

ARSITEKTUR UNIFIED LEDGER UNTUK DONASI DIGITAL YANG TRANSPARAN DENGAN IDEMPOTENCY DAN SERVER-SENT EVENTS

Unified Ledger Architecture for Transparent Digital Donations with Idempotency and Server-Sent Events

Rifky Septian Rizki^{1*}

Fathoni Mahardika²

Dani Indra Junaedi³

Asep Saeppani⁴

¹⁻⁴ Program Studi
Informatika, Fakultas Teknologi
Informasi, Universitas Sebelas
April, Sumedang, Indonesia

*email:
rifikseptianrizki@gmail.com

Abstrak

Platform donasi digital dituntut memberikan transparansi yang cepat dan dapat diaudit, tetapi implementasi di dunia nyata sering menghadapi notifikasi gateway yang asinkron serta pengiriman *webhook at-least-once* yang dapat memicu duplikasi, inkonsistensi, dan membuat jendela transparansi menjadi singkat. Studi ini mengusulkan arsitektur terpusat yang menggabungkan (a) penerimaan *webhook* yang *idempotent* dengan *persistent audit log*, (b) *unified double-entry ledger* sebagai *system of record*, dan (c) publikasi real-time post-commit melalui server-sent events (SSE) sehingga *timeline* publik hanya dibentuk dari fakta ledger yang sudah *committed*. *Idempotency keys*, *signature validation*, dan *deterministic ledger posting* mencegah efek *double-spend* saat *webhook* dikirim ulang, sementara *audit log* menyimpan raw events untuk kebutuhan pemeriksaan forensik. Pendekatan ini diwujudkan dalam *prototipe* yang berjalan, *LuminaFund*, yang terintegrasi dengan *mainstream payment gateway*. Desain dievaluasi melalui pengujian berbasis skenario dan observasi operasional selama 1–13 Desember 2025 menggunakan lima indikator (K1–K5): efek *finansial exactly-once* pada kondisi retries, konsistensi rekonsiliasi antara *public dashboard* dan akuntansi, *disclosure latency*, *internal processing delay*, serta kelengkapan *audit-trail*. Hasilnya menunjukkan efek *idempoten* yang sempurna pada *webhook* berulang (K1=100%), konsistensi rekonsiliasi yang tinggi (K2≈91.95%), pengungkapan publik yang hampir real-time (K3 median=0.178 s; persentil 95≈2.92 s), *internal processing delay* yang minimal (K4 median≈1 ms), dan kelengkapan audit yang kuat (K5≈98.48%, 519/527 transaksi). Temuan ini mengindikasikan bahwa *unified-ledger ingestion* dengan *idempotency* dan *post-commit streaming* dapat meningkatkan transparansi dan akuntabilitas tanpa *operational overhead* dari sistem *on-chain*, tetap layak untuk institusi skala menengah, serta dapat diverifikasi secara mandiri oleh donatur, administrator, dan auditor eksternal.

Abstract

Digital donation platforms are expected to provide immediate, auditable transparency, yet real deployments often face asynchronous gateway notifications and at-least-once webhook delivery that can create duplicates, inconsistencies, and a short transparency window. This study proposes a centralized architecture that combines (a) an idempotent webhook intake with a persistent audit log, (b) a unified double-entry ledger as the system of record, and (c) post-commit real-time publication via server-sent events so that public timelines are derived only from committed ledger facts. Idempotency keys, signature validation, and deterministic ledger posting prevent double-spend effects while the audit log preserves raw events for forensic checks. The approach is instantiated in a working prototype, *LuminaFund*, integrated with a mainstream payment gateway. We evaluate the design through scenario-based tests and operational observations collected over 1–13 December 2025 using five indicators (K1–K5): exactly-once financial effects under retries, reconciliation consistency between the public dashboard and accounting, disclosure latency, internal processing delay, and audit-trail completeness. The results show perfect idempotent effects under repeated webhooks (K1=100%), high reconciliation consistency (K2≈91.95%), near-real-time public disclosure (K3 median=0.178 s; 95th percentile≈2.92 s), minimal internal processing delay (K4 median≈1 ms), and strong audit completeness (K5≈98.48%, 519/527 transactions). These findings indicate that unified-ledger ingestion with idempotency and post-commit streaming can improve transparency and accountability without the operational overhead of on-chain systems, while remaining feasible for medium-scale institutions and verifiable for donors, administrators, and external auditors independently.

