IMPLEMENTAÇÃO DE *BLOCKCHAIN* PARA RASTREABILIDADE NA CADEIA DE SUPRIMENTOS DA SOJA: UM ESTUDO DE CASO COM CONTRATOS INTELIGENTES

Matheus Oliveira Bitencourt Dos Santos [1]
Ricardo Zampolo Bertolucci Cruz [1]
Charles Boulhosa Rodamilans [1]

[1]Faculdade de Computação e Informática (FCI)
Universidade Presbiteriana Mackenzie São Paulo, SP – Brasil

<10390698,10389251@mackenzista.com.br>
<charles.rodamilans@mackenzie.br>

2024

Resumo

O setor agroindustrial enfrenta desafios para rastrear insumos ao longo da cadeia de suprimentos, devido à complexidade e ao envolvimento de diversas empresas. Este estudo investiga o uso de blockchain e contratos inteligentes para aprimorar a rastreabilidade na cadeia de suprimentos de soja, abordando questões de transparência, segurança, automação e segurança alimentar. Para isso, foi realizada uma análise de como a blockchain pode resolver estes desafios de rastreabilidade e foi desenvolvida uma aplicação web integrada com um contratos inteligente para registrar e rastrear a transação na cadeia de suprimento de soja de forma eficiente e transparente. O modelo proposto conseguiu fornecer uma maior transparência e confiabilidade, além de sincronização e integração, facilitando a interação entre as partes envolvidas na transação de soja.

Palavras-chave: *Blockchain*, Rastreabilidade Agrícola, Contratos Inteligentes, Cadeia de Suprimentos.

Abstract

The agro-industrial sector faces challenges in tracking inputs along the supply chain due to its complexity and the involvement of various companies. This study investigates the use of blockchain and smart contracts to enhance traceability in the soybean supply chain, addressing issues of transparency, security, automation, and food safety. To achieve this, an analysis was conducted on how blockchain can resolve these traceability challenges, and a web application integrated with a smart contract was developed to efficiently and transparently register and track transactions in the soybean supply chain. The proposed model was able to provide greater transparency and reliability, as well as synchronization and integration, facilitating interaction between the parties involved in the soybean transaction.

Keywords: Blockchain, Agricultural Traceability, Smart Contracts, Supply Chain.

1 Introdução

A cadeia de suprimentos de soja enfrenta desafios complexos em termos de rastreabilidade e transparência, exacerbados pela expansão global do mercado de soja e suas diversas aplicações, de alimentos a biocombustíveis (SHAKHBULATOV et al., 2020). A eficácia dos sistemas de rastreabilidade é crítica para garantir a segurança alimentar, conformidade com as regulamentações ambientais e sustentabilidade das práticas agrícolas (LIN et al., 2019). Contudo, os métodos tradicionais frequentemente falham em prover uma visibilidade completa e confiável devido à fragmentação e à falta de integração entre os diversos elos da cadeia (JABBAR et al., 2021).

Essa ineficiência dos sistemas convencionais de rastreabilidade na cadeia de suprimentos de soja poderia ser resolvida pela adoção da tecnologia *blockchain*, que utilizada de forma correta, pode superar essas limitações e oferecer um registro imutável e descentralizado das transações, o que siginifica uma melhorara significativa na integridade, na segurança e na confiança nos produtos de soja (SALAH et al., 2019).

Essa pesquisa tem como foco avaliar o impacto da implementação da tecnologia *blockchain* na rastreabilidade da cadeia de suprimentos de soja, utilizando principalmente pelo modelo proposto por (SALAH et al., 2019). Os objetivos específicos são:

1. Entender os principais desafios na rastreabilidade da cadeia de suprimentos de soja.
2. Analisar como a *blockchain* pode resolver esses desafios.
3. Desenvolver uma aplicação com *smart contracts* visando resolver o problema da rastreabilidade.

Esta pesquisa visa fornecer um estudo detalhado sobre a aplicação da tecnologia *blockchain* em um segmento específico da agricultura, com implicações para teorias de gestão de cadeias de suprimentos e inovação tecnológica, além de oferecer às organizações agrícolas uma ferramenta para melhorar a sustentabilidade e a segurança alimentar.

