbeda untuk menghindari deteksi.

Fitur-fitur tersebut merepresentasikan pola perilaku transaksi akun Ethereum, baik dari sisi waktu, frekuensi, maupun volume Ether yang dikirim dan diterima. Karakteristik perbandingan kedua kelas seperti yang ditunjukkan pada Tabel 2, yang menggambarkan perbedaan pola transaksi antara akun normal dan akun illicit secara kuantitatif dan deskriptif.

3.2. Hasil Preprocessing

Tahap pra-pemrosesan dilakukan untuk menyiapkan data sebelum masuk ke proses pelatihan model Extreme Gradient Boosting (XGBoost). Pada tahap ini, sistem terlebih dahulu menetapkan sepuluh fitur utama yang digunakan sebagai variabel prediktor berdasarkan hasil kajian literatur. Tabel 1 menunjukkan fitur-fitur yang akan digunakan pada model.

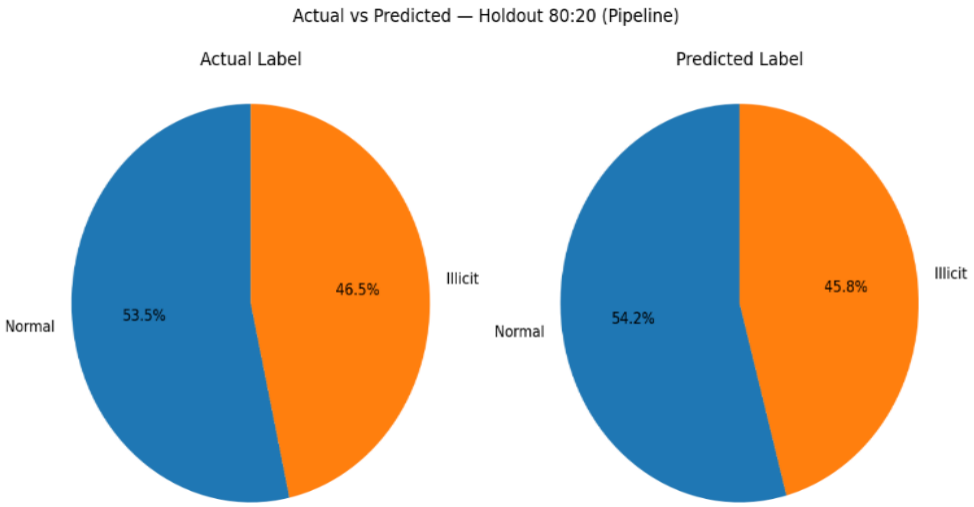
Sepuluh fitur tersebut kemudian diekstraksi dari DataFrame dan disusun menjadi matriks fitur X, sementara kolom FLAG dikonversi menjadi tipe bilangan bulat untuk membentuk vektor target yyy, dengan label 0 mewakili akun normal dan label 1 mewakili akun illicit. Proses ini dilakukan dengan membuat salinan terpisah dari dataset utama untuk mencegah perubahan tidak disengaja pada data asli.

Tabel 3. Hasil Preprocessing Data

Fitur	Kelas Normal	Kelas Illicit
Time_Diff_between_first_and_last_(Mins)	4815.43	704785.63
total_ether_balance	1.752.978.485	5.864.666.748
min_value_received	1	0
min_val_sent	1.000.875	0
avg_val_received	1.348.445	6.589.513
Avg_min_between_received_tnx	34.12	1093.71
Avg_min_between_sent_tnx	1457.31	844.26
Unique_Received_From_Addresses	10	40
max_value_received	2.501.052	45.806.785
avg_val_sent	5.842.916	1.200.681

3.3 Hasil Klasifikasi XGBoost

Klasifikasi aktivitas transaksi dilakukan menggunakan algoritma Extreme Gradient Boosting (XGBoost) yang berdasarkan 10 fitur terpengaruh berdasarkan literatur. Gambar 3 menunjukkan perbandingan distribusi aktual dan prediksi model. Secara Umum, distribusi hasil prediksi menunjukkan kecenderungan yang sejalan dengan distribusi data aktual. Pada data aktual, proporsi transaksi normal sebesar 53,5%, sedangkan transaksi illicit sebesar 46,5%. Hasil prediksi model menghasilkan proporsi yang sangat mendekati, yakni 54,2% untuk kelas normal dan 45,8% untuk kelas illicit.

