Uma proposta de framework de blockchain em Internet das Coisas com dados de geolocalização

Washington Luiz de Lima Praxedes Filho[1], **Cidcley Teixeira de Souza**[1]

[1]Programa de Pós Graduação em Ciência da Computação –
Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)
Fortaleza – CE – Brazil

washington.luiz.lima01@aluno.ifce.edu.br, cidcley@ifce.edu.br

Abstract. *IoT applications that process geolocation data face challenges related to security, privacy, and the limited computational capabilities of devices. This paper proposes a blockchain-based framework for geolocation data in IoT, exploring the execution of blockchain nodes at the network edge. The framework integrates authentication, data integrity, and pseudonymization mechanisms, and is evaluated under edge and cloud execution scenarios. Results indicate that edge-based execution reduces latency, improves throughput, and increases predictability compared to cloud-based execution.*

Resumo. *Aplicações de Internet das Coisas (IoT) que tratam dados de geolocalização enfrentam desafios relacionados à segurança, privacidade e limitações computacionais dos dispositivos. Este trabalho propõe um framework baseado em blockchain para dados de geolocalização em IoT, explorando a execução de nós na borda da rede. A proposta integra mecanismos de autenticação, integridade e pseudonimização, sendo avaliada em cenários de execução na borda e na nuvem. Os resultados indicam que a execução na borda reduz a latência, melhora o throughput e aumenta a previsibilidade em comparação à execução em nuvem.*

1. Introdução

Dados de geolocalização são amplamente utilizados em aplicações de Internet das Coisas (IoT), como rastreamento e monitoramento de ativos. Entretanto, a exposição dessas informações pode comprometer aspectos de privacidade, integridade e autenticidade dos dados [Li et al. 2020, Zafar et al. 2020]. Nesse contexto, blockchain tem sido investigada como alternativa para o registro imutável e verificável de informações de localização, permitindo também o uso de mecanismos de autenticação e controle de acesso baseados em *smart contracts* [Khalid et al. 2020].

Apesar disso, trabalhos existentes geralmente tratam requisitos como autenticação, privacidade e integridade de forma isolada, além de explorarem de maneira limitada o impacto da execução de nós blockchain próximos aos dispositivos IoT.

Diante desse cenário, este trabalho propõe um framework baseado em blockchain para aplicações IoT com dados de geolocalização, explorando a execução de nós na borda da rede. A proposta integra mecanismos de autenticação, integridade e pseudonimização dos dados, além de avaliar experimentalmente o impacto da execução de nós blockchain na borda em comparação a uma infraestrutura remota na nuvem.

As principais contribuições deste trabalho são:

- Um framework baseado em blockchain para aplicações IoT com dados de geolocalização;
- A integração de mecanismos de autenticação, integridade e pseudonimização;
- Uma avaliação experimental comparando a execução de nós blockchain na borda e na nuvem.

2. Trabalhos Relacionados

A fim de identificar lacunas relacionadas ao uso de blockchain em aplicações IoT com dados de geolocalização, foi conduzida uma revisão sistemática da literatura em bases digitais da área. A busca inicial retornou 642 estudos potenciais, dos quais 14 foram selecionados após a aplicação de critérios de inclusão, exclusão e qualidade. A Tabela 1 apresenta os trabalhos mais aderentes ao escopo da proposta, considerando borda, autenticação, integridade, privacidade e desempenho.

Diversos estudos investigam o uso de blockchain em aplicações IoT com dados de geolocalização, abordando aspectos como verificação de localização, integridade dos dados, privacidade e autenticação de dispositivos [Zafar et al. 2020, Yao et al. 2022, Khalid et al. 2020]. Algumas propostas exploram mecanismos de preservação de privacidade e pseudonimização [Sun et al. 2021, Zhang et al. 2020, Wu et al. 2020], enquanto outras discutem o uso de blockchain em ambientes de borda ou névoa para apoiar aplicações distribuídas [Liang et al. 2020, Dedeoglu et al. 2019].

Trabalho	Nós na borda	Autenticação	Integridade	Privacidade	Performance
[Zhang et al. 2020]	✓	–	✓	✓	–
[Wu et al. 2020]	✓	✓	–	✓	–
[Sun et al. 2021]	✓	–	–	✓	–
[Ren et al. 2023]	–	–	✓	–	–
[Liang et al. 2020]	✓	✓	✓	–	–
[Dedeoglu et al. 2019]	–	–	✓	–	–
[Peelam et al. 2024]	–	✓	✓	✓	–
Framework proposto	✓	✓	✓	✓	✓

Table 1. Comparação entre trabalhos relacionados

De forma geral, os resultados da revisão indicam que as abordagens existentes tratam requisitos como autenticação, integridade, privacidade e execução na borda de maneira predominantemente isolada. Além disso, poucas propostas avaliam experimentalmente o impacto da execução de nós blockchain próximos aos dispositivos IoT. O framework proposto busca integrar esses mecanismos em uma única abordagem, considerando também aspectos de desempenho.

