INTERGRITAS DATA RIWAYAT KOPI GAYO MELALUI PROTOKOL ZERO-TRUST ETHEREUM

Haekal Mimtazulfaqhi Zaydan[1], Devi Damayanti[2]
Program Studi Teknik Informatika, Fakultas Ilmu Komputer
Universitas Pamulang[1,2]
Jalan Raya Puspitek No. 46, Buaran, Kec.Pamulang, Kota Tangerang Selatan, Banten
zaydan281003@gmail.com[1], dosen02390@unpam.ac.id[2]

Abstrak

Arsitektur sistem informasi logistik konvensional pada rantai pasok Kopi Gayo memiliki kerentanan struktural berupa titik kegagalan tunggal (*single point of failure*), di mana ketergantungan pada otorisasi terpusat memicu risiko manipulasi data retrospektif (*database tampering*). Hal ini mendegradasi transparansi dan gagal memberikan jaminan nirsangkal (*non-repudiation*) secara komputasional. Penelitian ini mengusulkan model pelacakan rantai pasok berbasis arsitektur hibrida Web2 dan Web3 untuk memitigasi asimetri informasi melalui implementasi protokol *Zero-Trust* pada jaringan Ethereum (Sepolia Testnet). Sistem ini memisahkan beban kerja komputasi: basis data relasional bertindak sebagai *buffer* berlatensi rendah untuk konsensus otorisasi berjenjang (*Maker-Checker*), sementara *smart contract* berbasis Solidity difungsikan sebagai lapisan notarisasi terdesentralisasi. *Payload* logistik yang tervalidasi dikunci secara kriptografis ke dalam blok jaringan untuk memastikan kekekalan data (*immutability*). Evaluasi arsitektural menunjukkan bahwa sistem berhasil memfasilitasi ekstraksi data *Zero-Trust*; di mana konsumen dapat memvalidasi *Transaction Hash* (TxHash) secara independen melalui pemindaian kode QR, yang secara langsung mem- *bypass* peladen internal untuk menarik data dari *node blockchain*. Pendekatan ini terbukti secara empiris mampu menciptakan integritas riwayat produk yang anti-manipulasi dan transparan.

Kata Kunci: *Blockchain Ethereum*, Integritas Data, Protokol *Zero-Trust*, *Smart Contract*, Kopi Gayo

Abstract

The conventional logistics information system architecture in the Gayo coffee supply chain suffers from a structural vulnerability in the form of a single point of failure, where reliance on centralized authorization introduces the risk of retrospective database tampering. This degrades transparency and fails to provide computational non-repudiation guarantees. This research proposes a supply chain tracking model based on a hybrid Web2 and Web3 architecture to mitigate information asymmetry through the implementation of a Zero-Trust protocol on the Ethereum network (Sepolia Testnet). The system decouples computational workloads: a relational database acts as a low-latency buffer for tiered authorization consensus (Maker-Checker), while a Solidity-based smart contract serves as a decentralized notarization layer. Validated logistical payloads are cryptographically locked into network blocks to ensure data immutability. Architectural evaluation demonstrates that the system successfully facilitates Zero-Trust data extraction; consumers can independently validate the Transaction Hash (TxHash) via QR code scanning, directly bypassing internal servers to retrieve data from blockchain nodes. This approach is empirically proven to establish anti-manipulation and transparent product history integrity.

***Keyword**: Ethereum Blockchain, Data Integrity, Zero-Trust Protocol, Smart Contract, Gayo Coffee*

PENDAHULUAN

Rantai pasok komoditas kopi global, termasuk Kopi Gayo, memiliki tingkat kompleksitas operasional yang tinggi dan sangat rentan terhadap asimetri informasi serta kendala transparansi (Ruggieri et al., 2026). Sistem informasi logistik konvensional yang beroperasi saat ini mayoritas masih bertumpu pada arsitektur basis data yang terpusat, yang menciptakan kerentanan struktural berupa titik kegagalan tunggal atau *single point of failure* (Farina et al., 2025). Ketergantungan pada otorisasi sentralistik ini membuka celah keamanan yang signifikan terhadap risiko manipulasi data secara retrospektif (*database tampering*) oleh pemegang hak akses internal, sehingga sistem gagal memberikan jaminan transparansi dan akuntabilitas nirsangkal (*non-repudiation*) bagi seluruh

pemangku kepentingan. Akibatnya, konsumen dan rantai ritel sering kali menghadapi "kotak hitam" operasional yang mengaburkan visibilitas rekam jejak produk dan menurunkan tingkat kepercayaan terhadap keaslian indikasi geografis serta kualitas komoditas tersebut.