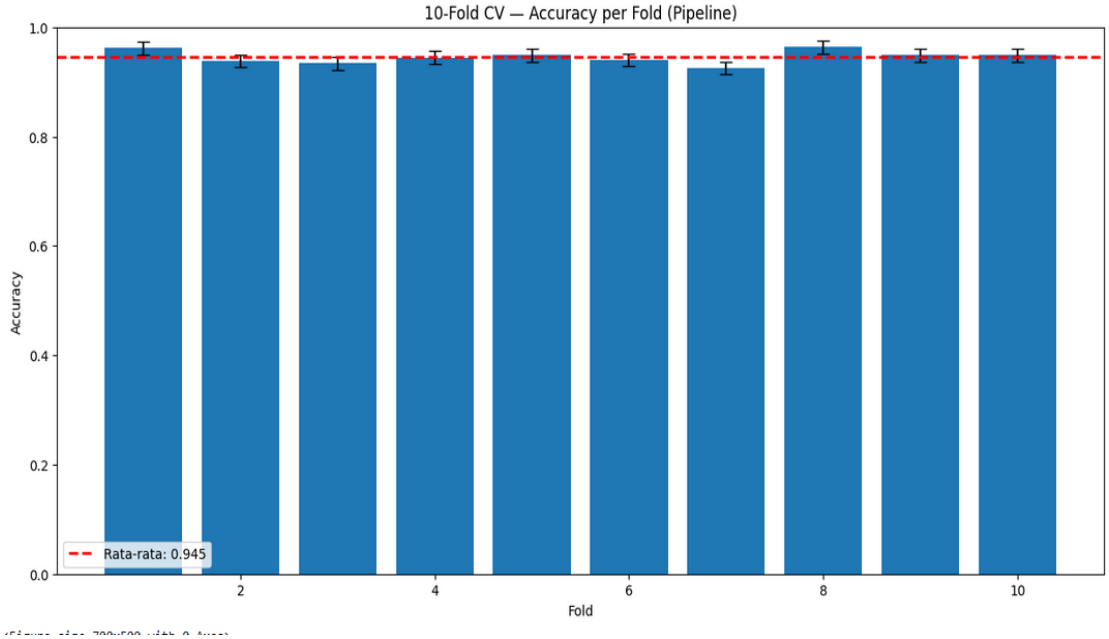


Gambar 2. Hasil Klasifikasi XGBoost

3.4 Hasil Pengujian K-Fold Cross Validation

Evaluasi performa sistem dilakukan menggunakan metode k-fold cross validation sebanyak 10 fold untuk mengukur kemampuan generalisasi model XGBoost terhadap data yang belum pernah dilihat sebelumnya. Gambar 4 memperlihatkan variasi nilai akurasi pada setiap fold selama proses validasi. Hasil

pengujian menunjukkan bahwa model XGBoost menghasilkan tingkat akurasi yang sangat stabil, dengan nilai akurasi pada tiap fold berada di kisaran 0,93 hingga 0,97, serta rata-rata akurasi keseluruhan sebesar 0,945. Nilai akurasi yang konsisten di seluruh fold menunjukkan bahwa model memiliki kemampuan generalisasi yang baik dalam mengenali pola transaksi normal dan illicit.



Gambar 3. Hasil Pengujian K-Fold Cross Validation

3.5 Hasil Pengujian Confusion Matrix

```
Akurasi: 0.9520
Confusion Matrix:
 [[482  19]
 [ 26 410]]
Classification Report (Holdout):
              precision    recall  f1-score   support

      Normal     0.9488    0.9621    0.9554       501
     Illicit     0.9557    0.9404    0.9480       436

    accuracy                         0.9520       937
   macro avg     0.9523    0.9512    0.9517       937
weighted avg     0.9520    0.9520    0.9519       937
```

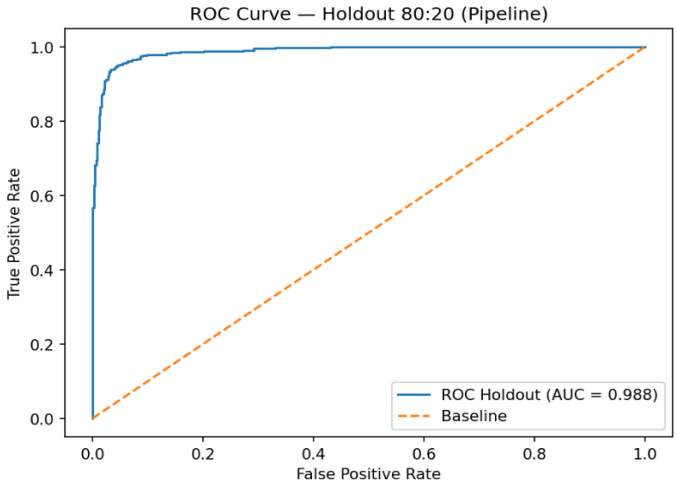
Gambar 4. Hasil Pengujian Confusion Matrix

