Modelo de Monitoramento Descentralizado com Privacidade de Dados em Redes Blockchain Empresariais

Jeffson Sousa[1,2], **Alan Veloso**[1], **Mateus Bastos**[1],
Bruno Evaristo[1,2], **Antônio Abelém**[1],

[1] Universidade Federal do Pará (UFPA)
Belém – PA – Brazil

[2]Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD)
Campinas – SP – Brasil

{jeffson, elderb}@cpqd.com.br, {aveloso, abelem}@ufpa.br,
{mateus.araujo}@icen.ufpa.br

Resumo. *Este artigo propõe um modelo de monitoramento descentralizado com privacidade para redes blockchain permissionadas, priorizando a privacidade dos nós. A arquitetura federada permite que cada nó envie métricas por meio de resumos criptográficos, revelando detalhes apenas em casos críticos. A solução garante autonomia, evita a exposição de dados sensíveis e oferece auditoria confiável, promovendo governança robusta e escalabilidade em ambientes empresariais que exigem resiliência e confidencialidade.*

Abstract. *This article proposes a decentralized monitoring model with privacy for permissioned blockchain networks, prioritizing node confidentiality. The federated architecture allows each node to submit operational metrics through cryptographic summaries, revealing details only in critical situations. The solution ensures autonomy, prevents the exposure of sensitive data, and provides reliable auditing, promoting robust governance and scalability in enterprise environments that require resilience and confidentiality.*

1. Introdução

A tecnologia blockchain adota um modelo descentralizado onde os participantes colaboram diretamente sem um controle central. Essa abordagem já é amplamente aplicada em setores como educação, transporte e cadeias de suprimentos [Fakhri et al. 2021]. A blockchain funciona como um banco de dados distribuído, no qual transações são agrupadas em blocos encadeados, gerando um registro permanente e imutável [Kanga et al. 2023, Di Pierro 2017].

Em redes privadas e permissionadas, cada organização é representada por um ou mais nós responsáveis por validar transações e participar do consenso. Esses nós devem operar de forma autônoma, atendendo aplicações distribuídas e empresariais. No entanto, o monitoramento desses componentes não deve apenas garantir desempenho e segurança, mas também preservar a confidencialidade de métricas sensíveis. Mesmo em ambientes permissionados, a exposição irrestrita de dados operacionais pode revelar vulnerabilidades ou comprometer a governança entre os participantes [Fakhri et al. 2021].

Apesar da adoção crescente da tecnologia blockchain por consórcios empresariais, a exposição de dados operacionais pode comprometer a confiança e a soberania dos participantes [Sunny et al. 2022]. Monitorar segurança, desempenho e integridade continua

sendo essencial, mas é necessário evitar que informações como uso de recursos, tempo de resposta ou taxas de proposição de blocos sejam compartilhadas de forma identificável ou correlacionável.

Segundo Bastos et al. (2024) [Bastos et al. 2024], o maior desafio dos sistemas atuais de monitoramento é a centralização, que concentra controle, expõe dados sensíveis e representa um ponto único de falha. Para redes permissionadas, é fundamental adotar um modelo descentralizado que minimize os dados compartilhados, utilizando técnicas como hashing e criptografia para preservar a privacidade.

Este trabalho propõe um framework de monitoramento descentralizado e federado com suporte à camada de privacidade, voltado para redes blockchain permissionadas. A solução permite que cada nó envie hashes das métricas monitoradas, revelando detalhes apenas em situações críticas. Isso garante confidencialidade, autonomia e auditabilidade sem comprometer a segurança do sistema. O modelo elimina pontos centralizados, é modular, escalável e adaptável a diferentes redes, promovendo governança cooperativa com preservação da privacidade.

O artigo está estruturado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados; a Seção 3 descreve a arquitetura do framework; a Seção 4 detalha o cenário experimental; a Seção 5 discute os resultados obtidos; e a Seção 6 traz as conclusões e direções futuras.