3. Framework Proposto

3.1. Fluxo e funcionamento

O framework proposto registra dados de geolocalização produzidos por dispositivos IoT em uma blockchain executada próxima à origem dos dados. Conforme apresentado na Figura 1, os dispositivos enviam registros de localização para um nó blockchain localizado na borda

da rede, responsável por validar transações e executar os *smart contracts* utilizados no controle de acesso e no registro das informações.

Após o armazenamento das transações na blockchain local, o estado da cadeia pode ser periodicamente ancorado em uma blockchain pública. Esse processo registra externamente o *hash* do último bloco produzido na borda, permitindo a verificação posterior da integridade dos registros sem exigir que todos os dados de geolocalização sejam publicados em uma rede externa.

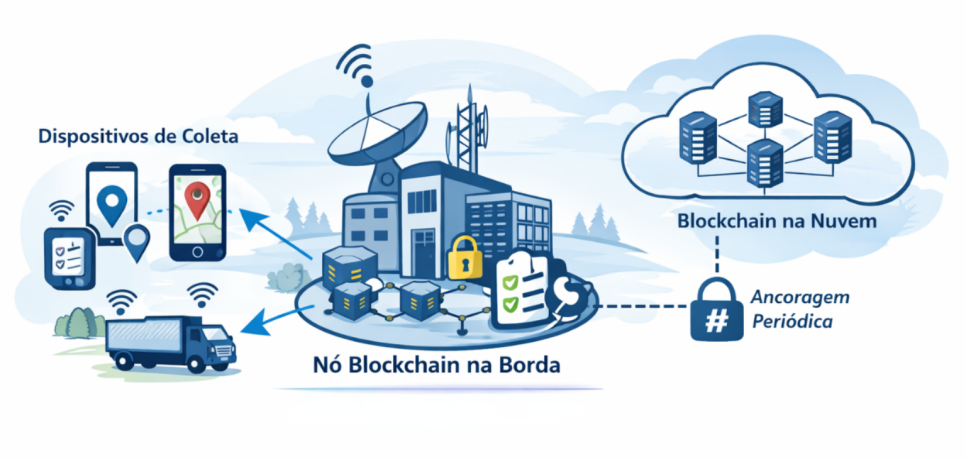


Figure 1. Estrutura do framework proposto.

3.2. Mecanismos de segurança

O framework incorpora três mecanismos principais de segurança. O primeiro refere-se à autenticação dos dispositivos, garantindo que apenas entidades autorizadas possam registrar dados de geolocalização. O segundo mecanismo está relacionado à integridade dos registros, garantida pelo armazenamento imutável das transações na blockchain e pelo processo de ancoragem em uma rede pública. Por fim, a privacidade é tratada por meio da utilização de identificadores pseudonimizados, reduzindo a exposição da identidade real dos dispositivos nos registros armazenados.

4. Experimentos

A avaliação comparou dois cenários de execução: (i) blockchain em infraestrutura remota na nuvem, utilizada como baseline; e (ii) blockchain executada na borda da rede, com ancoragem periódica em uma blockchain pública. A implementação utilizou uma blockchain compatível com a Ethereum Virtual Machine (EVM) e *smart contracts* em Solidity. No cenário de borda, foi utilizada uma rede EVM com nó validador dedicado; as credenciais dos dispositivos são previamente provisionadas e usadas na geração de tokens de sessão validados pelo *smart contract*.

Os dispositivos IoT foram simulados para enviar registros periódicos de geolocalização ao *smart contract*, utilizando credenciais de autenticação. As rodadas experimentais foram compostas por 200 operações de escrita, com até 10 dispositivos simultâneos. A avaliação considerou os percentis de latência de confirmação das transações (p50, p95 e p99), o TPS, o coeficiente de variação da latência e testes funcionais de autenticação, integridade por ancoragem e pseudonimização.