Kata Kunci:
Idempotensi;
Server-sent Events;
Transparansi;
Unified ledger.

Keywords:
Idempotency;
Server-sent Events;
Transparency;
Unified ledger.

Submit Tgl.: 06-Januari-2026

Diterima Tgl.: 10-Januari-2026

Diterbitkan Tgl.: 13-Januari-2026

Cara mengutip Rizki, R. S., Mahardika, F., Junaedi, D. I., & Saeppani, A. (2026). Arsitektur Unified Ledger untuk Donasi Digital yang Transparan dengan Idempotency dan Server-Sent Events. *Jurnal Informatika, Multimedia Dan Teknik*, 2(2), 100–108. <https://doi.org/10.71456/jimt.v2i2.1590>

PENDAHULUAN

Platform donasi digital telah menjadi kanal arus utama untuk filantropi, penggalangan dana universitas, dan crowdfunding berbasis komunitas. Di samping kemudahan, donor semakin menuntut transparansi: bukti yang jelas bahwa dana dicatat dengan benar, terlindungi dari penyalahgunaan, dan disalurkan sesuai tujuan kampanye yang dinyatakan. Studi empiris pada konteks donasi daring dan crowdfunding secara konsisten menunjukkan bahwa isyarat transparansi dan sinyal tata kelola memengaruhi kepercayaan serta niat berdonasi (Dethier et al., 2023; Lima et al., 2021). Namun, banyak institusi masih mengoperasikan sistem donasi sebagai aplikasi web konvensional tanpa mekanisme eksplisit untuk traceability end-to-end lintas penyedia pembayaran, catatan internal, dan pelaporan publik.

Dua tantangan integrasi berulang kali melemahkan transparansi dan akuntabilitas pada platform donasi. Pertama, payment gateway memberi tahu merchant melalui webhook tentang perubahan status (pending, settled, expired), dan callback ini umumnya dikirim dengan semantik at-least-once. Duplikasi, keterlambatan, dan event yang tidak berurutan dapat memicu double-posting atau status yang saling bertentangan jika platform tidak idempotent. Kedua, timeline yang dilihat donor sering diperbarui dari application state yang sementara, bukan dari fakta akuntansi yang telah direkonsiliasi; kondisi ini menciptakan transparency window ketika donor sudah membayar tetapi belum dapat mengonfirmasi pencatatan yang akurat, yang dapat meningkatkan sengketa dan menurunkan perceived performance (Dethier et al., 2024; Harris et al., 2021; Morchid et al., 2025).

Platform charity berbasis blockchain sering diusulkan untuk mengatasi tamper resistance dan public verifiability dengan memanfaatkan distributed ledger pada domain yang intensif transaksi (Bank for International Settlements, 2023), termasuk rancangan

yang spesifik untuk donasi (Ahmed et al., 2024; Ibañez et al., 2023; Maiti et al., 2021; Nairi et al., 2024; Zhang et al., 2024). Walaupun pendekatan tersebut dapat meningkatkan traceability, pendekatan ini juga dapat menambah overhead operasional, kompleksitas tata kelola, dan friksi integrasi dengan payment rails yang sudah ada terutama bagi institusi skala menengah. Karena itu, alternatif yang lebih feasible adalah merekayasa transparansi di dalam stack terpusat dengan memperkuat properti correctness (idempotency), mengonsolidasikan kebenaran finansial (unified ledger), serta menyediakan visibilitas near-real-time (event streaming).

Jurnal ini menyajikan arsitektur engineered transparency untuk donasi digital yang menegakkan correctness di bawah notifikasi gateway yang asinkron, sambil menjaga disclosure kepada donor tetap cepat dan dapat diaudit. Arsitektur ini mengintegrasikan intake webhook yang idempotent dengan bukti callback yang eksplisit, unified double-entry ledger sebagai system of record, serta publikasi pasca-commit melalui server-sent events (SSE) sehingga tampilan publik diturunkan dari fakta ledger yang sudah committed, bukan dari best-effort updates (Kim, 2025).