2 Referencial teórico na cadeia de suprimentos

A cadeia de suprimentos, ou *supply chain* em inglês, refere-se à rede de todas as entidades, atividades, recursos e tecnologias envolvidas no processo de produção e distribuição de um produto ou serviço desde a origem até o consumidor final. Isso inclui a obtenção de matérias-primas, a produção, o armazenamento, a gestão de estoques, o transporte e a entrega dos produtos ou serviços ao cliente (MARKUS; BUIJS, 2022).

O objetivo principal da gestão da cadeia de suprimentos é otimizar e sincronizar os processos internos e externos para maximizar a eficiência e reduzir custos, mantendo ao mesmo tempo a qualidade e a satisfação do cliente.

Porém a cadeia de suprimentos agrícola enfrenta desafios significativos, incluindo a variabilidade de condições de produção devido a fatores climáticos, a necessidade de coordenação entre numerosos agentes, desde pequenos agricultores até grandes corporações globais, e a complexidade logística de transportar produtos perecíveis em condições adequadas. Ademais, questões como fraude, perda de matéria-prima e ineficiências logísticas são recorrentes, exigindo soluções robustas para garantir a eficiência e a integridade da cadeia (JABBAR et al., 2021).

2.1 A importância da cadeia de suprimentos no agronegócio

No agronegócio, a cadeia de suprimentos desempenha um papel fundamental, pois conecta produtores agrícolas com mercados globais, garantindo que produtos como alimentos, fibras e combustíveis cheguem aos consumidores de maneira eficiente e sustentável. Uma gestão eficaz da cadeia de suprimentos é crucial para maximizar a produtividade e a rentabilidade, ao mesmo tempo em que minimiza os impactos ambientais e garante a conformidade com as regulamentações cada vez mais rigorosas em termos de segurança alimentar e práticas sustentáveis (GEORGE et al., 2019). A capacidade de rastrear a origem e o manejo de produtos agrícolas, do campo à mesa, não só aumenta a confiança do consumidor, mas também permite uma resposta rápida a problemas de qualidade e segurança (SHAKHBULATOV et al., 2020).

2.2 *Blockchain* como solução para a rastreabilidade

O *blockchain* (YAGA et al., 2018) surge como uma solução para os desafios enfrentados na cadeia de suprimentos agrícola. Com sua capacidade de fornecer um registro transparente, imutável e descentralizado de todas as transações, o *blockchain* pode reduzir as perdas de matéria-prima e combater a fraude, ao mesmo tempo que facilita uma maior automação e eficiência na rastreabilidade de produtos. Sistemas baseados em *blockchain* podem ajudar a garantir que todos os envolvidos na cadeia de suprimentos — de agricultores a distribuidores e varejistas — tenham acesso a informações precisas e em tempo real sobre o movimento de produtos, contribuindo para uma gestão mais eficaz e para a redução de extravios e desperdícios (SALAH et al., 2019). A implementação do *blockchain* no agronegócio pode ajudar o setor trazendo benefícios tangíveis não apenas para os produtores e distribuidores, mas também para os consumidores, que demandam cada vez mais transparência e responsabilidade das práticas agrícolas (DUTTA et al., 2020).

A Figura 1 apresenta a cadeia de suprimento agrícola integrada a um contrato inteligente baseado em Ethereum. O sistema conecta fazendeiros, empresas de sementes, elevadores de grãos, processadores, distribuidores, varejistas e clientes. Todas as transações,

desde a compra de sementes até a venda ao consumidor final, são registradas no contrato inteligente. O funcionamento do *blockchain* para a implementação eficaz de um contrato inteligente é apresentado a seguir.

