Penerapan Blockchain untuk Transparansi RKAT dan KAK di SIPIM UNISRI

Moenawar Kholil[a,1,*], Arif Sutikno [b,2], Rina Robiulana Fathona[b,3]

[abc]Program Studi Pendidikan Teknologi Informasi, Universitas Slamet Riyadi, Jl. Sumpah Pemuda No.18, Surakarta 57136, Indonesia
[1] moenawarkholil@gmail.com *; [2] arif.stk@gmail.com;; [3]rinarfl107@gmail.com

Submission:18/12/2025 , Revision: 24/02/2026 , Accepted : 03/03/2026

Abstract

Budget management in higher education requires transparency, accountability, and reliable audit mechanisms to prevent undocumented changes and ensure traceability of financial decisions. This study proposes and implements a permissioned blockchain event ledger integrated with the Leadership Information System (SIPIM) at Universitas Slamet Riyadi Surakarta to enhance the integrity of RKAT and KAK processes. The research adopts a design science research approach by designing a sidecar architecture that preserves the existing relational database while adding an append-only cryptographic audit layer. Document integrity is ensured through SHA-256 hashing and hash-chaining mechanisms, while chain validity is evaluated using quantitative integrity metrics. Experimental testing was conducted under transaction loads of 100, 300, and 500 blocks, including controlled manipulation scenarios. Results show that the system maintains 100% chain validity under normal conditions and successfully detects inconsistencies after unauthorized modifications. Performance evaluation indicates that block formation time remains below 7 milliseconds, demonstrating minimal computational overhead. The findings confirm that integrating a permissioned blockchain as an audit layer can strengthen transparency and tamper-evident control without disrupting operational systems in higher education institutions.

Keywords: blockchain, transparency, RKAT, KAK, SIPIM, audit trail

Abstrak

enelitian ini bertujuan untuk merancang dan mengimplementasikan *permissioned blockchain event ledger* sebagai lapisan audit tambahan pada Sistem Informasi Kepemimpinan (SIPIM) Universitas Slamet Riyadi Surakarta guna meningkatkan transparansi serta integritas pengelolaan Rencana Kerja dan Anggaran Tahunan (RKAT) dan Kerangka Acuan Kerja (KAK). Permasalahan utama yang dihadapi adalah risiko manipulasi data tanpa rekam jejak yang jelas serta keterbatasan mekanisme log pada basis data relasional konvensional. Metode yang digunakan adalah *Design Science Research* (DSR) dengan perancangan arsitektur integrasi *sidecar* yang mempertahankan sistem utama dan menambahkan mekanisme pencatatan kriptografis berbasis *hash-chaining*. Integritas dokumen diuji menggunakan fungsi *hash* SHA-256, sedangkan validitas rantai dievaluasi melalui pengujian kuantitatif pada skenario 100, 300, dan 500 blok, termasuk simulasi manipulasi data. Hasil penelitian menunjukkan bahwa seluruh blok berada pada kondisi valid (100%) pada skenario normal, dan sistem mampu mendeteksi inkonsistensi segera setelah terjadi perubahan tidak sah. Waktu pembentukan blok tercatat di bawah 7 milidetik sehingga tidak mengganggu kinerja sistem utama secara signifikan. Penelitian ini menyimpulkan bahwa integrasi *blockchain* secara noninvasif efektif dalam meningkatkan transparansi, keterlacakan, dan sifat *tamper-evident* pada sistem penganggaran perguruan tinggi

Kata kunci: blockchain, transparansi, RKAT, KAK, SIPIM, audit.

1. Pendahuluan

Pengelolaan anggaran di perguruan tinggi merupakan proses strategis yang menentukan keberlangsungan program akademik, penelitian, dan pengabdian kepada masyarakat. Proses tersebut tidak hanya berkaitan dengan perencanaan alokasi dana, tetapi juga mencerminkan tata kelola institusi, tingkat akuntabilitas pimpinan, serta transparansi dalam pengambilan keputusan. Pada praktiknya, pengelolaan anggaran melibatkan proses berjenjang yang mencakup pengajuan rencana kerja oleh unit, penyusunan Rencana Kerja dan Anggaran Tahunan (RKAT), pengajuan Kerangka Acuan Kerja (KAK), verifikasi substansi, validasi administratif, dan persetujuan pimpinan, hingga pelaporan realisasi serta evaluasi kinerja.

Kompleksitas tahapan tersebut menghadirkan tantangan tersendiri, terutama dalam memastikan bahwa setiap transaksi dan perubahan anggaran dapat ditelusuri secara akurat. Dalam banyak kasus, permasalahan yang muncul tidak hanya berkaitan dengan keterlambatan administrasi, tetapi juga mencakup potensi ketidaksesuaian data, duplikasi pengajuan, perubahan nilai nominal tanpa rekam jejak yang jelas, serta ketidakselarasan antara dokumen perencanaan dan realisasi. Situasi tersebut dapat menimbulkan persepsi kurangnya transparansi, bahkan dalam kondisi ketika tidak terjadi pelanggaran secara langsung.

Salah satu persoalan yang sering muncul dalam sistem penganggaran konvensional adalah risiko "kebocoran" anggaran akibat lemahnya mekanisme kontrol dan audit. Kebocoran tersebut tidak selalu merujuk pada tindakan koruptif, tetapi dapat berupa ketidaktepatan pencatatan, perubahan data yang tidak terdokumentasi, atau revisi dokumen tanpa histori yang jelas. Selain itu, dalam sistem berbasis basis data relasional tradisional, perubahan data dapat dilakukan melalui operasi pembaruan (*update*) oleh pengguna dengan hak akses tertentu. Meskipun sistem log dapat merekam aktivitas tersebut, keberadaannya sangat bergantung pada konfigurasi aplikasi serta kebijakan retensi data. Dalam beberapa kasus, data log tersebut rentan dihapus, ditimpa, atau tidak tersimpan secara konsisten.

Permasalahan lainnya berkaitan dengan keterlacakan (*traceability*) status anggaran. Pimpinan sering kali membutuhkan kepastian terkait identitas pihak yang melakukan perubahan terakhir, waktu perubahan dilakukan, versi dokumen yang telah disetujui, serta validitas dokumen yang beredar apakah identik dengan dokumen yang telah disahkan. Tanpa mekanisme verifikasi integritas yang kuat, proses audit sepenuhnya bergantung pada pemeriksaan manual dan kepercayaan subjektif antarpihak. Kondisi tersebut berpotensi menurunkan tingkat kepercayaan terhadap sistem informasi penganggaran yang digunakan.

Perkembangan teknologi *blockchain* menawarkan pendekatan baru dalam membangun sistem pencatatan yang bersifat *append-only*, terhubung melalui fungsi hash, serta mampu menyediakan bukti integritas secara kriptografis. Kajian literatur oleh Zhang dkk. menunjukkan bahwa *blockchain* memiliki potensi signifikan dalam mendukung auditability melalui karakteristik immutability dan distributed verification [1] . Dalam konteks audit trail, mekanisme *hash-chaining* terbukti efektif dalam mendeteksi perubahan data yang tidak sah [2]. Sifat ini menjadikan *blockchain* relevan sebagai solusi untuk memperkuat jejak audit dalam sistem yang melibatkan banyak aktor dan tahapan persetujuan.

Sejumlah penelitian juga menunjukkan bahwa penerapan *blockchain* dapat meningkatkan transparansi dan efisiensi operasional organisasi. Analisis pada sektor bisnis menunjukkan peningkatan akuntabilitas dan efisiensi transaksi setelah adopsi *blockchain* [3] . Pada sistem seleksi pendanaan riset, pendekatan konsorsium *blockchain* telah digunakan untuk menjamin transparansi proses evaluasi dan mencegah manipulasi data [4] Dalam bidang akuntansi, *blockchain* dinilai berpotensi memperkuat integritas pencatatan transaksi dan mengurangi risiko perubahan data yang tidak terdokumentasi [5]. Kajian lain juga menekankan peluang dan tantangan penerapan *blockchain* dalam sistem informasi akuntansi modern [5].

Pada sektor publik, integrasi *blockchain* telah diuji dalam sistem pengadaan barang dan jasa untuk meningkatkan transparansi dan akuntabilitas [6] . Implementasi pada pengelolaan data aparatur sipil negara juga menunjukkan peningkatan konsistensi dan integritas data antar instansi [7] . Di industri keuangan, *blockchain* dilaporkan mampu meningkatkan keamanan data dan meminimalkan risiko manipulasi transaksi [8], sementara pada sektor fintech teknologi ini dikaji sebagai solusi untuk transparansi transaksi digital [9].

