UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

EDINEI DA MOTTA MARTINELLO

UMA ABORDAGEM PARA USO DE BLOCKCHAIN NA CADEIA DE SUPRIMENTOS DE VINHO

PATO BRANCO

2023

EDINEI DA MOTTA MARTINELLO

UMA ABORDAGEM PARA USO DE BLOCKCHAIN NA CADEIA DE SUPRIMENTOS DE VINHO

AN APPROACH FOR USING BLOCKCHAIN IN THE WINE SUPPLY CHAIN

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Bacharel em Engenharia de Computação do Curso de Bacharelado em Engenharia de Computação da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Me. Adriano Serckumecka

PATO BRANCO

2023

4.0 Internacional

Esta licença permite compartilhamento, remixe, adaptação e criação a partir do trabalho, mesmo para fins comerciais, desde que sejam atribuídos créditos ao(s) autor(es). Conteúdos elaborados por terceiros, citados e referenciados nesta obra não são cobertos pela licença.

EDINEI DA MOTTA MARTINELLO

UMA ABORDAGEM PARA USO DE BLOCKCHAIN NA CADEIA DE SUPRIMENTOS DE VINHO

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Bacharel em Engenharia de Computação do Curso de Bacharelado em Engenharia de Computação da Universidade Tecnológica Federal do Paraná.

Data de aprovação: 01/dezembro/2023

Adriano Serckumecka
Me. Computação Aplicada
Universidade Tecnológica Federal do Paraná

Luís Cassiano Goularte Rista
Me. Ciência da Computação
Universidade Tecnológica Federal do Paraná

Fábio Favarim
Dr. Engenharia Elétrica
Universidade Tecnológica Federal do Paraná

PATO BRANCO
2023

Pelo carinho, afeto e cuidados que meus pais,
minha irmã, cunhado, sobrinhas e meus
amigos que durante toda minha trajetória
acadêmica, me ajudaram, dedico esta
monografia a eles. Com muita gratidão.

AGRADECIMENTOS

À minha família pelo apoio, ajuda e por propiciar um ambiente adequado para eu poder realizar meus estudos.

Aos meus amigos, de infinita bondade e companheirismo, que foram de suma importância para eu poder chegar até aqui.

A Luiza Stringhini e Thiago Furtado, pelo apoio, incentivo e amparo durante o desenvolvimento deste trabalho.

Ao meu orientador Prof. Adriano Serckumecka, por acreditar no potencial deste estudo, sempre estando pronto para ajudar e auxiliar no desenvolvimento, onde aprendo muitas coisas importantes.

A instituição de ensino Universidade Tecnológica Federal do Paraná (UTFPR) por propiciar a realização de minha graduação em uma instituição pública.

Compreendo, que o trabalho realizado contribuiu significativamente para o avanço no entendimento e aplicação da tecnologia *Blockchain* na cadeia de suprimentos de vinho, seja como trabalho disponível para acesso da comunidade, seja por despertar a curiosidade dos colegas e desejar saber mais sobre o assunto e casos de uso. A quem desejar, o endereço do repositório no Github para consulta ou replicação: (***github.com/edineim/winechain***).

Se eu vi mais longe, foi por estar sobre ombros de gigantes - Isaac Newton

RESUMO

As cadeias de suprimentos atuais são vastas e espalhadas em todo o mundo, conectando várias etapas e diferentes entidades no processo de produção. Apesar das vantagens quando aplicados tais métodos de rastreio, também é possível destacar algumas dificuldades, como: adulteração de datas, adulteração de documentação, entre outras. As técnicas rastreio mais utilizadas são o código de barras e/ou etiquetas de rádio frequência, sendo armazenadas em um banco de dados central, que pode ser alterado posteriormente. Contudo, uma vez alteradas as informações, pode-se constatar que os dados foram manipulados ou estão sendo falsificados. A *Blockchain*, por ser um banco de dados público e distribuído, pode ser usada na melhoria do gerenciamento das cadeias e na segurança dos alimentos, como destacado em estudos realizados na área. Plataformas públicas como Bitcoin, desenvolvidas como forma de moeda digital, decentralizada e confiável, não possibilita nenhuma implementação relacionada à cadeia de abastecimento, pelo fato de seu foco ser a troca de dinheiro digital. Outras plataformas como Ethereum, desenvolvidas como uma máquina completa de Turing, viabilizam o desenvolvimento de tais aplicações. Contudo, pelo fato de depender de sua moeda Ether, a qual tem alto valor comercial e volatilidade, ela inviabiliza sua aplicação em uma cadeia de suprimentos. *Frameworks* de *Blockchain* privado, como Hyperledger Fabric, podem resolver alguns dos problemas de *Blockchains* públicas, como o tempo de resposta no processamento e o custo associado à execução da tarefa. A viabilização dessa implementação ocorreu por meio da modelagem da arquitetura da rede com base na cadeia de suprimentos de vinho para o framework Hyperledger Fabric, a implementação envolveu quatro organizações, simulando assim as principais fases na cadeia de suprimentos do vinho. Durante esse processo, foram realizadas operações cruciais, como criação, leitura e transferência de ativos na rede. O funcionamento detalhado da rede e a interação do cliente durante a consulta do histórico são apresentados com precisão, proporcionando uma compreensão abrangente do sistema implementado.

Palavras-chave: *blockchain*; cadeia de suprimentos; hyperledger fabric.

ABSTRACT

Today's supply chains are vast and spread across the world, connecting multiple steps and different entities in the production process. Despite the advantages when applying such screening methods, it is also possible to highlight some difficulties, such as: tampering with dates, tampering with documentation, among others. The most used tracking techniques are barcodes and/or radio frequency tags, which are stored in a central database, which can be changed later. However, once the information is changed, it may be found that the data has been manipulated or is being falsified. *Blockchain*, as it is a public and distributed database, can be used to improve chain management and food safety, as highlighted in studies carried out in the area. Public platforms such as Bitcoin, developed as a form of digital, decentralized and reliable currency, do not allow for any implementation related to the supply chain, due to the fact that their focus is on the exchange of digital money. Other platforms such as Ethereum, developed as a Turing complete machine, enable the development of such applications. However, because it depends on its currency Ether, which has high commercial value and volatility, it makes its application in a supply chain unfeasible. Private *Blockchain Frameworks*, such as Hyperledger Fabric, can solve some of the problems of public *Blockchains*, such as processing response time and the cost associated with executing the task. This implementation was made possible by modeling the network architecture based on the wine supply chain for the Hyperledger Fabric framework. The implementation involved four organizations, thus simulating the main phases in the wine supply chain. During this process, crucial operations such as creating, reading and transferring assets on the network were carried out. Detailed network operation and customer interaction during history consultation are accurately presented, providing a comprehensive understanding of the implemented system.

Keywords: *blockchain*; supply chain; hyperledger fabric.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTAGEM DE CÓDIGOS FONTE

LISTA DE ABREVIATURAS E SIGLAS

Siglas

API	Interface de Programação de Aplicação
DApps	*Decentralized applications*
DLT	*Distributed Ledger Technology*
ERP	*Enterprise Resource Planning*
GPRS	*General Packet Radio Service*
GPS	*Global Positioning System*
IBM	*International Business Machines Corporation*
ID	Identificador
IoT	*Internet of Things*
LAN	*Local Area Network*
PBFT	*Practical Byzantine Fault Tolerance*
PoS	*Proof of Stake*
PoSCS	*Proof of Supply Chain Share*
POST	Para inserir e atualizar dados de outros sistemas
PoW	*Proof of Work*
QR	*Quick Response*
RFID	Identificação por rádio frequência
RSA	Rivest-Shamir-Adleman
SCM	*Supply Chain Management*
SP	São Paulo
TI	Tecnologia de Infraestrutura
WSL	Subsistema Windows para Linux

SUMÁRIO

1 INTRODUÇÃO

A cadeia de suprimentos é um conceito que se refere ao conjunto de processos e atividades envolvidos na produção e distribuição de um produto, desde a matéria-prima até o consumidor final (Malik *et al.*, 2010). Atualmente essas cadeias são vastas e espalhadas em todo o mundo, conectando várias etapas e diferentes entidades no processo. Apesar das vantagens quando se aplicam tais procedimentos de rastreio, também é possível destacar algumas dificuldades, como: adulteração de datas, más condições de armazenagem, adulteração de documentação, entre outras, sendo um grupo de atividades realizadas intencionalmente ou não, visando ganho econômico (Adamashvili *et al.*, 2021).

A maioria dos sistemas de rastreabilidade de informações da cadeia de vinhos, utiliza código de barras e/ou Identificação por rádio frequência (RFID), para armazenar as informações de diferentes etapas da cadeia de abastecimento, essas informações são coletadas e armazenadas em um banco de dados central e quando necessárias essas informações são recuperadas e apresentadas. Contudo, o sistema apresenta falhas visto que essas informações podem ser manipuladas e falsificadas a qualquer momento, apresentando uma ineficiência na identificação de unidades falsas (Biswas, 2017).

Um estudo realizado por (Tse *et al.*, 2017) apresenta o conceito de tecnologia *Blockchain* e seu uso potencial na segurança da informação da cadeia de suprimentos quando comparada com a cadeia de suprimentos tradicional, chegando a conclusão que *Blockchain* é uma tecnologia que pode auxiliar no rastreamento, monitoramento e auditoria de toda a cadeia de suprimentos, apresentando um modelo genérico de sua estrutura.

Uma *Blockchain* consiste em um banco de dados público distribuído, em que todas as informações relevantes são armazenadas e não podem ser apagadas. Tendo o Bitcoin como sua aplicação mais bem sucedida, apresentando um modelo de dinheiro digital descentralizado e confiável. Posteriormente, surgiu o Ethereum apresentando uma arquitetura completa de Turing, que possibilita a realização de cálculos matemáticos, além do desenvolvimento de *smart contracts* e *Decentralized applications* (DApps) (Ferretti, 2020).

Soluções de *Blockchain* privadas como Hyperledger e Multichain surgiram com o propósito de acrescentar ao cotidiano soluções de baixo custo e validações de transações mais ágeis. Tais plataformas apresentam arquiteturas diferentes, mas funcionamento semelhante, como mecanismos de acesso à rede por terceiros e validação de transações.

Um estudo realizado por (Biswas, 2017), apresenta todas as etapas necessárias para a implementação de uma cadeia de suprimentos para o vinho, desde o produtor de uvas à prateleira do supermercado. Sendo esse estudo utilizado como modelo na implementação da cadeia de suprimento em *Blockchains* privadas.

A implementação ocorre com quatro organizações, utilizando a *blockchain* privada Hyperledger Fabric, dessa forma, simulando as principais etapas da cadeia de suprimentos do vinho, realizando operações de criação, leitura e transferência de ativo na rede, sendo apresen-

tado o funcionamento de cada etapa, a iteração das entidades com rede e a consulta do cliente sobre o histórico do seu produto.

1.1 Objetivos

O objetivo geral deste trabalho é aprimorar a segurança na cadeia de suprimentos de vinho por meio da aplicação da tecnologia *Blockchain*. Especificamente, o *framework* Hyperledger Fabric é utilizado como base para implementar melhorias na cadeia de suprimentos de vinho.

1.1.1 Objetivos específicos

a) Definição da arquitetura com base na cadeia de suprimentos de vinho para o Hyperledger;

b) Implementar arquitetura utilizando o framework;

c) Realização de testes e coleta de dados.

1.2 Estrutura do trabalho

Este trabalho está organizado inicialmente em 5 partes, na Seção 2.1 apresentando com detalhes a tecnologia *blockchain*, os principais componentes, funcionamento, tipos, *frameworks* privados como: Hyperledger Fabric. Na Seção 2.2, é demonstrado modelos de organização, etapas, problemas, aplicações, transparência e os detalhes da cadeia de suprimentos de vinho. Na Seção 2.3, é apresentado as diferenças entre modelos tradicionais e descentralizados, e uma abordagem de gerenciamento da cadeia de suprimentos usando IoT e *blockchain*. No Capítulo 3, são descritos os materiais e métodos utilizados, além da modelagem detalhada da arquitetura de rede e detalhes da implementação. No Capítulo 4 é apresentado os resultados alcançados.

2 REFERENCIAL TEÓRICO

2.1 *Blockchain*

Uma *blockchain* é uma plataforma digital pública e descentralizada de “livro de registro” de transações. Como o nome sugere, esta plataforma se organiza pelas transações. Sua operacionalização se apoia em uma rede de nós descentralizados de processamento que garantem tanto a continuidade do crescimento do *blockchain*, através da inclusão de novos blocos, como a validação consensual de legitimidade da cadeia que está construída(Lima, 2021).

Dentre as principais características, citadas por (Atlam, 2019) estão:

a) Descentralização: Diferente da arquitetura centralizada que apresenta vários problemas, sendo ponto único de falha e escalabilidade, o *blockchain*, que por sua vez, usa um registro descentralizado e distribuído usando a capacidade de processamento de todos os usuários participantes na rede, reduzindo a latência e o ponto único de falha;

b) Imutabilidade: Nas arquiteturas centralizadas tradicionais, os bancos de dados podem ser alterados, sendo preciso ter confiança em terceiros para garantir a integridade das informações. Um recurso essencial do *blockchain* é a capacidade de garantir a integridade das transações criando livros contábeis imutáveis. Uma vez que cada bloco no *ledger* (registro distribuído e imutável de transações financeiras ou dados) se vincula ao bloco anterior, formando uma cadeia de blocos, as informações contidas nos blocos são permanentemente registradas e não podem ser alteradas, desde que o participante mantenha ativamente a integridade da rede.

c) Transparência: Em um ambiente *blockchain*, não há necessidade de terceiros que melhoram a facilidade de negócios e garantem um fluxo de trabalho confiável. O *blockchain* oferece um alto nível de transparência, compartilhando detalhes de transações entre todos os usuários participantes envolvidos nessas transações;

d) Segurança: Mesmo a segurança tendo um papel essencial para a maioria das tecnologias, o *blockchain* oferece melhor segurança, pois usa infraestrutura de chave pública que protege contra ações maliciosas para alterar os dados. Os usuários participantes da rede confiam nos recursos de integridade e segurança do mecanismo de consenso. Além disso, o *blockchain* elimina o ponto único de falha que afeta todo o sistema;

e) Eficiência: A arquitetura centralizada clássica apresenta menor eficiência quanto a: custo, velocidade de liquidação e gerenciamento de risco. O *blockchain*, melhora a arquitetura centralizada clássica distribuindo registros de banco de dados entre vários usuários envolvidos na rede. A distribuição das transações torna mais transparente a verificação de todos os registros armazenados no banco de dados.

A evolução dos *blockchains* pode ser dividida em três formas:

Blockchain 1.0: Moeda

Refere-se à criação do Bitcoin, que foi a primeira aplicação de um *blockchain* para resolver o problema de gastos duplos em compras digitais. O problema do gasto duplo é a falha potencial em uma moeda digital em que o mesmo *token* digital único pode ser gasto mais de uma vez. Isso é possível porque um *token* digital consiste em um arquivo digital que pode ser duplicado ou falsificado (Chohan, 2021).

A tecnologia foi proposta por Nakamoto em 2008 como forma de dar maior segurança às transações financeiras digitais. Ao usar um selo digital, as transações financeiras poderiam ser registradas permanentemente na *blockchain* do Bitcoin, o que evitaria que o mesmo recurso financeiro fosse gasto duas vezes. Os dois pilares da tecnologia são a criptografia de dados e o poder de processamento distribuído, também conhecido como *Distributed Ledger Technology* (DLT) (Lima, 2021).

Dentro da *blockchain*, todas as transações são únicas, públicas e verificáveis por qualquer membro pertencente a ela. Portanto, a tecnologia possibilitou a descentralização do sistema financeiro, eliminando a necessidade de um terceiro central responsável pela intermediação financeira entre duas pessoas ou instituições (Lima, 2021).

Bitcoin

Uma das primeiras e mais bem-sucedidas implementações de *blockchain* foi o Bitcoin, que surgiu em 2008. Foi criado por um indivíduo (ou grupo) chamado Satoshi Nakamoto, que publicou um artigo intitulado "*Bitcoin: A Peer-To-Peer Electronic Cash System*". O artigo descrevia uma versão ponto a ponto (*peer-to-peer*) de dinheiro digital que permitia que pagamentos online fossem enviados diretamente de uma parte para outra sem passar por uma instituição financeira, tornando-o o primeiro de seu tipo (Crosby *et al.*, 2016).

O Bitcoin funciona como uma forma de dinheiro digital que pode ser adquirido em sites especiais e trocado por moeda nacional. Sua taxa de câmbio é determinada pelo mercado, dependendo da oferta e da demanda. Os pagamentos podem ser feitos entre pessoas via *software*, sendo que cada pessoa possui uma carteira necessária para o pagamento. Carteiras Bitcoin são informações digitais que podem ser armazenadas via *software* ou *hardware*, como um pen drive usado para armazenar Bitcoin. As carteiras armazenam a chave privada, necessária para enviar ou receber criptomoedas. Quem estiver de posse dessa chave tem acesso a todas as criptomoedas armazenadas naquela carteira, possibilitando a realização de transações.