Untuk memitigasi kerentanan arsitektural pada sistem terpusat, integrasi teknologi *blockchain* dengan kerangka *Zero-Trust Architecture* (ZTA) hadir sebagai paradigma keamanan siber yang transformatif dan tangguh. Berbeda dengan model keamanan perimeter tradisional, protokol *Zero-Trust* beroperasi pada prinsip fundamental "tidak pernah percaya, selalu verifikasi", yang memastikan bahwa setiap interaksi dan permintaan akses diautentikasi secara ketat tanpa memandang lokasi jaringan (Uzougbo et al., 2025). Ketika dikombinasikan dengan buku besar terdesentralisasi (*distributed ledger*) dari teknologi *blockchain*, arsitektur ini mampu menciptakan lapisan notarisasi yang menjamin kekekalan data (*immutability*). Pemanfaatan *smart contract* sebagai lapisan notarisasi dalam ekosistem ini memungkinkan otomatisasi validasi data logistik secara kriptografis, sehingga rekam jejak produk terjamin kekekalannya (*immutability*) dan resisten terhadap modifikasi sepihak oleh entitas perantara (Zheng et al., 2022).

Berdasarkan urgensi tersebut, penelitian ini mengusulkan pengembangan model pelacakan rantai pasok Kopi Gayo yang mengimplementasikan arsitektur hibrida antara lingkungan Web2 dan Web3 melalui pendekatan protokol *Zero-Trust*. Sistem ini dirancang untuk mendistribusikan beban kerja secara asinkron; memanfaatkan basis data relasional sebagai penyangga operasional (*buffer*) berlatensi rendah untuk memfasilitasi konsensus otorisasi berjenjang (*Maker-Checker*), sekaligus mengeksekusi *smart contract* pada jaringan Ethereum (*Sepolia Testnet*) sebagai pencatat kekekalan data paska-otorisasi. Pendekatan hibrida ini tidak hanya memecahkan masalah inefisiensi transaksi pada rantai pasok, tetapi juga memungkinkan ekstraksi riwayat data secara independen oleh konsumen akhir. Melalui pemindaian *Quick Response* (QR) *Code*, konsumen dapat memvalidasi bukti transaksi (*TxHash*) langsung dari *node blockchain* dengan memotong jalur ketergantungan pada peladen internal distributor, sehingga menciptakan ekosistem logistik Kopi Gayo yang sepenuhnya transparan, anti-manipulasi, dan dapat dipertanggungjawabkan secara komputasional.

PENELITIAN RELEVAN

Beberapa penelitian terdahulu telah mengkaji evolusi arsitektur sistem informasi dalam manajemen rantai pasok dan logistik. Pada tingkat infrastruktur terpusat (Web2), Tarigan et al. (2024) membuktikan bahwa pengembangan sistem kontrol inventaris terkomputerisasi sangat krusial untuk meningkatkan visibilitas stok barang dan riwayat transaksi operasional secara efisien. Meskipun arsitektur konvensional tersebut sangat efektif untuk pengawasan internal, titik penyimpanannya yang terpusat masih membutuhkan eskalasi pengamanan untuk mencegah manipulasi data sepihak. Oleh karena itu, penelitian terkini mulai mengadopsi teknologi desentralisasi guna menutup celah tersebut. Sebagai contoh, Petrillo et al. (2025) mengembangkan kerangka aplikasi seluler yang mengintegrasikan teknologi blockchain, RFID, dan kode batang untuk melacak data rantai pasok kopi secara komprehensif, di mana sistem tersebut terbukti mampu meningkatkan transparansi, pelacakan, serta efisiensi operasional dari petani hingga ke konsumen. Di sisi lain, dalam konteks keamanan jaringan dan perangkat, Nie et al. (2025) mengusulkan mekanisme kontrol akses *zero-trust* berbasis *blockchain* dan enkripsi *inner-product* pada lingkungan *Internet of Things* (IoT). Penelitian tersebut menunjukkan bahwa penerapan arsitektur *zero-trust* terdesentralisasi sangat efektif dalam mengelola identitas dan membatasi akses entitas secara dinamis tanpa bergantung pada otoritas terpusat, sehingga mampu memitigasi kerentanan titik kegagalan tunggal (*single point of failure*) secara signifikan.