Dari sisi pengendalian akses, pendekatan role-based access control berbasis *blockchain* telah dikembangkan untuk meningkatkan kontrol peran pengguna dalam sistem terdistribusi [10] . Implementasi private *blockchain* juga telah diterapkan dalam konteks autentikasi layanan untuk menjaga integritas komunikasi data [11]. Selain itu, penggunaan smart contract dilaporkan dapat meningkatkan transparansi dan keamanan eksekusi aturan bisnis pada jaringan *blockchain* [12]. Dalam konteks pendidikan tinggi, penerapan *blockchain* telah dilakukan untuk meningkatkan keamanan data akademik dan mencegah pemalsuan dokumen [13] . Sementara itu, pendekatan proof-of-work yang umum digunakan pada *blockchain* publik, seperti dalam implementasi supply chain, menunjukkan karakteristik desentralisasi penuh yang belum tentu sesuai untuk kebutuhan organisasi dengan kontrol akses terbatas [14].

Meskipun berbagai penelitian tersebut menunjukkan manfaat *blockchain* dalam meningkatkan transparansi, keamanan, dan akuntabilitas, penerapan pada sistem penganggaran internal perguruan tinggi

masih relatif terbatas. Sebagian besar studi berfokus pada domain bisnis, fintech, akuntansi umum, pengadaan publik, atau data akademik, sementara integrasi *blockchain* pada workflow penganggaran seperti RKAT dan KAK belum banyak dibahas secara spesifik. Selain itu, banyak penelitian mengembangkan sistem *blockchain* sebagai platform baru yang berdiri sendiri, bukan sebagai lapisan audit tambahan yang terintegrasi dengan sistem informasi yang telah berjalan.

Di Universitas Slamet Riyadi Surakarta, proses penganggaran difasilitasi oleh Sistem Informasi Kepemimpinan (SIPIM). Sistem tersebut telah mendukung digitalisasi pengajuan serta persetujuan RKAT dan KAK. Namun, sebagaimana sistem berbasis basis data relasional pada umumnya, mekanisme audit pada SIPIM masih bergantung pada log aplikasi dan kontrol akses pengguna. Dalam situasi tertentu, revisi dokumen atau perubahan nilai nominal anggaran dapat memicu keraguan mengenai keaslian serta konsistensi versi dokumen. Oleh karena itu, diperlukan sebuah pendekatan yang mampu menyediakan bukti integritas data tanpa harus mengganti sistem yang telah berjalan saat ini.

Penelitian ini berfokus pada perancangan dan implementasi *permissioned blockchain ledger* sebagai *event ledger* yang terintegrasi dengan SIPIM. Berbeda dengan *blockchain* publik yang menerapkan mekanisme *Proof-of-Work* (PoW), pendekatan *permissioned* memungkinkan pengelolaan keanggotaan dan pembatasan hak akses yang disesuaikan dengan struktur organisasi. Dokumen penganggaran tetap disimpan secara luar rantaian (*off-chain*) untuk menjaga efisiensi serta kerahasiaan data, sementara nilai *hash* dokumen dan metadata transaksi dicatat pada rantai (*on-chain*) guna menyediakan bukti integritas serta keterlacakan yang permanen.

Tujuan penelitian ini adalah: (1) merancang arsitektur integrasi SIPIM–Ledger yang kompatibel dengan alur RKAT dan KAK tanpa mengganggu proses bisnis yang ada, (2) mengembangkan struktur blok dan mekanisme hash-chaining untuk pencatatan transaksi anggaran, serta (3) mengevaluasi kemampuan sistem dalam meningkatkan auditability melalui verifikasi integritas dokumen dan keterlacakan status transaksi. Dengan pendekatan ini, diharapkan sistem penganggaran perguruan tinggi dapat memiliki mekanisme tamper-evident yang memperkuat transparansi dan akuntabilitas tanpa mengorbankan stabilitas infrastruktur yang telah digunakan.

Hasil penelitian ini diharapkan menjadi model implementasi bertahap bagi perguruan tinggi yang menghadapi permasalahan serupa dalam pengelolaan anggaran, sekaligus memberikan kontribusi praktis dalam pengembangan sistem informasi berbasis *blockchain* yang kontekstual dan realistis untuk lingkungan pendidikan tinggi.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan *design science research* yang berorientasi pada perancangan dan implementasi artefak sistem berupa *permissioned blockchain event ledger* untuk mendukung modul RKAT dan KAK pada Sistem Informasi Kepemimpinan (SIPIM). Pendekatan ini dipilih karena penelitian tidak hanya bertujuan menjelaskan fenomena, tetapi menghasilkan model teknis yang dapat diuji, direplikasi, dan dievaluasi secara kuantitatif. Dalam konteks ini, artefak yang dikembangkan adalah mekanisme pencatatan transaksi anggaran berbasis ledger kriptografis yang terintegrasi dengan sistem yang telah berjalan.

Secara konseptual, rancangan metode mengacu pada prinsip audit berbasis *blockchain* sebagaimana dibahas dalam kajian literatur oleh Zhang dkk. [1] , yang menekankan bahwa *blockchain* menyediakan karakteristik *immutability*, *traceability*, dan *distributed verification*. Mekanisme *hash-chaining* sebagai fondasi *audit trail* diadopsi dari model yang dijelaskan oleh Regueiro dkk. [3] , di mana setiap blok data terhubung secara kriptografis dengan blok sebelumnya sehingga perubahan histori dapat dideteksi. Selain itu, pendekatan konsorsium atau *permissioned blockchain* merujuk pada implementasi sistem seleksi pendanaan riset yang menggunakan model kontrol keanggotaan terbatas [4] . Model ini relevan dengan lingkungan perguruan tinggi yang memiliki struktur organisasi dan otoritas berjenjang.

Integrasi *blockchain* dalam konteks sistem akuntansi dan tata kelola organisasi merujuk pada kajian Ramadhani, Ananda, dan Azmi [5] yang menegaskan bahwa teknologi *blockchain* memiliki potensi memperkuat integritas pencatatan transaksi akuntansi melalui mekanisme kriptografis yang tidak mudah dimanipulasi. Dalam sistem akuntansi, setiap transaksi harus memenuhi prinsip keandalan dan keterverifikasian. Oleh karena itu, metode penelitian ini tidak hanya memandang *blockchain* sebagai teknologi penyimpanan data, tetapi sebagai instrumen penguatan integritas pencatatan anggaran. Perspektif ini diperkuat oleh kajian Palidita Febriana dkk. [8] yang menyoroti peluang penerapan *blockchain* dalam sistem informasi akuntansi modern, serta oleh Kusumawati dkk. [6] yang menunjukkan bahwa integrasi *blockchain* dalam sektor publik dapat meningkatkan transparansi dan akuntabilitas proses administrasi.

Objek penelitian adalah transaksi penganggaran RKAT dan KAK yang mencakup tahapan pengajuan, verifikasi substansi, validasi administratif, persetujuan pimpinan, revisi, hingga pengesahan akhir. Sistem eksisting berbasis basis data relasional (MySQL) dengan kontrol akses berbasis peran (*role-based*

access control). Namun, sebagaimana dijelaskan dalam model RBAC berbasis *blockchain* oleh Rahman [10], kontrol akses saja tidak cukup menjamin *non-repudiation* apabila histori data masih dapat dimodifikasi oleh administrator sistem. Oleh karena itu, dirancang lapisan ledger tambahan yang bersifat *append-only*, sehingga setiap transaksi yang telah dicatat tidak dapat diubah tanpa meninggalkan jejak inkonsistensi kriptografis.

Tahap pertama dalam metode ini adalah pembentukan model hash dokumen sebagai representasi kriptografis dari setiap dokumen anggaran. Prinsip penggunaan fungsi hash sebagai dasar integritas data dijelaskan dalam [1] dan [3], di mana fungsi hash menghasilkan nilai unik yang sensitif terhadap perubahan sekecil apa pun pada data sumber. Model matematis hash dokumen dirumuskan sebagai berikut:

$$D_i = SHA256(File_i) \quad (1)$$

Pada Persamaan (1), (D_iDi) adalah nilai hash dokumen ke-i, sedangkan ($File_i$) adalah isi dokumen RKAT atau KAK dalam bentuk digital. Fungsi SHA256 menghasilkan keluaran sepanjang 256-bit. Sifat deterministik memastikan bahwa dokumen yang identik akan menghasilkan hash yang sama, sedangkan perubahan satu karakter saja akan menghasilkan nilai hash yang berbeda secara signifikan. Model ini mencerminkan prinsip integritas pencatatan transaksi akuntansi sebagaimana dibahas dalam [5] , di mana setiap transaksi harus dapat diverifikasi keasliannya.

