E-ISSN: 2964-6219, P-ISSN: 2964-6200
Volume 4 Number 2 August 2026.
pp: 136-144. DOI: https://doi.org/10.58477/cj.v4i2.490.

Computer Journal

RESEARCH ARTICLE Open Access

Implementasi Metode *Proof of Reserve* pada Sistem Pengiriman Barang untuk Menjaga Integritas Data

Dwi Saidina Zulfela Sembiring [1*], **Ardiansyah Putra** [2], **Alex Zander Siregar** [3], **Alfito Surya Pradana** [4], **Rico Wijaya Dewantoro** [5]

[1*,2,3,4,5] Program Studi Teknik Industri, Fakultas Sains dan Teknologi, Universitas Prima Indonesia, Kota Medan, Provinsi Sumatera Utara, Indonesia.
[1*,2,3,5] PUI Transportasi dan Logistik Perkotaan, Kota Medan, Provinsi Sumatera Utara, Indonesia.

*Correspondence email: dwisaidina710@gmail.com.

Received: 22 July 2026.
Revised: 24 August 2026.
Accepted: 28 August 2026.
Published: 30 August 2026.

Full list of author information is available at the end of the article.

Abstract

This study implements the Proof of Reserve (PoR) method in a blockchain-based shipment data validation system to support data integrity, authenticity, and reliability. The system was developed on a single server with three CouchDB nodes, consisting of one primary node and two backup nodes. Each shipment record was processed using the SHA-256 hashing algorithm and linked through interconnected prev_hash values to form a cryptographic data chain. This structure enables data modifications to be detected through hash inconsistency across the stored records. Validation was performed using a majority consensus mechanism among the nodes, classifying data as VALID or INVALID based on hash consistency. Simulations conducted in Jupyter Notebook showed that the system could detect data manipulation in both single-node and multi-node scenarios. The system also included an auto-recovery mechanism to restore corrupted or manipulated nodes using data from valid nodes. In addition, the prototype was developed into a web-based interface for real-time shipment tracking number verification. The results indicate that the PoR method can help maintain the consistency, transparency, and accountability of shipment data without requiring a full blockchain implementation.

Keywords: Proof of Reserve; Data Integrity; Blockchain; SHA-256; Majority Consensus; Decentralized Logistics System.

Abstrak

Penelitian ini mengimplementasikan metode Proof of Reserve (PoR) pada sistem validasi data pengiriman berbasis blockchain untuk mendukung integritas, keaslian, dan keandalan data. Sistem dikembangkan pada satu server dengan tiga node CouchDB, yang terdiri atas satu node utama dan dua node cadangan. Setiap rekaman data pengiriman diproses menggunakan algoritma hashing SHA-256 dan dihubungkan melalui nilai prev_hash sehingga membentuk rantai data kriptografis. Struktur ini memungkinkan perubahan data terdeteksi melalui ketidaksesuaian nilai hash pada data yang tersimpan. Proses validasi dilakukan menggunakan mekanisme konsensus mayoritas antar-node dengan mengklasifikasikan data sebagai VALID atau INVALID berdasarkan konsistensi nilai hash. Simulasi yang dilakukan menggunakan Jupyter Notebook menunjukkan bahwa sistem mampu mendeteksi manipulasi data pada skenario satu node maupun beberapa node. Sistem juga dilengkapi mekanisme auto-recovery untuk memulihkan node yang rusak atau dimanipulasi menggunakan data dari node yang valid. Selain itu, prototipe dikembangkan menjadi antarmuka berbasis web untuk verifikasi nomor pelacakan pengiriman secara real-time. Hasil penelitian menunjukkan bahwa metode PoR dapat membantu menjaga konsistensi, transparansi, dan akuntabilitas data pengiriman tanpa memerlukan implementasi blockchain secara penuh.

Kata Kunci: Proof of Reserve; Integritas Data; Blockchain; SHA-256; Konsensus Mayoritas; Sistem Logistik Terdesentralisasi.

