E-ISSN: 2964-6219, P-ISSN: 2964-6200
Volume 5 Number 1 February 2027.
pp: 1-11. DOI: https://doi.org/10.58477/cj.v5i1.507.

Computer Journal

RESEARCH ARTICLE Open Access

Implementasi *Machine Learning* untuk Deteksi Kejujuran Wakif pada Sistem Wakaf Digital Berbasis *Blockchain*

Rahma Nadiya [1*]

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

Correspondence email:
rahmanadiya1712@gmail.com.

Article History
Received: 2 September 2026.
Revised: 3 September 2026.
Accepted: 27 September 2026.
Available Online: 5 November 2026
Published: 1 February 2027.

Funding Information
Universitas Nusa Mandiri.

Abstract
Digital waqf requires a validation mechanism that not only protects data integrity after storage but also evaluates transaction credibility before the data becomes immutable on a blockchain. This study develops an intelligent pre-validation mechanism through a hybrid architecture integrating a web application, machine learning, a backend API, smart contracts, and blockchain. The dataset combined the Ethereum Fraud Detection Dataset (9,841 transactions and 51 attributes) with transaction and behavioral data from the digital waqf system. Data processing included cleaning, missing-value handling, categorical encoding, StandardScaler normalization, feature engineering, and Isolation Forest anomaly detection. The resulting anomaly score was normalized into a 0–100 trust score and passed to the smart contract to process high-trust transactions, route medium-risk transactions to nazhir review, and block high-risk transactions before on-chain recording. Built using Python, Scikit-learn, PHP, MySQL, Solidity, Ganache, and MetaMask, the prototype demonstrated an end-to-end pre-validation flow from waqif input to on-chain decision-making. Representative tests yielded trust scores of 92 (normal), 68 (review), and 27 (fraud), showing that separating off-chain inference from on-chain validation provides an effective control layer against garbage in, garbage out without imposing machine learning computation on the smart contract.

Keywords: Digital Waqf; Blockchain; Machine Learning; Isolation Forest; Smart Contract; Trust Score; Intelligent Pre-Validation.

Abstrak
Digitalisasi wakaf memerlukan mekanisme yang tidak hanya menjamin integritas data setelah tersimpan, tetapi juga menilai kredibilitas transaksi sebelum memperoleh sifat *immutable* pada *blockchain*. Penelitian ini mengembangkan mekanisme *intelligent pre-validation* melalui arsitektur *hybrid* yang mengintegrasikan aplikasi web, *machine learning*, *backend* API, *smart contract*, dan *blockchain*. Data penelitian menggabungkan karakteristik *Ethereum Fraud Detection Dataset* (9.841 transaksi dan 51 atribut) dengan data transaksi serta *behavioral data* dari sistem wakaf digital. Pengolahan data mencakup *data cleaning*, penanganan *missing value*, *categorical encoding*, normalisasi StandardScaler, *feature engineering*, dan deteksi anomali menggunakan Isolation Forest. *Anomaly score* yang dihasilkan dinormalisasi menjadi *trust score* (0–100) sebagai parameter keputusan *smart contract* untuk memproses transaksi berkepercayaan tinggi, mengarahkan transaksi berisiko sedang ke *review* nazhir, dan menghentikan transaksi berisiko tinggi sebelum pencatatan *blockchain*. Prototipe yang dibangun menggunakan Python, Scikit-learn, PHP, MySQL, Solidity, Ganache, dan MetaMask ini berhasil menjalankan alur *pre-validation* dari input wakif hingga keputusan *on-chain*. Pengujian representatif menghasilkan *trust score* 92 (normal), 68 (*review*), dan 27 (*fraud*). Hasil ini membuktikan bahwa pemisahan inferensi *off-chain* dan validasi *on-chain* mampu membentuk lapisan kontrol untuk menekan risiko *garbage in, garbage out* tanpa membebani *smart contract* dengan komputasi *machine learning*.

Kata Kunci: Wakaf Digital; Blockchain; Machine Learning; Isolation Forest; Smart Contract; Trust Score; Intelligent Pre-Validation.

© 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

Pemanfaatan teknologi digital pada filantropi Islam telah mengubah cara penghimpunan, pengelolaan, verifikasi, dan pelaporan aset wakaf. Platform digital memungkinkan wakif melakukan registrasi, memasukkan informasi aset, mengunggah dokumen, mengajukan transaksi, serta memantau status wakaf tanpa harus hadir secara fisik. Transformasi tersebut membuka peluang untuk memperluas akses masyarakat, mempercepat layanan, dan meningkatkan akuntabilitas pengelolaan. Namun, digitalisasi juga memperluas celah risiko. Semakin banyak proses yang dipindahkan ke kanal elektronik, semakin penting kemampuan sistem untuk memastikan bahwa data identitas, dokumen, nominal, aktivitas transaksi, dan pola interaksi pengguna mempunyai tingkat kredibilitas yang memadai sebelum diproses lebih jauh (Adinugraha *et al.*, 2024; Amaliyah *et al.*, 2022; Maisyarah & Hadi, 2024). *Blockchain* banyak dipertimbangkan untuk memperkuat tata kelola wakaf digital karena mempunyai sifat *distributed ledger*, transparansi, *traceability*, dan *immutability*. Data yang telah divalidasi dan dicatat ke jaringan sulit diubah secara sepihak sehingga riwayat transaksi dapat diaudit secara lebih konsisten. Kajian terkait penggunaan *blockchain* untuk keberlanjutan wakaf tunai menekankan potensi teknologi tersebut dalam meningkatkan transparansi, akuntabilitas, dan efisiensi (Anwar *et al.*, 2024; Nasywa & Lahuri, 2025). Pemanfaatan *smart contract* juga memperkuat otomatisasi proses bisnis karena aturan dapat dieksekusi secara konsisten ketika kondisi yang telah ditentukan terpenuhi (Setiawan & Nurjaman, 2022). Di sisi lain, integrasi *blockchain* dan kecerdasan buatan mulai dikembangkan pada sektor keuangan Islam untuk memperluas fungsi analitik dan mendukung pengambilan keputusan berbasis data (Hamzah *et al.*, 2025; Mukit *et al.*, 2026).

