



UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS DE QUIXADÁ
CURSO DE GRADUAÇÃO EM REDES DE COMPUTADORES

SAMUEL BRANDÃO MAIA LIMA

RASTREABILIDADE DA CADEIA PRODUTIVA DO MEL COM *BLOCKCHAIN*

QUIXADÁ

2023

SAMUEL BRANDÃO MAIA LIMA

RASTREABILIDADE DA CADEIA PRODUTIVA DO MEL COM *BLOCKCHAIN*

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Redes de Computadores do Campus de Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de tecnólogo em Redes de Computadores.

Orientador: Prof. Dr. Antonio Rafael Braga.

QUIXADÁ

2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

- L71r Lima, Samuel Brandão Maia.
Rastreabilidade da cadeia produtiva do mel com blockchain / Samuel Brandão Maia Lima. – 2023.
63 f. : il. color.
- Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Quixadá,
Curso de Redes de Computadores, Quixadá, 2023.
Orientação: Prof. Dr. Antonio Rafael Braga.
1. Blockchain (Base de dados). 2. Rastreabilidade. 3. Mel. 4. Redes de computadores. I. Título.
CDD 004.6
-

SAMUEL BRANDÃO MAIA LIMA

RASTREABILIDADE DA CADEIA PRODUTIVA DO MEL COM *BLOCKCHAIN*

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Redes de Computadores do Campus de Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de tecnólogo em Redes de Computadores.

Aprovada em: 21/07/2023.

BANCA EXAMINADORA

Prof. Dr. Antonio Rafael Braga (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Isac Gabriel Abrahão Bomfim
IFCE Campus Crateús

Prof. Me. Roberto Cabral Rabêlo Filho
Universidade Federal do Ceará - UFC

Ao Deus da minha salvação, seja dada toda honra, glória e louvor.

AGRADECIMENTOS

À Deus, primeiramente, porque ele bom; porque a sua misericórdia dura para sempre.

À minha família, por todo o carinho, amor e cuidado que me deram em toda a vida; aos meus pais, á quem devo tudo o que sou; aos meus irmãos que sempre me apoiam e me motivam a crescer e em quem me inspiro.

Aos professores que contribuíram com o meu aprendizado ao longo do curso; especialmente ao Prof. Dr. Rafel Braga, pela parceria nesta jornada, por todo apoio, contribuição e pela excelente orientação.

Aos professores participantes da banca examinadora Prof. Dr. Isac Gabriel e Prof. Me. Roberto Cabral pelo tempo, pelas valiosas colaborações e sugestões.

RESUMO

Nos últimos vinte anos a fraude alimentar tem se tornado um problema recorrente nos Estados Unidos e em todo o mundo, acarretando prejuízos para a indústria de alimentos. A fraude alimentar tem sido custado caro e causado perdas das receitas anuais e riscos à saúde pública e tem contribuído para o enfraquecimento do mercado alimentício. Com o mercado do mel não é diferente, o mel é o terceiro alimento que mais sofre fraude, ficando atrás apenas do leite e do azeite. Com potencial de causar um colapso nos preços dos produtos e o declínio da produtividade, a fraude do mel coloca em risco produtores de mel autêntico e gera uma catástrofe econômica para os produtores. A rastreabilidade de produtos em uma cadeia produtiva tem o potencial de melhorar o gerenciamento da produção, diminuir os custos e melhorar a qualidade dos produtos. Neste contexto é que esse trabalho tem como objetivo explorar o potencial da tecnologia *Blockchain* para melhorar a rastreabilidade da cadeia produtiva do mel. Para isso foi desenvolvido um protótipo de uma aplicação web que possibilita o registro e a visualização da produção, industrialização e distribuição do mel, além de possibilitar o rastreio de produtos tanto pelos produtores como consumidores de mel. Ademais foram desenvolvidos os contratos inteligentes que permitem a interação entre a rede *blockchain* e a aplicação *web*, bem como foi realizada a avaliação da rede *blockchain* e da aplicação. Os resultados obtidos neste trabalho demonstram o uso da tecnologia *blockchain* é uma solução viável para prover a rastreabilidade da cadeia produtiva do mel.

Palavras-chave: *Blockchain* (Base de dados); Rastreabilidade; Mel; Redes de computadores.

ABSTRACT

Over the past twenty years, food fraud has become a recurring problem in the United States and worldwide, resulting in significant losses for the food industry. Food fraud has incurred substantial costs, causing annual revenue losses and public health risks, thereby contributing to the weakening of the food market. The honey market is no exception, with honey being the third most targeted food for fraud, ranking only behind milk and olive oil. With the potential to cause price collapses and decline in productivity, honey fraud poses a risk to authentic honey producers and creates an economic catastrophe for them. Improving product traceability within a production chain has the potential to enhance production management, reduce costs, and improve product quality. In this context, this study aims to explore the potential of Blockchain technology to enhance the traceability of the honey production chain. To achieve this, a web application prototype was developed, facilitating the registration and visualization of honey production, processing, and distribution. The application allows both honey producers and consumers to effectively trace products. Smart contracts were also developed to enable interaction between the Blockchain network and the web application. Lastly, an evaluation of the Blockchain network and the application was conducted. The results obtained in this study demonstrate that the use of Blockchain technology is a viable solution to enhance traceability in the honey production chain.

Keywords: Blockchain; Traceability; Honey; Network computer.

LISTA DE TABELAS

Tabela 1 – Cenários de teste	54
--	----

LISTA DE QUADROS

Quadro 1 – Requisitos de informações da cadeia produtiva do mel.	33
--	----

LISTA DE CÓDIGOS-FONTE

Código-fonte 1 – Código fonte em Solidity	46
Código-fonte 2 – Código fonte em Solidity	48
Código-fonte 3 – Código fonte em Solidity	49
Código-fonte 4 – Código fonte em Solidity	50
Código-fonte 5 – Código fonte em Solidity	51
Código-fonte 6 – Código fonte em Solidity	51
Código-fonte 7 – Arquivo Gênese	62
Código-fonte 8 – Código fonte em ShellScript	64

LISTA DE ABREVIATURAS E SIGLAS

ABI	<i>Application Binary Interface</i>
AWS	<i>Amazon Web Service</i>
Dapps	<i>Decentralized Application</i>
EC2	<i>Elastic Compute Cloud</i>
P2P	<i>Peer-to-peer</i>
pBFT	<i>Practical Byzantine Fault Tolerance</i>
PoS	<i>Proof of Stake</i>
PoW	<i>Proof of Work</i>
TCP	<i>Transmission Control Protocol</i>
USDA	<i>United States Department of Agriculture</i>

SUMÁRIO

1	INTRODUÇÃO	13
1.1	OBJETIVOS	14
<i>1.1.1</i>	<i>Objetivo Geral</i>	14
<i>1.1.2</i>	<i>Objetivos específicos</i>	14
2	TRABALHOS RELACIONADOS	16
2.1	Utilização de Blockchain na Rastreabilidade da Cadeia Produtiva do Leite	16
2.2	QRQueijo: Sistema de Emissão e Validação de Identificadores de Queijos Utilizando <i>Blockchain</i>	17
2.3	Uso de <i>Blockchain</i> para Registro de Dados de Cadeia de Suprimentos Verde da Indústria Sucroenergética	17
2.4	<i>Blocks for Bees: Solving Bee Business Problems with Blockchain</i>	18
2.5	Este trabalho	20
3	FUNDAMENTAÇÃO TEÓRICA	21
3.1	Apicultura	21
<i>3.1.1</i>	<i>História e definição</i>	21
<i>3.1.2</i>	<i>O Mel</i>	22
<i>3.1.3</i>	<i>Cadeia produtiva do mel</i>	22
<i>3.1.3.1</i>	<i>Insumos</i>	22
<i>3.1.3.2</i>	<i>Produção e manejo das abelhas</i>	23
<i>3.1.3.3</i>	<i>Processamento e industrialização</i>	23
<i>3.1.3.4</i>	<i>Comercialização</i>	24
<i>3.1.3.5</i>	<i>Mercado Consumidor</i>	24
3.2	<i>Blockchain</i>	25
<i>3.2.1</i>	<i>Estrutura e Organização de uma blockchain</i>	26
<i>3.2.1.1</i>	<i>Organização dos dados</i>	26
<i>3.2.1.2</i>	<i>Redes Blockchain</i>	27
<i>3.2.1.3</i>	<i>Mecanismo de consenso</i>	28
<i>3.2.1.4</i>	<i>Contratos inteligentes</i>	30
3.3	Análise de Desempenho	31
4	METODOLOGIA	33

4.1	Escolha da plataforma <i>blockchain</i>	33
4.2	Requisitos de Rastreabilidade	33
4.3	Desenvolvimento dos contratos inteligentes	37
4.4	Desenvolvimento da aplicação <i>web</i>	37
4.4.1	<i>Arquitetura Dapp</i>	37
4.5	Implementação da rede <i>blockchain</i>	38
4.6	Análise de desempenho	38
5	RESULTADOS	40
5.1	Apresentação do sistema	40
5.1.1	<i>Aplicação Web</i>	40
5.1.1.1	<i>Perfil do Produtor</i>	41
5.1.1.2	<i>Perfil do Processador</i>	42
5.1.1.3	<i>Perfil do Distribuidor</i>	44
5.1.1.4	<i>Perfil do Comerciante</i>	45
5.1.2	<i>Desenvolvimento dos Contratos Inteligentes</i>	45
5.1.2.1	<i>Contrato Authentication</i>	46
5.1.2.2	<i>Contrato Production</i>	48
5.1.2.3	<i>Contrato Processing</i>	49
5.1.2.4	<i>Contratos Distribution e Merchant</i>	50
5.1.2.5	<i>Contrato UpdateTransaction</i>	51
5.2	Análise de Desempenho	53
5.2.1	<i>A Rede Blockchain</i>	53
5.2.1.1	<i>Cenários de teste</i>	54
5.2.1.2	<i>Resultados do Experimento 1</i>	54
5.2.1.3	<i>Resultados do Experimento 2</i>	54
5.2.1.4	<i>Resultados do Experimento 3</i>	56
6	CONCLUSÕES E TRABALHOS FUTUROS	59
	REFERÊNCIAS	60
	APÊNDICE A –ARQUIVO DE CONFIGURAÇÃO DO BLOCO GÊNE- SIS	62
	APÊNDICE B –SCRIPT DE INICIALIZAÇÃO DOS NÓS DA REDE BLOCKCHAIN	64

1 INTRODUÇÃO

Nos últimos vinte anos a fraude alimentar tem se tornado um problema recorrente em todo o mundo, acarretando prejuízos para a indústria de alimentos (PHIPPS, 2020). Estima-se que a fraude alimentar custe para a indústria alimentícia entre 10 e 15 bilhões de dólares por ano e que as empresas de alimentos percam de 2% a 15% das receitas anuais com perdas de vendas decorrentes de fraude. Embora a fraude alimentar seja motivada no ganho econômico ilícito, ela representa riscos reais ou potenciais à saúde pública (JOHNSON, 2014). Esses fatores contribuem para diminuição da confiança do consumidor e o enfraquecimento do mercado.

O mel é o terceiro alimento que mais sofre fraude, ficando atrás apenas do leite e do azeite (GARCÍA, 2018). A fraude causada pela adulteração de mel tem resultado em colapso no preço do mel e o declínio da produtividade. Os impactos causados no mercado do mel decorrentes do aumento de produtos fraudulentos têm colocado em risco produtores de mel autêntico e gerado uma catástrofe econômica para os produtores, resultando em prejuízos de aproximadamente US\$ 1 bilhão (PHIPPS, 2020).

Em García (2018), o mel é descrito como o produto resultante da interação entre plantas e abelhas. O mel é composto em sua maioria por açúcares e água, além de outras substâncias. De acordo com os padrões do *Codex Alimentarius* (coleção de padrões alimentares estabelecida pela FAO e OMS para proteger a saúde do consumidor), para o mel ser considerado autêntico ele não deve conter qualquer adição ou remoção de substâncias contrárias ao processo natural das abelhas.

A rastreabilidade aplicada à indústria de alimentos pode ser vista como fonte de vantagem competitiva e trazer benefícios às empresas ao reduzir os custos com *recalls*, baratear os sistemas de distribuição e melhorar a gestão de suprimentos auxiliando a minimizar o impacto dos riscos à segurança, além de aumentar a receita da empresa e a confiança do consumidor no sistema alimentar (GOLAN *et al.*, 2004).