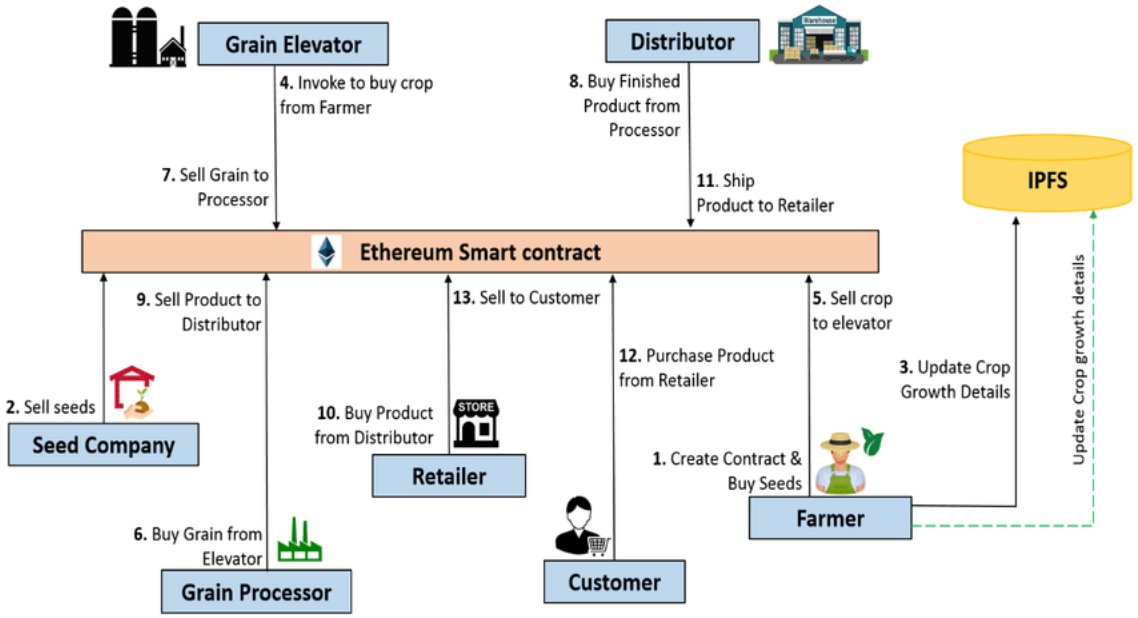

Figura 1 – Visão geral do sistema (SALAH et al., 2019).

2.3 Blockchain

O conceito de *blockchain* foi definido no final dos anos 80 com Leslie Lamport, ele elaborou o protocolo Paxos, que propôs um modelo de consenso para redes de computadores. Porém apenas em 2008 com Satoshi Nakamoto, pseudônimo por trás da criação do Bitcoin, combinou esses conceitos com outras tecnologias e conceitos computacionais para criar a primeira aplicação moderna de *blockchain*: uma forma de dinheiro eletrônico *peer-to-peer*. Como afirmado no documento, "O papel de Nakamoto continha o esquema que a maioria dos esquemas de criptomoeda moderna segue (embora com variações e modificações)."(YAGA et al., 2018).

Uma *blockchain* é composta por uma série de elementos inter-relacionados que sustentam sua estrutura e funcionalidade em um ambiente descentralizado, entre eles os principais elementos são (YAGA et al., 2018):

- Funções Criptográficas de *Hash*: As funções de *hash* criptográfico são usadas para calcular uma saída única para dados de entrada, garantindo a integridade dos dados através de suas propriedades de resistência a pré-imagem, segunda pré-imagem e colisão, veja o exemplo com a criptográfia SHA-256, criptográfia que a *bitcoin* utiliza (Figura 2).

- Transações: No contexto das criptomoedas, as transações representam a transferência de ativos digitais entre usuários da rede *blockchain*. Cada bloco em uma *blockchain* pode conter zero ou mais transações, sendo estas fundamentais para a transferência de valor e o registro de atividades.

Texto de entrada	Saida com a criptografia SHA-256 aplicada
1	0x6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	0xd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
Hello, World!	0xdffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

Figura 2 – Exemplos de entrada e saída do SHA-256. Traduzido de (YAGA et al., 2018).

- Endereços e Derivação de Endereços: "Algumas redes *blockchain* fazem uso de um endereço, que é uma sequência curta e alfanumérica de caracteres derivados da chave pública do usuário"(YAGA et al., 2018).