Kesenjangan Penelitian dan Kebutuhan Desain

Meskipun transparansi banyak didorong dalam filantropi, banyak platform masih belum memiliki tautan yang dapat diaudit antara event dari payment provider, catatan akuntansi internal, dan laporan kampanye yang dilihat donor (Chu et al., 2023; Dethier et al., 2023). Dalam praktik, webhook retries yang digabung dengan CRUD updates yang mutable dapat menciptakan posting ganda dan total yang tidak konsisten. Studi ini menangani kesenjangan tersebut dengan menegakkan efek finansial exactly-once di bawah pengiriman at-least-once, serta menurunkan laporan publik dari fakta ledger yang sudah direkonsiliasi, bukan dari application state yang sementara (Fielding et al., 2022; Overeem et al., 2021).

Berdasarkan kesenjangan tersebut dan kriteria mutu dari reviewer, kami merumuskan kebutuhan desain berikut untuk arsitektur transparansi yang feasible pada setting institusi: R1 Efek finansial exactly-once di bawah callback at-least-once (pemrosesan aman terhadap duplikasi); R2 Satu sumber kebenaran (single source of truth) bagi status finansial donasi dengan provenance links yang immutable; R3 Disclosure real-time bagi donor yang diturunkan hanya dari event akuntansi yang sudah diverifikasi dan committed; R4 Traceability operasional untuk audit dan incident response, termasuk kemampuan merekonstruksi riwayat pemrosesan dari input mentah; serta R5 Kompatibel dengan payment gateway dan web stack arus utama untuk menurunkan adoption barriers

Prinsip Desain

Untuk memenuhi kebutuhan tersebut, arsitektur menerapkan empat prinsip: commit-first publication (tampilan publik hanya diperbarui setelah commit ledger), deterministic state transitions, modular boundaries yang mengisolasi kegagalan, serta traceability yang dapat diverifikasi dengan mengaitkan setiap pembaruan publik ke posting yang sudah committed dan bukti webhook.

METODE PENELITIAN

Penelitian ini menerapkan metodologi design-and-evaluate. Tahap awal dilakukan dengan mengelitisasi kebutuhan fungsional dan akuntabilitas dari alur donasi institusional, kemudian merancang arsitektur yang menegaskan correctness di bawah notifikasi pembayaran yang asinkron. Sistem kerja (LuminaFund) selanjutnya diimplementasikan menggunakan Node.js dan PostgreSQL, dan desain divalidasi melalui pengujian berbasis skenario serta pengukuran berbasis log dalam jendela observasi terkontrol pada 1 sampai 13 Desember 2025.

Arsitektur Sistem

LuminaFund diimplementasikan sebagai web backend modular dengan enam komponen logis: Donation Service, Payment Orchestrator, Webhook Receiver, Idempotency Guard, Unified Ledger Service, dan Dashboard Streamer yang menggunakan server-sent events (SSE). Payment Orchestrator berkomunikasi dengan payment gateway API untuk membuat transaksi dan mengambil status snapshot, sedangkan Webhook Receiver menangani notifikasi asinkron. Idempotency Guard memastikan bahwa setiap event gateway yang unik menghasilkan paling banyak satu efek finansial. Unified Ledger menyimpan posting double-entry yang immutable beserta metadata event, dan Dashboard Streamer menyiarkan pembaruan yang sudah diverifikasi hanya setelah commit ledger sehingga dashboard publik merefleksikan fakta ledger yang sudah committed

Tabel 1. Komponen LuminaFund dan kontrol integritas

Komponen	Tanggung jawab	Kontrol Integritas Utama
Donation Service	Mengumpulkan donor intent, pemilihan campaign, amount, dan metadata donor.	Validasi input; pengecekan status campaign.
Payment Orchestrator	Membuat transaksi gateway; menyimpan donation order; mengekspos status ke UI.	Identifier donation yang deterministik; panggilan yang retry-safe.
Webhook Receiver	Menerima dan memvalidasi callback (signature / secret).	Autentikasi dan validasi payload; raw event logging.
Idempotency Guard	Menghapus duplikasi callback berulang; menegakkan side effects exactly-once.	Event key unik; processed-event registry; transaction boundaries.
Unified Ledger	Menambahkan (append) posting debit/credit yang immutable dan metadata event.	Double-entry balancing; foreign-key traceability; audit logs.
Dashboard Streamer (SSE)	Mempublikasikan update yang sudah ledger-committed ke clients.	Publish-after-commit; reconnect support; access controls.