Nesse contexto, apesar de a tecnologia *blockchain* ter surgido como uma aplicação para transações financeiras, os seus benefícios também podem ser aproveitados na indústria de alimentos. *Blockchain* possibilita a criação de registros distribuídos e imutáveis fornecendo transparência na produção, visibilidade de toda a cadeia de suprimentos, além de proporcionar rastreabilidade da produção, que por sua vez, ajuda na prevenção de fraude. (BUMBLAUSKAS *et al.*, 2020).

O uso de *blockchain* como uma solução viável para rastreabilidade da cadeia de

suprimentos já vem sendo demonstrada. Em Mendonça *et al.* (2020), dados capturados por sensores são armazenados em uma *blockchain*, através de contratos inteligentes, para rastrear a produção de leite. Em Morais *et al.* (2020) é desenvolvida uma aplicação, intitulada QRQueijo, que, por meio da leitura de um código QR, permite acessar informações sobre o queijo, armazenadas em uma *blockchain*. No trabalho de Silva *et al.* (2020) os autores realizaram a simulação de uma rede *blockchain* com o intuito de prover rastreabilidade da cadeia de suprimentos verde da indústria sucroenergética.

Em Dobbins *et al.* (2018) os autores discutem a possibilidade da tecnologia *blockchain* ser empregada para oferecer rastreabilidade da cadeia produtiva do mel por meio do monitoramento das atividades e condições gerais das colmeias, ao vincular os dados sobre peso antes e depois da coleta do mel a cada recipiente de mel produzido. Além disso, os autores apresentam como a *blockchain* pode ajudar na prevenção de fraude, contribuir para melhorar o mercado de polinização e na criação de um mercado de seguro de apiários mais eficiente.

Com base no trabalho de outros autores que utilizaram *blockchain* para rastrear cadeias produtivas, este trabalho propõe desenvolver uma aplicação baseada em *blockchain* para prover a rastreabilidade da cadeia produtiva do mel. Com isso, ajudar produtores de mel a agregar valor ao seu produto, contribuindo para melhorar a qualidade e garantir genuinidade do mel produzido, conferindo, assim, confiança ao consumidor.

1.1 OBJETIVOS

1.1.1 *Objetivo Geral*

O objetivo geral deste trabalho é prover a rastreabilidade da cadeia produtiva do mel por meio da implementação e avaliação de uma aplicação *web* baseada em *blockchain*.

1.1.2 *Objetivos específicos*

- a) Desenvolver uma aplicação na linguagem de programação *JavaScript*, que fará a integração com a *blockchain*, de forma a registrar e acessar informações na *blockchain* sobre a produção de mel, tais como, peso, localização, data e hora da colheita, especialidade do mel;
- b) Desenvolver contratos inteligentes;
- c) Implementação de uma rede *blockchain* privada para realizar a análise de desem-

- penho da aplicação;
- d) Realizar a análise de desempenho da *blockchain*, avaliando o tempo de processamento do bloco, a taxa de propagação das transações e a taxa de sucesso das requisições recebidas.

2 TRABALHOS RELACIONADOS

Nesta sessão serão apresentados os trabalhos cujos temas estão relacionados com os objetivos propostos por este trabalho.

2.1 Utilização de Blockchain na Rastreabilidade da Cadeia Produtiva do Leite

Em Mendonça *et al.* (2020) é proposta uma arquitetura para rastreabilidade da cadeia produtiva do leite baseada em *blockchain*. A arquitetura utiliza três módulos principais que farão o controle operacional da aplicação. O módulo rastreabilidade, responsável por coletar os dados captados por sensores ao longo da cadeia de suprimentos e disponibilizar na *blockchain*; o módulo cliente, responsável por prover acesso público aos dados coletados em qualquer ponto da cadeia de produção, proporcionando a rastreabilidade do produto ao consumidor e o módulo sensores, que prove suporte à comunicação dos sensores externos ao sistema.

Neste trabalho foi utilizada uma rede privada baseada na *blockchain Ethereum* para a implementação da arquitetura proposta. Esta arquitetura foi utilizada para armazenar as informações do produto e dos membros da rede de forma segura e confiável através de contratos inteligentes. Para a realização dessa tarefa, dois contratos inteligentes, escritos na linguagem *Solidity*, foram utilizados. O primeiro contrato, nomeado Inicialização, é responsável por inserir, gerenciar e validar os usuários autorizados a inserir dados do produto na rede *blockchain*. O segundo contrato é o de Inserção, ele é responsável por gerenciar a inserção de informações na rede, realizar a autenticação de usuários e retornar os dados para o rastreamento de produtos. Os contratos inteligentes interagem com os módulos rastreabilidade e cliente possibilitando o registro e acesso as informações de rastreamento de produtos sempre que for solicitado por algum usuário da aplicação.

Os autores avaliaram a aplicação proposta criando dois cenários de testes, contendo 1 e 2 nós respectivamente, e foram avaliados o tempo gasto para efetivar uma transação na *blockchain* e o tamanho da fila de espera ao inserir uma transação. Os valores obtidos no resultado do experimento em relação ao tempo de espera fora de 3,89 segundos de média para o cenário 1 e 3,61 segundos para o cenário 2. Em relação ao tamanho da fila de espera, os valores de média para o cenário 1 são de 1,74 e para o cenário 2 de 1,86. Os autores consideraram que os resultados apresentados demonstram a viabilidade do uso da *blockchain* para a rastreabilidade da cadeia de suprimentos do leite. E para trabalhos futuros apontaram uma ampliação da avaliação

da metodologia de forma escalável.

2.2 QRQueijo: Sistema de Emissão e Validação de Identificadores de Queijos Utilizando *Blockchain*

Motivado pela falta de informação dos consumidores de queijo regionais do estado de Pernambuco, Morais *et al.* (2020) apresentam uma solução baseada em *blockchain*, para suprir a falta de informações e garantias dos consumidores por meio da criação de uma aplicação móvel, intitulada QRQueijo, a fim de proporcionar rastreabilidade e transparência da cadeia produtiva do queijo.

A aplicação desenvolvida é constituída de um Sistema de Registro, que permitirá aos usuários cadastrados no sistema realizarem as seguintes funcionalidades: visualizar a rede *blockchain*, realizar o cadastro de novos queijos e obter informações detalhadas dos queijos cadastrados. Uma aplicação móvel foi desenvolvida para realizar a leitura de um *QRcode*, impresso na embalagem do produto, a fim de obter informações sobre o produto cadastrado, atualizar a localização do queijo e armazená-la na *blockchain*.

Neste trabalho os autores realizam uma simulação de uma rede *blockchain* desenvolvida em Node.js. Para isso os autores desenvolveram uma rede *blockchain* local, baseada na aplicação desenvolvida por Hartikka (2017), para armazenar os dados gerados a partir da aplicação. A rede foi construída contendo 10 nós instanciados por meio do uso de *containers Docker* para realizar a simulação dos nós da rede.

2.3 Uso de *Blockchain* para Registro de Dados de Cadeia de Suprimentos Verde da Indústria Sucroenergética

Em Silva *et al.* (2020), é apresentado uma simulação de registros de CSV na indústria sucroenergética em um sistema baseado em tecnologia *blockchain*, que tem como motivação, a crescente demanda do mercado consumidor por transparência de informações da cadeia de produção, o alto custo para implantação de um sistema que forneça informações de maneira segura e confiável e o surgimento do conceito de Cadeia de Suprimentos Verde (CSV) para orientar a produção em busca de melhorar a sustentabilidade operacional das empresas.

O conceito da Cadeia de Suprimentos Verde (CSV) tem como objetivo frear o aumento da poluição e o aquecimento global, a partir da imposição de políticas e requisitos para

a seleção e desenvolvimento de fornecedores ambientalmente corretos. Além de promover a diminuição de impactos ambientais causados pela indústria, a adoção da CSV promove a redução de custos e consumo de energia, reutilização e reciclagem de resíduos e melhora da imagem e desempenho econômico das empresas.

Na elaboração deste trabalho os autores seguiram um modelo da cadeia de suprimentos da indústria sucroenergética com base na pesquisa de DE ANDRADE et al. (2012). Neste modelo são analisados os dados das atividades relacionadas a cadeia de produção da cana-de-açúcar, tais como, Colheita da cana-de-açúcar, Produção de Açúcar e Álcool, e distribuição da Produção e registrados em um sistema baseado em *blockchain*.

Neste trabalho, utilizando a plataforma de desenvolvimento *Remix*, os autores realizaram a criação e simulação de contratos inteligentes, escritos na linguagem *Solidity*, para registro e acesso de dados em uma rede *blockchain Ethereum* privada. Após criado o contrato inteligente, a plataforma *Remix* possibilita ao usuário interagir com o contrato inteligente para registrar informações relacionadas aos fornecedores e a produção da cana-de-açúcar e recuperar essas informações por meio do número do lote da cana-de-açúcar que foi recebido na usina.

2.4 *Blocks for Bees: Solving Bee Business Problems with Blockchain*

Dobbins *et al.* (2018) apresentam como a tecnologia *blockchain* pode ser útil na resolução de alguns problemas enfrentados por apicultores na produção e comercialização do mel. Após uma breve revisão bibliográfica demonstrando a aplicação de *blockchain* em outras áreas que vão além da moeda como saúde e agricultura, por exemplo. Os autores apresentam como a *blockchain* pode ser utilizado em conjunto com outras tecnologias para monitoração da produção e como isso pode implicar na detecção de fraude alimentar, no mercado de polinização e no mercado de seguros de apiário.

Segundo os autores, para aproveitar os benefícios da *blockchain* para prover rastreabilidade na produção de mel e outras atividades apícolas, é preciso primeiro coletar dados das colmeias e armazená-los em um banco de dados. Utilizando equipamentos de medição, como sensores, é possível obter de forma automatizada, dados de temperatura, umidade, localização, peso e hora do dia. Após a obtenção e análise dos dados, características sobre quantidade de mel produzida, atividades de polinização e saúde da colmeia podem ser registradas em uma *blockchain*. Dessa forma é possível obter segurança e confiabilidade aos dados, pois uma vez registrados na *blockchain* os mesmos tornam-se imutáveis.

O primeiro problema apresentado, onde soluções baseadas em *blockchain* se mostram promissoras, é a adulteração de mel. Ela tem causado instabilidade no mercado e preocupado os produtores, que veem seus produtos desvalorizados e a sua produção em declínio. Segundo os autores, é possível que consumidores e produtores de produtos beneficiados consigam determinar facilmente a genuinidade do mel que estão comprando referenciando os dados armazenados em uma *blockchain* à dados vinculados em cada frasco ou recipiente específico de mel produzido, sobre o peso antes e após a coleta de mel. Além de permitir aos consumidores identificarem a origem e especialidade do mel produzido.

Anualmente nos EUA o mercado de polinização movimentava mais de US \$410 milhões, porém os contratos de polinização geram muitos riscos aos apicultores, por conta de pesticidas e equipamentos agrícolas que podem causar danos às colmeias. Nesse contexto os autores apresentam como a tecnologia *blockchain* pode ser utilizada, por meio de contratos inteligentes, para melhorar os atuais contratos de polinização, através do monitoramento das colmeias é possível mensurar quando e quais obrigações foram atendidas e estabelecer formas de pagamento baseados em evidência. Dessa forma é possível oferecer maior segurança para os apicultores, proporcionando controle de risco a danos causados às colmeias e estabelecer condições de contratação mais transparentes e precisas com critérios bem definidos entre apicultores e agricultores.

Além de ser possível combater a fraude alimentar e melhorar o mercado de polinização, a tecnologia *blockchain* também apresenta grande potencial para o desenvolvimento da indústria de seguros de apiários. Pode oferecer maior segurança e eficácia para as seguradoras, que através do monitoramento da saúde das abelhas possibilita a criação de melhores práticas para manutenção e prevenção de perda das colmeias. Além disso, devido a sua natureza imutável *blockchain* pode fornecer um sistema de auditoria e prevenção de fraude, comparando dados para determinar se os apicultores seguiram recomendações relevantes para mitigar potenciais perdas.

A adoção de novas tecnologias como *blockchain* tem um enorme potencial de melhorar as práticas de apicultura, diminuir prejuízos causados pela comercialização de produtos adulterados e melhorar a vida e sobrevivência das abelhas, tornando a apicultura um setor mais acessível, eficiente e rentável.

2.5 Este trabalho

Nesta sessão é feito um comparativo entre os trabalhos relacionados e este trabalho, apresentando as semelhanças e diferenças que há entre eles. Semelhante aos trabalhos descritos anteriormente, neste trabalho propõe-se a rastreabilidade de cadeias produtivas por meio do uso da tecnologia *Blockchain* para registrar dados de maneira descentralizada.

