

# COTTONTRUST: Análise dos Tempos de Criação de Entidades com Base em Identidades Autossoberanas

Gilson S. Junior<sup>1</sup>, Gabriel F. C. Da Silva<sup>1</sup>, Janaína F. B. Duarte<sup>1</sup>, Maurício A. Pillon<sup>1</sup>

<sup>1</sup> Departamento de Ciência da Computação (DCC)  
Universidade do Estado de Santa Catarina (UDESC)

{gilson.sj, gabriel.silva111, janaina.duarte}@edu.udesc.br  
mauricio.pillon@udesc.br

**Resumo.** A rastreabilidade dos produtos, bem como o uso de selos de certificação, tornaram-se essenciais para satisfazer as expectativas dos consumidores por segurança, sustentabilidade, qualidade e transparência nas cadeias de suprimentos. Atualmente, a maioria dos sistemas de informação dessas cadeias opera com sistemas centralizados, ou explora a tecnologia blockchain como uma solução potencial para aprimorar a integridade e rastreabilidade na cadeia. No entanto, desafios como fragmentação de dados, vulnerabilidades, custos de implementação e preocupações com privacidade de dados são obstáculos para essas soluções. Dessa forma, o artigo explora o uso das Identidades Autossoberanas (SSI), especificamente no projeto COTTONTRUST, que adota a SSI para melhorar a integridade e rastreabilidade da cadeia algodoeira. O foco está na análise dos tempos de transação para criar identidades autossoberanas da cadeia do algodão, avaliando a escalabilidade do COTTONTRUST.

## 1. Introdução

Nos últimos anos, a rastreabilidade dos produtos tornou-se crucial para atender as demandas dos consumidores por segurança, sustentabilidade, qualidade e transparência nas cadeias de suprimentos. Os selos de certificação desempenham um papel importante para aumentar a transparência ao longo dessas cadeias e informar sobre a qualidade, segurança e sustentabilidade dos produtos. No entanto, a impressão desses selos nos produtos facilita a falsificação, comprometendo sua confiabilidade, e não há uma maneira fácil para os consumidores verificarem a autenticidade dessas informações.

Atualmente, a maioria dos sistemas de informação da cadeia algodoeira coleta, transmite e armazena registros em sistemas centralizados, ou utiliza a tecnologia blockchain como uma solução potencial para aprimorar a integridade e rastreabilidade na cadeia [Cocco et al. 2021, Agrawal et al. 2021, Hader et al. 2022, Sezer et al. 2022, Malik et al. 2021, Manoj et al. 2023]. No entanto, desafios persistem pois os sistemas centralizados criam silos de dados fragmentados, vulneráveis a falhas únicas, e os custos de implementação, juntamente com preocupações com regulamentações de privacidade de dados, representam barreiras significativas para implementar soluções baseadas em blockchain. Essas limitações apresentam desafios para estabelecer fatores de confiança, como transparência, rastreabilidade, integridade e privacidade entre os intervenientes envolvidos na cadeia algodoeira.

Neste contexto, o COTTONTRUST é um projeto que aborda os desafios mencionados, explorando os conceitos de SSI [Preukschat and Reed 2021]. Em contraste com as abordagens convencionais, a SSI descentraliza o controle e a propriedade de informações pessoais, oferecendo potencial para aprimorar a confiança, rastreabilidade e verificabilidade na cadeia do algodão. Desta forma, este artigo analisa os tempos envolvidos nas transações para criação das identidades das entidades autossoberanas, que fazem parte da cadeia algodoeira, com foco na

escalabilidade do COTTONTRUST, e está organizado da seguinte forma: (i) a Seção 2 introduz o COTTONTRUST; (ii) a Seção 3 detalha o ambiente experimental; (iii) a Seção 4 discute os resultados obtidos e, por fim, a Seção 5 apresenta as considerações finais e os trabalhos futuros.

## 2. COTTONTRUST

O COTTONTRUST é uma arquitetura descentralizada baseada no modelo SSI, implementada por meio da blockchain Hyperledger Indy, com o objetivo de alcançar rastreabilidade, confiabilidade e verificabilidade na cadeia algodoeira. O COTTONTRUST adota uma abordagem de *design* de sistema que conceitua a cadeia algodoeira como uma rede interconectada de nós (entidades participantes da cadeia). A Figura 1 mostra parte dessa cadeia, focando a produção e comercialização de fardos de algodão.