Idempotent Webhook Handler

Payment gateway dapat melakukan retry pengiriman webhook pada kondisi network loss, timeout, dan duplikasi notifikasi status. LuminaFund menegakkan idempotency pada batas webhook dengan mengikuti konsep Idempotency-Key untuk HTTP APIs (Irawan et al., 2025a; Overeem et al., 2021). Setiap callback yang tervalidasi dipetakan ke idempotency key yang deterministik dan direkam (payload hash, hasil validasi, timestamp) ke dalam log WebhookEvents untuk keperluan audit. Handler kemudian memeriksa apakah PostingGroup untuk key tersebut sudah pernah committed; jika ya, handler mengembalikan outcome yang sudah dihitung sebelumnya. Jika belum, handler menjalankan satu transaksi atomik yang memperbarui status donasi, menulis posting double-entry yang bersesuaian, serta memublikasikan SSE event hanya setelah commit. Mekanisme ini menghasilkan efek finansial exactly-once di bawah pengiriman at-least-once, sekaligus mendukung rekonsiliasi dan auditabilitas operasional (Alsaqer et al., 2023; Fielding et al., 2022; Hunt et al., 2022; Overeem et al., 2021).

Secara operasional, callback handler memverifikasi signature webhook, menormalkan event key yang deterministik, menyimpan callback mentah untuk audit, mendaftarkan event key secara atomik untuk mencegah replay side effects, menerapkan aturan deterministic status progression, memposting entri ledger yang seimbang dalam satu database transaction, dan memublikasikan pembaruan dashboard hanya setelah commit ledger berhasil.

Unified Double-Entry Ledger dan Traceability

Unified ledger adalah single source of truth untuk akuntabilitas finansial. Ledger ini menggunakan aturan posting double-entry sehingga setiap debit memiliki credit yang korespondensinya, dan posting bersifat immutable setelah committed. Setiap posting group mengaitkan transaksi donasi dengan status pembayaran, timestamp, serta webhook evidence yang menjadi

asalnya; dengan demikian, dimungkinkan rekonsiliasi end-to-end antara event gateway, akuntansi internal, dan timeline yang dilihat donor. Dashboard publik dan tampilan audit adalah projection yang diturunkan dari ledger, sehingga mengurangi drift antara apa yang dilihat donor dan apa yang dapat diaudit institusi (Coyne et al., 2023).

Transparansi Real-Time melalui Server-Sent Events

Setelah sebuah event webhook tervalidasi dan posting ledger yang terkait telah committed, LuminaFund memublikasikan event yang ringkas dan telah diverifikasi kepada klien yang berlangganan menggunakan server-sent events (SSE). SSE dipilih karena menyediakan kanal streaming satu arah yang sederhana di atas HTTP, mendukung client reconnection otomatis, dan memiliki overhead rendah untuk aplikasi bergaya dashboard (Jena et al., 2025). Untuk menghindari kebocoran informasi yang belum terverifikasi, streamer hanya memancarkan event pasca-commit yang diturunkan dari ledger, bukan dari application state yang sementara. Klien dapat membangun ulang tampilan saat ini dengan meminta snapshot (current donation status projection), lalu berlangganan untuk menerima incremental updates (Foucart et al., 2021).

Desain Evaluasi dan Metrik (K1-K5)

Evaluasi dilakukan sebagai penilaian black-box menggunakan application logs, gateway records, dan ledger entries yang dikumpulkan antara 1 dan 13 Desember 2025. Evaluasi berfokus pada reliabilitas, rekonsiliasi, ketepatan waktu, dan kelengkapan audit. Tabel II mendefinisikan lima indikator yang digunakan dalam jurnal ini.

Tabel II. Indikator evaluasi untuk reliabilitas, rekonsiliasi, latensi, dan auditabilitas



Indikator	Definisi	Pengukuran
K1 Webhook Duplicate-Prevention Reliability	Proporsi callback webhook yang ditangani tanpa side effects duplikat yang berbahaya.	Jumlah callback tanpa duplicate ledger posting / total callback.
K2 Reconciliation Consistency	Konsistensi status transaksi di antara catatan gateway, state DB aplikasi, dan ledger postings.	Sampel yang konsisten / total transaksi yang disampling.
K3 End-to-End Propagation Latency	Waktu dari konfirmasi gateway sampai verified update yang sesuai muncul di public dashboard.	Distribusi latency: median, P95, P99.
K4 Internal Processing Delay	Waktu dari penerimaan webhook sampai SSE emission segera setelah ledger commit.	Distribusi latency: median, P95, worst-case.
K5 Audit-Trail Completeness	Fraksi transaksi dengan linked records yang lengkap di seluruh webhook logs, status events, dan balanced ledger postings.	Complete trails / total transaksi yang diperiksa.