1. Pendahuluan

Sistem pengiriman merupakan salah satu komponen penting dalam rantai pasok modern karena berfungsi memastikan kelancaran distribusi produk dari produsen hingga konsumen. Dalam praktiknya, sistem ini melibatkan berbagai pemangku kepentingan dan proses yang kompleks sehingga memerlukan pengelolaan data yang akurat dan andal. Integritas data menjadi aspek penting karena kesalahan pencatatan, keterlambatan pembaruan, atau manipulasi data dapat memengaruhi kepercayaan pelanggan dan kinerja perusahaan logistik. Seiring dengan perkembangan teknologi, *blockchain* mulai dimanfaatkan untuk mendukung transparansi dan keamanan data dalam rantai pasok. Teknologi ini memungkinkan pencatatan data secara terdistribusi dan permanen sehingga setiap transaksi dapat dilacak serta diverifikasi (Dewantoro, Chrysia, & Vagga, 2025). Selain itu, penggunaan teknologi digital dalam sistem logistik dapat mendukung efisiensi operasional dan pengambilan keputusan berbasis data. Beberapa penelitian menunjukkan bahwa integrasi *blockchain* berpotensi memperkuat integritas sistem pengiriman (Alexander *et al.*, 2025). Melalui sistem pelacakan yang transparan, risiko penipuan dan ketidakkonsistenan data dapat diminimalkan sehingga sistem pengiriman menjadi objek yang relevan untuk penerapan teknologi *blockchain* dalam menjaga integritas data (Sharabati & Jreisat, 2024).

Meskipun digitalisasi telah diterapkan, masalah integritas data masih sering terjadi dalam sistem pengiriman. Permasalahan tersebut mencakup kesalahan pencatatan, keterlambatan pembaruan status, dan manipulasi data. Selain itu, sistem terpusat memiliki risiko kehilangan data dan serangan siber yang dapat menurunkan kualitas layanan serta kepercayaan pengguna. Pemantauan sistem yang lemah juga menjadi salah satu penyebab rendahnya keandalan data pengiriman (Rahayu *et al.*, 2022). Kurangnya transparansi dalam proses pelacakan dapat menimbulkan potensi sengketa antara penyedia layanan dan pengguna (Douglas *et al.*, 2025). Oleh karena itu, diperlukan sistem yang mampu memastikan integritas dan validitas data secara lebih terukur agar informasi pengiriman dapat diandalkan (Muzaki *et al.*, 2024). Dalam penelitian ini, metode *Proof of Reserve* (PoR) digunakan sebagai mekanisme kriptografi untuk membantu memastikan ketersediaan dan integritas data secara transparan (Lazirko, Appelbaum, & Vasarhelyi, 2025).

Metode tersebut dikombinasikan dengan teknologi *blockchain* melalui penggunaan *hash* dan *prev_hash* untuk membentuk keterkaitan antardata. Setiap entri data juga diamankan menggunakan tanda tangan digital untuk memastikan keaslian dan mencegah manipulasi yang tidak terdeteksi. Struktur *Merkle Tree* digunakan untuk mengorganisasi data dalam bentuk pohon *hash* sehingga proses verifikasi dapat dilakukan melalui perbandingan *root hash*. Data disimpan pada beberapa *node* (*multi-node*) untuk mendukung redundansi, sedangkan proses validasi dilakukan melalui verifikasi *hash* dan tanda tangan digital guna mendeteksi ketidakkonsistenan data (Nadime *et al.*, 2023). Apabila ditemukan kesalahan, sistem melakukan pemulihan dengan mengambil data valid dari *node* lain untuk memperbaiki *node* yang mengalami kerusakan. Dengan pendekatan ini, sistem diarahkan tidak hanya untuk mendeteksi perubahan data, tetapi juga untuk memulihkan data secara otomatis. Kombinasi *Proof of Reserve*, *blockchain*, tanda tangan digital, *Merkle Tree*, dan mekanisme *auto-recovery* digunakan sebagai pendekatan untuk menjaga integritas data dalam sistem pengiriman (Kim *et al.*, 2025).

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis dan mengimplementasikan metode *Proof of Reserve* (PoR) pada sistem pengiriman guna menjaga integritas dan keaslian data. Implementasi dilakukan dengan memanfaatkan teknologi *blockchain* melalui *hash*, *prev_hash*, tanda tangan digital, dan struktur *Merkle Tree* dalam proses verifikasi data. Selain itu, penelitian ini mengevaluasi kemampuan sistem dalam mendeteksi manipulasi data serta mengembangkan mekanisme *multi-node* dan *auto-recovery* untuk menjaga integritas dan ketersediaan data pada sistem pengiriman.

2. Metode

2.1 Desain Penelitian dan Sumber Data

Metode penelitian yang digunakan adalah deskriptif-analitis dengan pendekatan kualitatif untuk memahami implementasi *Proof of Reserve* (PoR) dalam sistem pengiriman berbasis *blockchain*. Pendekatan ini dipilih karena penelitian berfokus pada proses verifikasi, integritas data, dan mekanisme pemulihan dalam sistem, bukan hanya pada hasil akhir (Lazirko, Appelbaum, & Vasarhelyi, 2025; Kim *et al.*, 2025). Data yang digunakan berupa *dataset* pengiriman yang diperoleh dari JNE Cabang Bajak 2 sebagai sumber data utama. *Dataset*

tersebut mencakup informasi nomor pelacakan, status pengiriman, tanggal, dan kota tujuan. Data sensitif dianonimkan atau dikecualikan untuk menjaga privasi, sedangkan informasi yang diperlukan untuk proses validasi tetap dipertahankan (Rahayu *et al.*, 2022; Muzaki *et al.*, 2024).

