UNIVERSIDADE ESTADUAL DE PONTA GROSSA
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS GRADUAÇÃO EM
COMPUTAÇÃO APLICADA

HUGO LEONARDO PETLA SILVA

MÉTODO DE RASTREABILIDADE DE PRODUTOS AGRÍCOLAS COM A UTILIZAÇÃO DE *BLOCKCHAIN*

PONTA GROSSA
2020

HUGO LEONARDO PETLA SILVA

MÉTODO DE RASTREABILIDADE DE PRODUTOS AGRÍCOLAS COM A UTILIZAÇÃO DE *BLOCKCHAIN*

Dissertação apresentada para obtenção do título de Mestre em Computação Aplicada na Universidade Estadual de Ponta Grossa. Área de concentração: Modelagem Computacional Aplicada.

Orientador: Prof.ª. Drª. Maria Salete Marcon Gomes Vaz

PONTA GROSSA

2020

Silva, Hugo Leonardo Petla
S586 Método de rastreabilidade de produtos agrícolas com a utilização de *blockchain* / Hugo Leonardo Petla Silva. Ponta Grossa, 2020.
42 f.

Dissertação (Mestrado em Computação Aplicada - Área de Concentração: Computação para Tecnologias em Agricultura), Universidade Estadual de Ponta Grossa.

Orientadora: Profa. Dra. Maria Salete Marcon Gomes Vaz.

1. Blockchain. 2. Cadeia de suprimentos. I. Vaz, Maria Salete Marcon Gomes. II. Universidade Estadual de Ponta Grossa. Computação para Tecnologias em Agricultura. III.T.

CDD: 004

Ficha catalográfica elaborada por Maria Luzia Fernandes Bertholino dos Santos- CRB9/986

UNIVERSIDADE ESTADUAL DE PONTA GROSSA
Av. General Carlos Cavalcanti, 4748 - Bairro Uvaranas - CEP 84030-900 - Ponta Grossa - PR - https://uepg.br

TERMO

DE APROVAÇÃO

Hugo Leonardo Petla Silva

MÉTODO DE RATREABILIDADE DE PRODUTOS AGRÍCOLAS COM A UTILIZAÇÃO DE BLOCKCHAIN

Dissertação aprovada como requisito parcial para obtenção do grau de Mestre no Programa de Pós-Graduação em Computação Aplicada da Universidade Estadual de Ponta Grossa, pela seguinte banca examinadora:

Prof(a). Dr(a). Maria Salete Marcon Gomes Vaz - *UEPG*

Prof. Dr. Antonio Carlos de Francisco - *UTFPR*

Prof. Dr. Arion de Campos Junior - *UEPG*

Ponta Grossa, 29 de maio de 2020.

Documento assinado eletronicamente por **Maria Salete Marcon Gomes Vaz**, **Professor(a)**, em 02/06/2020, às 10:18, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Arion de Campos Junior**, **Professor(a)**, em 02/06/2020, às 10:20, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ANTONIO CARLOS DE FRANCISCO**, **Usuário Externo**, em 02/06/2020, às 11:48, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.uepg.br/autenticidade informando o código verificador **0224659** e o código CRC **EA6C2F4E**.

RESUMO

O modelo de produção e consumo de alimentos percorre uma grande cadeia logística até chegar ao consumidor final. O uso da cadeia de suprimentos prevê todas as atividades de movimentação e armazenagem, desde o momento em que um produto é adquirido até o momento do consumo, a um custo razoável. O aumento da preocupação dos consumidores com a procedência dos alimentos, demanda sistemas de rastreabilidade inseridos nas cadeias produtivas. Uma melhora potencial para a rede de suprimentos é a utilização da *blockchai. Blockchain* permite a geração de protocolos de transações de maneira segura. Os objetivos da dissertação são levantar o estado da arte da gestão da cadeia de suprimentos, desenvolver o método baseado em *blockchain* e aplicar o método na rastreabilidade de produtos agrícolas. Para validação do método foi definida a erva-mate na cadeia de suprimentos. Foi utilizado Node.js para o desenvolvimento da *blockchain*, seguindo as definições e necessidades principais de imutabilidade de dados e segurança dos dados. A rastreabilidade e a transparência de transações voltadas a *commodities* resultam o aumento da confiança dos utilizadores. O fato da rastreabilidade ser acessível e a proteção que a criptografia da *blockchain* garante, evitam ocorrências de má conduta e há diminuição na existência de dados falhos ou que não correspondem com a realidade. Conclui-se que *blockchain* é uma maneira de entrega de alimentos seguros de uma forma transparente, pois torna todos os dados gerados verificáveis e acessíveis.

Palavras-chave: *blockchain;* cadeia de suprimentos;

ABSTRACT

The food production and use model runs through a large logistics chain until it reaches the final consumer. The use of the supply chain provides the awareness of all the storage activities, from the moment a product is purchased until the moment of consumption, at a reasonable cost. With the increase in consumer concern with the origin of food, create the necessity for traceability systems inserted in the production chains. A potential improvement that can bring to the supply chain is the use of blockchain. Blockchain allows the generation of transaction protocols in a secure manner. The objectives of the dissertation are to survey the state of the art of supply chain management, develop the blockchain-based method and apply it to the traceability of agricultural products. For the development, the 'erva-mate' was defined for the study of its supply chain. Node.js was used for the development of the blockchain, following the main definitions and needs of data immutability and data security. The traceability and transparency of transactions applied to commodities result in the incresse of the user confidence. The fact that traceability is accessible to everyone and the protection that blockchain cryptography guarantees, remove the gaps for misconduct and there is also a decrease in the existence of data that is flawed or does not correspond with reality. It was concluded that blockchain is a way of delivering safe food in a transparent way, as it makes all generated data verifiable and accessible.

Keywords: blockchain; supply chain

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

1.1 MOTIVAÇÃO

O modelo de produção e consumo de alimentos percorre uma grande cadeia logística até chegar ao consumidor final. A falta de segurança dentro dessa cadeia permite a diminuição da qualidade e pode haver contaminação dos alimentos, colocando em risco a saúde dos consumidores e diminuindo a competitividade.

Ações foram criadas para eliminar ou prevenir riscos à saúde e intervir nos problemas sanitários decorrentes de várias fontes, como o controle de bens de consumo que, direta ou indiretamente, se relacionam com a saúde, compreendidas todas as etapas e processos, da produção ao consumo; e o controle da prestação de serviços que se relaciona direta ou indiretamente com a saúde (BRASIL, 1990).

A Agência Nacional de Vigilância Sanitária - ANVISA foi criada com o objetivo de proteger a saúde da população brasileira, e conta com a ajuda da sociedade na adoção de medidas (BRASIL, 1999). A criação da ANVISA mostrou a preocupação do brasileiro em torno da segurança e qualidade dos alimentos (MADEIRA; FERRÃO, 2002).

O Comitê da Organização das Nações Unidas para Alimentação e Agricultura (FAO), estimou que os principais problemas relacionados à saúde no mundo são causados por doenças oriundas de alimentos contaminados (JOINT et. al., 1984). Akutsu et. al.(2005), comprovaram que doenças oriundas de alimentos são, na grande maioria, contribuintes para os índices de morbidade nos países da América Latina e a qualidade higiênico-sanitária deve continuar sendo amplamente estudada e discutida, uma vez que a população depende de alimentos e, ao mesmo tempo, é afetada por doenças relacionadas a falta de controle sanitário.

Existem fatores que compreendem a redução da efetividade das ações realizadas para o controle sanitário. Entre eles destacam-se (PIOVESAN, 2005): uma abordagem fracionada do campo de atuação, pouca troca de informação e articulações intra e interinstitucional, falta de recursos humanos, qualificação técnica de má qualidade entre os profissionais, sistemas de informação pouco desenvolvidos e que não abrangem a totalidade dos processos, despreparo para uso de dados disponíveis, assim como falta de mobilização e desinformação da sociedade.

Atualmente, está ocorrendo uma evolução na logística, passando a ser um recurso chave na competitividade de empresas. Anteriormente, a logística era confundida apenas com o transporte e armazenamento de *commodities*, e agora passou a ser crucial e reconhecida pela integração dos processos de controle de produtos, atuando ativamente no gerenciamento da cadeia de suprimentos.

O uso da cadeia de suprimentos prevê todas as atividades de movimentação e armazenagem, desde o momento em que um produto é adquirido até o momento do consumo, a um custo razoável. Portanto, as cadeias produtivas correspondem aos produtores, fornecedores, agentes de distribuição e comercialização, indústrias e consumidores finais. A gestão da logística e de todas as informações produzidas na cadeia, permite a avaliação dos pontos fortes e fracos da cadeia de fornecimento, auxilia a tomada de decisões, diminui os custos para manter um nível de operações próximo do ideal, aumenta da qualidade e a partir disso há aumento da competitividade, agregando valor (LUSTOSA et. al., 2008). É possível verificar a relevância competitiva da *supply chain* nas empresas, e com isso torna necessárias a transparência e a segurança entre as informações, já que se dados relevantes forem armazenados de maneira local, com cada entidade contendo seu banco de dados torna-se fácil burlar e alterar esses dados.

O Brasil, numa visão global, é considerado grande potência na produção de alimentos. O Brasil utilizou cerca de 246.629 mil hectares na produção agropecuária, sendo 28% na produção agrícola, 69% na produção pecuária e 3% no plantio de florestas, segundo dados do Censo Agropecuário (IBGE, 2019). As preocupações internacionais pela preservação ambiental e da mata nativa, leva a um maior controle sobre a expansão de terras para produção agropecuária. Há demanda de solução para o crescimento da oferta para o aumento da produtividade e para o controle do desperdício que ocorre pós-colheita nas etapas de manipulação, armazenagem, processamento, distribuição e consumo (PARFITT et. al., 2010).