Setelah nilai hash dokumen diperoleh, tahap berikutnya adalah pembentukan blok ledger menggunakan mekanisme *hash-chaining*. Konsep ini dijelaskan secara teknis dalam [3], di mana setiap blok mengandung hash blok sebelumnya untuk membentuk rantai yang tidak dapat dimodifikasi tanpa terdeteksi. Model hash blok dirumuskan sebagai:

$$H_i = \text{SHA256}(M_i \parallel D_i \parallel H_{i-1}) \quad (2)$$

Pada Persamaan (2), (H_iH_i) adalah hash blok ke-i. Variabel (M_i) merepresentasikan metadata transaksi, yang meliputi indeks blok, waktu pencatatan (*timestamp*), identitas transaksi, aktor, unit kerja, serta status persetujuan. Variabel (D_i) adalah hash dokumen sebagaimana didefinisikan dalam Persamaan (1), dan (H_{i-1}) adalah hash blok sebelumnya. Operator (parallel) menyatakan proses konkatenasi dalam urutan tetap sebelum dilakukan hashing. Model ini mengimplementasikan prinsip *tamper-evident ledger* yang menjadi karakteristik utama *blockchain* [1]

Validasi integritas rantai dilakukan dengan menghitung ulang seluruh hash blok dan membandingkannya dengan nilai yang tersimpan. Tingkat validitas sistem dihitung menggunakan:

$$V = \frac{B_{valid}}{B_{total}} \times 100\% \quad (3)$$

Pada Persamaan (3), (V) adalah tingkat validitas rantai dalam persen, (B_{valid}) adalah jumlah blok yang hash-nya sesuai dengan hasil perhitungan ulang, dan (B_{total}) adalah total blok dalam ledger. Jika (V = 100%), maka seluruh rantai dinyatakan valid. Model ini merepresentasikan mekanisme verifikasi terdistribusi yang dijelaskan dalam [1] dan pendekatan konsorsium dalam [4]

Untuk mengukur efisiensi sistem, dilakukan analisis waktu pembentukan blok. Literatur implementasi *blockchain* privat pada sektor keuangan [10] dan sistem privat berbasis autentikasi [13] menunjukkan bahwa waktu proses menjadi parameter penting dalam lingkungan organisasi. Waktu pembentukan blok dirumuskan sebagai:

$$T_{block} = T_{hash} + T_{write}\} \quad (4)$$

Pada Persamaan (4), (T_{block}) adalah total waktu pembentukan blok, (T_{hash}) adalah waktu komputasi fungsi SHA256, dan (T_{write}) adalah waktu penyimpanan metadata ke basis data. Pengujian dilakukan pada tiga skenario beban transaksi, yaitu 100, 300, dan 500 blok, masing-masing dengan tiga kali replikasi. Parameter yang diamati meliputi waktu hashing, waktu penyimpanan, total waktu blok, serta tingkat validitas rantai. Selain pengujian performa sistem sebagaimana dihitung menggunakan Persamaan (4), penelitian ini juga melakukan simulasi manipulasi data untuk mengevaluasi secara langsung kemampuan sistem dalam menjawab permasalahan yang telah diuraikan pada bagian pendahuluan, yaitu potensi perubahan data tanpa rekam jejak yang jelas, lemahnya keterlacakan, serta risiko modifikasi histori transaksi oleh pihak yang memiliki akses administratif.

Simulasi manipulasi dilakukan dengan pendekatan eksperimental terkontrol. Pada tahap ini, peneliti terlebih dahulu membentuk rantai blok yang valid berdasarkan transaksi RKAT dan KAK yang telah disahkan. Setiap dokumen dihitung nilai hash-nya menggunakan Persamaan (1), kemudian dibentuk blok ledger melalui mekanisme hash-chaining sebagaimana didefinisikan dalam Persamaan (2). Rantai blok dibangun secara berurutan mulai dari blok genesis hingga blok ke-n. Setelah seluruh blok terbentuk, dilakukan proses verifikasi awal untuk memastikan bahwa tingkat validitas sistem berada pada kondisi maksimal. Validitas dihitung menggunakan Persamaan (3). Pada kondisi normal tanpa manipulasi, nilai validitas harus menunjukkan konsistensi penuh (100%), yang berarti seluruh blok memiliki hash yang sesuai dengan hasil perhitungan ulang.

Tahap berikutnya adalah skenario manipulasi. Dalam penelitian ini, manipulasi dilakukan pada satu blok tertentu yang bukan blok terakhir, misalnya blok ke-k, dengan cara mengubah salah satu parameter metadata dalam M_i, seperti nilai nominal anggaran, status persetujuan, atau identitas aktor yang melakukan transaksi. Perubahan ini mensimulasikan kondisi nyata di mana terdapat revisi tidak sah atau perubahan data tanpa prosedur formal.

Setelah perubahan dilakukan, sistem tidak langsung memperbarui nilai hash secara otomatis. Sebaliknya, dilakukan proses verifikasi ulang seluruh rantai blok dengan menghitung kembali setiap H_i mulai dari blok pertama hingga blok terakhir menggunakan Persamaan (2). Karena nilai M_i pada blok ke-k telah berubah, maka hash blok tersebut akan berbeda dari nilai sebelumnya. Perubahan ini secara kriptografis menyebabkan ketidaksesuaian pada blok tersebut dan seluruh blok setelahnya, karena H_{i-1} yang menjadi input pada blok berikutnya juga berubah.

Dampak dari perubahan ini kemudian diukur menggunakan Persamaan (3). Apabila hasil perhitungan ulang menunjukkan bahwa nilai validitas turun di bawah 100%, maka sistem dinyatakan berhasil mendeteksi inkonsistensi. Dengan kata lain, sistem bersifat tamper-evident, yaitu setiap perubahan histori yang tidak sesuai prosedur akan menghasilkan jejak inkonsistensi yang dapat diverifikasi secara matematis.

Pendekatan ini secara langsung menjawab permasalahan yang diidentifikasi pada bagian pendahuluan, yaitu: (1) Masalah perubahan nominal anggaran tanpa histori yang jelas. Dengan model hash-chaining pada Persamaan (2), perubahan nominal sekecil apa pun akan mengubah D_i dan menyebabkan H_i berbeda dari nilai sebelumnya. (2) Masalah keterlacakan status persetujuan. Karena metadata transaksi (M_i) mencakup informasi aktor, waktu, dan status, maka setiap perubahan status akan mengubah struktur hash blok dan dapat dilacak secara kronologis melalui indeks blok. (3) Masalah potensi manipulasi oleh administrator basis data. Walaupun data pada sistem relasional dapat diperbarui, ledger bersifat append-only dan terhubung secara kriptografis. Manipulasi langsung pada satu entri akan menyebabkan ketidaksesuaian rantai yang terdeteksi saat validasi ulang. endekatan ini tidak hanya bersifat teknis, tetapi juga memiliki relevansi konseptual terhadap sistem akuntansi. Ramadhani, Ananda, dan Azmi [15]

Selain itu, pengujian dilakukan dalam beberapa skenario beban transaksi, yaitu 100, 300, dan 500 blok, untuk memastikan bahwa mekanisme deteksi manipulasi tetap konsisten pada skala transaksi yang lebih besar. Pada setiap skenario, simulasi manipulasi dilakukan minimal satu kali pada blok acak, kemudian dihitung kembali nilai validitas dan waktu proses verifikasi menggunakan Persamaan (4). Dengan demikian, penelitian tidak hanya mengevaluasi kemampuan deteksi manipulasi, tetapi juga mempertimbangkan implikasi performa ketika jumlah blok bertambah.

Dari sisi metodologis, pendekatan ini bersifat eksperimental-kuantitatif karena: (1) Terdapat variabel terkontrol (jumlah blok, jenis manipulasi). (2) Terdapat variabel terukur (waktu pembentukan blok dan tingkat validitas). (3) Terdapat replikasi pengujian untuk mengurangi bias hasil.