2.2 Persiapan Data dan Arsitektur Sistem

Dataset pengiriman dikonversi ke dalam format JSON sebelum disimpan pada tiga *node* CouchDB, yaitu *Primary*, *Backup* 1, dan *Backup* 2. Ketiga *node* tersebut berfungsi sebagai unit penyimpanan yang identik untuk mendukung redundansi data dan proses verifikasi antar-*node* (Nadime *et al.*, 2023). Arsitektur ini digunakan agar setiap data pengiriman memiliki salinan pada beberapa *node*, sehingga ketidaksesuaian data dapat dideteksi melalui proses perbandingan antar-*node*. Dengan pengaturan tersebut, sistem dapat memeriksa konsistensi data yang tersimpan pada *node* utama dan *node* cadangan sebelum menentukan status validitas data.

2.3 Mekanisme Validasi Kriptografis

Setiap entri data diproses menggunakan algoritma SHA-256 untuk menghasilkan nilai *hash*. Nilai *hash* tersebut digunakan untuk membentuk rantai data melalui mekanisme *prev_hash* sehingga setiap entri saling terhubung secara kriptografis. Selain itu, seluruh nilai *hash* data pengiriman disusun ke dalam struktur *Merkle Tree* untuk menjaga integritas data secara hierarkis dan memungkinkan verifikasi perubahan data melalui perbandingan *root hash* (Kim *et al.*, 2025). Setiap nilai *hash* data kemudian ditandatangani menggunakan algoritma kriptografi asimetris RSA untuk menghasilkan tanda tangan digital. Tanda tangan ini digunakan untuk memastikan keaslian data dan mencegah modifikasi yang tidak terdeteksi selama proses validasi (Prasetijowati *et al.*, 2023). Validasi dilakukan dengan membandingkan nilai *hash* yang dihitung ulang, struktur *Merkle Tree*, dan hasil verifikasi tanda tangan digital pada seluruh *node*. Data dianggap valid apabila seluruh hasil pemeriksaan sesuai dan tanda tangan digital dapat diverifikasi. Sebaliknya, jika ditemukan ketidakkonsistenan antar-*node*, data diklasifikasikan sebagai tidak valid atau mengalami kerusakan (Nadime *et al.*, 2023; Kim *et al.*, 2025). Mekanisme ini memungkinkan sistem mendeteksi perubahan data berdasarkan perbedaan nilai *hash*, ketidaksesuaian *root hash*, atau kegagalan verifikasi tanda tangan digital.

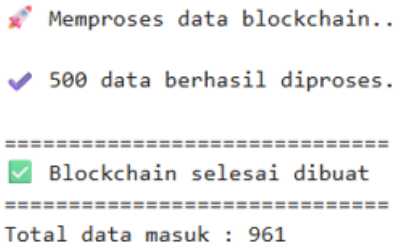
2.4 Simulasi Manipulasi, Pemulihan, dan Visualisasi

Untuk menguji ketahanan sistem, manipulasi data disimulasikan pada satu atau beberapa *node* tanpa memperbarui nilai *hash*, *Merkle Tree*, atau tanda tangan digital. Setelah manipulasi dilakukan, sistem menjalankan kembali proses validasi untuk mendeteksi perubahan dan mengidentifikasi *node* yang mengalami ketidaksesuaian (Kim *et al.*, 2025). Jika ditemukan ketidakkonsistenan pada suatu *node*, sistem melakukan proses pemulihan dengan mengambil data valid dari *node* lain sebagai referensi untuk memperbaiki *node* yang mengalami kerusakan. Proses ini bertujuan menjaga konsistensi data dan keandalan sistem selama masih tersedia *node* valid yang dapat digunakan sebagai sumber pemulihan (Lazirko, Appelbaum, & Vasarhelyi, 2025; Kim *et al.*, 2025). Hasil validasi, status *node*, dan jejak *audit* disajikan dalam bentuk laporan serta antarmuka berbasis *web*. Visualisasi ini digunakan untuk memantau integritas data, mengevaluasi hasil verifikasi, dan menampilkan status sistem berdasarkan mekanisme keamanan berbasis *blockchain* yang didukung oleh *Merkle Tree* dan tanda tangan digital (Onu *et al.*, 2024).