(MENDONÇA *et al.*, 2020) propõem uma arquitetura, baseada em *blockchain*, para rastreabilidade da cadeia produtiva do leite. (MORAIS *et al.*, 2020) propõe uma solução para a rastreabilidade e transparência da cadeia produtiva do queijo e (SILVA *et al.*, 2020) apresenta uma simulação de registros de CSV na indústria sucroenergética baseado em *blockchain*, este trabalho propõe uma solução para a rastreabilidade da cadeia produtiva do mel baseada em *blockchain*, tendo como base os problemas enfrentados na produção e comercialização do mel e sugestões de solução apresentadas em (DOBBINS *et al.*, 2018).

Em (MENDONÇA *et al.*, 2020) é feita a implementação da arquitetura proposta, implementação de contratos inteligentes, avaliação da arquitetura. Foi utilizada a *blockchain* Ethereum para implantação dos contratos inteligentes. Em (MORAIS *et al.*, 2020) foi realizado o desenvolvimento de uma aplicação e a simulação de uma rede *blockchain* feita em Node.js. Em (SILVA *et al.*, 2020) foi realizado o desenvolvimento e simulação de um contrato inteligente utilizando a plataforma de desenvolvimento Remix. Neste trabalho foi desenvolvida uma aplicação web, realizada a implementação de contratos inteligentes, a configuração de uma rede *blockchain* Ethereum privada e avaliação de desempenho da aplicação.

3 FUNDAMENTAÇÃO TEÓRICA

Nesta sessão será descrito o referencial teórico necessário para compreensão deste trabalho. Serão abordados os conceitos de apicultura, a tecnologia *blockchain* e análise de desempenho de sistemas.

3.1 Apicultura

Nesta sessão é abordado um breve histórico da apicultura no Brasil, a definição e relevância socioeconômica da apicultura e a caracterização do mel e da cadeia produtiva do mel.

3.1.1 História e definição

O início da apicultura no Brasil se deu em 1839, por meio de imigrantes europeus que importaram alguns enxames de abelhas melíferas (*Apis mellifera*) de raças europeias. Segundo Magalhães *et al.* (2007), a história da apicultura no Brasil pode ser dividida em três etapas: a primeira corresponde ao período de implantação da apicultura no país, que ocorreu entre os anos de 1839 a 1955; a segunda iniciou em 1956, referente ao período de africanização dos apiários, resultado do cruzamento entre populações de abelhas de raças europeias com uma raça africana; e a terceira, iniciou em 1970, marcada pelo Primeiro Congresso Brasileiro de Apicultura em Florianópolis, que marcou o início da recuperação e expansão da apicultura brasileira.

A apicultura consiste na criação racional de abelhas do gênero *Apis*. Essa atividade pecuária representa grande importância para o agronegócio pela obtenção de produtos como mel, própolis, cera, geleia real e apitoxina, além de oferecer grande contribuição tanto para a preservação da biodiversidade como para o aumento da produtividade de culturas agrícolas, devido às atividades de polinização (GORROI *et al.*, 2020).

As abelhas, importantes agentes na manutenção da biodiversidade, são responsáveis por polinizar cerca de 30% das plantas utilizadas para alimentação humana. Portanto, a apicultura, além de comprovada rentabilidade e importância econômica, caracteriza-se como uma atividade essencialmente ecológica e sustentável sendo uma das poucas atividades agropecuárias que preenche os requisitos do tripé da sustentabilidade: o econômico, por gerar renda para os apicultores; o social, pois ajuda a diminuir o êxodo rural, através do trabalho no campo; e o ecológico, pois, além de não precisar desmatar, a criação de abelhas contribui para conservação das espécies (SANTOS; RIBEIRO, 2009).

3.1.2 O Mel

Em Ferreira e Assis (2020) o mel é descrito como o produto alimentício proveniente das abelhas melíferas, que recolhem o néctar das plantas e outras secreções, realizam uma série de transformações físicas e químicas e armazenam nos favos da colmeia até que ele amadureça e esteja pronto para o consumo. No processo de formação e maturação do mel, o teor de umidade do néctar é reduzido até atingir valores inferiores a 20%.

O mel é uma solução composta por açúcares, principalmente glicose e frutose, água, além de uma mistura complexa de outras substâncias. As variações de concentração desses elementos atribuem ao mel diferentes propriedades físicas, aromas e sabores. Há diversos fatores que podem interferir na qualidade do mel da abelha melífera, como condições climáticas, processamento, armazenamento e a espécie vegetal.

Para o mel ser comercializado de forma segura para a saúde dos consumidores ele deve atender a uma série de exigências e parâmetros para atestar a qualidade do produto. Não pode haver adição de açúcares ou quaisquer substâncias estranhas que alterem sua composição original, bem como o superaquecimento, que é proibido por lei. Outro indicador de qualidade é a presença de grãos de pólen. O mel deve necessariamente apresentar grãos de pólen, portanto a ausência de grãos de pólen no mel pode ser um indicativo de fraude. Ademais, o mel pode ser classificado quanto a sua origem, processo de obtenção, apresentação e características sensoriais.

3.1.3 Cadeia produtiva do mel

Segundo Fleck e Bellinaso (2008), uma cadeia produtiva pode ser definida como um conjunto de elementos em processos produtivos que interagem para oferecer produtos e/ou serviços ao mercado consumidor. Na agroindústria a cadeia de produção pode ser dividida em três grandes segmentos: produção, transformação e comercialização. Nesta seção serão apresentados os principais elos que compõem a cadeia produtiva do mel e seus atores, sendo eles: insumos, produção, processamento e industrialização, comercialização e mercado consumidor.

3.1.3.1 Insumos

Para a prática das atividades apícolas como instalação e manutenção de apiários, povoamento de apiários e colheita de mel são utilizados diversos materiais e equipamentos como a vestimenta utilizada para proteção do apicultor, que é composta de macacão, máscara, luvas

e botas. Dentre o material utilizado no apiário pode-se destacar fumigador, formão, núcleo (utilizado na captura de novos enxames), cera alveolada (utilizada para facilitar e adiantar o trabalho das abelhas) e a colmeia (no Brasil o modelo mais utilizado é o *Langstroth*), entre outros. Os materiais utilizados na apicultura podem ser encontrados em lojas especializadas ou fabricadas pelo próprio apicultor (GORROI *et al.*, 2020).

Vidal (2020) relata uma carência na região nordeste de insumos, máquinas e equipamentos, enquanto que na região sul do país há deficiências na confecção de indumentárias de qualidade que proporcione maior conforto ao apicultor.

3.1.3.2 *Produção e manejo das abelhas*

A apicultura caracteriza-se pela presença elevada de pequenos produtores (GORROI *et al.*, 2020). Estes são caracterizados por possuírem até 150 colmeias, utilizar mão de obra familiar, manter atividades paralelas, trabalhar em cooperação com outros produtores para diminuir os custos sem deixar de ser independente. O médio produtor caracteriza-se pela exploração de 150 a 1500 colmeias, são mais especializados que pequenos, utilizam mais capital e possuem mão de obra contratada. Os grandes produtores possuem acima 1500 colmeias, são mais especializados que os demais e possuem mão de obra inteiramente contratada. (BUAINAIN *et al.*, 2007).

A apicultura é uma atividade que não requer necessariamente uma dedicação exclusiva, porém para obter melhores resultados na produtividade é preciso que o apicultor realize manutenções periódicas no apiário (GORROI *et al.*, 2020). No processo de monitoramento das colmeias, deve-se observar aspectos como a coloração e estrutura dos favos, a presença de ovos e larvas nos favos, a presença de realeiras, a disponibilidade de alimento para a colônia e sinais de doença, bem como, se o enxame está forte ou fraco. O monitoramento constante das colmeias irá ajudar o apicultor a se manter informado, identificar possíveis problemas e manter os enxames sempre fortes e populosos.

3.1.3.3 *Processamento e industrialização*

Segundo Ferreira e Assis (2020), para assegurar a qualidade do mel, preservando suas características é imprescindível que a colheita e extração do mel sejam realizadas de forma adequada. Na colheita, os quadros coletados devem possuir mais de 80% da sua área operculada, para evitar a colheita de “mel verde”, é imprescindível que a colheita seja realizada em dias

ensolarados, para evitar que o mel absorva a umidade do ambiente.

Após a colheita, as melgueiras (parte da colmeia destinada ao armazenamento do mel), são transportadas para a Unidade de Extração e Beneficiamento de Produtos das Abelhas (UEPA). Nesta fase de processamento e industrialização são realizadas as seguintes etapas: i) desoperculação, que consiste na retirada da camada fina de cera cobre os alvéolos na superfície dos favos; ii) centrifugação, onde o mel é retirado dos favos pela força centrífuga; iii) filtração e decantação, que tem o objetivo de retirar impurezas e bolhas; iv) envase, pode ser realizado em diferentes tipos de frascos, dependendo do destino e do tipo de produto comercializado; v) armazenamento, deve ser feito em local fresco, seco, e ao abrigo da luz; vi) expedição, última etapa no processamento do produto, deve ocorrer com o mínimo de exposição ao sol.

Para Vidal (2020), a informalidade na produção representa uma grande dificuldade para o setor apícola, principalmente na fase de processamento, devido ao número unidades de extração e beneficiamento que estão em desacordo com as normas do Ministério da Agricultura, Pecuária e Abastecimento (MAPA).

3.1.3.4 Comercialização

Na cadeia produtiva do mel a comercialização, dependendo do volume da produção, é realizada por diversos canais intermediários sendo estes atacadistas, varejistas, representantes, etc. Além desses, outros tipos de intermediação são os entrepostos estaduais e entidades associativas atuando na comercialização tanto no varejo como no atacado. Os entrepostos nacionais são responsáveis por comercializar o mel para os revendedores, para a indústria e para exportação (ALMEIDA; CARVALHO, 2009).

Vidal (2020) destaca, que na cadeia apícola nordestina a distribuição e comercialização de mel ocorre de maneira diversificada, pelo próprio apicultor ou intermediários sendo estes apicultores, entrepostos, associações ou cooperativas que comercializam o produto em mercados atacadistas, varejistas ou diretamente para o consumidor final. Estes agentes desempenham um importante papel na cadeia produtiva do mel escoando a produção em locais de difícil acesso.

3.1.3.5 Mercado Consumidor

De acordo com Vidal (2020) atualmente o Brasil está entre os maiores produtores de mel do mundo, principalmente pela produção de mel orgânico, que é apreciado no mercado internacional. Em 2018, o país produziu 42,3 mil toneladas de mel, destacando-se como 11º

maior produtor mundial (FAO, 2020). O mel orgânico é um dos mais valorizados no mercado americano. De acordo com o (*United States Department of Agriculture (USDA)*), em 2018, 91% das importações de mel orgânico dos Estados Unidos foram provenientes do Brasil.

O mel é um produto amplamente utilizado na indústria seja como ingrediente na mistura de produtos e receitas ou como medicamento devido às suas qualidades antissépticas e cicatrizantes (ALMEIDA; CARVALHO, 2009). Porém, o mercado consumidor de mel no Brasil ainda é pequeno se comparado com o mercado internacional. Enquanto em países como Alemanha, que tem consumo superior a 1 kg per capita ao ano e Estados Unidos, em torno 0,6 kg, em 2017 o consumo brasileiro não ultrapassou 100 g (VIDAL, 2020).

Com o baixo consumo interno o mercado internacional se torna uma alternativa, porém, a crescente preocupação com produtos contaminados e adulterados requer atenção às exigências do mercado consumidor em relação a qualidade. Portanto, são necessários investimentos para melhorar a qualidade, agregar valor ao produto e diversificar a produção (VIDAL, 2020). Além, claro, de criar mecanismos de controle de qualidade, rastreabilidade e fiscalização mais rigorosos e eficazes.

3.2 Blockchain

Conforme Swan (2015), a *blockchain* surgiu como o livro-razão público de todas as transações do *Bitcoin*. A *blockchain* pode ser entendida como um livro-razão que registra transações de maneira transparente e descentralizada, compartilhando as informações com todos os nós de uma rede. As transações são agrupadas em blocos criptografados com *hash*. Cada novo bloco adicionado possui uma referência do bloco anterior, formando assim, uma cadeia de blocos imutáveis.

A principal inovação tecnológica da *blockchain* consiste na capacidade do sistema em realizar transações sem ter que estabelecer a confiança entre as partes ou pela presença de um intermediário. Dessa forma, as possibilidades de aplicação da *blockchain* tornam-se realmente amplas sendo usado não apenas para transações, mas também como um sistema de rastreamento, monitoramento e registro de todos os tipos de ativos.

