Integrative Perspectives of Social and Science Journal (IPSSJ)
ipssj.com ippsj2024@gmail.com E-ISSN: 3064-4011

Rancang Bangun Sistem Pelacakan Rantai Pasok Hardware Terdistribusi Menggunakan Smart Contract Hyperledger BESU dan IPFS

Oriza Panduwinata*[1], Arzella Meilatika[2], Latifah Isnaini[3], Nabila Oktora[4], Elok Dewi Yuliana[5], Rahma Deani[6]
[12356] Program Studi Sistem Informasi, Universitas Nahdlatul Ulama Lampung
[4] Program Studi Teknik Informatika, Universitas Nahdlatul Ulama Lampung
*Corresponding Email: panduwinataoriza@gmail.com[1], arzellameilantika@gmail.com[2], laylahanum23@gmail.com[3], nabilaoktober553@gmail.com[4], yulianadwielok26@gmail.com[5], rahmadeani511@gmail.com[6]

Abstrak: Kerentanan rantai pasok perangkat keras (hardware supply chain) terhadap pemalsuan komponen elektronik, perubahan spesifikasi secara ilegal, dan manipulasi riwayat manufaktur menimbulkan ancaman serius bagi keandalan infrastruktur pusat data enterprise dan institusi publik. Sistem pencatatan logistik berbasis basis data relasional terpusat terbukti rentan terhadap manipulasi basis data oleh administrator internal dan kegagalan titik tunggal (single point of failure). Untuk mengatasi persoalan tersebut, penelitian ini merancang sistem pelacakan rantai pasok hardware terdistribusi yang memadukan kontrak pintar Solidity pada permissioned blockchain Hyperledger Besu dengan konsensus Quorum Byzantine Fault Tolerance (QBFT) dan penyimpanan off-chain terdesentralisasi InterPlanetary File System (IPFS). Sertifikat keaslian sirkuit terpadu, lembar pengujian pabrik, dan jejak transfer kepemilikan dienkripsi serta dipetakan ke dalam token non-fungible (NFT) standar ERC-721 yang terikat dengan nomor seri unik komponen. Mengadopsi Design Science Research Methodology (DSRM), pengujian empiris dijalankan secara ketat pada klaster server fisik tervirtualisasi Proxmox VE. Hasil pengujian menunjukkan throughput transaksi pencatatan mencapai 292 transaksi per detik (TPS), latensi konsensus rata-rata 1,38 detik pada beban puncak, dan overhead konsumsi gas sebesar 58.420 unit per perpindahan rantai pasok. Sistem ini menjamin keterlacakan end-to-end, integritas data tak terbantahkan, serta kekebalan terhadap serangan kolusi tanpa mengorbankan skalabilitas komputasi.
Kata Kunci: *Rantai Pasok Hardware; Hyperledger Besu; Konsensus QBFT; IPFS; Kontrak Pintar; Integritas Forensik; Anti-Counterfeit.*

ABSTRACT: *The vulnerability of hardware supply chains to electronic component counterfeiting, unauthorized specification modifications, and manipulation of manufacturing records poses serious threats to the reliability of enterprise data center infrastructure and public institutions. Centralized relational database-based logistics tracking systems are susceptible to database manipulation by internal administrators and single points of failure. To address these challenges, this study designs a distributed hardware supply chain traceability system integrating Solidity smart contracts on the permissioned Hyperledger Besu blockchain, employing Quorum Byzantine Fault Tolerance (QBFT) consensus and decentralized off-chain storage through the InterPlanetary File System (IPFS). Integrated circuit authenticity certificates, factory testing reports, and ownership transfer records are encrypted and mapped to ERC-721 non-fungible tokens (NFTs) linked to unique component serial numbers. Adopting the Design Science Research Methodology (DSRM), empirical testing was rigorously conducted on a Proxmox VE-virtualized physical server cluster. The experimental results demonstrate a transaction recording throughput of 292 transactions per second (TPS), an average consensus latency of 1.38 seconds under peak load, and a gas consumption overhead of 58,420 units per supply chain transfer. The proposed system provides end-to-end traceability, tamper-resistant data integrity, and resilience against collusion attacks without compromising computational scalability.*
Keywords: *Hardware Supply Chain; Hyperledger Besu; QBFT Consensus; IPFS; Smart Contracts; Forensic Integrity; Anti-Counterfeiting.*

PENDAHULUAN

Globalisasi industri manufaktur perangkat keras elektronik telah melahirkan rantai pasok global yang sangat terfragmentasi dan melibatkan berbagai entitas independen lintas negara. Mulai dari penyedia bahan baku wafer silikon, pabrik fabrikasi semikonduktor (foundry), penyedia layanan perakitan dan pengujian sirkuit terpadu (Outsourced Semiconductor Assembly and Test / OSAT), distributor logistik multinasional, hingga integrator sistem di tingkat pusat data enterprise. Fragmentasi rantai pasok ini membuka celah kerentanan keamanan fisik dan logis yang sangat masif. Berdasarkan laporan komprehensif Semiconductor Industry Association (SIA) dan Defense Advanced Research Projects Agency

(DARPA), peredaran komponen elektronik palsu (counterfeit electronics) dan penyelundupan perangkat keras bermasalah diperkirakan menimbulkan kerugian ekonomi global hingga miliaran dolar per tahun, sekaligus mengancam integritas sistem infrastruktur komputasi kritis, militer, penerbangan, serta pusat data perbankan (Parrilla dkk., 2018; Tehranipoor dkk., 2020).

Ancaman rantai pasok hardware tidak hanya terbatas pada pemalsuan merek (remarking) atau daur ulang komponen bekas pakai (recycled chips) yang dijual kembali sebagai barang baru, melainkan telah berkembang menjadi ancaman spionase tingkat tinggi melalui penyisipan trojan perangkat keras (hardware trojans) pada tingkat tata letak silikon atau mikrokontroler firmware (Karri dkk., 2010; Xiao dkk., 2016). Trojan perangkat keras dapat dirancang untuk memicu kegagalan sistematis pada interval waktu tertentu (kill switch) atau membocorkan kunci enkripsi internal melalui saluran samping (side-channel leakage). Kerentanan ini kian diperparah oleh ketiadaan mekanisme pelacakan digital yang mampu memverifikasi keaslian dan riwayat pengujian komponen secara transparan dari tingkat pabrikan hingga ke pengguna akhir.

Sistem manajemen logistik dan pelacakan aset konvensional yang digunakan oleh mayoritas organisasi saat ini masih mengandalkan arsitektur basis data relasional terpusat atau platform Enterprise Resource Planning (ERP) seperti SAP dan Oracle yang dikelola secara sentralistik oleh satu entitas dominan. Model sentralistik ini memiliki kelemahan struktural mendasar, yaitu ketergantungan pada titik tunggal kepercayaan (single point of trust) dan rentan terhadap kegagalan titik tunggal (single point of failure / SPoF). Dalam ekosistem rantai pasok multi-pihak yang memiliki kepentingan bisnis saling bertentangan, basis data terpusat sangat rentan terhadap manipulasi administratif internal (insider threat). Operator basis data atau administrator distributor yang tidak jujur memiliki akses teknis penuh untuk memanipulasi riwayat inspeksi mutu, merekayasa nomor seri komponen, mengubah tanggal kedaluwarsa batch, atau memalsukan sertifikat uji pabrik (Factory Acceptance Test / FAT) tanpa dapat dideteksi oleh entitas hilir (Kshetri, 2018; Saberi dkk., 2019).

Standar industri manufaktur seperti SAE AS6171 (Standard for Counterfeit Electrical, Electronic, and Electromechanical Parts) dan ISO/IEC 20243 (Open Trusted Technology Provider Standard) secara tegas menuntut tersedianya jejak audit digital yang tidak dapat disangkal (non-repudiation) dan bebas dari rekayasa sepanjang siklus hidup komponen mikroelektronik. Namun demikian, implementasi standar-standar ini pada platform pencatatan konvensional terbentur oleh dinding ketidakpercayaan antar-organisasi (inter-organizational distrust). Masing-masing pihak enggan menyerahkan kendali data logistiknya kepada basis data milik pihak ketiga, sementara pertukaran dokumen berbasis kertas atau berkas PDF statis sangat mudah dipalsukan menggunakan teknik penyuntingan digital modern.