Keunggulan *blockchain* tersebut tetap menyisakan persoalan mendasar: *blockchain* menjamin integritas data setelah pencatatan, tetapi tidak secara otomatis menjamin kebenaran atau kredibilitas data sebelum pencatatan. Apabila data yang salah, manipulatif, atau tidak wajar lolos pada tahap awal, sifat *immutable* justru membuat kesalahan menjadi lebih sulit dikoreksi. Kondisi ini dikenal melalui prinsip *garbage in, garbage out*, yang menunjukkan bahwa mekanisme penyimpanan yang kuat tidak serta-merta menyelesaikan masalah kualitas masukan. Pada konteks wakaf digital, validitas masukan sangat penting karena transaksi melibatkan identitas wakif, informasi aset, nominal, tujuan wakaf, dokumen legal, dan metadata transaksi yang kemudian menjadi dasar pengelolaan aset serta pertanggungjawaban lembaga (Hamzah *et al.*, 2025; Kunhibava *et al.*, 2024). Praktik verifikasi yang hanya mengandalkan pemeriksaan manual oleh nazhir atau administrator juga memiliki keterbatasan. Pemeriksaan dokumen satu per satu dapat menimbulkan ketergantungan tinggi pada operator, variasi keputusan, risiko *human error*, dan potensi keterlambatan ketika volume transaksi meningkat. Verifikasi manual juga kurang efektif untuk menangkap pola perilaku digital yang tidak tampak dari dokumen, misalnya durasi pengisian formulir yang tidak wajar, perubahan data berulang, penggunaan perangkat tertentu, pola akses berdasarkan alamat IP, atau intensitas transaksi yang menyimpang. Sebaliknya, menyerahkan seluruh validasi kepada *smart contract* juga belum memadai karena *smart contract* pada dasarnya mengeksekusi aturan deterministik yang sudah diprogram dan tidak dirancang untuk menemukan pola anomali baru secara adaptif (Feng *et al.*, 2023; Mustagfiroh & Khoirina, 2025).

Kebutuhan tersebut mengarah pada arsitektur *hybrid* yang memisahkan analisis cerdas dari eksekusi *blockchain*. Proses *machine learning* ditempatkan pada lingkungan *off-chain* agar dapat mengolah fitur transaksi dan *behavioral data* dengan biaya komputasi yang lebih efisien. Hasil analisis tidak langsung dipakai sebagai keputusan final, melainkan dikonversi menjadi *trust score* yang mewakili tingkat kepercayaan terhadap transaksi dan diteruskan melalui *backend* API ke *smart contract*. Selanjutnya, *smart contract* menggunakan nilai tersebut untuk menentukan apakah transaksi dapat diterima, harus diperiksa manual oleh nazhir, atau perlu dihentikan sebelum data masuk ke *blockchain* (Hamzah *et al.*, 2025; Mukit *et al.*, 2026). Pemilihan algoritma Isolation Forest dalam arsitektur ini didasarkan pada karakteristik masalah deteksi anomali, mengingat data *fraud* pada domain wakaf digital belum tersedia secara melimpah dan pola penyimpangan dapat berubah dari waktu ke waktu. Isolation Forest mengidentifikasi observasi yang mudah diisolasi melalui *random isolation tree*, di mana transaksi yang lebih cepat terpisah dari mayoritas data memperoleh indikasi anomali lebih tinggi. Pendekatan ini relevan untuk membentuk mekanisme *pre-validation* secara *off-chain* karena fokusnya bukan semata-mata mengklasifikasikan *fraud* yang sudah dikenal, melainkan menyaring transaksi berkarakteristik menyimpang sebelum hasil inferensinya dikirim ke lingkungan *on-chain* untuk pencatatan permanen (Amirillah, 2025; Vanini *et al.*, 2023; Wibawa & Karyawati, 2023). Kontribusi penelitian ini terletak pada penggunaan *trust score* sebagai penghubung antara hasil *anomaly detection* dan keputusan *smart contract* sebelum transaksi memperoleh sifat *immutable*. Dengan mekanisme tersebut, *blockchain* berfungsi sebagai lapisan integritas dan audit, sedangkan *machine learning* berfungsi sebagai lapisan analitik yang bekerja tanpa membebani *smart contract* dengan kompleksitas dan

biaya eksekusi inferensi (Hasan *et al.*, 2024; Sabharwal *et al.*, 2025). Berdasarkan landasan tersebut, penelitian ini bertujuan mengimplementasikan mekanisme *intelligent pre-validation* pada sistem wakaf digital berbasis *blockchain*, membangun model Isolation Forest untuk menghasilkan *anomaly score* dan *trust score*, mengintegrasikan hasil inferensi melalui *backend* API ke *smart contract*, serta memverifikasi alur penyimpanan transaksi yang disetujui ke jaringan Ethereum lokal. Evaluasi implementasi difokuskan pada keterhubungan antarkomponen, konsistensi logika keputusan, representasi hasil prediksi, serta kemampuan sistem mencegah transaksi berisiko tinggi masuk ke *blockchain* sebelum proses verifikasi selesai.