Com o aumento da preocupação dos consumidores com a procedência dos alimentos, são necessários sistemas de rastreabilidade inseridos nas cadeias produtivas, descrevendo a vida de um produto. Rastreabilidade é a habilidade de manter o registro do ciclo de vida de elementos de um sistema (GOTEL el. al., 1994), envolvendo conhecimento da sua origem e a razão da sua existência. Esta rastreabilidade registra todas as conexões existentes dentro de uma cadeia de suprimentos.

Para a rastreabilidade efetiva, com garantia de dados verídicos e transparentes, é necessário haver com clareza a forma de estruturação e armazenamento dos dados. Uma

melhora potencial que pode trazer para a *supply chain* é a utilização da *blockchain*, com uma arquitetura descentralizada e encriptação que garante maior segurança dos dados.

A Tecnologia *Blockchain* (FOROGLOU; TSILIDOU, 2015) permite a geração de protocolos de transações de maneira segura. A primeira aplicação dessa tecnologia *blockchain* foi o *Bitcoin*, um modelo de dinheiro eletrônico *peer-to-peer,* funcionando como uma rede de computadores, onde cada nó funciona ao mesmo tempo como cliente e como servidor, compartilhando serviços e dados sem a necessidade de um servidor central.

Com o aumento na demanda por alimentos e o Brasil é um grande produtor de *commodities,* de uma forma geral, e um distribuidor chave para países ao redor do mundo, há necessidade de preservação de áreas produtivas, e geração de soluções para o aumento da produtividade e a diminuição do desperdício. E, com o aumento da exigência por maior qualidade, fazendo com que a entrega do produto final seja um produto com as características exigidas e seguras, é preciso manter o controle sobre logística e garantir a entrega de um produto de qualidade e seguro, utilizando um sistema de gerenciamento da cadeia logística.

1.2 OBJETIVOS

O objetivo desta dissertação é validar o uso de *blockchain* como um método de rastreabilidade de produtos agrícolas.

Os objetivos específicos são os que seguem:

- Realizar pesquisa descritiva sobre gestão da cadeia de suprimentos e *blockchain*;
- Desenvolver uma cadeia de *blockchain* que possa gerenciar rastreabilidade*;*
- Validar condições do método na rastreabilidade em produtos agrícolas.

1.3 ESTRUTURA DA DISSERTAÇÃO

Esta dissertação está estruturada, além deste capítulo introdutório, como segue. No Capítulo 2, é descrita uma revisão da literatura abordando a gestão da cadeia de suprimentos, rastreabilidade empregada na cadeia, e a tecnologia *blockchain*. No Capítulo 3 são abordados os materiais e métodos empregados para apresentação de um modelo de rastreabilidade

baseado na tecnologia *blockchain*. No Capítulo 4 são apresentados os resultados e discussões. No Capítulo 5, são apresentadas as conclusões e perspectivas de pesquisas futuras.

2 GESTÃO DA CADEIA DE SUPRIMENTOS E RASTREABILIDADE

2.1 GESTÃO DA CADEIA DE SUPRIMENTOS

A Gestão da Cadeia de Suprimentos tem se mostrado um método eficaz para empresas que buscam vantagem competitiva, e que é vista como um método de gestão melhorado, que inclui toda a cadeia produtiva de maneira integrada. E, pode agregar toda a cadeia produtiva na qual se encontra, como por exemplo, a relação dos fornecedores da matéria prima, fornecedores e clientes (BALLOU, 2001).

Com o surgimento da gestão da cadeia de suprimentos, é alterada a maneira como a competição no mercado ocorre, passando a ser uma competição entre cadeias produtivas e não mais entre unidades de negócio. Com a gestão da cadeia de suprimentos é possível criar uma unidade virtual de negócio que é formada pelo conjunto de unidades, representadas por empresas distintas que fazem parte de uma determinada cadeia produtiva (FIGUEIREDO, 2006). Este modelo garante uma preocupação com o desempenho da cadeia como um todo e principalmente com o produto da unidade virtual diante do consumidor final. Isto faz com que gere a necessidade de uma gestão integrada da cadeia produtiva, requerendo estreitamento entre as relações das empresas e a criação de competências conjuntas entre as unidades.

Devido aos avanços que a tecnologia que vem sofrendo nos últimos anos, permitiu com que a gestão da cadeia de suprimentos ganhe espaço e aumente sua eficiência. Com isso o consumidor final tende a ganhar, pois há melhoria na forma de abastecimento da cadeia de suprimentos (SEURING; MÜLLER, 2008). Os Sistemas *ERP* (*Enterprise Resource Planning*), permitem com que muitos processos sejam realizados de forma digital, como a compra de materiais até a entrega do produto final ao consumidor. Estes avanços, permitiram reduzir o tempo, dando agilidade entre os processos, e dando maior flexibilidade e redução de custos. São claros os benefícios da tecnologia, e a informação que ela gera se torna base na tomada de decisões, por isso há constatação do efeito de procura por tecnologias e a busca por inovações que garantam um benefício competitivo (SEURING; MÜLLER, 2008).

A gestão da cadeia de suprimentos busca unir sinergias entre as partes da cadeia produtiva, com o intuito de proporcionar um maior benefício para o consumidor final, diminuindo os custos, e prezando o produto final. Para haver uma diminuição dos custos é preciso ocorrer a diminuição do uso e de registros em papéis, custos de transporte e estocagem, e a garantia da entrega de um produto homogêneo. Com todos esses esforços

ocorre a adição de valor aos produtos, através da criação de bens e serviços customizados, e do conjunto de competências entre empresas. E isso faz com que seja benéfico tanto para o lado dos fornecedores como para os clientes, pois faz com que gere aumento de lucratividade (FIGUEIREDO, 2006).

A utilização da gestão da cadeia de suprimentos permite a simplificação e obtenção de uma cadeia produtiva eficiente. Tais como, a reestruturação e consolidação de fornecedores e clientes resultando em parcerias entre empresas que desejam desenvolver relação colaborativa. O contato entre as empresas envolvidas na gestão resulta no desenvolvimento de novos produtos, que a partir da demanda identificada, o desenvolvimento se torna ágil e reduz tempo e custos.

O uso de gestão da cadeia de suprimentos tem sido significativo, e torna o que poderia ser distante, como inovações, em ações concretas inovadoras em áreas significativas nas empresas (CHRISTOPHER; TOWILL, 2002).

Formas comuns de mediação dessas cadeias de suprimentos são o *outsourcing* (terceirização) e *benchmarking* (avaliação comparativa). O *outsourcing* é a participação de uma determinada empresa externa, que visa um relacionamento colaborativo com uma certa cadeia de suprimentos, onde essa empresa entra no papel de desenvolvedora e mantenedora da infraestrutura para atender todos os envolvidos da cadeia de suprimentos, mantendo a colaboração mútua (WILLIAMSON, 2008). E, o benchmark é a disponibilização e obtenção de informações do mercado, com o objetivo de promover a integração das estratégias competitivas das cadeias produtivas (CHRISTOPHER, 1999).

O paradigma internacional que envolve a competitividade é baseado em inovação. A competitividade no meio industrial se refere ao aumento de produtividade, em termos de menores custos comparados aos seus concorrentes e se refere a capacidade de entregar um produto com um maior valor agregado que justifique a cobrança de um valor elevado (PORTER et. al., 1995).

É possível notar um efeito internacional, onde indústrias competitivas deixam de ser aquelas com baixos valores de venda ou com larga escala de produção, mas sim aquelas indústrias que possuem a capacidade de melhorar e inovar continuamente. Também, é considerado uma vantagem um conjunto de características que proporcionam valor aos clientes, criar um destaque perante a concorrência e obtendo vantagem de mercado (PORTER et. al., 1995).

Apenas inovar não é sinônimo de vantagem competitiva, essa diferença deve ser entendida pelo cliente como um valor da empresa, algo que se deseja obter. Sem existir um produto, processo, etc., que agregue para o cliente, deixa de ser uma possível vantagem para se tornar um desperdício de recursos. A vantagem deve ser montada em algo que não possa ser substituído por outra ação que a neutralize. Também, é necessário verificar a capacidade de se autossustentar, pois se com o tempo a vantagem não for capaz de se manter e ser facilmente copiada pela concorrência, não trará o benefício esperado pelo esforço despendido (DE VASCONCELOS; BRITO, 2004).

Uma vantagem competitiva está atrelada ao valor, nesse caso, se referindo diretamente ao preço final gerado. Produtos parecidos em concorrentes, mas onde um se destaca por possuir benefícios maiores em um aspecto específico, fazem com que haja uma compensação pelo seu valor mais alto (BALLOU, 2001).

Existem dois tipos básicos de vantagem competitiva, que são: a liderança no custo, onde as empresas visam diminuir ao máximo seu custo logístico em torno de todos os processos, e a diferenciação, que é um conceito relacionado em possuir um destaque em relação aos demais concorrentes (PORTER et. al., 1995).

As vantagens permitem um melhor posicionamento de mercado, podendo ser a principal fonte de competitividade. Agregar valor ao produto final possibilita uma vantagem competitiva a empresa que emprega e adota um sistema de rastreabilidade.

2.2 RASTREABILIDADE

Rastreabilidade é a maneira de manter dados do ciclo de vida, conjunto de fases que um determinado produto percorrerá durante toda a sua existência (KAMILOGLU, 2019). Essa maneira com que os dados são mantidos envolvem a origem de um elemento até o final do seu ciclo.