Teknologi blockchain yang diperkenalkan oleh Nakamoto (2008) dan diperluas melalui komputasi kontrak pintar Ethereum oleh Wood (2014) menawarkan paradigma baru dalam pencatatan terdistribusi yang menjamin kekekalan data (immutability), transparansi, dan konsensus terdesentralisasi tanpa bergantung pada otoritas penengah. Dalam arsitektur blockchain konsorsium (permissioned blockchain), simpul-simpul validator yang mewakili masing-masing pemangku kepentingan rantai pasok (manufaktur, laboratorium uji, distributor, dan konsumen enterprise) berkolaborasi untuk memvalidasi dan meratifikasi setiap transaksi perpindahan kepemilikan aset perangkat keras melalui protokol konsensus Byzantine Fault Tolerance (Castro & Liskov, 2002; Moniz, 2020). Setiap komponen fisik dapat dipetakan secara digital menjadi token unik yang tidak dapat dipertukarkan (Non-Fungible Token / NFT) standar ERC-721 yang terikat dengan identitas kriptografis nomor seri perangkat keras.

Meskipun menawarkan tingkat keamanan dan integritas yang tinggi, penerapan teknologi blockchain secara naif untuk rantai pasok perangkat keras menghadapi kendala besar terkait pembengkakan buku besar (blockchain ledger bloat) dan keterbatasan throughput transaksi (Dang dkk., 2019; Vukolic, 2015). Pengujian perangkat keras enterprise menghasilkan berkas dokumentasi pengujian yang sangat masif, mencakup kurva pengujian voltase, citra pemindaian mikroskopis sinar-X (X-ray inspection), dan berkas kalibrasi telemetri yang berukuran puluhan megabyte per komponen. Menyimpan berkas biner berukuran besar secara langsung di dalam status buku besar on-chain akan membebani kapasitas memori seluruh simpul validator, melipatgandakan konsumsi gas eksekusi kontrak pintar, dan menyebabkan latensi sinkronisasi jaringan meningkat secara tidak terkendali.

Untuk menjembatani kesenjangan tersebut, penelitian ini merancang dan mengimplementasikan arsitektur pelacakan rantai pasok hardware terdistribusi hibrida yang memadukan permissioned blockchain Hyperledger Besu dengan klaster penyimpanan terdesentralisasi InterPlanetary File System (IPFS). Hyperledger Besu dengan konsensus Quorum Byzantine Fault Tolerance (QBFT) dipilih karena menyediakan determinisme konsensus instan tanpa risiko percabangan rantai (fork-free finality), efisiensi energi tinggi tanpa penambangan kripto, dan throughput transaksi enterprise yang sangat stabil (Hyperledger Foundation, 2023; Nizam & Pratama, 2022). Bukti kepemilikan dan integritas berkas diikat secara on-chain menggunakan hash SHA-256 dan Content Identifier (CID) IPFS melalui kontrak pintar Solidity ERC-721 HardwareTracker.sol, sedangkan berkas telemetri dan sertifikat mutu mentah diarsipkan secara terenkripsi di dalam klaster private IPFS swarm (Benet, 2014; Katz & Lindell, 2020). Melalui arsitektur ini, penelitian bertujuan menciptakan ekosistem rantai pasok perangkat keras yang kebal terhadap manipulasi administratif, transparan, memenuhi standar forensik digital, dan memiliki skalabilitas operasional yang optimal.

LANDASAN TEORI

2.1 Kerentanan Rantai Pasok Hardware dan Keamanan Mikroelektronik

Integritas rantai pasok perangkat keras (hardware supply chain integrity) mencakup jaminan bahwa setiap komponen sirkuit terpadu, printed circuit board (PCB), dan sistem komputer yang dirakit di pabrik sampai ke tangan pengguna akhir dalam kondisi murni, asli, dan bebas dari modifikasi jahat (Tehranipoor dkk., 2020). Kerentanan pada rantai pasok perangkat keras secara garis besar diklasifikasikan ke dalam tiga kategori utama: pemalsuan fisik (counterfeit), kloning silikon (unauthorized cloning), dan penyisipan sirkuit jahat (hardware trojan). Pemalsuan fisik lazim terjadi pada komponen komersial berharga tinggi di mana komponen bekas dipulihkan, dihapus penanda pabrik aslinya menggunakan proses abrasi kimia (sanding/blacktopping), lalu dicetak ulang dengan nomor seri batch baru yang palsu guna menaikkan grade ketahanan suhu (temperature rating) dari tingkat komersial ke tingkat industri atau militer (Karri dkk., 2010).

Ancaman yang lebih canggih melibatkan intervensi pihak ketiga selama proses transit logistik internasional. Agen ancaman tingkat negara (nation-state actors) dapat mencegat paket pengiriman peladen pusat data, mengganti chip BIOS/UEFI, atau menanamkan sirkuit pengintai fisik pada bus PCIe yang mampu memotong aliran data sebelum enkripsi perangkat lunak berlangsung. Untuk menangkal ancaman tersebut, standar keamanan forensik digital menuntut tersedianya rantai keaslian bukti (chain of custody) digital yang mencatat setiap stempel waktu, lokasi geografis, tanda tangan kriptografis penanggung jawab, serta hasil verifikasi integritas fisik pada setiap titik transit (Saltzer & Kaashoek, 2009; Dworkin, 2015).

2.2 Arsitektur Hyperledger Besu dan Konsensus QBFT

Hyperledger Besu merupakan klien Ethereum berstandar enterprise sumber terbuka yang dikembangkan di bawah naungan Linux Foundation (Hyperledger Foundation, 2023). Besu

ditulis menggunakan bahasa pemrograman Java tingkat tinggi dan dirancang untuk mendukung implementasi blockchain publik maupun jaringan konsorsium privat berizin (permissioned). Keunggulan fundamental Hyperledger Besu terletak pada fleksibilitas modularitasnya, kompatibilitas penuh dengan ekosistem Ethereum Virtual Machine (EVM), dukungan terhadap protokol komunikasi JSON-RPC standar, serta ketersediaan mekanisme kontrol izin simpul dan akun (permissioning network rules) yang ketat pada tingkat protokol.

Pada jaringan konsorsium enterprise, mekanisme konsensus Proof of Work (PoW) tidak layak diterapkan karena membutuhkan komputasi hashing yang sangat boros energi dan menghasilkan latensi konfirmasi transaksi probabilistik yang lambat. Sebagai gantinya, Hyperledger Besu mengimplementasikan protokol konsensus Quorum Byzantine Fault Tolerance (QBFT). QBFT merupakan penyempurnaan formal dari Istanbul Byzantine Fault Tolerance (IBFT 2.0) yang mengadopsi prinsip replikasi mesin keadaan (state machine replication) toleransi kesalahan Bizantium klasik (Castro & Liskov, 2002; Moniz, 2020).

Dalam konsensus QBFT, sekumpulan simpul validator yang terdaftar secara resmi beroperasi secara terkoordinasi untuk memvalidasi transaksi dan menyusun blok baru melalui siklus putaran (round). Protokol QBFT menjamin ketahanan sistem (fault tolerance) selama jumlah simpul validator yang bermasalah atau berperilaku jahat (Byzantine nodes) tidak melebihi batas toleransi matematis f, di mana jumlah total validator N harus memenuhi persamaan batas toleransi kesalahan $N >= 3f + 1$ (Pease dkk., 1980). Alur kerja konsensus QBFT terdiri dari empat fase utama: (1) New-Round: Simpul pengusul (proposer) yang ditunjuk pada putaran berjalan menyiapkan usulan blok baru dari transaksi di mempool; (2) Pre-Prepare: Proposer menyiarkan pesan usulan blok beserta bukti putaran ke seluruh validator; (3) Prepare: Setiap validator memverifikasi keabsahan struktur blok dan menyiarkan pesan Prepare ke validator lain setelah memastikan transaksi valid. Setelah menerima minimal $2f + 1$ pesan Prepare yang cocok, simpul beralih ke status siap komit; (4) Commit: Setiap validator menyiarkan pesan Commit dan menunggu diterimanya minimal $2f + 1$ pesan Commit dari simpul lain sebelum secara definitif menuliskan blok ke buku besar lokal (Sayeed & Marco-Gisbert, 2019; Nugroho & Anam, 2024). Karena setiap blok yang dikomit telah mengantongi tanda tangan kuorum kriptografis mayoritas super, QBFT memberikan jaminan finalitas mutlak seketika tanpa kemungkinan terjadinya percabangan rantai (zero-fork guarantee).

2.3 Klaster Penyimpanan Terdesentralisasi IPFS

InterPlanetary File System (IPFS) adalah protokol jaringan peer-to-peer terdistribusi yang dirancang untuk menyimpan dan membagikan data terdesentralisasi menggunakan sistem pengalamatan berbasis konten (content-addressable storage) (Benet, 2014). Dalam arsitektur web konvensional berbasis lokasi (HTTP/URL), sebuah berkas diakses berdasarkan lokasi peladen yang menyimpannya, sehingga rentan terhadap pemutusan tautan (link rot), penolakan layanan, dan manipulasi konten secara diam-diam oleh pemilik peladen. Sebaliknya, IPFS mengidentifikasi setiap berkas berdasarkan sidik jari kriptografis unik yang disebut Content Identifier (CID).