3. Hasil dan Pembahasan

3.1 Hasil

Sistem verifikasi data pengiriman berbasis *blockchain* telah diimplementasikan dengan arsitektur *multi-node* yang terdiri atas NODE_1 sebagai *node* utama serta NODE_2 dan NODE_3 sebagai *node* cadangan. Setiap *node* menyimpan salinan data yang identik sehingga proses validasi silang dapat dilakukan untuk memeriksa konsistensi data. Sebelum proses verifikasi dijalankan, sistem membangun struktur *blockchain* dari data pelacakan pengiriman. Setiap entri data diubah menjadi blok yang memuat nilai *hash*, *prev_hash*, dan *signature*, sebagaimana ditunjukkan pada Gambar 1.



Gambar 1. Data Pengiriman Berhasil Disimpan dalam Sistem *Blockchain*

Pengujian verifikasi dilakukan dengan memasukkan nomor pelacakan ke dalam sistem. Setelah nomor pelacakan diterima, sistem memeriksa nilai *hash*, *signature*, konsistensi *chain*, dan *Merkle Root* pada seluruh *node*. Pada kondisi normal, seluruh *node* memiliki nilai *hash* yang identik karena nilai tersebut dihasilkan dari kombinasi data dan *prev_hash* yang sama. Status "Signature Valid: True" pada setiap *node* menunjukkan bahwa *signature* yang dibuat menggunakan *private key* sesuai dengan nilai *hash* data ketika diverifikasi menggunakan *public key*. Selain itu, *Global Merkle Root* yang identik menunjukkan bahwa keseluruhan data dalam sistem berada dalam kondisi konsisten, sebagaimana ditampilkan pada Gambar 2.

Gambar 2. Hasil Verifikasi Pengiriman dalam Kondisi Normal

Pengujian berikutnya dilakukan pada kondisi *signature* tidak valid. Dalam skenario ini, salah satu *node*, yaitu NODE_1, menunjukkan status "Signature Valid: False". Kondisi tersebut terjadi karena data pada *node* telah dimodifikasi sehingga menghasilkan nilai *hash* yang berbeda, sedangkan *signature* tidak diperbarui. Karena *signature* dihasilkan dari nilai *hash* asli menggunakan *private key*, perubahan pada data menyebabkan ketidaksesuaian ketika proses verifikasi dilakukan menggunakan *public key*. Meskipun *prev_hash* masih konsisten dan *chain* belum terputus, data tetap diklasifikasikan tidak valid karena proses autentikasi gagal. Kondisi ini juga memengaruhi nilai *Merkle Root* karena perubahan pada satu data berdampak pada representasi integritas data secara keseluruhan. Pada skenario *chain* terputus, sistem mendeteksi ketidaksesuaian antara nilai *prev_hash* pada suatu blok dan nilai *hash* dari blok sebelumnya. Kondisi ini menunjukkan bahwa keterhubungan antarblok dalam rantai data telah terganggu. Jika ketidaksesuaian tersebut terjadi pada salah satu blok, blok setelahnya juga berpotensi terdampak karena struktur *blockchain* bergantung pada keterkaitan nilai *hash* antardata. Hasil verifikasi pada kondisi *chain* terputus ditampilkan pada Gambar 3.

Gambar 3. Hasil Verifikasi Pengiriman dengan *Chain* Terputus

Simulasi manipulasi *blockchain* dilakukan untuk menguji kemampuan sistem dalam mendeteksi perubahan data dan dampaknya terhadap integritas sistem. Manipulasi dilakukan secara berurutan mulai dari *node*

utama untuk mengamati pengaruh perubahan terhadap validasi *hash*, verifikasi *signature*, dan nilai *Merkle Root*. Pada simulasi ini, data pada *node* utama dimodifikasi dengan mengubah nilai berat dan tujuan. Perubahan tersebut memengaruhi nilai *hash* karena *hash* dihasilkan dari kombinasi data dan *prev_hash*. Hasil simulasi manipulasi data ditampilkan pada Gambar 4.

Gambar 4. Simulasi Manipulasi Data

Berdasarkan hasil simulasi, sistem menghitung ulang nilai *hash* dan membandingkannya dengan nilai yang tersimpan. Pada skenario tertentu, nilai *hash* tetap terlihat valid karena *hash* yang tersimpan telah dihasilkan dari data yang dimodifikasi [cek data]. Kondisi ini menunjukkan bahwa validasi *hash* hanya memastikan konsistensi data, tetapi belum cukup untuk memastikan keaslian data. Validasi *signature* kemudian mendeteksi manipulasi karena *signature* tidak diperbarui setelah perubahan data dilakukan. Hasil tersebut menyebabkan NODE_1 diklasifikasikan tidak valid, sedangkan *node* cadangan tetap valid. Selain itu, perubahan pada data juga berdampak pada *Merkle Root*, sehingga sistem dapat mengidentifikasi bahwa integritas global telah berubah meskipun manipulasi hanya dilakukan pada satu *node*. Sistem *auto-recovery* diterapkan untuk memulihkan *blockchain* ke kondisi konsisten ketika terjadi kerusakan atau manipulasi data pada satu atau beberapa *node*. Proses pemulihan dilakukan dengan membandingkan seluruh *node* dan memilih *node* valid berdasarkan hasil validasi *hash*, *signature*, dan *chain*. Pada skenario pemulihan berhasil, sistem masih memiliki setidaknya satu *node* valid yang dapat digunakan sebagai referensi. *Node* valid tersebut digunakan untuk menyinkronkan ulang *node* lain yang mengalami kerusakan sehingga seluruh *node* kembali memiliki nilai *hash*, *prev_hash*, dan *signature* yang identik. Proses *auto-recovery* yang berhasil ditampilkan pada Gambar 5.