Rastreabilidade de uma *commoditie* ou produto alimentício é a forma como se documenta e mantém informações relacionadas ao processo da cadeia de suprimentos. A rastreabilidade permite com que ocorra um grau de confiabilidade ao consumidor e demais parceiros pertencentes a cadeia produtiva, mostrando a proveniência deste produto desde a sua origem, localização e histórico de existência, assim como possibilita o auxílio na identificação de falhas e possíveis fontes de contaminação (OPARA, 2003).

Tendo em vista que em produtos alimentícios, a rastreabilidade representa a habilidade de deferir ao consumidor a realização de *track back* (rastreabilidade para trás) e *track foward* (rastreabilidade para frente), que se refere ao acompanhamento de todas as etapas e processos atingidos entre dois estágios no tempo, quando determina seu local específico e ciclo dentro da rede de suprimentos (OPARA, 2003).

Todo processo contribui para a transparência da rede de suprimentos com o uso apenas de dados verificados. A rastreabilidade concede valor para qualidade do sistema de gerenciamento por conta da providência de identificação, verificação e isolamento de fontes que não estiverem de acordo com os padrões de consumo.

Existem seis valores de rastreabilidade que devem ser alcançados dentro de cadeias de suprimentos voltados a plantas e grãos:

- Rastreabilidade do produto, indicando a sua localização física em qualquer estágio da cadeia de suprimentos, facilitando a logística e gerenciamento de estoque;
- Rastreabilidade dos processos, verificando o tipo e a sequência de atividades que afetaram o produto durante o seu crescimento e pós-colheita;
- Rastreabilidade genética, determinando a constituição genética do produto, com informações sobre tipo e origem e se tratando de um produto geneticamente modificado;
- Rastreabilidade de insumos, determinando por exemplo, fertilizantes, produtos químicos, modo de irrigação, entre outros;
- Rastreabilidade de doenças e pragas, permitindo o rastreamento da epidemiologia de pestes, bactérias, vírus e outros patógenos; e
- Rastreabilidade de medição, permitindo a estabilização de um padrão, ao qual deve ser seguido e comparado dentro da cadeia de produção.

Para implementação ou estudo de um sistema de rastreabilidade permitindo garantir a qualidade e segurança dos alimentos, estes valores são necessidades básicas para gerarem informações suficientes para averiguação de tipo, localidade, origem, entre outros, para que seja possível realizar ações de correção. O processo de rastreabilidade demanda trabalho e necessita do auxílio de tecnologias como apoiadoras desse processo, e algumas tecnologias que automatizam esse processo de rastreabilidade com escalabilidade tornaram-se tópico de pesquisa na área, como mostra a Tabela 1.

Quadro 1: Principais tecnologias utilizadas em rastreabilidade.

Método	**Características**
Recuperação de informação (IR-based tracing methods em inglês)	Recuperação da informação (IR) é uma técnica que envolve documentos textuais. São necessários documentos de envio e destino. Após um pré-processamento pode ser automatizada. (CLELAND-HUANG, et. al. , 2007)
Métodos baseados em mineração de dados e aprendizado de máquina (Data mining and machine learning-based methods em inglês)	De um modo geral, os métodos de rastreabilidade baseados em algoritmos de mineração geram padrões a partir das informações de ocorrência (GERVASI e ZOWGHI, 2011)
Métodos baseados em recursos (Feature-based methods em inglês)	É utilizado como mediador de um relacionamento entre duas entidades (POSHYVANYK, 2007)
Métodos baseados em ontologia (ontology-based methods em inglês)	Como os artefatos gerados a partir de uma cadeia são na maioria textuais, é possível aplicar uma ontologia como um mecanismo de raciocínio dos elementos (ASSAWAMEKIN, 2010)
Métodos baseados e regras (Rule-based methods em inglês)	São utilizados para gerarem links automáticos de rastreabilidade. Converte artefatos de origem e destino em representações formais. (JIRAPANTHONG, 2015)
Método baseado em exames (Swarm-based methods)	Enfatizam a utilização de algoritmos inteligentes para gerar a conexão de rastreabilidade entre artefatos textuais (SULTANOV e HAYES, 2010)
Métodos de rastreamento baseados em framework (Framework-based tracing methods em inglês)	Visam fornecer frameworks para dar suporte a geração de links de rastreamento (MATÉ e TRUJILLO, 2012)
Métodos de rastreamento orientados para Agile (Agile-oriented tracing methods em inglês)	Principal vantagem deste processo é a resolução do problema de mudança frequente de requisitos (REMPEL e MADER, 2015)

Fonte: O autor.

Como é possível verificar, existe uma gama de métodos de rastreabilidade com diferentes tecnologias. Para atingir um nível de confiança elevado, *blockchain* vem sendo

estudada e aplicada também para rastreabilidade, uma vez que já está consolidada sua utilização no mercado financeiro.

2.3 BLOCKCHAIN

Blockchain é uma tecnologia caracterizada como um livro digital que possibilita com que uma rede de usuários rastreie qualquer transação comercial, armazenando dados digitais públicos (CARLOZO, 2017). As informações basicamente são gravadas em blocos, que são *linkados* entre si, criando a característica de imutabilidade.

A partir do momento que um bloco de dados é *linkado* a outro, este não pode ser modificado. Todos os blocos de dados são disponibilizados publicamente, basta apenas fazer uma busca para encontrar os dados disponibilizados.

A *blockchain* introduziu conceitos de redes e criptografia que quando aplicados no meio das transações trazem confiança, realizando um registro global de transações. É notável como a *blockchain* surgiu como uma maneira de alterar o estado da arte no que se refere há gerenciamento e processamento de dados.

A criptografia por sua vez é a criação de um protocolo que permite que usuários se comuniquem através de canais inseguros, onde garantam que a transmissão seja privada e autentificada (CORON, 2006). Um esquema criptografado é seguro somente se provado matematicamente que um ataque não pode ser bem-sucedido, exceto talvez por negligência dos usuários. Um esquema de criptografia deve fornecer aos usuários uma chave utilizada para criptografar e descriptografar a comunicação. Nesses sistemas é assumido que os usuários mantêm as chaves sobre sigilo.

As tecnologias que atuam em conjunto e recebem o nome de *blockchain*, podem ser definidas como uma base de dados eletrônica distribuída e criptografada que é capaz de transmitir dados a uma rede de usuários, sem a necessidade de um órgão centralizador. Os dados *linkados* em blocos podem ser de qualquer natureza, podendo ser aplicado em diversas áreas e de diversas maneiras. Esta tecnologia se mostra eficaz, e um exemplo de aplicação seria a inserção de um bloco com a escritura de propriedade de uma residência, a medida que o usuário faz a inserção de uma foto desse documento, por exemplo, ele estaria disponível para sempre para provar os direitos de posse da mesma, fazendo com que ninguém consiga alterar essa informação uma vez inserida na *blockchain* (FOROGLOU; TSILIDOU, 2015).

Os blocos são *linkados* através de uma assinatura *hash*, em *blockchain* essa assinatura é criada a partir por uma função hash criptografia. Essa função criptografada é difícil de ser transcrita e faz que qualquer *string* (cadeia de caracteres) de entrada se tenha uma saída única de 64 dígitos, sendo que a mesma entrada possui a mesma saída. Uma hash é criada a partir dos dados contidos dentro de um bloco, fazendo com que caso haja uma mudança em um bloco da cadeia, este se descontinue com o próximo bloco, e tenha um custo elevado para alterar todos os blocos que estão em sequência.

Um uso emergente de *blockchain* durante os últimos anos é a utilização de *smart contracts* (contratos inteligentes em tradução livre), que são acordos digitais que podem ser estabelecidos a partir certas condições cumpridas. E esta verificação é feita de maneira eficiente por máquinas pessoais. Todo processo que precise de uma terceira parte para validação pode ser codificada para se tornar parte de uma *blockchain*, integrada a plataforma de sua preferência. Um *smart contract* pode ser utilizado para confirmar o status de uma transação (FOROGLOU; TSILIDOU, 2015).

2.4 RASTREABILIDADE E *BLOCKCHAIN*

Todos os envolvidos em uma cadeia de suprimentos a partir de produtores, distribuidores, indústrias, processadores, supermercados, e etc., tem como objetivo demonstrar ao consumidor a superioridade de seus métodos e produtos (SMITH, 2008). O uso de *blockchain* simplifica essa tarefa unificando todas as partes, fornecendo integração de dados entre os participantes.

A *blockchain* facilita a estrutura de dados, na medida em que pode descrever os atributos provenientes da *commoditie.* Os principais usos de *blockchain* dentro de uma cadeia de suprimentos são (GALVEZ; MEJUTO; SIMAL-GANDARA, 2018):

- Transparência: a função principal de uma *blockchain* é facilitar a troca de informação, criar cópias digitais de toda a informação e validar a qualidade da *commoditie* em torno de toda cadeia de suprimentos. Esse objetivo é cumprido à proporção que cada participante pode compartilhar seus dados das condições atuais do produto, ajudando cada participante a identificar informações de toda a vida útil de uma *commoditie*. E, com essas informações é possível definir com precisão os atributos desse produto.

- Eficiência: *Blockchain* é uma parte da infraestrutura que permite novas transações entre diferentes integrantes que ainda não se conhecem ou que nunca fizeram transações anteriormente. *Smart contracts* são instruções que geram automaticamente uma avaliação da adição de uma nova transação. Os participantes dividem as informações que são compartilhadas de forma segura. Dessa forma, a rastreabilidade não precisa aguardar com que um negócio disponibilize seus dados, pois eles já estarão disponíveis de forma não centralizada.
- Segurança: *blockchain* é usada para criação de blocos únicos criptografados, se tratando de uma estrutura pública e descentralizada, acaba ganhando notoriedade em segurança. Quando registros são efetuados nos blocos interligados, não é possível extrair um de seus blocos de maneira localizada e individual. Para tal tarefa, seria necessário um poder computacional capaz de quebrar a criptografia, modificar o conteúdo dos blocos e validar para que cadeia de blocos continue válida. Por isso, cada vez mais diferentes setores e empresas vem adotando está nova tecnologia.