As transações ocorrem como pagamentos feitos por meio de débito na conta do remetente e crédito na conta do destinatário. Esses pagamentos são feitos por meio da troca de mensagens criptografadas que são verificadas na rede do usuário. A transação começa quando

B envia sua chave de criptografia pública para A. A então escreve uma ordem de pagamento para B e a assina com sua chave privada. Nesse momento, a ordem de pagamento é emitida para a rede do usuário Bitcoin, que agora precisa confirmar/verificar a transação para que ela se torne válida (Segendorf, 2014).

O mecanismo de consenso ocorre quando a rede chega a um consenso através da *Proof of Work* (PoW), onde o poder de processamento dos computadores conectados à rede determina a maioria, validando ou não a transação e gerando recompensas aos usuários envolvidos (Nakamoto, 2008).

Os indivíduos que dedicam seu poder de computação para gerar esse consenso são chamados de mineradores. Para cada bloco criado e extraído na rede, é gerada uma recompensa para os mineradores, também chamada de Bitcoin (Nakamoto, 2008).

Embora o Bitcoin tenha sido a primeira implementação bem-sucedida do *blockchain* e atualmente seja a moeda com maior capitalização, sua arquitetura é única e permite apenas a troca de dinheiro digital de forma descentralizada e confiável. Portanto, não é viável desenvolver uma solução de cadeia de suprimentos dentro de sua rede.

Blockchain 2.0: Contratos

A versatilidade do *blockchain* permitiu o surgimento de contratos inteligentes (*smart contracts*), propriedades inteligentes (*smart properties*), DApps e outras formas de soluções descentralizadas e autônomas. Isso marca uma mudança do propósito original do *blockchain* como uma ferramenta para transações monetárias para uma ferramenta para registrar qualquer tipo de transação e ativos.

O Ethereum, um *blockchain* programável que permite a criação de aplicativos descentralizados, desempenhou um papel significativo nessa etapa de desenvolvimento.

Ethereum

Em 2014, Vitalik Buterin *et al.* (2014) desenvolveu um protocolo *blockchain* chamado Ethereum após Bitcoin. Ethereum é uma plataforma de software baseada em *blockchain* que permite a construção e execução de contratos inteligentes e DApps. Esta plataforma também é a base para uma moeda virtual relacionada chamada Ether.

O Ethereum fornece uma linguagem de programação Turing completa que permite criar programas e executá-los no *blockchain*, chamados de contratos inteligentes (Ferretti, 2020). Contratos inteligentes, aplicativos descentralizados e Turing completo são descritos com mais detalhes na Seção 2.1.

Seu funcionamento é baseado em contas e seus saldos, que mudam por meio das transições de estado. O estado indica os saldos atuais de todas as contas, além de outros possíveis dados extras, e não é armazenado diretamente no *blockchain*. Em vez disso, ele é

codificado e mantido por contas em uma estrutura de dados separada, organizada como uma árvore Merkle Patricia[1], permitindo ao usuário da rede Ethereum a verificação por conta própria, sem ter acesso ao estado completo da *blockchain*. (Ferretti, 2020; Vujičić, 2018).

Existem duas categorias de contas diferentes na plataforma Ethereum: contas de propriedade externa, controladas por pessoas, semelhantes ao Bitcoin, consistindo em *nonce*, saldo em Ether, *hash* de código e armazenamento raiz; e contas de contrato, controladas por algum código de contrato inteligente. Uma vez ativado por uma conta externa, as configurações feitas são executadas, o que pode gerar outras transações (Ferretti, 2020). Isso é feito encapsulando um conjunto de regras criptográficas que são executadas apenas se certas condições forem atendidas. Eles são desenvolvidos usando uma linguagem de programação proprietária chamada *Solidity* (Buterin *et al*., 2014).

O processo de validação da plataforma Ethereum, que começou em julho de 2015 e durou até 15 de setembro de 2022, contou com o mecanismo PoW, semelhante ao Bitcoin. No entanto, o Ethereum passou por uma transição para um novo mecanismo de consenso, chamado *Proof of Stake* (PoS), por meio de um evento chamado "*The Merge*". Durante este evento, a camada de execução original do Ethereum, conhecida como *Mainnet*, que existe desde o bloco de gênese, se fundiu com a nova camada de consenso PoS, chamada de *Beacon Chain*.

Inicialmente, a *Beacon Chain* operava independentemente da *Mainnet*. Enquanto a *Beacon Chain* funcionava em paralelo usando PoS, a Ethereum *Mainnet*, com todas as suas contas, saldos, contratos inteligentes e estado de *blockchain*, continuou a ser protegida por PoW. A fusão marcou a integração final desses dois sistemas e resultou na substituição permanente do PoW pelo PoS. Esta descontinuação oficial do PoW levou a uma redução no consumo de energia em aproximadamente 99,95% (Ethereum, 2023).

A partir disso, eliminando a necessidade de mineração com o uso intensivo de energia, a rede adotou uma abordagem inovadora ao ser protegida por meio de Ether apostado, que funciona como uma forma de garantia. Ao utilizar Ether apostado como garantia, a rede incentiva a integridade. Caso ocorra alguma detecção de inconsistência no bloco proposto, a entidade que tentar burlar a rede enfrentará a perda dos ativos que foram "apostados"como garantia (Menezes, 2020). Essa estratégia não apenas reduz significativamente o consumo de energia, mas também promove a honestidade na rede. Para obter mais informações sobre a PoS, consulte a Seção sobre o mecanismo de consenso na referência 2.1.1.

Embora a plataforma Ethereum seja uma arquitetura Turing completa e seja possível implementar uma cadeia de suprimentos, todas as transações e construções realizadas na rede requerem sua moeda Ether, que teve forte valorização nos últimos anos. Isso encarece finan-

[1] Essa estrutura de mapeamento de valor-chave que nos permite verificar a integridade dos dados, se duas árvores tiverem pares iguais, tem-se que o *hash* raiz da árvore deve ser o mesmo e quando um par de valores-chave for atualizado, o *hash* raiz da árvore será diferente. Assim, pode-se realizar a verificação de um par de chave-valor sem o acesso a todos os nós.

ceiramente o uso da plataforma, além do custo adicional de recompensar os mineradores pela validação de blocos.

Contratos Inteligentes, Aplicativos Descentralizados e Turing Completo

Em 1994, o cientista da computação e jurista Nick Szabo (1997) cunhou o termo "contrato inteligente", ao definí-lo como "um protocolo de transação computadorizado que executa os termos de um contrato". A principal vantagem do uso de contratos inteligentes em relação aos contratos tradicionais é a eficiência do processo contratual. Os termos descritos no contrato são autoexecutáveis e podem incluir referências a contratos legais, minimizando o risco de execuções maliciosas e acidentais e a necessidade de intermediários confiáveis. Portanto, um contrato inteligente é um software capaz de tomar certas decisões quando condições predeterminadas são atendidas (Kolvart, 2016).

Isso só é possível graças ao mecanismo de programação completa Turing disponível na plataforma Ethereum, que representa um sistema de regras de manipulação de dados. Regras seguidas em sequência em dados arbitrários podem produzir o resultado de qualquer cálculo.

Um DApps é um programa de *software* que opera em uma rede *blockchain*. Como um desktop tradicional ou aplicativo móvel, um DApps tem uma interface de usuário que permite aos usuários interagir com ele. No entanto, a forma como os dados e o processamento são realizados em um DApps é diferente dos modelos tradicionais, pois são fornecidos pelo *blockchain*.

Existem várias diferenças entre usar *blockchain* em um DApps e usar métodos tradicionais de armazenamento e processamento de dados. Por exemplo, como os contratos inteligentes no *blockchain* são transparentes e visíveis publicamente, os usuários podem ver o que acontecerá antes de executar uma função ou enviar qualquer dado. Depois que uma interação é realizada no *blockchain*, ela não pode ser retirada, editada ou excluída, devido à imutabilidade e à natureza inviolável do *blockchain*. Por fim, a governança em um DApps é descentralizada, o que significa que os usuários têm voz ativa em sua gestão, ao contrário dos modelos tradicionais de governança centralizada (Yano *et al.*, 2020).

Blockchain 3.0: Além das Moedas e Contratos

A tecnologia *blockchain* tem aplicações de longo alcance além de transações financeiras, contratos inteligentes e propriedades inteligentes. Tem o potencial de transformar múltiplas indústrias e até mesmo a organização social. Em essência, é um novo paradigma organizacional que facilita interações eficientes e sem atrito em escala global (Swan, 2015). Esse potencial desbloqueia maior eficiência de alocação de recursos e automação nas indústrias. Também permite maior coordenação e colaboração social.

Do ponto de vista social, Tapscott e Tapscott (2018) explorou o potencial do *blockchain* em vários aspectos da organização humana. A tecnologia *blockchain* pode facilitar a inclusão

social e financeira por meio de micropagamentos e microfinanças. Pode revolucionar os processos democráticos, como serviços governamentais, eleições, política e justiça. Também pode ajudar na distribuição de direitos autorais e permitir a colaboração coletiva.

2.1.1 *O Bloco*

Conforme descrito por (Nakamoto, 2008), um bloco é a unidade fundamental de uma *blockchain*. A *blockchain* cresce e se organiza através do encadeamento sucessivo e criptográfico de blocos de transações. Um bloco contém diversas transações eletrônicas, que são agrupadas e, após serem revisadas e validadas pelos usuários da rede, são adicionadas ao final da cadeia existente. Uma transação representa uma atualização ou declaração do estado de um objeto físico ou digital, como uma transferência financeira, registro de propriedade, autenticação de documento ou estado do usuário.

A transparência do *blockchain* e a sequência cronológica distribuída são alcançadas através do uso de *hashes* criptografados de assinaturas digitais, que formam uma cadeia imutável de blocos. Cada bloco tem seu endereço único e inclui o endereço do bloco anterior como parte de seu registro. Esse mecanismo de ligação permite que o *blockchain* seja rastreado até o bloco original, também conhecido como bloco de gênese, a qualquer momento.

Depois que uma transação é registrada no *blockchain*, ela não pode ser removida ou alterada. Qualquer tentativa de adulteração de uma transação já incluída na *blockchain* seria detectada pelo mecanismo de consenso da rede, que rejeitaria automaticamente o bloqueio falso e a tentativa de adulteração.

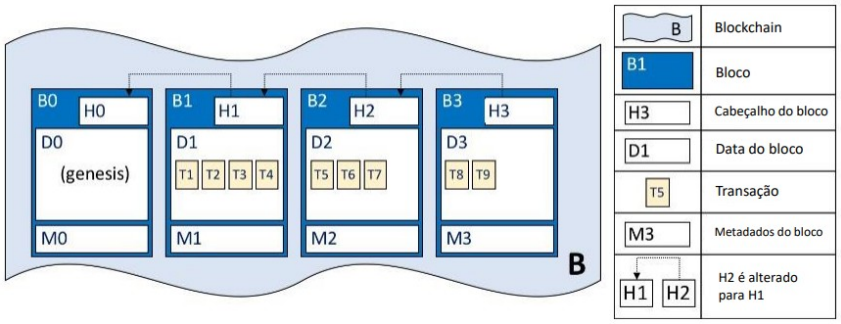
A Figura 1 ilustra a estrutura de uma *blockchain* B, contendo blocos B0, B1, B2, B3. B0 é o primeiro bloco do *blockchain*, o bloco gênese. É o ponto de partida do livro razão, embora não contenha nenhuma transação do usuário. Em vez disso, contém uma transação de configuração contendo o estado inicial do canal de rede (não mostrado).

Cada bloco B1, B2 e B3 contém um conjunto criptografado de registros de transação D e um cabeçalho H que inclui seu próprio registro de endereço e o registro de endereço do bloco anterior. Na imagem, pode-se observar que o bloco B2 possui um bloco de dados D2 que contém as transações: T5, T6, T7. Mais importante ainda, B2 possui um cabeçalho de bloco H2, que contém um hash criptográfico de todas as transações em D2, bem como um hash de H1. Desta forma, os blocos estão inextricavelmente e imutavelmente ligados uns aos outros.

A Figura 2 representa em maior detalhes a estrutura de um bloco de uma *blockchain*. O cabeçalho H2, por sua vez, armazena o número do bloco 2, um número inteiro começando em 0 (o bloco gênese) e aumentando em 1 para cada novo bloco anexado, um *hash* das transações CH2 pertencentes ao próprio bloco atual e uma cópia do *hash* do bloco predecessor PH1.

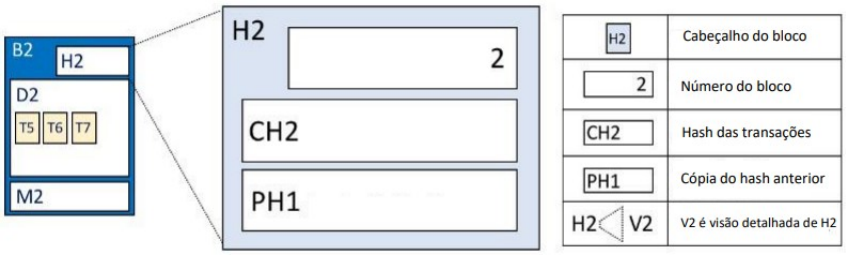
Por fim, a Figura 3 representa em maior detalhes a estrutura de informações contidas em um registro de transações. A transação T4 nos dados do bloco D1 do bloco B1 consiste no

Figura 1 – Esquema de uma *blockchain* "B"composta por 4 blocos e 9 transações.



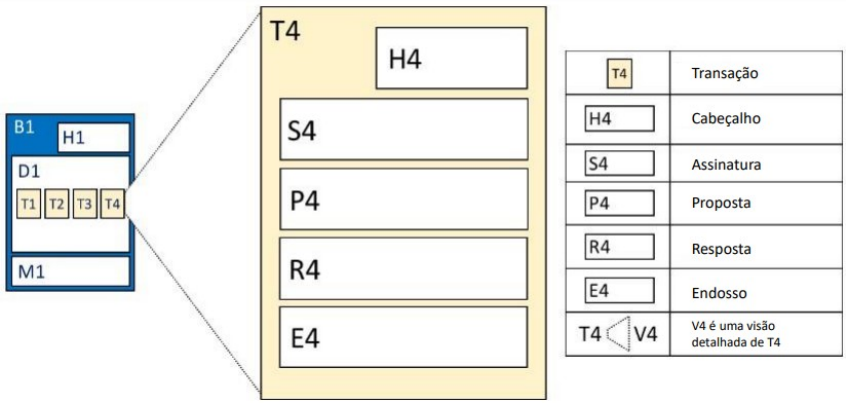
Fonte: Adaptacao de (Hyperledger, 2022).

Figura 2 – Detalhes do registro de uma transação.



Fonte: Adaptação de (Hyperledger, 2022).

Figura 3 – Esquema de um bloco.



Fonte: Adaptação de (Hyperledger, 2022).

cabeçalho da transação, H4, uma assinatura da transação, S4, uma proposta de transação P4, uma resposta da transação, R4, e uma lista de endossos, E4.

A transação T4, da Figura 3, contém os seguintes registros:

a) Cabeçalho (H4): Contém informações da transação, utilizada para a checagem da veracidade da transação;

b) Assinatura (S4): Assinatura criptográfica da transação, utilizada para a checagem da veracidade da transação;

c) Proposta (P4): A transação, são escritos na forma de parâmetros de entrada que serão tratados e que vão alterar o estado atual do registro no *blockchain*;

d) Resposta (R4): A resposta para a transação, registra o estado anterior e o novo estado do objeto da transação;

e) Endosso (E4): Assinaturas de validação da transação, podem ser exigências contratuais, pré-requisitos ou aprovações de membros pertencentes à organização.

De maneira resumida, um *blockchain* é estrutura como uma sequência de blocos de transações conectados por criptografia. Cada bloco contém um conjunto de transações que alteram ou atualizam os estados dos objetos registrados na *blockchain*.

O mecanismo de consenso

Componente crucial da tecnologia *blockchain*, servindo como base para validar transações e manter a integridade do registro compartilhado. Tanto a validação da cadeia de blocos existente na rede quanto a inserção de um novo bloco de transações devem ser aprovadas pela própria rede por meio de um mecanismo de consenso (Lima, 2021). Os dois mecanismos de consenso mais usados são PoW e PoS (Atlam, 2019).

A principal diferença entre os mecanismos de consenso está na maneira como o *blockchain* delega e a recompensa o trabalho de validação das transações realizadas (Lima, 2021).

PoW é um mecanismo de consenso usado no Bitcoin que depende de mineradores para validar transações e adicionar novos blocos ao *blockchain*. Os mineradores usam o poder computacional para resolver instâncias PoW e criar novos blocos, com a recompensa por minerar um novo bloco baseado em uma função *hash* (SHA-256) e encontrar um valor *nonce* que satisfaça uma determinada condição. Outros nós na rede podem verificar o PoW verificando o *hash* do bloco. O PoW foi projetado para impedir que uma única entidade controle a rede, exigindo uma quantidade significativa de poder computacional para minerar novos blocos (Segendorf, 2014), (Gervais *et al*., 2016).