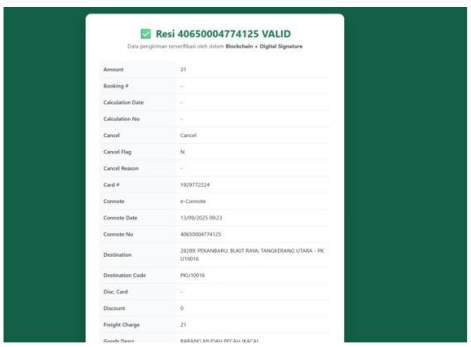
Gambar 5. Proses *Auto-Recovery* Berhasil

Namun, *auto-recovery* memiliki keterbatasan ketika seluruh *node* mengalami kerusakan. Dalam kondisi tersebut, sistem tidak memiliki sumber data yang dapat dijadikan referensi tepercaya untuk proses pemulihan. Akibatnya, proses *auto-recovery* tidak dapat dilakukan dan sistem mengklasifikasikan kondisi tersebut sebagai kegagalan pemulihan. Kondisi *auto-recovery* gagal ditampilkan pada Gambar 6.

```
================================================================
AUTO RECOVERY SYSTEM (FINAL SAFE MODE)
================================================================

================================================================
FAILURE AT RESI 40650004774125
================================================================
❌ Tidak ada node valid (signature + hash rusak semua)

================================================================

================================================================
RECOVERY FAILED
================================================================
❌ Chain tidak bisa dipulihkan
```

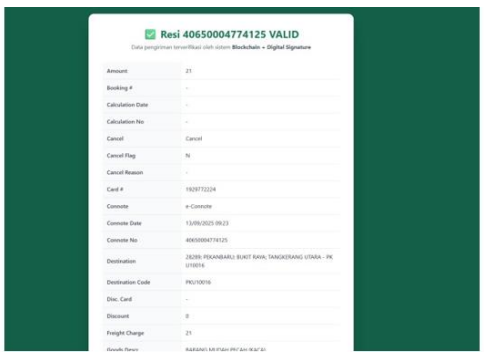
Gambar 6. Proses *Auto-Recovery* Gagal

Sistem verifikasi selanjutnya diintegrasikan ke dalam aplikasi berbasis *web* agar pengguna dapat melakukan verifikasi nomor pelacakan tanpa menggunakan terminal. Pengguna memasukkan nomor pelacakan, kemudian sistem secara otomatis melakukan validasi pada data *blockchain*. Jika nomor pelacakan valid dan seluruh *node* berada dalam kondisi konsisten, sistem menampilkan informasi pengiriman secara lengkap. Tampilan hasil pelacakan valid ditunjukkan pada Gambar 7.



Gambar 7. Tampilan Hasil Pelacakan Valid

Sebaliknya, jika nomor pelacakan tidak valid atau tidak ditemukan, sistem tidak menampilkan data pengiriman. Jika sistem menemukan ketidakkonsistenan, seperti *signature* tidak valid atau *chain* terputus, tampilan data diblokir sebagai tindakan pengamanan. Tampilan hasil pelacakan tidak valid ditunjukkan pada Gambar 8.



Gambar 8. Tampilan Hasil Pelacakan Tidak Valid

Pada implementasi *web*, sistem menjalankan proses validasi *backend* yang sama dengan proses validasi utama, yaitu perhitungan ulang *hash*, verifikasi *signature* menggunakan *public key*, serta pemeriksaan integritas *chain*. Jika salah satu proses validasi gagal, sistem mengklasifikasikan data sebagai tidak valid dan mencegah data tersebut ditampilkan kepada pengguna. Implementasi ini menunjukkan bahwa mekanisme verifikasi dapat diterapkan pada antarmuka pengguna untuk mendukung pemeriksaan data pengiriman secara langsung.