2.5 ARMAZENAMENTO DE DADOS

A maneira com que os dados são guardados evoluíram com o passar dos anos, assim como a sua forma de captar dados, que por muito tempo precisou contar com a confiança do usuário, mas que dispõem de sistemas automatizados para captura dos dados.

O uso da internet das coisas (*IoT – internet of things)*, permite com que informações sejam facilmente obtidas (REYNA, 2018). A internet das coisas emergiu de tecnologias como sensores sem rede (WSN) e rádio frequência (RFID), que proveem a capacidade de sensoriamento, atuação e comunicação via internet. E, permite o monitoramento em tempo real e gravação de informações (umidade, temperatura, tempo de estoque, etc.) sobre o sistema monitorado, permitindo com que seja gerenciado de uma maneira eficaz.

Um sistema envolvendo internet das coisas, permite uma tomada assertiva de decisões, como por exemplo, qual lote de um determinado produto deve ser dado prioridade para descarga ou venda, pensando na possibilidade de evitar perdas.

Uma maneira de reforçar a confiabilidade dos dados envolvendo internet das coisas é a distribuição dos serviços entre todos os participantes, para garantir que os dados sejam

imutáveis (REYNA, 2018). Se todos os participantes possuírem os dados e o meio necessário para verificar que os dados não foram alterados, é possível atingir confiabilidade. Caso seja atingido o estado de confiabilidade, esses dados poderiam ser usados para diversos propósitos, inclusive governamentais.

Uma nova maneira de armazenar dados foi projetada para que o processo de invasão seja muito custoso e para que não seja possível a modificação de dados que já pertencem a cadeia de suprimentos, não sendo possível corromper os seus dados (MARTINS, 2018).

Em um modelo tradicional de banco de dados é necessário que haja um terceiro elemento confiável, intermediando as transações, enquanto na tecnologia *blockchain,* todas as transações são anunciadas, não precisando identificar a entidade que gerou esse dado. Dessa maneira, *blockchain* pode ser tratada como um livro-razão público que possui dados mantidos continuamente. Os dados de uma *blockchain* são semelhantes aos de uma bolsa de valores, onde os negócios individuais são tornados públicos, mas sem dizer quem eram as partes e onde as identidades dos participantes são como "chaves públicas anônimas" (NAKAMOTO, 2008).

Diferente das bases de dados tradicionais, *blockchain* pode ser utilizado como uma base de dados distribuída e que passa por verificações recorrentemente para que toda a sua informação armazenada esteja refletindo dados reais. Uma *blockchain* é uma cadeia de blocos, onde cada bloco possui os seus dados, uma *hash* (um identificador único) e um *hash* anterior, para que seja possível fazer o seu encadeamento (NAKAMOTO, 2008). Através de um período de tempo definido, todos os usuários que fazem parte da *blockchain* são requisitados para fazerem a validação e aprovação de novos blocos, inserindo nesta hora a criptografia dos dados e fazendo o registro de maneira ordenada na *blockchain.*

O ato de inserir um novo bloco em uma *blockchain* possui um custo computacional no momento de criptografar os dados e também faz com que seja gerado uma prova de trabalho (do inglês, *proof-of-work*), o usuário que realiza esta ação é chamado de minerador (RODRIGUES, 2018). Esse novo bloco é aceito somente se as transações ou dados inseridos neste bloco sejam válidos, pois o mesmo não poderá sofrer um processo de alterações (NAKAMOTO, 2008).

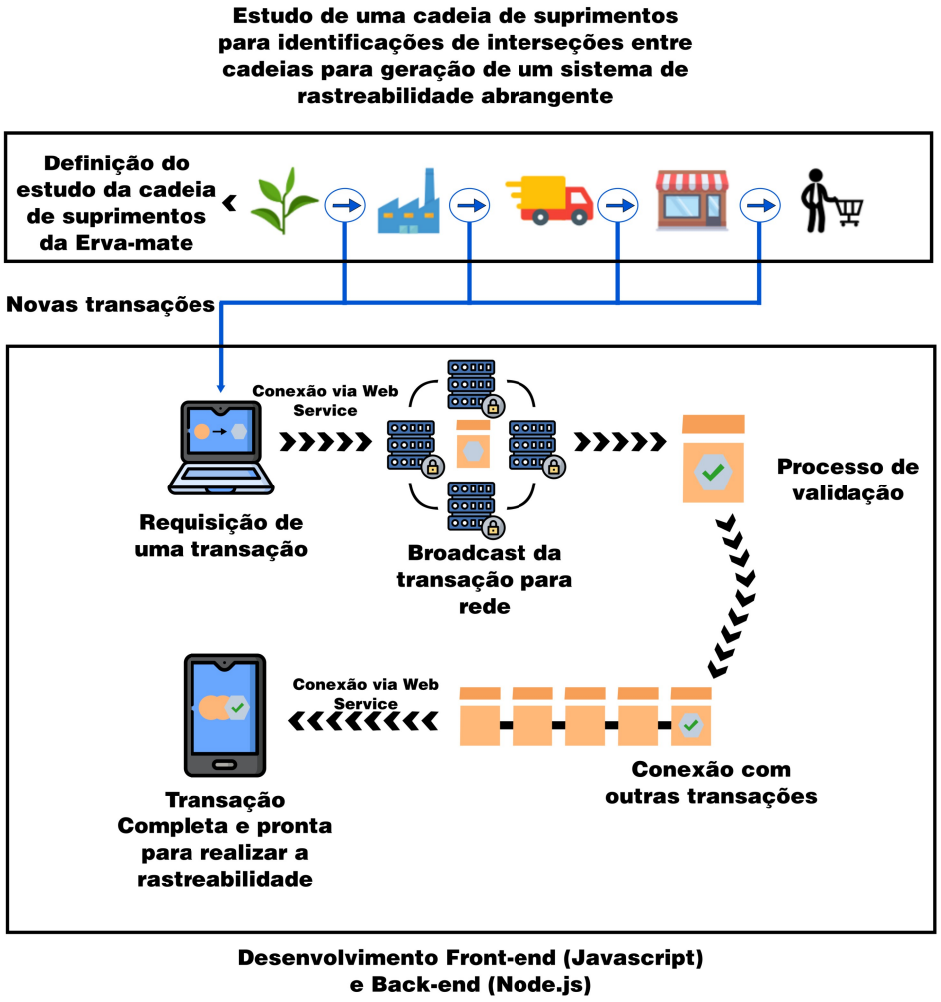
Esse processo de mineração, faz que os dados permaneçam seguros, onde um usuário malicioso ou invasor (*hacker*) só poderá fazer com um dado dentro de um bloco seja alterado, após primeiramente quebrar a criptografia, que é um processo que demanda muito poder computacional e pode levar dias, após isso o usuário malicioso deverá refazer a prova de

trabalho do bloco que foram alteradas as informações e também refazer as provas de trabalho dos nós seguintes que estão validados de acordo com os dados anteriores antes da modificação.

3 MATERIAIS E MÉTODOS

Neste capítulo são apresentados os materiais e métodos empregados para criação do método de rastreabilidade de produtos agrícolas baseado na tecnologia *blockchain*. A Figura 1 representa a forma com que serão abordados os processos de desenvolvimento do método.

Figura 1. Rastreabilidade em sistemas de produção.



Fonte: autor.

3.1 DEFINIÇÃO DO PRODUTO AGRÍCOLA

Primeiramente, foi definida a *Commodity* Erva-Mate*,* importante no Estado do Paraná, com aplicações na indústria e presente em boa parte da Região dos Campos Gerais. Em seguida, estudado o funcionamento da cadeia de suprimentos voltados a erva-mate e as tecnologias podem ser aplicadas às unidades desta cadeia e seus relacionamentos.

A erva-mate foi um dos principais produtos de exportação brasileira, e ainda é conhecida como uma das principais fontes de emprego e renda, em especial para pequenos e médios produtores (RODIGHERÍ, 1997), formando um dos sistemas agroflorestais mais característicos do Sul do Brasil. É usada como (MAZUCHOWSKI; RUCKER, 1997): bebida – chimarrão, tererê, chá-mate, refrigerantes e sucos; insumo para alimentos – corante natural, conservante alimentar, sorvete, balas bombons e caramelos, chicletes e gomas; medicamentos – compostos para tratamento de hipertensão, bronquite e pneumonia; higiene pessoal – bactericida e antioxidante hospitalar e doméstico, esterilizante, tratamento de esgoto e reciclagem de lixo urbano e; produto de uso pessoal – desodorantes, cosméticos, perfumes e sabonetes.

Na fase de mapeamento da cadeia da erva mate, uma análise da cultura foi feita, assim como a proposta por Silva (2018) mostra os pontos críticos da cadeia produtiva, possuindo cinco principais entidades: (i) o Produtor, responsável por gerir os dados de quais insumos foram inseridos, quais as mudas utilizadas, a localização da plantação e se essa área é uma área com sombreamento ou não, fator importante pois afeta a qualidade e também define qual será o tipo da erva, e também como está sendo feito o armazenamento, atentando sempre para duas variáveis de ambiente durante esse processo que são a temperatura e luminosidade, pois afetam diretamente a qualidade da erva-mate; (ii) a Transportadora, responsável por fornecer a rota, condições de armazenamento, tempo de transporte e datas de início e fim de percurso realizado em dois momentos, no envio da erva para a Indústria e também no envio do produto final para a Comercialização; (iii) a Indústria, responsável por fornecer dados de beneficiamento da erva, como por exemplo a secagem e fragmentação; (iv) a Comercialização, fornecedora do tempo de prateleira, lote e prazo de validade da erva-mate industrializada; e (v) o consumidor final do produto, permite a rastreabilidade dos demais processos realizados pelas entidades que estão dispostos anteriormente a eles.