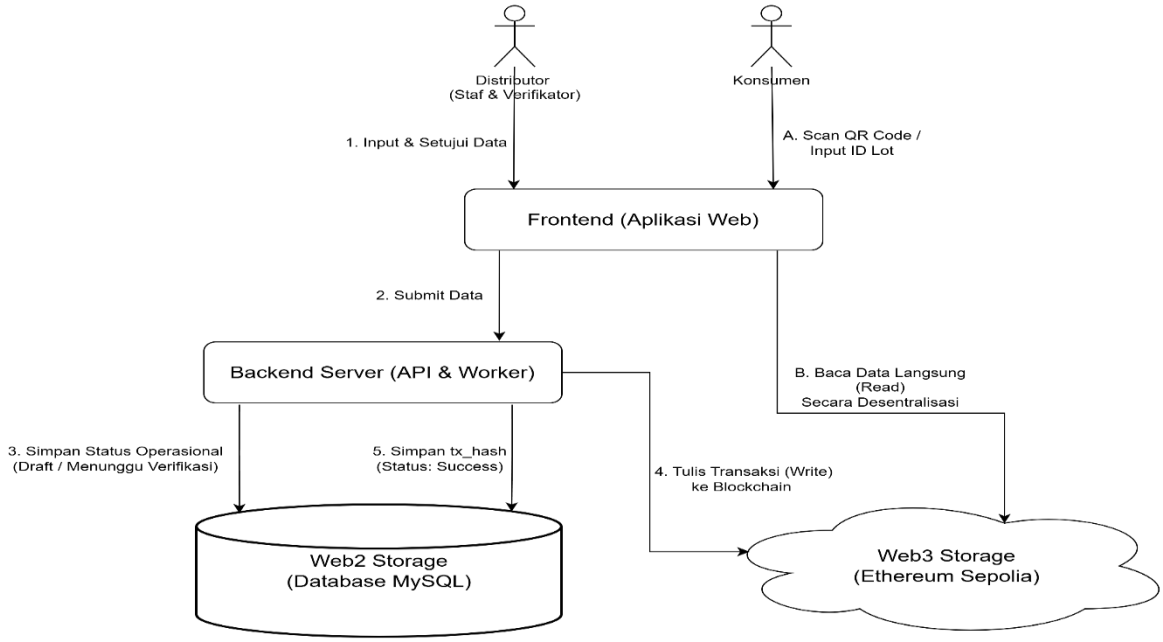
Meskipun inovasi ketertelusuran dan keamanan *zero-trust* telah banyak dieksplorasi, tantangan fundamental terkait keandalan data dari dunia nyata yang dimasukkan ke dalam jaringan *blockchain* yang dikenal dengan istilah *Oracle Problem* masih menjadi celah keamanan yang kritis. Caldarelli dan Ornaghi (2026) menganalisis kerentanan ini dan menegaskan bahwa solusi teknis desentralisasi semata tidak cukup untuk mencegah manipulasi data; diperlukan mekanisme tata kelola dan desain prosedural yang terstruktur pada titik masuk data (*oracle*) untuk memastikan validitas informasi yang direkam. Berdasarkan tinjauan tersebut, penelitian-penelitian terdahulu umumnya masih berfokus pada pelacakan produk secara fungsional atau arsitektur keamanan infrastruktur semata, namun

belum ada yang secara spesifik merancang arsitektur pelacakan hibrida (Web2 dan Web3) yang mengintegrasikan otorisasi berjenjang (*Maker-Checker*) guna memitigasi kesalahan *oracle* secara internal. Penelitian ini mengisi kesenjangan (*research gap*) tersebut dengan menerapkan protokol *Zero-Trust* dan validasi internal pada jaringan Ethereum (Sepolia Testnet), yang bertujuan untuk mengunci integritas data logistik Kopi Gayo secara nirsangkal (*non-repudiation*) serta mencegah terjadinya manipulasi basis data retrospektif secara diam-diam.

METODE PENELITIAN

Metodologi yang diterapkan dalam penelitian ini adalah *Design Science Research* (DSR), sebuah pendekatan iteratif yang difokuskan pada perancangan dan validasi artefak teknologi informasi secara empiris guna mengeliminasi titik kegagalan tunggal (*single point of failure*) pada arsitektur manajemen logistik Kopi Gayo (Hassan & Smith, 2024). Objek penelitian ini berpusat pada mekanisme perlindungan integritas data logistik dari fase pascapanen hingga distribusi, dengan ruang lingkup implementasi berfokus pada protokol *Zero-Trust* menggunakan teknologi *blockchain*. Teknik pengumpulan data dilakukan melalui observasi terhadap alur pencatatan konvensional yang rentan terhadap manipulasi basis data (*database tampering*), serta studi literatur sistematis mengenai efisiensi arsitektur terdesentralisasi. Rancangan kegiatan penelitian dieksekusi melalui empat tahapan sistematis: identifikasi arsitektur masalah, perancangan solusi struktural, implementasi sistem (pengembangan artefak), dan evaluasi keandalan komputasional.