Hasil evaluasi performa model XGBoost berdasarkan confusion matrix dan classification report. Model memperoleh tingkat akurasi sebesar 95,20% dengan nilai macro average F1-score sebesar 0,9517 dan weighted average F1-score sebesar 0,9519 mengindikasikan bahwa performa model seimbang di antara kedua kelas. Pada kelas Normal, diperoleh nilai precision sebesar 0,9488 dan recall sebesar 0,9621, menghasilkan F1-score sebesar 0,9554. Nilai tersebut menandakan bahwa sebagian besar transaksi normal berhasil dikenali dengan benar, dan hanya sebagian kecil yang keliru diklasifikasikan sebagai illicit. Sementara itu, pada kelas Illicit, model mencapai precision sebesar 0,9557 dan recall sebesar 0,9404, dengan F1-score sebesar 0,9480. Hal ini menunjukkan bahwa model mampu mengenali sebagian besar

transaksi mencurigakan secara akurat, meskipun terdapat beberapa kasus false negative yang terdeteksi sebagai transaksi normal.

3.6 Hasil Pengujian Receiver Operating Characteristic(ROC)

Hasil ROC Curve untuk XGBoost yang diuji menggunakan skema holdout validation dengan rasio pembagian data 80:20. Kurva ROC digunakan untuk mengevaluasi kemampuan model dalam membedakan antara kelas Normal dan Illicit berdasarkan perbandingan antara True Positive Rate (TPR) dan False Positive Rate (FPR) pada berbagai ambang batas klasifikasi. Berdasarkan hasil pengujian, model XGBoost menghasilkan nilai Area Under Curve (AUC) sebesar 0,988, yang menunjukkan performa klasifikasi yang sangat baik. Nilai AUC yang mendekati 1 menandakan bahwa model memiliki kemampuan tinggi dalam membedakan transaksi normal dari transaksi mencurigakan (illicit). Garis diagonal oranye pada grafik merepresentasikan baseline acuan untuk prediksi acak dengan AUC sebesar 0,5.



Gambar 5. Hasil Pengujian ROC

4. Kesimpulan

Penelitian ini menghasilkan model yang berfungsi untuk mendeteksi dan mengklasifikasikan aktivitas pencucian uang pada transaksi cryptocurrency dengan menggabungkan proses preprocessing dan pemodelan ke dalam satu pipeline. Tahapan preprocessing dilakukan menggunakan metode Simple Imputer dengan strategi mean untuk imputasi nilai hilang, sedangkan proses klasifikasi menggunakan algoritma XGBoost dengan fungsi objektif binary:logistic. Fitur yang digunakan terdiri atas sepuluh variabel numerik yang merepresentasikan karakteristik transaksi pada jaringan cryptocurrency. Berdasarkan hasil pengujian dan analisis, sistem memperoleh akurasi rata-rata sebesar 94,53% melalui skema 10-fold cross-validation, dengan akurasi tertinggi mencapai 96,16% dan terendah 92,52%. Pengujian pada data uji menghasilkan akurasi sebesar 95,20%, sedangkan evaluasi menggunakan kurva ROC menunjukkan nilai Area Under Curve (AUC) sebesar 0,988. Nilai AUC yang mendekati 1 menandakan bahwa model memiliki kemampuan yang sangat baik dalam membedakan transaksi Normal dan Illicit, sehingga sistem pipeline XGBoost yang diusulkan terbukti efektif dan andal dalam mendeteksi potensi aktivitas pencucian uang pada ekosistem cryptocurrency.

Referensi

[1] O. Japinye, "Integrating Machine Learning in Anti-Money Laundering through Crypto: A Comprehensive Performance Review," Eur. J. Accounting, Auditing and Finance Research, vol. 12, no. 4, pp. 54–80, Mar. 2024, doi: 10.37745/EJAAFR.2013/VOL12N45480.

[2] E. Godspower-Akpomiemie and K. Ojah, "Money Laundering, Tax Havens and Transparency," Routledge, pp. 248–266, 2022, doi: 10.4324/9781315169477-15.

[3] M. Calafos and G. Dimitoglou, "Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency," in Financial Cybersecurity Risk Management, Springer, 2022, pp. 271–300, doi: 10.1007/978-3-031-10507-4_12.