  Os endereços são utilizados como identificadores públicos na rede *blockchain* e são derivados das chaves públicas dos usuários através de funções criptográficas de *hash*.

- Criptografia Assimétrica: A criptografia assimétrica envolve um par de chaves - uma pública e uma privada - permitindo a verificação da autenticidade das transações e fornecendo uma relação de confiança entre usuários desconhecidos.

- Blocos (*Blocks*): Cada bloco contém um cabeçalho e dados do bloco, com o cabeçalho incluindo metadados como número do bloco, *hash* do bloco anterior e *timestamp*. Os dados do bloco consistem em uma lista de transações validadas.

- Encadeamento de Blocos (*Chaining Blocks*): Este encadeamento torna possível detectar e rejeitar blocos alterados, garantindo a imutabilidade e integridade do *blockchain* (Figura 3).

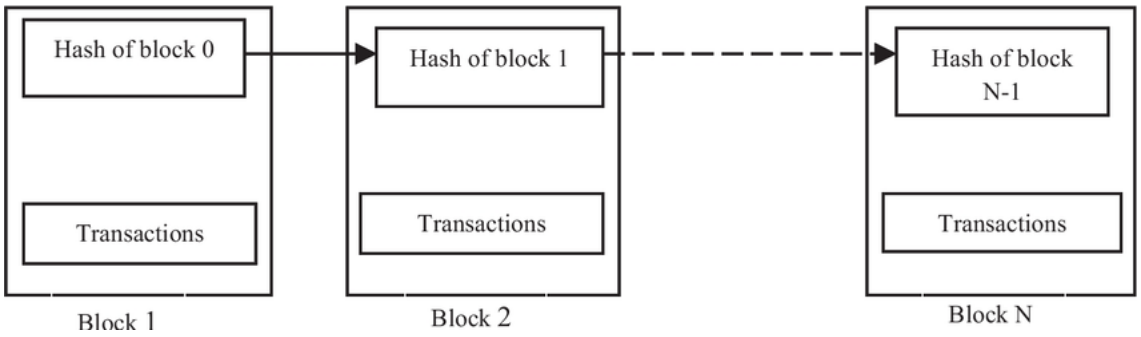

Figura 3 – Encadeamento dos blocos (CHAKRABORTY; GHOSH; PRATAP, 2023).

A *blockchain* combinada com contratos inteligentes, permite resolver desafios específicos, como a rastreabilidade. A *blockchain* oferece uma infraestrutura descentralizada e segura, enquanto os contratos inteligentes permitem a automação e o registro transparente das transações. Esse conjunto de tecnologias pode superar as dificuldades de rastreabilidade na cadeia de suprimentos, garantindo que todas as etapas da transação sejam monitoradas, registradas e validadas de forma eficiente e imutável, aumentando a confiança e a transparência entre as partes envolvidas.

2.4 Contratos inteligentes

Contratos inteligentes, conceituados inicialmente por Nick Szabo em 1994, são protocolos automatizados que executam os termos de um contrato (YAGA et al., 2018).

Quanto ao seu *design*, visa cumprir condições contratuais enquanto minimiza exceções e a necessidade de intermediários (YAGA et al., 2018).

Esses contratos utilizam a tecnologia *blockchain*, compreendendo código e dados implantados por meio de transações criptografadas na rede *blockchain*. Sua execução envolve todos os nós dentro da rede, garantindo consenso e registrando resultados na *blockchain*.

Os usuários interagem com os contratos inteligentes criando transações que invocam funções públicas dentro do contrato, possibilitando diversos serviços como cálculos, armazenamento de informações e transferências automáticas de fundos. Notavelmente, os contratos inteligentes não precisam se limitar a funções financeiras, conforme demonstrado por sua aplicação na geração de números aleatórios.

Em redes *blockchain* permissionadas como o Ethereum (DABBAGH et al., 2021), os usuários incorrem em custos para executar o código do contrato inteligente para evitar abusos e consumo de recursos. Por outro lado, redes privada como o Hyperledger Fabric (DABBAGH et al., 2021) podem não impor tais custos, dependendo de participantes conhecidos e de mecanismos alternativos para prevenir comportamentos maliciosos.