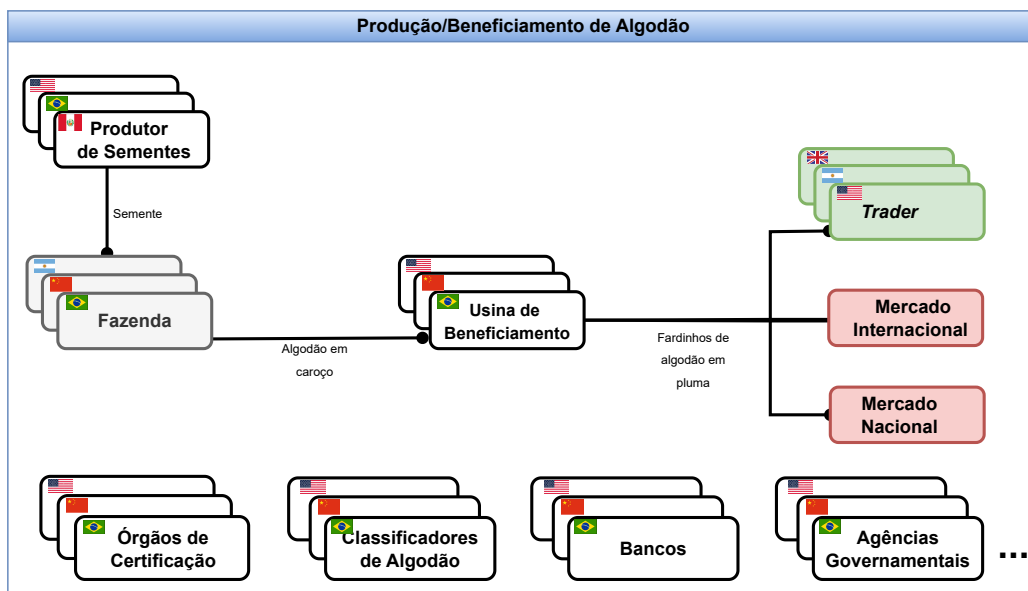


Figura 1. Cadeia Algodoeira.

As entidades participantes da cadeia incluem: (i) Produtor de Sementes; (ii) Fazenda; (iii) Usina de Beneficiamento; (iv) *Trader* (intermedia a negociação e comércio de algodão); (v) Compradores do Mercado Internacional; (vi) Compradores do Mercado Nacional; (vii) Órgãos Certificadores; (viii) Classificadores de Algodão (especialistas credenciados que avaliam e classificam o algodão); (ix) Bancos e (x) Agências Governamentais. Por natureza, a cadeia algodoeira é inerentemente descentralizada, conforme evidenciado na Figura 1, alinhando-se aos princípios do SSI.

## 3. Análise experimental

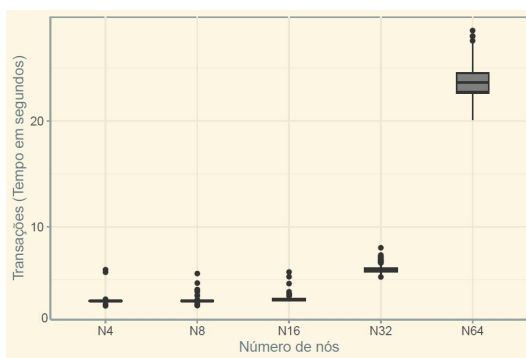
O protótipo do COTTONTRUST retrata um cenário simplificado de produção e venda de fardinhos de algodão, originados de uma fazenda, processados por uma usina de beneficiamento e negociados com um cliente do mercado internacional. Na prática, várias entidades podem se envolver em cada etapa da cadeia produtiva. Cada entidade inicia sua participação registrando-se na blockchain, criando seu DID e obtendo sua carteira digital. Isso marca a fase inicial das transações envolvendo operações de escrita no livro-razão, fase esta que é objeto de análise deste trabalho.

O protótipo foi implementado em uma máquina física com as seguintes especificações: 148 GB de RAM e um processador Intel(R) Xeon(R) CPU E5-2620 v2 @ 2,10 GHz, com 4 núcleos físicos e um total de 8 núcleos lógicos. O sistema operacional utilizado foi Linux Ubuntu Focal Fossa 20.04.6 LTS, com Kernel Linux 5.4.0-164-generic. As ferramentas empregadas incluíram Docker na versão 24.0.6 (compilação ed223bc), Docker-Compose 1.25.0, Docker-py 4.1.0 e Python3 3.8.10. Na avaliação de desempenho do protótipo, adotou-se o tempo total de transação como a métrica principal para medir a eficiência nas transações. Os testes visam avaliar a escalabilidade do sistema e seu comportamento sob diferentes cargas de transação, com resultados esperados para obter uma compreensão mais aprofundada sobre a eficiência, escalabilidade e a capacidade do COTTONTRUST gerenciar efetivamente seus recursos.