Validasi Berbasis Skenario

Selain indikator berbasis log, kami menjalankan pengujian skenario untuk memvalidasi correctness pada kondisi yang merugikan. Skenario ini dimaksudkan untuk memverifikasi bahwa sistem mempertahankan konsistensi ledger dan memberikan perilaku transparansi yang stabil tanpa mengarang klaim kinerja numerik yang baru. Tabel III mencantumkan skenario dan outcome yang diharapkan.

Tabel III. Matriks validasi berbasis skenario

Skenario	Kondisi Uji	Hasil yang Diharapkan
S1 Duplicate callback	Gateway mengirim ulang payload status yang identik beberapa kali.	Diproses sekali; duplikat dicatat (logged); tidak ada duplicate ledger postings.
S2 Out-of-order statuses	Menerima status yang lebih akhir sebelum status yang lebih awal (misalnya settled lalu pending).	Aturan transisi yang deterministik mencegah rollback yang tidak valid; ledger tetap konsisten.
S3 Signature mismatch	Webhook signature tidak cocok dengan secret key.	Ditolak; dicatat sebagai tidak valid; tidak ada perubahan state.
S4 Network interruption	Outage sementara saat penanganan callback.	Retry diproses secara idempotent setelah pemulihan; tidak ada

S5 Dashboard reconnect	Client melakukan reconnect setelah terputus.	efek ganda (double effects). Snapshot + SSE menghasilkan public view yang konsisten yang diturunkan dari ledger.
-------------------------------	--	---

Model Data dan Aturan Posting

Unified ledger diimplementasikan dengan dua tabel inti: LedgerPostings (baris debit/credit yang immutable) dan LedgerEvents (business event envelope yang mengaitkan posting ke donation identifiers, gateway transaction identifiers, dan webhook provenance). Untuk memastikan akuntansi yang konsisten di berbagai status, LuminaFund menerapkan posting rules yang memetakan setiap verified status transition menjadi balanced posting group. Aturan posting bersifat deterministik dan dapat diaudit, sehingga setiap transisi status yang terverifikasi menghasilkan tepat satu balanced posting group yang traceable ke webhook provenance-nya.

Keamanan, Privasi, dan Kontrol Tata Kelola

Karena sistem donasi memproses personally identifiable information (PII) dan event finansial, transparansi harus diseimbangkan dengan privasi dan keamanan. LuminaFund mengadopsi kontrol berlapis yang mencakup autentikasi webhook menggunakan shared secret atau signature verification, validasi skema yang ketat yang dipadukan dengan replay-safe idempotency keys, role-based access control untuk dashboard administratif, serta minimisasi data donor yang diekspos pada tampilan publik sehingga stream publik hanya membawa informasi status yang non-sensitif dan agregat tingkat kampanye. Catatan ledger tetap menyimpan trace lengkap yang dibutuhkan untuk audit yang berwenang, sambil mencegah pengungkapan atribut donor yang privat pada kanal publik.

Tata kelola diperlakukan sebagai bagian dari metode. Aksi administratif (pembuatan kampanye,

pembaruan beneficiary, persetujuan disbursement) dicatat sebagai event yang terhubung dengan ledger sehingga properti auditabilitas yang sama juga berlaku untuk perubahan non-pembayaran. Untuk semakin memperkuat tamper evidence, sistem dapat secara berkala menghitung Merkle root atau hash chain atas event ledger harian dan menyimpan digest tersebut pada registry terpisah yang access-controlled atau pada layanan notarization eksternal (Gao et al., 2023; Nairi et al., 2024).