Os benefícios da tecnologia da *blockchain* e seu potencial revolucionário apresentam capacidade para mudar paradigmas sociais e suas operações. Swan (2015), divide a *blockchain* em três categorias potenciais de atuação: *Blockchain 1.0*, a utilização de cripto moedas em aplicações relacionadas ao dinheiro; *Blockchain 2.0*, vai além de transações simples em dinheiro,

abrangendo toda a área de economia e mercado financeiro; e *Blockchain 3.0*, a utilização do *blockchain* como aplicativo, expandindo da moeda e mercado financeiro para áreas do governo, saúde, ciência, literatura, etc.

3.2.1 *Estrutura e Organização de uma blockchain*

Nesta sessão é apresentado uma visão geral da estrutura e organização de uma rede *blockchain*, sendo esta a organização dos dados criptográficos, a rede, o mecanismo de consenso distribuído e a estrutura de contratos inteligentes. Cada um desses tópicos é descrito logo abaixo.

3.2.1.1 *Organização dos dados*

Do ponto de vista da organização de dados a *blockchain* pode ser entendido como uma *string* de crescimento infinito, onde cada nó mantém uma réplica da estrutura de dados da *blockchain* organizada em três níveis hierárquicos, as transações, os blocos e a cadeia de blocos (WANG *et al.*, 2019).

subseção Transações

Uma transação é uma transferência de valores entre um conjunto de endereços, que são identificadores únicos utilizados pelos usuários para realizar uma transação (BASHIR, 2017). Cada transação é um registro estático contendo o endereço dos participantes da transação, o valor da transação e o estado de recepção. A segurança e autenticidade da transação é fornecida através do algoritmo de *hashing* criptográfico e criptografia assimétrica:

- **Função *hash*:** uma função *hash* recebe uma entrada de tamanho arbitrário e gera uma saída de tamanho fixo, ou seja, um resumo da função *hash*. Uma função *hash* deve possuir as seguintes propriedades: i) resistência a colisão: dadas duas mensagens diferentes, é computacionalmente inviável encontrar um mesmo valor de resumo; ii) resistência à pré-imagem: essa propriedade garante que é computacionalmente inviável recuperar o valor de entrada a partir do seu valor de resumo; iii) resistência à segunda pré-imagem: é computacionalmente inviável encontrar duas mensagens quaisquer que mapeiam no mesmo valor de resumo.
- **Criptografia assimétrica:** em uma rede *blockchain* cada transação é assinada com um sistema de chaves públicas, sendo necessário ao enviar um valor, uma chave privada para assinar uma transação e a chave pública do usuário a receber o valor. Dessa forma, somente o detentor da chave privada, que faz par com a chave

pública, conseguirá decifrar a transação.

subseção Os blocos e a Cadeia de blocos

Um bloco é formado principalmente por um conjunto de registros de transações criado por nós através do processo de consenso e um cabeçalho. Cada bloco inserido na *blockchain* possui em sua estrutura um ponteiro de *hash* e uma estrutura de dados criptográficos da árvore de Markle, usados para garantir a ordem e integridade da cadeia de blocos, e gerar um resumo inviolável de todas as transações de um bloco, além de outros campos auxiliares que podem variar de acordo com o protocolo de consenso utilizado para geração de blocos (WANG *et al.*, 2019).

- **Ponteiro de *hash*:** na *blockchain*, cada novo bloco adicionado possui em seu cabeçalho um código de *hash* para identificar o bloco atual e um ponteiro de *hash* que faz referência ao bloco anterior na cadeia de blocos. Assim, o bloco reconhece que as transações do bloco anterior são criadas antes das do bloco atual.
- **Árvore de Merkle:** uma árvore de Merkle é definida como uma estrutura de árvore binária que representa as transações de um bloco. Na *blockchain* essa estrutura é utilizada para resumir de maneira eficiente as transações de um bloco e facilitar a verificação dessas transações por outros nós de consenso. Na criação da árvore de Merkle, cada folha armazena o *hash* de uma transação. As folhas são agrupadas em pares formando um nó pai. Este processo é repetido até não haver mais pares, restando apenas a raiz de Merkle.

3.2.1.2 Redes Blockchain

Na *blockchain* a rede é formada por entidades lógicas representada pelos nós da rede. Cada nó na rede é referente a um usuário e não a um dispositivo físico. Os nós são organizados como uma rede *Peer-to-peer* (P2P) sobreposta. Em uma rede de acesso aberto qualquer usuário pode se juntar a rede sem a necessidade de qualquer permissão e ativar livremente as funcionalidades disponíveis. Ao contrário das redes sem permissão, nas redes *blockchain* de consórcio, ou seja, com permissão somente os nós aleatorizados podem ter acesso a determinadas funcionalidades, como participação de consenso e propagação dos dados. Na *blockchain* os blocos realizam uma conexão *Transmission Control Protocol* (TCP) para transmitir as transações e os blocos através da inundação de links P2P, dessa forma a *blockchain* é replicada

em todos os nós da rede.

Em uma rede *blockchain* os nós podem ser classificados em nós leves e nós completos, a depender das suas funcionalidades, que podem ser: i) roteamento, presente em todos os nós, ii) armazenamento simples, onde o nó mantém apenas o cabeçalho de cada bloco, iii) armazenamento completo, onde o nó guarda uma réplica completa de toda a cadeia de blocos, e iv) consenso, que permite ao nó a funcionalidade de participar do consenso. Os nós completos são aqueles que possuem todas as funcionalidades, já os nós leves possuem apenas as funcionalidades de roteamento e armazenamento simples (WANG *et al.*, 2019).

3.2.1.3 Mecanismo de consenso

O consenso é um processo entre os nós de uma rede para chegar a um acordo sobre um estado final de dados. Esse processo pode ser facilmente realizado entre dois nós, porém, em um sistema distribuído, com vários participantes chegar ao consenso torna-se uma tarefa difícil. Para isso, utiliza-se mecanismos de consenso, que consiste em um conjunto de etapas executadas por todos os nós, ou a maioria, para concordarem sobre uma proposta de estado ou valor (BASHIR, 2017).

Para obter o resultado esperado um mecanismo de consenso de cumprir vários requisitos: (i) os nós honestos devem chegar a um acordo, como mencionado anteriormente; (ii) o processo de consenso deve ser encerrado por todos os nós; (iii) o valor proposto inicialmente e o valor acordado por todos os nós honestos deve ser o mesmo; (iv) o algoritmo deve funcionar, mesmo na presença de nós maliciosos ou defeituosos; (v) para cada novo ciclo de consenso, os nós devem tomar decisão apenas uma vez. Diferentes algoritmos podem ser usados para se alcançar o consenso. Alguns desses algoritmos serão brevemente descritos abaixo:

- **Prova de Trabalho (do inglês, *Proof of Work (PoW)*):** O PoW é um mecanismo que se baseia na prova de que foram gastos recursos computacionais suficientes antes de propor um valor (BASHIR, 2017). Dois princípios devem ser seguidos neste algoritmo. Primeiro, a PoW deve ser uma tarefa difícil e trabalhosa, ou seja, que demande alto poder computacional, mas não impossível de ser realizada; e segundo, verificar o PoW deve ser uma tarefa fácil e rápida. O *bitcoin* é o principal exemplo de plataforma que utiliza a prova de trabalho como mecanismo de consenso (CHICARINO *et al.*, 2017).

A ideia principal deste algoritmo está na recompensa que os nós recebem por

meio da competição do poder de *hashing*. Com base nas informações do bloco anterior diferentes nós da rede procuram solucionar um problema matemático. O primeiro nó a solucionar o problema pode criar um novo bloco e obter sua recompensa (MINGXIAO *et al.*, 2017).

No *bitcoin* a prova trabalho funciona da seguinte forma: Primeiro, os nós mineradores devem coletar todas as transações pendentes após o último bloco gerado, calcular a raiz de Merkle das transações e preencher outros campos do cabeçalho como *hash* do bloco anterior, *hash* do bloco atual, o *nonce* e outras informações. O valor de *hash* do bloco atual deverá ser calculado incrementando o *nonce* (variável usada para modificar a saída da função *hash*), até que o valor de *hash* obtido corresponda aos requisitos especificados pela dificuldade, que é uma colisão parcial de *hash*. Por exemplo, se a dificuldade for configurada para o primeiro bit sendo zero, qualquer valor de *hash* que inicie com um zero será considerado válido (CHICARINO *et al.*, 2017).

- **Prova de Posse (do inglês, *Proof of Stake (PoS)*):** Diferente do PoW que recompensa os participantes que geram novos blocos através do mecanismo de mineração, no PoS a participação requer uma quantia de moedas. Este algoritmo utiliza o conceito de idade da moeda, onde a idade é calculada multiplicando o seu valor pelo período de tempo decorrido após a sua criação. Os nós obtêm direitos de participação e valor de recompensa de acordo com o tempo de retenção e idade da moeda.

No PoS a dificuldade de mineração é inversamente proporcional a idade da moeda. Desta forma os participantes são encorajados a aumentar o tempo de retenção da moeda. Além de utilizar melhor os recursos e diminuir o gasto de energia, pois não depende inteiramente da prova de trabalho, o PoS também aumenta a dificuldade de ataques, devido a necessidade de acumular um grande número de moedas por um longo período de tempo para realizar um ataque (MINGXIAO *et al.*, 2017).

- **Algoritmo de Tolerância a Falha Bizantina (do inglês, *Practical Byzantine Fault Tolerance (pBFT)*):** Este algoritmo propõe uma solução para o problema das falhas bizantinas BFP. As falhas bizantinas são falhas arbitrárias ocasionadas por nós maliciosos ou defeituosos que exibem um comportamento arbitrário.

O pBFT é um algoritmo de replicação de máquina de estados, que oferece vivacidade e segurança para no máximo $\lfloor (n-1)/3 \rfloor$ de um total de n réplicas defeituosas, ou seja, o pBFT garante consistência e integridade desde que menos de $1/3$ dos nós da rede se tornem defeituosos. O pBFT é o primeiro algoritmo de replicação de estado de máquina seguro em ambientes assíncronos, como a Internet (CASTRO; LISKOV, 2002).

O algoritmo pBFT funciona da seguinte forma:

- i) O cliente envia uma solicitação para o nó líder da rede (servidor mestre).
- ii) O líder transmite a mensagem para os outros nós servidor e estes decidem se aceitarão a solicitação ou não. Se $2/3$ dos nós escolher aceitar a solicitação, ela será confirmada.
- iii) Quando um nó recebe a confirmação de $2/3$, ele conclui que a maioria dos nós chegou a um consenso em aceitar a solicitação.
- iv) Os nós executam as instruções na mensagem de solicitação e enviam a resposta para todos os nós servidor da rede e para o cliente.

3.2.1.4 Contratos inteligentes

O conceito de contratos inteligentes foi introduzido por Nick Szabo na década de 1990. Szabo descreve os contratos inteligentes como um protocolo de transação computadorizado que executa os termos de um contrato com o objetivo de satisfazer condições contratuais comuns e minimizar execuções maliciosas, acidentais e a necessidade de intermediários (SZABO, 1994).

Contratos inteligentes são programas de computador ou *scripts*, que são executados automaticamente quando certas condições são atendidas. Eles também devem ser seguros e imparáveis, isso significa que eles devem ser projetados para serem tolerantes a falhas e executados em um período de tempo razoável. Outra propriedade dos contratos inteligentes é que devem apresentar o mesmo resultado, se executado por qualquer nó da rede, caso contrário, o consenso entre os nós da rede não pode ser alcançado, o que acarretará na falha do consenso distribuído, um dos pilares do funcionamento da *blockchain* (BASHIR, 2017).

Outras características dos contratos inteligentes descritas em Swan (2015) são: a autonomia, autossuficiência e descentralização. Contratos inteligentes são autônomos, pois, após o seu lançamento e execução, um contrato e seu agente não precisam permanecer em contato. Em segundo lugar, podem ser autossuficientes, possuem a capacidade de gerenciar recursos,

arrecadando fundos ao fornecer serviços e gastá-los em recursos necessários, como capacidade de processamento e armazenamento. E em terceiro, contratos inteligentes são descentralizados, ou seja, não subsistindo em um único servidor, mas distribuídos pelos nós da rede.

3.3 Análise de Desempenho

Avaliação de desempenho consiste em um conjunto de atividades empregadas para avaliar o desempenho de um sistema. Para realizar a avaliação de desempenho de um sistema, três técnicas de avaliação podem ser utilizadas, sendo elas: medição, modelagem e simulação (YADAV *et al.*, 2018).