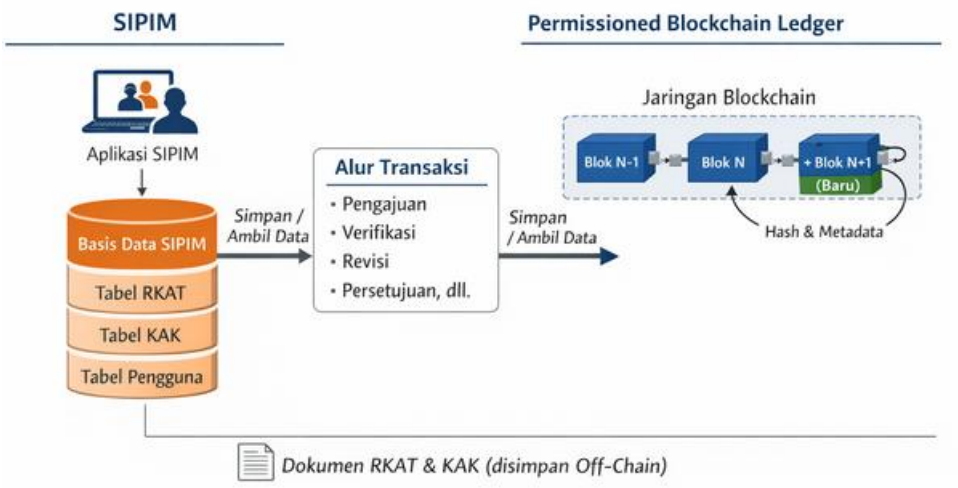
Dengan rancangan tersebut, metode penelitian tidak hanya membuktikan secara konseptual bahwa blockchain dapat meningkatkan integritas, tetapi juga menunjukkan secara empiris bahwa mekanisme hash-chaining mampu mendeteksi permasalahan nyata yang sering terjadi dalam pengelolaan anggaran perguruan tinggi, yaitu perubahan data tanpa jejak audit yang kuat. Dengan demikian, bagian metode ini secara eksplisit mengaitkan model matematis (Persamaan (1)–(4)) dengan permasalahan praktis yang telah diuraikan pada pendahuluan. Pendekatan ini memastikan bahwa artefak yang dikembangkan tidak hanya bersifat teoretis, tetapi operasional dan teruji dalam konteks sistem penganggaran yang sesungguhnya.

3. Hasil dan Pembahasan

3.1 Arsitektur Integrasi SIPIM–Ledger

Hasil pertama penelitian ini adalah terbentuknya arsitektur integrasi antara Sistem Informasi Kepemimpinan (SIPIM) dan *permissioned blockchain event ledger* menggunakan pendekatan *sidecar architecture*. Pada pendekatan ini, SIPIM tetap menjadi sistem utama yang mengelola proses bisnis penganggaran, sedangkan ledger berfungsi sebagai pencatat peristiwa kriptografis yang bersifat *append-only*. Setiap peristiwa penting dalam alur RKAT dan KAK—seperti pengajuan, verifikasi, revisi, dan persetujuan—menghasilkan satu blok baru pada ledger. Pembentukan blok mengikuti mekanisme yang telah dirumuskan pada Persamaan (1) dan Persamaan (2) pada bagian Metode Penelitian.

Dokumen RKAT dan KAK tetap disimpan secara *off-chain*, sedangkan ledger hanya menyimpan nilai hash dokumen dan metadata transaksi. Dengan demikian, integritas dapat diverifikasi tanpa mengungkap isi dokumen.



Gambar 1. Arsitektur integrasi SIPIM dengan permissioned *blockchain* ledger

Pada Gambar 1 terlihat bahwa arsitektur integrasi dirancang dalam dua domain utama, yaitu domain operasional SIPIM dan domain pencatatan kriptografis ledger *blockchain*. Pemisahan ini menunjukkan bahwa sistem penganggaran tetap berjalan pada struktur basis data relasional yang sudah ada, sedangkan ledger ditempatkan sebagai lapisan audit tambahan (*audit layer*) yang bekerja secara paralel.

Bagian kiri gambar merepresentasikan lingkungan SIPIM. Pada lapisan paling atas terdapat aplikasi SIPIM yang digunakan oleh pengguna (unit pengaju, verifikator, dan pimpinan). Aplikasi ini terhubung langsung dengan basis data SIPIM yang menyimpan tabel-tabel utama seperti tabel RKAT, tabel KAK, dan tabel pengguna. Seluruh proses bisnis—mulai dari pengajuan, verifikasi, revisi, hingga persetujuan—tetap diproses dan divalidasi pada basis data relasional tersebut. Hal ini menegaskan bahwa tidak terjadi perubahan terhadap struktur tabel utama maupun mekanisme *role-based access control* yang sudah berjalan.

Di bagian tengah gambar ditunjukkan komponen "Alur Transaksi" yang menggambarkan peristiwa-peristiwa penting dalam siklus penganggaran. Setiap peristiwa pada alur tersebut tidak langsung disimpan sebagai blok, melainkan terlebih dahulu diproses oleh layanan integrasi (*service layer*). Layanan ini mengambil metadata transaksi dari basis data SIPIM, menghitung nilai hash dokumen sebagaimana dijelaskan pada Persamaan (1), kemudian membentuk hash blok sesuai Persamaan (2).

Bagian kanan gambar merepresentasikan jaringan *permissioned blockchain*. Blok-blok ditampilkan dalam bentuk rangkaian berurutan (Blok N-1, Blok N, dan Blok N+1). Panah penghubung antarblok menunjukkan keterikatan melalui hash blok sebelumnya. Struktur berantai ini menggambarkan bahwa setiap blok bergantung pada hash blok sebelumnya, sehingga perubahan pada satu blok akan memengaruhi seluruh blok setelahnya. Inilah mekanisme yang membuat sistem bersifat *tamper-evident*.

Di bagian bawah gambar terlihat bahwa dokumen RKAT dan KAK tetap disimpan secara *off-chain*. Artinya, ledger tidak menyimpan isi dokumen, melainkan hanya nilai hash dan metadata. Hal ini menunjukkan dua hal penting: (1) Efisiensi penyimpanan tetap terjaga karena ukuran dokumen tidak masuk ke dalam blok. (2) Kerahasiaan dokumen tetap dilindungi karena ledger hanya menyimpan representasi kriptografisnya.

Secara keseluruhan, Gambar 1 menegaskan bahwa ledger tidak menggantikan basis data utama SIPIM. Ledger hanya menerima ringkasan kriptografis dari setiap transaksi yang telah diproses oleh sistem utama. Dengan demikian, apabila terjadi perubahan data pada basis data relasional setelah pencatatan blok, sistem dapat mendeteksinya melalui ketidaksesuaian nilai hash saat proses validasi ulang.

Arsitektur ini menunjukkan bahwa integrasi dilakukan secara non-invasif, yaitu tanpa memodifikasi struktur inti sistem operasional. Ledger berfungsi sebagai mekanisme penguatan integritas dan keterlacakan, bukan sebagai pengganti sistem penganggaran yang telah berjalan.

3.2 Struktur Blok dan Mekanisme Pencatatan

Struktur blok pada ledger dirancang berdasarkan model matematis yang telah dijelaskan pada bagian Metode Penelitian dan divisualisasikan pada Gambar 1. Pada arsitektur tersebut, setiap peristiwa dalam SIPIM—seperti pengajuan, verifikasi, revisi, dan persetujuan—tidak mengubah histori yang telah tercatat, melainkan menghasilkan blok baru pada rantai ledger.

Proses pembentukan blok dilakukan melalui dua tahap utama. Tahap pertama adalah perhitungan hash dokumen menggunakan Persamaan (1). Pada tahap ini, sistem mengambil dokumen RKAT atau KAK yang tersimpan secara *off-chain*, kemudian menghitung nilai hash untuk menghasilkan (D_i). Nilai (D_i) merupakan representasi kriptografis unik dari dokumen pada transaksi ke-(i). Sifat deterministik fungsi hash memastikan bahwa dokumen yang identik menghasilkan nilai (D_i) yang sama, sedangkan perubahan sekecil apa pun akan menghasilkan nilai yang berbeda.

Tahap kedua adalah pembentukan hash blok menggunakan Persamaan (2). Pada tahap ini, sistem menggabungkan metadata transaksi (M*i*), nilai hash dokumen (D*i*), dan hash blok sebelumnya (H_{i-1}) untuk menghasilkan hash blok saat ini (H*i*). Dengan mekanisme ini, setiap blok selalu terikat secara kriptografis dengan blok sebelumnya.