Por meio da integração com tecnologias como Ethereum, os contratos inteligentes automatizam transações, eliminam intermediários e asseguram a imutabilidade dos registros. Isso permite que todas as partes envolvidas – desde fazendeiros até consumidores finais – tenham acesso a informações verificáveis e confiáveis sobre a origem e o estado dos produtos. Essa abordagem reduz custos, aumenta a eficiência operacional e promove a confiança entre os participantes, se tornando uma possível solução para problemas de controle, rastreamento e gerenciamento na cadeia de suprimento de soja e outros produtos agrícolas.

3 Metodologia

O estudo propõe compreender as tecnologias de *blockchain* e contratos inteligentes para solucionar o problema de rastreabilidade na cadeia de suprimentos de soja. Primeiramente, buscou-se entender os desafios na rastreabilidade. Em seguida, realizou-se uma análise de como a *blockchain* pode resolver estes desafios. Por fim, foi desenvolvida uma aplicação baseada em contratos inteligentes para registrar e rastrear essas etapas de forma eficiente e transparente. A aplicação foi baseada no modelo de (SALAH et al., 2019) (Figura 4), com foco nos agentes fazendeiro (Farmer) e distribuidor (Distributor), devido à sua importância na rastreabilidade. O fazendeiro insere dados iniciais sobre a produção, enquanto o distribuidor gerencia a logística e entrega. Foram realizadas adaptações para nos nomes dos agentes, onde fazendeiro se transformou em vendedor, enquanto distribuídor se tornou comprador.

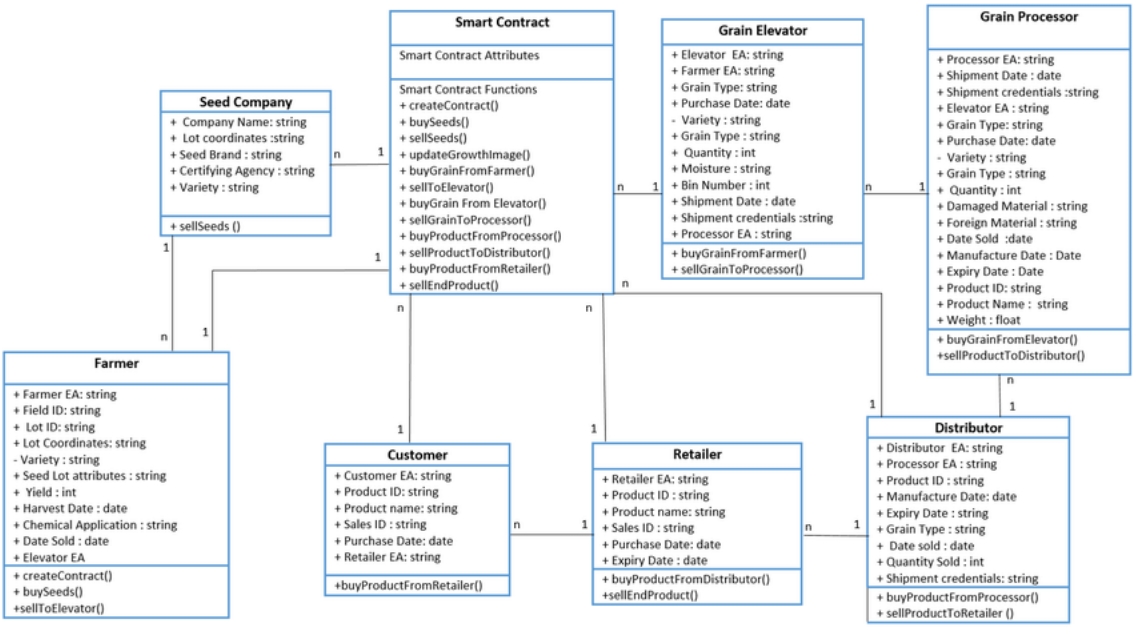

Figura 4 – Diagrama de classe (SALAH et al., 2019).