- **Medição:** utiliza-se da aplicação de cargas de trabalho para mensurar o desempenho de sistemas com base em dados coletados. Esta técnica é aplicada em sistemas reais cujo objetivo é obter afirmações sobre o comportamento de sistemas através de medições.
- **Modelagem:** nesta técnica utiliza-se de modelos matemáticos para representar modelos do mundo real. O objetivo da modelagem de sistemas é demonstrar a relação entre diferentes componentes de um sistema buscando uma melhor compreensão do seu funcionamento. Alguns exemplos de modelos matemáticos que contribuem para modelagem de sistemas são as Redes de Petri, Cadeias de Markov e Teoria de Filas.
- **Simulação:** técnica empregada na análise de desempenho sistemas, pode ser entendida como o processo de projetar um modelo de um sistema real para conduzir experimentos cujo objetivo é entender o comportamento do sistema e sua operação (CENTENO, 1996). Baseado no tipo de sistema estudado a simulação pode ser classificada quanto ao tipo de modelo podendo ser matemáticos ou físicos, instantâneos ou dinâmicos, determinísticos ou estocásticos e discretos ou contínuos.

Realizar avaliação de desempenho em sistemas *blockchain* é um passo fundamental antes da implantação do sistema real. Vários ambientes de simulação já foram propostos para avaliar o desempenho de *blockchains*. Alguns desses ambientes serão brevemente descritos abaixo: *SimBlock*, *BlockSim*, *Remix*, entre outros.

O *BlockSim* é um *framework* utilizado para fornecer assistência nas fases de projeto, implementação e avaliação de *blockchains*. Seguindo um modelo de simulação estocástica,

é capaz de representar fenômenos aleatórios por amostragem a partir de uma distribuição de probabilidade. O *BlockSim* fornece um conjunto de componentes e uma estrutura personalizada para simular a cadeia de blocos, sendo possível configurar parâmetros de entrada, criar lotes de transações, entre outras funcionalidades.

Outro simulador de *blockchain* é o *SimBlock*, um simulador orientado a evento, onde os nós participantes geram as mensagens e os eventos de mineração. Este simulador utiliza três conjuntos de parâmetros: (i) parâmetros de bloco, como tamanho do bloco e intervalo de geração de blocos; (ii) parâmetros do nó, como número de nós, número de nós vizinhos e capacidade de geração de blocos; e (iii) parâmetros de rede, como largura de banda e atraso de propagação.

Por fim, a plataforma de simulação de contratos inteligentes *Remix*. Esta é uma plataforma online e de código aberto, útil para promover o ensino e aprendizagem da *blockchain Ethereum*. Nela é possível desenvolver, implantar e administrar contratos inteligentes para *blockchains Ethereum*. Os contratos são escritos, usando a linguagem de programação *Solidity*, uma linguagem de alto nível e orientada a objeto desenvolvida pela própria *Ethereum*.

4 METODOLOGIA

Nesta seção é apresentado o passo-a-passo de execução que foi seguido neste trabalho para se alcançar os objetivos propostos. Os procedimentos estão listados em ordem de execução.

4.1 Escolha da plataforma *blockchain*

Esta etapa dedicou-se a escolha da plataforma *blockchain* a ser utilizada. A escolha da plataforma foi definida a partir do estudo mais aprofundado das principais plataformas que possuam suporte nativo a contratos inteligentes. A plataforma de Blockchain Ethereum foi escolhida para a realização deste trabalho devido maior facilidade de documentação, maior transparência, por permitir a implementação tanto em uma rede pública ou uma rede privada e por ser a plataforma mais utilizada.

4.2 Requisitos de Rastreabilidade

Nesta etapa foram definidos os critérios de rastreabilidade da cadeia produtiva do mel, as informações referentes aos agentes da cadeia produtiva e informações referentes a produção, processamento distribuição e comercialização do mel necessárias para prover a rastreabilidade de produtos.

Para possibilitar a rastreabilidade da cadeia de suprimentos é necessário saber quais informações sobre os produtos precisam ser armazenadas em cada elo da cadeia. (DONNELLY *et al.*, 2008) apresenta uma lista padronizada de dados necessários para rastrear da cadeia produtiva do mel. Neste trabalho, as informações referentes ao mel que serão registradas na produção, processamento, distribuição e comercialização do mel, foram escolhidas com base no trabalho de (DONNELLY *et al.*, 2008). Os agentes da cadeia de produção deverão registrar informações referentes ao recebimento, produção e despacho de unidades comerciais ou logísticas. Estas informações estão listadas na tabela a seguir.

Quadro 1 – Requisitos de informações da cadeia produtiva do mel.

Elementos de dados	Descrição	Exemplos
PRODUTORES DE MEL		
Continua na próxima página...		

Elementos de dados	Descrição	Exemplos
PARA CADA UNIDADE COMERCIAL CRIADA		
ID produtor	Identificador do produtor de mel	3264679
ID unidade	Identificador da unidade comercial criada	321346548
Peso	Peso da unidade descrito em quilos	20Kg
Recipiente	Descrição do tipo físico da unidade	Tambor de plástico
Florada	Tipo de vegetação que a abelha colhe o néctar	laranjeira
Data fabricação	Data da colheita do mel	05/07/2023 15:10
PARA CADA UNIDADE LOGÍSTICA CRIADA		
ID unidade	Identificador da unidade de logística criada	321346548
IDs unidades	Lista de identificadores das unidades comerciais na unidade logística	(unidade 1, unidade 2, ...)
PARA CADA UNIDADE DESPACHADA		
ID unidade	Identificador da unidade despachada	3264679
ID transportador	Identificador do transportador para quem a unidade é despachada	321346548
Data de envio	Data e hora da transferência	05/07/2023 15:10
PROCESSADORES DE MEL		
PARA CADA UNIDADE RECEBIDA		
Continua na próxima página...		

Elementos de dados	Descrição	Exemplos
ID unidade	Identificador da unidade recebida	3264679
IDs unidades	Lista de identificadores das unidades comerciais na unidade logística (se recebido como unidade logística)	(unidade 1, unidade 2, ...)
ID transportador	Identificador do transportador de quem a unidade foi recebida	321346548
Data de recebimento	Data e hora da transferência	05/07/2023 15:10
PARA CADA UNIDADE COMERCIAL CRIADA		
ID da unidade	Identificador da unidade comercial criada	3264679
ID da matéria-prima	Identificador do mel recebido que será beneficiado	641346548
Variedade	Tipo de vegetação que a abelha colhe o néctar	Silvestre
Composição	Lista de nomes	Carboidrato - 100 %
Peso	Peso da unidade descrito em gramas	200g
Recipiente	Descrição do tipo físico da unidade	Pote de vidro
Tipo	X	orgânico
Validade	Melhor antes ou venda até a data, conforme apropriado	05/07/2023
PARA CADA UNIDADE LOGÍSTICA CRIADA		
ID unidade	Identificador da unidade de logística criada	89465138258
Continua na próxima página...		

Elementos de dados	Descrição	Exemplos
IDs unidades	Lista de identificadores das unidades comerciais na unidade logística	(unidade 1, unidade 2, ...)
PARA CADA UNIDADE DESPACHADA		
ID unidade	Identificador da unidade despachada	3264679
ID transportador	Identificador do transportador para quem a unidade é despachada	321346548
Data de recebimento	Data e hora da transferência	05/07/2023 15:10
DISTRIBUIDORES DE MEL		
PARA CADA UNIDADE RECEBIDA		
ID da unidade	Identificador da unidade recebida	321346548
ID fornecedor	Empresa alimentar de quem a unidade foi recebida	3264679
Local de envio	Endereço onde é feita a entrega	Rua A, 456
Data de envio	Data e hora da transferência	05/07/2023 15:10
PARA CADA UNIDADE DESPACHADA		
ID da unidade	Identificador da unidade despachada	321346548
ID destinatário	Empresa alimentar a quem a unidade é expedida	3264679
Local de envio	Endereço onde é feita a entrega	Rua A, 456
Data de envio	Data e hora da transferência	05/07/2023 15:10
COMERCIANTES DE MEL		
Continua na próxima página...		

Elementos de dados	Descrição	Exemplos
PARA CADA UNIDADE RECEBIDA		
ID da unidade	Identificador da unidade recebida	321346548
ID fornecedor	Empresa alimentar de quem a unidade foi recebida (transportador ou processador)	3264679
Data de recebimento	Data e hora da transferência	05/07/2023 15:10

Fonte: Elaborado pelo autor.

4.3 Desenvolvimento dos contratos inteligentes

Após estabelecer os requisitos de rastreabilidade da cadeia produtiva do mel foi realizada a implementação dos contratos inteligentes responsáveis por implementar a lógica necessária para alcançar os objetivos propostos neste trabalho. Os detalhes de implementação estão descritos na sessão 5, Resultados, sub-sessão 5.1.2, Desenvolvimento dos Contratos Inteligentes.

4.4 Desenvolvimento da aplicação *web*

Nesta etapa foi realizado o desenvolvimento da aplicação *web*. A aplicação desenvolvida é constituída de um *frontend*, escrito em *Javascript* e *React*, executado em um navegador web com suporte ao *Metamask* e contratos inteligentes executados em uma rede *Blockchain Ethereum*. O *frontend* possibilita a interação do usuário dentro da aplicação. A aplicação está descrita em mais detalhes na sessão Solução 5.

4.4.1 Arquitetura *Dapp*

No ecossistema Ethereum, os Aplicativos descentralizados (*Decentralized Application* (Dapps)) são aplicações compostas por um *frontend* combinado com contratos inteligentes executados em uma rede descentralizada (ETHEREUM, 2023). Este *frontend* se comunica com

os contratos inteligentes, implantados na rede *Blockchain*, por meio de uma interface binária de aplicação de contrato, do inglês (*Application Binary Interface (ABI)*). Os contratos inteligentes, são responsáveis pela interação com a rede *blockchain* executando novas transações e lendo os dados registrados na cadeia de blocos.

A interação entre o *frontend* da aplicação e a rede *blockchain* é feita através de um provedor de acesso. O provedor é composto por duas partes, um nó da rede *blockchain* fornecendo uma API JSON-RPC e uma camada de software no *frontend* da aplicação, a biblioteca "Web3.js". O gerenciador de carteiras *Metamask* foi utilizado para gerenciar as contas dos usuários, assinar transações e estabelecer a conexão com a rede através da biblioteca web3.

4.5 Implementação da rede *blockchain*

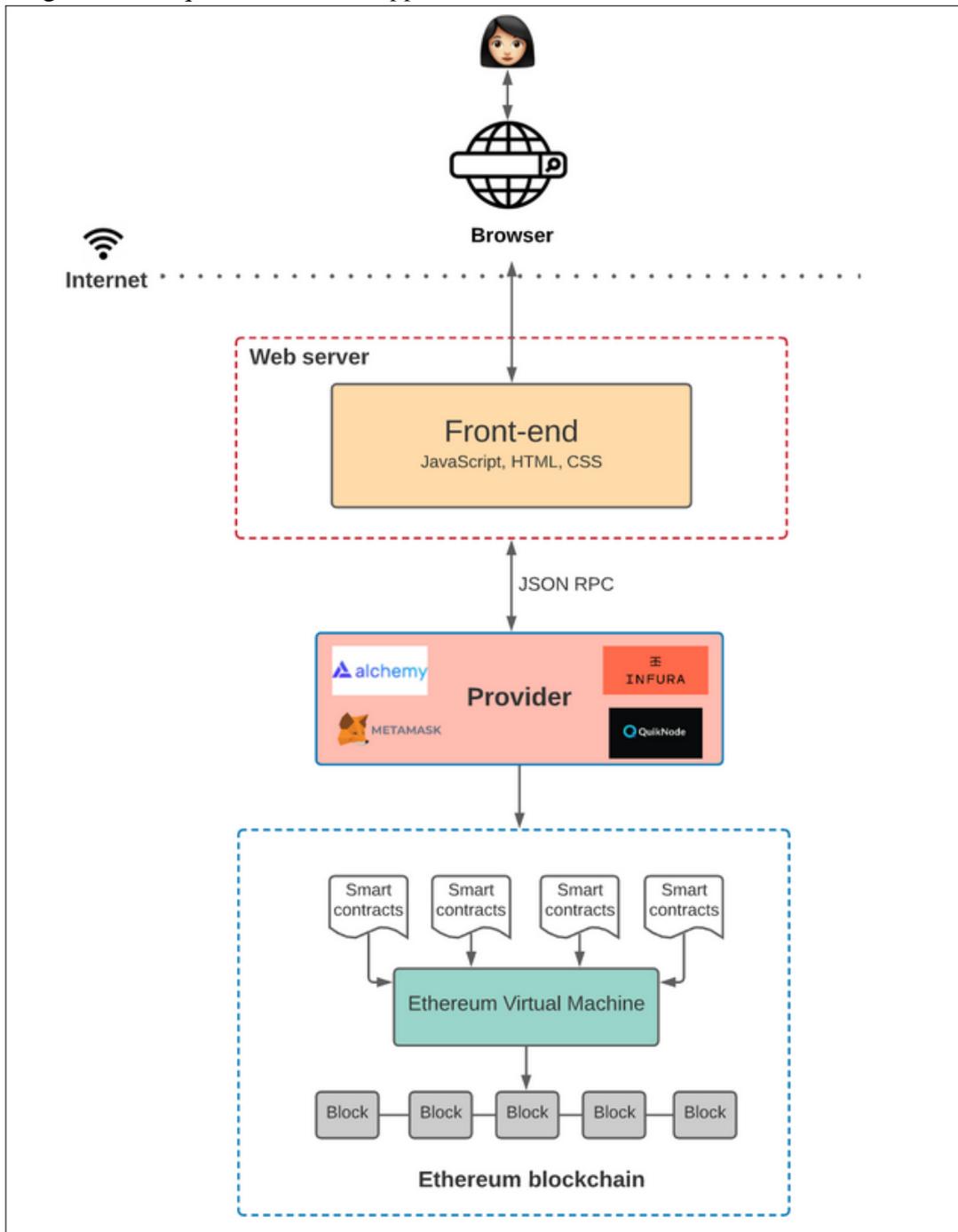
Nesta etapa, após a escolha da plataforma *blockchain* a ser utilizada, foi realizada a implementação da rede *blockchain* no ambiente de nuvem da AWS, para analisar o desempenho da aplicação desenvolvida. Os detalhes sobre a implementação da rede estão descritos na sessão Resultados 5.