5. Resultados e Discussões

5.1. Performance de interações com Blockchain

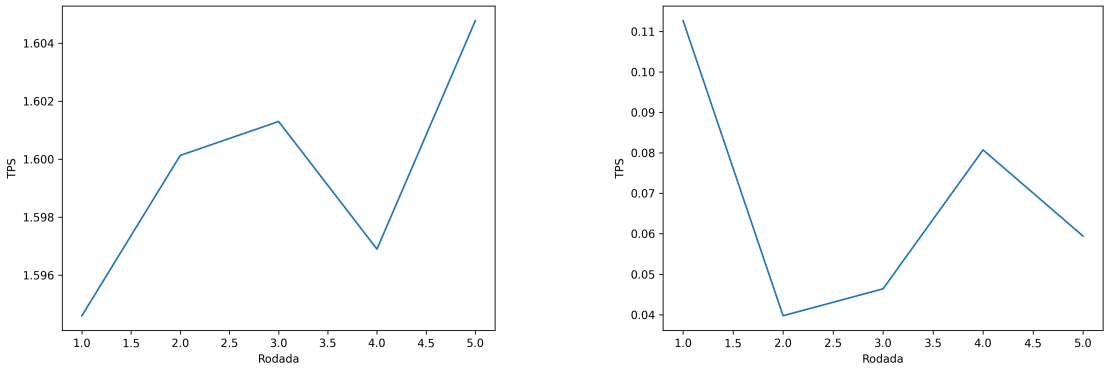
A avaliação de desempenho considerou os percentis de latência de confirmação das transações (p50, p95 e p99), a taxa de processamento em transações por segundo (TPS) e o coeficiente de variação (CV) da latência entre as rodadas. Cada rodada experimental foi composta por 200 operações de escrita realizadas por até 10 dispositivos simultâneos. Para reduzir efeitos de variações pontuais, o valor final de cada percentil corresponde à mediana dos percentis obtidos ao longo das rodadas executadas.

A Tabela 2 apresenta a comparação entre os cenários avaliados. Na execução da blockchain na borda da rede, as latências permaneceram abaixo de 200 ms, com valores de 121 ms, 145 ms e 158,1 ms para p50, p95 e p99, respectivamente. No cenário em nuvem, as latências foram substancialmente maiores, com p50 de 11.942 ms e p99 de 22.129,2 ms. A diferença também se refletiu no throughput, com 1,599 TPS na borda e 0,059 TPS na nuvem. O CV da latência também foi menor na borda (0,132–0,163) do que na nuvem (0,364–0,932), indicando maior previsibilidade no tempo de confirmação das transações.

Métrica	Blockchain na borda	Blockchain na nuvem
Latência p50 (ms)	121.0	11 942.0
Latência p95 (ms)	145.0	20 414.2
Latência p99 (ms)	158.1	22 129.2
TPS mediano (tx/s)	1.599	0.059
CV da latência	0,132–0,163	0,364–0,932

Table 2. Resultados de desempenho por cenário

A Figura 2 reforça a maior estabilidade da borda, enquanto a nuvem apresentou menor TPS e maior variabilidade, efeito associado à dependência de uma rede pública de testes.



(a) Blockchain na borda (b) Blockchain na nuvem

Figure 2. Evolução do throughput (TPS) nas abordagens avaliadas.

5.2. Casos de teste dos mecanismos de segurança

Os mecanismos de segurança foram avaliados por meio de testes funcionais voltados à autenticação, integridade e privacidade dos registros de geolocalização. Na autenticação, o

smart contract rejeitou transações sem autenticação prévia ou com token inválido, aceitando apenas registros associados a credenciais válidas, conforme ilustrado nas Figuras 3(a), 3(b) e 3(c).

```
node-1  | eth_estimateGas
node-1  |   Contract call:       DeviceAuthGeo#recordLocation
node-1  |   From:                0xf39fd6e51aad88f6f4ce6ab8827279cfffb92266
node-1  |   To:                  0x5fbdb2315678afecb367f032d93f642f64180aa3
node-1  |   Value:               0 ETH
node-1  |
node-1  |   Error: reverted with reason string 'not authenticated'
node-1  |
```

(a) Tentativa de registro sem autenticação prévia.

```
node-1  | eth_estimateGas
node-1  |   Contract call:       DeviceAuthGeo#recordLocation
node-1  |   From:                0xf39fd6e51aad88f6f4ce6ab8827279cfffb92266
node-1  |   To:                  0x5fbdb2315678afecb367f032d93f642f64180aa3
node-1  |   Value:               0 ETH
node-1  |
node-1  |   Error: reverted with reason string 'invalid token'
node-1  |
```

(b) Tentativa de registro com token inválido.

```
node-1  |   Contract call:       DeviceAuthGeo#recordLocation
node-1  |   Transaction:         0xcce9f1516e06d245fb9647c02581ad42d00c4ad1508312708bcdade40232ef9d
node-1  |   From:                0xf39fd6e51aad88f6f4ce6ab8827279cfffb92266
node-1  |   To:                  0x5fbdb2315678afecb367f032d93f642f64180aa3
node-1  |   Value:               0 ETH
node-1  |   Gas used:            31813 of 31813
node-1  |   Block #21:           0x00943f149ea09cbb50d8ffcda4c3351d68f6c345a78ef9a5448ea1c4532eb4da
node-1  |
```

(c) Registro realizado com token válido.