4 Resultados e discussão

Como resultado da pesquisa se obteve o contrato inteligente nomeado `SoybeanTrade` desenvolvido na *blockchain Ethereum*, utilizando da linguagem de programação *Solidity* , (Solidity Team, 2021), operando na versão 0.8.0 do compilador. O projeto desenvolvido pode ser encontrado em (CRUZ; SANTOS, 2024).

A Figura 5 apresenta uma representação visual dos componentes implementados no contrato `SoybeanTrade`, incluindo as entidades Contrato, Produtor, e Consumidor, bem como as ferramentas e tecnologias integradas: *Hardhat, (Nomic Foundation, 2022), MetaMask, (ConsenSys, 2022), e Ethereum Network*. A implementação se concentrou nas entidades Contrato, Produtor e Consumidor, que constituem a base funcional do sistema. A descrição de cada elemento são apresentadas a seguir.

Contrato: define as regras e lógica para a execução das transações de compra e venda de lotes de soja. Seus atributos incluem informações sobre o lote, status da transação, valores e endereços envolvidos. Métodos principais incluem o registro de lotes, a confirmação de compra e o controle de transferência de fundos.

Produtor: representa o vendedor de soja. Seus atributos incluem o identificador, nome, localização e os lotes disponíveis para venda. Métodos principais incluem o registro de lotes e a confirmação de envio.

Consumidor: representa o comprador. Seus atributos incluem identificador, saldo disponível e histórico de compras. Métodos principais incluem a seleção de lotes, a compra e a confirmação de recebimento.

Hardhat: Utilizado para desenvolvimento, teste e implantação do contrato inteligente.

MetaMask: Ferramenta para autenticação e assinatura de transações, permitindo a interação do usuário com o contrato.

Ethereum Network: Rede *blockchain* utilizada para executar e validar as transações de forma segura e descentralizada.

