REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

Desenvolvimento de uma Infraestrutura Blockchain Offline para Rastreabilidade em Processos Produtivos

Development of an Offline Blockchain Infrastructure for Traceability in Production Processes

Desarrollo de una Infraestructura Blockchain Offline para la Trazabilidad en Procesos Productivos

Alan Thiago Santos de Oliveira
Pós-graduando em Ciências de dados e big data, Manaus, Amazonas, Brasil.
E-mail: alan.oliveira@kodigos.com.br
Orcid: https://orcid.org/0009-0000-2873-6886

Ayumi Aoki Santana
Mestranda em Informática
E-mail: ayumi.aoki@kodigos.com.br
Orcid: https://orcid.org/0009-0005-5372-4533

Deangelly Coitinho Figueirado
Bacharel em Engenharia da Computação, Manaus, Amazonas, Brasil.
E-mail: deangelly.figueiredo@kodigos.com.br
Orcid: https://orcid.org/0009-0005-6330-5244

Pedro Henrique Souza Soprano
Bacharel em Ciência da Computação, Manaus, Amazonas, Brasil.
E-mail: pedro.soprano@kodigos.com.br
Orcid: https://orcid.org/0009-0004-9249-5844

Sandro Breval Santiago
Doutor em Engenharia de Produção, Manaus, Amazonas, Brasil.
E-mail: sbreval@ufam.edu.br

Resumo

A Indústria 4.0 ampliou a demanda por rastreabilidade confiável nos processos de manufatura, necessidade nem sempre atendida por sistemas tradicionais. A tecnologia blockchain oferece integridade verificável e auditabilidade, porém redes públicas são inadequadas para requisitos industriais como baixa latência e operação offline. Este trabalho apresenta o desenvolvimento e a validação experimental de uma arquitetura de blockchain privada e offline, concebida como um microsserviço genérico para registro com integridade verificável e detecção de adulteração. Após uma Rapid Review sobre o estado da arte, foi implementada uma rede permissionada utilizando mecanismo de consenso inspirado em Proof-of-Authority (PoA), baseado em validadores previamente configurados, API REST e persistência local em arquivos JSON. Os resultados experimentais em ambiente containerizado demonstraram estabilidade, com vazão superior a 1.000 transações por segundo, latência abaixo de 10 ms e detecção eficaz de tentativas de adulteração. A arquitetura proposta atua como uma camada independente de registro e auditoria para suporte à rastreabilidade industrial, fornecendo integridade verificável em ambientes controlados e offline..

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

Palavras-chave: Indústria 4.0; Blockchain; Rastreabilidade Industrial; Rede Permissionada; Proof-of-Authority.

Abstract

Industry 4.0 has increased the demand for reliable traceability in manufacturing processes, a need that traditional systems do not always meet. Blockchain technology offers verifiable integrity and auditability, but public networks are unsuitable for industrial requirements such as low latency and offline operation. This work presents the development and experimental validation of a private, offline blockchain architecture, conceived as a generic microservice for record-keeping with verifiable integrity and tamper detection. Following a Rapid Review of the state of the art, a permissioned network was implemented using a consensus mechanism inspired by Proof-of-Authority (PoA), based on previously configured validators, a REST API, and local persistence in JSON files. Experimental results in a containerized environment demonstrated stability, with throughput above 1,000 transactions per second, latency below 10 ms, and effective detection of tampering attempts. The proposed architecture acts as an independent logging and auditing layer to support industrial traceability, providing verifiable integrity in controlled and offline environments.

Keywords: Industry 4.0; Blockchain; Industrial Traceability; Permissioned Network; Proof-of-Authority.

Resumen

La Industria 4.0 ha ampliado la demanda de trazabilidad confiable en los procesos de manufactura, una necesidad no siempre atendida por los sistemas tradicionales. La tecnología blockchain ofrece integridad verificable y auditabilidad, pero las redes públicas resultan inadecuadas para requisitos industriales como la baja latencia y la operación sin conexión. Este trabajo presenta el desarrollo y la validación experimental de una arquitectura de blockchain privada y offline, concebida como un microservicio genérico para el registro con integridad verificable y detección de adulteración. Tras una Rapid Review sobre el estado del arte, se implementó una red permisionada utilizando un mecanismo de consenso inspirado en Proof-of-Authority (PoA), basado en validadores previamente configurados, API REST y persistencia local en archivos JSON. Los resultados experimentales en un entorno contenerizado demostraron estabilidad, con un rendimiento superior a 1.000 transacciones por segundo, latencia inferior a 10 ms y detección eficaz de intentos de adulteración. La arquitectura propuesta actúa como una capa independiente de registro y auditoría para respaldar la trazabilidad industrial, proporcionando integridad verificable en entornos controlados y fuera de línea.

Palabras clave: Industria 4.0; Blockchain; Trazabilidad Industrial; Red Permisionada; Prueba de Autoridad (Proof-of-Authority).

1. Introdução

A Indústria 4.0 ampliou o uso de tecnologias digitais na manufatura, como IoT, sistemas ciberfísicos, análise de dados e automação (Xu et al., 2018). Com isso, aumentou a geração de registros de produção, inspeção, qualidade, materiais e equipamentos. Nesse cenário, a rastreabilidade é importante em setores que

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

dependem de registros confiáveis, como aeroespacial (Cohen et al., 2021), semicondutores (Murgai, 2024) e manufatura (Kuo & Yang, 2025).

Sistemas como MES e bancos de dados relacionais apoiam o controle da produção (Saenz de Ugarte et al., 2015), mas não oferecem, por si só, imutabilidade e verificação distribuída. Blockchain pode apoiar a integridade e a auditabilidade dos registros (Nakamoto, 2008), embora apresente desafios de segurança, consenso, escalabilidade e integração (Zheng et al., 2018; Casino et al., 2019). Em ambientes industriais, requisitos como baixa latência, controle de acesso e operação local favorecem redes privadas e permissionadas (Fernández-Caramés & Fraga-Lamas, 2019). Assim, este trabalho tem como objetivo desenvolver e validar uma arquitetura de blockchain privada e offline para registro auditável de dados e eventos industriais.

Para apoiar as decisões da arquitetura, foi conduzida uma Rapid Review sobre blockchain aplicada à rastreabilidade industrial (Cartaxo et al., 2018). A revisão identificou o uso de redes permissionadas, smart contracts, sensores, IoT, sistemas industriais e estratégias de armazenamento (Mohamed & Al-Jaroodi, 2019; Kuhn et al., 2021; Jia & Wang, 2024; Wu et al., 2025). Com base nesses achados e nos requisitos da solução, foi implementada uma rede privada e permissionada, com consenso inspirado em Proof-of-Authority, comunicação P2P, API REST e persistência local. O uso de PoA é adequado a redes com validadores conhecidos (De Angelis et al., 2018).

Nos testes, a rede com três nós apresentou latência média inferior a 10 ms, throughput superior a 1.000 transações por segundo e processou mais de 100.000 transações em 10.000 blocos. Os testes também mostraram que a solução detecta alterações nos registros por meio dos hashes encadeados com SHA-256, rejeita blocos corrompidos e trata bifurcações por meio das rotinas de sincronização.

A principal contribuição é uma arquitetura genérica, privada, permissionada e offline para registro auditável de eventos industriais. A proposta segue características já usadas em aplicações de blockchain na manufatura e rastreabilidade (Chen et al., 2022; Ali et al., 2022; Košťál et al., 2024) e fornece mecanismos de integridade,

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

detecção de alterações, rastreabilidade e auditoria com operação local.

2. Referencial Teórico

2.1. Indústria 4.0

A Indústria 4.0 representa uma mudança nos processos produtivos, marcada pela integração entre sistemas físicos e digitais. Xu et al. (2018) associam esse paradigma ao uso de IoT, sistemas ciberfísicos, análise de dados, automação e conectividade entre equipamentos. Esses recursos permitem coletar e compartilhar dados ao longo da produção, criando novas demandas de controle, monitoramento e auditoria.

A rastreabilidade industrial depende da capacidade de registrar e recuperar o histórico de produtos, componentes, processos e operações. Guo, Zhang e Zhang (2022) relacionam blockchain-enabled smart manufacturing a segurança, confiança, compartilhamento de dados e coordenação. Song e Zhu (2022) analisam blockchain em sistemas de manufatura inteligente, destacando rastreabilidade, transparência e registro de dados no ciclo de vida do produto.

Em produtos complexos, a rastreabilidade exige controle sobre peças, submontagens, operações, inspeções e recursos produtivos. Cohen e Rozenes (2023) propõem o uso de Bill of Assembly e smart contracts para digitalização e rastreabilidade de montagem. Cohen, Nabrzyski e Taylor (2021) aplicam blockchain ao contexto de montagem aeroespacial. Kuhn et al. (2021) propõem uma aplicação baseada em blockchain para rastrear estruturas de montagem complexas, incluindo peças, lotes e relações hierárquicas.

A integração de tecnologias digitais também aparece em soluções voltadas à rastreabilidade industrial. Chen et al. (2022) discutem blockchain em PLM para manufatura inteligente. Jie et al. (2025) integram inspeção, qualidade e rastreabilidade de dados em manufatura verde. Roumeliotis et al. (2024) analisam a integração entre blockchain e digital twins na Indústria 4.0. Zhang et al. (2026)

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

propõem rastreabilidade confiável em manufatura de bobinas de transformadores com internet industrial e digital twin.