2. Metode

Penelitian ini menggunakan pendekatan pengembangan prototipe sistem dengan pengujian terintegrasi terhadap komponen aplikasi web, *machine learning*, *backend* API, *smart contract*, *blockchain*, dan *monitoring dashboard*. Alur kerja dibangun sebagai mekanisme *end-to-end*, dimulai ketika wakif mengirimkan data melalui antarmuka web, kemudian *backend* melakukan validasi format dan penyimpanan sementara sebelum modul *machine learning* memproses fitur transaksi. Hasil inferensi selanjutnya dikonversi menjadi *trust score* dan diteruskan oleh *backend* ke *smart contract* untuk menentukan status transaksi, di mana transaksi yang memenuhi kriteria persetujuan langsung dicatat ke *blockchain*, sedangkan transaksi berisiko menengah diarahkan ke nazhir untuk *review* manual. Untuk mendukung alur tersebut, arsitektur sistem dibagi menjadi lingkungan *off-chain* (mencakup aplikasi web, basis data, *preprocessing*, *feature engineering*, model Isolation Forest, dan *backend* API) serta lingkungan *on-chain* (mencakup *smart contract* dan *blockchain* Ethereum lokal). Pembagian ini dipilih karena inferensi *machine learning* memerlukan operasi numerik dan pengolahan data yang tidak efisien jika dijalankan langsung pada *blockchain*, sehingga *smart contract* dipertahankan sebagai komponen deterministik yang menerima parameter hasil inferensi dan mengeksekusi aturan keputusan secara konsisten. Pada sisi *user layer*, wakif berinteraksi langsung dengan aplikasi untuk melakukan registrasi, pengisian identitas, input informasi aset, penentuan nominal, pengunggahan dokumen, dan pemantauan status transaksi. Selain data eksplisit tersebut, aplikasi mencatat *behavioral data* secara otomatis, termasuk waktu akses, alamat IP, perangkat, pola navigasi, dan frekuensi perubahan data, sehingga sistem tidak hanya menilai apa yang diinput pengguna, tetapi juga bagaimana proses input dilakukan. Interaksi ini didukung oleh *web application layer* yang terdiri atas *frontend*, *backend server*, dan basis data. *Frontend* menyediakan formulir registrasi, formulir data wakaf, fitur *upload* dokumen, dan *dashboard* status, sedangkan basis data menyimpan data pengguna, transaksi, dokumen, serta log aktivitas. Adapun *backend* menjalankan autentikasi, otorisasi, validasi format, penyimpanan sementara, pengelolaan transaksi, serta mengubah data transaksi dan metadata perilaku ke struktur JSON agar pertukaran data antarkomponen dengan modul *machine learning* dan *blockchain* dapat dilakukan secara konsisten (Baiquni & Dirgahayu, 2023).

Machine learning layer ditempatkan secara *off-chain* sebagai pusat analisis kualitas transaksi yang menjalankan *preprocessing*, *feature engineering*, dan *inference*. Setelah data dibersihkan, ditransformasikan, dan dinormalisasi, data dipetakan ke fitur yang mewakili karakteristik transaksi dan perilaku pengguna untuk dianalisis menggunakan algoritma Isolation Forest melalui pembentukan *isolation tree* guna mencari observasi yang mudah dipisahkan dari mayoritas data (Amirillah, 2025; Ayudewi & Rafifah, 2026). Keluaran dari lapisan ini diteruskan ke *backend* API dan *trust score engine* yang berfungsi sebagai *middleware* penghubung antara situs web, model, dan *smart contract*. Setelah menerima *anomaly score*, *trust score*, dan *prediction label*, *backend* membentuk *payload* JSON yang memuat *Transaction ID*, *Wallet Address*, *Trust Score*, *Prediction*, dan *Timestamp*, lalu memanggil fungsi *smart contract* melalui pustaka Web3.js atau Ethers.js. Dengan pola ini, situs web tidak berkomunikasi langsung dengan *blockchain*, dan layanan *machine learning* dapat diperbarui secara fleksibel tanpa memindahkan proses numerik kompleks ke jaringan *on-chain*. Pada lingkungan *on-chain*, *smart contract layer* dikembangkan menggunakan bahasa Solidity dan dijalankan pada jaringan Ethereum lokal melalui Ganache dengan MetaMask sebagai dompet digital pengujian. *Smart contract* tidak menjalankan Isolation Forest, tidak membaca dataset, dan tidak melakukan *preprocessing*, melainkan menerjemahkan *trust score* menjadi status operasional berdasarkan aturan bisnis yang ditetapkan, mengeluarkan *event* transaksi, serta memastikan hanya transaksi tervalidasi yang berlanjut ke pencatatan. Transaksi yang telah disetujui kemudian disimpan secara permanen pada *blockchain layer* dalam bentuk *transaction hash*, *wallet address*, *timestamp*, *block number*, status *smart contract*, dan metadata transaksi terkait sebagai jejak audit yang bersifat *immutable* dan *traceable*. Seluruh status transaksi, distribusi hasil keputusan, riwayat pembayaran atau proses, serta informasi operasional selanjutnya disajikan melalui *monitoring dashboard* bagi administrator dan nazhir. Data transaksi yang digunakan dalam penelitian ini berasal dari dua sumber. Sumber pertama adalah *Ethereum Fraud Detection Dataset* dari Kaggle yang digunakan sebagai referensi karakteristik transaksi *blockchain*, terdiri atas 9.841 transaksi dengan

51 atribut yang mencakup *sent transaction*, *received transaction*, *average time between transaction*, *balance*, aktivitas token ERC20, pembuatan *smart contract*, dan atribut FLAG. Sumber kedua adalah data yang dihasilkan oleh sistem wakaf digital, meliputi identitas wakif, jenis wakaf, nominal, waktu transaksi, *wallet address*, dokumen pendukung, durasi pengisian formulir, frekuensi perubahan data, *device fingerprint*, alamat IP, dan pola aktivitas pengguna. Integrasi kedua sumber tersebut dilakukan melalui *feature mapping* dan *feature engineering* untuk memilih karakteristik yang dapat direpresentasikan secara konsisten pada kedua domain. *Wallet address* dipetakan dengan *wallet* wakif, *transaction timestamp* dengan waktu transaksi, *total transaction* dengan frekuensi transaksi wakaf, sedangkan *average time between transaction* dipadankan dengan durasi pengisian formulir sebagai *behavioral time*, sebagaimana disajikan pada Tabel 1. Selain itu, fitur tambahan dibentuk untuk menggambarkan konsistensi identitas, intensitas transaksi, perubahan data, lokasi akses, perangkat, dan pola interaksi.