Struktur minimal blok yang digunakan dalam prototipe ditunjukkan pada Tabel 1.

Tabel 1. Struktur Data Minimal pada Ledger

Field	Deskripsi	Contoh
index	Nomor urut blok ke-(i)	128
timestamp	Waktu pencatatan transaksi	2024-11-20 09:15:33
tx_type	Jenis transaksi	approve_kak
actor*i*d	Identitas pengguna	usr_0091
unit*i*d	Identitas unit	unit_03
doc_hash	Nilai hash dokumen (D*i*)	9f2c…a18b
prev_hash	Hash blok sebelumnya (H_{i-1})	ab01…c923
curr_hash	Hash blok saat ini (H*i*)	7d4e…1f90
signature	Tanda tangan digital (opsional)	base64(...)

Jika dikaitkan dengan Persamaan (1) dan Persamaan (2):

1. Kolom doc_hash menyimpan nilai (D*i*) yang dihasilkan melalui Persamaan (1).
2. Kolom prev_hash menyimpan nilai (H_{i-1}), yaitu hash blok sebelumnya.
3. Kolom curr_hash menyimpan nilai (H*i*), yang dihitung melalui Persamaan (2) menggunakan kombinasi (M*i*), (D*i*), dan (H_{i-1}).

Metadata transaksi (M*i*) pada implementasi ini direpresentasikan oleh kombinasi *field: indeks, timestamp, tx_type, actori dan uniti* . *Field-field* tersebut membentuk representasi metadata transaksi ke-(i). Relasi antara (H_{i-1}) dan (H*i*) membentuk rantai hash (*hash chain*). Jika terjadi perubahan pada salah satu elemen dalam blok ke-(i), misalnya pada (M*i*) atau (D*i*), maka nilai (H*i*) akan berubah. Perubahan tersebut menyebabkan ketidaksesuaian pada blok ke-(i+1), karena nilai (H*i*) yang digunakan sebagai (H_{i-1}) pada blok berikutnya tidak lagi cocok.

Dengan demikian, struktur ini memastikan bahwa:

1. Setiap blok bersifat tidak dapat diubah tanpa terdeteksi (*tamper-evident*).
2. Integritas histori transaksi dapat diverifikasi ulang menggunakan Persamaan (3).
3. Ledger bekerja sebagai lapisan audit tambahan tanpa mengubah struktur basis data utama SIPIM sebagaimana ditunjukkan pada Gambar 1.

3.3 Hasil Pengujian Fungsional

Pengujian fungsional dilakukan untuk memastikan bahwa integrasi *permissioned blockchain ledger* dengan SIPIM berjalan sesuai dengan rancangan arsitektur pada Gambar 1 serta mekanisme matematis yang

telah dirumuskan pada Persamaan (1) dan Persamaan (2). Pengujian mencakup seluruh tahapan operasional dalam siklus penganggaran RKAT dan KAK, mulai dari pengajuan awal hingga persetujuan akhir, termasuk simulasi manipulasi dokumen setelah pencatatan.

Tabel 2. Ringkasan Hasil Uji Skenario Prototipe

Skenario	Output Ledger	Hasil
Submit RKAT	Blok terbentuk dan hash dokumen tercatat	Lulus
Verifikasi RKAT	Blok terikat dengan (H_{i-1})	Lulus
Revisi RKAT	Nilai (D_i) berubah dan blok baru terbentuk	Lulus
Approve RKAT	Status akhir tercatat dalam metadata (M_i)	Lulus
Submit KAK	Blok terbentuk dan tercatat	Lulus
Verifikasi KAK	Riwayat transaksi tersimpan berurutan	Lulus
Approve KAK	Rantai blok tetap konsisten	Lulus
Simulasi ubah dokumen	Terjadi ketidaksesuaian hash	Terdeteksi

Hasil pada Tabel 2 menunjukkan bahwa setiap peristiwa dalam sistem SIPIM menghasilkan blok baru pada ledger tanpa mengubah blok yang telah ada sebelumnya. Pada saat unit melakukan *submit* RKAT, sistem menghitung nilai hash dokumen menggunakan Persamaan (1) untuk menghasilkan (Di). Nilai ini kemudian digunakan bersama metadata transaksi (M*i*) dan hash blok sebelumnya (H_{i-1}) untuk membentuk hash blok baru (H*i*) sebagaimana dirumuskan dalam Persamaan (2). Blok yang terbentuk berhasil tersimpan dan terhubung dengan blok sebelumnya, menunjukkan bahwa mekanisme keterikatan hash berjalan sesuai rancangan.

Pada tahap verifikasi dan persetujuan, perubahan status transaksi direpresentasikan dalam metadata (M*i*). Sistem tidak memperbarui blok lama, tetapi membentuk blok baru yang merekam perubahan status tersebut. Hal ini menunjukkan bahwa ledger bekerja berdasarkan prinsip *append-only*, sehingga setiap perubahan dicatat sebagai entitas histori tersendiri. Rantai blok tetap valid karena setiap (H*i*) konsisten dengan (H_{i-1}). Ketika dilakukan revisi dokumen, nilai hash dokumen (D*i*) dihitung ulang menggunakan Persamaan (1). Perubahan isi dokumen menghasilkan nilai hash yang berbeda dari versi sebelumnya. Sistem kemudian membentuk blok baru yang merepresentasikan versi revisi tanpa menghapus histori sebelumnya. Dengan demikian, setiap versi dokumen memiliki jejak kriptografis tersendiri yang dapat ditelusuri secara kronologis.

Skenario manipulasi dokumen dilakukan untuk menguji permasalahan utama yang diidentifikasi pada bagian pendahuluan, yaitu potensi perubahan data tanpa rekam jejak yang jelas. Dalam pengujian ini, dokumen yang telah dicatat diubah secara langsung pada penyimpanan *off-chain* tanpa membentuk blok baru. Ketika dilakukan proses verifikasi ulang, sistem menghitung kembali nilai (D*i*) menggunakan Persamaan (1) dan membandingkannya dengan nilai doc_hash yang tersimpan pada ledger. Hasil menunjukkan terjadinya ketidaksesuaian hash (*hash mismatch*), yang menyebabkan nilai validitas rantai menurun ketika dihitung menggunakan Persamaan (3). Temuan ini membuktikan bahwa sistem mampu mendeteksi manipulasi pasca pencatatan.

Selain validitas integritas, pengujian juga mengevaluasi stabilitas rantai pada seluruh tahapan operasional. Tidak ditemukan kasus pemutusan rantai (*broken chain*) atau inkonsistensi hash pada kondisi normal. Hal ini menunjukkan bahwa mekanisme pembentukan blok berbasis Persamaan (2) bekerja secara konsisten pada berbagai jenis transaksi, baik pengajuan, verifikasi, revisi, maupun persetujuan akhir.

Secara keseluruhan, hasil pengujian fungsional membuktikan bahwa integrasi ledger tidak mengganggu proses bisnis utama SIPIM, tetapi memperkuat aspek integritas dan keterlacakan transaksi. Setiap perubahan status maupun perubahan isi dokumen direpresentasikan sebagai blok baru yang terikat secara kriptografis. Dengan demikian, sistem mampu menjawab permasalahan yang telah diuraikan pada bagian pendahuluan, khususnya terkait risiko perubahan data tanpa histori yang jelas dan keterbatasan mekanisme log konvensional.

Temuan ini sejalan dengan konsep *blockchain-based audit trail* yang dikemukakan oleh Regueiro dkk. [2] serta mendukung pandangan Zhang dkk. [1] bahwa karakteristik *immutability* dan keterikatan hash antarblok mampu memperkuat auditabilitas sistem. Dalam konteks sistem akuntansi, hasil ini juga konsisten dengan Ramadhani, Ananda, dan Azmi [15] yang menegaskan bahwa teknologi *blockchain* dapat meningkatkan integritas pencatatan transaksi melalui pendekatan kriptografis.

Berbeda dengan pendekatan yang membangun sistem *blockchain* sebagai platform utama yang menggantikan sistem lama, penelitian ini menunjukkan bahwa ledger dapat diintegrasikan sebagai lapisan audit tambahan tanpa mengubah struktur basis data utama. Pendekatan ini lebih realistis dan sesuai dengan kebutuhan institusi pendidikan tinggi yang telah memiliki sistem operasional yang stabil.

Dengan demikian, hasil pengujian fungsional tidak hanya menunjukkan bahwa sistem bekerja secara teknis, tetapi juga membuktikan secara empiris bahwa mekanisme *hash-chaining* mampu meningkatkan integritas, *traceability*, dan kemampuan deteksi manipulasi dalam pengelolaan anggaran perguruan tinggi.