Apesar desses recursos, a coleta de dados não garante que os registros permaneçam íntegros depois de gerados. Saenz de Ugarte, Artiba e Pellerin (2015) descrevem MES como sistemas voltados ao acompanhamento e execução da manufatura, mas esse tipo de solução não fornece imutabilidade nativa. Por isso, mecanismos adicionais de verificação, auditoria e preservação de evidências tornam-se relevantes em ambientes industriais.

2.2. Blockchain

Blockchain é uma tecnologia de registro distribuído baseada em blocos encadeados por funções criptográficas. Nakamoto (2008) apresentou essa estrutura em uma rede peer-to-peer para transações eletrônicas. Cada bloco armazena seu próprio hash e o hash do bloco anterior, formando uma cadeia verificável. Zheng et al. (2018) explicam que alterações nos dados modificam o hash correspondente, comprometendo a consistência da cadeia.

Essas características permitem o uso da blockchain como mecanismo de integridade e auditoria. Casino, Dasaklis e Patsakis (2019) classificam aplicações blockchain em diferentes domínios e discutem desafios como privacidade, escalabilidade e interoperabilidade. Wang, Han e Beynon-Davies (2019) analisam blockchain em cadeias de suprimentos e destacam sua relação com rastreabilidade e transparência. Mohamed e Al-Jaroodi (2019) discutem sua aplicação em cenários de Indústria 4.0.

Em ambientes de manufatura, a blockchain pode registrar eventos, medições, inspeções, documentos e associações entre componentes. Ali, Shin e Song (2022) propõem um sistema de qualidade aberta baseado em blockchain para manufatura inteligente. Kuhn et al. (2021) usam blockchain para rastrear estruturas de montagem complexas. Yousef et al. (2025) integram IoT, inspeção de defeitos e blockchain em processos de fundição.

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

Redes públicas de blockchain apresentam limitações para aplicações industriais. Fernández-Caramés e Fraga-Lamas (2019) discutem desafios de adoção de blockchain em fábricas inteligentes, incluindo segurança, desempenho e integração com IoT industrial. Em fábricas, a operação pode exigir baixa latência, controle de acesso e funcionamento em rede local. Por isso, redes privadas, permissionadas ou de consórcio são mais adequadas quando os participantes são conhecidos e autorizados.

O consenso define como os nós concordam sobre a validade dos blocos. Mingxiao et al. (2017) revisam diferentes algoritmos de consenso e apontam diferenças de desempenho, segurança e custo computacional. Em redes permissionadas, De Angelis et al. (2018) discutem Proof-of-Authority como uma alternativa baseada em validadores autorizados. Esse modelo reduz custos de mineração e melhora a previsibilidade, o que favorece ambientes industriais controlados.

Alguns estudos da Rapid Review adotam configurações permissionadas. Jia e Wang (2024) utilizam Hyperledger Fabric em um sistema de rastreabilidade para montagem de robôs. Košťál et al. (2024) aplicam Hyperledger Fabric em uma abordagem ERP para transparência na indústria automotiva. Kuhn et al. (2021) utilizam Ethereum de consórcio, Proof-of-Authority, smart contracts e tokens para representar peças, lotes e estruturas de montagem.

A blockchain também aparece integrada a digital twins, IoT e sistemas de qualidade. Roumeliotis et al. (2024) analisam blockchain e digital twins na Indústria 4.0. Wu et al. (2025) revisam a gestão da qualidade de produtos com blockchain em manufatura inteligente. Yousef et al. (2025) aplicam blockchain a dados de inspeção em fundição. Esses trabalhos mostram que a blockchain atua como camada de registro e auditoria, enquanto sensores, sistemas industriais e mecanismos de identificação continuam responsáveis pela geração e validação inicial dos dados.

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

3. Metodologia

A abordagem metodológica deste trabalho foi organizada em quatro etapas: Rapid Review, definição da arquitetura, desenvolvimento do microsserviço e avaliação experimental. As etapas foram conduzidas de forma sequencial, de modo que os resultados da revisão apoiassem as decisões de projeto.

Inicialmente, foi realizada uma Rapid Review para identificar como blockchain tem sido aplicada à rastreabilidade na manufatura inteligente. Os achados ajudaram a definir as principais características da solução, incluindo o uso de uma rede privada e permissionada, o mecanismo de consenso e o modelo de persistência offline. Em seguida, foram realizadas a modelagem da arquitetura, a implementação do microsserviço e a definição do protocolo experimental utilizado para avaliar a solução, conforme descrito nas subseções seguintes.

3.1. Rapid Review

A revisão foi conduzida como uma Rapid Review, seguindo a perspectiva de Cartaxo, Pinto e Soares [1], que destacam esse tipo de revisão como uma abordagem útil para apoiar a tomada de decisão em contextos práticos de Engenharia de Software. A escolha por uma Rapid Review ocorreu devido à necessidade de obter, em curto prazo, uma visão estruturada sobre o uso de blockchain em processos de rastreabilidade na manufatura, com foco em apoiar decisões técnicas e arquiteturais para uma infraestrutura de rastreabilidade industrial, motivada originalmente por cenários de manufatura eletrônica e linhas SMT.

O objetivo da revisão foi identificar como a blockchain tem sido aplicada em ambientes industriais, especialmente em contextos de Indústria 4.0, manufatura inteligente e rastreabilidade de processos produtivos. De forma mais específica, buscou-se compreender quais problemas são tratados pelas soluções existentes, quais elementos são rastreados, quais tecnologias são integradas à blockchain, quais configurações de blockchain são utilizadas e quais desafios são reportados na literatura.

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

A questão de pesquisa que orientou a revisão foi: Como a blockchain tem sido utilizada para apoiar rastreabilidade, auditabilidade, integridade de dados e registro seguro de eventos em processos de manufatura inteligente?

A busca foi realizada na base Scopus, em 08 de junho de 2026, escolhida por sua cobertura interdisciplinar nas áreas de Computação, Engenharia, Sistemas Industriais e Manufatura. Não foi aplicado recorte temporal à busca, de modo que publicações de qualquer ano poderiam ser recuperadas, desde que atendessem aos demais critérios estabelecidos. A estratégia de busca foi construída a partir de três grupos principais de termos: blockchain, rastreabilidade e contexto industrial/manufatura. A string utilizada foi:

TITLE-ABS-KEY("blockchain" OR "distributed ledger technology" OR DLT OR "smart contract*") AND TITLE-ABS-KEY(traceability OR "product traceability" OR "manufacturing traceability" OR "process traceability") AND TITLE-ABS-KEY("printed circuit board*" OR PCB OR "surface mount technology" OR SMT OR "electronics manufacturing" OR "smart manufacturing")

A busca foi realizada nos campos de título, resumo e palavras-chave. A string combinou termos do contexto da solução, como placas de circuito impresso, SMT e manufatura eletrônica, com termos mais amplos, como *smart manufacturing*, para incluir estudos de rastreabilidade industrial em contextos semelhantes. Foram consideradas publicações científicas revisadas por pares, publicadas em periódicos ou anais de conferências. Nesta seção, o termo “estudo” refere-se a essas publicações, independentemente do veículo. Foram considerados artigos completos revisados por pares publicados em periódicos ou anais de conferências. Trabalhos classificados pela base como workshop, pôster, demonstração, painel ou formatos equivalentes foram excluídos por decisão de escopo da Rapid Review, independentemente de eventual processo editorial próprio desses veículos. Os critérios de inclusão e exclusão são apresentados na Tabela 1.

Critérios de Inclusão

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

CI01	O estudo deve estar no contexto de blockchain ou tecnologias de registro distribuído aplicadas a ambientes industriais, manufatura inteligente, Indústria 4.0 ou manufatura eletrônica.
CI02	O estudo deve propor, aplicar, avaliar ou revisar uma solução, arquitetura, framework, modelo ou mecanismo baseado em blockchain relacionado à rastreabilidade, auditabilidade, integridade de dados, registros imutáveis ou registro seguro de eventos em processos de manufatura.
Critério de Exclusão	
CE01	O estudo não é uma publicação revisada por pares, incluindo prefácio, livro, editorial, dissertação de mestrado, tese, pôster, painel, palestra, mesa-redonda, workshop ou demonstração.
CE02	O estudo não está escrito em inglês.
CE03	O estudo é duplicado.
CE04	O estudo não atende a nenhum dos critérios de inclusão

Tabela 1: Critérios de inclusão e exclusão da rapid review

O processo de seleção foi realizado em duas etapas. Na primeira, os estudos foram avaliados com base em título, resumo e palavras-chave e classificados como incluídos ou excluídos conforme os critérios definidos. Na segunda, os estudos selecionados foram lidos integralmente para verificar sua aderência ao foco da revisão. Foram excluídos trabalhos que tratavam blockchain de forma genérica ou cujo foco principal estava em cadeia de suprimentos, sustentabilidade, decisões gerenciais ou planejamento produtivo, sem relação direta com rastreabilidade, auditabilidade, integridade de dados ou registro seguro de eventos em manufatura inteligente.

A seleção inicial foi realizada por um pesquisador e validada de forma independente por um segundo pesquisador. A extração dos dados também foi conduzida por um pesquisador e posteriormente revisada por outro. Para manter a revisão compatível com seu caráter rápido, foram extraídos apenas campos essenciais: identificação, título, ano, tipo de estudo, contexto industrial, objetivo da solução, objeto rastreado, tecnologias integradas, configuração blockchain, estratégia de armazenamento, forma de validação, principais resultados e desafios ou limitações.

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

Esses campos permitiram comparar os estudos quanto ao tipo de contribuição, contexto de aplicação, objeto rastreado e tecnologias utilizadas. A configuração blockchain reuniu informações sobre plataforma, tipo de rede, mecanismo de consenso e uso de smart contracts. A estratégia de armazenamento identificou abordagens on-chain, off-chain ou híbridas, incluindo uso de hashes e bancos de dados externos.