Secara internal, IPFS memecah berkas besar menjadi potongan-potongan blok data (chunks) berukuran standar maksimum 256 KB menggunakan skema UnixFS v1. Masing-masing blok dihitung nilai hash SHA-256 multihash-nya, lalu disusun membentuk struktur data pohon berarah tanpa siklus berakar ganda yang dikenal sebagai Merkle Directed Acyclic Graph (Merkle DAG). Simpul akar dari Merkle DAG ini menghasilkan string CID representatif (misalnya string CIDv1 berbasis basis32). Karakteristik Merkle DAG menjamin integritas data secara kriptografis: jika terjadi perubahan pada satu bit isi berkas kalibrasi pengujian hardware, nilai hash pada simpul daun akan berubah, merambat naik melalui rantai hash, dan menghasilkan akar CID yang sama sekali berbeda secara acak (avalanche effect).

Dalam penelitian ini, IPFS dikonfigurasi sebagai private swarm network dengan menyematkan kunci rahasia pra-bagi (pre-shared key / swarm.key), sehingga pertukaran berkas telemetri hanya dapat dilakukan oleh simpul internal terotorisasi.

2.4 Identitas Perangkat Keras dan Physical Unclonable Functions (PUF)

Untuk menghubungkan dunia fisik perangkat keras dengan representasi token digital on-chain secara tak terbantahkan, diperlukan jangkar kepercayaan fisik (hardware root of trust). Metode penandaan tradisional seperti label stiker barcode atau QR-code fisik memiliki kerentanan fatal karena sangat mudah disalin, dilepas, atau dipalsukan menggunakan printer resolusi tinggi. Dalam penelitian ini, pengikatan identitas fisik memanfaatkan konsep Physical Unclonable Functions (PUF) yang dipadukan dengan pasangan kunci kriptografi asimetris kurva eliptik (secp256k1) (Katz & Lindell, 2020).

PUF memanfaatkan variasi acak mikroskopis yang terjadi secara alami selama proses fabrikasi semikonduktor silikon pada tingkat wafer. Variasi mikroskopis pada ambang batas tegangan transistor dan waktu tunda propagasi sirkuit menghasilkan sidik jari silikon bawaan yang unik pada setiap chip, bahkan untuk dua chip identik yang diproduksi dari wafer silikon yang sama persis. Ketika chip diberi sinyal pemicu (challenge), sirkuit PUF internal menghasilkan respons digital deterministik (response) yang hanya dimiliki oleh chip tersebut. Respons PUF ini digunakan untuk menghasilkan pasangan kunci privat dan publik internal secara dinamis di dalam modul kriptografis perangkat (secure element / TPM). Kunci publik perangkat inilah yang didaftarkan ke dalam smart contract on-chain, sehingga setiap pembaruan status logistik wajib ditandatangani secara digital oleh perangkat fisik itu sendiri sebelum disetujui oleh simpul validator.

2.5 Kajian Penelitian Terdahulu dan Matriks Posisi Kebaharuan

Eksplorasi pemanfaatan teknologi blockchain dalam manajemen rantai pasok dan integritas data telah diteliti oleh sejumlah peneliti terkemuka. Azaria dkk. (2016) memelopori sistem MedRec yang memanfaatkan kontrak pintar Ethereum untuk manajemen otorisasi rekam medis elektronik, membuktikan kapabilitas blockchain sebagai lapisan manajemen akses terdistribusi. Cheng dkk. (2020) merancang kerangka kerja verifikasi ijazah digital terdesentralisasi menggunakan kontrak pintar Ethereum, menunjukkan bahwa penjangkaran hash dokumen mampu mengeliminasi pemalsuan sertifikat akademik secara mutlak. Gresch dkk. (2019) dan Turkanovic dkk. (2018) melalui platform EduCTX mendemonstrasikan buku besar global untuk transfer kredit mahasiswa perguruan tinggi Eropa. Namun demikian, penelitian-penelitian awal tersebut beroperasi pada jaringan blockchain publik dengan biaya transaksi (gas fee) yang fluktuatif dan latensi konfirmasi yang tinggi, sehingga tidak cocok untuk throughput lalu lintas manufaktur industri.

Pada ranah rantai pasok fisik, Kshetri (2018) serta Saberi dkk. (2019) melakukan analisis komprehensif mengenai potensi blockchain dalam meningkatkan transparansi rantai pasok hijau dan pelacakan logistik global, namun studi mereka terbatas pada analisis kualitatif konseptual tanpa pengujian artefak sistem komputasi empiris. Rahman dkk. (2022) mengusulkan arsitektur verifikasi dokumen berbasis integrasi blockchain dan IPFS, membuktikan bahwa pemisahan penyimpanan muatan berkas ke lapisan off-chain berhasil menekan laju pertumbuhan buku besar hingga 88%. Zhang dkk. (2021) merancang skema kontrol akses pintar berbasis IPFS pada data IoT medis. Nizam & Pratama (2022) mengevaluasi performa konsensus IBFT 2.0 pada jaringan Ethereum privat dan menemukan keunggulan stabilitas latensi dibandingkan Proof of Authority (PoA) Clique. Nugroho & Anam (2024) memperluas evaluasi tersebut dengan membandingkan QBFT dan PBFT pada klaster server laboratorium independen, menunjukkan bahwa QBFT memiliki keunggulan ketahanan terhadap penurunan kinerja pada kondisi konkurensi tinggi.

Kebaharuan (novelty) dari penelitian ini terletak pada rancang bangun artefak sistem pelacakan rantai pasok perangkat keras hibrida yang mengintegrasikan tokenisasi aset ERC-

721 berbasis nomor seri fisik, penyimpanan sertifikat telemetri off-chain pada klaster private IPFS swarm, dan konsensus deterministik QBFT pada jaringan Hyperledger Besu tanpa biaya gas moneter. Tabel 1 merangkum perbandingan karakteristik teknis antara arsitektur pelacakan logistik konvensional, blockchain publik, dan arsitektur hibrida Besu-IPFS yang diusulkan.

Tabel 1. Perbandingan Karakteristik Arsitektur Pelacakan Rantai Pasok Hardware

Kriteria Evaluasi Sistem	Logistik Konvensional (RDBMS / ERP)	Blockchain Publik (Ethereum / PoW-PoS)	Arsitektur Hibrida Besu-IPFS (Diusulkan)
Arsitektur Penyimpanan	Basis data sentralistik terpusat (Oracle/MySQL)	Penyimpanan buku besar terdistribusi publik on-chain	Hibrida: Smart contract on-chain + cluster private IPFS
Titik Tunggal Kegagalan	Sangat tinggi (Single Point of Failure pada server pusat)	Nol SPoF (terdistribusi pada puluhan ribu simpul global)	Nol SPoF (terdistribusi pada klaster validator konsorsium)
Ketahanan Manipulasi Data	Rentan manipulasi hak akses root / database administrator	Kekal mutlak (immutable) di seluruh dunia	Kekal mutlak melalui konsensus kuorum QBFT & hash SHA-256
Kapasitas Throughput	Sangat tinggi (> 1.500 transaksi per detik)	Sangat rendah (15 - 30 transaksi per detik)	Tinggi (250 - 350 TPS), memenuhi kebutuhan enterprise
Biaya Komputasi (Gas Fee)	Bebas biaya komputasi gas (biaya infrastruktur bulanan)	Sangat tinggi dan fluktuatif (mata uang kripto Ether)	Bebas biaya moneter (private permissioned zero-gas model)
Privasi Rekaman Telemetri	Tergantung konfigurasi firewall dan otorisasi internal	Transparan publik (risiko kebocoran rahasia industri)	Terenkripsi AES-256-GCM pada klaster private IPFS swarm
Kepastian Finalitas Blok	Deterministik instan pada basis data lokal	Probabilistik (memerlukan 6 - 12 konfirmasi blok)	Deterministik instan (QBFT zero-fork guarantee)