Tabel 1. Feature Mapping Dataset

Ethereum Fraud Detection Dataset	Sistem Wakaf Digital	Fitur Penelitian
Wallet Address	Wallet Wakif	Wallet Address
Transaction Timestamp	Waktu Transaksi	Transaction Time
Total Transaction	Frekuensi Transaksi Wakaf	Transaction Frequency
Average Time Between Transaction	Durasi Pengisian Formulir	Behavioral Time

Sebelum pemodelan dilakukan, data melewati tahapan *data cleaning* untuk menghapus duplikasi dan memperbaiki inkonsistensi, penanganan *missing value*, transformasi atribut kategorikal menjadi numerik, pemilihan fitur, serta normalisasi atribut numerik menggunakan StandardScaler. Tahap normalisasi ini diperlukan karena dataset menggabungkan atribut transaksi dan atribut perilaku yang memiliki rentang nilai berbeda, sehingga penyamaan skala menjaga agar pembentukan *isolation tree* tidak didominasi oleh perbedaan rentang numerik antarfitur. Selanjutnya, model dikembangkan menggunakan Python, Pandas, NumPy, Scikit-learn, dan Joblib dengan konfigurasi Isolation Forest berupa n_estimators sebesar 300 dan random_state sebesar 42, sedangkan parameter contamination dikalibrasi berdasarkan proporsi *fraud* pada data referensi pelatihan (fraud_ratio). Melalui konfigurasi tersebut, proses *fitting* membangun pola isolasi dari data, sementara parameter contamination memberikan estimasi proporsi observasi yang diperlakukan sebagai anomali untuk menghasilkan *anomaly score* pada setiap transaksi.

Anomaly score yang dihasilkan model kemudian ditransformasikan menjadi *trust score* pada rentang 0–100 dengan arah interpretasi yang berlawanan terhadap tingkat anomali: semakin tinggi nilai *trust score*, semakin dekat karakteristik transaksi dengan pola normal, dan sebaliknya. Transformasi ke rentang 0–100 dipilih agar hasil model mudah dipahami oleh pengelola dan dapat digunakan langsung sebagai parameter keputusan *smart contract*. Dalam implementasi pengambilan keputusan tiga tingkat, *trust score* minimal 80 (ge 80) menghasilkan status *Approve* yang meneruskan transaksi ke pencatatan *blockchain*, rentang nilai 50–79 menghasilkan status *Review* yang mengalihkan transaksi ke verifikasi manual oleh nazhir sebelum keputusan akhir, sedangkan nilai di bawah 50 (< 50) menghasilkan status *Reject* yang menghentikan alur transaksi. Mekanisme ini memastikan bahwa *machine learning* dapat menyaring risiko secara otomatis sambil tetap mempertahankan peran manusia pada transaksi yang berada di area abu-abu. Rancangan evaluasi sistem mencakup pengujian performa model (*accuracy, precision, recall, F1-score,* dan ROC-AUC), distribusi *trust score*, *confusion matrix*, *success rate* dan *execution time* pada *smart contract*, *gas used*, *gas fee*, *transaction latency*, *throughput*, serta pengujian *black box* dan *white box*, sebagaimana dirinci pada Tabel 2. Pendekatan evaluasi yang menggabungkan kinerja model *machine learning* dengan aspek keamanan dan proses transaksi *blockchain* ini mengacu pada pengembangan mekanisme *fraud detection* terintegrasi (Ashfaq *et al.*, 2022). Pada pelaporan implementasi prototipe ini, evaluasi difokuskan pada verifikasi fungsional integrasi antarkomponen dan pengujian representatif keluaran prediksi.

Tabel 2. Skenario Pengujian Penelitian

No	Komponen yang Diuji	Tujuan Pengujian	Metrik yang Diukur	Hasil yang Diharapkan
1	Model *Machine Learning* (Isolation Forest)	Mengukur kemampuan model dalam mendeteksi transaksi anomali sebelum transaksi diproses lebih lanjut.	*Accuracy, Precision, Recall, F1-Score,* ROC-AUC	Model mampu mengidentifikasi transaksi normal dan anomali secara konsisten dengan tingkat akurasi yang tinggi.
2	*Trust Score*	Mengevaluasi kemampuan model dalam	Distribusi *Trust Score*, *Confusion*	*Trust score* mampu merepresentasikan tingkat

		menghasilkan *trust score* berdasarkan karakteristik transaksi dan perilaku pengguna.	*Matrix*	kepercayaan terhadap transaksi dan membedakan transaksi normal dari transaksi berisiko.
3	*Smart Contract*	Menguji mekanisme validasi otomatis berdasarkan *trust score* yang diterima dari modul *machine learning*.	*Success Rate, Execution Time, Gas Used*	*Smart contract* mampu menjalankan fungsi *Approve*, *Review*, dan *Reject* sesuai nilai *threshold* yang telah ditentukan.
4	*Blockchain*	Mengukur performa pencatatan transaksi ke *blockchain* setelah proses validasi selesai dilakukan.	*Gas Fee, Transaction Latency, Throughput*	Transaksi berhasil dicatat secara permanen dengan waktu eksekusi dan biaya transaksi yang efisien.
5	Sistem secara Keseluruhan	Memastikan seluruh modul sistem dapat berjalan sesuai kebutuhan fungsional dan logika sistem.	*Black Box Testing, White Box Testing*	Seluruh fungsi sistem dapat berjalan dengan baik serta integrasi antarkomponen berlangsung tanpa kesalahan.