3.2 Pembahasan

Hasil implementasi menunjukkan bahwa penggunaan struktur *blockchain* sederhana dengan *hash*, *prev_hash*, *signature*, dan *Merkle Tree* dapat mendukung proses verifikasi integritas data pengiriman. Keterkaitan antarblok melalui *prev_hash* membuat perubahan pada satu data lebih mudah dideteksi

karena perubahan tersebut dapat memengaruhi hubungan dengan blok sebelum atau sesudahnya. Selain itu, penggunaan *Merkle Root* memberikan representasi ringkas terhadap kondisi keseluruhan data, sehingga perubahan pada satu entri dapat ditelusuri melalui perubahan nilai akar. Temuan ini sejalan dengan kajian tentang penerapan teknologi pelacakan dalam rantai pasok yang menekankan pentingnya transmisi informasi yang dapat diverifikasi untuk menjaga integritas data antaraktor dalam proses distribusi (Li *et al*., 2024).

Validasi *hash* dalam sistem ini berperan penting untuk memeriksa konsistensi data, tetapi hasil pengujian menunjukkan bahwa validasi tersebut belum cukup untuk memastikan keaslian data. Pada skenario manipulasi, data dapat terlihat konsisten apabila nilai *hash* telah disesuaikan dengan data yang berubah. Oleh karena itu, tanda tangan digital menjadi komponen penting karena *signature* menghubungkan nilai *hash* dengan otorisasi kriptografis melalui pasangan *private key* dan *public key*. Ketika data berubah tanpa pembaruan *signature* yang sah, sistem dapat mendeteksi bahwa data tidak autentik. Hal ini memperlihatkan bahwa kombinasi validasi konsistensi dan autentikasi lebih kuat dibandingkan pemeriksaan *hash* secara tunggal. Penerapan arsitektur *multi-node* juga memberikan manfaat dalam proses validasi silang. Ketika salah satu *node* mengalami manipulasi, *node* lain yang masih valid dapat digunakan sebagai pembanding untuk menentukan kondisi data. Prinsip ini relevan dengan kebutuhan integritas rantai pasok, karena keandalan informasi tidak hanya bergantung pada pencatatan data, tetapi juga pada kemampuan sistem untuk menjaga konsistensi informasi di antara pihak atau unit penyimpanan yang terlibat. Rashid *et al*. (2018) menekankan bahwa sistem ketertelusuran berperan dalam menjaga integritas rantai pasok melalui keterhubungan data dan kepercayaan antaraktor. Dalam konteks penelitian ini, keterhubungan tersebut diwujudkan melalui replikasi data pada beberapa *node* dan pemeriksaan konsistensi antar-*node*.

Hasil pengujian *auto-recovery* menunjukkan bahwa sistem mampu memulihkan data ketika masih tersedia *node* valid sebagai sumber referensi. Mekanisme ini penting karena sistem pengiriman memerlukan ketersediaan data yang konsisten untuk mendukung proses pelacakan. Namun, hasil juga menunjukkan adanya keterbatasan ketika seluruh *node* mengalami kerusakan. Dalam kondisi tersebut, sistem tidak memiliki referensi yang dapat dipercaya untuk memulihkan data. Keterbatasan ini menunjukkan bahwa redundansi tiga *node* belum sepenuhnya menghilangkan risiko kegagalan, terutama apabila kerusakan terjadi secara menyeluruh. Oleh karena itu, penerapan sistem pada skala yang lebih besar perlu mempertimbangkan jumlah *node*, strategi pencadangan, dan mekanisme konsensus yang lebih kuat. Verifikasi data pengiriman tidak hanya berkaitan dengan keamanan teknis, tetapi juga dengan kualitas layanan dan kepercayaan pengguna. Keterlambatan, ketidaksesuaian status, atau kesalahan informasi dapat memengaruhi persepsi pengguna terhadap layanan pengiriman. Kajian Marsello *et al*. (2023) menunjukkan bahwa keterlambatan pengiriman menjadi salah satu persoalan penting dalam layanan logistik, sedangkan Sinnun dan Putri (2020) menekankan pentingnya sistem informasi dalam mendukung pemesanan dan pengelolaan jasa pengiriman barang. Berdasarkan hal tersebut, sistem verifikasi berbasis *web* dalam penelitian ini dapat membantu pengguna memeriksa status data pengiriman secara lebih mudah, meskipun efektivitasnya terhadap kecepatan layanan dan kepuasan pengguna masih perlu diuji lebih lanjut.