A síntese foi realizada de forma qualitativa, agrupando os estudos em categorias relacionadas às finalidades da blockchain na manufatura, objetos rastreados, tecnologias integradas, configurações adotadas e desafios reportados. A análise buscou identificar padrões recorrentes e aspectos úteis ao desenvolvimento da solução, sem assumir que a maior frequência de uma tecnologia ou configuração indica superioridade técnica.

3.2. Descrição arquitetural do serviço

A solução foi estruturada como um microsserviço genérico e independente, organizado em três camadas principais (Figura 1): integração, rede descentralizada e persistência. Essa separação permite isolar as responsabilidades do sistema e reduzir o acoplamento com regras de negócio específicas. Diferentes aplicações podem enviar dados para registro auditável, com verificação de integridade e detecção de alterações por meio do encadeamento criptográfico.

A camada de integração expõe os endpoints REST usados por sistemas externos. A camada de rede descentralizada gerencia a comunicação entre os nós validadores, a propagação de transações, a sincronização da cadeia e o consenso. A camada de persistência armazena localmente os blocos, as transações e o estado da cadeia em cada nó. Como o microsserviço é genérico, os dados registrados não seguem um modelo fixo de processo produtivo. Eles podem representar eventos operacionais, medições, identificadores de dispositivos, estados de equipamentos, movimentações de materiais, registros de inspeção e outras informações usadas em rastreabilidade e auditoria.

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

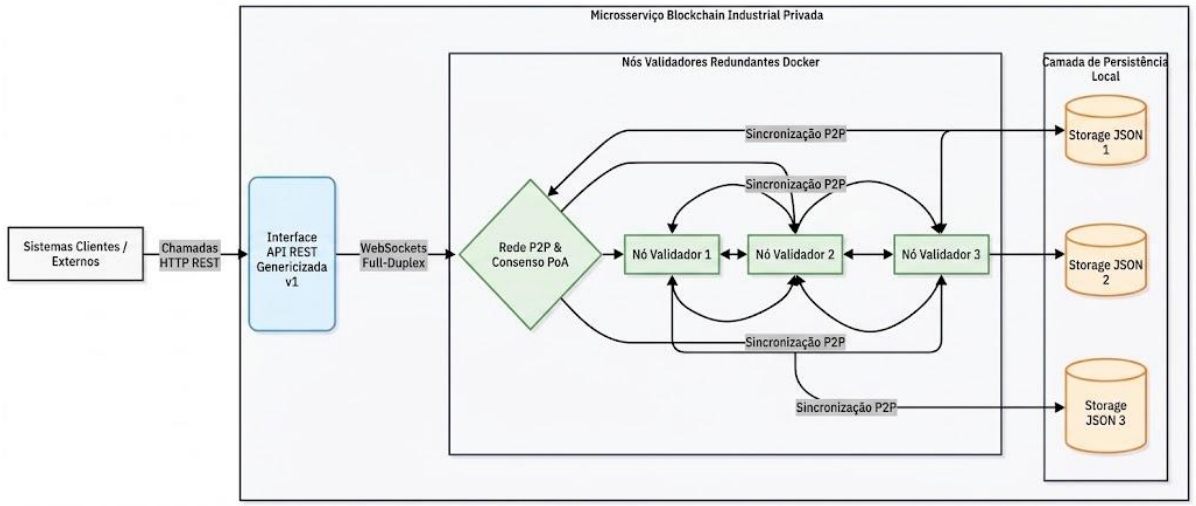

Figura 1: Desenho arquitetural da solução

3.3. Interface API REST genericizada

A camada superior de interface expõe endpoints RESTful padronizados, desenvolvidos com ASP.NET Core sob o framework .NET 8.0. Essa especificação agnóstica viabiliza que múltiplos sistemas externos interajam com o ecossistema distribuído por meio de chamadas HTTP tradicionais. As operações expostas cobrem a gravação de dados, a checagem de integridade, a recuperação de históricos, a validação da cadeia e o monitoramento dos nós. As principais rotas programáticas implementadas para a integração do serviço genérico estão descritas na Tabela 2.

Método	Endpoint	Descrição
POST	/api/v1/blockchain/record	Registrar dados estruturados e eventos operacionais no barramento de persistência.
POST	/api/v1/blockchain/verify	Verificar a integridade criptográfica de um registro de dados específico e detectar eventuais alterações.
GET	/api/v1/blockchain/history/{identifier}	Recuperar o histórico completo associado a um identificador genérico ou código de dispositivo.
GET	/api/v1/blockchain/chain	Obter a estrutura completa e a sequência de blocos que compõem a blockchain.
POST	/api/v1/blockchain/validate	Validar a integridade matemática e criptográfica de toda a cadeia local.

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

Método	Endpoint	Descrição
GET	/api/v1/node/health	Executar o health check para checagem de disponibilidade e status do nó ativo.
GET	/api/v1/node/peers	Listar os nós adjacentes e pares conectados à rede descentralizada.

Tabela 2: Principais endpoints da API REST do microsserviço.

A adoção de uma API REST genericizada permite que o serviço seja integrado a sistemas industriais existentes sem exigir alterações profundas em sua lógica interna. Dessa forma, a blockchain atua como uma camada de registro e auditoria, mantendo independência em relação às regras específicas de cada aplicação consumidora.

A implementação atual opera em rede local isolada (air-gapped), sem exposição à internet pública. Esse isolamento reduz a superfície de exposição externa, mas não constitui, por si só, um mecanismo de autenticação criptográfica. A versão experimental não implementa autenticação por JWT/API Key, assinatura criptográfica individual dos blocos ou autenticação criptográfica dos peers. O modelo de dados prevê campo destinado à assinatura digital de transações e a configuração contempla parâmetros para futura ativação de autenticação e criptografia. A validação dos dados submetidos inclui verificação dos campos obrigatórios e restrições temporais, enquanto mecanismos adicionais de autenticação, autorização e proteção do canal são previstos como evolução da arquitetura.

3.4. Camada de rede P2P e mensageria

A comunicação entre os nós validadores ocorre de forma descentralizada por uma rede P2P baseada em WebSockets, permitindo a troca assíncrona de mensagens na rede local, com operação offline e sem dependência da internet pública. O protocolo gerencia a descoberta de pares, a propagação de transações e blocos e a sincronização da cadeia; os tipos de mensagens implementados são apresentados na Tabela 3.

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

A comunicação P2P é executada em uma rede Docker isolada e não utiliza TLS (WSS), decisão adotada para o ambiente experimental controlado, mas que representa uma limitação da solução. Como evolução, prevê-se o uso de TLS mútuo (mTLS) para autenticação dos nós e proteção do canal.

O mecanismo de consenso é inspirado em Proof-of-Authority (PoA), com validadores previamente autorizados na rede local e escolha do produtor do bloco por rotação determinística em round-robin, sem competição entre os nós. O termo "inspirado em PoA" se justifica porque o protótipo não implementa todos os mecanismos de soluções PoA completas, como assinatura criptográfica dos blocos e autenticação dos validadores por certificados. Mantém-se ainda um cálculo auxiliar de nonce na formação do bloco, que não interfere na escolha do produtor nem na autoridade do validador.

ID	Mensagem	Descrição
1	NEW_BLOCK	Propagar um novo bloco criado e validado pelo protocolo de consenso aos demais nós da rede.
2	NEW_TRANSACTION	Propagar uma nova transação pendente para compor o pool de validação dos pares.
3	REQUEST_CHAIN	Solicitar a cópia integral da blockchain para um dos pares conectados na malha.
4	CHAIN_RESPONSE	Enviar a blockchain solicitada para fins de alinhamento e atualização de estado.
5	SYNC_REQUEST	Executar uma solicitação de sincronização incremental entre nós desatualizados.
6	PEER_DISCOVERY	Localizar e estabelecer comunicação com peers pertencentes ao conjunto previamente configurado de participantes autorizados. A descoberta não implica autorização automática de novos validadores.

Tabela 3: Tipos de mensagens implementadas no protocolo P2P.

A descoberta de peers deve ser distinguida da autorização para participar do consenso. O mecanismo de descoberta apenas auxilia o estabelecimento de comunicação entre os nós; a aceitação de um participante como validador permanece condicionada à lista previamente configurada. Na implementação experimental, entretanto, essa identidade não é vinculada criptograficamente ao peer

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

por certificados ou chaves individuais, limitação considerada no modelo de ameaças.

3.4.1 Resolução de Forks (Bifurcações de Cadeia) Embora a criação de blocos seja atribuída a um único validador por rodada, bifurcações temporárias ainda podem ocorrer por falhas transitórias de comunicação, diferenças de relógio ou reintegração de nós, associando blocos distintos ao mesmo índice. O protocolo P2P trata a situação em quatro etapas: detecção, sincronização, seleção da cadeia canônica e persistência do estado resolvido. A detecção ocorre quando um nó recebe uma mensagem NEW_BLOCK com o mesmo índice do último bloco local, porém com hash diferente; nesse caso, interrompe a anexação direta e envia REQUEST_CHAIN ao par de origem, que responde com CHAIN_RESPONSE contendo sua cadeia completa, permitindo comparar as ramificações antes da seleção.

O critério de seleção prioriza o comprimento: a ramificação recebida é considerada canônica quando possui mais blocos válidos que a local. Em caso de empate, utiliza-se o carimbo temporal do bloco conflitante, prevalecendo o de menor valor, isto é, o proposto primeiro. Esse critério secundário é determinístico e simétrico, assegurando que todos os nós cheguem ao mesmo resultado ao avaliar o mesmo par de ramificações, o que impede oscilações sucessivas entre ramos concorrentes.