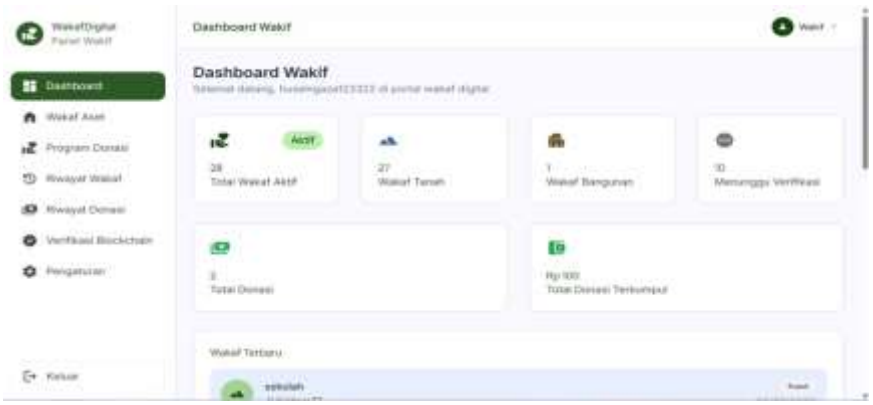
3. Hasil dan Pembahasan

3.1 Hasil

Prototipe sistem wakaf digital mengintegrasikan aplikasi web, modul machine learning, backend API, smart contract, dan blockchain dalam satu mekanisme intelligent pre-validation. Situs web yang dikembangkan menggunakan PHP dan MySQL berfungsi sebagai antarmuka utama bagi wakif, nazhir, dan administrator. Alur interaksi diawali pada halaman login sebagaimana ditunjukkan pada Gambar 1, yang menjadi gerbang autentikasi sebelum pengguna memperoleh akses ke sistem. Pengguna memasukkan alamat email dan kata sandi yang telah terdaftar untuk diverifikasi terhadap basis data pengguna. Setelah autentikasi berhasil, pengguna diarahkan ke halaman dashboard utama (Gambar 2) sesuai perannya guna membatasi akses terhadap fungsi transaksi dan pengelolaan data. Pada sisi wakif, dashboard menampilkan ringkasan aset atau transaksi wakaf, status transaksi, riwayat wakaf, serta pintasan untuk mengajukan transaksi baru, sedangkan pada sisi nazhir dan administrator, halaman ini berfungsi sebagai pusat pemantauan transaksi, verifikasi, distribusi status, dan kondisi operasional sistem.



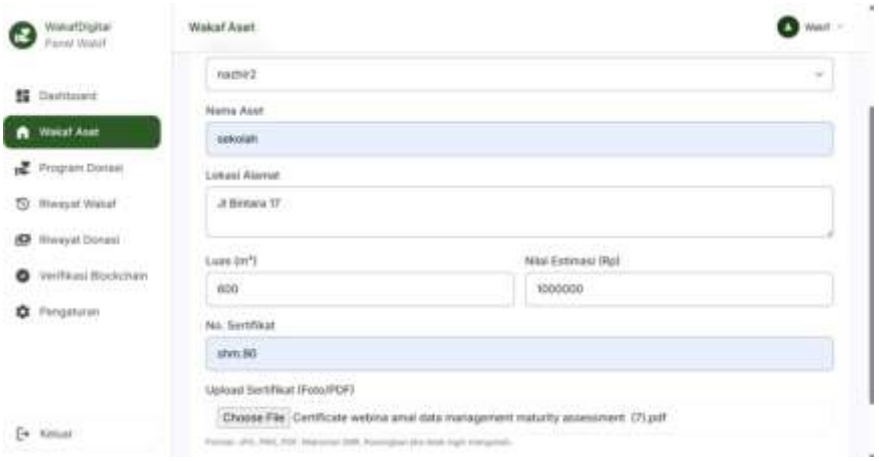
Gambar 1. Halaman Login



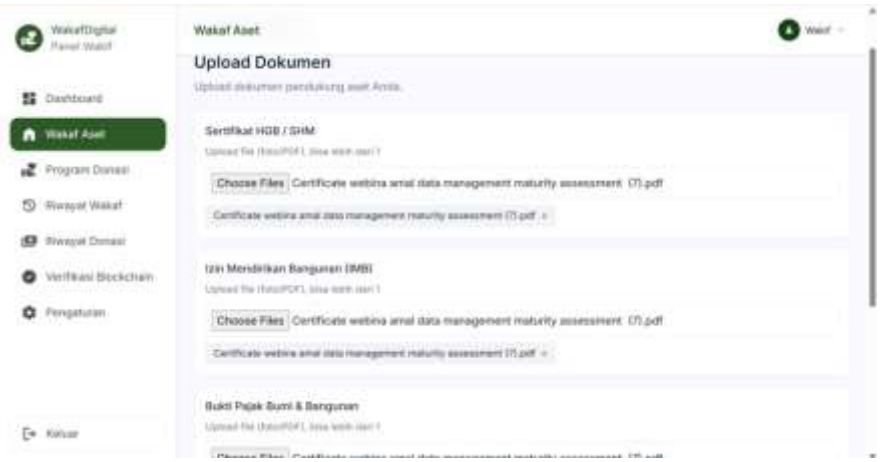
Gambar 2. Halaman Dashboard

Pengajuan wakaf baru dilakukan melalui halaman formulir transaksi wakaf yang ditampilkan pada Gambar 3. Formulir ini mengumpulkan informasi utama seperti identitas wakif, jenis aset, nominal, tujuan wakaf, lokasi aset, serta informasi pendukung lainnya. Selama wakif mengisi formulir tersebut, aplikasi secara simultan merekam behavioral data yang mencakup durasi pengisian, frekuensi perubahan data, perangkat yang digunakan, dan lokasi akses sebagai masukan pada tahap feature engineering bagi model Isolation

Forest. Selanjutnya, untuk melengkapi persyaratan administratif, wakif mengunggah dokumen pendukung seperti identitas diri, bukti kepemilikan aset, atau sertifikat tanah melalui halaman upload dokumen pada Gambar 4. Seluruh dokumen disimpan pada peladen (server) aplikasi dan dikaitkan dengan ID transaksi yang bersangkutan, sehingga dapat digunakan oleh nazhir untuk melakukan pemeriksaan mendalam apabila transaksi memperoleh status Review.



Gambar 3. Halaman Formulir Transaksi Wakaf



Gambar 4. Halaman Upload Dokumen

Modul machine learning yang diimplementasikan menggunakan Python, Scikit-learn, Pandas, dan NumPy menjalankan proses intelligent pre-validation secara off-chain, sebagaimana ditunjukkan pada Gambar 5. Berdasarkan hasil penggabungan dan prapemrosesan data transaksi aplikasi dengan Ethereum Fraud Detection Dataset (melalui data cleaning, penanganan missing value, encoding atribut kategorikal, normalisasi StandardScaler, dan feature engineering), model Isolation Forest yang dikonfigurasi dengan n_estimators sebesar 300, random_state sebesar 42, dan contamination sesuai rasio fraud data referensi menghasilkan anomaly score untuk setiap transaksi. Nilai tersebut kemudian dikonversi menjadi trust score pada rentang 0–100 sebagai parameter keputusan. Hasil pengujian prediksi terhadap tiga sampel transaksi representatif disajikan pada Tabel 3.