Penerapan *Proof of Reserve* (PoR) dalam penelitian ini lebih diarahkan sebagai mekanisme pembuktian ketersediaan dan integritas data, bukan sebagai pembuktian cadangan aset sebagaimana lazim digunakan pada konteks keuangan. Dalam sistem ini, PoR diadaptasi melalui keberadaan salinan data pada beberapa *node*, pembuktian konsistensi melalui *hash*, serta verifikasi keaslian melalui tanda tangan digital. Dengan demikian, pendekatan yang digunakan dapat dipahami sebagai penerapan konsep pembuktian berbasis kriptografi untuk menjaga keandalan data pengiriman. Hal ini sejalan dengan pandangan bahwa integritas rantai pasok memerlukan kerangka yang mampu menjaga keaslian, keterlacakan, dan konsistensi informasi dari satu proses ke proses berikutnya (Zulfakar *et al*., 2014). Meskipun sistem yang dikembangkan mampu mendeteksi manipulasi dan menjalankan pemulihan pada kondisi tertentu, hasil penelitian ini masih memiliki beberapa batasan. Sistem dikembangkan pada arsitektur tiga *node* sehingga kemampuan konsensusnya masih terbatas. Selain itu, penelitian belum menyajikan pengukuran kuantitatif seperti waktu verifikasi, waktu pemulihan, jumlah skenario pengujian, atau tingkat keberhasilan deteksi pada volume data yang lebih besar. Oleh karena itu, hasil penelitian ini lebih tepat dipahami sebagai bukti implementasi awal bahwa mekanisme PoR berbasis *blockchain* dapat digunakan untuk mendukung integritas data pengiriman, bukan sebagai klaim bahwa sistem telah optimal untuk seluruh kondisi operasional logistik.

4. Kesimpulan dan Saran

Penelitian ini mengimplementasikan metode *Proof of Reserve* (PoR) pada sistem validasi data pengiriman berbasis *blockchain* dengan menggunakan algoritma SHA-256, tanda tangan digital, dan *Merkle Tree* pada arsitektur tiga *node* CouchDB. Setiap data pengiriman disimpan sebagai blok yang saling terhubung melalui mekanisme *previous hash*, sehingga perubahan data dapat dideteksi melalui proses verifikasi. Validasi dilakukan melalui pemeriksaan nilai *hash*, autentikasi tanda tangan digital, dan pengecekan konsistensi antar-*node* menggunakan mekanisme konsensus sederhana. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi manipulasi data pada skenario yang diuji serta melakukan proses pemulihan selama masih tersedia *node* valid sebagai sumber referensi. Dengan demikian, sistem yang dikembangkan dapat mendukung keamanan, transparansi, keandalan, dan kepercayaan terhadap data pengiriman.

Berdasarkan hasil penelitian, pengembangan sistem pada penelitian selanjutnya dapat dilakukan melalui integrasi *smart contract* untuk mengotomatisasi proses verifikasi, pencatatan, dan audit pengiriman secara aman dan *real-time*. Penelitian berikutnya juga disarankan untuk menggunakan jumlah *node* yang lebih banyak agar mekanisme konsensus menjadi lebih kuat dan keandalan sistem dapat ditingkatkan. Selain itu, integrasi teknologi *Internet of Things* (IoT), seperti *sensor* dan perangkat GPS, dapat diterapkan untuk menyelaraskan kondisi fisik barang dengan catatan digital pengiriman. Pengembangan tersebut diharapkan dapat memperluas penerapan sistem pengiriman berbasis *blockchain* dalam menjaga integritas dan transparansi data.

Referensi

Adiningrum, N. T. R. (2023). Analisis penyebab keterlambatan pengiriman barang pada Pos Express menggunakan metode Six Sigma. *LOGISTIK, 16*(1), 42–53. [cek referensi: pastikan apakah nama penulis lengkap hanya N. T. R. Adiningrum atau ada penulis lain]

Alexander, N., Monalisa, M., Wijaya, B. A., & Dewantoro, R. W. (2025). Penerapan blockchain untuk keamanan data rekam medis elektronik: Literatur review. *AT-TAKLIM: Jurnal Pendidikan Multidisiplin, 2*(3), 191–201. https://journal.hasbaedukasi.co.id/index.php/at-taklim

Choobineh, M., Arabnya, A., Khodaei, A., & Zheng, H. (2023). Game-theoretic peer-to-peer solar energy trading on blockchain-based transaction infrastructure. *e-Prime - Advances in Electrical Engineering, Electronics and Energy, 5*. https://doi.org/10.1016/j.prime.2023.100192

Dewantoro, R. W., Chrysia, C., & Vagga, C. P. (2025). Analisis perbandingan blockchain publik dan privat: Keuntungan dan tantangan dalam sektor bisnis. *AT-TAKLIM: Jurnal Pendidikan Multidisiplin, 2*(4), 31–39. https://journal.hasbaedukasi.co.id/index.php/at-taklim