Pada tahap analisis dan perancangan, penelitian ini memformulasikan pemodelan sistem menggunakan *Unified Modeling Language* (UML) untuk memetakan alur otorisasi berjenjang (*Maker-Checker*). Perancangan ini menghasilkan arsitektur hibrida asimetris, di mana infrastruktur Web2 (Node.js, Express.js, MySQL) diimplementasikan sebagai *operational buffer* berlatensi rendah, sedangkan infrastruktur Web3 (Ethereum Sepolia Testnet, Solidity) difungsikan murni sebagai lapisan notarisasi nirsangkal (*non-repudiation*). Pada tahap implementasi, sistem menjembatani infrastruktur basis data *off-chain* dan jaringan *on-chain* menggunakan *middleware* Ethers.js guna membentuk arsitektur hibrida asimetris yang menyeimbangkan efisiensi komputasi latensi rendah dengan transparansi mutlak (Li & Wang, 2023). Sebagai validasi teknis, tahap uji coba menerapkan *White Box Testing* berbasis *Basis Path Testing* untuk mengukur dan memverifikasi *Cyclomatic Complexity* pada fungsi-fungsi asinkronus kritis, serta pengujian fungsionalitas antarmuka (*Black Box Testing*) untuk memastikan presisi pemindaian kode QR *Zero-Trust* oleh pengguna akhir tanpa latensi yang signifikan.



Gambar 1. Arsitektur Sistem Hibrida Web2 dan Web3 KopiChain

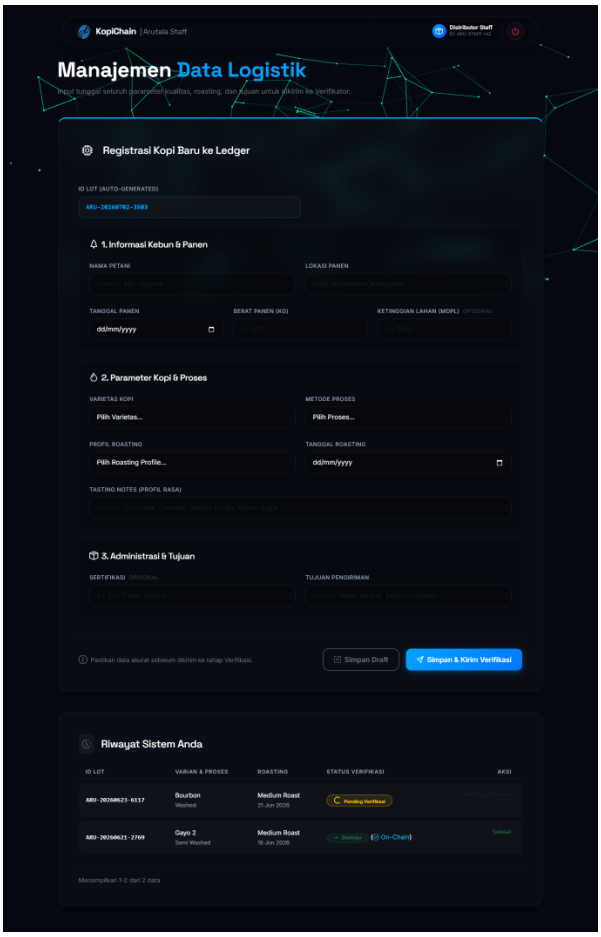
e-ISSN : 2715-8756

HASIL DAN PEMBAHASAN

Hasil dari penelitian ini merepresentasikan implementasi fungsional artefak teknologi yang dibangun berdasarkan metodologi *Design Science Research* (DSR) guna meruntuhkan asimetri informasi pada ekosistem logistik Kopi Gayo. Perangkat lunak yang dikembangkan secara empiris berhasil mendistribusikan beban kerja komputasi melalui pendekatan arsitektur hibrida (*Asymmetric Trust*). Sistem memanfaatkan sistem manajemen basis data relasional (MySQL) sebagai penyangga status operasional (*buffer*) berlatensi rendah pada lingkungan eksternal (*off-chain*), sekaligus mengintegrasikan *smart contract* di jaringan desentralisasi Ethereum (Sepolia Testnet) sebagai lapisan notarisasi absolut (*on-chain*). Evaluasi komprehensif terhadap performa arsitektur, fungsionalitas antarmuka, dan keandalan logika komputasi dijabarkan pada poin-poin berikut:

1. Implementasi Entri Data dan Otorisasi *Off-Chain*

   Tahap inisiasi data logistik dioperasikan melalui Dasbor Staf Distributor yang difungsikan sebagai titik masuk data pertama (*Maker*). Pada lapisan ini, sistem secara terstruktur menangkap parameter fisik seperti data asal kebun, metode pemrosesan, dan profil penyangraian (*roasting*) untuk direkam ke dalam basis data lokal dengan status transisional berupa 'Draf'. Arsitektur ini membuktikan bahwa kesalahan input manual dari operator (anomali *Oracle*) dapat direduksi secara internal tanpa menimbulkan kerugian biaya transaksi (*gas fee*) pada jaringan *blockchain*.

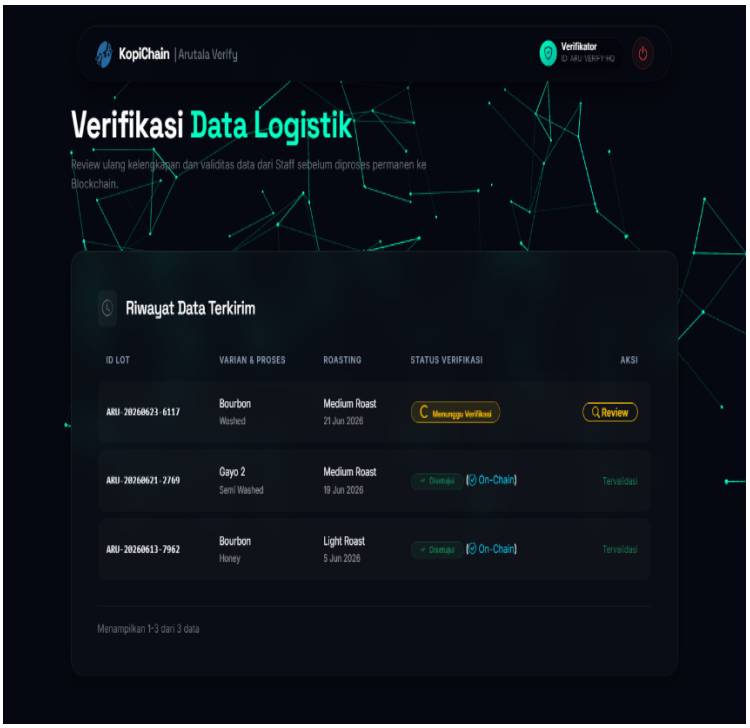


Gambar 2. Dasbor Staf Distributor

2. Eksekusi Konsensus Internal dan Injeksi *Smart Contract*

   Mekanisme pengamanan tingkat lanjut direalisasikan melalui modul Dasbor Verifikator yang bertindak sebagai lapis pengawasan akhir (*Checker*). Ketika Verifikator memvalidasi kesesuaian dokumen fisik dan memberikan persetujuan, sistem tidak sekadar memperbarui status pada basis data MySQL, melainkan memicu proses latar belakang (*background worker*) secara asinkron.

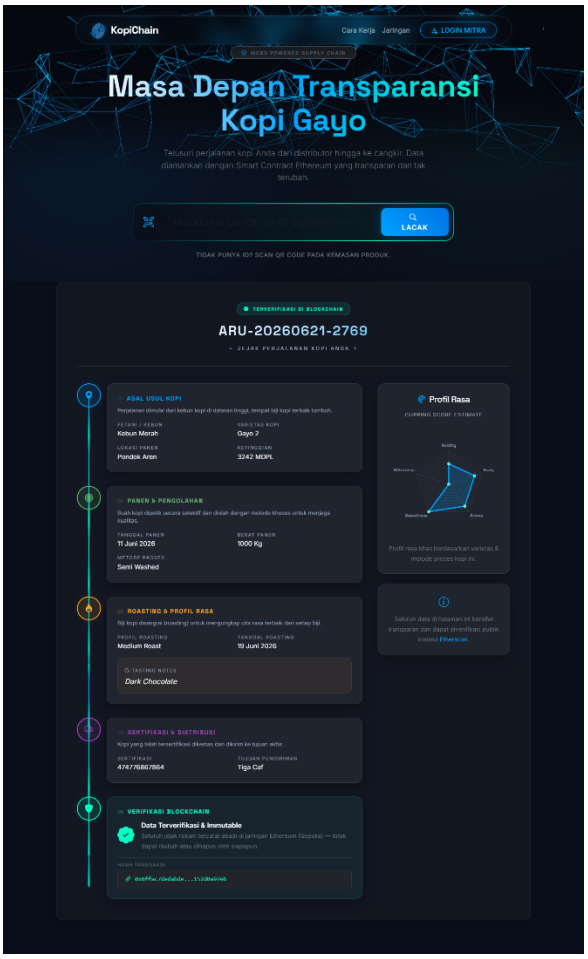
Proses komputasi ini memanfaatkan pustaka ethers.js untuk menyusun, menandatangani, dan menyebarkan muatan data (*payload*) menuju *smart contract* CoffeeTrace.sol di jaringan Ethereum. Eksekusi ini menghasilkan *Transaction Hash* (TxHash) yang ditarik kembali ke sistem lokal sebagai referensi integritas nirsangkal (*non-repudiation*).