3.2 DEFINIÇÃO DO AMBIENTE COMPUTACIONAL

Para criação do método de rastreabilidade de produtos agrícolas utilizando *blockchain* foram seguidas as fases de *setup* do ambiente de trabalho e mapeamento da cadeia de erva-mate. Na fase de construção da rede de dados da *blockchain*, foi utilizado um computador pessoal com processador Intel Core I7, de 8ª geração, 8GB de memória RAM com Sistema Operacional Windows 10 de 64 bits. Então, foram instalados Node.js para o desenvolvimento do *backend,* correspondendo a *blockchain*.

O Node.js é um ambiente de desenvolvimento do servidor, de código aberto e multiplataforma, baseado na Linguagem de Programação *Javascript,* com funcionamento assíncrono, ou seja, o sistema desenvolvido não possui travamentos, realizando funções de *callback* ou até mesmo disparo de eventos (TILKOV; VINOSKI, 2010).

3.3 DEFINIÇÃO DE ESTRUTURA DE WEB SERVICE

Para interação entre as entidades da cadeia de suprimentos, foi necessário o desenvolvimento de um *Web Service*, possibilitando a *blockchain* ser usada independente de plataforma de acesso. Web Services são aplicações modulares que podem ser descritas, publicadas e invocadas sobre uma rede, que nesse caso comumente é a Web. Ou seja, é uma interface que descreve uma coleção de operações que são acessíveis pela rede através de mensagens em formato XML padronizadas. Permitem uma integração de serviços de maneira rápida e eficiente.

Uma *web service* é independente de implementação em uma plataforma específica. É escrita através de uma linguagem de descrição de serviços, disponíveis através de um registro padrão. Este pode ser utilizado através de uma API – *Application Program Interface*, compondo outros serviços.

A principal vantagem de uma *web service* é a comunicação entre aplicações, pois não depende de uma linguagem de programação específica e não demanda conhecimento da plataforma a ser utilizada. Isso é possível pela utilização de metadados, dados sobre dados. São um conjunto de palavras, frases ou sentenças que resumem ou descrevem o conteúdo de um site *WEB*, uma página WEB individual ou um recurso computacional com o objetivo de beneficiar o trabalho de agentes de busca (BABU, 2001).

Para o desenvolvimento do Web Service, foi definido e configurado no *Framework Express,* amplamente utilizado e desenvolvido em *Javascript.* O *Express* permite a criação de

um *Web* Server, interpretando requisições e conexões através da *web* (RAO; SU, 2004). O *Express* foi configurado para receber requisições HTTP de *GET,* utilizado na recuperação de dados, e *POST,* utilizado para inserção de dados, definidas pelo Protocolo *HTTP – Hypertext Transfer Protocol* (FIELDING, 1999).

3.4 DEFINIÇÃO DO *FRONT END*

O *front-end,* possibilita uma interface amigável ao usuário. E, para seu desenvolvimento, foi configurado o *framework* conhecido como *React.js*, baseado em *Javascript, de* código aberto e permitindo a criação de páginas web com múltiplos componentes dinâmicos e com design simples (FEDOSEJEV, 2015). *O React.js* permite que os desenvolvedores criem grandes aplicativos web que podem alterar dados, sem recarregar a página. O objetivo principal do *React* é ser rápido, escalonável e simples. O *front-end* tem como principal função visualizar e explorar os blocos registrados dentro da *blockchain*.

3.5 DEFINIÇÃO DE ESTRUTURA DE ARMAZENAMENTO DE DADOS

Uma arquitetura das bases de dados permite que dados sejam operacionalizados por indivíduos confiáveis que registrarão novas transações na base mestre (GANTORI, 2017). Bases de dados tradicionais podem ser escaláveis através de replicações, o que pode fazer com que ocorra uma diminuição no tempo investido para recuperar, consultar ou modificar as informações (LOSCIO et. al., 2011). Diferente das bases de dados tradicionais, *blockchain* foi utilizado como uma base de dados distribuída e que passa por verificações recorrentemente para que toda a sua informação armazenada esteja refletindo dados reais.

4 RESULTADOS E DISCUSSÕES

Neste capítulo são apresentados os resultados e discussões na definição de um modelo de rastreabilidade baseado na tecnologia *blockchain*. Os testes foram realizados, basicamente, sobre as funcionalidades e usabilidade da *blockchain.*

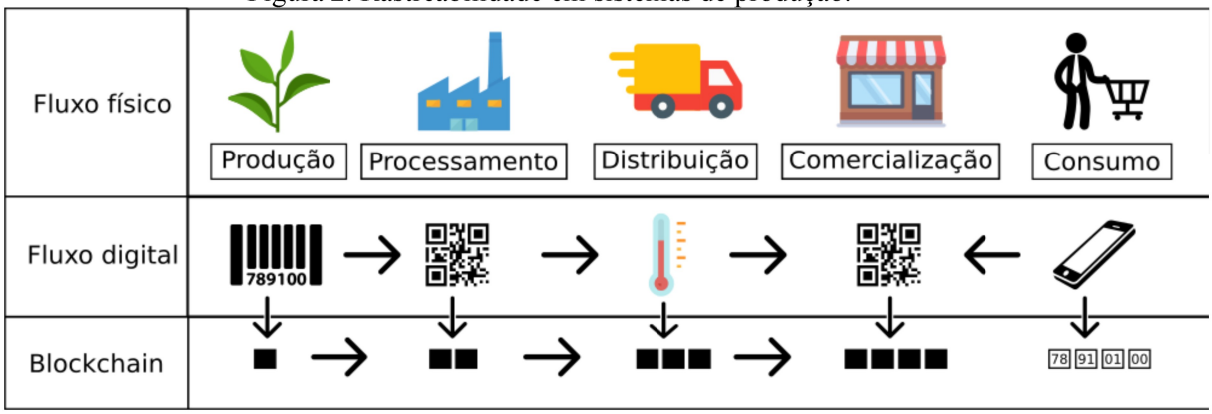
4.1 MÉTODO DE RASTREABILIDADE COM BLOCKCHAIN

O método de rastreabilidade de produtos agrícolas utilizando blockchain, retrata o fluxo da informação da cadeia de produção da erva-mate, trabalhando de forma conjunta com *blockchain* e demais tecnologias.

A Figura 2 apresenta três camadas retratando os fluxos físico e digital, mostrando diversas tecnologias aplicadas para melhoramento das informações (como código de barras, QR Code, RFID, sensores e atuadores, celulares, etc.) e a camada de *blockchain,* responsável por captar toda informação gerada pelas tecnologias disponíveis na rede, gerando informações aceitas por todos os participantes e tornando-se uma informação imutável.

Todos os participantes da rede devem aceitar e validar a nova informação gerada de cada transação. Após o bloco de informação ser validado, é inserido na cadeia de transações, tornando um dado permanente do processo.

Figura 2. Rastreabilidade em sistemas de produção.



Fonte: autor.

Após cada estágio percorrido da cadeia de suprimentos, diferentes tecnologias estão sendo envolvidas e diferentes dados estão sendo registrados. Produção, contendo informações sobre o local da plantação, pesticida e fertilizante, safra, ano, maquinário utilizado, condições

climáticas, etc. Processamento, contendo Informações sobre a indústria e equipamentos, o processo e métodos utilizados, informações de transações realizadas com a produção etc. Distribuição, contendo detalhes de entrega, trajeto percorrido, condições de armazenagem, tempo de transição, informações de transações realizadas com o processamento, etc. Comercialização, contendo detalhes sobre cada produto alimentício, sua qualidade e quantidade atual, datas de validade, condições de armazenamento, tempo gasto na prateleira, informações de transações realizadas com a distribuição, etc. Consumo, onde o consumidor final pode utilizar um celular conectado à *internet* para escanear o *QR Code* associado com o item de consumo e ver em detalhes todas as informações associadas com o produto.

O Node.js permitiu a criação de uma solução de *Blockchain* completa. Utilização a metodologia *Test Driven Development* – TDD (Desenvolvimento Guiado por testes). O TDD é uma técnica que se baseia na verificação e validação, onde um desenvolvedor cria um caso de teste desejado para logo após aplicar uma melhoria no sistema (KOSKELA, 2007). Com a utilização de TDD há economia de tempo e evita a necessidade de uma equipe de testes.

Considerando que *blockchain* é uma corrente de blocos de objetos, cada bloco gera sua *hash* baseada nos seus próprios dados com a *hash* do bloco anterior. E se iniciar a *blockchain,* será necessário inserir dados iniciais. Por isso *blockchain,* possui o conceito do bloco Gênesis visto no Quadro 2, codificado de maneira fixa com dados em todas os seus atributos, gerando um bloco para iniciar a *blockchain,* permitindo um novo bloco ser inserido e receber o valor do *hash* anterior do bloco gênesis.

Quadro 2. Configurações da blockchain

```
...
const GENESIS_DATA = {
        timestamp : 1,
        lastHash : '----',
        hash : 'hash-one',
        data : [],
        lastProcessHash: -1
};...
```

Fonte: O autor.

Em seguida, é feita a criação da classe bloco*,* que será a *blockchain* propriamente dito. Basicamente, blocos são formados por quatro parâmetros:

- *hash:* é um valor único de um bloco, gerado a partir de todo o conteúdo do mesmo;

- *timestamp*: para gravar quando o bloco foi criado. Deve ser criado e inicializado de forma automática;
- *lastHash*: que equivale ao valor da *hash* do bloco anterior;
- *data:* os dados a serem armazenados no bloco, podendo ser uma string, um vetor de números, um objeto, etc.;
- *LastProcessHash:* é equivalente a *hash* da transação anterior, para que seja possível a criação da rastreabilidade.