HASIL DAN PEMBAHASAN

Bagian ini melaporkan indikator yang diukur (K1-K5) dan membahas bagaimana unified ledger, idempotency guard, serta publikasi SSE secara bersama-sama mendukung transparansi dan akuntabilitas. Semua nilai kuantitatif yang dilaporkan di sini diambil dari system logs dan validasi yang dijelaskan pada jendela evaluasi prototipe, dan bukan merupakan pengukuran yang baru dirancang.

Reliabilitas dan Konsistensi

Reliabilitas webhook diukur sebagai kemampuan untuk memproses callback gateway tanpa menghasilkan duplikasi side effects yang merugikan. Selama jendela observasi, pengiriman webhook mencakup retries dan notifikasi berulang. Idempotency guard mencegah duplicate ledger postings dan mempertahankan efek finansial exactly once untuk callback yang berulang, sehingga menghasilkan $K1=100\%$ untuk duplicate-prevention reliability.

Untuk menilai rekonsiliasi, kami membandingkan status donasi antara application state internal, projection unified ledger, dan catatan payment gateway. Pada pengecekan rekonsiliasi yang disampel, 514 dari 559 kasus konsisten, sehingga diperoleh $K2\approx 91.95\%$. Ketidakkonsistenan yang tersisa terutama disebabkan oleh timing gaps dan external status updates yang

datang setelah internal snapshot diambil, yang memperkuat kebutuhan akan alur rekonsiliasi yang eksplisit (Fielding et al., 2022; Overeem et al., 2021; Ramayanti et al., 2024).

Transparansi dan Latensi

Ketepatan waktu merupakan pusat dari transparansi yang dipersepsikan. Latensi end-to-end dari penyedia pembayaran ke timeline publik (K3) menunjukkan median 0.178 s (178 ms), dengan 95th percentile sekitar 2.86 s, yang mengindikasikan bahwa bahkan tail delays tetap berada dalam beberapa detik. Internal processing delay dari penerimaan webhook sampai commit (K4) sangat minimal (median ≈ 1 ms; P95 ≈ 11 ms; worst-case ≈ 26.36 ms). Hasil ini mendukung SSE sebagai kanal streaming satu arah yang ringan untuk dashboard donor ketika post-commit publication diperlukan (Irawan et al., 2025b; Jena et al., 2025).

Kelengkapan Audit-Trail dan Traceability

Auditabilitas dinilai dari apakah setiap transaksi mempertahankan data trail yang lengkap yang mengaitkan input webhook mentah, status events yang telah tervalidasi, dan balanced ledger postings. Cakupan audit digital (K5) mencapai sekitar 98.48% (519 dari 527 transaksi yang diperiksa), yang menunjukkan bahwa hampir semua transaksi mempertahankan traceability lengkap di seluruh webhook logs dan ledger entries. Unified ledger memberikan catatan immutable tentang apa yang terjadi, sementara webhook log mempertahankan provenance untuk forensik. Kasus yang tidak lengkap umumnya terkait dengan log operasional yang parsial saat terjadi isu sementara (transient issues), sehingga menunjukkan bahwa penguatan operasional (durable message queues, replicated logging, dan monitoring) dapat lebih lanjut meningkatkan cakupan.

**Tabel IV.** Ringkasan hasil evaluasi (K1-K5)

Indicator	Result (from evaluation logs)
K1 Duplicate-prevention reliability	100% (no harmful duplicates observed).
K2 Reconciliation consistency	≈91.95% (514/559 consistent samples).
K3 Median propagation latency	0.178 s (P95 ≈ 2.86 s; P99 ≈ 4.33 s).
K4 Median internal delay	≈1 ms (P95 ≈ 11 ms; max ≈26.36 ms).
K5 Audit-trail completeness	≈98.48% (519/527 complete trails).

Engineered Transparency vs. Blockchain Transparency

Pendekatan yang diusulkan berbeda dari rancangan charity yang blockchain-first (Bank for International Settlements, 2023; Hunt et al., 2022; Saraswat et al., 2022; Sung et al., 2023). Alih-alih memindahkan settlement donasi menjadi on-chain, pendekatan ini memperkuat transparansi di dalam sistem terpusat dengan menggabungkan ingestion idempotent yang deterministik, unified ledger, dan post-commit publication. Hal ini menurunkan friksi integrasi dengan payment gateway yang sudah ada sambil tetap menyediakan audit evidence yang kuat.