Gambar 3. Dasbor Verifikator

3. Ekstraksi Data Pelacakan Berbasis Protokol *Zero-Trust*
   Implementasi arsitektur *Zero-Trust* pada sistem ini dibuktikan secara teknis melalui antarmuka pelacakan konsumen. Saat konsumen input id lot atau memindai *Quick Response (QR) Code* pada kemasan produk, algoritma *frontend* pada peramban web memotong jalur komunikasi terhadap peladen *backend* internal distributor. Skrip klien secara independen melakukan *Remote Procedure Call* (RPC) ke node publik Ethereum untuk menarik data logistik yang bersifat *immutable* secara langsung dari blok jaringan. Sistem kemudian merender data tersebut menjadi linimasa riwayat logistik visual yang dilengkapi dengan tautan verifikasi penjelajah blok (Etherscan), memastikan bahwa transparansi informasi terbebas dari ancaman modifikasi peladen terpusat (*server-side tampering*).

e-ISSN : 2715-8756



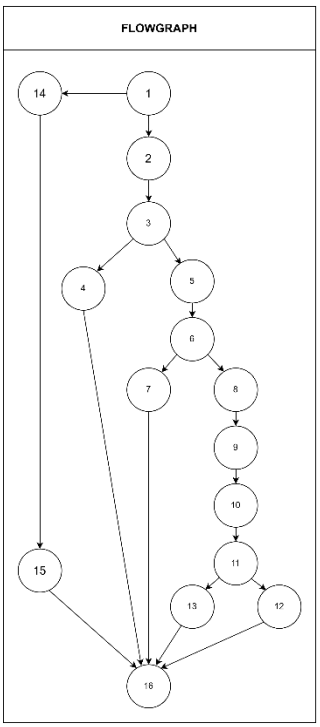
Gambar 4. Halaman Hasil Pelacakan Publik

4. Validasi Keandalan Arsitektur Melalui Pengujian Perangkat Lunak

Keandalan sistem (*system reliability*) diukur secara empiris menggunakan dua pendekatan pengujian teknis yang ketat untuk memastikan fungsionalitas lintas arsitektur berjalan tanpa galat (*error-free*). Pada tahap pertama, pengujian *Black Box* dieksekusi guna memvalidasi interaksi antarmuka operasional. Hasil pengujian mengonfirmasi bahwa mekanisme autentikasi *stateless* berbasis JSON Web Token (JWT) berfungsi dengan presisi, dan fitur pemindaian Quick Response (QR) Code pada sisi klien berhasil mengekstrak *Transaction Hash* secara *Zero-Trust*, memutus jalur ketergantungan pada peladen *backend* untuk menarik data langsung dari *node* publik Ethereum.

Pada tahap kedua, guna memastikan stabilitas logika asinkronus (*asynchronous logic*) pada arsitektur hibrida, diterapkan pengujian *White Box* menggunakan metode *Basis Path Testing*. Pengujian ini secara spesifik difokuskan pada modul komputasi paling kritis di dalam sistem, yaitu Fungsi Persetujuan Lot Kopi dan Pencatatan Blockchain (PUT /api/verify/approve/:idLot). Fungsi ini bertugas menjembatani perubahan *state* di basis data MySQL lokal dengan eksekusi *Smart Contract* di jaringan Ethereum Sepolia secara konkuren.

Untuk memetakan seluruh kemungkinan jalur eksekusi algoritma, logika *backend* ditransformasikan ke dalam representasi *Flowgraph* (Grafik Aliran Kontrol) yang mematuhi kaidah *Single Entry, Single Exit*. Berdasarkan pemodelan tersebut, teridentifikasi 16 *Nodes* (titik eksekusi) dan 19 *Edges* (jalur transisi).