4.6 Análise de desempenho

Nesta etapa será definido os cenários de teste e as características da rede *blockchain* que serão utilizadas para a realização dos testes e avaliação da proposta, tais como, topologia de rede, quantidade de usuários simultâneos, quantidade de nós de consenso, dentre outros. Preliminarmente, as métricas selecionadas para análise foram: a tempo de processamento do bloco, a taxa de propagação das transações e a taxa de transações por segundo. Foi utilizado a ferramenta de monitoramento de desempenho *Prometheus* para coletar as métricas da rede Blockchain.¹

¹ <https://prometheus.io/>

Figura 1 – Arquitetura de um *dapp*



Fonte: <https://www.web3dev.com.br/lorenzobattistela/a-arquitetura-de-um-aplicativo-da-web-30-33bp>

5 RESULTADOS

A seguinte sessão destina-se a apresentação dos resultados alcançados com este trabalho: o desenvolvimento da aplicação web e as funcionalidades do sistema, o desenvolvimento dos contratos inteligentes e a avaliação de desempenho da aplicação.

5.1 Apresentação do sistema

A seguinte sessão apresenta o desenvolvimento da aplicação web proposta neste trabalho, a arquitetura do sistema, principais funcionalidades da aplicação e o desenvolvimento dos contratos inteligentes utilizados na solução proposta.

5.1.1 Aplicação Web

A aplicação web desenvolvida tem como objetivos principais permitir aos usuários, agentes na cadeia de produção, registrar seus produtos no sistema, visualizar sua produção, realizar transações de produtos entre os elos da cadeia e rastreá-los ao longo de toda a cadeia de produção.

A aplicação web está dividida em duas partes, uma destinada aos produtores, processadores, distribuidores e comerciantes de mel, estes precisam registrar-se no sistema para ter acesso as operações citadas a cima. A outra parte destina-se aos consumidores, onde poderão rastrear a origem do mel que estão consumindo.

A Figura 2 mostra a tela de rastreio de produtos. Esta pagina é composta por um formulário de consulta, que busca as informações sobre um determinado produto por meio do seu id, e uma tabela que mostrará os dados de rastreio do produto, informações de sua origem e informações de registro na *blockchain* por meio do *hash* da transação.

As Figuras 3 e 4 a seguir apresentam as páginas de cadastro e *login* dos usuários, respectivamente. No formulário de registro de usuários as informações como nome, *email*, companhia de alimentos, endereço, certificação, se houver, senha e o perfil de usuário. O *login* dos usuários no sistema é realizado utilizando as informações de *email* e senha fornecidos no registro de usuários.

As sub-sessões a seguir apresentam a aplicação web na visão de cada um dos perfis de usuários cadastrados produtores, processadores, distribuidores e comerciantes.

Figura 2 – Página de rastreio de produtos

Fonte: Elaborada pelo autor.

Figura 3 – Página de cadastro de novos usuários

Fonte: Elaborada pelo autor.

5.1.1.1 Perfil do Produtor

Na página principal do Produtor encontram-se os recursos que podem ser acessados por este perfil de usuário. Na Figura 5 podem ser vistos os recursos disponíveis para este usuário, tais como, registrar novos produtos, listar os produtos, despachar e rastrear os produtos. Para cadastrar novos produtos o usuário deverá clicar na barra de navegação "Registrar" e será direcionado à tela de registro de produtos. Nesta tela é possível escolher entre registrar uma unidade comercial ou unidade de logística, como pode ser visto na Figura 6.

Ao transferir um produto para outro elo da cadeia produtiva o produtor deve registrar este item como produto despachado. Esta ação é feita na tela de despacho de produtos, como mostrado na Figura 7. Ao despachar o produto, o *hash* da transação é capturado e a transação é

Figura 4 – Página de *login*

Fonte: Elaborada pelo autor.

Figura 5 – Página Principal do Produtor

Código	Lote	Recipiente	Florada	Fabricação	Produtor	Peso
01325689...	91346550	Tambor de plástico	Eucalipto	07/44/2023 às 09:44	15610056	20 kg
01325689...	91346550	Tambor de plástico	Eucalipto	07/44/2023 às 09:44	15610056	20 kg
01325689...	91346550	Tambor de plástico	Eucalipto	07/44/2023 às 09:44	15610056	20 kg
01325689...	91346550	Tambor de plástico	Eucalipto	07/44/2023 às 09:44	15610056	20 kg
01325689...	91346550	Tambor de plástico	Eucalipto	07/44/2023 às 09:44	15610056	20 kg

Destino	Unidade	Data de envio
60249358	913465501	06/04/2023 às 14:04
60249358	913465502	07/01/2023 às 19:01

Transação anterior	Transação atual	Origem	Destino	Unidade	Data
913465501	0xc70788b696e51a78c57173ea16837d564f5689a6d0ff9bc2b5f6c298d081b44...	15610056	60249358	913465501	06/04/2023 às 14:04

Fonte: Elaborada pelo autor.

atualizada no contrato *UpdateTransation.sol*.

5.1.1.2 Perfil do Processador

Na página principal do Processador encontram-se os recursos que podem ser acessados por este perfil de usuário. Os recursos que podem ser acessados por este usuário assemelham-se aos recursos do produtor e podem ser vistos na figura 8. O cadastro de novos produtos é

Figura 6 – Produtor: página de registro de produtos

Bem vindo, Samuel Brandao Registrar Despachar Sair

← Voltar

Cadastrar novo mel

Descreva as propriedades do seu mel!

Tambor de Mel Paleta

Código
03213589447526

Peso
20

Recipiente
Tambor de plástico

Sabor
Eucalipto

Fabricação
06/07/2023-09:22:55

Lote
91345550 Gerar Lote

Adicionar

Fonte: Elaborada pelo autor.

Figura 7 – Página de despacho de produtos

Samuel Brandao, produtor Registrar Despachar Sair

← Voltar

Informações de envio

Destinatário
60249358

ID da unidade
798517751

Data de envio
08/07/2023-11:25:35

Identificação da unidade
paleta

Despachar

Fonte: Elaborada pelo autor.

feito na página Registrar Produtos, nela o usuário dispõe de um formulário onde deve inserir as informações do mel produzido conforme descrito na tabela 1. Nesta tela é possível escolher entre registrar uma unidade comercial ou unidade de logística, como pode ser visto na Figura 9. Diferente do Produtor a página principal do Processador tem a opção de receber um carregamento de produtos.

Ao transferir um produto dentro da cadeia produtiva o produtor deve registrar este item como produto despachado. Esta ação é feita na tela de despacho de produtos, como mostrado na Figura 10. Ao despachar o produto, o *hash* da transação é capturado e a transação é atualizada no contrato *UpdateTransation.sol*.

Figura 8 – Página Principal do Processador

Jose Almeida, processador Registrar Receber Despachar Sair

Produtos Recebidos

Unidade	Distribuidor	Data de recebimento
15610056		07/07/2023-19:10:55
913465503	95566008	07/07/2023-20:17:30
913465504	95566008	07/07/2023-21:50:26
913465505	95566008	07/07/2023-21:50:26
913465506	95566008	07/07/2023-21:50:26

Produção

unidade	Lote	Materia-prima	Tipo	Variedade	Peso	Recipiente	Validade	Composiç...
26313420...	26313420	913465503	organico	Eucalipto	100 kg	pote de vidro	07/31/2023 às 22:31	carboidrat...
26313420...	26313420	913465503	organico	Eucalipto	100 kg	pote de vidro	07/31/2023 às 22:31	carboidrat...
26313420...	26313420	913465503	organico	Eucalipto	100 kg	pote de vidro	07/31/2023 às 22:31	carboidrat...
26313420...	26313420	913465503	organico	Eucalipto	100 kg	pote de vidro	07/31/2023 às 22:31	carboidrat...
26313420...	26313420	913465503	organico	Eucalipto	100 kg	pote de vidro	07/31/2023 às 22:31	carboidrat...

Produtos Despachados

Distribuidor	Unidade	Data de envio
36810097	26313420...	08/07/2023-13:28
36810097	82995636	08/07/2023-13:34

Fonte: Elaborada pelo autor.

Figura 9 – Processador: página de registro de produtos

Jose Almeida, processador Registrar Receber Despachar Sair

[Voltar](#)

Beneficiamento Caixa Paleta

ID do beneficiador do mel
913465503

Tipo do mel
Comum

Variedade do mel
Eucalipto

Peso
100

Recipiente
pote de vidro

Validade
07/07/2023-20:37:34

Composição
carboidrato - 100%

Lote
8299566 **Gerar Lote**

Adicionar

Fonte: Elaborada pelo autor.

5.1.1.3 Perfil do Distribuidor

Na página principal do distribuidor encontram-se os recursos que podem ser acessados por este perfil de usuário. Os distribuidores de mel logados na aplicação irão registrar o recebimento e o despacho de produtos, e visualizar a listagem dos produtos recebidos e despachados pelo usuário, como mostrado na Figura 11. As telas referentes ao recebimento e despacho de produtos é semelhante para todos os perfis de usuário e seguem o mesmo padrão de informações da Tabela 1.

Figura 10 – Processador: página de envio de produtos

Jose Almeida, processador Registrar Receber **Despachar** Sair

[← Voltar](#)

Informações de envio

Destinatário
36810097

ID da unidade
2631342042

Data de envio
08/07/2023-13:08:20

Especificação da Unidade
caixa

Despachar

Fonte: Elaborada pelo autor.

Figura 11 – Página Principal do Distribuidor

Pedro Augustos, distribuidor Receber Despachar Sair

Produtos recebidos

Unidade	Origem	Data de envio	Local da entrega
02215643	22658893...	07/20/2023 às 16:20	Rua A, 458
02215644	22658893...	07/20/2023 às 16:20	Rua A, 458
02215645	22658893...	07/20/2023 às 16:20	Rua A, 458
02215646	22658893...	07/20/2023 às 16:20	Rua A, 458

Produtos despachados

Unidade	Destino	Data de envio	Local da entrega
02215643	11223344	08/07/2023-17:16:37	Comercial Seu Joao
02215644	11223344	08/07/2023-17:16:37	Comercial Seu Joao
02215644	11223344	08/07/2023-17:16:37	Comercial Seu Joao
02215645	11223344	08/07/2023-17:16:37	Comercial Seu Joao
02215646	11223344	08/07/2023-17:16:37	Comercial Seu Joao

Fonte: Elaborada pelo autor.

5.1.1.4 Perfil do Comerciante

Os comerciantes logados na aplicação poderão registrar o recebimento de produtos, visualizar o estoque de produtos e rastrear os produtos enviados por seus fornecedores, as telas referente as ações do comerciante estão apresentadas nas Figuras 12 e 13.