O PoS foi desenvolvido para lidar com os altos custos de energia associados à mineração PoW e tornar o processo mais ecológico (Saleh, 2021). Em vez de depender do poder computacional, o PoS exige que os participantes mantenham uma certa quantidade de criptomoeda (por exemplo, Ether) como participação na rede. Os participantes que detêm uma aposta são incentivados a agir honestamente e validar as transações corretamente porque correm o risco de perder sua aposta ao se comportarem de forma desonesta (Wackerow, 2022).

2.1.2 *Banco de dados*

Um banco de dados clássico é uma estrutura de dados usada para armazenar informações. Usando um modelo relacional para fornecer formas mais compostas de consulta e coleta de dados, vinculando informações de vários bancos de dados, armazenando em elementos em

tabelas que contém campos, estes contém colunas para descrever o campo e as linhas para definir um registro armazenado no banco de dados (Atlam, 2019).

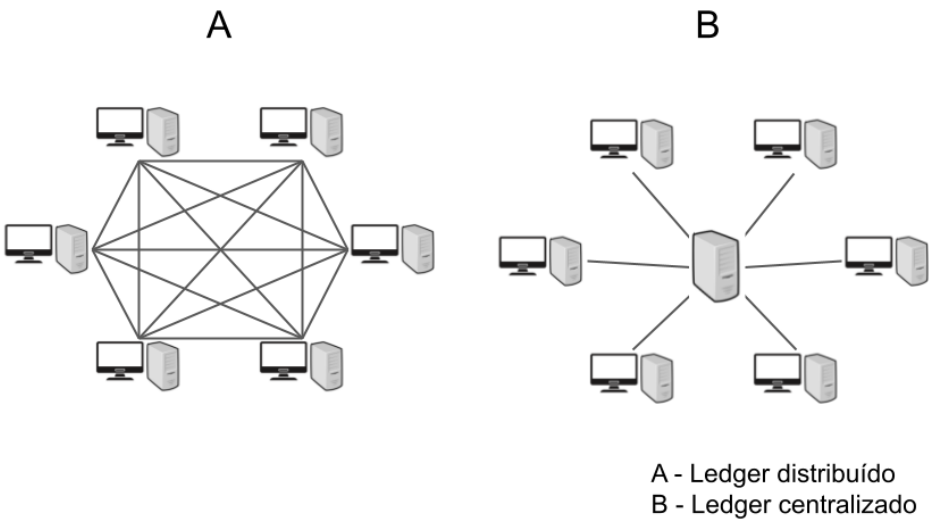
No *blockchain*, este não é um banco de dados clássico, contendo linhas e colunas, em vez disso, é um registro de todas as transações anteriores para todos os usuários participantes na rede *blockchain*. Esse modelo de banco de dados é caracterizado por ter alto rendimento, controle descentralizado, baixa latência, armazenamento de dados imutável e segurança integrada (Atlam, 2019).

2.1.3 *Distributed Ledger Technology*

Uma *blockchain* é um tipo de tecnologia de contabilidade distribuída DLT. Este livro-razão registra todo o histórico de transações já realizadas no *blockchain* sendo considerado distribuído pelo fato de estar armazenando em múltiplos computadores simultaneamente. O principal objetivo de uma DLT é garantir que toda a rede valide o conteúdo do livro-razão e certifique consensualmente a inserção de novos blocos de transações (Lima, 2021).

O sistema distribuído que permite que a *blockchain* funcione assim é o ponto a ponto, na qual, dados e recursos computacionais provenientes da colaboração de várias máquinas conectadas a Internet de maneira uniforme, distribuindo a carga de trabalho de maneira equilibrada, sem ocorrer sobrecarga indevida nos computadores, demonstrando eficiência quando usado para armazenar conjuntos muito grandes de dados imutáveis (Coulouris *et al.*, 2013). A Figura 4 A, apresenta uma representação do sistema ponto a ponto. Ao lado, na Figura 4 B, apresenta uma conexão convencional, em que todo o processamento está centralizado em uma unidade.

Figura 4 – Representação de redes diferentes.

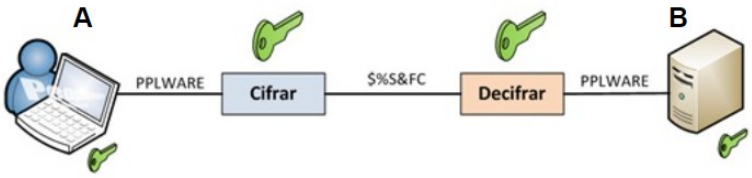


Fonte: Adaptacao de (Coulouris *et al.*, 2013).

2.1.4 Criptografia

Nas estruturas de criptografia usadas pela *blockchain*, são utilizados algoritmos para diferentes funcionalidades, como a assinatura digital e assinatura de blocos. De forma geral e simplificada, a criptografia de dados consiste no ato de embaralhar as informações de forma que apenas os que detém a chave para descriptografar tenha acesso às informações. Dentre os métodos de criptografia reversível, tem-se a simétrica e a assimétrica, além dos algoritmos de *hash*, não reversíveis (Stallings, 2006).

Figura 5 – Criptografia Simétrica.

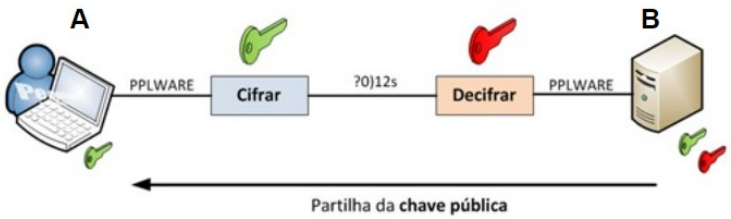


Fonte: Adaptação de (Pplware, 2010).

A criptografia simétrica, é baseada numa chave secreta que será usada em seu funcionamento, tendo como detalhamento as etapas do processo: um texto claro que passa por um algorítimo de encriptação, realizando diversas alterações e transformações no texto, usando uma única chave secreta compartilhada entre o emissor (A) e destinatário do conteúdo (B), obtendo assim um texto cifrado, produzido pelo algoritmo de encriptação. Para a decriptação da mensagem é necessária a chave secreta num processo inverso utilizando o algorítimo de decriptografia, tornando assim o texto claro novamente (Stallings, 2006), como representado da Figura 5.

Na criptografia assimétrica, há uma chave secreta composta de duas partes, sendo uma privada e outra pública e que se relacionam por meio de um algorítimo. Num cenário como representando na Figura 6, dois usuários A (chave verde) e B (chave vermelha) com um par de chaves de criptografia cada, quando A deseja enviar uma mensagem criptografada para B, ele usa a chave pública de B para criptografar a mensagem que só pode ser descriptografada usando a chave privada de B, então, B é a única pessoa que pode ler a mensagem (Stallings, 2006; Segendorf, 2014), como representado na Figura 6.

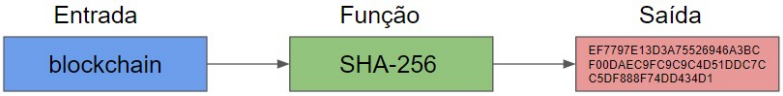
Figura 6 – Criptografia Assimétrica.



Fonte: Adaptação de (Pplware, 2010).

Nas funções de *hash*, também chamadas de resumo de mensagem, o algoritmo utilizado recebe uma mensagem de tamanho arbitrário como entrada e produz um resumo de mensagem de tamanho fixo. As funções de *hash* possuem propriedades adicionais que permitem serem usada para verificar a integridade de uma mensagem e como parte de esquemas de assinatura digital. Um sistema de criptografia assimétrica, por exemplo, o Rivest-Shamir-Adleman (RSA) ou Eliptic Curve, também podem ser usados como método de assinatura, embora os algoritmos específicos de *hash* tendem a ser mais rápidos para essa função (Garg; Yadav, 2014).

Figura 7 – Função *Hash*.



Fonte: Autoria Própria.

Em sistemas baseados em *blockchain*, a chave secreta é usada para assinar a mensagem e a chave pública é usada para verificar a assinatura dos envolvidos no processo. Já para garantir a integridade de uma transação, uma função de *hash* é utilizada para gerar um resumo (*hash*), como por exemplo a SHA-256, a qual recebe como entrada uma mensagem com comprimento máximo de até 2^{64} - 1 bits e retorna uma mensagem de 256 bits (Penard; Werkhoven, 2008).

2.1.5 Os tipos de *Blockchain*

Existem três tipos de *blockchain*: público, privado e em consórcio. As principais características de cada um deles resumidas são apresentadas na Tabela 1.

Os três tipos se diferem, principalmente, no tipo de acesso e no tipo de controle exercido sobre os nós participantes. (Atlam, 2019) apresenta detalhes e exemplos de cada dos tipos:

Blockchain pública

É um *blockchain* que permite que qualquer usuário anônimo seja adicionado à rede *blockchain*, envie uma transação, verifique os blocos recém-adicionados e leia o conteúdo do *blockchain*. O *blockchain* público está aberto para todos os tipos de entidades participarem da rede. A proteção do *blockchain* público é feita usando cripto economia, a qual é uma mistura de verificação criptográfica e incentivos econômicos usando mecanismos de consenso como PoW ou PoS. Dentre os *blockchains* publicas, as mais conhecidas são: Bitcoin, Ethereum e Cardano.

Blockchain privada

Nesse tipo de *blockchain*, apenas uma organização específica tem autoridade para ingressar na rede *blockchain*, enviar uma nova transação e participar do mecanismo de consenso.

Tabela 1 – Descrição dos Tipos de *Blockchain*

	Tipos de Blockchain		
	Pública	Privada	Consórcio
Acesso	Público	Público ou Restrito	Público ou Restrito
Consumo	Alto	Baixo	Baixo
Velocidade de transação	Mais alta	Mais baixa	Mais alta
Eficiência	Alta	Baixa	Alta
Segurança	PoW, PoS e outros	Participantes pré-aprovados para participação e consenso por votação, multipartido	Participantes pré-aprovados para participação e consenso por votação, multipartido
Imutabilidade	Praticamente impossível de alterar dados	Possibilidade de alteração dos dados	Possibilidade de alteração dos dados
Transparência	Informações disponíveis para todos os nós	Informações restrita às partes envolvidas, controle sobre privacidade de dados	Informações restrita às partes envolvidas, controle sobre privacidade de dados
Processo de consenso	Sem restrição de acesso e anônimo	Permissão para acesso e nós conhecidos	Permissão para acesso e nós conhecidos
Determinação de consenso	Todos os nós mineradores	Organização central	Nó líder determinado para cada tipo de transação
Rede	Totalmente descentralizada	Centralizada	Semi-centralizada
Tipo de ativo	Ativo específico por blockchain	Qualquer ativo	Qualquer ativo
Tempo de operação	Ordem de minutos	Ordem de milisegundos	Ordem de milisegundos

Fonte: (Lima, 2021).

Os usuários dispostos a participar precisam obter suas permissões da organização antes de ingressar na rede *blockchain*. Dentre os aplicativos prováveis que usam *blockchain* privado, incluem banco de dados e gerenciamento. Comparado com *blockchain* publico, o *blockchain* privado é mais fácil, pois com um número menor de participantes a verificação dos novos blocos não exige grande poder de processamento e tempo, além de, somente os identificados na rede poderem ler as transações. Dentre as *blockchain* privadas, as mais conhecidas são: Hyperledger Fabric, Multichain Enterprise, Ripple.

Blockchain em consórcio

É considerado como *blockchain* parcialmente privado, operado sob a autoridade de um grupo de empresas ou organizações. Ao contrário do *blockchain* público, o *blockchain* de consórcio é mais rápido e oferece melhor escalabilidade e privacidade. Dentre exemplos destes, destacam: R3, EWF e B3i.

2.1.6 *Blockchain*: aplicações

A tecnologia *blockchain* tem várias aplicações além de seu caso de uso inicial de moedas digitais como o Bitcoin. Hoje, existem mais de 600 moedas digitais usando a tecnologia *blockchain* como camada de tecnologia subjacente. Alguns dos casos de uso mais promissores apresentados por (Abeyratne; Monfared, 2016) incluem:

a) Trocas: *Blockchain* pode ser usado para criar sistemas descentralizados que permitem a troca de moedas digitais como Bitcoin ou qualquer outro ativo com uma identidade digital em uma rede. Exemplos de trocas de moeda digital existentes incluem Coinbase, ItBit e Kraken.

b) Mercado de ações: os mercados de ações descentralizados movidos pela tecnologia *blockchain* podem permitir a negociação de ações em uma plataforma que não é controlada por nenhum órgão governamental único. Os usuários podem ter certeza de que as trocas serão realizadas corretamente, pois o sistema funcionará apenas conforme descrito pelo protocolo do sistema. No entanto, esta aplicação ainda não foi adotada.

c) Identidade digital: a tecnologia *Blockchain* pode permitir um serviço de identidade descentralizado que dimensiona a identidade digital a custos baixos com melhorias significativas na segurança. Em vez de vários governos emitirem identidades ou passaportes para os cidadãos, um serviço de identidade descentralizado usando a tecnologia *blockchain* poderia fornecer aos usuários de todo o mundo sua própria identidade digital.

d) Votação: a tecnologia *Blockchain* pode autenticar o processo de votação usando “chaves privadas” para cada eleitor. O protocolo do sistema pode ser projetado para validar as identidades dos usuários, mantendo-os anônimos ao calcular o resultado final da eleição em tempo real. Como o protocolo é transparente, os eleitores podem ter certeza de que os resultados são precisos e não vulneráveis a manipulação e fraude.

e) Aplicações de engenharia: sistemas de engenharia complexos são considerados o próximo domínio de aplicação potencial para a tecnologia *blockchain*. As transações relacionadas à engenharia que podem se beneficiar imediatamente da abordagem *blockchain* incluem o controle de transações financeiras entre e dentro das empresas, rastreamento de ativos e produtos durante e após a fabricação, controle da qualidade e dos testes, projetos modulares distribuídos para máquinas e sistemas e a cadeia de suprimentos de fabricação, que é o foco principal deste artigo.

f) Rastreamento de ativos: *Blockchain*s podem ser usados para rastrear ativos físicos e manter um registro de propriedade de cada ativo. Por exemplo, a Everledger rastreia diamantes criando uma identidade digital para cada diamante em uma rede *blockchain*,

o que ajuda na autenticação de transações e evita que "diamantes de sangue", entrem no mercado de joias.

No Brasil, destaque ao primeiro projeto no setor canavieiro brasileiro, utilizando rastreamento de ativos, sendo ele o açúcar mascavo, desenvolvido por uma equipe de especialistas da Embrapa Agricultura Digital - São Paulo (SP). O projeto possibilita que os dados de fabricação do produto sejam armazenados em blocos digitais, usando a *blockchain* para construir uma sequência temporal e imutável dos registros e garantido, assim, a integridade das informações geradas ao longo do processo de produção. Por meio de um QR Code estampado na embalagem, qualquer pessoa poderá verificar informações sobre a origem e o processo de fabricação do açúcar. Informações como: data de produção, variedade da cana utilizada, identificação e geolocalização da propriedade rural que forneceu a matéria-prima, podem ser acessadas (Embrapa, 2022).

Na Figura 8, apresenta a embalagem do açúcar que chegará ao consumidor, com destaque ao QR Code do produto, localizado no canto inferior esquerdo, aonde poderão ser acessados as informações.

Figura 8 – Primeiro açúcar mascavo rastreado no Brasil.

Fonte: (Embrapa, 2022).

2.1.7 Hyperledger Fabric

Conforme descrito em sua documentação, o Hyperledger é uma plataforma *blockchain* privada hospedada pela Linux Foundation, desenvolvido em parceria com a *International Business Machines Corporation* (IBM), sendo pioneiro no atendimento a empresas. Com suporte para contratos inteligentes que se adaptam a diversos aplicativos em diferentes domínios, permite que as organizações participantes implementem soluções *blockchain* de maneira eficaz (Hyperledger, 2022).

A plataforma é composta por vários nós que hospedam o *blockchain* e executam contratos inteligentes, conhecidos como *chaincodes*, mantendo coletivamente o estado do livro-razão.

Os *chaincodes* podem ser compartilhados entre todas as entidades em um consórcio ou podem ser privados, acessíveis apenas a determinados nós.

Durante a configuração, os nós requerem criptografia para autenticar os pares na rede, garantindo que apenas participantes autorizados tenham acesso. Além disso, a plataforma utiliza um serviço de pedidos para gerenciar as transações aceitas na rede por canal.

Os *chaincodes* manipulam um estado de armazenamento chamado valor-chave, utilizando métodos de leitura e gravação, com suporte para diferentes bancos de dados, incluindo o LevelDB e CouchDB. As transações são realizadas de acordo com um processo que envolve o cliente, os pontos de endossamento e o serviço de pedidos.