Definida a cadeia canônica, o nó preterido substitui integralmente sua estrutura local e persiste o novo estado em armazenamento não volátil, de modo que a resolução sobreviva a reinicializações do processo. O bloco descartado não é reincorporado à cadeia; suas transações ausentes da ramificação canônica permanecem elegíveis ao pool de pendências para inclusão em blocos subsequentes, e todos os nós convergem para uma única sequência.

O mecanismo é funcionalmente equivalente à regra da cadeia mais longa (longest chain rule), adaptada ao contexto permissionado desta arquitetura. A diferença conceitual está no significado do comprimento: em redes públicas baseadas em prova de trabalho, a altura funciona como proxy do esforço computacional acumulado; aqui, expressa o número de blocos

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

validados por nós previamente autorizados, de modo que reescrever o histórico exigiria o controle de identidades autorizadas, e não apenas capacidade computacional. Soma-se a isso a comunicação em canal full-duplex sobre a rede local, cuja baixa latência de propagação restringe a janela temporal de formação de bifurcações e limita sua profundidade típica a poucos blocos.

3.4.2 Protocolo de consenso e seleção de validadores

O mecanismo de consenso é inspirado em Proof-of-Authority (PoA) e foi adaptado a uma rede privada, permissionada e offline, com validadores previamente conhecidos e autorizados. A seleção do produtor do bloco ocorre por rotação determinística em round-robin, evitando competição entre os nós. A concordância sobre o estado da cadeia não depende apenas dessa rotação, mas da validação independente dos blocos, da propagação e sincronização P2P e, em caso de bifurcação, da aplicação de um critério determinístico para escolha da cadeia canônica.

As transações recebidas pela API são propagadas pela rede e mantidas como pendentes. Quando chega sua vez, o validador reúne as transações elegíveis, cria o bloco, associa-o ao bloco anterior e calcula seu hash com SHA-256. O bloco é então enviado aos demais nós pela mensagem NEW_BLOCK. Cada nó verifica a autorização do validador, a continuidade do índice, o hash do bloco anterior e a integridade criptográfica antes de incorporá-lo à cadeia. Blocos inválidos são rejeitados.

A aceitação do bloco não depende de votação ou quórum adicional. Cada nó realiza a validação de forma independente e persiste o bloco quando as condições são atendidas. Caso um nó fique temporariamente indisponível, ele pode recuperar o estado atual da cadeia por meio do mecanismo de sincronização P2P ao retornar à rede.

Quando existem cadeias válidas concorrentes, a arquitetura seleciona como canônica aquela com maior número de blocos. Em caso de empate,

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

prevalece a cadeia cujo bloco conflitante possui menor carimbo temporal. A implementação também mantém um cálculo auxiliar de nonce, mas esse valor não participa da escolha do produtor nem da definição de sua autoridade. Detalhes em nível de código não são apresentados devido às restrições de propriedade intelectual e confidencialidade do projeto industrial.

3.5. Modelo de dados e persistência

O modelo de dados do serviço define a anatomia estrutural dos elementos armazenados na cadeia. Cada bloco funciona como um contêiner de auditoria e possui metadados rígidos, incluindo índice posicional na cadeia, carimbo de data e hora, endereço do nó validador, contador de controle e lista de transações integradas.

A segurança estrutural é garantida pelos campos de hash atual e hash do bloco anterior, calculados de forma encadeada por meio do algoritmo SHA-256. A estrutura lógica de um bloco é apresentada a seguir:

```
Block {
  "index": 0,
  "timestamp": "2026-06-08T11:12:21Z",
  "transactions": [],
  "previousHash": "string",
  "hash": "string",
  "validator": "string",
  "nonce": 0
}
```

O campo nonce do bloco é utilizado como variável do cálculo de hash durante sua formação, permitindo variar a entrada do SHA-256 até que seja satisfeita a dificuldade configurada no protótipo. Esse mecanismo é auxiliar à formação do bloco e não participa da seleção do validador, que é determinada pela rotação entre os nós previamente autorizados. A prevenção de replay de transações é tratada separadamente por meio da identificação única das transações e das verificações de duplicidade realizadas pela aplicação.

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

As transações são encapsuladas dentro dos blocos e registram as operações de forma detalhada. A estrutura de dados de uma transação individual segue a formatação de atributos agnósticos listada abaixo:

```
Transaction  {
  "transactionId": "string",
  "timestamp": "2026-06-08T11:12:21Z",
  "processId": "string",
  "equipmentCode": "string",
  "status": "string",
  "data": {}
}
```

O objeto interno Data foi projetado de forma abstrata para abrigar as variáveis de estado de diferentes processos industriais. Campos como identificadores de processos, códigos de equipamentos, status operacionais e coleções genéricas de métricas podem ser representados nesse objeto, permitindo o rastreamento flexível de atividades fabris.

A camada de persistência, situada na base da arquitetura, utiliza armazenamento local baseado em arquivos estruturados no formato JSON. Cada nó validador mantém uma cópia independente do estado da cadeia em seu armazenamento local. Essa redundância contribui para a disponibilidade do serviço e para a tolerância a falhas na rede local.

A opção por persistência local em JSON foi adotada em função do caráter experimental da solução e da necessidade de operação offline. Essa escolha permite validar os mecanismos de registro, sincronização e verificação criptográfica sem depender de serviços externos de banco de dados ou infraestrutura em nuvem.

3.6. Protocolo de implementação e ambiente de testes

Para validar a arquitetura proposta e fornecer subsídio à etapa de avaliação experimental, o microsserviço foi containerizado com a tecnologia Docker. Por meio do utilitário Docker Compose, estruturou-se um ambiente capaz de instanciar de forma coordenada os nós validadores independentes, assegurando isolamento de recursos e reprodutibilidade da configuração entre execuções.

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

O ambiente laboratorial foi composto por três nós validadores executados em contêineres sobre um único host físico, organizados em topologia full mesh e interconectados por uma rede virtual do tipo bridge. Cada nó recebeu alocação restrita de recursos computacionais, de modo a reproduzir condições de operação em infraestrutura local de pequeno porte, ressaltamos que a alocação não equivale à medição de consumo. O ambiente experimental foi configurado conforme as especificações técnicas apresentadas na tabela 4.

Componente	Especificação
Sistema Operacional host	Ubuntu 22.04.4 LTS (Jammy Jellyfish)
Imagem base dos contêineres	mcr.microsoft.com/dotnet/aspnet:8.0 (Debian 12 Bookworm)
Runtime	.NET 8.0.11
SDK de build	.NET SDK 8.0
Memória alocada por nó	4 GB RAM
CPU alocada por nó	2 vCPUs (Intel Xeon E5-2686 v4 @ 2.30 GHz)
Docker Engine	versão 25.0.3
Docker Compose	versão 2.24.5
Rede virtual	Docker bridge network, sub-rede 192.168.1.0/24
Latência de rede entre contêineres	< 0,5 ms
Número de nós validadores	3 (topologia full-mesh via TCP/WebSockets)
Hardware do host físico	Intel Xeon E5-2686 v4, 8 vCPUs, 32 GB RAM, SSD NVMe
Protocolo P2P	TCP com mensagens JSON serializadas (buffer 4096 bytes)
Healthcheck	HTTP GET /api/node/health a cada 30s

Tabela 4: Ambiente experimental configurado

3.7 Propriedades de Segurança

A arquitetura foi projetada para atender a propriedades de segurança derivadas dos requisitos de rastreabilidade laboratorial. Diferentemente de blockchains públicas, cujo modelo de ameaça pressupõe adversários anônimos e economicamente motivados, o contexto é o de uma rede permissionada, em ambiente controlado e com participantes previamente conhecidos. A ênfase recai sobre integridade, auditabilidade e não-repúdio dos registros, e não sobre resistência

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

à censura ou a ataques Sybil. A Tabela 5 sintetiza as propriedades, os mecanismos que as implementam e os procedimentos de verificação.

Propriedade	Mecanismo implementado	Verificação
Integridade verificável	Hash encadeado SHA-256 por bloco (CalculateHash)	Testes TA-01 e TA-02
Auditabilidade	Cadeia com índice, timestamp e validador; API REST de consulta	Recuperação de histórico por testId e barcode
Consistência entre réplicas	Sincronização P2P via SYNC_REQUEST / CHAIN_RESPONSE	Teste de queda e reintegração de nó
Controle de acesso	Lista de validadores pré-configurada (PoA)	Teste TA-03
Disponibilidade local	Persistência local JSON; rede Gigabit local; 3 réplicas	Ensaios com 100.000 transações
Resistência a fork	Protocolo de resolução de conflito P2P (longest chain)	Teste TA-04
Não-duplicação	Verificação de transaction.Id único (UUID)	Teste TA-05

Tabela 5: Propriedades de segurança e sua implementação.

A integridade verificável decorre do encadeamento criptográfico: cada bloco armazena o hash do anterior, calculado com SHA-256 a partir de seus dados, de modo que qualquer alteração invalida o hash e rompe a sequência, situação detectada pelas rotinas de validação e avaliada nos testes TA-01 e TA-02. A não duplicação é garantida pelo UUID de cada transação, cujo transaction.Id é comparado com os registros existentes antes da inclusão em bloco, rejeitando reinserções, conforme o teste TA-05.