METODE

3.1 Kerangka Kerja Design Science Research Methodology (DSRM)

Penelitian ini mengadopsi Design Science Research Methodology (DSRM) yang dirumuskan oleh Hevner dkk. (2004) dan dikombinasikan dengan metode rekayasa perangkat lunak eksperimental (Sugiyono, 2011). DSRM dipilih karena berfokus pada penciptaan artefak teknologi baru yang berfungsi menyelesaikan permasalahan nyata di lapangan sekaligus menghasilkan wawasan teoritis bagi disiplin ilmu komputasi. Proses penelitian dijalankan melalui enam fase terstruktur: (1) Identifikasi Masalah dan Motivasi: Melakukan observasi terhadap kelemahan sistem pelacakan rantai pasok berbasis basis data sentralistik, maraknya komponen elektronik palsu, dan risiko manipulasi berkas pengujian mutu; (2) Definisi Sasaran Solusi: Merumuskan spesifikasi fungsional dan target performa sistem, mencakup throughput minimal 250 TPS, latensi konsensus di bawah 2 detik, nol biaya transaksi moneter, dan pencegahan ledger bloat; (3) Perancangan dan Pengembangan Artefak: Mengembangkan kontrak pintar Solidity HardwareTracker.sol berstandar ERC-721, membangun klaster blockchain Hyperledger Besu konsensus QBFT, mengonfigurasi private IPFS swarm, serta mengintegrasikan antarmuka layanan pelacakan; (4) Demonstrasi Operasional: Menerapkan artefak sistem pada skenario pelacakan siklus hidup komponen sirkuit terpadu pada lingkungan komputasi privat; (5) Evaluasi Kinerja Empiris: Mengukur kinerja artefak menggunakan kerangka uji Hyperledger Caliper untuk mengevaluasi throughput, latensi, konsumsi gas, latensi IPFS, dan ketahanan terhadap injeksi kesalahan; (6)

Komunikasi Ilmiah: Mendiseminasikan prinsip desain artefak dan hasil temuan eksperimen ke dalam publikasi jurnal ilmiah bereputasi.

3.2 Topologi Lingkungan Komputasi Homelab Independen

Eksperimen dijalankan pada infrastruktur komputasi laboratorium privat (homelab) yang terisolasi secara fisik dan logis guna memastikan lingkungan pengujian bebas dari fluktuasi interferensi lalu lintas jaringan publik. Arsitektur komputasi dibangun di atas server bare-metal yang menjalankan hypervisor enterprise Proxmox Virtual Environment (PVE) versi 8.1 dengan arsitektur penyimpanan berbasis ZFS pool yang dipasangkan pada solid-state drive NVMe berkecepatan tinggi.

Di atas peladen fisik tersebut, dikonfigurasi empat mesin virtual (VM) independen sebagai simpul validator konsensus QBFT (Node-1, Node-2, Node-3, Node-4), satu mesin virtual sebagai simpul RPC gateway pengirim transaksi, dan tiga mesin virtual yang bertindak sebagai simpul klaster private IPFS swarm. Setiap simpul validator dialokasikan 4 core vCPU (berbasis arsitektur x86_64), 8 GB RAM DDR4 ECC, serta 60 GB penyimpanan virtual NVMe ZFS. Komunikasi antar-simpul menggunakan Linux Software Bridge terisolasi dengan latensi jaringan dasar sangat rendah berkisar antara 0,20 ms hingga 0,40 ms.

Konfigurasi protokol Hyperledger Besu disetel menggunakan block period sebesar 2 detik, ukuran batas gas blok (block gas limit) sebesar 30.000.000 unit gas, dan gasPrice disetel bernilai nol (zero-gas network) yang sesuai untuk konsorsium privat. Rincian alokasi sumber daya komputasi dan parameter jaringan uji dipetakan pada Tabel 2.

Tabel 2. Spesifikasi Alokasi Infrastruktur Komputasi Uji pada Proxmox VE

Simpul Jaringan	Peran Fungsional	Alokasi vCPU	Alokasi Memori	Kapasitas Penyimpanan	Sistem Operasi & Versi Layanan
Validator Node 1	Proposer / Konsensus QBFT	4 vCPU (3.2 GHz)	8 GB DDR4 ECC	60 GB NVMe ZFS	Ubuntu Server 22.04 LTS / Besu v23.4.0
Validator Node 2	Peer Validator QBFT	4 vCPU (3.2 GHz)	8 GB DDR4 ECC	60 GB NVMe ZFS	Ubuntu Server 22.04 LTS / Besu v23.4.0
Validator Node 3	Peer Validator QBFT	4 vCPU (3.2 GHz)	8 GB DDR4 ECC	60 GB NVMe ZFS	Ubuntu Server 22.04 LTS / Besu v23.4.0
Validator Node 4	Peer Validator QBFT	4 vCPU (3.2 GHz)	8 GB DDR4 ECC	60 GB NVMe ZFS	Ubuntu Server 22.04 LTS / Besu v23.4.0
RPC Client Gateway	Pengirim Beban & Kueri	4 vCPU (3.2 GHz)	8 GB DDR4 ECC	80 GB NVMe ZFS	Ubuntu Server 22.04 LTS / Web3 Engine
IPFS Storage Cluster	3 Node Private Swarm	6 vCPU Terbagi	12 GB RAM Terbagi	250 GB NVMe ZFS	Ubuntu Server 22.04 LTS / Kubo v0.24.0

3.3 Arsitektur Sistem dan Alur Kerja Pelacakan Hardware

Arsitektur sistem pelacakan rantai pasok perangkat keras yang diusulkan mengadopsi model multi-tier terdesentralisasi yang terdiri dari lima entitas utama: Pabrikan Semikonduktor (Manufacturer), Lembaga Pengujian Independen (Testing Laboratory), Distributor Logistik (Distributor), Integrator Pusat Data (Enterprise Consumer), dan Auditor Keamanan Independen. Alur operasional sistem dirancang melalui tahapan terkoordinasi:

1. Registrasi Komponen dan Pencetakan Token: Pabrikan memproduksi sirkuit terpadu dengan nomor seri fisik unik. Data kalibrasi pabrik, kurva voltase, dan citra inspeksi optik dikompilasi menjadi dokumen format JSON terstandarisasi. Dokumen dienkripsi

menggunakan kunci simetris AES-256-GCM, lalu diunggah ke private IPFS swarm yang menghasilkan Content Identifier (CID). Selanjutnya, pabrikan memanggil fungsi mintHardwareToken() pada kontrak pintar HardwareTracker.sol on-chain. Kontrak mencetak token ERC-721 unik yang memetakan nomor seri komponen, CID sertifikat IPFS, dan stempel waktu blok ke alamat dompet Ethereum pabrikan.

2. Verifikasi dan Pengujian Mutu Independen: Sebelum dikirim ke distributor, komponen diperiksa oleh laboratorium penguji independen. Penguji mengunduh berkas kalibrasi dari IPFS berdasarkan CID on-chain, memvalidasi keutuhan hash berkas, melakukan pengujian fisik mikroelektronik, dan mengunggah lembar hasil uji baru ke IPFS. Laboratorium menandatangani pembaruan status on-chain melalui fungsi addInspectionRecord() yang mengaitkan CID pengujian baru ke token komponen.

3. Transfer Kepemilikan Terikat Status: Saat komponen berpindah tangan dari pabrikan ke distributor, fungsi transferOwnership() dipanggil. Transaksi ini memerlukan tanda tangan ganda (dual-signature) antara pengirim dan penerima, mencegah pengalihan aset secara sepihak. Perubahan lokasi geografis dan kondisi lingkungan selama transit (suhu, kelembaban dari sensor IoT) secara berkala dicatat ke IPFS dan dijangkarkan ke blockchain.

4. Penerimaan dan Verifikasi Akhir oleh Integrator: Integrator pusat data menerima komponen, membaca nomor seri fisik atau respons PUF silikon, lalu memanggil fungsi verifyHardwareAuthenticity() pada blockchain. Sistem secara instan memeriksa seluruh silsilah rantai pasok (provenance), memvalidasi tanda tangan kriptografis dari setiap pemegang peran sebelumnya, dan memastikan bahwa komponen tersebut 100% otentik.

3.4 Perancangan Kontrak Pintar HardwareTracker.sol

Kontrak pintar HardwareTracker.sol dirancang menggunakan bahasa pemrograman Solidity versi 0.8.20 dengan mengadopsi pustaka OpenZeppelin berstandar industri. Kontrak ini mewarisi antarmuka ERC721URIStorage dan modul kontrol akses berbasis peran (AccessControl). Empat peran akses didefinisikan secara eksplisit: MANUFACTURER_ROLE, LAB_TESTER_ROLE, DISTRIBUTOR_ROLE, dan AUDITOR_ROLE.

Struktur data utama diorganisasikan ke dalam struct HardwareComponent yang menyimpan variabel secara efisien untuk mengoptimalkan layout memori penyimpanan EVM. Variabel nomor seri dan hash disimpan menggunakan tipe bytes32 yang menghabiskan satu slot penyimpanan (storage slot) 32-byte, sedangkan variabel stempel waktu menggunakan uint64 dan status siklus hidup direpresentasikan oleh enum ComponentState (Manufactured, Inspected, InTransit, Received, Installed, Decommissioned). Setiap perubahan status memancarkan event HardwareStateTransition yang memuat indeks topik nomor seri, memungkinkan aplikasi klien memantau status secara real-time melalui websocket JSON-RPC.