2. Trabalhos Relacionados

Trabalho	**Tipo de Rede**	**Estrutura de Monitoramento**	**Principais Métricas**	**Objetivo**
[Kanga et al. 2023]	Pública	Centralizado	*logs*, CPU, Tráfego	Coleta funcional, sem foco em privacidade.
[Fakhri et al. 2021]	Permissionada	Distribuído	CPU, Memória, Tráfego	Monitoramento por agente, sem anonimização.
[Ko et al. 2018], [Lee et al. 2019]	Pública, Permissionada	Centralizado	Análise de dados	Interpretação central com risco de exposição.
[Zheng et al. 2018], [Kanga et al. 2020]	Pública, Permissionada	Centralizado	RPC, CPU, Memória	Coleta RPC eficiente, sem controle de privacidade.
Proposta	Pública, Permissionada	Federado, Descentralizado	Todas as métricas (statusHash, severidade, alertas)	Monitoramento com privacidade seletiva e descentralização.

Tabela 1. Representação dos Trabalhos Relacionados.

As soluções de monitoramento em redes blockchain variam entre sistemas públicos e permissionados, com ênfase crescente na descentralização e proteção de dados sensíveis. No entanto, estudos como [Bang and Choi 2019] e [Kanga et al. 2020] mostram que a maioria das abordagens ainda adota arquiteturas centralizadas, compostas por agentes e servidores responsáveis por coleta, análise e visualização de métricas. Embora funcionais, essas estruturas expõem dados operacionais a terceiros, o que compromete a confidencialidade, especialmente em redes corporativas com múltiplos participantes.

Propostas como a de [Fakhri et al. 2021] evoluem para agentes distribuídos em cada nó, permitindo monitoramento mais localizado. Ainda assim, a ausência de mecanismos de anonimização, hashing ou controle de exposição mantém vulnerabilidades em relação à privacidade dos dados. Trabalhos como [Ko et al. 2018] e [Lee et al. 2019]

reforçam essa limitação ao focarem na análise centralizada dos dados enviados, desconsiderando os riscos de exposição intra-consórcio.

A Tabela 1 apresenta uma comparação detalhada dos trabalhos existentes com relação à estrutura de monitoramento e às estratégias de privacidade. A proposta deste trabalho se diferencia ao propor uma abordagem federada e descentralizada com privacidade seletiva. Os nós participantes reportam seu estado por meio de hashes criptográficos, e apenas em eventos críticos detalhes são revelados. Essa arquitetura garante soberania organizacional, auditabilidade distribuída e alinhamento com as necessidades de redes blockchain permissionadas, oferecendo um avanço frente às limitações dos modelos anteriores.

3. Arquitetura da Proposta

A arquitetura como um todo evidencia uma solução completa e pragmática para os desafios contemporâneos de monitoramento em redes blockchain permissionadas. Ao combinar coleta local com controle de privacidade, publicação seletiva on-chain e integração com ferramentas de visualização externas, o framework proposto oferece um alto grau de adaptabilidade a diferentes cenários corporativos. Sua estrutura modular permite a inclusão de novos tipos de métricas, personalização das condições de alerta e adaptação a diferentes plataformas de blockchain, como Hyperledger Besu, Fabric e Indy.

Além disso, a abordagem federada elimina o ponto único de falha típico de sistemas centralizados, distribuindo a responsabilidade do monitoramento entre os próprios participantes da rede. Isso fortalece a governança descentralizada e permite que organizações compartilhem métricas operacionais de forma segura, auditável e com controle granular sobre o que é revelado. O uso de eventos blockchain, como StatusReported e CriticalAlert, amplia as possibilidades de reatividade automatizada, alimentando mecanismos de resposta em tempo real ou processos internos baseados em SLA.