Pada konteks yang membutuhkan tamper evidence yang lebih kuat, opsi hybrid adalah melakukan anchoring hash ledger secara periodik ke registry eksternal sambil mempertahankan core operasional tetap terpusat (Ahmed et al., 2024; Nairi et al., 2024).

Pertimbangan Etika

Mekanisme transparansi tidak boleh mengekspos identitas donor atau atribut yang sensitif. Timeline publik diturunkan dari fakta ledger yang sudah committed tanpa personal identifiers, sedangkan tampilan audit memerlukan authenticated access dan secret yang dilindungi untuk webhook verification.

KESIMPULAN

Jurnal ini mengusulkan arsitektur unified-ledger untuk donasi digital transparan yang menggabungkan idempotent webhook handling, akuntansi ledger double-entry, dan post-commit publikasi real-time melalui server-sent events. Dengan menggunakan LuminaFund sebagai prototipe kerja, evaluasi menunjukkan efek finansial exactly-once di bawah retries (K1=100%), konsistensi rekonsiliasi sekitar 91.95% (K2), disclosure near-real-time (K3 median=0.178 s) dengan internal delay yang minimal (K4 median≈1 ms), serta kelengkapan audit-trail yang tinggi (K5≈98.48%, 519/527 transaksi).

Kontribusi utama adalah pola terpusat yang praktis untuk menghasilkan transparansi yang dapat diaudit tanpa overhead operasional settlement on-chain: timeline yang dilihat donor merupakan proyeksi dari fakta ledger yang sudah committed, dan setiap transisi status dapat ditelusuri kembali ke webhook evidence dan entri akuntansi. Keterbatasan meliputi evaluasi pada satu gateway dan jendela observasi yang dibatasi waktu; penelitian selanjutnya perlu memperluas pengujian ke skenario multi-gateway dan multi-currency, mengevaluasi perilaku jangka panjang pada volume yang lebih tinggi, serta mengeksplorasi ekstensi tamper evidence opsional seperti hash anchoring periodik dan antarmuka audit pihak ketiga.

REFERENSI

- Ahmed, I., Anwer, S., Narayanasamy, R. S., Algarni, M. M., & Ali, N. M. (2024). Blockchain-empowered decentralized philanthropic charity for social good. *Sustainability*, 16(1), 210. doi: 10.3390/su16010210
- Alsaqer, M. S., Alsulami, M. H., Alkhawaji, R. N., & Alaboudi, A. A. (2023). Analyzing the Impact of BlockchainModels for Securing Intelligent Logistics through Unified Computational Techniques. *Computers, Materials and Continua*, 77(3), 3943–3968. doi: 10.32604/cmc.2023.042379