A auditabilidade é apoiada pelos metadados de cada bloco, como índice, timestamp e identificação do validador, e pela API REST, que permite consultar o histórico por identificadores da aplicação sem acesso direto aos arquivos de persistência. A sincronização P2P mantém a consistência entre réplicas e permite que nós reintegrados recuperem a cadeia atual; havendo bifurcação, aplica-se a regra determinística de seleção da cadeia canônica, avaliada no teste TA-04.

O controle de acesso baseia-se em lista pré-configurada de validadores: apenas nós autorizados podem propor blocos, e propostas de participantes não autorizados são rejeitadas, conforme o teste TA-03. A persistência local em cada nó permite que a rede siga operando durante indisponibilidades temporárias de um participante.

Essas propriedades têm limitações. A integridade garante a detecção de alterações após o registro, mas não assegura a veracidade do dado

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

original: um dado incorreto vindo de fonte autorizada é armazenado de forma íntegra, e a correção deve ocorrer por novo registro, preservando o histórico. A arquitetura também não oferece tolerância a validadores maliciosos em conluio nem reivindica tolerância a falhas bizantinas, permanecendo a confiança no conjunto de participantes autorizados.

A confidencialidade igualmente não é garantida pela blockchain, pois os dados são replicados entre os nós. Em cenários com informações sensíveis, recomenda-se manter o conteúdo em repositórios externos protegidos e registrar na cadeia apenas identificadores e hashes necessários à verificação.

3.8 Modelo de falhas e ameaças

O modelo de ameaça considera uma rede privada e permissionada, desconectada da internet e operando em ambiente fabril controlado. Com isso, o foco deixa de ser o adversário externo anônimo, comum em blockchains públicas, e passa a ser um agente interno com acesso legítimo à planta ou à infraestrutura de rede. Assume-se que esse adversário possa acessar e alterar os arquivos de persistência de um ou mais nós, além de interceptar e forjar mensagens na rede P2P local.

Por outro lado, assume-se que o adversário não consiga comprometer simultaneamente a maioria dos validadores, condição expressa por $f<\lfloor |V|/2 \rfloor+1$, em que f representa o número de nós comprometidos e V o conjunto de validadores autorizados. Essa premissa limita o alcance do modelo de ameaça e permite definir quais garantias podem ser avaliadas. A Tabela 6 relaciona as ameaças consideradas às contramedidas implementadas.

ID	Categoria	Descrição	Contramedida
A1	Adulteração de dados	Modificação direta dos arquivos JSON de persistência	Verificação encadeada SHA-256; ValidateChain() detecta quebra de integridade
A2	Injeção de bloco forjado	Submissão de bloco por nó não autorizado	ValidateBlock() verifica block.Validator ∈ V
A3	Fork (bifurcação)	Indução de cadeias concorrentes	Protocolo de resolução via SYNC_REQUEST / ChainResponse
A4	Replay attack	Reenvio de transação já registrada	AddTransactionAsync rejeita transaction.Id duplicado

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

A5	DoS local	Sobrecarga de nó validador	Conexões TCP com timeout de 5s; buffer de 4096 bytes; retry com backoff exponencial

Tabela 6: Ameaças modeladas e contramedidas implementadas.

A ameaça A1 representa a edição direta dos registros persistidos por um adversário com acesso ao sistema de arquivos. A alteração não é impedida, mas pode ser detectada por ValidateChain(), que recalcula os hashes e identifica a quebra do encadeamento. Na sincronização seguinte, a cadeia divergente pode ser substituída pela cadeia válida dos demais nós. A ameaça A2 considera a emissão de mensagens por um nó não autorizado. Nesse caso, ValidateBlock() verifica se block.Validator pertence à lista de validadores configurados e rejeita propostas externas. Essa proteção, porém, depende da forma como a identidade declarada é vinculada ao nó emissor.

As ameaças A3 e A4 atuam sobre o protocolo. A3 envolve a criação de cadeias concorrentes por partições ou entrega seletiva de blocos, situação tratada pela sincronização e pela seleção determinística da cadeia canônica. A4 corresponde ao reenvio de uma transação já registrada, rejeitada por AddTransactionAsync antes da inclusão em bloco. Já a ameaça A5 está relacionada à disponibilidade. Timeout nas conexões, buffer limitado e política de retry com backoff exponencial ajudam a conter os efeitos de falhas ou sobrecarga e permitem que os nós não afetados continuem operando.

Alguns ataques permanecem fora do escopo. A solução não protege contra adulteração dos dados antes de sua entrada na blockchain, como em sensores ou CLPs comprometidos, nem contra o comprometimento da maioria dos validadores. Ataques externos pela internet também não foram considerados, pois a arquitetura foi avaliada em uma rede offline. Assim, a solução oferece mecanismos de integridade e rastreabilidade a partir do momento em que o dado é registrado, enquanto a confiabilidade da informação antes desse ponto depende de controles externos. Como evolução, assinaturas digitais na origem podem ampliar a verificação de autoria e integridade dos dados.

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

4. Resultados e Discussão

Esta seção apresenta os resultados da Rapid Review e da validação experimental do microsserviço proposto. Primeiro, são descritos o processo de seleção dos estudos e os principais achados da literatura. Em seguida, são apresentados os resultados obtidos nos testes de desempenho, escalabilidade e segurança criptográfica.

4.1. Resultados da Rapid Review

A busca na Scopus retornou 68 estudos. O primeiro filtro foi realizado por meio da análise de título, resumo e palavras-chave. Nessa etapa, 43 estudos foram incluídos e 25 foram excluídos. No segundo filtro, os estudos selecionados foram avaliados por meio da leitura completa do artigo. Após essa etapa, 23 estudos foram incluídos para extração e síntese. Dos 20 estudos excluídos nessa etapa, 17 foram excluídos por baixa aderência ao foco da revisão e 3 foram excluídos por indisponibilidade do texto completo.

Os estudos selecionados apresentam diferentes tipos de contribuições. Foram identificadas revisões, frameworks conceituais, protótipos, experimentos e estudos aplicados. Essa variedade indica que o tema ainda reúne contribuições teóricas e propostas técnicas em validação. A Tabela 7 apresenta a caracterização dos estudos selecionados.

ID	Título	Tipo de estudo	Contexto industrial	Foco principal
E01	*Applying Blockchain in Industry 4.0 Applications*	Proposta conceitual	Indústria 4.0 e smart manufacturing	Segurança, confiança e rastreabilidade industrial
E02	*Designing an Experimental Setup for Data Provenance Tracking using a Public Blockchain*	Experimento / estudo de caso	Planta de envase de água	Proveniência de dados com blockchain pública

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

ID	Título	Tipo de estudo	Contexto industrial	Foco principal
E03	*Blockchain applications in PLM towards smart manufacturing*	Revisão / framework	PLM e smart manufacturing	Blockchain no ciclo de vida do produto
E04	*Blockchain-integrated IoT device for advanced inspection of casting defects*	Protótipo / experimento	Inspeção de fundição	Inspeção de defeitos com IoT, IA e blockchain
E05	*A Review of Blockchained Product Quality Management Towards Smart Manufacturing*	Revisão sistemática	Gestão da qualidade	Gestão confiável de dados de qualidade
E06	*Design and Application of an Intelligent Inspection and Product Quality Data Traceability System*	Protótipo / aplicação experimental	Manufatura verde e inteligente	Inspeção e rastreabilidade de dados de qualidade
E07	*Hierarchical Blockchain for Mapping Manufacturing Process Flow*	Framework / experimento	Fluxo de manufatura	Registro de eventos produtivos
E08	*A Comprehensive Review of Blockchain Technology-Enabled Smart Manufacturing*	Revisão	Smart manufacturing	Segurança, confiança, dados e coordenação
E09	*Virtual reality integration and credible traceability management method of transformer coil manufacturing process based on industrial internet and digital twin*	Método / experimento	Bobinas de transformadores	Rastreabilidade com blockchain e digital twin
E10	*Smart manufacturing supply chain process strategy using intelligent computation techniques*	Framework / estudo aplicado	Smart manufacturing e supply chain	Rastreabilidade de produtos com IoT, ML e blockchain
E11	*Research on Robot Assembly Traceability System based on Fabric*	Protótipo / implementação	Montagem de robôs	Rastreabilidade com Hyperledger Fabric
E12	*Blockchain-based application for the traceability of complex assembly structures*	Aplicação / protótipo	Montagem complexa	Rastreabilidade de peças, lotes e estruturas

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

ID	Título	Tipo de estudo	Contexto industrial	Foco principal
E13	*Industry 4.0 Innovation: A Systematic Literature Review on the Role of Blockchain Technology in Creating Smart and Sustainable Manufacturing Facilities*	Revisão sistemática	Manufatura inteligente e sustentável	Blockchain em instalações industriais
E14	*Blockchain-Enabled Open Quality System for Smart Manufacturing*	Revisão / framework	Gestão da qualidade	Qualidade aberta com blockchain
E15	*Application of thermal energy efficiency utilization based on computer technology in green manufacturing blockchain production traceability*	Sistema / estudo aplicado	Manufatura verde	Rastreabilidade de dados térmicos
E16	*Blockchain for smart manufacturing systems: a survey*	Survey / revisão	Sistemas de manufatura inteligente	Blockchain no ciclo de vida do produto
E17	*Enhancing Supply Chain Transparency in the Automotive Industry: A Blockchain-Based ERP System Approach*	Protótipo / framework	Manufatura automotiva e ERP	ERP baseado em blockchain
E18	*Traceable and Intelligent Supply Chain based on Blockchain and AI*	Metodologia / framework	Smart manufacturing e supply chain	Cadeia rastreável e inteligente
E19	*New Framework for Complex Assembly Digitalization and Traceability...*	Framework	Montagem complexa	Bill of Assembly e smart contracts
E20	*Blockchain Solutions for Enhancing Security and Privacy in Industrial IoT*	Framework / avaliação	IIoT e smart factories	Segurança, privacidade e integridade
E21	*Blockchain and Digital Twins in Smart Industry 4.0*	Revisão	Digital twins e supply chain	Integração entre blockchain e digital twins

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

ID	Título	Tipo de estudo	Contexto industrial	Foco principal
E22	*Enhancing Distributed Security and Reliability in Semiconductor Supply Chains...*	Framework	Semicondutores	Rastreabilidade química e conformidade
E23	*Framework for Block-Chain Deployment in Assembly of an Air-Craft or a Space-Craft*	Framework	Montagem aeroespacial	Documentação segura e rastreável de montagem

Tabela 7: Caracterização geral dos estudos selecionados.