Também, foi definida uma função de inicialização apresentada no Quadro 3, a partir dos dados configurados para o bloco gênesis. Também, foi criada a função de mineração de um bloco, que basicamente é o ato de adicionar novos blocos a uma rede. Um bloco é fundamental para criação da *blockchain*, pois para criar uma cadeia de blocos demanda definir a instância mínima de um bloco.

Quadro 3. Criação de um novo bloco através do método de mineração

```
...
static mineBlock({lastBlock, data, lastProcessHash}){
   const timestamp = Data.now();
       const lastHash = lastBlock.hash;
       return new Block({
          timestamp,
          lastHash,
          data,
                   hash: cryptoHash(timestamp, lastHash, data,
lastProcessHash),
          lastProcessHash
        });
     }
...
```

Fonte: O autor

Como é possível identificar na função de mineração, a criação de uma *hash* corresponde a um processo de criptografa que envolve todos os dados da transação de um bloco. Foi utilizada uma função validada e amplamente aplicada e desenvolvida pela Agência de Segurança Nacional dos EUA conhecida como *SHA – Secure Hash Algorithm* (Algoritmo do *hash* Seguro), que faz operações matemáticas em dados digitais, resumindo essa informação em 256 bits e utilizados como verificação de integridade de uma mensagem (YOSHIDA; BIRYUKOV, 2005).

Como é possível verificar, foi definida a função de criptografia de uma *hash* de maneira que sejam aceitos diversos parâmetros e que mesmo que sejam inseridos em ordens diferentes, obtenham o mesmo resultado, como mostrado no Quadro 4.

Quadro 4. Função de criptografia

```
...
const cryptoHash = (...inputs) => {
        const hash = crypto.createHash('sha256');
        hash.update(inputs.sort().join(' '));
        return hash.digest('hex');
};

...
```

Fonte: O autor

É necessário gerar um valor único para os blocos dentro da *blockchain,* realizado através da junção de todos os atributos do bloco. O algoritmo utilizado para criptografia é o SHA-256 - *Secure Hash algorithm A – 256,* Algoritmo A de segurança – 256, sendo que 256 representam 256 bits para o tamanho da *hash*.

A partir da criação da classe bloco, foi criada a estrutura da *blockchain,* com os seguintes fundamentos:

1. É uma corrente de blocos;
2. O primeiro bloco gerado precisa ser o bloco Gênesis;
3. É necessário possuir a habilidade de inserir um novo bloco e adicioná-lo ao final da corrente de blocos; e
4. O bloco que será adicionado deve ser baseado no bloco que vem antes, dessa forma deve ser baseado no último bloco da *blockchain.*

Todos esses quesitos são respeitados, a partir da classe criada. Pode ser conferido através da criação dos novos blocos, conforme Quadro 5.

Quadro 5. Função para adicionar um novo bloco

```
...
addBlock({ data }) {
        const newBlock = Block.mineBlock({
            lastBlock: this.chain[this.chain.length - 1],
            data,
            lastProcessHash
        });
        this.chain.push(newBlock);
    } ...
```

Fonte: O autor

Pode constar a função *isValidChain(),* representada no Quadro 6, representando toda a lógica de validação da *blockchain.* Existem três principais validações que devem ser respeitadas, são elas: todos os blocos precisam possuir os atributos corretamente, o valor equivalente ao *lastHash* precisa ser uma referência ao bloco anterior para que ocorra uma conexão entre os blocos e por fim o valor da *hash* precisa ser um valor válido.

Quadro 6. Função validação da blockchain

```
...
static isValidChain(chain) {
                        if   (JSON.stringify(chain[0])   !==
JSON.stringify(Block.genesis())) return false;
        for (let i = 1; i < chain.length; i++) {
              const { timestamp, lastHash, hash, data } =
chain[i];
            const actualLastHash = chain[i - 1].hash;
            if (lastHash !== actualLastHash) return false;
               const validatedHash = cryptoHash(timestamp,
lastHash, data);
            if (hash !== validatedHash) return false;
        }
        return true;
    } ...
```

Fonte: O autor

4.2 VALIDAÇÃO DO MÉTODO

Com o objetivo de avaliar a tecnologia da *Blockchain,* no desempenho do papel de unificação dos dados de transações entre as unidades da cadeia de suprimentos, disponibilizando esses dados de maneira transparente, foi implementada uma rede *Blockchain*. Dessa maneira, foi simulado um ambiente controlado de rastreabilidade dos processos da erva-mate, de maneira que ocorra a transparência no seu rastreio através da tecnologia da *blockchain* aplicada, avaliando os termos de eficiência e confiança dos dados.

A primeira vantagem da adoção de novas tecnologias aliadas a *blockchain,* foi tornar o processo de rastreabilidade automatizado, evitando falhas humanas, como na captura de dados de condições de ambiente, utilizando sensores.

Foram inseridos testes para as principais atividades realizadas dentro da *blockchain*. Na classe do bloco um dos testes é inerente à mineração de um novo bloco, garantindo que todos os dados passam pelo processo de criptografia como mostra o Quadro 7.

Quadro 7. Teste feito para garantir a mineração correta

```
...
describe('mineBlock()', () =>{
        const lastBlock = Block.genesis();
        const data = 'mined data';
        const minedBlock = Block.mineBlock({lastBlock, data});
        it('returns a Block instance', () => {
            expect(minedBlock instanceof Block).toBe(true);
        });
          it('sets the "lastHash" to be the "hash" of the lastBlock', ()
=>{
expect(minedBlock.lastHash).toEqual(lastBlock.hash);
        });
        it('sets the "data"', () => {
            expect(minedBlock.data).toEqual(data);
        });
        it('sets a "timestamp"', () => {
expect(minedBlock.timestamp).not.toEqual(undefined);
        });
        it('sets a "lastProcessHash"', () => {
expect(minedBlock.lastProcessHash).not.toEqual(undefined);
        });
        it('creates a SHA-256 hash based on the proper inputs', () => {
expect(minedBlock.hash).toEqual(cryptoHash(minedBlock.timestamp,
lastBlock.hash, data))
        });
    })
...
```

Fonte: O autor

Também, foram realizados testes para que seja possível garantir a existência, sempre, de um bloco inicial gênesis, como é possível ver no Quadro 8.

Quadro 8. Teste feito para garantir a mineração correta

```
describe('genesis()', () => {
        const genesisBlock = Block.genesis();
        it('returns a Block instance', () => {
                                expect(genesisBlock  instanceof
Block).toBe(true);
        });
        it('return the genesis data', () => {
            expect(genesisBlock).toEqual(GENESIS_DATA);
        });
    });
```

Fonte: O autor

Com a adoção e criação do campo *lastProcessHash* na classe *Block,* permitiu que o processo de rastreabilidade da erva-mate seja concluída e acessada desde a entidade do usuário final até o produtor, concluindo o Fluxo *end-to-end*. Neste caso, o *lastProcessHash* guarda o valor do último bloco da transação referente àquele produto, assim como o registro do *timestamp* da execução da transação. Com estes dados disponíveis, a todos os usuários da *blockchain,* é possível a realização de auditorias, tanto pelos órgãos competentes como pelos demais usuários participantes.

A validação de uma *blockchain* é necessária pois permite inspecionar uma rede. Dessa forma, é garantido que cada bloco foi construído de maneira correta. E para checar se está correto, existem algumas regras que precisam ser estabelecidas para haver um bloco dentro dessa rede:

- Um bloco precisa consistir dos campos corretos;
- O *lastHash* precisa ser uma referência do bloco que está dentro da rede. Isso é relevante para que ocorram ligações entre blocos em uma *blockchain*;
- O *hash* gerado precisa ser um valor válido. Essa validação é crucial para *blockchain,* pois caso sejam utilizados todos os valores contidos em um bloco para gerar o seu hash e este valor não corresponda com o valor de *hash* já existente nesse bloco, é possível perceber que seus dados foram alterados. Basta apenas um carácter ser alterado para que mude também o seu valor de *hash.*

Alguns testes como é possível ver Quadro 9 foram realizados e houve constatação da eficiência da *blockchain*.

Quadro 9. Teste criado para avaliação da blockchain

```
//Chain Validation Três principais regras 1) Precisa possuir todos os
atributos corretos (timestamp, data, lastHash, Hash)
    // 2) O LastHash precisa ser uma referencia do block anterior ( para
existir os links)
    // 3) A Hash do bloco precisa ser válida
    describe('isValidChain()', () => {
        describe('when the chain does not start with a genesis block', ()
=> {
            it('returns false', () => {
                        blockchain.chain[0] = { data: 'fake-genesis' }
expect(Blockchain.isValidChain(blockchain.chain)).toBe(false);
            });
        });
        describe('quando a blockchain começa com o bloco genesis e possui
diversos blocos', () => {
            beforeEach(() => {
                blockchain.addBlock({ data: 'Plantado' });
                blockchain.addBlock({ data: 'Colhido' });
                blockchain.addBlock({ data: 'Teste' });
            });
            describe('Um lastHash possui valor alterado', () => {
                it('returns false', () => {
                        blockchain.chain[length - 1].lastHash = 'broken-
lastHash'   expect(Blockchain.isValidChain(blockchain.chain)).toBe(false);
                });});
             describe('Blockchain possui um campo com dados inválidos', ()
=> {
                it('returns false', () => {
                            blockchain.chain[length - 1].data = 'dados-
maliciosos';
expect(Blockchain.isValidChain(blockchain.chain)).toBe(false);
                });});
            describe('A blockchain possui nenhum dado incorreto', () => {
                                            it('return   true',   ()   =>
{     expect(Blockchain.isValidChain(blockchain.chain)).toBe(true);
                });            });});});
```

Fonte: O autor

A validação permitiu constatar de forma precisa, que a mesma cadeia de blocos estará distribuída em diversos usuários. É preciso que a mineração de blocos seja feita seguindo um padrão, para impedir que dados inválidos ou maliciosos sejam inseridos dentro desta cadeia. Os testes realizados devem garantir que cada bloco tenha um valor de *hash* único. Também, foi determinado que cada bloco continha a *hash* do bloco anterior, para garantir a união dos blocos. Quando uma informação em um bloco é editada de qualquer maneira, o valor da *hash* desse bloco muda, embora o seu valor de *hash* no bloco anterior não mude. Essa discrepância faz com que seja extremamente difícil a alteração de uma *blockchain, sem ser detectada*.