5.1.2 Desenvolvimento dos Contratos Inteligentes

Os Contratos Inteligentes utilizados na aplicação foram desenvolvidos em linguagem de programação *Solidity* na versão 0.8.17. Para o desenvolvimento e implantação dos contratos na rede foi utilizado o *framework Truffle*. O *Truffle* é uma ferramenta para desenvolvimento

Figura 12 – Página Principal do Comerciante

João Figueredo, comerciante Receber Sair

Unidade	Distribuidor	Data do recebimento
02215645	18578769	07/08/2023 às 18:48
02215646	18578769	07/08/2023 às 18:48

Rastreo de Produtos

23569875 Buscar

Transação anterior	Transação atual	Origem	Destino	Unidade	Data
23569875	0x35a6c4266456d714e791297207c2ea54973a73c2fe9a0c31a589eaa7f351701c	18578769	60414668	23569875	07/20/2023 às 18:20
0x35a6c4266456d714e791297207c2ea54973a73c2fe9a0c31a589eaa7f351701c	0xd9f2a01908bc2c88d683aebdc5bee1d22051d98526acfb8f9254320b104ecc8d7	18578769	60414668	23569875	07/21/2023 às 18:21

Fonte: Elaborada pelo autor.

Figura 13 – Comerciante: página de recebimento de produtos

João Figueredo, comerciante Receber Sair

← Voltar

Registrar Recebimento de Produtos

Fornecedor/Distribuidor
18578769

Unidade
23569875

Idem que compõem a unidade
235698751,235698752,235698753,235698754

Data do recebimento
07/08/2023

Tipo de unidade
caixa

Registrar

Fonte: Elaborada pelo autor.

de contratos inteligentes que facilita o desenvolvimento, compilação, configuração de testes automatizados e criação de *scripts* para implantação dos contratos. Foram desenvolvidos seis contratos, a as sessões a seguir descrevem as funcionalidades de cada contrato.

5.1.2.1 Contrato Authentication

O contrato *Authentication* implementa as funções de cadastro de novos usuários no sistema e a autenticação destes usuários conforme o papel do usuário no sistema, além de fornecer permissões para executar funções que alteram o estado da *blockchain*. A Figura 1 apresenta a implementação da função *register()*. A função *register* recebe como parâmetros de entrada uma estrutura de dados do tipo *User* e um *password*.

Código-fonte 1 – Código fonte em Solidity

```
1     function register(User memory _user, string memory _password)
2         public {
3             bytes32 password = keccak256(abi.encodePacked(_user.email,
4                 _password));
5             uint hashDigits = 8;
6             uint hashModulus = 10 ** hashDigits;
7             uint _hash = uint(
8                 keccak256(
9                     abi.encodePacked(
10                        _user.addr,
11                        _user.name,
12                        _user.email,
13                        block.timestamp
14                    )
15                )
16            );
17            string memory _id = uintToString(_hash % hashModulus);
18            users[_id] = User(
19                _user.addr,
20                _id,
21                _user.name,
22                _user.email,
23                _user.certification,
24                _user.company,
25                _user.role
26            );
27            login[password] = _id;
28            status[_id] = true;
29        }
```

Fonte: Elaborado pelo autor.

5.1.2.2 Contrato *Production*

O contrato *Production* implementa as funcionalidades referente aos produtores de mel. Por meio deste contrato os produtores logados na aplicação web poderão cadastrar novos produtos, que podem ser unidades comerciais ou unidades de logística, listar os produtos cadastrados e registrar os produtos despachados. A figura 2 mostra a implementação da função *newDrum()*.

Código-fonte 2 – Código fonte em Solidity

```
1     function newDrum(  
2         string memory _userId,  
3         string memory _batch,  
4         string memory _code,  
5         uint64 _weight,  
6         string memory _packing,  
7         string memory _flowering,  
8         string memory _dateTime,  
9         string[] memory _hivesId  
10    ) public onlyOWNER(_userId) {  
11        string memory _id = string(  
12            abi.encodePacked(_batch, uintToString(serialNumber))  
13        );  
14        require(bytes(drums[_id].id).length == 0);  
15        drums[_id] = Drum(  
16            _id,  
17            _batch,  
18            _code,  
19            _userId,  
20            _weight,  
21            _packing,  
22            _flowering,  
23            _dateTime,  
24            _hivesId  
25    );
```

```

26     drumsId[_batch].push(_id);
27     serialNumber++;
28     emit NewUnit(_userId, _id);
29 }

```

Fonte: Elaborado pelo autor.

5.1.2.3 Contrato Processing

O contrato *Processing* implementa as funcionalidades referente aos processadores de mel. Por meio deste contrato os processadores poderão registrar o recebimento de de novos carregamentos, cadastrar novos produtos, listar os produtos cadastrados e registrar os produtos despachados. A figura 3 mostra a implementação da função *newHoney()*.

Código-fonte 3 – Código fonte em Solidity

```

1     function newHoney(
2         Honey memory _honey,
3         string memory _userId
4     ) public onlyOWNER(_userId) {
5         string memory _id = string(
6             abi.encodePacked(_honey.batch, uintToString(
7                 serialNumber))
8         );
9         require(bytes(honeys[_id].id).length == 0);
10        honeys[_id] = Honey(
11            _id,
12            _honey.batch,
13            _honey.code,
14            _honey.feedstockBatch,
15            _honey.honeyType,
16            _honey.variety,
17            _honey.weight,
18            _honey.packaging,
19            _honey.validity,
20            _honey.composition

```

```

20     );
21     honeysId[_userId].push(_id);
22     serialNumber++;
23     emit NewUnit(_userId, _id);
24 }

```

Fonte: Elaborado pelo autor.

5.1.2.4 Contratos *Distribution* e *Merchant*

O contrato *Distribution* e *Merchant* implementam as funcionalidades referente respectivamente aos distribuidores de mel e comerciantes, tanto atacadistas como varejistas. Por meio destes contratos os distribuidores e comerciantes de mel poderão registrar o recebimento de novos carregamentos, listar os produtos cadastrados e registrar os produtos despachados. As Figuras 4 e 5 mostram respectivamente a implementação da função *dispatcher()*, no contrato *Distribution* e da função *receiver()*, no contrato *Merchant*.

Código-fonte 4 – Código fonte em Solidity

```

1     function dispatcher(
2         string memory _id,
3         string memory _distributor,
4         string memory _receiver,
5         string memory _dateTime,
6         string memory _local,
7         UnitType _unitType
8     ) public onlyOWNER(_distributor) {
9         dispatchedUnits[_id] = DispatchedUnit(
10            _id,
11            _receiver,
12            _dateTime,
13            _local,
14            _unitType
15        );
16        dispatchedUnitsId[_distributor].push(_id);
17    }

```

Fonte: Elaborado pelo autor.

Código-fonte 5 – Código fonte em Solidity

```
1     function receiver(  
2         string memory _sender,  
3         string memory _receiver,  
4         string memory _unit,  
5         string[] memory _units,  
6         string memory _date,  
7         UnitType _unitType  
8     ) public onlyOWNER(_receiver) {  
9         registerReceivedUnit(  
10            _unit,  
11            _units,  
12            _sender,  
13            _date,  
14            _unitType,  
15            _receiver  
16        );  
17    }
```

Fonte: Elaborado pelo autor.

5.1.2.5 Contrato *UpdateTransaction*

Por fim, o contrato *UpdateTransaction* implementa as funções de registrar e listar as transações de produtos feitas entre os usuários ao longo de toda a cadeia produtiva. A função *updateTr()* utiliza uma estrutura associativa de chave e valor para armazenar uma lista de transações referentes a um determinado produto. A função *search()* possibilita o rastreamento de um determinado produto passando o id do produto para a função *search()*. A Figura 6 mostra a implementação da função *updateTr()*.

Código-fonte 6 – Código fonte em Solidity

```
1     function updateTr(  
2         string memory _currentTx,  
3         string memory _sender,  
4         string memory _receiver,  
5         string memory _unit,  
6         string memory _date  
7     ) public onlyOWNER(_sender) {  
8         string memory previousTx;  
9         if (transactions[_unit].length == 0) {  
10            previousTx = _unit;  
11        } else {  
12            Transaction memory tr = transactions[_unit][  
13                transactions[_unit].length - 1  
14            ];  
15            require(  
16                keccak256(abi.encodePacked(_receiver)) ==  
17                    keccak256(abi.encodePacked(tr.receiver)) ||  
18                    keccak256(abi.encodePacked(_sender)) ==  
19                    keccak256(abi.encodePacked(tr.receiver)),  
20                "Transacao Inconcistente!"  
21            );  
22            previousTx = tr.currentTx;  
23        }  
24        transactions[_unit].push(  
25            Transaction(  
26                previousTx,  
27                _currentTx,  
28                _sender,  
29                _receiver,  
30                _unit,  
31                _date  
32            )  
33        );  
34        userTransactions[_sender].push(_unit);
```

Fonte: Elaborado pelo autor.

5.2 Análise de Desempenho

Esta sessão destina-se a apresentação dos testes realizados para avaliar o desempenho e funcionalidades da aplicação, desde a preparação do ambiente de teste, configuração da rede de teste e coleta das métricas de avaliação e análise dos resultados.

5.2.1 A Rede *Blockchain*

A Rede *Blockchain* utilizada para a realização dos testes foi implantada no ambiente da plataforma de nuvem *AWS Academy*. Esta sessão destina-se a descrever as configurações feitas na plataforma de nuvem *Amazon Web Service (AWS)* e a configuração e implementação da rede *Blockchain* utilizada para realização de testes.

Os nós da rede foram instanciados usando *Geth*, um cliente *Ethereum* escrito em Go para execução de um nó *Ethereum*. Cada nó *Ethereum* que compõe a rede está sendo executado em uma instância *Elastic Compute Cloud (EC2)* do tipo *t2.medium*, exceto o *bootnode* que está sendo executado em uma instância do tipo *t2.micro*. Cada nó foi instanciado com SO Ubuntu 22.04. O arquivo de configuração do bloco gênese está apresentado no Apêndice A. Neste arquivo são estabelecidas as informações necessárias para a criação do primeiro bloco da cadeia, além de definir o algoritmo de consenso, a quantidade de ativos disponíveis na rede, os nós de consenso, a taxa de criação de blocos, etc.

A topologia da rede está disposta da seguinte forma. Um nó de inicialização *bootnode* foi configurado para iniciar a rede e permitir a conexão entre os demais nós da rede. Após a inicialização do *bootnode* os nós de consenso e os nós de execução podem se conectar á rede usando a *flag* `-bootnodes` na inicialização. Os nós de consenso são responsáveis por gerar novos blocos e adicioná-los na cadeia de blocos, essa função é habilitada usando a *flag* `-miner` na inicialização do nó. Por fim, um nó de execução foi configurado para receber novas transações e enviá-las para os nós de consenso, essa função é habilitada através da API JSON-RPC. O script *start-geth.sh* foi escrito para realizar a inicialização dos nós, cada um com sua configuração específica, como pode ser visto no Apêndice B.

5.2.1.1 Cenários de teste

Nesta sessão foram definidos os cenários de testes para avaliação de desempenho da rede *blockchain* com o intuito de analisar o comportamento da rede ao simular a execução de múltiplas transações na rede simultaneamente. Foram criados três cenários de testes, onde em cada cenário cinco usuários, com o perfil Produtor, realizam trinta transações referentes a criação de um novo produto, alterando em cada cenário de teste a quantidade de nós de consenso na rede, como descrito na Tabela 1.

A ferramenta de monitoramento *Prometheus* foi utilizada para monitorar o comportamento da rede e coletar os dados para serem apresentados no *Grafana*. Com essas duas ferramentas foi possível medir o tempo de processamento dos blocos, a taxa da propagação das transações, a taxa de requisições por segundo, além de monitorar o consumo de recursos do sistema como uso de CPU, memória, disco e rede.

Tabela 1 – Cenários de teste

Cenários	Usuários	Transações	Nós validadores
Cenário 1	5	30	3
Cenário 2	5	30	4
Cenário 3	5	30	5

Fonte: elaborada pelo autor.

5.2.1.2 Resultados do Experimento 1

As figuras 14, 15 e 16 mostram os resultados obtidos no primeiro cenário de testes onde a rede utilizada para o teste foi configurada com três nós de consenso. A Figura 14 mostra que o tempo de execução e validação dos blocos, durante o envio das transações, foi em média de 777 μ s e 47 μ s respectivamente. A Figura 15 mostra a taxa de propagação das transações válidas, representa o número de transações válidas que foram aceitas pelo nó e estão prontas para serem processadas. Em média 1,20 transações/s. Já a Figura 16 mostra a taxa de sucesso das chamadas RPC recebidas pelo nó de execução. No primeiro teste a média foi de 2,07 req/s.

5.2.1.3 Resultados do Experimento 2

No segundo cenário de teste foram realizadas as mesma operações do primeiro, alterando a quantidade de nós de consenso da rede de três para quatro nós. Os resultados deste

Figura 14 – Taxa de processamento do bloco (experimento 1)



Fonte: Elaborada pelo autor.