Gambar 5. Flowgraph

Berdasarkan pemodelan *Flowgraph* tersebut, kompleksitas algoritmik dari fungsionalitas persetujuan diukur menggunakan metrik *Cyclomatic Complexity* (CC) standar industri rekayasa perangkat lunak dengan formula V(G) = E - N + 2 (Pressman & Maxim, 2024). Hasil kalkulasi komputasional menunjukkan V(G) = 19 - 16 + 2 = 5. Nilai kompleksitas sebesar 5 ini merepresentasikan arsitektur kode yang sangat terstruktur dan membutuhkan 5 jalur independen (*Independent Paths*) untuk mencapai cakupan pengujian yang komprehensif (*full path coverage*), yaitu:

a. Path 1: 1 - 2 - 3 - 4 – 16
b. Path 2: 1 - 2 - 3 - 5 - 6 - 7 – 16
c. Path 3: 1 - 2 - 3 - 5 - 6 - 8 - 9 - 10 - 11 - 12 – 16
d. Path 4: 1 - 2 - 3 - 5 - 6 - 8 - 9 - 10 - 11 - 13 – 16
e. Path 5: 1 - 14 - 15 – 16

Kelima jalur independen tersebut kemudian diuji menggunakan parameter masukan (*input*) yang merepresentasikan kondisi ideal (*Happy Path*) maupun anomali eksternal (*Edge Cases*).

Tabel 1. Tabel Hasil Pengujian *Basis Path*

Path	Input	Proses	Keterangan
1	Mengirim request API dengan idLot acak yang tidak terdaftar di database MySQL.	Sistem mengeksekusi blok kondisional pembacaan DB (Node 3) dan merespons bahwa data kosong, lalu mengeksekusi Node 4 (Return HTTP 404) dan berhenti di Node 16.	Berhasil
2	Mengirim idLot yang terdaftar, namun nilai status_verifikasi di database disetel sebagai "Draft" atau "Ditolak".	Sistem menemukan data di Node 3, lalu membaca status di Node 6. Karena tidak sesuai aturan, Node 7 dieksekusi (Return HTTP 400) dan berhenti di Node 16.	Berhasil
3	Mengirim idLot valid berstatus "Menunggu Verifikasi" dengan jaringan Ethereum (RPC Infura) terhubung normal.	Sistem memperbarui DB (Node 8), memberi respons 200 (Node 9), masuk blok Try (Node 10), memanggil fungsi Smart Contract (Node 11), menyimpan Hash Tx ke DB (Node 12), dan bermuara ke Node 16.	Berhasil
4	Mengirim idLot valid (seperti Path 3), namun	Eksekusi berjalan normal hingga Node 9, namun gagal di Node 11. Eksepsi ditangkap oleh blok Catch internal, lalu	Berhasil

	koneksi internet diputus paksa (simulasi error jaringan Blockchain).	Node 13 dieksekusi untuk men-set status "Failed", dan berakhir di Node 16.	
5	Mematikan service MySQL (database down) sebelum mengirim request API persetujuan.	Modul gagal melakukan kueri awal, sistem melempar Exception ke blok Catch utama (Node 14), mengeksekusi Node 15 (Return HTTP 500 Kesalahan Server), lalu berhenti di Node 16 tanpa membuat aplikasi mati (crash).	Berhasil

Hasil pengujian pada tabel di atas membuktikan kapasitas toleransi kesalahan (*fault tolerance*) sistem yang sangat tangguh. Pada Path 3, sistem berhasil mengeksekusi integrasi mulus antara pembaruan MySQL dan injeksi *Smart Contract*. Lebih lanjut, pada pengujian ekstrem di Path 4 (simulasi anomali pemutusan koneksi *node* RPC Ethereum) dan Path 5 (simulasi kegagalan *service* MySQL), sistem secara presisi mampu menangkap eksepsi melalui blok *catch* internal. Sistem berhasil menginisiasi degradasi elegan (*graceful degradation*) dengan merespons status *Failed* atau HTTP 500 tanpa memicu kegagalan sistem total (*system crash*). Hal ini memverifikasi bahwa arsitektur hibrida KopiChain memenuhi standar keandalan tinggi (*high availability*) untuk diimplementasikan pada skenario rantai pasok industri.

SIMPULAN

Penelitian ini telah berhasil mengonstruksi dan mengimplementasikan arsitektur pelacakan rantai pasok Kopi Gayo berbasis hibrida (Web2 dan Web3) guna mengeliminasi kerentanan *single point of failure* serta asimetri informasi pada sistem logistik konvensional. Pendekatan *Asymmetric Trust* yang dirancang terbukti sangat efisien dalam mendistribusikan beban komputasi, di mana basis data relasional (MySQL) beroperasi secara optimal sebagai *buffer* operasional berlatensi rendah, sementara *smart contract* pada jaringan Ethereum (Sepolia Testnet) berfungsi secara absolut sebagai lapisan notarisasi desentralisasi yang menjamin kekekalan data (*immutability*).