Os estudos analisados mostram que a blockchain tem sido utilizada como camada de confiança em ambientes industriais. Seu papel principal é registrar dados, eventos e evidências de forma imutável e auditável.

Os objetos rastreados variam entre os estudos. Foram identificados produtos, peças, lotes, eventos produtivos, dados de inspeção, documentos técnicos e recursos de produção. Essa variação indica que a rastreabilidade industrial não se limita ao produto final. Ela também envolve processos, operações, medições e associações entre entidades físicas. A Tabela 8 resume os principais elementos rastreados.

Objeto rastreado	Estudos relacionados	Exemplos de aplicação
Produto ou item final	E02, E10, E13, E16, E18	Histórico do produto e informações de produção
Peças e componentes	E11, E12, E19, E22, E23	Partes, componentes, materiais e submontagens
Lotes e batches	E12, E16, E18	Representação de lotes e grupos de produção
Eventos produtivos	E01, E07, E09, E20	Operações, estados e fluxo produtivo

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

Objeto rastreado	Estudos relacionados	Exemplos de aplicação
Dados de inspeção	E04, E05, E06, E14	Defeitos, medições e resultados de qualidade
Documentos técnicos	E03, E19, E21, E23	BOA, BOM, registros de PLM e logs
Recursos produtivos	E09, E19, E23	Máquinas, operadores, sensores e estações

Tabela 8: Objetos rastreados nos estudos selecionados.

A blockchain apareceu frequentemente combinada com outras tecnologias da Indústria 4.0. As integrações mais recorrentes envolvem IoT, sensores, inteligência artificial, digital twin, ERP, RFID, QR Code, oráculos e smart contracts. A Tabela 9 sintetiza essas integrações.

Tecnologia integrada	Estudos relacionados	Papel na solução
IoT e sensores	E04, E06, E10, E15, E20	Coleta automática de dados industriais
Inteligência artificial / machine learning	E04, E06, E10, E18	Inspeção, predição, classificação e apoio à decisão
Digital twin	E07, E09, E19, E21, E23	Representação virtual do produto ou processo
ERP / PLM	E03, E17, E19	Integração com sistemas de gestão industrial
RFID / QR Code / identificação	E02, E09, E23	Identificação de produtos, partes ou recursos
Oráculos	E09	Envio confiável de dados externos para a blockchain

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

Tecnologia integrada	Estudos relacionados	Papel na solução
Smart contracts	E02, E11, E12, E17, E19, E22, E23	Automação de validações, registros e regras
Edge computing	E20	Apoio à segurança e processamento em IIoT

Tabela 9: Tecnologias integradas à blockchain.

A análise também identificou diferentes configurações de blockchain. Alguns estudos detalham plataforma, tipo de rede e consenso. Outros discutem a tecnologia apenas em nível conceitual. A Tabela 10 apresenta as configurações mais relevantes.

Configuração blockchain	Estudos relacionados	Observação
Hyperledger Fabric	E11, E17	Usada em cenários permissionados e industriais
Ethereum de consórcio	E12	Associada a Proof of Authority e smart contracts
Blockchain pública	E02	Usada para proveniência de dados
Blockchain de consórcio	E06, E12	Aplicada quando há participantes conhecidos
Blockchain privada ou permissionada	E11, E17, E20	Alinhada a ambientes industriais controlados
Proof of Authority	E12	Usado para validação em rede de consórcio
Smart contracts	E02, E11, E12, E17, E19, E22, E23	Usados para registro, validação e automação
Tokens / NFTs / ERC-1155	E09, E12	Usados para representar ativos físicos ou digitais
Não informado ou conceitual	E01, E03, E05, E08, E13, E14, E16, E18, E21	Não há detalhamento técnico da configuração

Tabela 10: Configurações blockchain identificadas.

Entre os estudos que detalham explicitamente a configuração da blockchain, foram identificadas redes públicas, privadas, permissionadas e de

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

consórcio. Redes privadas, permissionadas ou de consórcio aparecem em diferentes aplicações do corpus, especialmente em cenários industriais com participantes conhecidos. Esses resultados mostram a utilização dessas configurações nos estudos analisados, mas não permitem concluir que sejam tecnicamente superiores a outras alternativas.

O uso de smart contracts também aparece de forma recorrente. Eles são usados para automatizar validações, registrar transações, representar regras de montagem e apoiar conformidade. As estratégias de armazenamento também variam entre os estudos. Foram identificados registros on-chain, abordagens híbridas e combinações com bancos de dados ou sistemas externos. A Tabela 11 apresenta essas estratégias.

Estratégia de armazenamento	Estudos relacionados	Característica
Registro on-chain de eventos	E02, E11, E12, E17	Eventos e transações registrados na cadeia
Armazenamento híbrido	E06, E07, E09, E21	Blockchain registra evidências, hashes ou eventos centrais
Blockchain associada a banco de dados	E11, E17	Dados operacionais sincronizados com sistemas externos
Blockchain associada a digital twin	E07, E09, E21	Cadeia mantém histórico confiável para o modelo virtual

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

Estratégia de armazenamento	Estudos relacionados	Característica
Não detalhado	E01, E03, E05, E08, E10, E13, E14, E15, E16, E18, E19, E20, E22, E23	O modelo não é especificado claramente

Tabela 11: Estratégias de armazenamento identificadas.

As estratégias híbridas indicam preocupação com volume de dados, custo e desempenho. Em ambientes industriais, nem sempre é adequado registrar todos os dados diretamente na blockchain. Os desafios reportados foram agrupados em categorias. A Tabela 12 apresenta os principais desafios observados.

Desafio	Estudos relacionados	Implicação
Escalabilidade	E04, E05, E08, E13, E20, E21	Alto volume de eventos pode afetar desempenho
Custo computacional	E05, E08, E13, E15, E20	A infraestrutura pode elevar custos
Latência	E07, E12, E17, E20	Processos em tempo real exigem baixa demora
Interoperabilidade	E03, E05, E08, E17, E20, E21	Integração com sistemas legados ainda é um obstáculo
Privacidade e controle de acesso	E03, E17, E20, E21, E22	Dados industriais podem ser sensíveis
Qualidade da entrada de dados	E02, E09, E14, E20	Blockchain não garante que o dado original seja correto
Armazenamento de dados grandes	E06, E07, E09, E21	Dados de sensores podem exigir armazenamento externo
Padronização	E05, E08, E13, E21	Falta de padrões dificulta adoção ampla

Tabela 12: Desafios e limitações identificados.

Um ponto recorrente é que a blockchain garante a integridade verificável após o registro. Porém, ela não garante sozinha a confiabilidade da coleta inicial. Por isso, vários estudos integram sensores, IoT, oráculos, identificação digital ou sistemas industriais.

4.2. Resultados experimentais

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

4.2.1 Avaliação experimental dos mecanismos de segurança

Os parâmetros utilizados na avaliação experimental são apresentados na Tabela 13, incluindo o número de nós validadores, o total de transações submetidas, a quantidade de transações por bloco, o nível de concorrência, a taxa de injeção de carga, a duração dos testes e demais configurações do ambiente. Com base nesse protocolo, a integridade da rede foi verificada por testes de adulteração deliberada, nos quais o estado da blockchain ou o fluxo de submissão foram modificados para avaliar a resposta dos mecanismos de validação. Cada cenário representou uma ameaça ao modelo de confiança, com resultado esperado definido previamente; a Tabela 14 apresenta os cenários, métodos e resultados observados.

Parâmetro	Valor
Número de nós validadores	3
Total de transações submetidas	100.000
Total de blocos gerados	10.000
Transações por bloco (configurado)	10 (MaxTransactionsPerBlock)
Requisições concorrentes	100
Taxa de injeção de carga	~1.150 req/s (medida)
Duração total do teste de carga	~87 segundos
Tamanho médio do payload por transação	~480 bytes (JSON com TestResultData)
Ferramenta de geração de carga	Script Python assíncrono com aiohttp (TCPConnector, 100 conexões simultâneas)
Timeout por requisição	10 segundos
Número de repetições do teste	3 execuções (valores reportados: média das 3 rodadas)
Algoritmo de hash	SHA-256 (System.Security.Cryptography)
Dificuldade do cálculo auxiliar do bloco	2 (prefixo "00" no hash)
BlockTime configurado	5.000 ms
Protocolo de comunicação P2P	TCP com serialização JSON (System.Text.Json)

Tabela 13: Parâmetros do protocolo de benchmark

Os cenários TA-01 e TA-02 alteraram diretamente o arquivo JSON de persistência local: a modificação do campo datainvalidou o hash

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

SHA-256 do bloco, detectada por ValidateChain(), enquanto a alteração do previousHash rompeu o encadeamento entre blocos, identificada por ValidateBlock(). Já o TA-03 submeteu um bloco com validador não autorizado, e a rejeição evidenciou que a aceitação do bloco depende tanto da integridade criptográfica quanto da autorização do participante.