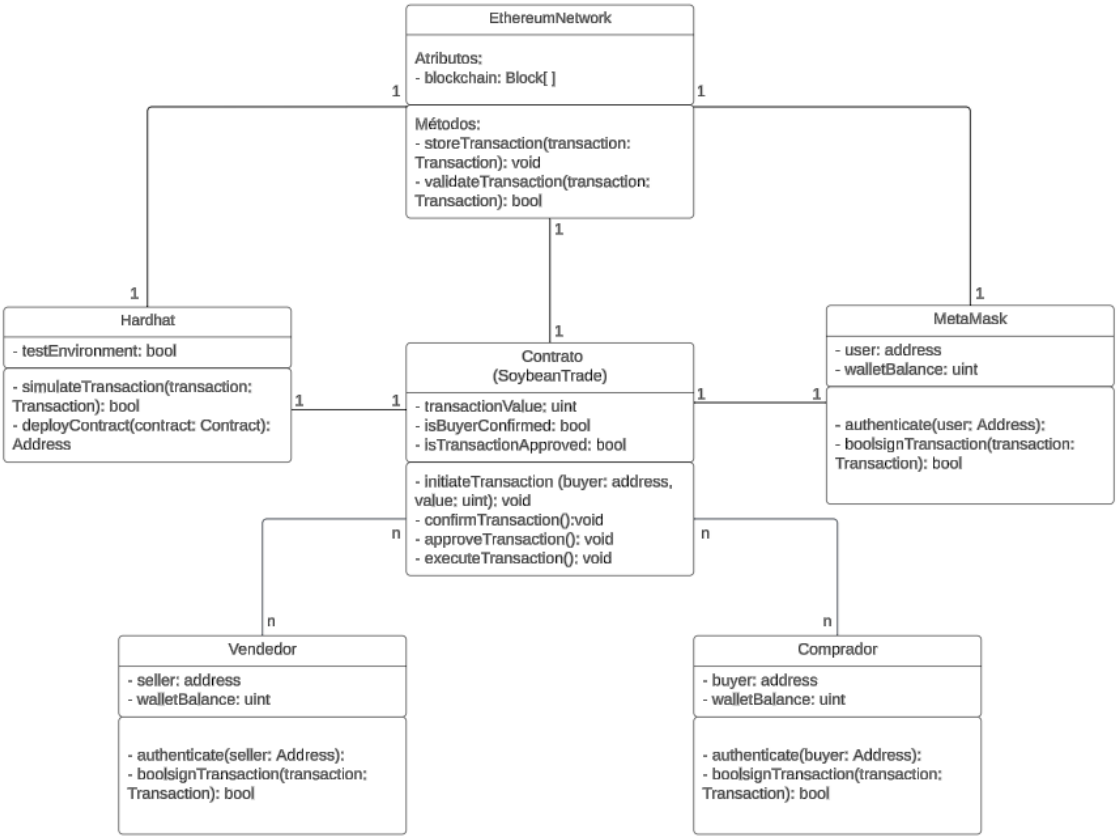

Figura 5 – Elementos do contrato e das ferramentas. Fonte: Autoria própria.

Os resultados obtidos pelo contrato `SoybeanTrade` e implementação da aplicação web foram:

- **Sistema de Transações Seguro e Confiável:** as implementações de segurança garantiram um ambiente de transação seguro, eliminando riscos de ataques comuns e controlando o acesso às funções.
- **Automação e Transparência para os Usuários:** o fluxo de transação foi automatizado, e os estados de cada etapa foram registrados na *blockchain* através de eventos, permitindo que as partes acompanhassem o status da transação em tempo real.
- **Integração com o *front-end*:** a integração com o *front-end* permitiu uma interação intuitiva com o contrato. A interface exibe o status atualizado das transações e notifica o usuário sobre as ações necessárias para a execução da transação.
- **Rastreabilidade e Confiabilidade no Processo de Transação:** com o uso de eventos para cada etapa do processo, o contrato oferece rastreabilidade, permitindo aos usuários verificarem todas as ações e confirmações na *blockchain*.

5 Conclusão

Os resultados demonstraram que o `SoybeanTrade` alcançou, com base no modelo proposto por (SALAH et al., 2019), uma solução eficaz para transações de soja na cadeia de suprimentos com base , promovendo segurança e transparência. Vale salientar que os testes do contrato inteligente `SoybeanTrade` foram inicialmente realizados em um ambiente local, utilizando a ferramenta Hardhat para simular uma *blockchain Ethereum* no computador do desenvolvedor. No entanto, para garantir a robustez e a confiabilidade do sistema em diferentes cenários de uso, é necessário expandir a fase de testes.

O trabalho permitiu aprimorar as soluções relacionadas a segurança, sincronização e integração, garantindo que o `SoybeanTrade` alcançasse os objetivos definidos. O uso de eventos para notificação e o armazenamento de estados proporcionaram transparência e rastreabilidade, enquanto a interface *front-end*, desenvolvida em *React*, facilitou a interação dos usuários com o contrato..

6 Trabalhos Futuros

Apesar do projeto ter conseguido garantir os pontos apresentados anteriormente, ainda faltam alguns tópicos para que ele ser desenvolvido. A seguir estão alguns pontos que podem ser aprimorados e explorados em trabalhos futuros:

- **Testes em máquinas distribuídas e em ambientes distribuídos**: Essa abordagem permitirá avaliar o comportamento do contrato em situações reais de rede, verificar a interoperabilidade entre dispositivos e validar a estabilidade do sistema em diferentes configurações. Essa etapa é essencial para assegurar que o contrato funcione de forma consistente e confiável em condições variadas, aproximando-se do ambiente de produção final;
- **Projeto e Implementação dos demais agentes**: Essa etapa envolverá o desenvolvimento de novos contratos e módulos para abranger outros agentes na cadeia de suprimentos, como transportadores, armazéns e distribuidores. A implementação desses agentes permitirá um sistema mais completo, com funcionalidades adicionais que representam todas as etapas do fluxo de produtos agrícolas;
- **Expansão do Contrato para Múltiplos Produtos**: O contrato atual é específico para transações de soja. Trabalhos futuros poderiam expandir a funcionalidade para abranger múltiplos produtos agrícolas, permitindo um sistema mais versátil e útil para outras partes da cadeia de suprimentos.
- **Sistema de Pagamento com Criptomoedas Alternativas**: A integração de diferentes criptomoedas no contrato, além do Ether, pode proporcionar mais flexibilidade aos usuários. Isso poderia ser implementado por meio de uma funcionalidade que aceita moedas digitais variadas, ampliando o alcance do contrato.
- **Mecanismos de Disputa e Mediação**: Futuras versões do contrato podem incluir um sistema de resolução de disputas para lidar com possíveis problemas entre comprador e vendedor. Esse sistema poderia utilizar contratos inteligentes adicionais para automatizar uma mediação ou mesmo delegar a mediação a uma terceira parte confiável.