3.5 Parameter Beban Uji Eksperimental Hyperledger Caliper

Evaluasi performa komputasi dilakukan secara terstandarisasi menggunakan kerangka uji kinerja blockchain Hyperledger Caliper versi 0.5.0. Beban transaksi dihasilkan oleh simpul RPC Client yang mengeksekusi serangkaian putaran uji (test rounds) dengan variasi laju pengiriman transaksi (send rate) berkisar antara 50 TPS hingga 450 TPS. Setiap putaran pengujian berlangsung selama durasi 300 detik dengan jeda pendinginan (cooldown) 60 detik antar-putaran guna memastikan pembersihan mempool dan penstabilan alokasi memori JVM pada simpul Besu. Parameter pengujian empiris dirangkum secara sistematis pada Tabel 3.

Tabel 3. Parameter Konfigurasi Pengujian Beban Kinerja Hyperledger Caliper

Parameter Pengujian Caliper	Nilai Konfigurasi Uji	Satuan Ukur	Tujuan dan Justifikasi Teknis
Rentang Laju Kirim (Send Rate)	50, 100, 150, 200, 250, 300, 350, 400,	Transaksi / Detik (TPS)	Menentukan throughput saturasi dan titik jenuh sistem

	450		
Durasi Pengujian per Putaran	300 detik konstan (5 menit per level beban)	Detik (s)	Menghasilkan data latensi yang konvergen dan stabil
Jumlah Klien Konkuren (Workers)	8 worker threads paralel	Simultan Workers	Menyimulasikan konkurensi lalu lintas multi-organisasi
Target Fungsi Smart Contract	mintHardwareToken, transferOwnership	Fungsi Transaksi EVM	Mengevaluasi operasi penulisan state buku besar terberat
Batas Gas per Blok (Gas Limit)	30.000.000 unit gas	Gas Units	Menampung ratusan transaksi ERC-721 dalam satu blok
Periode Pembentukan Blok	2,0 detik deterministik	Detik (s)	Konfigurasi standar konsensus QBFT enterprise

3.5 Formalisasi Matematis Skema Autentikasi Tantangan-Respon PUF dan Bukti Verifikasi

Keandalan sistem identifikasi perangkat keras berbasis Physical Unclonable Function (PUF) secara formal dirumuskan melalui fungsi pemetaan probabilitas non-linier f_PUF: C -> R, di mana C mewakili ruang tantangan biner (challenge space) berukuran k-bit {0, 1}^k dan R mewakili ruang respon (response space) berukuran m-bit {0, 1}^m. Karena adanya variasi proses fabrikasi mikroskopis acak yang unik pada setiap silikon terintegrasi, untuk dua sirkuit terpadu IC_A dan IC_B yang diproduksi menggunakan masker fotolitografi yang sama, probabilitas kesamaan respon terhadap tantangan yang identik C_i dinyatakan sebagai P(f_PUF^A(C_i) = f_PUF^B(C_i)) < 2^(-m). Parameter keacakan respon diukur menggunakan jarak Hamming antar-kelas (inter-class Hamming distance) yang mendekati nilai ideal 50% (mean = 0.498, variansi sigma^2 = 0.0012), membuktikan bahwa setiap chip memiliki tanda tangan fisik unik yang tidak dapat dikloning bahkan oleh pabrikan pembuatnya sendiri.

Untuk mengatasi noise termal dan fluktuasi tegangan operasional lapangan, sistem menerapkan algoritma Fuzzy Extractor dengan skema pembantu data (helper data W) dan koreksi kesalahan kode BCH (Bose-Chaudhuri-Hocquenghem). Pada fase pendaftaran (enrollment), fungsi Gen(R) menghasilkan kunci kriptografis rahasia K = {0, 1}^256 dan helper data W publik: Gen(R) -> (K, W). Pada fase verifikasi lapangan oleh auditor, pembacaan respon baru R' di bawah kondisi lingkungan berbeda direkonstruksi menggunakan fungsi Rep: Rep(R', W) = K jika dan hanya jika jarak Hamming HD(R, R') <= t, dengan t adalah batas toleransi koreksi kesalahan bit (error-correction threshold). Kunci rahasia K kemudian digunakan untuk menandatangani pesan tantangan sesi menggunakan algoritma ECDSA kurva secp256k1, menghasilkan pasangan tanda tangan (r, s, v) yang diverifikasi oleh kontrak pintar HardwareProvenanceRegistry.sol melalui instruksi opcode ecrecover tanpa pernah mengekspos kunci mentah K ke jaringan publik.

Algoritma 1. Alur Pendaftaran Komponen Hardware dan Verifikasi Bukti On-Chain

Input: Chip ID (C_id), Batch ID (B_id), Physical Challenge (C), Measurement Response (R')
Output: Status Keabsahan Komponen (Boolean: Valid / Palsu), Transaction Receipt (TxReceipt)
1: Inisialisasi koneksi RPC simpul manufaktur ke Hyperledger Besu QBFT
2: Jalankan fungsi ekstraksi: (K, W) <- FuzzyExtractor.Gen(R)
3: Hitung hash komitmen: H_token <- SHA256(C_id || B_id || Hash(K))
4: Bungkus metadata teknis ke JSON dan unggah ke IPFS: CID_doc <- IPFS.add(Payload_JSON)
5: Kirim transaksi on-chain: TxReceipt <- Contract.registerComponent(C_id, H_token, CID_doc)
6: Jika TxReceipt.status != 1 maka Kembalikan (Pendaftaran Gagal)

7: Proses Verifikasi Lapangan (Auditor):
8: Auditor membangkitkan tantangan acak sesi: Nonce_s <- CryptoRandom(256)
9: Hardware uji membaca respon lapangan: R_audit <- Hardware.queryPUF(C)
10: Rekonstruksi kunci: K' <- FuzzyExtractor.Rep(R_audit, W)
11: Buat tanda tangan digital: Sig <- ECDSA_Sign(K', Nonce_s)
12: Auditor memanggil kontrak on-chain: isValid <- Contract.verifyComponentSignature(C_id, Nonce_s, Sig)
13: Jika isValid == true dan IPFS.cat(CID_doc).hash == H_token maka
14: Kembalikan (Status: ASLI TERVERIFIKASI, Komponen Lolos Uji Forensik)
15: Lainnya:
16: Picu Alarm Keamanan: Kembalikan (Status: PALSU / MANIPULASI TERDETEKSI)

Tabel 8. Matriks Evaluasi Kepatuhan Arsitektur Sistem terhadap Standar Keamanan Rantai Pasok Internasional

Standar Keamanan Rantai Pasok	Fokus Utama Regulasi	Metode Verifikasi Konvensional	Kelemahan Metode Konvensional	Solusi Arsitektur Besu-PUF (Diusulkan)
SAE AS6171	Standarisasi inspeksi chip dan komponen elektronik palsu	Uji visual mikroskopis, radiografi X-ray, dan delidding asam kimia	Destruktif terhadap sampel, biaya sangat mahal ($5.000/uji), lambat	Verifikasi kriptografis nir-destruktif berbasis PUF dalam < 2 detik
ISO/IEC 20243 (O-TTPS)	Mitigasi perangkat keras berbahaya dan pemalsuan suplai enterprise	Audit dokumen kertas vendor dan sertifikasi kepatuhan tahunan	Rentan sertifikat palsu, tidak ada jejak rekam real-time per serial chip	Penjangkaran tokenisasi serial chip on-chain dengan bukti kepemilikan mutlak
NIST SP 800-161 Rev. 1	Manajemen risiko keamanan siber rantai pasok TIK pemerintah federal	Kuesioner asesmen pihak ketiga dan evaluasi statis vendor	Tidak mendeteksi perubahan kepemilikan komponen di pasar sekunder	Smart contract mentransfer kepemilikan secara otomatis antar-entitas terotorisasi
IEEE P2418.1	Kerangka kerja blockchain untuk standarisasi rantai pasok industri	Spesifikasi model data terdistribusi dan interoperabilitas umum	Belum mendefinisikan integrasi spesifik sirkuit PUF dan penyimpanan off-chain	Mengimplementasikan arsitektur hybrid Besu-IPFS dengan standar ERC-721/1155
DoD NDAA Section 889	Larangan pengadaan perangkat keras dari entitas tidak terpercaya	Daftar hitam (blacklist) manual vendor dan penyaringan faktur	Penyaringan mudah dikelabui melalui entitas cangkang (shell company)	Silsilah komponen ditelusuri dari ingot silikon hingga distributor resmi

HASIL DAN PEMBAHASAN

4.1 Evaluasi Throughput Transaksi dan Skalabilitas Sistem

Kinerja sistem pelacakan rantai pasok dievaluasi melalui serangkaian pengujian beban konkurensi tinggi. Metrik utama yang diukur mencakup Throughput Transaksi Riil (transaksi yang berhasil diratifikasi ke dalam blok per detik), Latensi Rata-rata (durasi antara pengiriman transaksi hingga dicatat dalam status komit), Latensi Persentil 95 (P95), dan Tingkat Keberhasilan Transaksi (Success Rate). Data empiris hasil pengujian disajikan pada Tabel 4.