No TA-04, blocos conflitantes submetidos em dois nós geraram cadeias concorrentes; o protocolo acionou a sincronização, selecionou a cadeia canônica conforme o critério definido e realinhou o nó divergente. O TA-05 reenviou uma transação já registrada, rejeitada por AddTransactionAsync antes da inclusão em bloco, confirmando o controle de unicidade na mempool. Nos cinco cenários os resultados corresponderam aos esperados, indicando que integridade, autorização, sincronização e unicidade funcionaram conforme especificado.

ID	Cenário	Método	Resultado esperado	Resultado observado	Detectado?
TA-01	Modificação do campo data em bloco persistido	Edição direta do arquivo JSON de persistência local	Quebra do hash SHA-256	ValidateChain() retornou false; log: "Block N is invalid"	Sim
TA-02	Modificação do previousHash de um bloco	Edição direta do arquivo JSON	Ruptura do encadeamento	ValidateBlock() detectou inconsistência: "Block N has invalid previous hash"	Sim
TA-03	Injeção de bloco por nó não autorizado	Submissão via API com Validator fora da lista	Rejeição pelo validador	ValidateBlock() retornou false: "validated by unauthorized validator"	Sim
TA-04	Indução de fork	Submissão paralela de blocos conflitantes em 2 nós	Resolução via protocolo P2P	SYNC_REQUEST disparado; cadeia mais longa prevaleceu; nó divergente realinhou	Sim
TA-05	Replay de transação	Reenvio de payload com mesmo transaction.Id	Transação duplicada rejeitada	AddTransactionAsync retornou false: "Transaction already exists"	Sim

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

Tabela 14: Matriz dos testes de adulteração e resultados

4.2.3 Distribuição estatística da latência de processamento

A latência de processamento foi caracterizada por sua distribuição completa, e não apenas por medidas de tendência central, uma vez que sistemas de registro sujeitos a requisitos de tempo quase real são avaliados sobretudo pelo comportamento de suas caudas superiores. A métrica foi definida como o intervalo entre a submissão da transação ao endpoint REST POST /api/blockchain/record-test e a confirmação de resposta HTTP 200 pelo nó receptor, medida no lado do cliente e agregada sobre as três rodadas de execução.

A mediana de 4,2 ms indica que metade das transações foi processada abaixo desse valor. Os percentis P90 e P95 foram de 7,8 ms e 8,9 ms, permanecendo abaixo do limite de 10 ms adotado como referência. O P99 foi de 11,3 ms e o valor máximo de 18,7 ms. Esses resultados indicam baixa latência na maior parte das requisições, com aumento restrito à cauda da distribuição.

O desvio padrão de 2,1 ms indica dispersão moderada. Nenhuma requisição se aproximou do timeout de dez segundos, o que mostra que a rede operou de forma estável sob a carga aplicada. Os maiores tempos podem estar relacionados à coincidência entre a chegada de uma requisição e a formação de um novo bloco, etapa que envolve construção, cálculo auxiliar do nonce, geração do hash, persistência e propagação.

A validação foi realizada em ambiente controlado, com três nós Linux executados em contêineres Docker sobre um único host físico, orquestrados por Docker Compose e com runtime .NET 8.0. Cada validador recebeu 4 GB de RAM. Sob carga sustentada, o throughput superou 1.000 transações por segundo, enquanto a latência média permaneceu abaixo de 10 ms. A Tabela 15 resume os principais resultados experimentais.

Métrica avaliada	Resultado observado	Interpretação

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

Throughput	Superior a 1.000 transações por segundo	Indica capacidade de processamento sob carga sustentada
Latência média	Inferior a 10 ms	Indica baixa demora em ambiente local
Carga acumulada	10.000 blocos e mais de 100.000 transações	Indica estabilidade do modelo sob carga volumétrica
Sincronização	Recuperação automática via SYNC_REQUEST	Indica consistência após falhas parciais
Detecção de adulteração	5/5 cenários apresentaram o comportamento esperado	Indica integridade criptográfica da cadeia
Injeção de blocos corrompidos	Blocos rejeitados pelos nós	Indica validação contra registros inválidos

Tabela 15: Síntese dos resultados experimentais.

Os ensaios de estresse volumétrico indicaram estabilidade do modelo de dados. O serviço processou uma carga acumulada de 10.000 blocos e mais de 100.000 transações. Diante da simulação de desligamentos forçados e quedas parciais de nós, a sincronização incremental restabeleceu a consistência da cadeia. Esse comportamento foi obtido por meio das mensagens SYNC_REQUEST.

Os testes de segurança demonstraram a capacidade da arquitetura de detectar as adulterações contempladas no protocolo experimental. Tentativas de modificação direta nos arquivos JSON de persistência local foram detectadas em todos os cenários testados. A alteração de um registro quebrou a integridade matemática dos hashes SHA-256 encadeados. Além disso, a injeção forjada de blocos corrompidos foi rejeitada pelos nós. Tentativas de induzir bifurcações foram mitigadas pelas rotinas de resolução de conflito do protocolo P2P.

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

4.3. Discussão

A *Rapid Review* indicou que soluções industriais frequentemente usam blockchain como camada de confiança para registrar eventos de forma imutável, com predomínio de redes permissionadas ou de consórcio. Esse padrão é coerente com a arquitetura implementada, baseada em rede privada, validadores conhecidos e consenso PoA.

A literatura também mostrou integração recorrente com sensores, IoT, sistemas de gestão, IA e *digital twins*, o que reforça o papel do microsserviço como camada independente de registro e auditoria. Nos experimentos, a solução apresentou baixa latência em rede local e detectou alterações nos arquivos de persistência pelo encadeamento criptográfico dos blocos, mesmo com armazenamento em JSON.

A blockchain, porém, não resolve problemas de qualidade do dado de origem, ainda dependente de sensores, CLPs e sistemas externos. Os resultados de desempenho, obtidos em ambiente controlado, demandam avaliações com redes maiores, maior volume de eventos e diferentes condições de falha.

Sua adoção também não implica superioridade sobre bancos de dados convencionais, logs *append-only* ou mecanismos WORM. A escolha decorreu dos requisitos do protótipo, especialmente replicação entre participantes autorizados, encadeamento criptográfico, validação distribuída e reconciliação de estado. Havendo autoridade central confiável, soluções tradicionais podem ser menos complexas. Assim, o estudo demonstra a viabilidade da arquitetura no contexto avaliado, sem reivindicar superioridade geral da blockchain.

5. Limitações

A *Rapid Review* apresenta limitações decorrentes das decisões adotadas para manter seu caráter rápido e orientado à tomada de decisão. A busca foi realizada apenas na Scopus, restrita a publicações em inglês com texto completo disponível, o que pode ter reduzido a abrangência e introduzido vieses de cobertura, idioma e disponibilidade. Os resultados representam, portanto, um panorama dos estudos recuperados pela estratégia adotada, e não um levantamento exaustivo da literatura.

O corpus reúne diferentes tipos de estudos, como experimentos, protótipos, frameworks e revisões. Essa heterogeneidade deve ser considerada na interpretação das frequências, pois estudos secundários podem sintetizar evidências de trabalhos primários também presentes no corpus. Como também não houve avaliação formal da qualidade metodológica, as frequências não representam necessariamente evidências independentes nem permitem inferir superioridade técnica das abordagens mais recorrentes.

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

Quanto à avaliação experimental, os testes ocorreram em ambiente controlado, com configuração limitada da rede e nós executados no mesmo host físico, de modo que os resultados caracterizam apenas as condições avaliadas. Não foram investigados sistematicamente cenários com maior número de nós, volumes superiores de eventos, falhas simultâneas, deriva de relógio entre hosts ou integração com equipamentos e sistemas industriais reais.

A avaliação também não contemplou mecanismos necessários a uma implantação segura em produção, como autenticação e autorização de usuários, controle de papéis, limitação de requisições, TLS na API REST, autenticação criptográfica individual dos peers e assinatura digital dos blocos. A autorização dos validadores baseia-se em configuração prévia, e os testes se restringiram aos cenários de adulteração definidos no protocolo experimental. A solução não reivindica tolerância a falhas bizantinas nem proteção contra validadores autorizados maliciosos ou ataques coordenados.

A persistência em arquivos JSON tem caráter experimental: não foram avaliados escrita atômica, recuperação após falhas, corrupção parcial ou sincronização forçada com o armazenamento, nem estabelecido limite específico para o conteúdo do campo Data, tendo os testes utilizado cargas controladas. Essa estratégia não deve ser interpretada como solução de persistência adequada a cenários produtivos de alto volume ou alta disponibilidade.

Não foi realizada análise longitudinal do crescimento do ledger, de modo que os efeitos do aumento contínuo da cadeia sobre armazenamento, inicialização, sincronização e consultas não foram caracterizados. Operações que dependem da transferência integral da cadeia podem tornar-se onerosas em volumes maiores, indicando a necessidade futura de paginação, sincronização incremental e indexação.

Por fim, a implementação utiliza a serialização do System.Text.Json, sem esquema formal de JSON canônico que garanta interoperabilidade criptográfica entre implementações distintas. Também não foram realizados benchmarks comparativos com bancos de dados tradicionais, logs *append-only*, mecanismos WORM ou outras plataformas blockchain. Os resultados caracterizam exclusivamente a implementação proposta nas condições avaliadas.