Componentes Principais do Hyperledger Fabric

a) *Peers* (Nós): Todos os membros da rede executam nós do Hyperledger Fabric. Cada membro da rede possui pelo menos um par de *peers* (um para endorsamento e outro para validação).

b) *Orderer* (Pedidos): A rede usa um ou mais nós *orderers* para criar blocos e manter a ordem correta das transações. Os *orderers* garantem a consistência da rede.

c) *Chaincode* (Smart Contracts): Os *chaincodes* definem a lógica de negócios para as transações na rede. Cada membro da rede, incluindo os validadores, implementa os *chaincodes* para processar transações relacionadas à cadeia de suprimentos.

d) Canais: É possível criar canais para segmentar a comunicação entre diferentes entidades. Os canais podem ser usados para garantir que certas transações sejam visíveis apenas para as partes relevantes.

e) Identidade e Política de Acesso: Cada membro da rede possui uma identidade digital que é usada para autenticação. Políticas de acesso são configuradas para definir quem pode executar que tipo de transação.

f) *Ledger* Distribuído: Cada membro da rede mantém uma cópia do *ledger* distribuído, que contém o histórico de todas as transações.

g) Mineração e Validação: Os validadores são responsáveis pela validação de transações. Eles verificam a legitimidade das transações antes de adicioná-las ao *ledger* compartilhado.

Políticas de Consenso e Segurança

O Hyperledger Fabric suporta mecanismos de consenso como Kafka e Raft, oferecendo uma abordagem personalizável com base nas necessidades específicas do aplicativo. Em termos de segurança, implementa medidas robustas, incluindo criptografia de ponta a ponta

e um modelo de identidade baseado em certificados X.509, garantindo a autenticidade dos participantes e a prevenção de acessos não autorizados.

Identidade e Política de Acesso

A identidade dos participantes é gerenciada por meio de certificados X.509 emitidos por uma autoridade confiável, controlando as permissões com base nos papéis e responsabilidades dos participantes na rede.

Integração e API

O Hyperledger Fabric oferece um amplo conjunto de ferramentas e API para integrar-se a sistemas e aplicativos existentes, permitindo o desenvolvimento de soluções personalizadas e a interação flexível com a rede de *blockchain*.

2.1.8 Multichain Enterprise

Caracteriza-se como uma plataforma completa para criação e implementação de *blockchains* privadas, fornecendo controle e privacidade, buscando resolver problemas relacionados à mineração, privacidade e gerenciamento de usuários.

Dentre seus objetivos estão: garantir que a atividade seja visível apenas para participantes escolhidos; introduzir controle sobre quais transações são permitidas e permitir que a mineração ocorra com segurança sem PoW e custos associados.

Em seu funcionamento, o minerador do primeiro bloco “gênesis” recebe todos os privilégios definindo a fase de configuração da cadeia, incluindo direitos de administrador para gerenciar os privilégios de outros usuários. Esses privilégios podem ser concedidos a outros usuários em transações cujas saídas contém os endereços desses usuários, com metadados que denotam privilégios conferidos. Para realizar uma alteração dos privilégios de administração e mineração de outros usuários, é necessário a realização de uma votação entre os administradores existentes. A votação ocorre em uma transação separada, aplicada no momento que houver consenso. Como as modificações nos privilégios são incorporadas nos metadados das transações, elas se propagam rapidamente para todos os nós da rede, criando consenso sobre o estado atual. Se alguma transação estiver acontecendo no momento pode ocorrer de alguns nós validarem e outros rejeitam. Essas diferenças serão resolvidas assim que as transações forem confirmadas no *blockchain*, fixando sua ordem final.

Para se caracterizar como uma *blockchain* privada, para cada endereço com permissão nessa cadeia, pelo menos um administrador deve conhecer a identidade real da entidade que usa esse endereço, contudo, a maioria dos participantes da cadeia não precisa conhecer as identidades uns dos outros.

A mineração realizada na plataforma resolve problemas colocados pelas *blockchains* privadas, onde pode ocorrer monopolização por um participante no processo de mineração. Sua solução visa restringir o número de blocos que podem ser criados pelo mesmo minerador dentro de uma determinada janela, utilizando um parâmetro chamado diversidade de mineração que pode variar entre 0 e 1, isso impõe um cronograma de escalonamento, onde os mineradores permitidos devem criar blocos válidos em rotação. O parâmetro define a proporção de mineradores permitidos que precisam conspirar para minar a rede. Um valor de 1 garante que todos os mineradores permitidos sejam incluídos na rotação, enquanto 0 não representa nenhuma restrição. Um valor sugerido é de 0,75.

Na mineração baseada em permissões, há taxas de transação e recompensas de blocos nulas por padrão, sendo possível, a realização de cobranças de taxas caso seja necessário, por uma taxa fixa, paga por meios tradicionais fora da *blockchain* (Greenspan *et al*., 2015).

2.2 Cadeia de Suprimentos: visão geral

Nos estágios iniciais da cadeia de suprimentos, ela consistia em um conjunto de processos lineares e individualizados que conectavam fabricantes, armazéns, atacadistas, varejistas e consumidores por meio de uma cadeia humano/papel. No entanto, devido à má comunicação e falta de coordenação, isso muitas vezes resultou em falta de comunicação entre os diferentes grupos. A sinergia de compras, planejamento e previsão de demanda, gerenciamento de estoque e modos de transporte ainda estava longe de ser possível.

Como a manufatura e o crescimento econômico prosperaram durante a década de 1950, desenvolveu-se um maior interesse na necessidade de SCM. Depois de 1950, SCM ganhou um impulso com os setores de produção e manufatura recebendo a maior atenção. O estoque passou a ser responsabilidade das áreas de marketing, contabilidade e produção, e o processamento de pedidos passou a ser parte da contabilidade e vendas. O SCM tornou-se um dos motores mais poderosos da transformação dos negócios, pois é a única área em que a eficiência operacional pode ser obtida. Reduz os custos organizacionais e melhora os serviços ao cliente.

Hoje, as empresas operam em um ambiente global, o que obriga as empresas, independentemente de localização ou base de mercado principal, a considerar o resto do mundo em sua análise de estratégia competitiva. As empresas não podem ignorar fatores externos, como tendências econômicas, situações competitivas ou inovações tecnológicas em outros países, especialmente se seus concorrentes estiverem competindo ou localizados nesses países. As empresas estão se tornando verdadeiramente globais com o SCM e, como tal, mudaram a maneira como gerenciam suas operações e atividades logísticas.

As mudanças no comércio, a expansão e modernização das infraestruturas de transporte e a intensificação da concorrência elevaram a importância da gestão de fluxos a novos patamares. SCM é um conceito ou mecanismo para melhorar a produtividade total das empre-

sas em uma cadeia de suprimentos, otimizando o tempo, a localização e a quantidade de fluxo de material dos fornecedores de matéria-prima para os consumidores finais do produto.

Em conclusão, o SCM percorreu um longo caminho desde seus estágios iniciais, onde consistia em um conjunto de processos lineares e individualizados. Tornou-se agora um dos motores mais poderosos de transformação de negócios, permitindo que as empresas operem globalmente e melhorem a eficiência operacional, reduzindo os custos organizacionais e aprimorando o atendimento ao cliente. Mudanças no comércio, transporte e concorrência elevaram a importância do gerenciamento de fluxo, e o SCM é o conceito ou mecanismo que pode ajudar as empresas a otimizar a produtividade de suas cadeias de suprimentos (Malik *et al.*, 2010).

2.2.1 O que é o SCM?

O conceito de SCM assenta em dois pilares fundamentais. A primeira é que é o esforço cumulativo de várias organizações trabalhando juntas para garantir que cada produto chegue ao usuário final. Essas organizações são coletivamente conhecidas como cadeia de suprimentos. O segundo pilar é que a maioria das organizações tende a focar apenas nas atividades dentro de suas próprias paredes, mesmo que as cadeias de suprimentos existam há muito tempo. Isso levou a uma gestão ineficiente das cadeias de suprimentos, com apenas um punhado de organizações capazes de entender e gerenciar toda a cadeia de atividades que entrega o produto ao cliente final.

SCM incorpora o planejamento e gerenciamento de todas as atividades envolvidas no fornecimento, aquisição, conversão e distribuição de produtos. Trata-se de obter sinergia com fornecedores, prestadores de serviços terceirizados e clientes. O SCM integra o gerenciamento de oferta e demanda dentro e entre as organizações, com o objetivo de maximizar o valor do cliente e alcançar uma vantagem competitiva sustentável.

O SCM eficaz envolve a coordenação e colaboração com todos os parceiros da cadeia de suprimentos, de fornecedores a clientes, para otimizar todos os aspectos do processo. Envolve gerenciar o fluxo de mercadorias e informações, desde matérias-primas até produtos acabados, e garantir que os produtos certos sejam entregues aos clientes certos no momento certo. Por meio do SCM, as empresas podem reduzir custos, melhorar a eficiência, aumentar a qualidade e aumentar a satisfação do cliente (Malik *et al.*, 2010).

2.2.2 Etapas (Modelo SCOR)

O SCM desempenha um papel vital em garantir que a cadeia de suprimentos de uma organização não seja apenas eficiente, mas também econômica. Uma cadeia de suprimentos compreende um conjunto de atividades que uma organização realiza para transformar matérias-

primas em produtos acabados. O SCM pode ser amplamente categorizado em cinco estágios, conhecidos como modelo SCOR:

a) Planejar: Uma estratégia é desenvolvida para abordar como o produto ou serviço da organização atenderá às necessidades dos clientes. A fase de planejamento também deve se concentrar na criação de uma cadeia de suprimentos ideal que seja eficiente e econômica;

b) Fonte: A organização identifica e estabelece fortes relacionamentos com fornecedores de matérias-primas necessárias na fabricação do produto final. Esta etapa envolve o planejamento de meios de transporte, entrega e pagamento, bem como a identificação de fornecedores confiáveis;

c) Fazer: Envolve a fabricação real do produto. Inclui testes, embalagem e programação do produto acabado para entrega;

d) Entregar: Nesta etapa, é executada a fase de logística. Os pedidos dos clientes são recebidos e o produto acabado é entregue aos clientes conforme solicitado;

e) Retorno: Esta etapa trata dos aspectos de atendimento ao cliente. Nesta fase, os clientes podem devolver produtos defeituosos e a organização trata das dúvidas e preocupações dos clientes.

Ao entender e implementar o modelo SCOR, as organizações podem otimizar o SCM, reduzir custos e melhorar a satisfação do cliente (Malik *et al.*, 2010).

2.2.3 Decisões da cadeia de fornecimento

O SCM envolve duas grandes categorias de decisões: operacionais e estratégicas. As decisões operacionais se concentram nas atividades do dia-a-dia e têm um escopo menor. Eles gerenciam de forma eficaz e eficiente o fluxo de produtos dentro da cadeia de suprimentos. Em contraste, as decisões estratégicas têm um escopo maior e requerem um horizonte de tempo mais longo. Eles lidam com estratégias de negócios e políticas diretas da cadeia de suprimentos em relação ao seu design. Segundo (Malik *et al.*, 2010), exitem quatro grandes áreas de decisão no SCM que abrangem decisões operacionais e estratégicas.

a) Localização: A seleção do local para instalações de fabricação, instalações de armazenamento e pontos de abastecimento são decisões primárias na criação de uma cadeia de suprimentos. Essas decisões determinam o melhor caminho para o fluxo do produto até os clientes finais e ajudam no desenvolvimento de táticas relacionadas a marketing, receita, custo e serviço. As decisões de localização otimizam os custos de produção,

impostos, direitos e devolução de direitos, tarifas, conteúdo local, custos de distribuição, limitações de produção, etc;

b) Produção: Essas decisões estratégicas envolvem a escolha de quais produtos produzir, em quais fábricas produzi-los, alocação de fornecedores para fábricas, fábricas para centros de distribuição e centros de distribuição para mercados de clientes. As decisões de produção têm impacto nas receitas, custos e atendimento ao cliente da empresa. As decisões operacionais se concentram na programação detalhada da produção, que inclui a construção de programas mestres de produção, programação da produção em máquinas e manutenção de equipamentos. Outras considerações incluem balanceamento de carga de trabalho e medidas de controle de qualidade em uma instalação de produção;

c) Inventário: Essas decisões lidam com o gerenciamento de estoques que existem em todas as etapas da cadeia de suprimentos como matéria-prima, produtos semi-acabados ou produtos acabados. O gerenciamento eficaz de estoques é de vital importância, pois manter estoques pode custar entre 20 a 40 por cento de seu valor;

d) Decisões de Transporte: As decisões de transporte estão intimamente ligadas às decisões de estoque, porque a melhor escolha de modo geralmente é encontrada ao negociar o custo de usar um determinado modo de transporte com o custo indireto de estoque associado a esse modo. As remessas aéreas podem ser rápidas, confiáveis e exigir estoques de segurança menores, mas são caras. O transporte marítimo ou ferroviário pode ser muito mais barato, mas exige a manutenção de quantidades relativamente grandes de estoque para amortecer a incerteza inerente a eles. Os níveis de atendimento ao cliente e a localização geográfica desempenham papéis vitais nessas decisões. Como o transporte representa mais de 30 por cento dos custos de logística, operar com eficiência faz sentido do ponto de vista econômico. O tamanho das remessas, a rota e a programação dos equipamentos são essenciais para o gerenciamento eficaz da estratégia de transporte da empresa.

2.2.4 Abordagens de modelagem da cadeia de suprimentos

No SCM, dois níveis de decisões requerem diferentes perspectivas, levando a duas áreas básicas de abordagens de modelagem. As decisões estratégicas têm abrangência global e envolvem diversos aspectos da cadeia de suprimentos, exigindo modelos de maior magnitude e volumes consideráveis de dados. Como resultado, esses modelos fornecem soluções aproximadas para as decisões descritas devido aos seus vastos requisitos de dados e amplo escopo. As decisões operacionais, por outro lado, abordam as operações do dia a dia da cadeia de suprimentos e exigem modelos muito específicos. Devido à sua perspectiva estreita,

esses modelos geralmente consideram grandes detalhes e fornecem soluções muito boas, se não ótimas, para decisões operacionais. Abordagens de modelagem podem ser categorizadas em duas áreas básicas:

Métodos de design de rede: Esses métodos fornecem modelos padrão para decisões mais estratégicas. Eles geralmente cobrem as quatro principais áreas de decisão descritas anteriormente e se concentram no aspecto de design da cadeia de suprimentos, incluindo o estabelecimento da rede e os fluxos associados. Esses métodos determinam a localização da produção, estoque, instalações de abastecimento e o caminho percorrido pelo produto através deles. Esses métodos geralmente são usados no início da cadeia de suprimentos e tendem a ser de grande escala. Os métodos baseados em design de rede agregam valor às empresas, estabelecendo estratégias futuras de fabricação e distribuição. É imperativo que as empresas tomem essas decisões integradas em algum momento, abrangendo produção, localização, estoque e transporte. No entanto, a revisão mostra que esses modelos têm um potencial considerável como direcionadores estratégicos no futuro, mas também apresentam deficiências. Sua própria natureza força esses problemas a serem de grande escala, tornando-os muitas vezes difíceis de resolver de maneira otimizada. Além disso, a maioria dos modelos nesta categoria são amplamente determinísticos e de natureza estática, e aqueles que consideram elementos estocásticos são muito restritivos. Em suma, ainda não parece haver um modelo abrangente que seja representativo da verdadeira natureza dos fluxos de materiais na cadeia de suprimentos.

Métodos de corte bruto: Este método lida com as decisões operacionais do SCM. Esses modelos normalmente assumem um único local de operação em uma rede e agregam a ele características da cadeia de suprimentos, como considerar o relacionamento do local com o restante da rede. Esses modelos formam a maior parte da literatura da cadeia de suprimentos e geralmente lidam com decisões mais operacionais. A maior parte da pesquisa integrativa (do contexto da cadeia de suprimentos) na literatura parece ter uma perspectiva de gerenciamento de estoque. De fato, o termo "Cadeia de Suprimentos", aparece pela primeira vez na literatura como uma abordagem de gerenciamento de estoque. O impulso dos modelos de corte bruto é o desenvolvimento de políticas de controle de estoque, considerando vários níveis ou escalões juntos. Esses modelos passaram a ser conhecidos como modelos de controle de estoque "multinível"(Malik *et al.*, 2010).

2.2.5 Problemas na gestão da cadeia de fornecimento

O principal objetivo do SCM é garantir o fluxo suave de informações relevantes e de alta qualidade que permitam aos fornecedores fornecer um fornecimento ininterrupto e precisamente cronometrado de materiais aos clientes. No entanto, flutuações de demanda imprevistas, bem como problemas no processo de execução da cadeia de suprimentos, podem criar problemas em toda a cadeia de suprimentos. Para alcançar um SCM bem-sucedido, é importante abordar as seguintes áreas problemáticas:

a) Configuração da rede de distribuição: este campo trata da determinação do número e localização apropriados de fornecedores, instalações de produção, centros de distribuição, armazéns e clientes potenciais;

b) Estratégias de distribuição: essas estratégias envolvem o caminho da remessa, o modo de transporte (incluindo carga de caminhão, ferrovia, frete marítimo ou frete aéreo) e controle de transporte, como transportadoras próprias, privadas ou contratadas;

c) Integração de informações: esta área envolve a integração de processos em toda a cadeia de suprimentos para compartilhar informações eficientes, incluindo demanda, previsões, estoque, transporte e colaboração potencial;

d) Gestão de estoque: este campo trata da localização e capacidade do estoque, incluindo matérias-primas, produtos semi-acabados e acabados;

e) Fluxo de caixa: esta área se concentra em organizar os métodos de pagamento para troca de fundos dentro da cadeia de suprimentos.