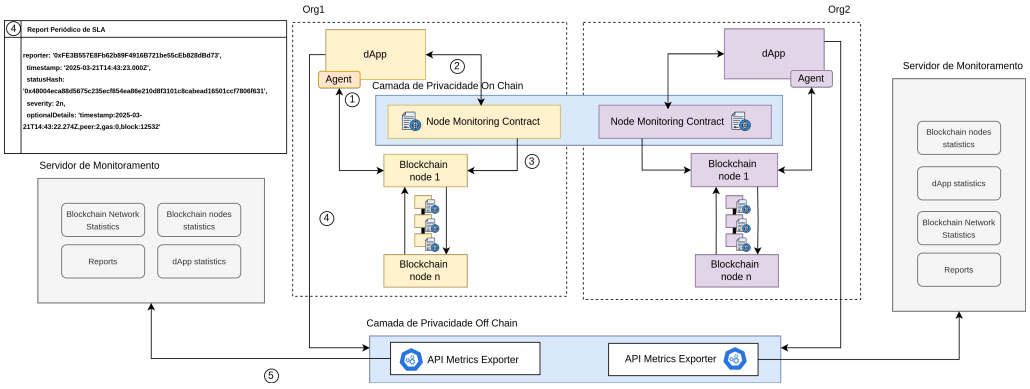


Figura 1. Arquitetura da proposta

Em síntese, a arquitetura apresentada na Figura 1 demonstra como é possível construir uma solução de monitoramento blockchain que equilibra segurança, transparência e privacidade — princípios frequentemente conflitantes em sistemas distribuídos. O framework não apenas atende aos requisitos técnicos de desempenho e escalabilidade, mas também responde às demandas regulatórias e organizacionais por proteção de dados sensíveis, tornando-se uma proposta robusta e viável para ambientes empresariais críticos.

A proposta do contrato inteligente *NodeHealthMonitor* constitui o núcleo da arquitetura descentralizada de monitoramento, funcionando como repositório imutável dos relatórios de integridade enviados pelos nós da rede. Cada nó, por meio de agentes locais, gera e envia periodicamente um resumo criptográfico (*statusHash*) das métricas coletadas. A função *reportStatus* recebe o grau de severidade, o hash das métricas e, opcionalmente, detalhes legíveis quando o alerta é crítico (severity 2), preservando a confidencialidade em situações regulares.

Essa abordagem garante privacidade por meio do envio de hashes, evitando a exposição direta de métricas sensíveis, como uso de recursos ou número de peers. Apenas em cenários críticos os detalhes são incluídos no campo *optionalDetails*, permitindo uma reação eficiente da rede sem comprometer a privacidade dos nós em operação normal.

Além da publicação seletiva, a solução oferece funcionalidades para auditoria e rastreamento. As funções *getLatestStatus* e *statusReports* permitem, respectivamente, acesso ao último status de um nó e consulta a todo seu histórico de relatórios. Isso viabiliza dashboards, validações automatizadas e análises temporais do comportamento da rede. O uso de eventos blockchain (StatusReported e CriticalAlert) como canal de notificação torna o sistema reativo e auditável em tempo real, eliminando a necessidade de varreduras contínuas.

4. Cenário de Avaliação

O processo de avaliação foi conduzido por meio de três configurações distintas de testes, cada uma voltada para uma função do contrato inteligente *NodeHealthMonitor*: `reportStatus`, `getLatestStatus` e `statusReports`. Para cada função, simulamos cargas crescentes de transações com taxas variando de 20 a 200 TPS, em intervalos de 20.