3.4 Hasil Pengujian Integritas Rantai

Pengujian integritas rantai dilakukan untuk mengevaluasi konsistensi keterikatan antarblok dalam ledger setelah seluruh transaksi dicatat. Validasi integritas dihitung menggunakan Persamaan (3), yaitu dengan membandingkan jumlah blok yang valid terhadap total blok dalam rantai. Pengujian dilakukan pada tiga skenario skala transaksi, yaitu 100, 300, dan 500 blok, untuk melihat stabilitas sistem pada volume transaksi yang berbeda.

Tabel 3. Hasil Validasi Tanpa Manipulasi

Jumlah Blok	Validitas (%)
100	100
300	100
500	100

Tabel 3 menunjukkan bahwa seluruh blok dalam rantai berada dalam kondisi valid ketika tidak terjadi perubahan pasca pencatatan. Nilai validitas sebesar 100% pada seluruh skenario menunjukkan bahwa setiap nilai (H*i*) yang dihitung ulang konsisten dengan nilai yang tersimpan pada ledger. Hal ini menegaskan bahwa mekanisme pembentukan blok berbasis Persamaan (2) menghasilkan struktur rantai yang stabil dan tidak mengalami inkonsistensi pada kondisi normal.

Pengujian selanjutnya dilakukan dengan mensimulasikan manipulasi pada satu blok yang bukan blok terakhir. Manipulasi dilakukan dengan mengubah salah satu elemen metadata (M*i*) atau isi dokumen yang memengaruhi nilai (D*i*), tanpa membentuk blok baru. Setelah perubahan dilakukan, sistem menghitung ulang nilai hash blok menggunakan Persamaan (2), kemudian menghitung tingkat validitas rantai menggunakan Persamaan (3).

Tabel 4. Hasil Validasi Setelah Manipulasi

Jumlah Blok	Blok Dimanipulasi	Validitas (%)
100	45	44
300	128	42.3
500	210	41.8

Tabel 4 menunjukkan bahwa setelah manipulasi dilakukan, nilai validitas rantai turun secara signifikan dari 100% menjadi di bawah 50% pada seluruh skenario. Penurunan ini terjadi karena perubahan pada satu blok menyebabkan ketidaksesuaian nilai (H*i*) pada blok tersebut, yang kemudian merambat ke seluruh blok setelahnya akibat keterikatan dengan (H_{i-1}). Dengan demikian, satu perubahan lokal menghasilkan dampak global terhadap konsistensi rantai.

Secara teknis, setelah manipulasi dilakukan, sistem menghitung ulang hash setiap blok menggunakan Persamaan (2). Karena nilai metadata atau dokumen berubah, nilai hash blok yang bersangkutan tidak lagi sama dengan nilai yang tersimpan. Blok berikutnya yang menggunakan nilai tersebut sebagai (H_{i-1}) juga menjadi tidak valid. Proses ini menyebabkan jumlah blok valid berkurang drastis ketika dihitung menggunakan Persamaan (3).

Hasil ini menunjukkan bahwa sistem memiliki karakteristik *tamper-evident*, yaitu setiap perubahan pada histori transaksi akan meninggalkan jejak inkonsistensi yang dapat dideteksi secara matematis. Mekanisme ini secara langsung menjawab permasalahan yang diidentifikasi pada bagian pendahuluan, khususnya risiko perubahan data tanpa rekam jejak yang jelas dan potensi modifikasi histori oleh pihak yang memiliki akses administratif.

Menariknya, nilai validitas setelah manipulasi relatif konsisten pada berbagai skala blok. Hal ini menunjukkan bahwa kemampuan deteksi tidak bergantung pada jumlah total transaksi, melainkan pada struktur keterikatan hash antarblok. Dengan kata lain, semakin panjang rantai, semakin besar dampak propagasi inkonsistensi akibat satu perubahan.

Temuan ini sejalan dengan konsep *hash-chaining* dalam literatur *blockchain-based audit trail* yang menyatakan bahwa perubahan pada satu blok akan memengaruhi seluruh blok berikutnya [2]. Selain itu, hasil ini mendukung karakteristik *immutability* dan *integrity assurance* sebagaimana dibahas oleh Zhang dkk. [1]. Dalam konteks sistem akuntansi, mekanisme ini relevan dengan prinsip keandalan pencatatan transaksi yang ditegaskan oleh Ramadhani, Ananda, dan Azmi [15], di mana setiap transaksi harus dapat diverifikasi dan tidak mudah dimodifikasi tanpa jejak.

Secara keseluruhan, pengujian integritas rantai membuktikan bahwa mekanisme validasi berbasis Persamaan (2) dan Persamaan (3) tidak hanya bekerja secara teoritis, tetapi juga efektif dalam mendeteksi perubahan tidak sah dalam konteks pengelolaan anggaran perguruan tinggi. Integrasi ledger sebagai lapisan audit tambahan mampu memberikan jaminan integritas yang lebih kuat dibandingkan mekanisme log konvensional pada basis data relasional.

3.5 Hasil Pengujian Performa

Selain pengujian integritas dan validitas rantai, penelitian ini juga mengevaluasi aspek performa sistem untuk memastikan bahwa integrasi *permissioned blockchain ledger* tidak menimbulkan beban komputasi yang signifikan terhadap proses operasional SIPIM. Parameter utama yang dianalisis adalah waktu pembentukan blok, yang dihitung menggunakan Persamaan (4), yaitu sebagai penjumlahan antara waktu komputasi hash dan waktu penulisan data ke basis data.

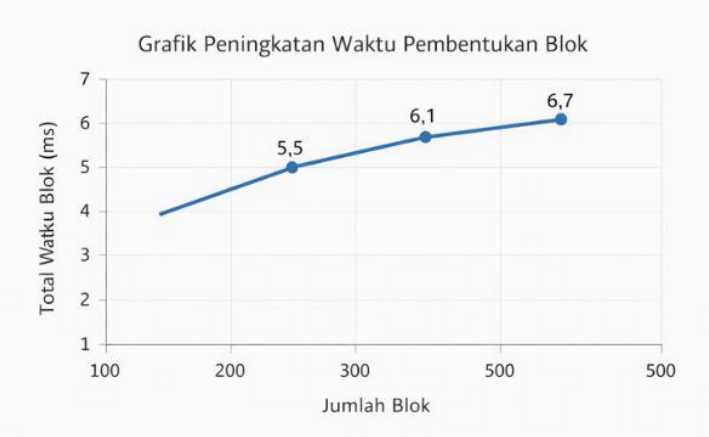
Pengujian dilakukan pada tiga skenario skala transaksi, yaitu 100, 300, dan 500 blok, dengan masing-masing skenario diuji melalui beberapa replikasi untuk memperoleh nilai rata-rata yang representatif. Hasil pengukuran dirangkum pada Tabel 5.

Tabel 5. Rata-rata Waktu Pembentukan Blok

Jumlah Blok	Waktu Hash (ms)	Waktu Tulis (ms)	Total Waktu Blok (ms)
100	2.1	3.4	5.5
300	2.3	3.8	6.1
500	2.5	4.2	6.7

Tabel 5 menunjukkan bahwa waktu komputasi hash relatif stabil pada rentang 2–3 milidetik, sementara waktu penulisan ke basis data berada pada rentang 3–4 milidetik. Nilai total waktu pembentukan blok dihitung berdasarkan Persamaan (4) dan menunjukkan peningkatan yang bersifat gradual seiring bertambahnya jumlah blok. Pada skenario 100 blok, waktu rata-rata pembentukan blok sebesar 5,5 milidetik. Ketika jumlah blok meningkat menjadi 300 dan 500, waktu rata-rata meningkat menjadi 6,1 dan 6,7 milidetik. Peningkatan ini bersifat hampir linear dan tidak menunjukkan lonjakan eksponensial. Dengan demikian, kompleksitas waktu pembentukan blok dapat dikategorikan stabil dalam rentang pengujian.

Gambar 2 menunjukkan tren peningkatan waktu pembentukan blok berdasarkan jumlah blok dalam rantai.