6. Considerações Finais

Este trabalho apresentou uma arquitetura de blockchain privada e offline, concebida como um microsserviço genérico para registro auditável de dados, com mecanismos de verificação de integridade e detecção de alterações. A proposta foi fundamentada por uma Rapid Review sobre o uso de blockchain em rastreabilidade, auditabilidade, integridade de dados e registro seguro de eventos na manufatura inteligente.

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

A revisão identificou padrões como o uso de blockchains permissionadas, redes de consórcio, smart contracts, integração com sensores, IoT e sistemas industriais, além de desafios relacionados à escalabilidade, latência, interoperabilidade, privacidade, qualidade dos dados e armazenamento. Esses achados forneceram referências para as decisões arquiteturais, em conjunto com os requisitos específicos da solução.

A arquitetura foi implementada como um microsserviço independente, com API REST, comunicação P2P via WebSockets, consenso inspirado em Proof-of-Authority e persistência local em arquivos JSON. Embora o PoA tenha aparecido na literatura, sua adoção não representa uma preferência estabelecida pelo corpus, mas uma decisão compatível com uma rede privada e permissionada composta por validadores conhecidos. Assim, o uso de JSON corresponde a uma decisão experimental de implementação.

Os resultados indicaram viabilidade técnica em ambiente controlado. A rede com três nós validadores apresentou latência média inferior a 10 ms, throughput superior a 1.000 transações por segundo e estabilidade no processamento de mais de 100.000 transações distribuídas em 10.000 blocos. Os testes de segurança também demonstraram a detecção de alterações nos registros por meio dos hashes encadeados com SHA-256, além da rejeição de blocos corrompidos e do tratamento de bifurcações pelas rotinas de sincronização e resolução de conflitos.

Assim, a principal contribuição do trabalho é uma arquitetura genérica, offline e permissionada para registro auditável de eventos industriais. Nas condições avaliadas, a solução reduz a dependência de conectividade externa e de redes públicas e fornece mecanismos de integridade verificável, detecção de adulteração, rastreabilidade e auditabilidade.

Como trabalhos futuros, propõe-se ampliar os mecanismos de segurança com assinaturas digitais nas transações e nos blocos e autenticação criptográfica dos peers, além de incorporar suporte a smart contracts. Também se recomenda

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

investigar mecanismos de interoperabilidade com outras redes blockchain e sistemas industriais e desenvolver um módulo de analytics com métricas operacionais, relatórios de auditoria, dashboards e monitoramento dos nós, blocos e transações.

Referências

Alazab, M., and S. Alhyari. “Industry 4.0 Innovation: A Systematic Literature Review on the Role of Blockchain Technology in Creating Smart and Sustainable Manufacturing Facilities.” *Information*, vol. 15, no. 2, 2024, p. 78.

Ali, S., et al. “Blockchain-Enabled Open Quality System for Smart Manufacturing: Applications and Challenges.” *Sustainability*, vol. 14, no. 18, 2022, p. 11677.

Cartaxo, B., et al. “The Role of Rapid Reviews in Supporting Decision-Making in Software Engineering Practice.” *Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018*, 2018, pp. 24-34.

Casino, F., et al. “A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues.” *Telematics and Informatics*, vol. 36, 2019, pp. 55-81.

Chen, S., et al. “Blockchain Applications in PLM towards Smart Manufacturing.” *The International Journal of Advanced Manufacturing Technology*, vol. 118, no. 7, 2022, pp. 2669-83.

Cohen, Y., and S. Rozenes. “New Framework for Complex Assembly Digitalization and Traceability Using Bill of Assembly and Smart Contracts.” *Applied Sciences*, vol. 13, no. 3, 2023, p. 1884.

Cohen, Y., et al. “Framework for Block-Chain Deployment in Assembly of an Air-Craft or a Spacecraft.” *IFAC-PapersOnLine*, vol. 54, no. 1, 2021, pp. 988-92.

De Angelis, S., et al. “PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain.” *Italian Conference on Cyber Security*, 2018.

Essaid, M., and H. Ju. “Blockchain Solutions for Enhancing Security and Privacy in Industrial IoT.” *Applied Sciences*, vol. 15, no. 12, 2025, p. 6835.

Fernández-Caramés, T. M., and P. Fraga-Lamas. “A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories.” *IEEE Access*, vol. 7, 2019, pp. 45201-18.

Guo, X., et al. “A Comprehensive Review of Blockchain Technology-Enabled Smart Manufacturing: A Framework, Challenges and Future Research Directions.” *Sensors*, vol. 23, no. 1, 2022, p. 155.

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

Jia, W., and S. Wang. “Research on Robot Assembly Traceability System Based on Fabric.” *2024 IEEE 4th International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA)*, vol. 4, IEEE, 2024, pp. 375-80.

Jie, Y., et al. “Design and Application of an Intelligent Inspection and Product Quality Data Traceability System in Green Smart Manufacturing.” *Proceedings of the 2025 6th International Conference on Computer Science and Management Technology*, 2025, doi:10.1145/3795154.3795358.

Karadgi, S., et al. “Traceable and Intelligent Supply Chain Based on Blockchain and Artificial Intelligence.” *Journal of Physics: Conference Series*, vol. 2070, no. 1, IOP Publishing, 2021, p. 012158.

Košťál, K., et al. “Enhancing Supply Chain Transparency in the Automotive Industry: A Blockchain-Based ERP System Approach.” *2024 6th International Conference on Blockchain Computing and Applications (BCCA)*, IEEE, 2024, pp. 481-88.

Kuhn, M., et al. “Blockchain-Based Application for the Traceability of Complex Assembly Structures.” *Journal of Manufacturing Systems*, vol. 59, 2021, pp. 617-30.

Kuo, T., and H. Yang. “Hierarchical Blockchain for Mapping Manufacturing Process Flow.” *2025 IEEE 21st International Conference on Automation Science and Engineering (CASE)*, IEEE, 2025, pp. 2657-62.

Mingxiao, D., et al. “A Review on Consensus Algorithm of Blockchain.” *2017 IEEE International Conference on Systems, Man, and Cybernetics*, IEEE, 2017, pp. 2567-72.

Mohamed, N., and J. Al-Jaroodi. “Applying Blockchain in Industry 4.0 Applications.” *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, 2019, pp. 852-58.

Mokalusi, O. L., et al. “Designing an Experimental Setup for Data Provenance Tracking Using a Public Blockchain: A Case Study Using a Water Bottling Plant.” *International Journal of Advanced Computer Science & Applications*, vol. 15, no. 6, 2024.

Murgai, S. “Enhancing Distributed Security and Reliability in Semiconductor Supply Chains with Blockchain and Chemistry Integration.” *2024 43rd International Symposium on Reliable Distributed Systems (SRDS)*, IEEE, 2024, pp. 350-60.

Nakamoto, S. “Bitcoin: A Peer-to-Peer Electronic Cash System.” *Decentralized Business Review*, 2008, p. 21260.

CC BY

REMUNOM
ISSN 2178-6925

Received: 26/07/2026 - **Accepted:** 01/08/2026
Vol: 13.19
DOI: 10.66104/1v068e67
Pages: 1-39

Roumeliotis, C., et al. “Blockchain and Digital Twins in Smart Industry 4.0: The Use Case of Supply Chain — A Review of Integration Techniques and Applications.” *Designs*, vol. 8, no. 6, 2024, p. 105.

Saenz de Ugarte, B., et al. “Manufacturing Execution System — A Literature Review.” *Production Planning & Control*, vol. 20, no. 6, 2015, pp. 525-39.

Song, Z., and J. Zhu. “Blockchain for Smart Manufacturing Systems: A Survey.” *Chinese Management Studies*, vol. 16, no. 5, 2022, pp. 1224-53.

Vijayapriya, R., et al. “Smart Manufacturing Supply Chain Process Strategy Using Intelligent Computation Techniques.” *International Journal on Interactive Design and Manufacturing (IJIDeM)*, vol. 19, no. 2, 2025, pp. 681-94.

Wang, Y., et al. “Understanding Blockchain Technology for Future Supply Chains: A Systematic Literature Review and Research Agenda.” *Supply Chain Management: An International Journal*, vol. 24, no. 1, 2019, pp. 62-84.

Westerkamp, M., et al. “Blockchain-Based Supply Chain Traceability: Token Recipes Model Manufacturing Processes.” *2018 IEEE International Conference on Internet of Things*, IEEE, 2018, pp. 1595-602.

Wu, L., et al. “A Review of Blockchained Product Quality Management towards Smart Manufacturing.” *Processes*, vol. 13, no. 8, 2025, p. 2622.

Xu, X., et al. “Industry 4.0: State of the Art and Future Trends.” *International Journal of Production Research*, vol. 56, no. 8, 2018, pp. 2941-62.

Yousef, N., et al. “Blockchain-Integrated IoT Device for Advanced Inspection of Casting Defects.” *Scientific Reports*, vol. 15, no. 1, 2025, p. 5300.

Yuan, B., and F. Wu. “Application of Thermal Energy Efficiency Utilization Based on Computer Technology in Green Manufacturing Blockchain Production Traceability.” *Thermal Science and Engineering Progress*, vol. 54, 2024, p. 102859.

Zhang, X., et al. “Virtual Reality Integration and Credible Traceability Management Method of Transformer Coil Manufacturing Process Based on Industrial Internet and Digital Twin.” *International Journal of Computer Integrated Manufacturing*, vol. 39, no. 1, 2026, pp. 1-28.

Zheng, Z., et al. “Blockchain Challenges and Opportunities: A Survey.” *International Journal of Web and Grid Services*, vol. 14, no. 4, 2018, pp. 352-75.

CC BY