Gambar 5. Implementasi Model Machine Learning

Tabel 3. Hasil Prediksi Model Isolation Forest

Transaction ID	Anomaly Score	Trust Score	Prediction
TX20260001	-0,31	92	Normal
TX20260002	0,12	68	Review
TX20260003	0,45	27	Fraud

Sebagaimana terlihat pada Tabel 3, pengujian menghasilkan tiga pola keputusan yang berbeda. Transaksi TX20260001 memperoleh *anomaly score* −0,31 dan *trust score* 92 sehingga dikategorikan *Normal*. Transaksi TX20260002 memiliki *anomaly score* 0,12 dan *trust score* 68 sehingga dikategorikan ke dalam *Review*, sedangkan transaksi TX20260003 memperoleh *anomaly score* 0,45 dan *trust score* 27 sehingga terindikasi sebagai *Fraud*. Hasil ini memperlihatkan fungsi *trust score* sebagai lapisan interpretasi yang menerjemahkan keluaran numerik model menjadi kategori risiko operasional. Keluaran dari modul *machine learning* tersebut selanjutnya diproses oleh *backend* API yang diimplementasikan sebagaimana tampak pada Gambar 6. Setelah menerima *anomaly score*, *trust score*, dan label prediksi, *backend* API menyusun *payload* berformat JSON yang memuat *Transaction ID*, *Wallet Address*, *Trust Score*, *Prediction*, dan *Timestamp*, lalu meneruskannya ke *smart contract* melalui pustaka Web3.js atau Ethers.js. Pada sisi *on-chain*, *smart contract* berbasis Solidity yang dijalankan pada jaringan Ethereum lokal Ganache (Gambar 7) mengeksekusi validasi otomatis dengan membandingkan *trust score* terhadap ambang batas (*threshold*) keputusan: nilai ≥80 (prediksi *Normal*) menghasilkan status *Approve*, rentang 50–79 menghasilkan status *Review*, dan nilai <50 (prediksi *Fraud*) menghasilkan status *Reject*.



Gambar 6. Implementasi Backend API

```
function approvePemerintah(bytes32 refId, bytes32 finalDataHash) external onlyAdmin {
    require(wakafExists[refId], "Record not found");
    require(wakafRecords[refId].approvalNazhirHash != bytes32(0), "Nazhir not approved");

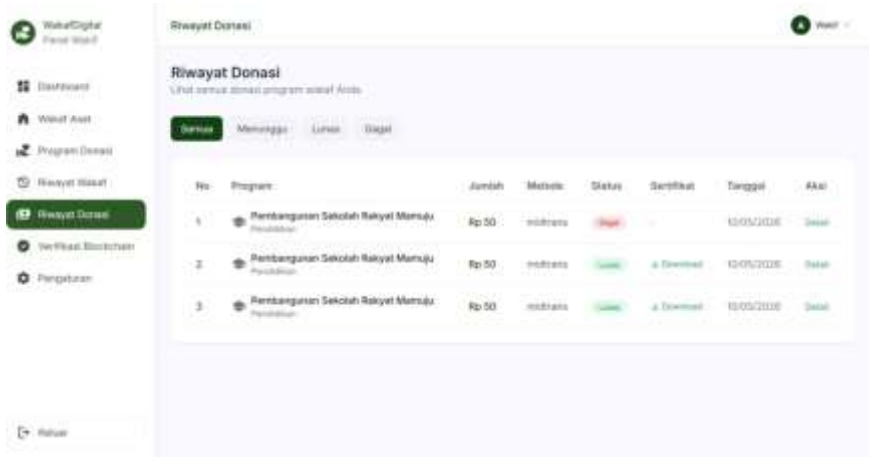
    wakafRecords[refId].approvalPemerintahHash = finalDataHash;
    wakafRecords[refId].pemerintahApprovedAt = block.timestamp;
    wakafRecords[refId].status = Status.ON_CHAIN;

    emit WakafApprovedPemerintah(refId, finalDataHash, block.timestamp);
}
```

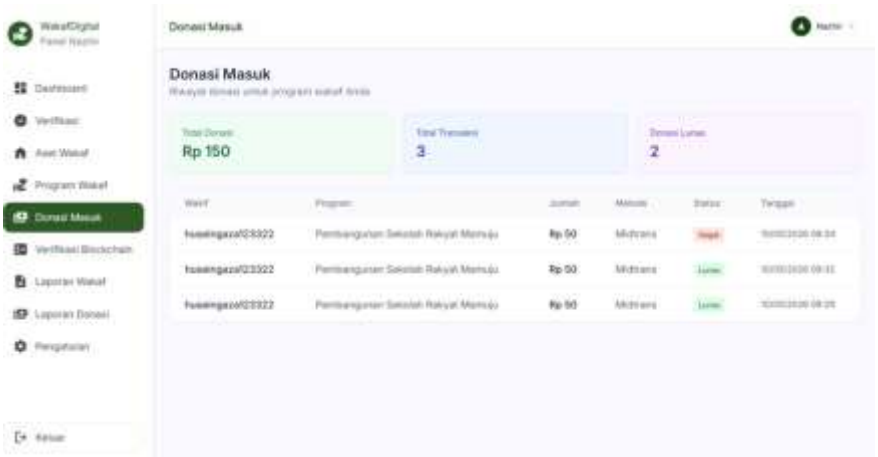
Gambar 7. Implementasi Smart Contract

Transaksi yang memperoleh status Approve dari smart contract langsung diteruskan ke jaringan Ethereum lokal menggunakan Ganache dan dompet digital MetaMask untuk pencatatan permanen, seperti ditunjukkan pada Gambar 8, sementara transaksi berstatus Review ditahan untuk verifikasi nazhir dan transaksi Reject dihentikan sebelum masuk ke ledger. Pencatatan pada blockchain menghasilkan jejak audit berupa transaction hash, wallet address, timestamp, block number, status transaksi, dan metadata terkait yang bersifat immutable, transparan, dan dapat ditelusuri kembali (traceable). Seluruh rangkaian proses dan

status akhir transaksi tersebut kemudian divisualisasikan secara real-time melalui halaman monitoring dashboard pada Gambar 9. Antarmuka pemantauan ini menampilkan total donasi, jumlah keseluruhan transaksi, jumlah donasi yang berhasil diproses, serta daftar rincian transaksi (nama wakif, program wakaf, nominal donasi, metode pembayaran, status, dan waktu transaksi) guna mendukung evaluasi operasional oleh nazhir dan administrator.