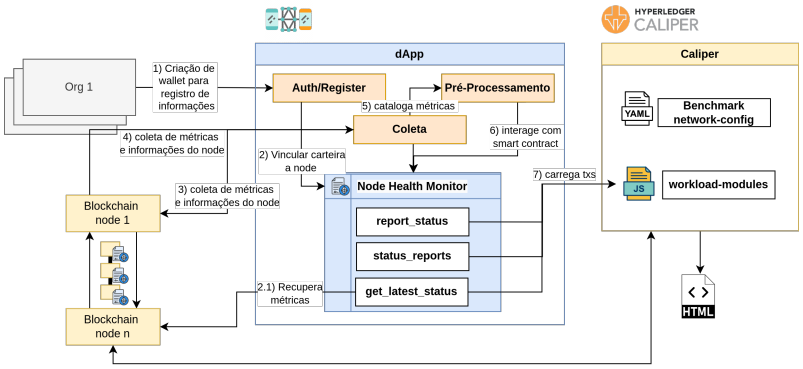


Figura 2. Cenário de Experimentação

A Figura 2 apresenta a arquitetura do framework de monitoramento descentralizado com suporte a testes de carga via Hyperledger Caliper. O cenário simula múltiplas organizações monitorando seus nós blockchain de forma segura e auditável, com privacidade preservada.

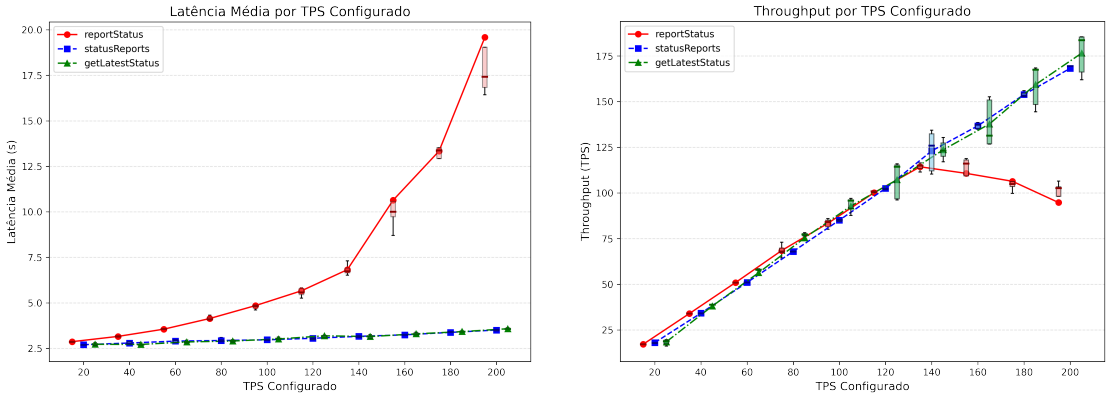
O fluxo inicia com a criação da identidade digital da organização e o vínculo com seu nó monitorado. A dApp coleta métricas operacionais (como blocos, peers e uso de gas), processa localmente os dados e avalia sua severidade. Em seguida, os dados são condensados em um hash (statusHash) e enviados ao contrato inteligente *NodeHealthMonitor*, que registra os status via a função `reportStatus`. Eventos `StatusReported`

e `CriticalAlert` são emitidos conforme o nível de criticidade, mantendo os detalhes ocultos em condições normais e revelando-os apenas em casos críticos.

5. Resultados

Para avaliar o desempenho do contrato inteligente `NodeHealthMonitor`, realizamos testes de carga com as funções `reportStatus`, `statusReports` e `getLatestStatus`, considerando apenas as métricas de throughput e latência. As rodadas foram configuradas com 20 segundos de duração e variação de TPS de 20 a 200, repetidas 5 vezes por configuração.

A Figura 3(a) mostra que a função `reportStatus`, por envolver gravações on-chain, apresentou crescimento acentuado na latência a partir de 80 TPS. Já as funções de leitura (`statusReports` e `getLatestStatus`) mantiveram latência baixa e estável, mesmo sob cargas elevadas. Isso evidencia a eficiência do modelo de separação entre leitura e escrita.



(a) Latência média por função e taxa de envio (TPS) (b) Throughput médio por função e taxa de envio (TPS)

Figura 3. Comparação entre as funções `reportStatus`, `statusReports` e `getLatestStatus` em termos de latência (a) e throughput (b).