[4] H. Almeida, P. Pinto, and A. F. Vilas, "A Review on Cryptocurrency Transaction Methods for Money Laundering," Proc. 20th Int. Conf. on Security and Cryptography (SECRYPT), pp. 114–121, 2023, doi: 10.5220/0011993300003494.

[5] A. Guidara, "Cryptocurrency and Money Laundering: A Literature Review," Corporate Law and Governance Review, vol. 4, no. 2, pp. 36–41, 2022, doi: 10.22495/clgrv4i2p4.

[6] A. Singh, J. Shaw, and V. Mishra, "A Systematic Analysis on Cryptocurrencies as a Financial Asset," Proc. IEEE Int. Conf. on Recent Trends in Management, Technology and Innovation (IRTM), 2022, doi: 10.1109/IRTM54583.2022.9791804.

[7] T. Labs, "2025 Crypto Crime Report," Chainalysis, Feb. 2025.

[8] A. Arbabi, A. Shojaeinasab, B. Bahrak, and H. Najjaran, "Mixing Solutions in Bitcoin and Ethereum Ecosystems: A Review and Tutorial," arXiv preprint arXiv:2310.04899, 2023.

[9] N. Pocher, M. Zichichi, F. Merizzi, M. Z. Shafiq, and S. Ferretti, "Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics," Electronic Markets, vol. 33, no. 1, pp. 1–17, 2023, doi: 10.1007/s12525-023-00654-3.

[10] P. Gao, D. Kong, and X. Li, "Implementation and Security Analysis of Cryptocurrencies Based on Ethereum," arXiv preprint arXiv:2504.21367, 2025.

[11] K. L. Du, R. Zhang, B. Jiang, J. Zeng, and J. Lu, "Understanding Machine Learning Principles: Learning, Inference, Generalization, and Computational Learning Theory," Mathematics, vol. 13, no. 3, pp. 1–57, 2025, doi: 10.3390/math13030451.

[12] İ. Kılıç and N. Yalçın, "A Novel Hybrid Methodology Based on Transfer Learning, Machine Learning, and ReliefF for Chickpea Seed Variety Classification," Applied Sciences, vol. 15, no. 3, pp. 1–15, 2025, doi: 10.3390/app15031334.

[13] F. Johannessen and M. Jullum, "Finding Money Launderers Using Heterogeneous Graph Neural Networks," arXiv preprint arXiv:2307.13499, 2023.

[14] T. S. Siddhesh, S. M. Rajagopal, and S. Bhaskaran, "Comparative Analysis of Machine Learning Algorithms for Anomaly Detection," Proc. 2024 IEEE 9th Int. Conf. on Convergence in Technology (I2CT), 2024, doi: 10.1109/I2CT61223.2024.10544217.

[15] S. Farrugia, J. Ellul, and G. Azzopardi, "Detection of Illicit Accounts over the Ethereum Blockchain," Expert Systems with Applications, vol. 150, p. 113318, 2020, doi: 10.1016/j.eswa.2020.113318.

[16] A. R. A. Talwalkar, M. Mohri, and A. Rostamizadeh, Foundations of Machine Learning, 2nd ed., MIT Press, 2018.

[17] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," Proc. 22nd ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining (KDD), pp. 785–794, 2016, doi: 10.1145/2939672.2939785.

[18] S. Q. Sultan, N. Javaid, N. Alrajeh, and M. Aslam, "Machine Learning-Based Stacking Ensemble Model for Prediction of Heart Disease with Explainable AI and K-Fold Cross-Validation: A Symmetric Approach," Symmetry, vol. 17, no. 2, pp. 1–26, 2025, doi: 10.3390/sym17020185.

[19] G. Azzopardi, S. Farrugia, and J. Ellul, "Detection of Illicit Accounts over the Ethereum Blockchain," DataverseNL, doi: 10.34894/GKAQYN.

[20] J. Li, "Area under the ROC Curve Has the Most Consistent Evaluation for Binary Classification," PLoS One, vol. 19, no. 12, Dec. 2024, doi: 10.1371/journal.pone.0316019.

[21] S. Gautam et al., "Performance evaluation of classification algorithms by k-fold and leave-one-out cross validation," Pattern Recognition, vol. 48, no. 9, pp. 2839–2848, 2015.

[22] Evaluation of four machine learning models for signal detection, SAGE Open Medicine, vol. 11, 2023.

[23] J. Han, M. Kamber, and J. Pei, Data Mining: Concepts and Techniques, 4th ed., Morgan Kaufmann, 2023