Gambar 2. Grafik Peningkatan Waktu Pembentukan Blok

Pada Gambar 2 terlihat bahwa kurva peningkatan waktu memiliki kemiringan yang relatif rendah. Hal ini menunjukkan bahwa pertambahan jumlah blok dalam rantai tidak menyebabkan degradasi performa yang signifikan. Waktu komputasi hash tidak dipengaruhi secara langsung oleh panjang rantai, karena perhitungan dilakukan pada blok yang sedang dibentuk. Sementara itu, peningkatan kecil pada waktu penulisan kemungkinan dipengaruhi oleh pertambahan ukuran tabel ledger dan indeks basis data.

Jika dikaitkan dengan kebutuhan operasional penganggaran perguruan tinggi, nilai waktu pembentukan blok yang berada di bawah 7 milidetik dapat dikategorikan sangat rendah dan tidak akan memengaruhi respons antarmuka pengguna secara signifikan. Hal ini menunjukkan bahwa integrasi ledger sebagai lapisan audit tambahan tetap mempertahankan efisiensi sistem utama.

Temuan ini juga menguatkan bahwa pendekatan *permissioned blockchain* yang digunakan lebih ringan dibandingkan model *proof-of-work* pada *blockchain* publik, yang umumnya memerlukan waktu komputasi jauh lebih besar. Dengan desain yang terkontrol dan tidak memerlukan mekanisme konsensus komputasi berat, sistem tetap mampu menjaga integritas tanpa mengorbankan performa.

Secara keseluruhan, hasil pengujian performa menunjukkan bahwa mekanisme pembentukan blok berbasis Persamaan (4) memiliki overhead yang minimal dan dapat diterima dalam konteks sistem informasi penganggaran. Dengan demikian, integrasi ledger tidak hanya efektif dari sisi integritas dan deteksi manipulasi, tetapi juga layak diterapkan dari sisi efisiensi operasional.

Hasil penelitian ini menunjukkan bahwa integrasi *permissioned blockchain ledger* sebagai lapisan audit tambahan pada SIPIM mampu menjawab permasalahan utama yang diidentifikasi pada bagian pendahuluan, yaitu risiko perubahan data tanpa rekam jejak yang jelas, keterbatasan audit trail berbasis log konvensional, serta potensi manipulasi histori transaksi oleh pihak yang memiliki akses administratif.

Integritas Data dan Immutability Integritas data dalam penelitian ini dijaga melalui mekanisme hash dokumen dan hash blok sebagaimana dirumuskan pada Persamaan (1) dan Persamaan (2). Mekanisme ini memastikan bahwa setiap dokumen RKAT dan KAK direpresentasikan dalam bentuk hash kriptografis yang bersifat unik dan deterministik. Setiap perubahan sekecil apa pun pada dokumen akan menghasilkan nilai hash yang berbeda, sehingga integritas dokumen dapat diverifikasi tanpa harus membandingkan isi file secara manual. Lebih lanjut, keterikatan antara hash blok saat ini dan hash blok sebelumnya membentuk struktur *hash chain* yang menciptakan sifat tidak dapat diubah tanpa terdeteksi (*tamper-evident*). Hasil pengujian integritas rantai pada bagian 3.4 menunjukkan bahwa manipulasi pada satu blok menyebabkan penurunan validitas rantai secara signifikan. Hal ini memperkuat karakteristik *immutability* yang dijelaskan oleh Zhang dkk. [1] , bahwa *blockchain* menyediakan jaminan integritas melalui mekanisme keterikatan kriptografis antarblok. Berbeda dengan sistem basis data relasional konvensional yang memungkinkan operasi *update* dan *delete*, pendekatan ini menerapkan prinsip *append-only*. Setiap perubahan status atau revisi dokumen tidak menggantikan data lama, tetapi menghasilkan blok baru yang merekam histori transaksi. Dengan demikian, sistem tidak hanya menjaga integritas data, tetapi juga membangun jejak audit yang kronologis dan konsisten.

Deteksi Manipulasi dan Audit Trail. Kemampuan deteksi manipulasi dalam penelitian ini dibuktikan melalui validasi berbasis Persamaan (3). Ketika dilakukan perubahan pada metadata atau isi dokumen setelah pencatatan blok, nilai hash yang dihitung ulang tidak lagi sesuai dengan nilai yang tersimpan pada ledger. Ketidaksesuaian ini menurunkan tingkat validitas rantai secara signifikan, sebagaimana ditunjukkan pada Tabel 4. Temuan ini menunjukkan bahwa sistem memiliki kemampuan deteksi manipulasi yang bersifat deterministik dan matematis. Deteksi tidak bergantung pada pemeriksaan manual atau kepercayaan terhadap administrator sistem, melainkan pada konsistensi perhitungan hash. Hal ini sejalan dengan konsep *blockchain-based audit trail mechanism* yang dikemukakan oleh Regueiro dkk [2] yang menekankan bahwa audit trail berbasis hash mampu mendeteksi perubahan histori secara otomatis melalui verifikasi kriptografis. Dalam konteks penganggaran perguruan tinggi, mekanisme ini sangat relevan untuk menjawab pertanyaan audit seperti: siapa yang melakukan perubahan, kapan perubahan dilakukan, dan apakah dokumen saat ini identik dengan dokumen yang telah disetujui. Dengan ledger yang terikat secara kriptografis, setiap perubahan pasca pencatatan akan meninggalkan jejak inkonsistensi yang dapat diverifikasi ulang kapan saja.

Implikasi terhadap Sistem Akuntansi. Dalam perspektif sistem akuntansi, hasil penelitian ini konsisten dengan pandangan Ramadhani, Ananda, dan Azmi [15] yang menyatakan bahwa *blockchain* memiliki potensi memperkuat integritas pencatatan transaksi melalui mekanisme kriptografis. Sistem akuntansi menuntut prinsip keandalan (*reliability*) dan keterverifikasian (*verifiability*). Mekanisme *hash-chaining* yang diterapkan dalam penelitian ini memenuhi kedua prinsip tersebut karena:

1. Setiap transaksi memiliki representasi kriptografis unik.
2. Histori transaksi tidak dapat diubah tanpa terdeteksi.
3. Proses verifikasi dapat dilakukan ulang secara independen.

Dengan demikian, ledger tidak hanya berfungsi sebagai pencatat teknis, tetapi sebagai instrumen penguatan tata kelola (*governance mechanism*). Integrasi ini memperluas fungsi sistem informasi dari sekadar pengolah data menjadi sistem yang menyediakan bukti integritas berbasis kriptografi.

Performa dan Kelayakan Implementasi. Dari sisi performa, hasil pada bagian 3.5 menunjukkan bahwa *overhead* pembentukan blok tetap berada di bawah 7 milidetik bahkan pada skala 500 blok. Peningkatan waktu bersifat linear dan tidak menunjukkan degradasi eksponensial. Hal ini menunjukkan bahwa mekanisme berbasis Persamaan (4) memiliki kompleksitas yang stabil dan dapat diterapkan tanpa mengganggu respons antarmuka pengguna. Temuan ini penting karena salah satu kritik terhadap teknologi *blockchain* adalah beban komputasi yang tinggi, terutama pada model *proof-of-work* sebagaimana dijelaskan pada implementasi *blockchain* publik [14]. Namun, pendekatan *permissioned blockchain* yang digunakan dalam penelitian ini tidak memerlukan mekanisme konsensus komputasi berat. Dengan demikian, sistem tetap efisien sekaligus mempertahankan integritas.

Kontribusi dan Perbedaan dengan Penelitian Terdahulu. Berbeda dengan pendekatan yang membangun *blockchain* sebagai sistem utama yang menggantikan sistem lama [3] penelitian ini menunjukkan bahwa *ledger* dapat diintegrasikan sebagai lapisan audit tambahan tanpa mengubah struktur basis data operasional yang telah berjalan. Pendekatan ini bersifat *non-invasif* dan realistis untuk institusi yang telah memiliki sistem informasi stabil.

Kontribusi utama penelitian ini terletak pada:

1. Perancangan arsitektur integrasi sidecar yang memungkinkan coexistence antara sistem relasional dan ledger *blockchain*.

2. Implementasi mekanisme *hash-chaining* sebagai *audit layer*, bukan sebagai platform pengganti.
3. Evaluasi empiris yang mencakup integritas, deteksi manipulasi, dan performa secara kuantitatif.

Dengan pendekatan ini, penelitian tidak hanya membuktikan konsep secara teoretis, tetapi juga menunjukkan kelayakan operasional dalam konteks pengelolaan anggaran perguruan tinggi.