O conceito básico do SCM é que os clientes pedem produtos de uma organização, a organização acompanha o que está vendendo e encomenda matéria-prima suficiente de seus fornecedores para atender à demanda do cliente. No entanto, a falta de coordenação pode levar a problemas, pois cada grupo (fornecedores, fabricantes, departamento de vendas, clientes) pode influenciar toda a cadeia fazendo pedidos demais ou de menos. As decisões tomadas por cada grupo também afetam umas às outras. Essa falta de coordenação, combinada com a capacidade de influenciar e ser influenciado por outros, leva ao que é conhecido como "Efeito Chicote". Por exemplo, a decisão de um distribuidor de perseguir uma demanda altamente sazonal pode causar aumentos significativos de custos para seus parceiros *upstream* (fornecedores e outros participantes da cadeia envolvidos na disponibilização da matéria-prima).

Para minimizar o efeito chicote, é importante fornecer melhores informações (como melhor comunicação ao longo da cadeia de suprimentos ou melhores previsões) para aumentar a coordenação entre os grupos. Para conseguir isso, as organizações precisam estudar as necessidades potenciais do cliente, pois a demanda do cliente e o consumo de estoque acionam pedidos de reposição em vários pontos da cadeia de suprimentos. As organizações devem ter como objetivo eliminar atrasos ao longo da cadeia de suprimentos e reduzir o tempo de entrega do pedido, o que consequentemente reduzirá as flutuações da cadeia de suprimentos (Malik *et al.*, 2010).

2.2.6 Aplicações de SCM

Enterprise Resource Planning (ERP): ERP é um processo computadorizado que integra todas as funções e departamentos de uma organização em uma rede eficiente. Ao reduzir

custos e melhorar a qualidade do tempo de trabalho, o ERP aproveita ao máximo os avanços tecnológicos e aumenta a capacidade de resposta às consultas de entrega de produtos. A integração do ERP no SCM ajuda a superar problemas como o efeito chicote, tornando a organização mais coordenada e eficiente.

Tecnologia de Infraestrutura (TI): O SCM envolve o fluxo de produtos e informações entre vários departamentos para chegar ao cliente final. A tecnologia da informação permite que as organizações disponham de boas informações de maneira fácil e eficiente, ajudando a coordenar as atividades necessárias para gerenciar a cadeia de suprimentos. O custo da informação diminuiu consideravelmente com os desenvolvimentos no setor de TI. No desenvolvimento e manutenção dos sistemas de informação da cadeia de suprimentos, tanto o software quanto o hardware devem ser abordados. Hardware inclui dispositivos de entrada/saída de computador e mídia de armazenamento, enquanto software inclui todo o sistema e programas aplicativos usados para processar transações, controle de gerenciamento, tomada de decisão e planejamento estratégico. Futuras inovações estratégicas e tecnológicas na cadeia de suprimentos impactarão a forma como as organizações compram e vendem produtos. No entanto, uma visão clara, um planejamento forte e uma percepção técnica dos recursos da Internet são necessários para garantir que as empresas maximizem o potencial da Internet para um melhor SCM e, por fim, maior competitividade.

Armazenagem: Armazéns são instalações na cadeia de abastecimento onde as mercadorias são armazenadas. O armazenamento afeta os níveis de atendimento ao cliente, as taxas de falta de estoque, as vendas e o sucesso do marketing. Os armazéns atuam como uma ponte entre os membros a montante e a jusante da cadeia de abastecimento. As funções de armazenamento podem ser categorizadas em benefícios econômicos e benefícios de serviço. Os benefícios econômicos incluem consolidação, cross-docking, processamento/adiamento e estocagem. Os benefícios do serviço que podem ser alcançados por meio do armazenamento são localização de estoque, mistura de estoque, produção, suporte e presença no mercado.

Setor de varejo: o gerenciamento de cadeias de suprimentos exige que os varejistas realizem um delicado ato de equilíbrio que atenda simultaneamente a várias necessidades. Enquanto fornecem altos níveis de serviço enquanto gerenciam cadeias de suprimentos globais, os varejistas devem manter os custos baixos para permanecerem competitivos. Outras pressões vêm de consumidores mais exigentes, bem como da natureza cada vez mais global da indústria, que faz com que os varejistas comprem e vendam produtos em mais lugares ao redor do mundo.

Assistência médica: uma solução integrada de SCM para assistência médica permite custos de atendimento mais baixos, prazos de entrega mais curtos e melhora a capacidade de se concentrar na prestação de serviços em vez de processos administrativos. Atualmente, as organizações de saúde estão procurando oportunidades para melhorar a eficiência operacional e reduzir custos sem afetar negativamente o atendimento ao paciente. A criação de uma cadeia de suprimentos que conecte os funcionários da instalação médica, promova a colaboração e ofereça aos fornecedores visibilidade da demanda e do suprimento é essencial para reduzir os

custos gerais da cadeia de suprimentos. O SCM ajuda a reduzir os custos de aquisição, elimina erros e redundâncias de suprimentos, aumenta a eficiência na cadeia de suprimentos de saúde e reduz os prazos de entrega. Ele oferece suporte às políticas organizacionais ao permitir que os funcionários façam pedidos de suprimentos on-line, aumenta a colaboração e fortalece os relacionamentos com os principais fornecedores. O SCM também ajuda a reduzir custos por meio de uma tomada de decisão aprimorada sobre custos de produtos, prazos e escolha de fornecedores (Malik *et al.*, 2010).

2.2.7 Transparência

A globalização tornou possível a produção de diversos produtos em escala mundial, distribuindo as etapas produtivas que vão desde o processo inicial com o produtor na origem, manufatura, beneficiamentos, distribuição, até a entrega ao consumidor final. As cadeias de suprimentos podem ser vastas e conter diversas etapas com diferentes entidades desde o início até o final do ciclo produtivo, o que por um lado melhora o processo produtivo por envolver agentes especializados em cada área e conectar regiões antes não abrangidas, também pode incorrer em problemas de gerenciamento e rastreamento (Iftekhar *et al.*, 2020). Toda essa ramificação traz dificuldade em rastrear os produtos em tempo hábil, podendo resultar na disseminação de produtos contaminados no mercado, além de problemas na identificação dos itens afetados, forçando muitas vezes o produtor a recolher uma quantidade muito maior de produtos do que deveria, além de poder manchar sua reputação (Adamashvili *et al.*, 2021).

Outro fator bastante preocupante em muitas cadeias de suprimentos está relacionada com a falsificação de produtos, trazendo prejuízos tanto aos envolvidos no processo produtivo, quanto aos clientes que acabam lesados e enganados. Além disso, algumas dessas práticas podem trazer risco à segurança alimentar e à saúde pública, como a adulteração de documentos, erros de impressão de ingredientes, temperaturas de armazenamento inadequadas e produtos fora de sua validade. Essas práticas de fraude alimentar refere-se a um grupo de atividades realizadas intencionalmente ou para ganho econômico (Iftekhar *et al.*, 2020).

Segundo (Berman, 2008), existem quatro tipos diferentes de produtos falsificados:

a) Uma cópia barata de baixa qualidade, com embalagem diferente da tradicional, adquiridos de um canal de distribuição incomum por consumidores cientes da falsificação;

b) Produtos genuínos que sofrem engenharia reversa por meio de plantas roubadas ou copiadas, onde o consumidor desconhece da falsificação do produto;

c) Produtos falsificados produzidos por um fornecedor terceirizado sem autorização do fabricante ou de conhecimento do cliente;

d) Produtos produzidos por fornecedores terceirizados que não atende aos padrões do fabricante e não foram destruídos.

As marcas utilizam diversas tecnologias para identificar e prevenir a falsificação, sendo essas tecnologias anti-falsificação baseadas em quatro atributos: dificuldade de duplicação, fácil identificação, visibilidade sem equipamentos especiais e complexidade de utilização. Podendo essas tecnologias ser abertas ou ocultas (Boissieu *et al.*, 2021).

Uma tecnologia aberta, como marcas de água, tinta que muda de cor, fios de segurança e numeração sequencial de produtos que são visíveis, simplifica a autenticação. Sendo técnicas usuais em embalagens anti-falsificação e podendo ser integradas ao produto. De outro modo, uma tecnologia oculta, como papéis de embalagem de segurança, tinta ou impressão, tinta UV, tinta termocrômica, marcas de água e marcadores biológicos e químicos são ocultos e visíveis apenas para administradores autorizados (Boissieu *et al.*, 2021).

O comércio global permitiu ainda o uso de tecnologias digitais, como RFID, códigos de barras e ferramentas *web*. Uma etiqueta RFID, por exemplo, pode ser fixada na embalagem de um produto e transmite um sinal para o centro de sistemas de informação da empresa, ajudando a localizá-lo (Boissieu *et al.*, 2021). Segundo (Biswas, 2017), o sistema de RFID é utilizado na maioria dos sistemas de rastreabilidade da cadeia de abastecimento de vinhos com o código de barras, responsável pelo armazenamento das informações em diferentes fases da cadeia de suprimentos. Essas informações são recuperadas manualmente e armazenadas em um banco de dados central. Por fim, uma interface *web* ou móvel é desenvolvida para exibir as informações aos usuários finais. Umas das principais preocupações nos sistemas de rastreabilidade existentes é a autenticidade da informação de origem, uma vez que é fácil reproduzir ou falsificar a informação a qualquer momento. Sendo assim, esses códigos de segurança amplamente utilizados não podem impedir a falsificação, limitando sua aplicação (Boissieu *et al.*, 2021).

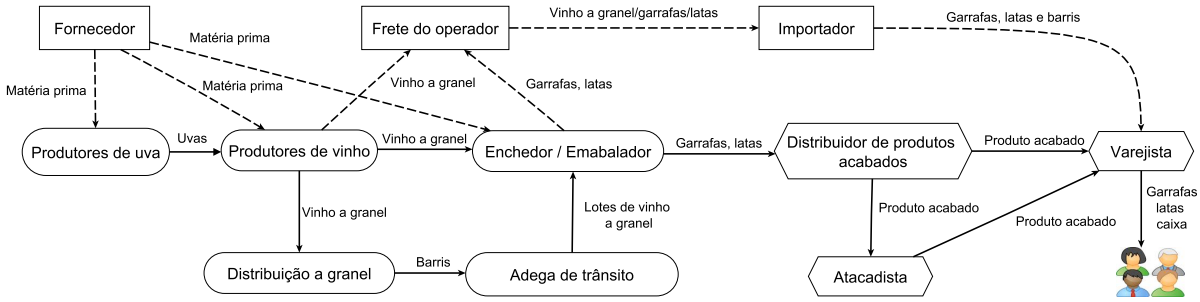
2.2.8 Cadeia de suprimentos do vinho

O vinho é um dos produtos alimentares mais falsificados, onde à falsificação pode surgir depois que uma empresa vende uma garrafa em que assume rótulos falsos ou reabastecendo com vinhos mais baratos. O caso de fraude envolvendo a Côtes du Rhône na França é um bom exemplo. Ele foi descoberto por órgão antifraude francês onde um comerciante tentou vender mais de 48 milhões de litros de vinhos falsificados como Côtes du Rhône (Danese, 2021).

Ameaças de perda de receita, imagem e confiança do cliente levaram os produtores de vinho a escolher outras medidas anti-falsificação e, em alguns casos pioneiros, a lançar projetos pilotos de *Blockchain*, buscando resolver esses problemas e garantir a qualidade dos produtos. Sendo necessário garantir a procedência do produto e a conformidade com as especificações de processo, essenciais a intermediários — como importadores de vinho, distribuidores, revendedores, dentre outras entidades envolvidas — visto que esses produtos falsificados encontrados por cliente então entre as principais causas de danos a reputação das empresas (Danese, 2021).

No trabalho realizado por (Biswas, 2017), são identificadas e apresentadas as principais entidades da cadeia de abastecimento de vinho em um modelo genérico simplificado, a saída gerada por cada entidade também é mostrada na Figura 9, a seguir:

Figura 9 – Entidades na cadeia de suprimentos de vinhos.



Fonte: Adaptação de (Biswas, 2017).

Produtores de uva

Os viticultores são uma das principais partes na cadeia de abastecimento do vinho, dado que a cadeia de abastecimento começa com eles nas vinhas. Eles estão realizando todo o cuidado das plantas e monitorando seus parâmetros de crescimento, como temperatura, umidade do solo e fertilidade. Além disso, são responsáveis por colher as uvas e entregá-las à adega. Nessa etapa os registros que devem ser mantidos na cadeia são: localização, altitude, categorias de videiras, origem, irrigação, tratamentos e data de poda ou depuração.

Produtores de vinho

Os produtores de vinho recebem as uvas e realizam uma série de procedimentos e operações para produzir vinhos a partir delas. Para garantir a rastreabilidade, devem ser mantidos na cadeia os registros dos processos e das matérias-primas utilizadas na produção. Inclui detalhes dos fornecedores, data de recebimento, descrição dos produtos recebidos, variedade de uvas, registros de procedimentos internos (como: decantação, fermentação e conservação), conteúdo químico, registros de distribuidores e aditivos(se houver). Nesta fase o vinho pode ser enviado a 3 locais diferentes: sendo, i) distribuidor de vinhos a granel, ii) um enchimento ou embalador e iii) outra adega produtora de vinho para loteamento.

Distribuidor a granel

O distribuidor a granel é responsável por receber o vinho a granel dos produtores de vinho e misturar e expedir os lotes de vinho para a adega de trânsito ou embalador. As informações que devem ser registradas nesta etapa são a data de recebimento, detalhes de

armazenamento, processamento, amostragem, análise do vinho a granel e data de expedição. Caso o distribuidor a granel realize o processo de blendagem, essa informação precisa ser registrada.

Adega de trânsito

O papel da adega de trânsito é quase semelhante ao dos distribuidores a granel, pois enviam lotes de vinho a granel para enchimento ou empacotador. Sendo responsável pela recepção, armazenamento, expedição, processamento, amostragem e análise do vinho a granel.

Enchedor/Embalador

Nessa etapa, recebe-se o vinho a granel da adega de trânsito ou distribuidor a granel e enche em diferentes recipientes, como garrafas, sacos ou barris. A identificação e rotulagem é realizada nesta fase, é muito importante garantir a consistência das informações rotuladas com os registros armazenados na e do produto físico correspondente. Essas informações incluem a recepção, armazenamento, processamento, amostragem, análise, enchimento, embalagem e expedição dos produtos acabados.

Distribuidor de produtos acabados

Os paletes e caixas recebidos pelo distribuidor do produto acabado são despachados para o atacadista ou varejista. As responsabilidades do distribuidor de produtos acabados são receber, armazenar, despachar e gerenciar o estoque de produtos acabados. Caso seja necessário reembalar ou rotular novamente, os detalhes devem ser armazenados na *Blockchain*.

Atacadista

O atacadista recebe paletes e caixas de vinho do distribuidor de produtos acabados e os despacha para as lojas de varejo. Nessa etapa, são responsáveis pelo recebimento, armazenamento e entrega das mercadorias.

Varejista

O varejista recebe produtos acabados na forma de garrafas, latas e caixas do atacadista ou distribuidor de produtos acabados e os vende aos consumidores finais. Quando uma garrafa ou caixa é vendida, as informações devem ser registradas no *Blockchain* para não ser possível

reutilizar o rótulo. Os varejistas são responsáveis por manter os detalhes dos itens recebidos, armazenamento e informações de venda. Ao armazenar as informações na *Blockchain*, o consumidor poderá ver a proveniência do vinho adquirido inserindo o número de identificação no site.

Outras entidades

Além das entidades acima referidas, existem ainda outros elementos na cadeia de abastecimento que não estão diretamente relacionadas com a produção ou transformação do vinho. São eles: fornecedores de matéria-prima, operadores de carga e importadores. A Figura 9, apresenta as transações entre as entidades da cadeia de abastecimento do vinho.

2.3 *Blockchain* na cadeia de suprimentos

As empresas de hoje enfrentam uma necessidade crítica de transparência na cadeia de suprimentos devido ao aumento da pressão regulatória sobre a fabricação para garantir a qualidade do produto e entender melhor suas fontes de suprimento. Ao mapear a rede da cadeia de suprimentos, as partes interessadas em todas as etapas podem identificar, mapear ou fornecer informações transparentes e precisas, garantindo o cumprimento dos requisitos de segurança, precisão, sustentabilidade e responsabilidade social (Mann *et al.*, 2018).

A tecnologia *blockchain* tem o potencial de reduzir significativamente os custos e as complicações da negociação, permitindo transparência entre os associados e reduzindo fraudes, processos de remessa, tempo de trânsito, desperdício e orçamento (Mann *et al.*, 2018). No contexto da cadeia de suprimentos, (Tse *et al.*, 2017), apresenta um modelo descentralizado de autenticação na cadeia de suprimentos, na qual apresenta as principais diferenças entre o modelo tradicional e o modelo descentralizado. Por sua vez, (Abeyratne; Monfared, 2016) enfatizam que a transparência e a rastreabilidade da cadeia de suprimentos estão se tornando cada vez mais importantes na indústria de manufatura, dada a crescente complexidade das cadeias de suprimentos globais. Eles propuseram um sistema distribuído descentralizado por meio da tecnologia *blockchain* para coletar, armazenar e gerenciar valores do ciclo de vida do produto e criar registros seguros e compartilhados de produtos.