Gambar 8. Implementasi Blockchain



Gambar 9. Halaman Monitoring Dashboard.

3.2 Pembahasan

Hasil implementasi memperlihatkan bahwa mekanisme validasi transaksi wakaf digital dapat didistribusikan secara efektif ke dalam tiga lapisan fungsional: aplikasi web untuk autentikasi serta perekaman data transaksi dan perilaku; lingkungan off-chain untuk deteksi anomali menggunakan Isolation Forest dan perhitungan trust score; serta lingkungan on-chain untuk eksekusi keputusan smart contract sebelum pencatatan ke blockchain. Keunggulan utama arsitektur ini terletak pada penempatan deteksi anomali di tahap pra-pencatatan. Blockchain tetap berperan menjaga integritas data pascapenyimpanan, tetapi setiap data yang akan masuk ke ledger harus melewati penyaringan berbasis pola transaksi dan perilaku pengguna terlebih dahulu. Dengan demikian, risiko garbage in, garbage out dapat ditekan karena transaksi berisiko tinggi langsung dihentikan sebelum memperoleh sifat immutable (Anwar *et al.*, 2024; Hasan *et al.*, 2024). Selain itu, penempatan inferensi pada lingkungan off-chain menjaga efisiensi sistem secara keseluruhan. Mengingat proses machine learning membutuhkan komputasi numerik yang tidak sesuai untuk dijalankan pada smart contract yang deterministik dan sensitif terhadap biaya eksekusi (gas), penggunaan backend API yang hanya mengirimkan trust score dan status prediksi mampu mempertahankan ketajaman analitis model tanpa membebani jaringan blockchain (Mukit *et al.*, 2026; Vanini *et al.*, 2023). Secara konseptual, trust score berfungsi sebagai jembatan antara model statistik dan aturan bisnis karena nilainya mudah diinterpretasikan oleh pengelola sekaligus dapat dieksekusi secara deterministik oleh smart contract. Penerapan kategori Review pada skor menengah (50–79) juga memastikan terjaganya prinsip human-in-the-loop, di mana transaksi di area abu-abu tidak langsung ditolak sebagai fraud, melainkan

diverifikasi ulang oleh nazhir melalui pemeriksaan dokumen dan identitas pendukung. Dalam konteks ini, istilah "deteksi kejujuran" pada sistem perlu dipahami sebagai penilaian atas kredibilitas pola transaksi dan kewajaran perilaku interaksi digital, bukan pengukuran atas niat atau karakter moral wakif secara personal. Oleh karena itu, keluaran Isolation Forest berfungsi sebagai indikator risiko objektif untuk mendukung ketepatan validasi lembaga, bukan sebagai vonis absolut terhadap individu.

Pengujian prototipe yang terdokumentasi telah membuktikan keterhubungan fungsional antarkomponen mulai dari aplikasi web, model machine learning, backend API, smart contract, jaringan blockchain lokal, hingga monitoring dashboard, sebagaimana ditunjukkan melalui variasi hasil pengujian trust score. Meskipun demikian, evaluasi pada tahap prototipe ini masih berfokus pada pembuktian konsep (proof-of-concept) alur end-to-end dan belum mencakup pengukuran komparatif secara menyeluruh terhadap metrik kinerja klasifikasi (accuracy, precision, recall, F1-score, dan ROC-AUC) maupun metrik performa jaringan (gas fee, latency, dan throughput) pada skala produksi. Oleh sebab itu, penelitian selanjutnya dapat diarahkan untuk memperluas pengujian pada jaringan blockchain publik (testnet atau mainnet), membandingkan kinerja Isolation Forest dengan algoritma deteksi anomali lainnya, mengintegrasikan metode explainable artificial intelligence (XAI) seperti SHAP atau LIME untuk meningkatkan transparansi alasan penolakan transaksi, serta menerapkan continuous learning menggunakan data riil dari berbagai lembaga wakaf guna menguji kemampuan generalisasi model terhadap pola transaksi yang dinamis (Černevičienė & Kabašinskas, 2024; Sabharwal *et al.*, 2025).

4. Kesimpulan

Hasil implementasi menunjukkan bahwa mekanisme *intelligent pre-validation* dapat diterapkan pada sistem wakaf digital melalui arsitektur *hybrid* yang mengintegrasikan aplikasi web, algoritma Isolation Forest, *backend* API, *smart contract*, dan *blockchain*. Dalam arsitektur ini, data transaksi dan *behavioral data* diproses pada lingkungan *off-chain* untuk menghasilkan *anomaly score* yang dinormalisasi menjadi *trust score* (0–100) sebagai dasar pengambilan keputusan *smart contract* sebelum transaksi dicatat secara permanen. Penerapan mekanisme keputusan tiga tingkat memungkinkan transaksi berkepercayaan tinggi langsung diproses, transaksi berisiko sedang diarahkan ke *review* nazhir, dan transaksi berisiko tinggi dihentikan, sebagaimana dibuktikan melalui pengujian representatif yang menghasilkan *trust score* 92 untuk transaksi normal, 68 untuk transaksi yang memerlukan *review*, dan 27 untuk transaksi yang terindikasi *fraud*. Integrasi ini membuktikan bahwa pemodelan *machine learning* dapat difungsikan sebagai lapisan kontrol pra-pencatatan, sehingga peran *blockchain* sebagai media penyimpanan yang transparan, *immutable*, dan dapat ditelusuri (*traceable*) dilengkapi dengan jaminan kualitas masukan. Kontribusi utama penelitian ini terletak pada pemanfaatan *trust score* sebagai jembatan operasional antara *anomaly detection* secara *off-chain* dan eksekusi keputusan *smart contract* secara *on-chain*, yang efektif menekan risiko *garbage in, garbage out* tanpa membebani *smart contract* dengan komputasi *machine learning*. Untuk menyempurnakan prototipe ini, penelitian selanjutnya perlu melengkapi evaluasi metrik kinerja model dan jaringan secara kuantitatif, memperluas pengujian pada jaringan *blockchain* publik atau *enterprise*, serta mengintegrasikan pendekatan *explainable AI* dan *continuous learning* menggunakan data lintas lembaga wakaf guna menguji kemampuan generalisasi serta efisiensi sistem secara menyeluruh.