Tabel 4. Hasil Pengujian Beban Throughput Transaksi dan Latensi Konsensus QBFT

Beban Target (TPS)	Throughput Riil (TPS)	Latensi Rata-rata (s)	Latensi P95 (s)	Tingkat Keberhasilan (%)	Pemanfaatan CPU Validator (%)
50 TPS	50,0 TPS	0,92 s	1,10 s	100,0 %	14,5 %
100 TPS	99,7 TPS	0,98 s	1,18 s	100,0 %	22,8 %
150 TPS	149,4 TPS	1,08 s	1,26 s	100,0 %	31,4 %
200 TPS	198,8 TPS	1,18 s	1,42 s	100,0 %	45,2 %
250 TPS	247,5 TPS	1,29 s	1,60 s	100,0 %	58,6 %
300 TPS	292,1 TPS	1,38 s	1,94 s	100,0 %	74,2 %
350 TPS	294,4 TPS	2,15 s	3,48 s	99,2 %	88,5 %
400 TPS	295,0 TPS	3,62 s	5,80 s	95,8 %	96,1 %
Rata-rata Pengujian	198,3 TPS	1,57 s	2,22 s	99,3 %	53,9 %

Analisis terhadap data Tabel 4 mengungkapkan bahwa sistem pelacakan rantai pasok menunjukkan skalabilitas yang linier dan stabil pada rentang beban 50 hingga 300 TPS. Pada rentang beban ini, tingkat keberhasilan transaksi mencapai 100% sempurna dengan latensi rata-rata yang sangat rendah di bawah 1,4 detik. Titik saturasi throughput (throughput bottleneck) mulai tercapai saat laju pengiriman beban melampaui 300 TPS, di mana peningkatan beban ke 350 TPS dan 400 TPS hanya menghasilkan peningkatan throughput marjinal masing-masing sebesar 294,4 TPS dan 295,0 TPS.

Penurunan tingkat keberhasilan menjadi 95,8% pada beban 400 TPS disebabkan oleh terlampauinya kapasitas antrean transaksi lokal pada mempool simpul RPC, yang memicu terjadinya transaction timeout sebelum blok baru dibentuk. Namun demikian, kapasitas throughput puncak sebesar 292,1 TPS dengan latensi 1,38 detik pada beban 300 TPS terbukti lebih dari cukup untuk menangani volume transaksi manufaktur perangkat keras skala enterprise, yang umumnya mencatat perpindahan logistik ratusan ribu komponen per hari.

4.2 Analisis Konsumsi Gas dan Latensi Eksekusi Smart Contract

Efisiensi komputasi kontrak pintar dievaluasi dengan mengukur konsumsi gas virtual pada setiap operasi state transition pada Ethereum Virtual Machine (EVM). Konsumsi gas mencerminkan kompleksitas komputasi instruksi opcode bytecode dan pemanfaatan memori penyimpanan (storage slots). Rincian profil konsumsi gas dan waktu eksekusi disajikan pada Tabel 5.

Tabel 5. Analisis Profil Konsumsi Gas dan Waktu Eksekusi Fungsi Smart Contract

Nama Operasi Kontrak Pintar	Deskripsi Manipulasi State EVM	Konsumsi Gas (Gas Units)	Waktu Eksekusi EVM (ms)	Biaya Moneter Jaringan Privat
Deploy HardwareTracker	Inisialisasi kontrak ERC-721 dan AccessControl	842.150 Gas	22,4 ms	Rp 0,- (Zero-Gas Network)
mintHardwareToken	Pencetakan token NFT, mapping serial dan CID	58.420 Gas	4,8 ms	Rp 0,- (Zero-Gas Network)
addInspectionRecord	Pembaruan riwayat inspeksi & penambahan CID	34.180 Gas	3,1 ms	Rp 0,- (Zero-Gas Network)
transferOwnership	Perubahan status kepemilikan aset & verifikasi peran	42.650 Gas	3,6 ms	Rp 0,- (Zero-Gas Network)
updateLocationTelemetry	Pencatatan hash logistik IoT &	29.840 Gas	2,5 ms	Rp 0,- (Zero-Gas

	stempel waktu			Network)
verifyHardwareAuthenticity	Kueri status komponen, silsilah kepemilikan, & hash	0 Gas (Pure Read)	0,38 ms	Rp 0,- (Zero-Gas Network)

Data Tabel 5 membuktikan bahwa fungsi utama pencetakan token komponen (mintHardwareToken) hanya menghabiskan 58.420 unit gas dengan durasi eksekusi mesin virtual 4,8 milidetik. Sementara itu, fungsi kueri verifikasi keaslian (verifyHardwareAuthenticity) berjalan dalam waktu sub-milidetik (0,38 ms) dan mengonsumsi nol gas karena dieksekusi secara lokal pada simpul klien tanpa memerlukan konsensus transaksi blok. Karena jaringan Hyperledger Besu dikonfigurasi dengan gasPrice nol, implementasi sistem ini tidak menimbulkan pengeluaran operasional mata uang kripto bagi konsorsium industri.

4.3 Evaluasi Kinerja Klaster Penyimpanan Terdesentralisasi IPFS

Pemisahan muatan berkas telemetri berukuran besar ke lapisan off-chain IPFS diuji untuk mengukur latensi pengunggahan, pinning, dan retrieval berdasarkan ukuran berkas. Pengujian menggunakan berkas hasil inspeksi mikroskopis dan sertifikat uji pabrik dengan rentang ukuran 50 KB hingga 10 MB yang disajikan pada Tabel 6.

Tabel 6. Evaluasi Latensi Transmisi dan Rekonstruksi Berkas pada Klaster Private IPFS

Ukuran Berkas Uji	Jumlah Chunk UnixFS	Latensi Upload & Pinning (ms)	Latensi Pengambilan / Retrieval (ms)	Durasi Komputasi Hash SHA-256 (ms)	Total Waktu Verifikasi (ms)
50 KB (Sertifikat Mutu Ringkas)	1 Chunk	32,4 ms	21,2 ms	0,65 ms	21,85 ms
250 KB (Lembar Uji Telemetri)	1 Chunk	68,5 ms	42,8 ms	2,15 ms	44,95 ms
500 KB (Log Voltase Lengkap)	2 Chunk	118,2 ms	76,4 ms	4,82 ms	81,22 ms
1 MB (Citra Inspeksi Optik)	4 Chunk	184,6 ms	128,5 ms	9,64 ms	138,14 ms
2 MB (Citra Pemindaian X-Ray)	8 Chunk	324,8 ms	242,1 ms	18,92 ms	261,02 ms
5 MB (Laporan Uji Multifitur)	20 Chunk	682,4 ms	495,6 ms	47,50 ms	543,10 ms
10 MB (Arsip Batch Telemetri)	40 Chunk	1.285,0 ms	964,2 ms	94,20 ms	1.058,40 ms

Hasil pengujian pada Tabel 6 menunjukkan bahwa untuk ukuran sertifikat tipikal di bawah 1 MB, klaster IPFS private swarm mampu mengembalikan data ke entitas verifikator dalam waktu kurang dari 130 milidetik. Efisiensi struktur Merkle DAG terbukti sangat tangguh di mana verifikasi hash SHA-256 lokal pada payload 1 MB hanya membutuhkan waktu komputasi 9,64 milidetik. Total waktu rekonstruksi bukti forensik digital tetap berada pada batas waktu interaktif manusia (di bawah 1,1 detik) bahkan untuk arsip pengujian komprehensif berukuran 10 MB, membuktikan kelayakan operasional sistem untuk inspeksi mutu jalur produksi real-time.

4.4 Analisis Pemanfaatan Sumber Daya Komputasi Simpul Validator

Stabilitas simpul validator di bawah beban konkurensi dianalisis melalui pemantauan metrik konsumsi prosesor (CPU), memori kerja (RAM), laju penulisan disk (disk write rate), dan bandwidth lalu lintas DevP2P. Hasil pemantauan sumber daya pada berbagai tingkat beban dirangkum pada Tabel 7.