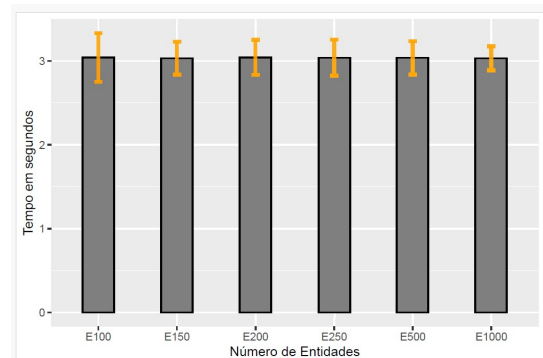
O primeiro cenário experimental consiste no registro de 100 entidades na blockchain, abrangendo a geração dos DIDs e o estabelecimento de consenso, com variação no número de nós (4, 8, 16, 32 e 64). Enquanto o segundo cenário experimental envolve a variação da quantidade de entidades (100, 150, 200, 250, 500, 1000), mantendo 64 nós para o consenso na blockchain. Todos os resultados são derivados da média de 10 iterações de execução.

#### 4. Discussão de resultados

Inicialmente, ao analisar o primeiro cenário experimental no qual o tempo total de transação é resumido pelo número de nós na blockchain (Figura 2), observou-se uma variação no tempo de transação à medida que o número de nós aumenta. Apesar dos resultados para 4, 8 e 16 nós mostrarem uma estabilidade relativamente constante, com tempos de transação consistentes em torno de 3s, o leve aumento no tempo de transação ao passar de 16 para 32 nós pode indicar um ponto de transição onde a complexidade da rede começa a impactar marginalmente o desempenho. Ao expandir de 32 para 64 nós, observou-se um aumento no tempo de transação, sugerindo uma possível influência do aumento da complexidade da rede. Essa tendência está relacionada à necessidade de consenso entre os nós para validar e registrar transações na blockchain, pois à medida que o número de nós aumenta, a complexidade do consenso também aumenta, uma vez que mais entidades precisam concordar sobre a validade das transações.



**Figura 2. Tempo de transação variando o número de nós**



**Figura 3. Tempo de transação variando o número de entidades**

Ao analisar os resultados do segundo cenário experimental (Figura 3), no qual o número de entidades foi variado mantendo-se 64 nós para o consenso na blockchain, observou-se uma consistência nos tempos de processamento. Independentemente do aumento gradativo na quantidade de entidades envolvidas, os tempos de consenso permaneceram praticamente constantes.

Esta uniformidade nos tempos de processamento sugere uma capacidade estável de processamento da rede, mesmo diante de variações na quantidade de entidades envolvidas e pode indicar uma boa escalabilidade vertical do COTTONTRUST, demonstrando sua capacidade de lidar eficientemente com um aumento no volume de transações sem comprometer significativamente o tempo de processamento.

## 5. Considerações finais e trabalhos futuros

O COTTONTRUST é uma arquitetura transparente e descentralizada, projetada para fornecer ferramentas de verificação de selos de certificação e rastreamento da cadeia algodoeira, baseada em SSI. O artigo analisa os tempos de transação para criar identidades autossobranas na cadeia algodoeira, avaliando sua escalabilidade. Para as próximas etapas de curto prazo, planeja-se a ampliação da variabilidade de nós no primeiro cenário experimental, com o intuito de observar se o aumento do tempo de transação segue uma tendência exponencial, ou tenderá a alcançar um equilíbrio. Para as direções de longo prazo, estão previstas análises de outros cenários de testes do COTTONTRUST, bem como análises comparativas variando o algoritmo de consenso, com foco na escalabilidade do sistema.

## Agradecimentos

Este trabalho é apoiado financeiramente pela Fundação de Amparo à Pesquisa e Inovação do Estado de Santa Catarina (FAPESC), Universidade do Estado de Santa Catarina (UDESC) e Laboratório de Processamento Paralelo e Distribuído (LabP2D).

## Referências

- Agrawal, T. K., Kumar, V., Pal, R., Wang, L., and Chen, Y. (2021). Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. *Computers & Industrial Engineering*, 154:107130.
- Cocco, L., Tonelli, R., and Marchesi, M. (2021). Blockchain and self sovereign identity to support quality in the food supply chain. *Future Internet*, 13(12):301.
- Hader, M., Tchoffa, D., Mhamedi, A. E., Ghodous, P., Dolgui, A., and Abouabdellah, A. (2022). Applying integrated blockchain and big data technologies to improve supply chain traceability and information sharing in the textile sector. *Journal of Industrial Information Integration*, 28:100345.
- Malik, S., Gupta, N., Dedeoglu, V., Kanhere, S. S., and Jurdak, R. (2021). Tradechain: Decoupling traceability and identity in blockchain enabled supply chains. In *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 1141–1152. IEEE.
- Manoj, T., Makkithaya, K., and Narendra, V. (2023). A blockchain-based credentials for food traceability in agricultural supply chain. In *2023 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*, pages 19–24. IEEE.
- Preukschat, A. and Reed, D. (2021). *Self-sovereign identity*. Manning Publications.
- Sezer, B. B., Topal, S., and Nuriyev, U. (2022). Tppsupply : A traceable and privacy-preserving blockchain system architecture for the supply chain. *Journal of Information Security and Applications*, 66:103116.