A Figura 3(b) demonstra que `reportStatus` atingiu seu pico de throughput próximo a 80 TPS, com redução posterior possivelmente causada por sobrecarga ou limitações de infraestrutura. Em contraste, as funções de leitura escalaram linearmente, sustentando maior volume de requisições sem perda significativa de desempenho.

6. Conclusões e Trabalhos Futuros

Este trabalho propôs uma arquitetura de monitoramento descentralizado com camada de privacidade para redes blockchain permissionadas, combinando uma dApp local autônoma com um contrato inteligente que registra resumos criptográficos das métricas dos nós. Os experimentos demonstraram que o modelo é eficaz para registrar eventos críticos com exposição seletiva dos dados, mantendo a rastreabilidade e a confidencialidade em ambientes com múltiplos participantes. A abordagem se mostrou compatível com princípios de governança federada, auditoria transparente e proteção de dados operacionais sensíveis.

Como próximos passos, pretende-se integrar o framework a sistemas de detecção de anomalias com inteligência artificial, utilizar oráculos para desencriptação seletiva de dados em consenso off-chain, e implementar mecanismos de incentivo ou penalidade para nós que não reportam regularmente. Essas melhorias visam ampliar a resiliência, escalabilidade e confiabilidade do modelo em cenários empresariais exigentes.

Agradecimentos

Os autores agradecem o apoio dado a este trabalho, pelo MCTI-Ministério da Ciência, Tecnologia e Inovação, com recursos financeiros do FUNTTEL e administrados pela FINEP, no âmbito especificamente do projeto AERF - Ações Estratégicas para Redes Futuras, Contrato 01.22.0471.00, Referência 1508/22.

Referências

Bang, J. and Choi, M.-J. (2019). Design and implementation of storage system for real-time blockchain network monitoring system. In *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pages 1–4, Matsue, Japan. IEEE.

Bastos, M., Silva, C., Veloso, A. T. S., Sousa, J. C., Correa, E. B. E., Formigoni Filho, J. R., and Abelem, A. J. G. (2024). Soluções de monitoramento de redes blockchain: Uma revisão sistemática da literatura. In *WORKSHOP EM BLOCKCHAIN: TEORIA, TECNOLOGIAS E APLICAÇÕES (WBLOCKCHAIN)*, Niterói, RJ. Sociedade Brasileira de Computação.

Di Pierro, M. (2017). What is the blockchain? *Computing in Science & Engineering*, 19(5):92–95.

Fakhri, M., Zegre, B., Omrane, N., and Jaziri, R. (2021). Speedchain: A framework for monitoring and alerting blockchain projects. In *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–5, Paris, France. IEEE.

Kanga, B. D., Azouazi, M., El Ghoumrari, Y. M., and Daif, A. (2023). *Methodology of the Blockchain Monitoring Framework*. IntechOpen.

Kanga, D. B., Azzouazi, M., El Ghoumrari, M. Y., and Daif, A. (2020). Management and monitoring of blockchain systems. *Procedia Computer Science*, 177:605–612.

Ko, K., Lee, C., Jeong, T., and Hong, J. W.-K. (2018). Design of rpc-based blockchain monitoring agent. In *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 1090–1095.

Lee, C., Kim, H., Maharjan, S., Ko, K., and Hong, J. W.-K. (2019). Blockchain explorer based on rpc-based monitoring system. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 117–119, Seoul, Korea (South). IEEE.

Sunny, F. A., Hajek, P., Munk, M., Abedin, M. Z., Satu, M. S., Efat, M. I. A., and Islam, M. J. (2022). A systematic review of blockchain applications. *IEEE Access*, 10:59155–59177.

Zheng, P., Zheng, Z., Luo, X., Chen, X., and Liu, X. (2018). A detailed and real-time performance monitoring framework for blockchain systems. In *Proceedings of the 40th International Conference on Software Engineering: Software Engineering in Practice*, pages 134–143, Gothenburg, Sweden. ACM.