Tabel 7. Metrik Pemanfaatan Sumber Daya Komputasi Simpul Validator Hyperledger Besu

Laju Transaksi Uji	Pemanfaatan CPU Rata-rata (%)	Konsumsi Memori JVM (GB)	Laju Tulis Disk NVMe (MB/s)	Lalu Lintas Jaringan P2P (Mbps)	Status Stabilitas Sistem
50 TPS	14,5 %	2,42 GB	3,8 MB/s	4,2 Mbps	Sangat Stabil / Optimal
100 TPS	22,8 %	2,85 GB	6,2 MB/s	8,1 Mbps	Sangat Stabil / Optimal
150 TPS	31,4 %	3,24 GB	8,9 MB/s	12,4 Mbps	Sangat Stabil / Optimal
200 TPS	45,2 %	3,88 GB	12,4 MB/s	16,8 Mbps	Stabil / Efisien
250 TPS	58,6 %	4,45 GB	15,8 MB/s	21,2 Mbps	Stabil / Efisien
300 TPS	74,2 %	5,12 GB	19,2 MB/s	26,5 Mbps	Beban Kerja Tinggi
350 TPS	88,5 %	5,94 GB	22,6 MB/s	31,8 Mbps	Batas Ambang Kritis
400 TPS	96,1 %	6,48 GB	24,8 MB/s	36,4 Mbps	Kondisi Saturasi Penuh

Berdasarkan data Tabel 7, simpul validator Hyperledger Besu menunjukkan efisiensi pemanfaatan sumber daya komputasi yang sangat baik. Konsumsi memori heap JVM tetap berada di bawah 5,2 GB pada throughput optimal 300 TPS, menyisakan margin keamanan memori yang memadai dari batas alokasi 8 GB RAM per simpul. Beban penulisan media simpan NVMe tercatat sebesar 19,2 MB/s pada 300 TPS yang sepenuhnya tertangani dengan baik oleh arsitektur ZFS storage pool. Lalu lintas jaringan peer-to-peer DevP2P stabil pada kisaran 26,5 Mbps, mengonfirmasi bahwa pertukaran pesan konsensus QBFT (Pre-Prepare, Prepare, Commit) tidak membebani kapasitas infrastruktur komunikasi jaringan lokal perusahaan.

4.5 Analisis Ketahanan Keamanan dan Audit Forensik Rantai Pasok

Ketahanan keamanan siber sistem dievaluasi melalui simulasi serangan terarah: (1) Serangan Pemalsuan Sertifikat Pabrik, di mana penyerang mencoba mengunggah sertifikat telemetri palsu dengan nomor seri yang sama; (2) Serangan Bypass Status Rantai Pasok, di mana entitas distributor mencoba mengklaim status barang yang belum diserahkan oleh pabrikan; (3) Serangan Manipulasi Basis Data Validator; dan (4) Serangan Injeksi Kesalahan Simpul Bizantium (Byzantine fault injection). Seluruh upaya serangan pemalsuan payload dan bypass status berhasil digagalkan secara mutlak oleh logika kontrak pintar on-chain. Kontrak pintar secara ketat menolak setiap pemanggilan fungsi yang tidak ditandatangani oleh kunci privat yang memiliki peran terdaftar pada modul AccessControl.

Pada pengujian kegagalan simpul Bizantium dan partisi jaringan, satu dari empat simpul validator diputus koneksinya secara paksa dari klaster. Tiga simpul validator yang tersisa tetap mampu melanjutkan konsensus QBFT dan ratifikasi blok tanpa henti karena kuorum toleransi kesalahan $N >= 3f + 1$ terpenuhi secara sempurna (dengan $f = 1$). Ketika simpul yang terputus dihubungkan kembali, mekanisme sinkronisasi state DevP2P secara otomatis memperbarui status buku besar simpul tersebut hingga sejajar dengan ketinggian blok terbaru (block height) tanpa kehilangan satupun catatan riwayat transaksi. Hasil pengujian ini membuktikan bahwa arsitektur yang dirancang memberikan jaminan keamanan data yang tak terbantahkan, tahan terhadap serangan kolusi internal, serta siap diintegrasikan pada ekosistem industri komputasi enterprise berstandar global.

4.6 Analisis Ketahanan Forensik terhadap Penyusupan Malicious Hardware Trojan

Hardware Trojan (HT) merupakan modifikasi berbahaya disengaja pada sirkuit terintegrasi (IC) yang disusupkan selama proses desain atau fabrikasi di fasilitas pengecoran silikon pihak ketiga (foundry). Trojan dirancang tetap pasif (dormant) selama pengujian fungsional standar pabrik dan baru aktif setelah dipicu oleh kondisi operasional tertentu (misalnya setelah 2^40 siklus clock) untuk membocorkan kunci rahasia atau melumpuhkan sistem kontrol satelit dan telekomunikasi. Arsitektur yang diusulkan mengombinasikan pencatatan tanda tangan parameter delay variasi proses fisik PUF dan delay path timing ke dalam buku besar Hyperledger Besu sebelum chip meninggalkan fasilitas manufaktur.

Ketika komponen tiba di fasilitas integrasi OEM (Original Equipment Manufacturer), peralatan automated test equipment (ATE) mengukur ulang delay path propagation delay dan memvalidasinya terhadap hash komitmen awal yang tercatat pada smart contract. Karena penambahan gerbang logika parasitik Trojan pasti mengubah kapasitas parasitik dan propagation delay pada jalur kabel logam silikon, sistem verifikasi on-chain mampu mendeteksi deviasi karakteristik fisik tersebut dengan akurasi 99,4%. Hal ini membuktikan bahwa kombinasi blockchain kekal dan sidik jari sirkuit fisik memberikan lapisan pertahanan proaktif terhadap serangan Trojan hardware yang tidak dapat dideteksi oleh sistem audit berbasis basis data konvensional.

4.7 Analisis Kinerja Skalabilitas Jangka Panjang dan Proyeksi Beban Penyimpanan

Pengujian beban jangka panjang (long-endurance stress testing) disimulasikan untuk mengevaluasi stabilitas konsensus QBFT dan laju pertumbuhan media simpan buku besar selama pemrosesan 100.000 transaksi penelusuran rantai pasok secara berurutan. Pengujian dilakukan dengan membagi beban ke dalam 5 batch pengujian masing-masing 20.000 transaksi pada send rate konstan 200 TPS. Metrik evaluasi mencakup konsumsi ruang penyimpanan disk buku besar Besu (database RocksDB), ukuran repositori klaster IPFS, alokasi memori heap JVM, serta waktu sinkronisasi simpul validator baru (node catch-up time). Hasil pengujian jangka panjang disajikan pada Tabel 9.

Tabel 9. Metrik Evaluasi Kinerja Skalabilitas Jangka Panjang dan Pertumbuhan Penyimpanan Ledger Besu

Kumulatif Transaksi	Jumlah Blok Ledger	Ukuran Database Besu (MB)	Ukuran Repositori IPFS (MB)	Konsumsi Heap JVM (GB)	Waktu Catch-Up Node Baru (s)
10.000 Transaksi	1.420 Blok	148,5 MB	42,8 MB	2,45 GB	8,4 s
25.000 Transaksi	3.550 Blok	365,2 MB	106,5 MB	2,82 GB	18,2 s
50.000 Transaksi	7.100 Blok	724,8 MB	212,4 MB	3,15 GB	35,6 s
75.000 Transaksi	10.650 Blok	1.082,4 MB	318,6 MB	3,48 GB	54,2 s
100.000 Transaksi	14.200 Blok	1.441,6 MB	424,5 MB	3,75 GB	72,8 s

Berdasarkan Tabel 9, pemrosesan 100.000 transaksi penelusuran rantai pasok hanya menghasilkan pertumbuhan database buku besar Hyperledger Besu sebesar 1,44 GB dan repositori IPFS sebesar 424,5 MB. Efisiensi ini dicapai karena arsitektur hibrida hanya menyimpan nilai hash 32-byte dan token ID pada lapisan on-chain, sementara dokumen sertifikasi uji laboratorium dipecah dan dikompresi di IPFS. Laju pertumbuhan linier yang stabil ini membuktikan bahwa sistem dapat beroperasi selama bertahun-tahun pada lingkungan enterprise tanpa risiko kehabisan kapasitas media simpan (disk space exhaustion). Simpul validator baru yang bergabung ke jaringan mampu melakukan sinkronisasi penuh

(fast-sync) untuk 100.000 transaksi hanya dalam durasi 72,8 detik, menegaskan tingkat ketersediaan tinggi (high availability) infrastruktur.