- Bank for International Settlements. (2023). *Blueprint for the future monetary system: improving the old, enabling the new*.
- Chu, V., & Luke, B. (2023). NPO Web-Based Accountability: How Can We Know If NPOs Are Doing Good Things? *Nonprofit and Voluntary Sector Quarterly*, 52(1), 75–105. doi: 10.1177/08997640211062856
- Coyne, J. G., Coyne, M. A., & Walker, J. (2023). Blockchain-based triple-entry accounting: A systematic literature review. *Journal of Information Systems*, 37(3), 101–132. doi: 10.2308/ISYS-2022-041
- Dethier, F., Delcourt, C., & Dessart, L. (2024). Donor Perceptions of Nonprofit Organizations' Transparency: Conceptualization and Operationalization. *Nonprofit and Voluntary Sector Quarterly*, 53(5), 1230–1260. doi: 10.1177/08997640231211212
- Dethier, F., Delcourt, C., & Willems, J. (2023). Transparency of nonprofit organizations: An integrative framework and research agenda. *Journal of Philanthropy and Marketing*, 28(4), e1725. doi: 10.1002/nvsm.1725
- Fielding, R. T., Nottingham, M., & Reschke, J. (2022). *HTTP Semantics*. doi: 10.17487/RFC9110
- Foucart, J., Pastur, T., & Jacquet, M. (2021). *The involvement of patients in simulations: the connection between the educational objective and the application framework*. Retrieved from <http://www.ssih.org/Dictionary>
- Gao, Y., Zhang, M., & Yang, H. (2023). Looking Good in the Eyes of Stakeholders: Corporate Giving and Corporate Acquisitions. *Journal of Business Ethics*, 185(2), 375–396. doi: 10.1007/s10551-022-05178-y
- Harris, E. E., & Neely, D. (2021). Determinants and Consequences of Nonprofit Transparency. *Journal of Accounting, Auditing & Finance*, 36(1), 195–220. doi: 10.1177/0148558X18814134
- Hunt, K., Kache, V. A., Krause, R. M., & Schilling, J. M. (2022). Blockchain in humanitarian operations management: A review of research and practice. *Socio-Economic Planning Sciences*, 83, 101311. doi: 10.1016/j.seps.2021.101311
- Ibañez, J. I., Bayer, C. N., Tasca, P., & Xu, J. (2023). REA, triple-entry accounting and blockchain: Converging paths to shared ledger systems. *Journal of Risk and Financial Management*, 16(9), 382. doi: 10.3390/jrfm16090382
- Irawan, A. Y., Nashir, M., & Pratama, S. A. (2025a). An application of payment gateway in client webhook method for transactions. *Journal of Informatics and Computer Science (JINACS)*, 6(2), 605–614.
- Irawan, A. Y., Nashir, M., & Pratama, S. A. (2025b). An application of payment gateway in client webhook method for transactions. *Journal of Informatics and Computer Science (JINACS)*, 6(2), 605–614.
- Jena, J., & Dalal, S. (2025). *The Idempotency-Key HTTP header field*. Internet Engineering Task Force (IETF). Retrieved from <https://datatracker.ietf.org/doc/draft-ietf-httpapi-idempotency-key-header/>
- Kim, M.-H. (2025). How Does Financial Transparency Influence Citizens' Trust in Nonprofit Organizations? The Moderating Role of Financial Information on Fiscal Stress. *VOLUNTAS: International Journal of Voluntary and Nonprofit Organizations*, 36, 458–472. doi: 10.1007/s11266-025-00734-2
- Lima, S., Correia, J., Araújo, F., & Cardoso, J. S. (2021). Improving observability in Event Sourcing systems. *Journal of Systems and Software*, 181, 111015. doi: 10.1016/j.jss.2021.111015
- Maiti, M., Kotliarov, I., Lipatnikov, V., & Lakhani, A. S. (2021). A future triple-entry accounting framework using blockchain technology. *Blockchain: Research and Applications*, 2(4), 100037. doi: 10.1016/j.bcr.2021.100037
- Morchid, A., Aoued, A., Elhassnaoui, I., & Hassani, A. E. (2025). Smart irrigation system based on IoT, Server-Sent Events, and real-time monitoring. *Scientific African*, 29, e02660. doi: 10.1016/j.sciaf.2025.e02660
- Nairi, C., Auger, B., & Sultan, A. (2024). Smart blockchain networks: Revolutionizing donation tracking in the Web 3.0 era. *Computer Communications*, 224, 155–171. doi: 10.1016/j.comcom.2024.05.008
- Overeem, M., de Vries, D. J., & Brinkkemper, S. (2021). An empirical characterization of event-sourced systems and their schema evolution. *Journal of Systems and Software*, 176, 110931. doi: 10.1016/j.jss.2021.110931
- Ramayanti, R., Kautsar, I., & Surendro, K. (2024). Exploring intention and actual use in digital payments: A systematic review and roadmap for future research. *Computers in Human Behavior Reports*, 13, 100348. doi: 10.1016/j.chbr.2023.100348
- Saraswat, D., Bhattacharya, P., & Bhattacharya, M. K. (2022). UpHaaR: Blockchain-based charity donation scheme to handle financial irregularities. *Journal of Information Security and Applications*, 68, 103246. doi: 10.1016/j.jisa.2022.103246
- Sung, J., Nguyen, H. T., & Park, S. (2023). Effect of a blockchain-based donation system on the trustworthiness of nonprofit organizations.



Information & Management, 60, 103812. doi:
10.1016/j.im.2023.103812

Zhang, S., Xia, S., Fan, W., Shi, B., Xiong, X., Zhong, Z.,
& Pei, D. (2024). *Failure Diagnosis in Microservice
Systems: A Comprehensive Survey and Analysis*.
Retrieved from
[https://www.theregister.com/2023/04/24/micros
oft_365_search_outage/](https://www.theregister.com/2023/04/24/micros
oft_365_search_outage/)