Secara arsitektural, sistem secara empiris berhasil mereduksi risiko manipulasi data retrospektif (*database tampering*). Integrasi protokol konsensus internal melalui skema otorisasi *Maker-Checker* yang secara tegas memisahkan wewenang antara staf penginput draf dan verifikator data telah efektif memitigasi kerentanan pada titik masuk data (*Oracle Problem*). Setiap muatan logistik yang tervalidasi secara komputasional langsung dikunci menjadi bukti *Transaction Hash* (TxHash) permanen. Mekanisme ini sukses membangun fondasi akuntabilitas nirsangkal (*non-repudiation*), yang memaksa entitas internal untuk bertanggung jawab mutlak atas setiap data yang didistribusikan.

Sebagai bentuk realisasi dari *Zero-Trust Architecture*, sistem memfasilitasi antarmuka pelacakan konsumen yang sepenuhnya memotong jalur ketergantungan (*bypass*) dari peladen internal distributor. Konsumen dapat melakukan kueri pembacaan data *on-chain* secara independen langsung ke *node* jaringan publik melalui pemindaian QR Code. Lebih lanjut, tingkat keandalan arsitektur ini telah divalidasi secara matematis melalui pengujian *White Box* (*Basis Path Testing*). Dengan nilai *Cyclomatic Complexity* sebesar 5, sistem mendemonstrasikan kapasitas toleransi kesalahan (*fault tolerance*) yang solid; mampu merespons anomali eksternal seperti pemutusan koneksi RPC secara asinkronus dengan degradasi elegan (*graceful degradation*) tanpa memicu kegagalan sistem secara total. Secara keseluruhan, artefak KopiChain ini terbukti menjadi solusi rekayasa perangkat lunak yang tangguh untuk menciptakan ekosistem rantai pasok agrikultur yang transparan, autentik, dan anti-manipulasi.

DAFTAR PUSTAKA

Caldarelli, G., & Ornaghi, A. (2026). The Oracle Problem in decentralized supply chain management: Governance mechanisms and structural design for reliable data entry. *Journal of Blockchain Research and Technology*, 4(1), 45-60.

Farina, L., Rossi, M., & Silva, A. (2025). Structural vulnerabilities in centralized logistics databases: The single point of failure dilemma in conventional tracking systems. *International Journal of Supply Chain Management*, 12(3), 210-225.

Hassan, Q., & Smith, J. (2024). Applying Design Science Research in blockchain system development: Methodological frameworks. *Journal of Systems and Software*, 201, 112-125.

Li, X., & Wang, Y. (2023). Hybrid Web2 and Web3 architectures for supply chain traceability: Bridging off-chain efficiency with on-chain security. *IEEE Access*, 11, 450-462.

Nie, X., Wang, Y., & Chen, H. (2025). Blockchain-based zero-trust access control with inner-product encryption for IoT environments. *IEEE Internet of Things Journal*, 12(4), 3045-3058.

Petrillo, A., De Felice, F., & Zomparelli, F. (2025). Integrating blockchain, RFID, and barcodes: A unified mobile framework for comprehensive coffee supply chain traceability. *Journal of Agricultural Informatics*, 16(2), 112-128.

Pressman, R. S., & Maxim, B. R. (2024). *Software Engineering: A Practitioner's Approach* (10th ed.). McGraw-Hill Education.

Ruggieri, R., Santoro, G., & Vrontis, D. (2026). Global coffee supply chains and information asymmetry: Mitigating transparency issues through decentralization. *Supply Chain Management: An International Journal*, 31(1), 55-72.

Uzougbo, E., Okoro, C., & Abiola, O. (2025). Rethinking cybersecurity with Zero-Trust Architecture: "Never trust, always verify" principles in distributed networks. *Journal of Information Security and Applications*, 75, 103-118.

Zheng, Z., Xie, S., & Dai, H. (2022). Smart contracts as decentralized notarization layers in Ethereum: Architectures and execution models. *ACM Computing Surveys*, 55(4), 1-35.

Tarigan, E., Damayanti, D., & Pratama, F. (2024). Pengembangan sistem inventory control dengan metode user-centered design dan evaluasi usability. *Jurnal Jaringan Sistem Informasi Robotik (JSR)*, 8(2), 143-150.