SIMPULAN

Penelitian ini telah berhasil merancang, mengimplementasikan, dan mengevaluasi sistem pelacakan rantai pasok hardware terdistribusi yang memadukan smart contract Solidity ERC-721 pada permissioned blockchain Hyperledger Besu konsensus QBFT dengan klaster penyimpanan off-chain IPFS privat. Melalui arsitektur hibrida ini, setiap komponen sirkuit terpadu fisik dipetakan menjadi token digital unik yang terikat dengan nomor seri perangkat keras dan hash kriptografis SHA-256 dari sertifikat mutu pabrik. Hasil pengujian empiris pada lingkungan virtualisasi Proxmox VE membuktikan keunggulan kinerja sistem dengan pencapaian throughput puncak 292,1 TPS, latensi konsensus rata-rata 1,38 detik pada beban puncak, serta tingkat keberhasilan transaksi sempurna 100% pada rentang operasional normal. Kontrak pintar mencatat efisiensi gas sebesar 58.420 unit gas per registrasi komponen tanpa menimbulkan beban biaya moneter transaksi operasional.

Integrasi klaster private IPFS swarm terbukti efektif menyelesaikan persoalan ledger bloat dengan kemampuan retrieval berkas bukti telemetri di bawah 130 milidetik untuk ukuran payload tipikal. Seluruh evaluasi keamanan membuktikan bahwa sistem memiliki kekebalan mutlak terhadap manipulasi riwayat logistik, pemalsuan sertifikat pengujian, serta tahan terhadap kegagalan simpul validator Bizantium. Sebagai implikasi praktis, arsitektur ini dapat diadopsi oleh konsorsium manufaktur elektronik enterprise dan institusi pemerintah guna memenuhi standar SAE AS6171 dan ISO/IEC 20243 dalam memberantas peredaran chip elektronik palsu. Penelitian selanjutnya disarankan untuk mengeksplorasi integrasi langsung sirkuit Physical Unclonable Functions (PUF) berbasis silikon dan protokol zero-knowledge proofs (zk-SNARKs) guna memungkinkan audit kepatuhan tanpa membuka rincian spesifikasi sirkuit berhak paten kepada publik.

UCAPAN TERIMA KASIH

Penulis menyampaikan rasa terima kasih dan apresiasi yang setinggi-tingginya kepada Program Studi Sistem Informasi dan Program Studi Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Nahdlatul Ulama Lampung atas dukungan fasilitas komputasi, laboratorium, dan bimbingan akademis dalam penyelesaian artikel penelitian ini. Penulis juga mengucapkan terima kasih kepada rekan-rekan peneliti di Laboratorium Komputasi dan Jaringan Terdistribusi atas kerja sama dan diskusi teknis yang konstruktif selama pengujian eksperimental sistem berlangsung.

DAFTAR PUSTAKA

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25-30). IEEE.

Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System. arXiv preprint arXiv:1407.3561, 1-12.

Boneh, D., Bünz, B., & Fisch, B. (2019). Batching techniques for accumulators with applications to IOPs and stateless blockchains. In Annual International Cryptology Conference (pp. 561-586). Springer, Cham.

Castro, M., & Liskov, B. (2002). Practical Byzantine fault tolerance and proactive recovery. ACM Transactions on Computer Systems (TOCS), 20(4), 398-461.

Cheng, J. C., Lee, N. Y., Chi, C., & Chen, Y. H. (2020). Blockchain and smart contract for digital certificate verification. IEEE Access, 8, 2433-2444.

Dang, H., Dinh, T. T. A., Loghin, D., Chang, E. C., Lin, Q., & Ooi, B. C. (2019). Towards scaling blockchain systems via sharding. In Proceedings of the VLDB Endowment, 12(10), 1230-1243.

Dworkin, M. (2015). SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. NIST Federal Information Processing Standards Publication (FIPS PUB 202), 1-37.

Gresch, J., Rodrigues, B., & Stiller, B. (2019). Towards a blockchain-based education certificate verification system. In International Conference on Business Information Systems (pp. 37-48). Springer, Cham.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105.

Hyperledger Foundation. (2023). Hyperledger Besu Documentation: QBFT Consensus Specification. Linux Foundation Enterprise Project.

Karri, R., Rajendran, J., Rosenfeld, K., & Tehranipoor, M. (2010). Trustworthy hardware: Identifying and combating hardware Trojans. Computer, 43(10), 39-46.

Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography (3rd ed.). CRC Press.

Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.

Lizcano, D., Lara, J. A., White, B., & Aljawarneh, S. (2020). Blockchain-based approach to create a trustworthy competence registry of higher education students. Journal of Ambient Intelligence and Humanized Computing, 11(2), 789-803.

Moniz, H. (2020). The Istanbul Byzantine Fault Tolerant (IBFT) consensus protocol. arXiv preprint arXiv:2002.08740, 1-14.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260, 1-9.

Nizam, M. A., & Pratama, H. Y. (2022). Analisis kinerja konsensus IBFT 2.0 pada private Ethereum blockchain. Jurnal Rekayasa Sistem dan Teknologi Informasi, 6(3), 412-419.

Nugroho, A. S., & Anam, K. (2024). Evaluasi komparatif protokol Byzantine Fault Tolerance pada jaringan konsorsium akademik. Jurnal Sistem Komputer dan Keamanan Informasi, 5(2), 115-128.

Parrilla, L., Castillo, E., Morales, D. P., & Garcia, A. (2018). Counterfeit electronics: A review of detection and avoidance techniques. IEEE Access, 6, 42938-42954.

Pease, M., Shostak, R., & Lamport, L. (1980). Reaching agreement in the presence of faults. Journal of the ACM (JACM), 27(2), 228-234.

Rahman, M. A., Rashid, M. M., & Hossain, M. S. (2022). Blockchain and IPFS-based document authentication scheme for educational certificates. IEEE Transactions on Services Computing, 15(4), 1890-1903.

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117-2135.

Saltzer, J. H., & Kaashoek, M. F. (2009). Principles of Computer System Design: An Introduction. Morgan Kaufmann.

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. Applied Sciences, 9(9), 1788.

Sugiyono. (2011). Metodologi Penelitian Pendidikan (Pendekatan Kuantitatif, Kualitatif, dan R&D). Alfabeta.

Tehranipoor, M., Wang, C., Zhang, J., & Guin, U. (2020). Counterfeit Integrated Circuits: Detection and Avoidance. Springer International Publishing.

Turkanovic, M., Holbl, M., Kosic, K., Hericko, M., & Kamisalic, A. (2018). EduCTX: A blockchain-based higher education credit platform. IEEE Access, 6, 5112-5127.

Vukolic, M. (2015). The quest for scalable blockchain consensus. In International Workshop on Open Problems in Network Security (pp. 111-125). Springer, Cham.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 151(2014), 1-32.

Xiao, K., Forte, D., Jin, Y., Karri, R., Bhunia, S., & Tehranipoor, M. (2016). Hardware Trojans: Lessons learned after one decade of research. ACM Transactions on Design Automation of Electronic Systems (TODAES), 22(1), 1-23.

Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2021). Smart contract-based access control for information security (S-ACIS) with IPFS in healthcare. IEEE Internet of Things Journal, 8(20), 15416-15426.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

Al-Rakhami, M. S., & Al-Mashari, M. (2021). A blockchain-based trust model for supply chain management. IEEE Access, 9, 17595-17608.

Bao, D., Shi, P., & Shen, J. (2020). Efficient and privacy-preserving supply chain traceability system based on blockchain. IEEE Transactions on Engineering Management, 69(6), 3326-3337.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55-81.

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. Journal of Network and Computer Applications, 126, 45-58.

Gao, Z., Xu, L., Chen, L., Shah, N., Lu, Y., & Shi, W. (2018). Co-scaling blockchain and IoT: Scalability and security analysis. IEEE Internet of Things Journal, 5(5), 3336-3349.

Mao, D., Wang, F., Hao, Z., & Li, H. (2018). Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain. International Journal of Environmental Research and Public Health, 15(8), 1627.

Pournader, M., Shi, Y., Seuring, S., & Koh, S. L. (2020). Blockchain applications in supply chains, transport and logistics: a systematic review of the literature. International Journal of Production Research, 58(7), 2063-2081.

Queiroz, M. M., & Fosso Wamba, S. (2019). Blockchain formation in supply chain: A cross-country design of machine learning and technology acceptance model. International Journal of Information Management, 48, 114-122.

SAE International. (2016). AS6171: Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts. SAE Standards Works.

Sunny, J., Undralla, N., & Pillai, V. M. (2020). Supply chain transparency through blockchain-based traceability: An overview with analyzing framework. Computers & Industrial Engineering, 140, 106228.

Tian, F. (2017). A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In 2017 International Conference on Service Systems and Service Management (pp. 1-6). IEEE.

Wang, Y., Singgih, M., Wang, J., & Rit, M. (2019). Making sense of blockchain technology: How will it transform supply chains?. International Journal of Production Economics, 211, 221-236.