Figura 15 – Taxa de propagação das transações (experimento 1)



Fonte: Elaborada pelo autor.

Figura 16 – Taxa de requisições por segundo (experimento 1)



Fonte: Elaborada pelo autor.

teste mostram uma diminuição do tempo de processamento do bloco, como visto na figura 17. A figura 18 mostra que a taxa de propagação das transações permaneceu praticamente a mesma do teste anterior, 1,31 transações/s em média. porém a taxa de requisições por segundo aumentou de 2,07 req/s para 6,75 req/s, como visto na Figura 19.

Figura 17 – Taxa de processamento dos blocos (experimento 2)



Fonte: Elaborada pelo autor.

Figura 18 – Taxa de propagação das transações (experimento 2)



Fonte: Elaborada pelo autor.

Figura 19 – Taxa de requisições por segundo (experimento 2)



Fonte: Elaborada pelo autor.

5.2.1.4 Resultados do Experimento 3

No terceiro cenário de teste foram realizadas as mesmas operações do primeiro e segundo cenários, alterando a quantidade de nós de consenso da rede para cinco nós. Os resultados obtidos deste teste mostram que a taxa de propagação das transações e a taxa de requisições recebidas pelo nó continuaram praticamente as mesmas em relação ao experimento anterior, como mostram as figuras 21 e 22, respectivamente. A figura 20 mostra que o tempo de processamento dos blocos aumentou de 25,2 μ s para 31,0 μ s.

Figura 20 – Taxa de processamento dos blocos (experimento 3)



Fonte: Elaborada pelo autor.

Figura 21 – Taxa de propagação das transações (experimento 3)



Fonte: Elaborada pelo autor.

Figura 22 – Taxa de requisições por segundo (experimento 3)



Fonte: Elaborada pelo autor.

Este trabalho propôs-se ao desenvolvimento de uma aplicação web que possibilitasse a rastreabilidade da cadeia produtiva do mel usando a tecnologia *Blockchain*. Após longo trabalho chegou-se aos seguintes resultados: foi desenvolvido um protótipo de uma aplicação web que possibilita o registro e a visualização da produção, industrialização e distribuição do mel, além de possibilitar o rastreio de produtos tanto pelos produtores como consumidores de mel, foram desenvolvidos contratos inteligentes que permitem a interação entre a rede blockchain e a aplicação web e por ultimo foi realizada a avaliação da rede blockchain e da aplicação.

Porém, algumas funcionalidades da aplicação podem ser melhoradas como a implementação de *QR code* para facilitar a leitura de dados no sistema. A integração do sistema com monitoramento de colmeias pode aumentar a confiabilidade do sistema. Além da realização de testes mais abrangentes que permitam dimensionar a escalabilidade do sistema.

6 CONCLUSÕES E TRABALHOS FUTUROS

Neste trabalho apresentamos uma proposta de aplicação web baseada em blockchain para prover a rastreabilidade da cadeia produtiva do mel, onde os registros de dados da criação e distribuição dos produtos ao longo da cadeia produtiva são armazenados na cadeia de blocos distribuídos da blockchain. A aplicação de blockchain na rastreabilidade da cadeia produtiva do mel mostra grande potencial para aumentar a confiança do consumidor e melhorar a qualidade do produto, visto que a natureza imutável do registro distribuído das redes blockchain torna as informações armazenadas mais confiáveis e transparentes.

Com base nos resultados obtidos nos testes da aplicação proposta, o uso da tecnologia blockchain é uma solução viável para prover a rastreabilidade da cadeia produtiva do mel. Porém mais teste precisam ser realizados que permitam medir o comportamento da rede à medida que a participação no consenso e a quantidade transações enviadas para a rede aumentam, podendo assim testar a escalabilidade do sistema.

Com a evolução contínua da tecnologia blockchain e pesquisas futuras, podemos esperar avanços significativos na rastreabilidade de alimentos e em outros setores, proporcionando benefícios tangíveis para a indústria e os consumidores.

REFERÊNCIAS

- ALMEIDA, M. A. D. d.; CARVALHO, C. M. S. Apicultura: uma oportunidade de negócio sustentável. **Salvador: SEBRAE Bahia**, 2009.
- BASHIR, I. **Mastering blockchain**. [S. l.]: Packt Publishing Ltd, 2017.
- BUAINAIN, A. M. *et al.* **Cadeias produtivas de flores e mel**. [S. l.]: Bib. Orton IICA/CATIE, 2007. v. 9.
- BUMBLAUSKAS, D.; MANN, A.; DUGAN, B.; RITTMER, J. A blockchain use case in food distribution: Do you know where your food has been? **International Journal of Information Management**, Elsevier, v. 52, p. 102008, 2020.
- CASTRO, M.; LISKOV, B. Practical byzantine fault tolerance and proactive recovery. **ACM Transactions on Computer Systems (TOCS)**, ACM New York, NY, USA, v. 20, n. 4, p. 398–461, 2002.
- CENTENO, M. A. An introduction to simulation modeling. In: IEEE. **Proceedings Winter Simulation Conference**. [S. l.], 1996. p. 15–22.
- CHICARINO, V.; JESUS, E. F.; ALBUQUERQUE, C.; ROCHA, A. A. Uso de blockchain para privacidade e segurança em internet das coisas. **Livro de Minicursos do VII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais**. Brasília: SBC, v. 28, 2017.
- DOBBINS, A.; SPRINKLE, A.; HADLEY, B.; CAZIER, J.; WILKES, J. Blocks for bees: Solving bee business problems with blockchain technology. **Bus. Students' Pers. Branding, Empirical Invest.**, v. 1, p. 11, 2018.
- DONNELLY, K. A.-M.; ROEST, J. van der; KARLSEN, K. M.; OLSEN, P. Traceability of honey—specification of the information to be recorded in honey distribution chains. **Nofima rapportserie**, Nofima AS, 2008.
- ETHEREUM. **INTRODUCTION TO DAPPS**. 2023. Acesso em: 30 mai. 2023. Disponível em: <https://ethereum.org/en/developers/docs/dapps/>.
- FAO. **Crops and livestock products**. 2020. Acesso em: 20 jul. 2021. Disponível em: <http://www.fao.org/faostat/en/?#data/QCL/visualize>.
- FERREIRA, T. S.; ASSIS, D. C. S. d. Os produtos apícolas: produção e características de identidade e qualidade do mel. **Cad. técn. Vet. Zoot.**, p. 51–63, 2020.
- FLECK, L.; BELLINASSO, J. Estudo da cadeia do mel e derivados: Território central rs. **Ministério do Desenvolvimento Agrário Secretaria de Desenvolvimento Territorial**. Porto Alegre-RS, 2008.
- GARCÍA, N. L. The current situation on the international honey market. **Bee World**, Taylor & Francis, v. 95, n. 3, p. 89–94, 2018.
- GOLAN, E. H.; KRISOFF, B.; KUCHLER, F.; CALVIN, L.; NELSON, K. E.; PRICE, G. K. **Traceability in the US food supply: economic theory and industry studies**. [S. l.], 2004.

- GORROI, G.; FREITAS, L. P. V. d.; ASSIS, D. C. S. d. Apicultura: o manejo das abelhas do gênero apis. **Cad. técn. Vet. Zoot.**, p. 9–36, 2020.
- JOHNSON, R. **Food fraud and economically motivated adulteration of food and food ingredients**. [S. l.]: Congressional research service Washington DC, 2014.
- MAGALHÃES, A.; CHAVES, R.; SALÉ, N.; ROESE, A.; SILVA, T. Mel no programa de alimentação escolar: oportunidade e desafio para o agronegócio apícola. In: **XLV Congresso da SOBER “Conhecimentos para Agricultura do Futuro**. [S. l.: s. n.], 2007.
- MENDONÇA, R. D.; GOMES, O. S.; PEREIRA, P. C.; VIEIRA, A. B.; NACIF, J. A. Utilização de blockchain na rastreabilidade da cadeia produtiva do leite. In: **SBC. Anais do III Workshop em Blockchain: Teoria, Tecnologia e Aplicações**. [S. l.], 2020. p. 55–60.
- MINGXIAO, D.; XIAOFENG, M.; ZHE, Z.; XIANGWEI, W.; QIJUN, C. A review on consensus algorithm of blockchain. In: **2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)**. [S. l.: s. n.], 2017. p. 2567–2572.
- MORAIS, A. M. de; SILVA, A. J. da; MENDONÇA, S. F. T. de O. Qrqueijo: Sistema de emissão e validação de identificadores de queijos utilizando blockchain. **GESTÃO. Org**, Universidade Federal de Pernambuco, v. 18, n. 2, p. 159–168, 2020.
- PHIPPS, R. **Investigating Food Fraud in the Honey Industry**. 2020. <https://www.news-medical.net/news/20210316/Investigating-Food-Fraud-in-the-Honey-Industry.aspx>. Acesso em: 13 jun. 2021.
- SANTOS, C. S. dos; RIBEIRO, A. de S. Apicultura uma alternativa na busca do desenvolvimento sustentável. **Revista verde de agroecologia e desenvolvimento sustentável**, Grupo Verde de Agroecologia e Abelhas, v. 4, n. 3, p. 1, 2009.
- SILVA, F.; CASTRO, A. d.; SILVA, F. da; YANO, I. Uso de blockchain para registro de dados de cadeia de suprimentos verde da indústria sucroenergética. In: **IN: ENCONTRO NACIONAL DE ENGENHARIA DE PRODUÇÃO, 40.**, 2020, FOZ DO IGUAÇU . . . **Embrapa Informática Agropecuária-Artigo em anais de congresso (ALICE)**. [S. l.], 2020.
- SWAN, M. **Blockchain: Blueprint for a new economy**. [S. l.]: "O'Reilly Media, Inc.", 2015.
- SZABO, N. **Smart contracts**. 1994. Acesso em: 10 ago. 2021. Disponível em: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>.
- VIDAL, M. d. F. Evolução da produção de mel na área de atuação do bnb. Banco do Nordeste do Brasil, 2020.
- WANG, W.; HOANG, D. T.; HU, P.; XIONG, Z.; NIYATO, D.; WANG, P.; WEN, Y.; KIM, D. I. A survey on consensus mechanisms and mining strategy management in blockchain networks. **IEEE Access**, v. 7, p. 22328–22370, 2019.
- YADAV, R.; SOUSA, E.; CALLOU, G. Performance comparison between virtual machines and docker containers. **IEEE Latin America Transactions**, IEEE, v. 16, n. 8, p. 2282–2288, 2018.

APÊNDICE B – SCRIPT DE INICIALIZAÇÃO DOS NÓS DA REDE *BLOCKCHAIN*

Código-fonte 8 – Código fonte em ShellScript

```

1 NODETYPE=$1
2 NETWORKID=5045
3 DATADIR=/home/ubuntu/data
4 BOOTNODEIP=<seu ip>
5 NODEIP=$2
6 BOOTNODEPORT=30305
7 MYNODEPORT=$3
8 ACCOUNT=$(cat data/keystore/* | jq ".address" | sed -e 's/\\"//g')
9 BOOTNODEID=e8fe2e9160d90c94b0799785960937e292511615950ff43a007c6c7ed9959
10 83cfb5c8a5b8245ca838206cae9b30be99c09af32cc2d29b0b5cb264dbbe51e9587
11
12 if [[ "$NODETYPE" == "node" ]]; then
13     sudo geth --datadir=$DATADIR --syncmode "full" --bootnodes "enode://
        $BOOTNODEID@$BOOTNODEIP:$BOOTNODEPORT" --networkid $NETWORKID --port
        $MYNODEPORT --netrestrict "172.31.0.0/16" --ws --ws.addr $NODEIP --ws.
        port 8546 --ws.api eth,net,web3,personal --ws.origins '*' --metrics --
        metrics.addr <ip> --metrics.port 6060 --metrics.expensive console
14 elif [[ "$NODETYPE" == "mine" ]]; then
15     sudo geth --datadir=$DATADIR --bootnodes "enode://$BOOTNODEID@$BOOTNODEIP:
        $BOOTNODEPORT" --networkid $NETWORKID --port $MYNODEPORT --netrestrict
        "172.31.0.0/16" --syncmode "full" --gcmode "archive" --miner.etherbase=
        $ACCOUNT --mine --unlock $ACCOUNT --password .password
16 elif [[ "$NODETYPE" == "boot" ]]; then
17     sudo geth --datadir=$DATADIR --nodekey ./boot.key --networkid $NETWORKID
        --netrestrict "172.31.0.0/16" --nat extip:$BOOTNODEIP --port
        $BOOTNODEPORT
18 fi

```

Fonte: Elaborado pelo autor.