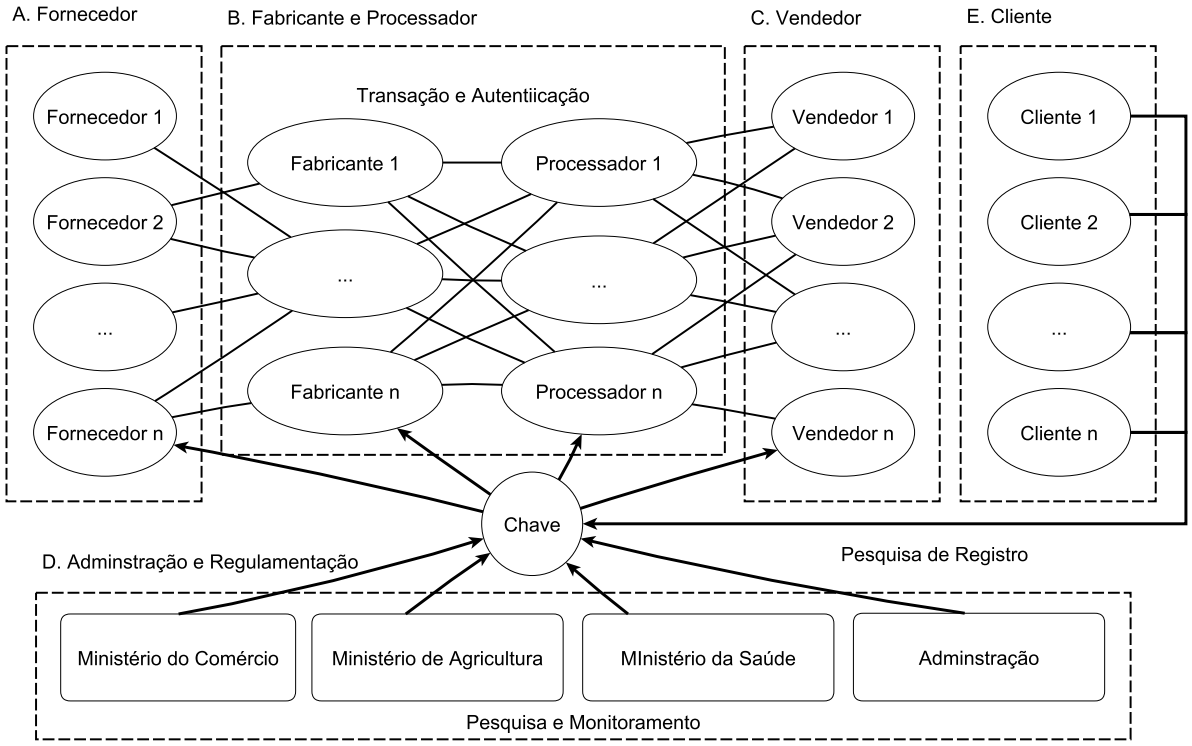
No entanto, implementar a tecnologia *blockchain* pode ser um desafio. Constando, (Abeyratne; Monfared, 2016) e (Banerjee, 2018) que essa tecnologia requer infraestrutura de tecnologia de informação específica e a capacidade de desempenho pode ser um gargalo. Enquanto em um estudo realizado por (Tse *et al.*, 2017) apresenta o conceito de tecnologia *blockchain* e seu uso potencial na segurança da informação da cadeia de suprimentos, chegando a conclusão que *blockchain* é uma tecnologia que pode auxiliar no rastreamento, monitoramento e auditoria de toda a cadeia de suprimentos, além de ajudar os fabricantes a registrar as

transações com autenticidade entre os clientes, fabricantes, departamentos de supervisão, e a melhorar a eficiência do processo durante a circulação de produto.

2.3.1 Diferenças entre modelos tradicionais e descentralizados

Um estudo realizado por (Tse *et al.*, 2017), apresenta um modelo descentralizado de autenticação na cadeia de suprimentos, onde seriam transferidos para o armazenamento na *blockchain*, informações de circulação de alimentos como a categoria, quantidade, qualidade, origem, entre outros. Sendo todas as transações registradas transparentes e abertas, para poder realizar pesquisas e visualização, enquanto que todos os nós podem rastrear informações de alimentos para onde foram transportados ou de onde vieram, ajudando todas as instituições a melhorar a gestão da rastreabilidade para a segurança alimentar.

Figura 10 – Modelo de cadeia de suprimentos descentralizada.

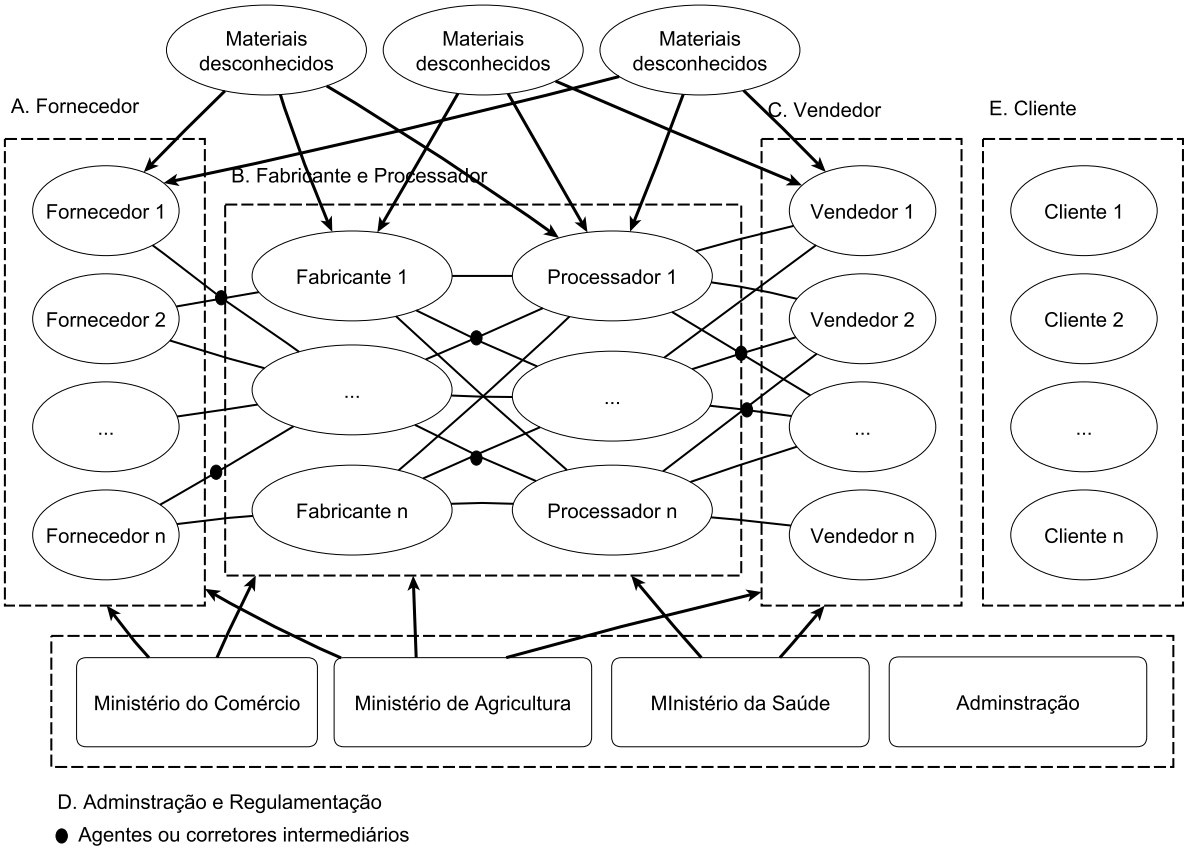


Fonte: Adaptação de (Tse *et al.*, 2017).

Como mostra a Figura 10, todas as elipses nas células das partes A, B e C atuam como o nó da raiz principal do *blockchain* que inclui os fornecedores de matérias-primas de alimentos, vendedores e outras empresas relevantes da indústria de alimentos (Tse *et al.*, 2017).

A linha completa entre essas elipses representam as transações entre esses nós diretamente, não mais através de agentes ou corretores. A Figura 11 apresenta o modelo de cadeia de suprimentos tradicional, com os agentes ou corretores.

Figura 11 – Modelo de cadeia de suprimentos tradicional.

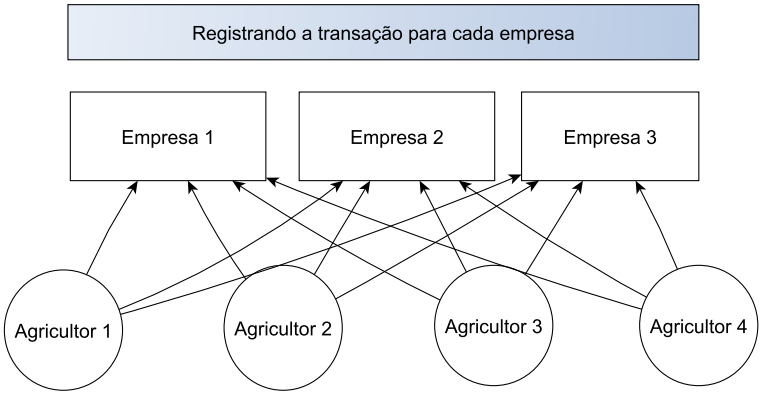


Fonte: Adaptação de (Tse *et al.*, 2017).

Quando uma transação aconteceu entre dois nós, o restante dos nós atuaram como institutos de identificação para verificar a autenticidade dessa transação e encontrar o registro da transação anterior usando a cópia do *blockchain* atualizada do *blockchain* principal. Nas elipses pertencentes a caixa pontilhada A atuam como criadora inicial de blocos, o que significa que todos os recursos que fluem para a rede *blockchain* são registrados primeiro nos fornecedores. Que atuam como fonte de toda a cadeia de suprimentos, que reuniu e adquiriu as matérias-primas necessárias dos agricultores ou dos indivíduos e registra as informações básicas desses materiais para criar os blocos iniciais para posterior transação e uso, como representado na Figura 12, (Tse *et al.*, 2017).

A parte E da Figura 10, representa o Departamento de Informações, que aloca a chave privada e pública para as A, B e C. O restante das instituições, parte D, pode realizar pesquisas na plataforma como uma plataforma de compartilhamento de informações. As setas indicam que as instituições têm uma conexão de mão única com as partes A, B e C. Sendo sua responsabilidade buscar todos os registros de transporte e monitorar fluxos de alimentos, caso necessário. Além disso, não possuem autoridade para modificar qualquer parte do registro na *Blockchain* (Tse *et al.*, 2017).

Figura 12 – Modelo da célula da parte A.



Fonte: Adaptação de (Tse *et al.*, 2017).

Outra responsabilidade da instituição de segurança alimentar é uma agência entre a rede *blockchain* e o cliente. Se o cliente quiser pesquisar as informações básicas do fluxo de alimentos, a instituição pode admitir parte da autoridade para realizar a solicitação do cliente, pelo fato de ser proprietário do par de chaves na *blockchain*. As elipses na parte E são clientes, sendo as setas representando o fato de poderem buscar informações de alimentos e dados de transporte através da parte D, sendo a instituição de segurança alimentar (Tse *et al.*, 2017).

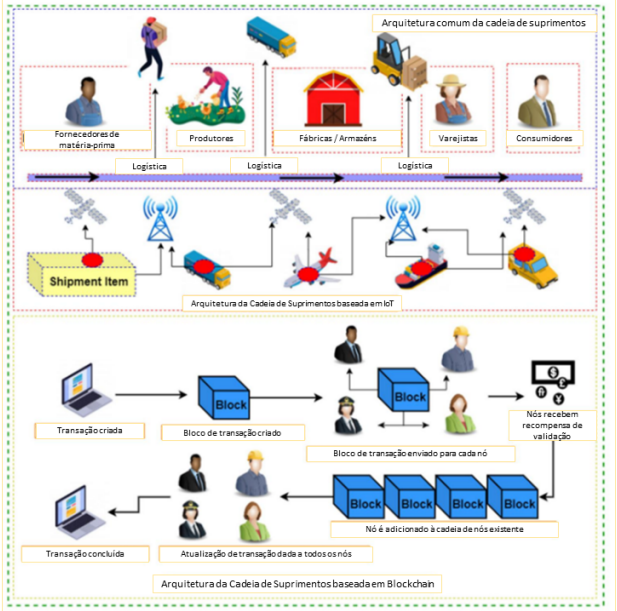
2.3.2 Proposta de SCM usando IoT e *Blockchain*

O SCM é um aspecto crítico de qualquer negócio, mas os métodos tradicionais de SCM são ineficientes, lentos e não atendem às necessidades das empresas modernas. Para resolver esses problemas, (Bhutta; Ahmad, 2021) propõem uma estrutura SCM confiável, auditável e rastreável que garante a integridade, imutabilidade e transparência da transação em todo o processo de remessa de produtos perecíveis.

O sistema SCM baseado em *blockchain* usa tecnologias IoT e *blockchain* para alcançar a entrega ideal e segura de itens. O sistema fornece uma representação digital coerente de ativos valiosos para todas as partes interessadas, desde fornecedores de matérias-primas até usuários finais ou consumidores. Cada parte interessada ingressa como um nó *blockchain* para fazer transações e participar da atualização do *blockchain*. Para garantir a segurança, cada nó recebe um par de chaves público/privado para operações criptográficas seguras de acordo com a arquitetura *blockchain*.

A Figura 13 mostra a estrutura conceitual do sistema SCM proposto. O sistema usa tecnologias IoT e *blockchain* para garantir que o mecanismo SCM seja seguro e confiável. Em um sistema SCM convencional, os fornecedores de matérias-primas fornecem materiais básicos para fabricantes como fábricas, fazendas agrícolas e outras indústrias. Esses fabricantes então fabricam produtos e os despacham usando procedimentos logísticos tradicionais. As partes

Figura 13 – Estrutura conceitual de SCM adotando as tecnologias de IoT e *blockchain*.



Fonte: Adaptação de (Bhutta; Ahmad, 2021).

interessadas terceirizadas armazenam os produtos em armazéns e, em seguida, os fornecem a varejistas ou mercados de compras onde os consumidores os compram.

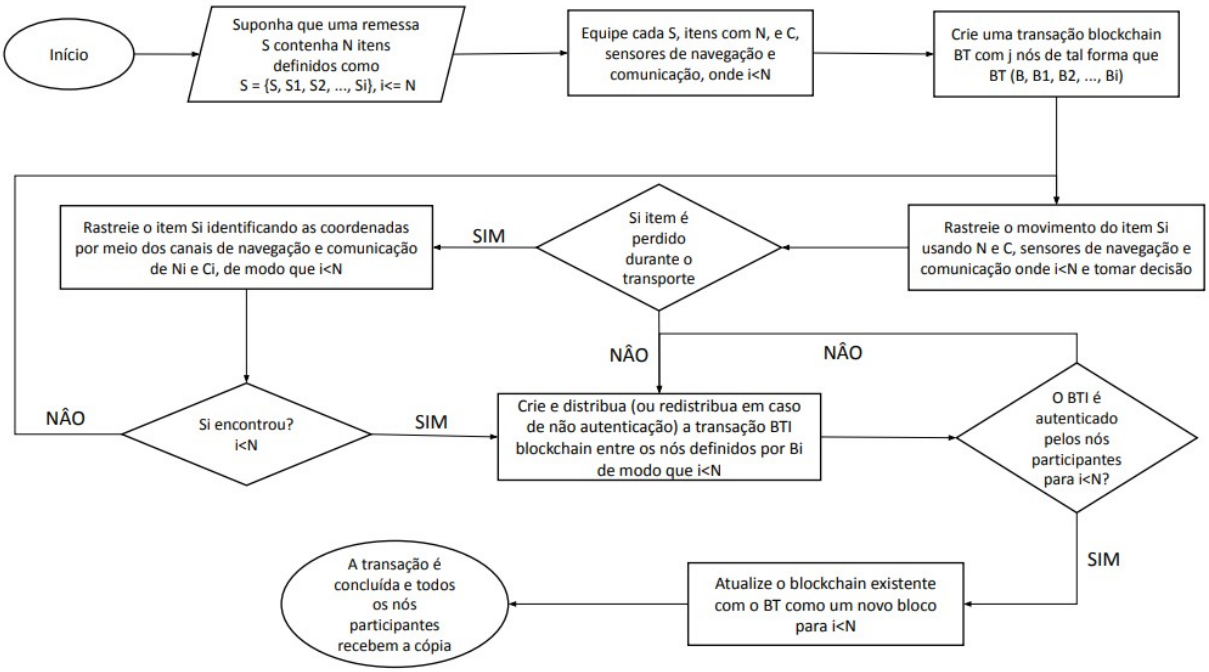
No entanto, todo o mecanismo SCM envolvido no antigo sistema de fornecimento produtor-consumidor carece de aspectos fundamentais de segurança, confiança, confiabilidade e integridade. É aqui que entra o sistema SCM proposto. Ao alavancar as tecnologias IoT e *blockchain*, o sistema pode garantir que todo o mecanismo SCM seja seguro, confiável e transparente.