Figure 3. Evidência dos registros de autenticação no *smart contract*.

A integridade foi verificada por meio da ancoragem periódica do *hash* do último bloco da blockchain local em uma rede pública. Como apresentado na Figura 4, esse registro permite comparar posteriormente o estado da cadeia local com o valor ancorado externamente, fornecendo evidência de preservação da integridade após a ancoragem.

```
On-chain latestSequence(edgeChainId): 0
OK seq=1 edgeBlock=212 latency_ms=5648 tx=0x05a46b96...
OK seq=2 edgeBlock=212 latency_ms=26505 tx=0x4edf13d0...
OK seq=3 edgeBlock=250 latency_ms=26553 tx=0xff887e0b...
OK seq=4 edgeBlock=307 latency_ms=26575 tx=0xafce56c7...
```

Figure 4. *Log* do registro de ancoragem do estado da blockchain na borda.

A privacidade foi tratada por meio de um *pseudoId* criptográfico rotacionado, calculado por $pseudoId = keccak256(deviceId \parallel token \parallel batch)$. Esse mecanismo evita a exposição direta do identificador real do dispositivo e reduz a correlação contínua dos registros ao longo do tempo.

6. Conclusão

Este trabalho apresentou um framework baseado em blockchain para aplicações IoT com dados de geolocalização, explorando a execução de nós na borda da rede e mecanismos de autenticação, integridade e pseudonimização. A avaliação experimental indicou que a

execução na borda reduziu a latência, aumentou o throughput e apresentou maior previsibilidade em comparação ao cenário em nuvem, reforçando o impacto da proximidade dos nós blockchain no desempenho da aplicação.

Os testes funcionais evidenciaram a viabilidade dos mecanismos avaliados, incluindo controle de acesso por *smart contracts*, ancoragem em blockchain pública e uso de identificadores pseudonimizados. Como limitações, destaca-se que os dispositivos foram simulados, que o baseline em nuvem utilizou uma rede pública de testes sujeita a variáveis externas e que o throughput obtido não permite generalizar a proposta para implantações com muitos dispositivos sem estratégias adicionais de escalabilidade.

Como trabalhos futuros, pretende-se comparar a proposta com blockchains permissionadas, avaliar infraestruturas privadas em nuvem, investigar particionamento ou múltiplos nós de borda e aprofundar a análise formal de segurança e privacidade.

References

Dedeoglu, V., Jurdak, R., Putra, G. D., Dorri, A., and Kanhere, S. S. (2019). A trust architecture for blockchain in iot. In *Proceedings of the 16th EAI international conference on mobile and ubiquitous systems: computing, networking and services*, pages 190–199.

Khalid, U., Asim, M., Baker, T., Hung, P. C., Tariq, M. A., and Rafferty, L. (2020). A decentralized lightweight blockchain-based authentication mechanism for iot systems. *Cluster Computing*, 23(3):2067–2087.

Li, D., Hu, Y., and Lan, M. (2020). Iot device location information storage system based on blockchain. *Future Generation computer systems*, 109:95–102.

Liang, H., Wu, J., Zheng, X., Zhang, M., Li, J., and Jolfaei, A. (2020). Fog-based secure service discovery for internet of multimedia things: a cross-blockchain approach. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, 16(3s):1–23.

Peelam, M. S., Shah, K., and Chamola, V. (2024). V-track: blockchain-enabled iot system for reliable vehicle location verification. *Digital Communications and Networks*.

Ren, Y., Huang, D., Wang, W., and Yu, X. (2023). Bsmd: A blockchain-based secure storage mechanism for big spatio-temporal data. *Future Generation Computer Systems*, 138:328–338.

Sun, Z., Wang, Y., Cai, Z., Liu, T., Tong, X., and Jiang, N. (2021). A two-stage privacy protection mechanism based on blockchain in mobile crowdsourcing. *International Journal of Intelligent Systems*, 36(5):2058–2080.

Wu, W., Liu, E., Gong, X., and Wang, R. (2020). Blockchain based zero-knowledge proof of location in iot. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pages 1–7. IEEE.

Yao, Y., Zhang, H., Lin, L., Lin, G., Shibasaki, R., Song, X., and Yu, K. (2022). Internet of things positioning technology based intelligent delivery system. *IEEE Transactions on Intelligent Transportation Systems*.

Zafar, F., Khan, A., Anjum, A., Maple, C., and Shah, M. A. (2020). Location proof systems for smart internet of things: Requirements, taxonomy, and comparative analysis. *Electronics*, 9(11):1776.

Zhang, J., Yang, F., Ma, Z., Wang, Z., Liu, X., and Ma, J. (2020). A decentralized location privacy-preserving spatial crowdsourcing for internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 22(4):2299–2313.