Referensi

Adinugraha, H. H., Shulthoni, M., & Sain, Z. H. (2024). Transformation of cash waqf management in Indonesia: Insights into the development of digitalization. *Review of Islamic Social Finance and Entrepreneurship*, *3*(1), 50–66. https://doi.org/10.20885/RISFE.vol3.iss1.art4

Amaliyah, N., Maslahah, M., Leviansyah, M. R., Pramuja, M. W., & Rahmawati, L. (2022). Wakaf uang digital: Transformasi dan implementasi di Indonesia. *Al-Infaq Jurnal Ekonomi Islam*, *13*(1), 26–46. https://doi.org/10.32507/alinfaq.v13i1.2097

Amirillah, C. D. R. (2025). Detecting fraudulent transaction in banking sector using rule-based model and machine learning. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, *14*(2), 96–102. https://doi.org/10.22146/jnteti.v14i2.17410

Anwar, I. F., Rahayu, S. B., Yusoff, Y., Lajin, N. F. M., & Atan, A. (2024). The sustainability of cash waqf using blockchain technology: A conceptual study. *International Journal of Trends in Accounting Research*, *5*(2), 70–82. https://doi.org/10.54951/ijtar.v5i2.664

Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A machine learning and blockchain based efficient fraud detection mechanism. *Sensors*, *22*(19), 7162. https://doi.org/10.3390/s22197162

Ayudewi, F. M., & Rafifah, U. R. (2026). Penerapan deteksi anomali menggunakan model Isolation Forest untuk analisis fraud pada transaksi keuangan akuntansi. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *10*(3), 4770–4777. https://doi.org/10.36040/jati.v10i3.18334

Baiquni, M. F., & Dirgahayu, R. T. (2023). Aplikasi terdesentralisasi berbasis blockchain dan smart contract untuk pengelolaan zakat. *AUTOMATA*, *4*(2), 1–10. https://journal.uii.ac.id/AUTOMATA/article/view/28628

Černevičienė, J., & Kabašinskas, A. (2024). Explainable artificial intelligence (XAI) in finance: A systematic literature review. *Artificial Intelligence Review*, *57*(8), 216. https://doi.org/10.1007/s10462-024-10854-8

Feng, Z., Li, Y., & Ma, X. (2023). Blockchain-oriented approach for detecting cyber-attack transactions. *Financial Innovation*, *9*(1), 81. https://doi.org/10.1186/s40854-023-00490-6

Hamzah, S. R., Ahmad, A., Ishak, N., & Rasedee, A. F. N. (2025). Revolutionizing financial inclusion: A blockchain-AI model for zakat and waqf management in Malaysia and beyond. *IECO: Islamic Economics Journal*, *3*(1), 173–193. https://unissa.edu.bn/journal/index.php/ieco/article/view/1339

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

Kunhibava, S., Muneeza, A., Mustapha, Z., Khalid, M., & Kiran, G. (2024). Blockchain use case in Islamic social finance. *ISRA International Journal of Islamic Finance*, *16*(1), 93–110. https://doi.org/10.55188/ijif.v16i1.659

Maisyarah, A., & Hadi, K. (2024). Implementasi model pengelolaan wakaf berbasis digital dalam meningkatkan tujuan pembangunan berkelanjutan (SDGs). *Jurnal Ilmiah Ekonomi Islam*, *10*(1), 887–894. https://doi.org/10.29040/jiei.v10i1.12079

Mukit, M. M. H., Hasan, F., Choudhury, T., Al Fadli, A., & Fadul, A. (2026). Machine learning & artificial intelligence powered credit scoring models for Islamic microfinance institutions: A blockchain approach. *Risks*, *14*(1), 12. https://doi.org/10.3390/risks14010012

Mustagfiroh, S., & Khoirina, N. N. (2025). Legal and regulatory challenges in the implementation of blockchain-based waqf in Indonesia. *Walisongo Journal of Sharia Economic Law*, *1*(1), 27–41. https://doi.org/10.21580/wishel.2025.1.1.29407

Nasywa, A. Z., & Lahuri, S. B. (2025). Teknologi blockchain sebagai upaya akuntabilitas wakaf. *SOSMANIORA: Jurnal Ilmu Sosial dan Humaniora*, *4*(1), 99–110. https://doi.org/10.55123/sosmaniora.v4i1.4964

Sabharwal, R., Miah, S. J., Wamba, S. F., & Cook, P. (2025). Extending application of explainable artificial intelligence for managers in financial organizations. *Annals of Operations Research*, *354*(1), 309–339. https://doi.org/10.1007/s10479-024-05825-9

Setiawan, A., & Nurjaman, M. S. (2022). Application of blockchain and smart-contract on waqf asset management: Is it necessary? *EL DINAR: Jurnal Keuangan dan Perbankan Syariah*, *10*(2), 85–101. https://doi.org/10.18860/ed.v10i2.15529

Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online payment fraud: From anomaly detection to risk management. *Financial Innovation*, *9*(1), 66. https://doi.org/10.1186/s40854-023-00470-w

Wibawa, I. M. S. T., & Karyawati, A. A. I. N. E. (2023). Isolation Forest dengan exploratory data analysis pada anomaly detection untuk data transaksi. *Jurnal Nasional Teknologi Informasi dan Aplikasinya*, *1*(3), 803–810. https://doi.org/10.24843/JNATIA.2023.v01.i03.p04