Douglas, M. A., Quade, M. J., Dickey, E. C., & Neubert, M. J. (2025). The ethics of sustainability in supply chain relationships: Through the lens of supply chain integrity. *Journal of Business Logistics, 46*(4). https://doi.org/10.1111/jbl.70043

Kim, B., Lee, D., Lee, J., & Lee, W. (2025). Snapshot cherry-picking attack in CEX proof of reserves and its mitigation. *IEEE Access, 13*. https://doi.org/10.1109/ACCESS.2025.3564999

Lazirko, M., Appelbaum, D., & Vasarhelyi, M. (2025). Proof of reserves: A double-helix framework. *The British Accounting Review*. https://doi.org/10.1016/j.bar.2025.101730

Li, P., Yang, J., Jiménez-Carvelo, A. M., & Erasmus, S. W. (2024). Applications of food packaging quick response codes in information transmission toward food supply chain integrity. *Trends in Food Science & Technology, 146*. https://doi.org/10.1016/j.tifs.2024.104384

Martono, R. V. (2020). *Supply chain 4.0: Berbasis blockchain dan platform*. Gramedia.

Muzaki, A., Ramadhan, F., Rahayu, G. S., Al Ghifari, M. F., Pratama, M. R., Kamisik, R. A., & Septiani, N. W. P. (2024). Perancangan sistem tracking pengiriman barang multi logistik. *Jurnal Riset dan Aplikasi Mahasiswa Informatika (JRAMI), 5*(1), 210–216. https://doi.org/10.30998/jrami.v5i1.10724

Nadime, K. L., Benhra, J., Benabbou, R., & Mouatassim, S. (2023). Automating attended home deliveries with smart contracts: A blockchain-based solution for e-commerce logistics. *E3S Web of Conferences, 469*, Article 00026. https://doi.org/10.1051/e3sconf/202346900026

Onu, P., Mbohwa, C., & Pradhan, A. (2024). Blockchain-powered traceability solutions: Pioneering transparency to eradicate counterfeit products and revolutionize supply chain integrity. *Procedia Computer Science, 232*, 1420–1427. https://doi.org/10.1016/j.procs.2024.01.140

Prasetijowati, T., Kurniawan, B. A., & Irawan, A. (2023). Peningkatan kualitas pelayanan jasa pengiriman barang di PT. Kereta Api Logistik Express Gubeng Surabaya. *Jurnal Sosial Humaniora Sigli, 6*(2), 484–490. https://doi.org/10.47647/jsh.v6i2.1674

Rahayu, A., Tambunan, W., Pawitra, T. A., & Tosungku, L. O. A. S. (2022). Penentuan prioritas perbaikan layanan pengiriman barang pada industri logistik. *Journal Industrial Servicess, 7*(2), 295–303. https://doi.org/10.36055/jiss.v7i2.14457

Rashid, N. A., Supian, K., & Bojei, J. (2018). Relationship between halal traceability system adoptions on halal food supply chain integrity and performance. *International Journal of Asian Social Science, 8*(8), 569–579. https://doi.org/10.18488/journal.1.2018.88.569.579

Saputro, R. W., & Mardiyati, S. (2024). Penggunaan teknologi blockchain dalam keamanan sistem pendistribusian data. *Journal of Multidisciplinary Inquiry in Science, Technology and Educational Research, 1*(4), 2049–2054. [cek referensi: tambahkan DOI atau URL jika tersedia]

Sharabati, A. A. A., & Jreisat, E. R. (2024). Blockchain technology implementation in supply chain management: A literature review. *Sustainability, 16*(7), Article 2823. https://doi.org/10.3390/su16072823

Sinnun, A., & Putri, I. A. (2019). Implementasi sistem informasi pemesanan jasa pengiriman barang kargo pada PT. Suksema Abadi Logistik dengan model waterfall. *Jurnal Riset Informatika, 2*(1), 37–42. https://doi.org/10.34288/jri.v2i1.114

United Nations Conference on Trade and Development. (2024). *Business e-commerce sales and the role of online platforms* (No. 1). United Nations. https://doi.org/10.18356/9789211064490

Zulfakar, M. H., Anuar, M. M., & Talib, M. S. A. (2014). Conceptual framework on halal food supply chain integrity enhancement. *Procedia - Social and Behavioral Sciences, 121*. https://doi.org/10.1016/j.sbspro.2014.01.1108.

How Cites

Sembiring, D. S. Z., Putra, A., Siregar, A. Z., Pradana, A. S., & Dewantoro, R. W. (2026). Implementasi Metode Proof of Reserve pada Sistem Pengiriman Barang untuk Menjaga Integritas Data. *Computer Journal*, *4*(2), 136-144. https://doi.org/10.58477/cj.v4i2.490.

Publisher's Note