Embora a maior parte da informação mantida em uma *blockchain* seja privada, a tecnologia por si só tem uma característica de disponibilização de dados, acessíveis para qualquer usuário, podendo ser uma desvantagem da tecnologia dependendo do seu uso.

Outro fator que pode servir como impedimento é a questão regulatória, que não nos fornece hoje nenhuma norma de implementação. Embora a tecnologia seja distribuída e possamos ter a validação em diversos computadores, os custos em torno da mineração de novos blocos estão relacionados ao consumo de energia pelo poder computacional.

A rastreabilidade e a transparência de transações voltadas a *commodities* são de grande importância para aumentar a confiança dos utilizadores. O fato da rastreabilidade ser acessível a todos e a proteção que a criptografia garante, acabam-se as brechas para realizações de má conduta e também ocorre-se uma diminuição na existência de dados falhos ou que não correspondem com a realidade.

Um sistema de informações baseado em *blockchain* remove a necessidade de uma organização confiável centralizando os dados e introduz uma nova abordagem para estabelecer a confiança entre os membros. Isso permite com que ocorra uma visualização instantânea dos dados, onde é possível confiar na informação disponibilizada, pelos participantes da cadeia. Com isso, pode ser implementado a rastreabilidade de produtos agrícolas e para toda a cadeia de mantimentos.

No desenvolvimento de sistemas de informação da cadeia de suprimentos agrícolas, a rastreabilidade pode ser considerada com base na integração entre a tecnologia *blockchain* e a Internet das coisas, a fim de melhorar a segurança e a qualidade dos produtos alimentícios e, ao mesmo tempo, diminuir a possibilidade de más condutas, como fraude, corrupção, adulteração e informações distorcidas.

É possível perceber através de simulações que a aplicação desenvolvida gera benefício a todos os usuários, desde consumidores até mesmo aos produtores, fornecendo a informação segura e refletindo a realidade.

4.3. TRABALHOS CORRELATOS

Existem trabalhos correlatos que exploram o uso de *blockchain* em diversas áreas. Como Benchoufi e Ravaud (2017) exploram o core de funcionalidades de *blockchain* aplicada a testes clínicos, ilustrando seus princípios, seguindo o protocolo proposto. Este trabalho

mostra o impacto da implementação de *blockchain* voltados para saúde. Enquanto Sikorski, Haughton e Kraft (2017) mostra a aplicação de blockchain para indústria química, apresentando a utilização e interação de blockchain na Iindústria 4.0, de máquina para máquina, envolvendo relacionamento de dois ou mais processadores eletrônicos.

É possível ver a apresentação de modelos para rastreabilidade de alimentos como Sikorski em 2017, onde definem como pode ser realizada a captação de dados e inserção em *blockchain,* voltadas para realidade de restaurantes. Já Bumblauskas (2020) faz uma análise das barreiras interinstitucionais envolvendo a *blockchain* aplicada para rastreabilidade.

Comparado com os trabalhos correlatos, esta dissertação apresenta uma maneira prática, e não apenas um modelo, de aplicação voltada para rastreabilidade com uso da tecnologia *blockchain,* utilizando uma tecnologia recente e com grande potencial para ser explorada que é o Node.js. O estudo específico direcionado para a erva-mate permite com que seja alterada, caso haja uma disruptura no modo que essa operação é feita hoje, na maneira com que as entidades dessa cadeia produtiva se relacionam, gerando assim uma rastreabilidade segura e confiável, pelo fato de ser um sistema distribuído entre as demais partes.

5 CONCLUSÕES E PERSPECTIVAS DE PESQUISAS FUTURAS

É possível concluir que com a criação de uma cadeia de suprimentos baseada em *blockchain* muitos valores serão atingidos, como por exemplo, a segurança e proteção alimentar. *Blockchain* é uma maneira de entrega de alimentos seguros de uma forma transparente, pois torna todos os dados gerados verificáveis e acessíveis.

O alimento se tornará mais seguro a medida em que todas as informações de condições de processamento, manejo e armazenamento serão registradas, prevenindo a entrega de alimentos contaminados ou armazenados de forma incorreta para população. É possível verificar também como a tecnologia se comporta e como pode ser combinada com novas tecnologias.

A *blockchain p*ermite um controle maior de datas de validade e condições de armazenamento, permitindo com que novas estratégias sejam criadas para evitar o desperdício. Vale ressaltar que a tecnologia permitirá uma maior consciência ambiental, uma vez que todos os dados de como estão sendo produzidos os alimentos, como por exemplo a forma que é tratada uma produção agrícola, estarão registrados e acessíveis a todas as partes desta rede de suprimentos, permitindo assim até mesmo uma maior e melhor fiscalização.

Também, pode ser utilizada a tecnologia como fonte de digitalização de dados decorrentes dos processos, fazendo com que muitas empresas mudem a maneira como operam. O próprio manejo da erva-mate ainda é feito de forma muito tradicionalista, pois segue com característica de ser uma produção feita por empresas familiares. Com a digitalização de documentos e toda a cadeia definida, ações de fiscalização de órgãos competentes, pode ser facilitado e ser também fator de competitividade, pois poderá agregar valor ao produto por possuir essa característica de transparência na forma em que foi mantido.

Uma transformação que a adoção da tecnologia pode fornecer é uma melhora na comunicação, permitindo uma interoperabilidade e rastreabilidade. No caso da erva-mate, a *blockchain* permite com que dados como a origem e destino, detalhes do processamento, transporte, detalhes de manejo, entre outras, sejam armazenados. Como a erva-mate é vista como fonte de renda de pequenos e médios produtores, a inclusão de novas tecnologias no apoio a informação e rastreabilidade, pode ser fator crucial de competitividade, para gerar mais valor agregado ao seu produto.

Para fazer com que haja uma comunicação padronizada entre empresas, já que cada uma pode possuir um sistema próprio, se fez necessária a criação de um *web service*, para permitir a integração.

A criação de uma rede *blockchain* voltada para *commodities* agrícola, que é a erva-mate, pode ser instrumento para criação de uma rede genérica, que possa abstrair outras *commodities*, e porventura também outras cadeias de suprimento, gerando todos os benefícios que a *blockchain* fornece.

Com a adoção da *blockchain*, é possível fazer a rastreabilidade dos produtos, sendo possível identificar gargalos de desperdício ou até mesmos lotes defeituosos e quais as suas origens, garantindo qualidade e segurança para o consumidor final.

Com a criação de um sistema de armazenamento de informações cruciais para a vida dos suprimentos, começando com um modelo como o proposto para a erva-mate, busca-se um maior uso no futuro por toda a rede logística em outras cadeias de suprimentos.

Com uma maior disponibilidade da informação pela adoção da tecnologia da *blockchain*, os produtos poderão ser rastreados, e fornecerão maior confiança. Também poderá ser fator de diferenciação perante os concorrentes na entrega do produto, fazendo assim com que agregue valor e seja um diferencial competitivo.

O cenário da fiscalização passará a mudar, pois poderá contar com a ajuda da nova cadeia de suprimentos, pois as informações de transações serão livres e refletem um dado seguro, vindo diretamente da sua fonte. Também é possível que as informações geradas possam ser utilizadas na tomada de decisões, fazendo com que até mesmo no futuro, pelos dados se encontrarem unidos, ocorra mudança referentes a rotas, preço do frete, entre outros aspectos de consenso.

Como perspectivas de trabalhos futuros, sugere-se o acompanhamento de sistemas com tecnologia *blockchain* implementada, com análise de custos, benefícios e impactos organizacionais; a integração de sistemas de internet das coisas gerando dados e avaliação de desempenho na adição de blocos em *blockchain*; e avaliar abertura de organizações pertencentes às cadeias produtivas com adoção de tecnologia *blockchain*.

REFERÊNCIAS

ASSAWAMEKIN, Namfon. An ontology-based approach for multiperspective requirements traceability between analysis models. In: **2010 IEEE/ACIS 9th International Conference on Computer and Information Science**. IEEE, 2010. p. 673-678.

AKUTSU, Rita de Cássia et al. Adequação das boas práticas de fabricação em serviços de alimentação. **Revista de Nutrição**, v. 18, n. 3, p. 419-427, 2005.

BABU, Sarat Chandra. E-learning standards. In: **ELELTECH INDIA-National seminar on "e-learning & elearning technologies**. 2001. p. 7-8.

BALLOU, Ronald H. **Gerenciamento da cadeia de suprimentos: planejamento, organização e logística empresarial**. Bookman, 2001.

BENCHOUFI, Mehdi; RAVAUD, Philippe. Blockchain technology for improving clinical research quality. **Trials**, v. 18, n. 1, p. 335, 2017.

BRASILIA. **Lei nº 8080, de 19 de setembro de 1990**. Diário Oficial da República Federativa do Brasil. [*S. l.*], 19 set. 1990.