- **Auditoria Automática de Transações**: A implementação de um sistema de auditoria automática para verificar transações e fluxos de trabalho pode melhorar a transparência e a conformidade com as normas, agregando valor ao contrato para uso corporativo em grande escala.
- **Integração com *IoT* para Monitoramento em Tempo Real**: A integração com dispositivos *IoT* pode proporcionar dados em tempo real sobre o transporte e armazenamento dos produtos. Isso aumentaria a confiabilidade das transações e forneceria aos compradores informações adicionais sobre a qualidade e localização dos produtos.

Essas sugestões visam aprimorar o contrato `SoybeanTrade`, bem como sua implementação, e estender seu uso para uma gama maior de casos na cadeia de suprimentos, promovendo ainda mais transparência e segurança para os envolvidos.

Referências

CHAKRABORTY, K.; GHOSH, A.; PRATAP, S. Adoption of blockchain technology in supply chain operations: a comprehensive literature study analysis. *Operations Management Research*, Springer, v. 16, n. 4, p. 1989–2007, 2023.

ConsenSys. *MetaMask Documentation*. [S.l.], 2022. Acessado em 8 de setembro de 2024. Disponível em: <https://metamask.io/>.

CRUZ, R. Z. B.; SANTOS, M. O. B. D. *TCCEntrega*. 2024. Disponível em: <https://github.com/RicardoBertolucci/TCCEntrega>.

DABBAGH, M. et al. A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities. *Computers Security*, v. 100, p. 102078, 2021. ISSN 0167-4048. Acessado em 5 de junho de 2024. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404820303515>.

DUTTA, P. et al. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation Research Part E: Logistics and Transportation Review*, v. 142, p. 102067, 2020. ISSN 1366-5545. Acessado em 10 de junho de 2024. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1366554520307183>.

GEORGE, R. V. et al. Food quality traceability prototype for restaurants using blockchain and food quality data index. *Journal of Cleaner Production*, v. 240, p. 118021, 2019. ISSN 0959-6526. Acessado em 10 de agosto de 2024. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0959652619328914>.

JABBAR, S. et al. Blockchain-enabled supply chain: analysis, challenges, and future directions. *Multimedia systems*, Springer, v. 27, p. 787–806, 2021.

LIN, Q. et al. Food safety traceability system based on blockchain and epcis. *IEEE Access*, v. 7, p. 20698–20707, 2019.

MARKUS, S.; BUIJS, P. Beyond the hype: how blockchain affects supply chain performance. *Supply Chain Management: An International Journal*, Emerald Publishing Limited, v. 27, n. 7, p. 177–193, 2022.

Nomic Foundation. *Hardhat Documentation*. [S.l.], 2022. Acessado em 8 de setembro de 2024. Disponível em: <https://hardhat.org/>.

SALAH, K. et al. Blockchain-based soybean traceability in agricultural supply chain. *IEEE Access*, v. 7, p. 73295–73305, 2019.

SHAKHBULATOV, D. et al. How blockchain enhances supply chain management: A survey. *IEEE Open Journal of the Computer Society*, v. 1, p. 230–249, 2020.

Solidity Team. *Solidity Documentation*. [S.l.], 2021. Acessado em 8 de setembro de 2024. Disponível em: <https://docs.soliditylang.org/>.

YAGA, D. et al. *Blockchain Technology Overview*. [S.l.]: NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, 2018.