Cada remessa de itens é registrada e controlada digitalmente com uma etiqueta de identificação digital exclusiva equipada com sensores de navegação e comunicação para rastrear e rastrear itens durante toda a entrega. O sistema pode rastrear a localização de itens perdidos ou danificados usando GPS e notificar os representantes locais com as localizações exatas. Scanners de código digital instalados em armazéns e pontos de embarque notificam o aplicativo sobre o status atualizado dos itens durante o processo de embarque.

O sistema SCM proposto integra uma estrutura baseada em *blockchain* para garantir o controle de qualidade e o compartilhamento abrangente de informações de transações digitais entre as partes interessadas do SCM de maneira segura. O sistema fornece um livro-razão distribuído seguro com inúmeras informações de qualidade, informações de remessa e informações de transação. O registro distribuído capacita o sistema para proteção aprimorada da privacidade por meio de contratos inteligentes. Recomendamos o uso de *Proof of Supply Chain Share* (PoSCS) como um mecanismo de consenso para adicionar novos blocos ao *blockchain* existente.

A estrutura SCM proposta é dividida em três camadas para melhor organização. A primeira camada é equipada com sensores que coletam dados em tempo real em um nível baixo.

Figura 14 – O quadro metodológico proposto de SCM.



Fonte: Adaptação de (Bhutta; Ahmad, 2021).

A segunda camada envolve o livro-razão digital que contém as informações de transação mais recentes e acordadas no contexto de atributos de dados, qualidade, logística e informações de transação relevantes. A terceira camada garante a privacidade e segurança das transações individuais, com contratos digitais assinados e distribuídos entre todos os nós da rede definida. Diferentes partes interessadas que participam de todo o processo residem na camada superior, encapsulando todas as três camadas.

A Figura 14 apresenta o arcabouço metodológico proposto para o SCM. A estrutura envolve uma sequência estruturada de etapas para o envio de itens e descrições de transações:

a) Cada remessa de itens de uma parte interessada para outra (no processo da cadeia de suprimentos) requer uma descrição padrão dos itens. Seja S a remessa contendo N itens definidos como S = S1, S2, S3, . . . , SN. Os itens individuais são produtos que devem ser entregues do ponto A ao ponto B;

b) Para preservar a originalidade de cada item e evitar perdas ou danos durante o transporte, a arquitetura SCM proposta equipa cada item Si com sensores dedicados de navegação e comunicação, Ni e Ci respectivamente (para i < N). Esses sensores ajudam a rastrear o curso da remessa e rastrear os itens específicos em caso de perda ou dano;

c) O sistema SCM proposto fornece uma representação digital de transações individuais por meio de um livro-razão digital. O registro contém informações sobre qualidade,

informações sobre transações, informações sobre as partes interessadas e outras informações relevantes. O sistema cria uma transação *blockchain*, BT, com j nós tais que BT = B1, B2, B3, . . . , Bj. Cada Bi representa um bloco de transação individual que hospeda as informações da estrutura de dados. Todas as partes interessadas relevantes devem autenticar cada Bi uma vez criado;

d) O sistema rastreia cada item de remessa Si empregando canais de navegação e comunicação Ni e Ci definidos (para i < N) e toma decisões relevantes com base no rastreamento. Se o item Si for perdido durante o transporte, o sistema notifica o item perdido e rastreia sua localização através dos sensores;

e) As coordenadas de localização dos itens Si são identificadas por meio de Ni e Ci (para i < N);

f) O sistema cria e distribui (ou redistribui em caso de não autenticação) transação *blockchain* BTi entre nós definidos por Bi de modo que i < N. Todos os nós participantes na rede devem autenticar a transação BTi flutuante;

g) Quando os nós autenticam a transação, o bloco de transação relevante é anexado ao *blockchain* existente (ou seja, BTi é inserido como um novo bloco para i < N);

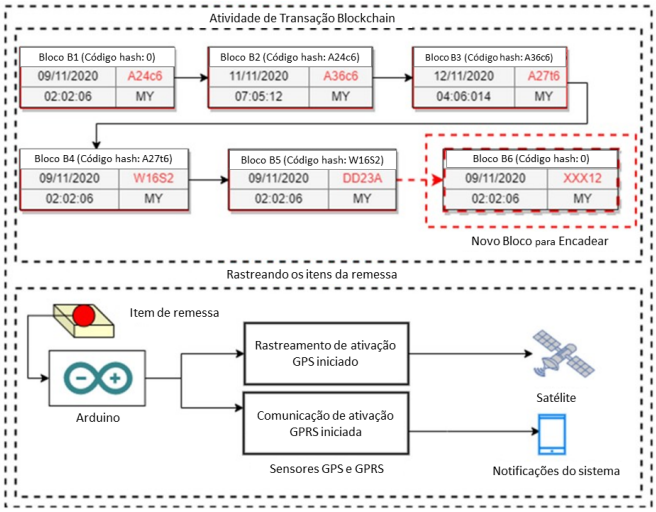
h) Finalmente, o sistema notifica a conclusão bem-sucedida da transação e encaminha a cópia das informações da transação acordada para todos os nós da rede.

O sistema SCM proposto oferece várias vantagens, incluindo a unanimidade acordada da maioria dos pares na rede *blockchain*, que é invariante por natureza e retrata total transparência. Além disso, ao contrário do armazenamento centralizado de arquivos de log que exigem que as partes interessadas estejam conectadas ao armazenamento centralizado, a conectividade de nível de par no caso de *blockchain* torna suficiente para dispositivos de detecção serem conectados em redes de pares para rastreabilidade eficiente e confiável de itens SCM. A arquitetura de *blockchain* SCM proposta aborda questões e desafios significativos dos mecanismos contemporâneos de SCM.

O sistema de SCM proposto oferece uma representação digital de transações individuais, criando um livro-razão digital que contém informações sobre qualidade, detalhes da transação, informações das partes interessadas e outros dados relevantes. Nesse sistema, cada remessa de itens é registrada e monitorada digitalmente, e cada item de remessa recebe uma etiqueta de identificação digital exclusiva, equipada com sensores de navegação e comunicação para rastrear os itens durante o processo de entrega.

A Figura 15 representa a estrutura de experimentação do sistema SCM proposto. No nível de implementação, é criada uma estrutura de dados representando os nós, com cada nó contendo informações da transação, incluindo número de identificação do bloco, código hash ou endereço do próximo bloco da transação na cadeia, informações de qualidade, data e hora,

Figura 15 – Estrutura de experimentação do SCM proposto.



Fonte: Adaptação de (Bhutta; Ahmad, 2021).

Tabela 2 – Envio de itens usando *Blockchain*.

Item ID	Bloco ID	Código Hash	Blocos apontando para o hash dos próximos blocos	Lista Estruturada
I1	B1	BT22D	2AXB9	B1
I2	B2	2AXB9	7CTT4	B1 → B2
I3	B3	7CTT4	JO76A	B1 → B2 → B3
I4	B4	JO76A	MH2T	B1 → B2 → B3 → B4
I5	B5	MH2T	B2B3S	B1 → B2 → B3 → B4 → B5
I6	B6	B2B3S	D25Y1	B → B6
I7	B7	D25Y1	AA7N2	B → B6 → B7
I8	B8	AA7N2	41FE9	B → B6 → B7 → B8
I9	B9	41FE9	SS2W1	B → B6 → B7 → B8 → B9
I10	B10	SS2W1	0	B → B6 → B7 → B8 → B9 → B10

Fonte: (Bhutta; Ahmad, 2021).

e outras diversas dados exigidos por todas as partes envolvidas no ciclo da cadeia de abastecimento. Por exemplo, o primeiro nó de estrutura (B1) aponta para o segundo nó de transação (B2). Quando um novo nó (B3) é criado, B2 adota o endereço hash de B3 e aponta para ele. Suponha que B6 seja o último nó da lista; nesse caso, ele possuirá um endereço de hash, mas não conterá o endereço de hash do próximo nó, pois a lista não contém o próximo nó. O bloco B6 apontará para o novo bloco B7 quando o sistema o criar, de comum acordo entre todos os envolvidos na cadeia.

Para rastrear os itens nesta remessa, sensores *Global Positioning System* (GPS) e *General Packet Radio Service* (GPRS) são instalados nos itens. As coordenadas de localização do item da remessa são registradas e, em caso de perda do item, o rastreador localiza a última localização do item e ajuda as unidades relevantes a rastrear o item perdido.

A Tabela 2 descreve o cenário de implementação das transações *blockchain*. Os itens de remessa recebem números de identificação, com cada item de remessa associado a um

número de identificação de bloco exclusivo. O ponteiro do código hash da estrutura de dados do bloco B1 aponta para o endereço hash do segundo bloco (B2). Da mesma forma, o ponteiro do bloco B2 aponta para o código hash do bloco B3 e assim por diante. O último bloco no conjunto de blocos não aponta para nenhum próximo bloco. Cada bloco é adicionado à lista existente de blocos assim que todas as partes interessadas autenticam e aprovam a transação específica. Uma vez acordado, o novo bloco é vinculado à lista vigente.

3 ARQUITETURA E IMPLEMENTAÇÃO

Nesse capítulo são descritos os materiais, coleta e tratamento dos dados, arquitetura e principais funções utilizadas.

3.1 Materiais

Os materiais utilizados para concepção desse foram, englobam ferramentas de desenvolvimento, tecnologias de programação, ferramentas de contêineres e a tecnologia *blockchain*.

Ferramentas de desenvolvimento:

a) Git: Sistema de controle de versão para rastrear alterações no código fonte;

b) Visual Studio Code: Ambiente de desenvolvimento integrado para diversas linguagens de programação;

c) WSL (Windows Subsystem for Linux): Ambiente de virtualização Linux no Windows;

d) Notebook Acer Nitro 5: Hardware utilizado para o desenvolvimento do projeto.

Tecnologias de programação:

a) JavaScript: Linguagem de programação utilizada no desenvolvimento, tanto no lado do cliente quanto no lado do servidor;

b) Node.js: Ambiente de execução para JavaScript no lado do servidor, utilizado para criar aplicativos web escaláveis.

Ferramentas de conteiners:

a) Docker: Plataforma para criação, implantação e execução de aplicativos em contêineres;

b) Docker Compose: Ferramenta para definir e executar aplicativos Docker multicontêiner por meio de um arquivo YAML.

Tecnologia:

a) Hyperledger Fabric 2.5: Estrutura de blockchain de código aberto projetada para aplicativos empresariais.

3.2 Arquitetura

Desenvolvimento da Aplicação baseada em Hyperledger

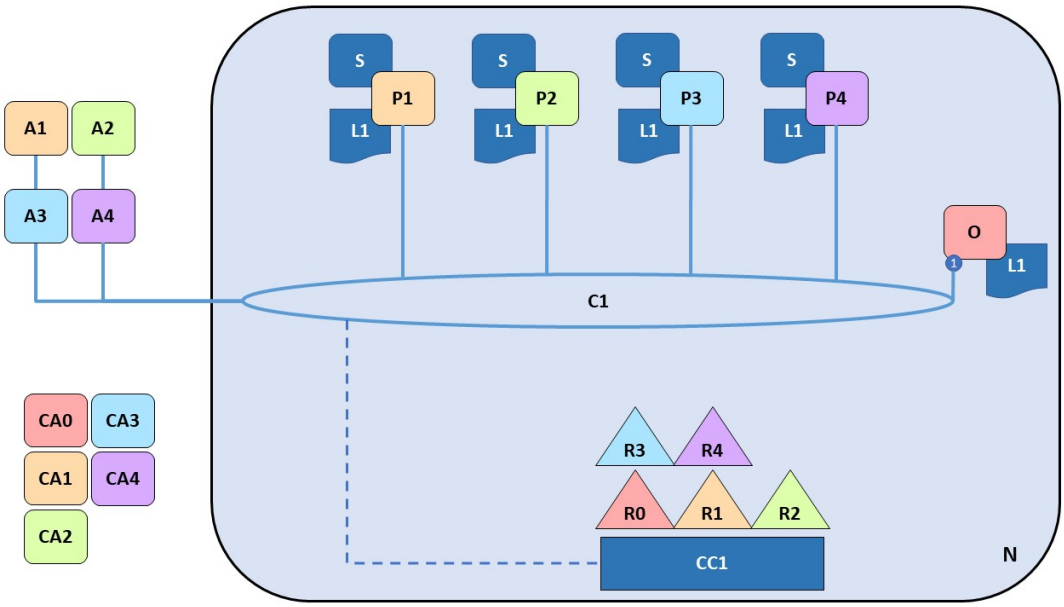
O desenvolvimento da aplicação *Blockchain* baseado no framework Hyperledger Fabric para a cadeia de suprimentos de vinho tem como base o estudo realizado por (Biswas, 2017), em que, foram descritas as etapas necessárias a serem consideram na cadeia e apresentado um modelo genérico sobre sua implementação, conforme demonstrado na Figura 9.

Na arquitetura citada como base, é utilizado o framework Multichain para demonstrar sua implementação, não dando detalhes de sua escolha de plataforma ou realizando comparativo com outras soluções. Na seção do artigo: “detalhes de implementação”, o autor apresenta imagens de captura de tela do *framework* demonstrando os resultados após as etapas serem realizadas, mas também não foi apresentado código-fonte utilizado no trabalho.

Compreendida a arquitetura proposta pelo autor, as entidades envolvidas e as etapas necessárias, é realizado o desenvolvimento de uma aplicação baseada em Hyperledger Fabric, modelando a arquitetura, conforme necessidades da aplicação, posteriormente, realizando a implementação, a realização de testes de funcionamento e coleta de dados.

Na Figura 16, apresenta o estado final da rede. Essa arquitetura implementa a rede *blockchain* sendo regida por políticas acordadas pelas organizações que formam a rede.

Figura 16 – Arquitetura de Rede.



Fonte: Autoria propria.

Quatro organizações, R1, R2, R3 e R4, juntamente com o serviço de pedido do canal, R0, concordam em estabelecer uma rede, N. Esta rede possui uma configuração CC1, com a qual todas as organizações concordam e que lista a definição das organizações, bem como as políticas que definem os papéis que cada organização desempenhará no canal.

Neste canal, R1, R2, R3 e R4 unem pares, denominados P1, P2, P3 e P4, ao canal C1, enquanto R0 possui O, o serviço de pedido do canal. Todos esses nós contêm uma cópia do razão (L1) do canal, onde as transações são registradas e o *chaincode* (S) instalado, embora as organizações não sejam obrigadas a instalar todos os *chaincodes*. R1, R2, R3, R4 e R0 também interagem com o canal através dos aplicativos A1, A2, A3 e A4, de sua propriedade. Todas as cinco organizações, mais o serviço de pedido, possuem uma Autoridade de Certificação (CA) que gera os certificados necessários para os nós, administradores, definições de organizações e aplicativos de sua organização. Em relação aos principais funções do *chaincode*, estão descritos no Apêndice B.

Coleta e tratamento de dados

3.3 Membros da Rede

Na Seção 2.2.8, o trabalho de (Biswas, 2017) apresenta em detalhes as principais entidades na cadeia de suprimentos de vinho, como viticultor, produtor de vinho, distribuidor a granel, enchedor/embalador, atacadista e varejista. No entanto, para simplificar o modelo, o autor reduz as entidades a viticultor, produtor de vinho, distribuidor a granel, enchedor/embalador e varejista, designando os produtores de vinho, distribuidores a granel e enchedores/embaladores como validadores.

Assim, os membros definidos na rede estão organizados da seguinte forma: os dados relacionados ao Viticultor, Produtor de Vinho e Enchedor/Embalador, estarão englobadas pelo Produtor de Vinho, assim, considerando a situação do Produtor receber uvas de mais de um Viticultor, e também, que o Produtor de Vinho muitas vezes realiza o engarrafamento e embalagem dos vinhos. Posteriormente, teremos o Distribuidor, Atacadista e o Varejista.

Nesse cenário, temos: Produtor de Vinho, Distribuidor, Atacadista e Varejista, definidos como entidades(nós) e validadores, sendo o Produtor de Vinho, sendo a entidade responsável por fazer a leitura do histórico da cadeia de suprimentos. A Figura 17 representa o fluxo de dados entre as diferentes entidades (nós) na cadeia, indicando a conexão com a rede e os validadores correspondentes.