BRASILIA. **Lei nº 9782, de 26 de janeiro de 1999**. Diário Oficial da República Federativa do Brasil. [*S. l.*], 26 jan. 1999.

BUMBLAUSKAS, Daniel et al. A blockchain use case in food distribution: Do you know where your food has been?. **International Journal of Information Management**, v. 52, p. 102008, 2020.

CARLOZO, Lou. What Is Blockchain? Here's a Primer on the Potentially Transformative Digital Ledger Technology. **Journal of Accountancy**, v. 224, n. 1, p. 29, 2017.

CHRISTOPHER, Martin. Logistics and Supply Chain Management: Strategies for Reducing Cost and Improving Service Financial Times: Pitman Publishing. London, 1998 ISBN 0 273 63049 0 (hardback) 294+ 1× pp. 1999.

CHRISTOPHER, Martin; TOWILL, Denis R. Developing market specific supply chain strategies. **The international journal of logistics management**, v. 13, n. 1, p. 1-14, 2002.

CLELAND-HUANG, Jane et al. Best practices for automated traceability. **Computer**, v. 40, n. 6, p. 27-35, 2007.

CORON, J.-S. What is cryptography?. **IEEE security & privacy**, v. 4, n. 1, p. 70-73, 2006.

DE VASCONCELOS, Flávio Carvalho; BRITO, Luiz Artur Ledur. Vantagem competitiva: o construto e a métrica. **RAE-Revista de Administração de Empresas**, v. 44, n. 2, p. 51-63, 2004.

FEDOSEJEV, Artemij. **React. js Essentials.** Packt Publishing Ltd, 2015.

FIGUEIREDO, Kleber. A logística enxuta. **Centro de Estudos em Logística–COPPEAD/UFRJ**, 2006.

FIELDING, Roy et al. Hypertext transfer protocol–HTTP/1.1. 1999.

FOROGLOU, George; TSILIDOU, Anna-Lali. Further applications of the blockchain. In: **12th student conference on managerial science and technology**. 2015. p. 1-8.

GALVEZ, Juan F.; MEJUTO, J. C.; SIMAL-GANDARA, J. Future challenges on the use of blockchain for food traceability analysis. **TrAC Trends in Analytical Chemistry**, v. 107, p. 222-232, 2018.

GANTORI, Sundeep et al. Cryptocurrencies Beneath the Bubble. **UBS. Tratto da https://www.ubs.com/content/dam/WealthManagementAmericas/cioimpact/ cryptocurrencies. pdf**, 2017.

GERVASI, Vincenzo; ZOWGHI, Didar. Mining requirements links. In: **International Working Conference on Requirements Engineering: Foundation for Software Quality**. Springer, Berlin, Heidelberg, 2011. p. 196-201.

GEORGE, Reno Varghese et al. Food quality traceability prototype for restaurants using blockchain and food quality data index. **Journal of Cleaner Production**, v. 240, p. 118021, 2019.

GOTEL, Orlena CZ; FINKELSTEIN, C. W. An analysis of the requirements traceability problem. In: **Proceedings of IEEE International Conference on Requirements Engineering.** IEEE, 1994. p. 94-101.

HANSEN, Roseli; CRESPO, S. Glue script: Uma linguagem específica de domínio para composição de web services. **Universiade do Vale do Rio dos Sinos**, 2003.

IBGE. Banco de Dados Agregados. Sistema IBGE de Recuperação Automática – SIDRA-Pesquisa Pecuária Municipal. Instituto Brasileiro de Geografia e Estatística. Disponível em: Disponível em: <http://www.ibge.gov.br>. Acesso em: 22 mai. 2019.

JIRAPANTHONG, Waraporn. Requirements traceability on web applications. In: **2015 7th International Conference on Information Technology and Electrical Engineering (ICITEE)**. IEEE, 2015. p. 18-23.

JOINT, F. A. O et al. The role of food safety in health and development: report of a joint FAO/WHO expert committee on food safety. In: **The role of food safety in health and development: report of a joint FAO/WHO expert committee on food safety**. 1984. p. 79-79.

KAMILOGLU, Senem. Authenticity and traceability in beverages. **Food chemistry**, v. 277, p. 12-24, 2019.

KOSKELA, Lasse. Test Driven: TDD and Acceptance TDD for Java Developers [Paperback]. 2007.

LÓSCIO, Bernadette Farias; OLIVEIRA, HR de; PONTES, JC de S. NoSQL no desenvolvimento de aplicações Web colaborativas. **VIII Simpósio Brasileiro de Sistemas Colaborativos**, v. 10, n. 1, p. 11, 2011.

LUSTOSA, Leonardo Junqueira; DE MESQUITA, Marco Aurélio; OLIVEIRA, RODRIGO J. **Planejamento e controle da produção**. Elsevier Brasil, 2008.

MADEIRA, Márcia; FERRÃO, Maria Eliza Marti. **Alimentos conforme a lei**. Editora Manole Ltda, 2002.

MARTINS, T F. Prova de existência de arquivos digitais utilizando a tecnologia *blockchain* do protocolo Bitcoin. Universidade Federal do Rio Grande do Sul, 2018.

MATÉ, Alejandro; TRUJILLO, Juan. A trace metamodel proposal based on the model driven architecture framework for the traceability of user requirements in data warehouses. **Information Systems**, v. 37, n. 8, p. 753-766, 2012.

MAZUCHOWSKI, J. Z.; RUCKER, N. G. de A. Erva-mate: prospecção tecnológica da cadeia produtiva. Curitiba: Secretaria de Estado da Agricultura e do Abastecimento, 1997. 23p.

NAKAMOTO, Satoshi; BITCOIN, A. A peer-to-peer electronic cash system. **Bitcoin.–URL: https://bitcoin. org/bitcoin**. pdf, v. 4, 2008.

OPARA, Linus U.; MAZAUD, Francois. Food traceability from field to plate. **Outlook on agriculture**, v. 30, n. 4, p. 239-247, 2001.

OPARA, Linus U. Traceability in agriculture and food supply chain: a review of basic concepts, technological implications, and future prospects. Journal of Food Agriculture and Environment, v. 1, p. 101-106, 2003.

PARFITT, Julian; BARTHEL, Mark; MACNAUGHTON, Sarah. Food waste within food supply chains: quantification and potential for change to 2050. **Philosophical transactions of the royal society B: biological sciences**, v. 365, n. 1554, p. 3065-3081, 2010.

PIOVESAN, Márcia Franke et al. Vigilância Sanitária: uma proposta de análise dos contextos locais. **Revista Brasileira de Epidemiologia**, v. 8, p. 83-95, 2005.

PORTER, Michael E.; VAN DER LINDE, Claas. Toward a new conception of the environment-competitiveness relationship. **Journal of economic perspectives**, v. 9, n. 4, p. 97-118, 1995.

POSHYVANYK, Denys et al. Feature location using probabilistic ranking of methods based on execution scenarios and information retrieval. **IEEE Transactions on Software Engineering**, v. 33, n. 6, p. 420-432, 2007.

RAO, Jinghai; SU, Xiaomeng. A survey of automated web service composition methods. In: **International Workshop on Semantic Web Services and Web Process Composition**. Springer, Berlin, Heidelberg, 2004. p. 43-54.

REMPEL, Patrick; MÄDER, Patrick. Estimating the implementation risk of requirements in agile software development projects with traceability metrics. In: **International Working Conference on Requirements Engineering: Foundation for Software Quality**. Springer, Cham, 2015. p. 81-97.

REYNA, Ana et al. On blockchain and its integration with IoT. Challenges and opportunities. **Future generation computer systems**, v. 88, p. 173-190, 2018.

RODIGHERÍ, Honorino Roque. **Rentabilidade econômica comparativa entre plantios florestais e sistemas agroflorestais com erva-mate, eucalipto e pinus e as culturas do feijão, milho, soja e trigo**. EMBRAPA-CNPF, 1997.

RODRIGUES, C.K.S. Uma análise simples de eficiência e segurança da Tecnologia *Blockchain*. Universidade de Brasília, 2018.

SEURING, Stefan; MÜLLER, Martin. From a literature review to a conceptual framework for sustainable supply chain management. **Journal of cleaner production**, v. 16, n. 15, p. 1699-1710, 2008.

SIKORSKI, Janusz J.; HAUGHTON, Joy; KRAFT, Markus. Blockchain technology in the chemical industry: Machine-to-machine electricity market. **Applied Energy**, v. 195, p. 234-246, 2017.

SILVA, José Amande da. Ontologia na rastreabilidade de dados agrícolas. 2018, 74f. Dissertação (Mestrado em Computação Aplicada), Universidade Estadual de Ponta Grossa, Ponta Grossa, 2018.

SMITH, B. Gail. Developing sustainable food supply chains. **Philosophical Transactions of the Royal Society B: Biological Sciences**, v. 363, n. 1492, p. 849-861, 2008.

SULTANOV, Hakim; HAYES, Jane Huffman. Application of swarm techniques to requirements engineering: Requirements tracing. In: **2010 18th IEEE International Requirements Engineering Conference**. IEEE, 2010. p. 211-220.

TILKOV, Stefan; VINOSKI, Steve. Node. js: Using JavaScript to build high-performance network programs. **IEEE Internet Computing**, v. 14, n. 6, p. 80-83, 2010.

WILLIAMSON, Oliver E. Outsourcing: transaction cost economics and supply chain management. **Journal of supply chain management**, v. 44, n. 2, p. 5-16, 2008.

YOSHIDA, Hirotaka; BIRYUKOV, Alex. Analysis of a SHA-256 variant. In: **International Workshop on Selected Areas in Cryptography**. Springer, Berlin, Heidelberg, 2005. p. 245-260.