4. Kesimpulan

Penelitian ini berhasil merancang dan mengimplementasikan integrasi *permissioned blockchain event ledger* sebagai lapisan audit tambahan pada Sistem Informasi Kepemimpinan (SIPIM) untuk mendukung pengelolaan anggaran RKAT dan KAK. Arsitektur integrasi yang dikembangkan memungkinkan sistem operasional tetap berjalan pada basis data relasional yang telah ada, sementara ledger berfungsi sebagai mekanisme pencatatan kriptografis yang bersifat *append-only*. Dengan pendekatan ini, tujuan penelitian untuk merancang arsitektur integrasi yang kompatibel tanpa mengganggu proses bisnis utama telah tercapai.

Struktur blok dan mekanisme *hash-chaining* yang diterapkan mampu menjamin integritas dokumen dan keterikatan histori transaksi secara kriptografis. Setiap perubahan pada dokumen atau metadata transaksi menghasilkan nilai hash yang berbeda dan membentuk blok baru yang terhubung dengan blok sebelumnya. Hasil pengujian menunjukkan bahwa seluruh blok berada dalam kondisi valid pada skenario tanpa manipulasi, sedangkan simulasi perubahan data pasca pencatatan menyebabkan penurunan validitas rantai secara signifikan. Temuan ini membuktikan bahwa sistem memiliki karakteristik *tamper-evident* dan mampu mendeteksi inkonsistensi histori transaksi secara matematis.

Dari sisi performa, waktu pembentukan blok menunjukkan peningkatan yang bersifat linear dan tetap berada dalam rentang milidetik, sehingga tidak menimbulkan degradasi kinerja yang berarti terhadap sistem utama. Hal ini menunjukkan bahwa integrasi ledger sebagai lapisan audit tambahan layak diterapkan dalam lingkungan operasional perguruan tinggi tanpa mengorbankan efisiensi sistem.

Secara praktis, penelitian ini memberikan model implementasi bertahap bagi institusi pendidikan tinggi yang ingin memperkuat transparansi dan akuntabilitas pengelolaan anggaran tanpa mengganti sistem informasi yang telah berjalan. Integrasi non-invasif ini membuka kemungkinan penerapan serupa pada modul keuangan lain seperti realisasi anggaran, monitoring kontrak, maupun pengadaan internal.

Untuk penelitian selanjutnya, pengembangan dapat diarahkan pada integrasi mekanisme tanda tangan digital terdistribusi, penerapan konsensus multi-node dalam skala institusi, serta evaluasi keamanan terhadap skenario serangan yang lebih kompleks. Selain itu, pengujian pada lingkungan produksi dengan volume transaksi yang lebih besar akan memberikan gambaran yang lebih komprehensif mengenai skalabilitas sistem. Dengan demikian, pendekatan ini memiliki potensi untuk dikembangkan lebih lanjut sebagai kerangka penguatan tata kelola berbasis kriptografi dalam sistem informasi perguruan tinggi

5. Ucapan Terima Kasih *(Optional)*

Penulis menyampaikan terima kasih kepada Universitas Slamet Riyadi Surakarta atas dukungan dan fasilitas yang diberikan dalam pelaksanaan penelitian ini, serta kepada tim pengelola SIPIM dan pihak-pihak terkait yang telah memberikan bantuan teknis, data, dan masukan selama proses perancangan, implementasi, dan pengujian sistem sehingga penelitian ini dapat terselesaikan dengan baik

6. Daftar Pustaka

[1] Y. Zhang, Z. Ma, dan J. Meng, "Auditing in the blockchain: a literature review," *Frontiers in Blockchain*, vol. 8, no. April, hlm. 1–6, 2025, doi: 10.3389/fbloc.2025.1549729.

[2] C. Regueiro, I. Seco, I. Gutiérrez-Agüero, B. Urquizu, dan J. Mansell, "A blockchain-based audit trail mechanism: Design and implementation," *Algorithms*, vol. 14, no. 12, 2021, doi: 10.3390/a14120341.

[3] A. P. Satria dan R. Ruliansyah, "Analisis Penerapan Blockchain untuk Meningkatkan Transparansi dan Efisiensi dalam Operasional Bisnis PT. Martimbang Jaya Utama," *Jurnal Pendidikan Tambusai*, vol. 8, no. 3, hlm. 46588–46598, 2024, [Daring]. Tersedia pada: http://jptam.org/index.php/jptam/article/view/22840

[4] T. I. Ramdhani, N. N. Faiza, M. Wulandari, A. D. Nastiti, dan H. Kurniawan, "*CFPChain*: Optimalisasi Sistem Seleksi Pendanaan Riset BRIN Menggunakan Pendekatan Berbasis Konsorsium *Blockchain*," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 11, no. 1, hlm. 27–36, 2024, doi: 10.25126/jtiik.20241116676.

[5] V. Palidita Febriana, T. Suci Wulandari, Z. Azmi, dan U. Muhammadiyah Riau, "Penggunaan Teknologi Blockchain Dalam Sistem Informasi Akuntansi : Peluang Dan Tantangan," *Jurnal Akuntansi AKTIVA*, vol. 5, no. 1, hlm. 39–45, 2024.

[6] E. D. Kusumawati, Karjono, dan Karmanis, "Integrasi Teknologi Blockchain terhadap Transparansi, Akuntabilitas, dan Efisiensi dalam Sistem Pengadaan Barang dan Jasa di Sektor Maritim," *Jurnal TRANSMA*, vol. 1, no. 2, hlm. 87–96, 2025, [Daring]. Tersedia pada: https://jurnal.poltekpelni.ac.id/index.php/transma/article/view/67

[7] S. Huda, K. Kusrini, dan K. Kusnawi, "Implementation of Blockchain for Integrated Civil Service Statistical Data (Case Study: Civil Service and Human Resource Development Agency of Madiun Regency, East Java Province)," *Journal of Electrical Engineering and Computer (JEECOM)*, vol. 7, no. 2, hlm. 374–382, 2025, doi: 10.33650/jeecom.v7i2.12170.

[8] M. Ismail, A. Azwar, B. Baharuddin, dan H. Hamria, "Analisis Penggunaan Teknologi Blockchain dalam Meningkatkan Keamanan Data: Studi Kasus Industri Keuangan," *Jurnal Janitra Informatika dan Sistem Informasi*, vol. 5, no. 1, hlm. 69–77, 2025, doi: 10.59395/m9krbe73.

[9] B. H. Purnomo, D. A. Rismayadi, dan M. R. F. Thoriq, "Adopsi Blockchain sebagai Solusi Keamanan dan Transparansi Transaksi Digital di Industri Fintech," *Jurnal Minfo Polgan*, vol. 13, no. 2, hlm. 2486–2492, 2025, doi: 10.33395/jmp.v13i2.14523.

[10] M. U. Rahman, "Scalable Role-based Access Control Using The EOS Blockchain," 2020, [Daring]. Tersedia pada: http://arxiv.org/abs/2007.02163

[11] M. N. Dzakie, A. Bhawiyuga, dan A. Basuki, "Sistem Berbasis Private Blockchain sebagai Penyedia Layanan Autentikasi Publisher-Broker-Subscriber Pada Protokol Message Queue Telemetry Transport," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 9, no. 4, hlm. 675–682, 2022, doi: 10.25126/jtiik.2022945752.

[12] H. P. Fitria, M. Anggraeni, D. T. Zulkifli, S. W. Datussyuhada, dan I. Rudiansyah, "Analisis Literatur: Peran Smart Contract dalam Meningkatkan Transparansi Akses dan Keamanan Data pada Jaringan Blockchain," *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, vol. 8, no. 1, hlm. 323–326, 2025, doi: 10.32672/jnkti.v8i1.8649.

[13] S. Abdullah, "Implementasi Blockchain untuk Keamanan Data Akademik dalam Sistem Informasi Perguruan Tinggi," *Go Infotech: Jurnal Ilmiah STMIK AUB*, vol. 31, no. 1, hlm. 149–160, 2025, doi: 10.36309/goi.v31i1.371.

[14] Annisya dan E. Haryatmi, "Implementasi Teknologi Blockchain Proof of Work Pada Penelusuran Supply Chain Produk Komputer," *Jurnal RESTI*, vol. 5, no. 3, hlm. 446–455, 2021, doi: 10.29207/resti.v5i3.3068.

[15] A. Ramadhani, D. A. Ananda, dan Z. Azmi, "Teknologi Blockchain dan Sistem Akuntansi : Potensi dan Tantangan," *Indonesian Journal of Economics , Management , and Accounting*, vol. 1, no. 1, hlm. 37–48, 2024.