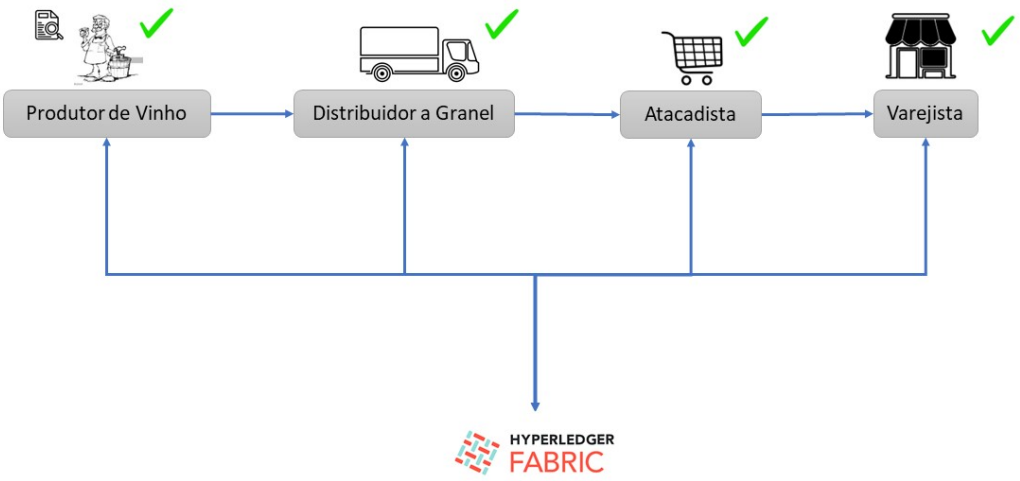
Cada nó irá conter informações referente a sua etapa. De acordo com (Guideline, 2008), as informações em cada etapa incluem:

Produtor de vinho: coleta as informações da colheita das uvas com o viticultor, transforma as uvas em vinho, enche e embala o vinho em garrafas e fornece informações sobre o processo. Os seguintes campos são preenchidos:

a) Viticultor:

    a) NomeViticultor: João da Silva

Figura 17 – Fluxo de dados entre entidades e sua conexão com a rede.



Fonte: Adaptação de (Biswas, 2017).

b) EnderecoViticultor: Fazenda Silva, Vinhedo, SP

c) VariedadeUva: Cabernet Sauvignon

d) DataColheita: 2023-09-15

b) NomeProdutorVinho: Vinhos do Vale

c) EnderecoProdutorVinho: Estrada do Vinho, 456, Vinhedo, SP

d) Lote: A123

e) IDRemessa: PV2023-001

f) DataEmbarque: 2023-10-01

g) HoraEmbarque: 14:30

Distribuidor: transporta o vinho do produtor de vinho para o atacadista. Os seguintes campos são preenchidos:

a) NomeProdutorDistribuidor: Distribuidora Vinífera

b) EnderecoProdutorDistribuidor: Av. dos Vinhos, 789, Distribuicidade, SP

c) Lote: A123

d) IDRemessa: DV2023-001

e) DataEmbarque: 2023-10-02

f) HoraEmbarque: 10:45

Atacadista: recebe paletes e caixas de vinho do distribuidor de produtos acabados e os despacha para as lojas de varejo. Os seguintes campos são preenchidos:

a) NomeAtacadista: Atacado dos Vinhos

b) EnderecoAtacadista: Rua das Garrafas, 101, Atacadópolis, SP

c) IDRemessaAtacadista: AV2023-001

d) DataRecebimentoAtacadista: 2023-10-03

e) HoraRecebimentoAtacadista: 08:15

f) QuantidadeRecebidaAtacadista: 500 caixas

Varejista: vende o vinho ao consumidor final e fornece informações sobre a venda. Os seguintes campos são preenchidos:

a) NomeVarejista: Vinhos & Mais

b) EnderecoVarejista: Praça da Taça, 7, Varejo City, SP

c) Lote: A123

d) IDRemessa: VR2023-001

e) DataEmbarque: 2023-10-04

f) HoraEmbarque: 11:20

3.4 Funcionamento da cadeia de suprimentos com a validação de cada etapa

Cada etapa da cadeia de suprimentos de vinho envolve a validação meticulosa das transações pelos validadores designados, incluindo os produtores de vinho, distribuidores a granel e enchedores/embaladores. Esses validadores são responsáveis por verificar a legitimidade e a conformidade de cada transação, garantindo que apenas transações válidas sejam registradas no *ledger* distribuído. O processo de validação é fundamental para manter a integridade dos dados e para assegurar que todas as transações sejam precisas e confiáveis.

Além disso, o consenso é alcançado por meio de algoritmos de consenso, como o algoritmo de consenso de ordem de entrega ou o algoritmo de *Practical Byzantine Fault Tolerance* (PBFT), garantindo que todos os nós da rede concordem com o estado atual do *ledger* distribuído. Isso ajuda a evitar a ocorrência de transações fraudulentas ou não autorizadas, protegendo a cadeia de suprimentos de vinho contra manipulações indesejadas e garantindo a imutabilidade dos registros (Hyperledger, 2022).

Dessa forma, a interação entre os componentes do Hyperledger Fabric e o processo de validação das transações pelos validadores contribuem para a operação eficiente e confiável da cadeia de suprimentos de vinho, garantindo a rastreabilidade e autenticidade de todos os produtos ao longo de todo o processo. Em seguida são descritos os detalhes de cada etapa, da comunicação das entidades com a rede:

Produtor de Vinho:

- Função Criar:
  - O produtor de vinho cria o bloco gênesis com os dados iniciais, incluindo: NomeViticultor, EnderecoViticultor, VariedadeUva, DataColheita, NomeProdutorVinho, EnderecoProdutorVinho, Lote, IDRemessa, DataEmbarque, HoraEmbarque;
  - Um ID único para o bloco genesis é gerado, e esse ID é usado como referência para toda a cadeia associada a esse produtor.
- Função Ler (opcional):
  - O produtor pode usar a função "ler"para verificar as informações que inseriu, com base no ID único.

Distribuidor:

- Função Transferir (do Produtor para Distribuidor):
  - O produtor utiliza a função "transferir"para registrar a venda de uvas para um distribuidor específico;
  - Os dados incluídos no bloco para essa transação podem conter informações como NomeProdutorDistribuidor, EnderecoProdutorDistribuidor, Lote, IDRemessa, DataEmbarque, HoraEmbarque.
- Função Ler (opcional):
  - Distribuidores podem usar a função "ler"para verificar as informações sobre as remessas que receberam, com base no Identificador (ID) único.

Atacadista:

- Função Transferir (do Distribuidor para Atacadista):
  - O distribuidor utiliza a função "transferir"para registrar o envio dos produtos para um atacadista específico;
  - Os dados incluídos no bloco para essa transação podem conter informações como NomeAtacadista, EnderecoAtacadista, IDRemessaAtacadista, DataRecebimentoAtacadista, HoraRecebimentoAtacadista, QuantidadeRecebidaAtacadista.
- Função Ler (opcional):
  - Atacadistas podem usar a função "ler"para verificar as informações sobre as remessas que receberam, com base no ID único.

Varejista:

- Função Transferir (do Atacadista para Varejista):
  - O atacadista utiliza a função "transferir"para registrar o envio dos produtos para um varejista específico;
  - Os dados incluídos no bloco para essa transação podem conter informações como NomeAtacadista, EnderecoAtacadista, Lote, IDRemessa, DataEmbarque, HoraEmbarque.
- Função Ler (opcional):
  - Varejistas podem usar a função "ler"para verificar as informações sobre as remessas que receberam, com base no ID único.

Responsabilidade do Produtor de Vinho na Visualização do Histórico:

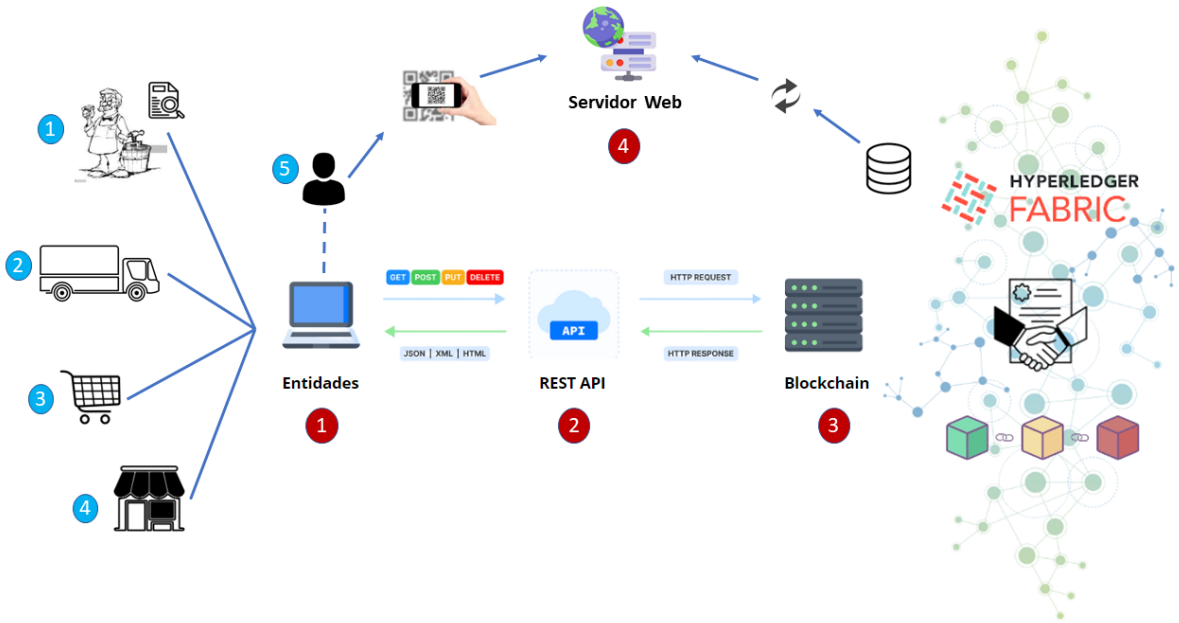
O produtor de vinho, como a entidade inicial na cadeia de suprimentos, é responsável por visualizar e compilar o histórico completo dos dados associados a cada lote de vinho produzido, podendo conter informações de mais de um viticultor. Essa visualização do histórico inclui dados desde a colheita da uva até as transações com distribuidores, atacadistas e varejistas.

Solicitação do Consumidor através de API e QR Codes:

Para permitir que os consumidores acessem esse histórico, o produtor disponibiliza um sistema baseado em API. Os consumidores fazer solicitações para visualizar o histórico de um lote específico escaneando um QR Code no rótulo do vinho. Esse QR Code contém informações como o ID único do bloco gênesis associado ao lote e o endereço do servidor web. Ao escanear o código, os consumidores são encaminhados à API, que recupera os dados correspondentes e os apresenta de maneira compreensível, mostrando desde a origem da uva até as informações de venda no varejo em uma página web.

Essa abordagem não só fornece transparência aos consumidores, permitindo que conheçam a procedência e a jornada do produto, mas também oferece uma maneira eficiente de compartilhar informações valiosas ao longo da cadeia de suprimentos do vinho. Na Figura 18, busca representar a comunicação de todas as entidades.

Figura 18 – Estrutura de comunicação entre entidades, plataforma API e *blockchain*.



Fonte: Autoria propria.

Identificadores em vermelho:

a) 1 - Entidades que interagem com a rede;

b) 2 - API, responsável pela comunicação das entidades com a Rede, utilizando requisições de inserção e consulta na rede;

c) 3 - Rede *Blockchain*, a qual possui o *chaincode* e o *ledger*;

d) 4 - Servidor Web, local onde o usuário poderá visualizar o histórico relacionado ao seu Vinho.

Identificadores em azul:

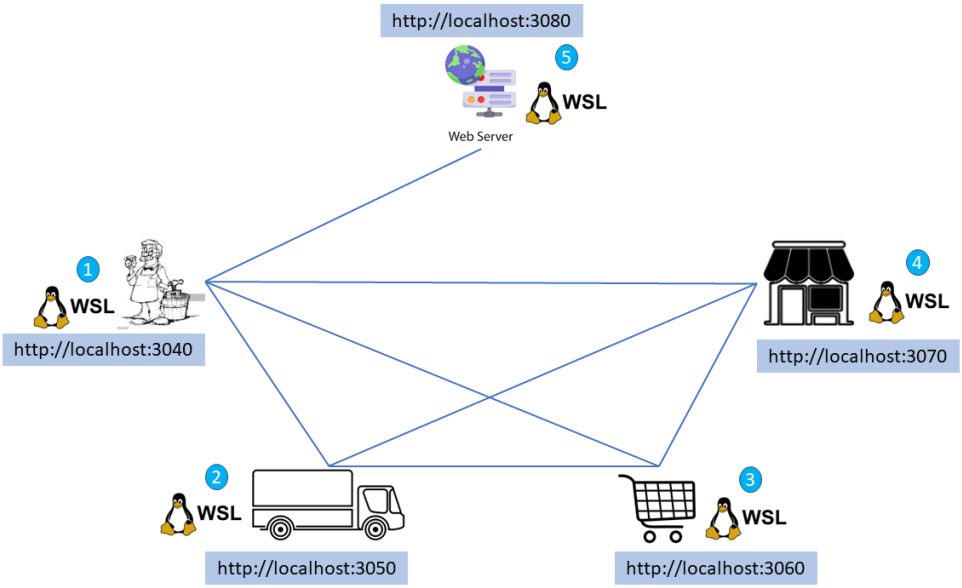
a) As entidades: 1 - Produtor, 2 - Distribuidor, 3 - Atacadista e 4 - Varejista, interagem com a rede utilizando a requisição POST na API, para inserir seus dados na Rede;

b) A entidade 5 - Visualização, representa o cliente que visualizará o histórico da rede utilizando o QR Code estampado na garrafa de vinho, com o ID do bloco gênesis (para identificar o histórico relacionado ao seu item, por meio de uma consulta a API) e a URL com o endereço virtual da página do servidor web, ao qual será redimensionado para o site que contem as informações.

4 RESULTADOS

Com a rede *blockchain* em execução, pode-se realizar as etapas de funcionamento como descrito na seção anterior. A rede está implementada em um servidor Linux Ubuntu 20LTS, Subsistema Windows para Linux (WSL), representado no Figura 19, nessa Figura tem a visão geral das entidades envolvidas, estas separadas, cada uma associada a uma porta diferente e rodando localmente em dockers associados, os quais permitem isolar cada entidade em seu próprio ambiente. Caso queira remanejar essas instâncias do docker em uma máquina física para cada entidade, essa infraestrutura permite, foi implementada localmente, por conta de facilidade de uso, teste e custo.

Figura 19 – Representação das entidades descentralizadas.



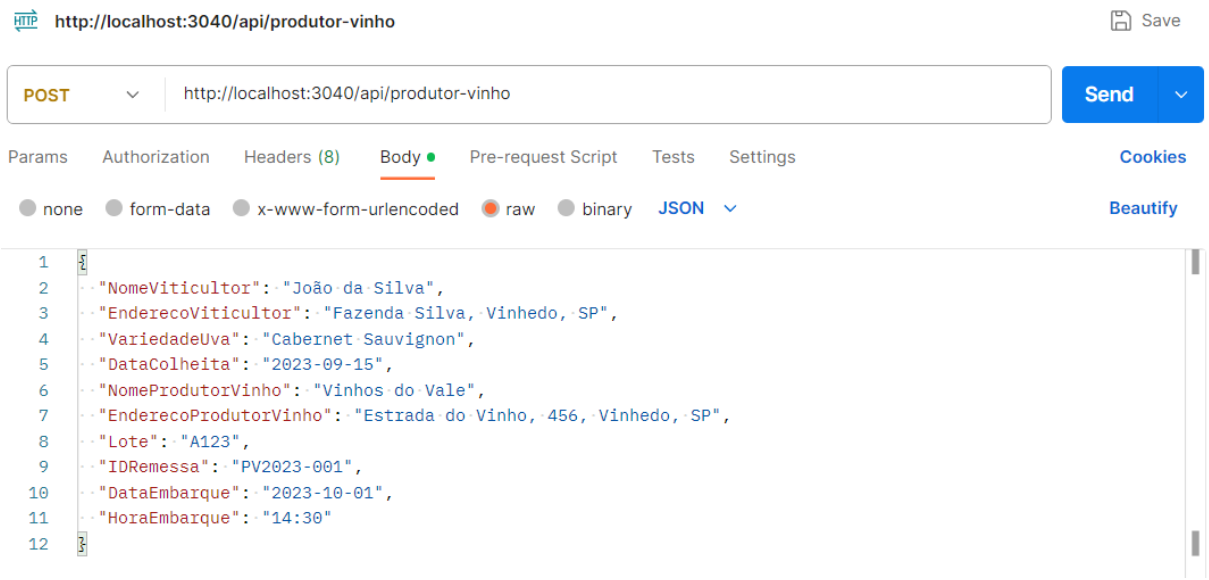
Fonte: Autoria propria.

O processo inicia-se com o (1) Produtor de vinho, que assume a responsabilidade de inserir os dados das uvas colhidas pelo Viticultor. Este Produtor de vinho, por sua vez, pode receber uvas de outros Viticultores, acrescentando os dados relativos a todos os envolvidos, além de incluir seus próprios dados no sistema. O produtor de vinho em posse de todos os dados realiza uma requisição API POST, como apresentado na Figura 20, esta requisição contém os campos com os dados preenchidos.

O Produtor de vinho desencadeia o processo de criação do bloco gêneses no *blockchain*, como apresentado na Figura 25, Apêndice A. A execução é iniciada com a invocação da função “Criar Ativo”, incumbida de consolidar os dados essenciais para a inclusão do ativo no *blockchain*.

Após a execução da função, o Produtor de vinho procede à assinatura digital dos dados gerados, garantindo a autenticidade e integridade do processo. Posteriormente, a validação

Figura 20 – Requisicão POST pelo Produtor de vinho.



Fonte: Autoria propria.

da assinatura é realizada novamente pelo Produtor de vinho, assegurando a legitimidade da criação do bloco gêneses.

O bloco é designado como o 12º bloco na rede *blockchain* e recebe o identificador único ’item-001’, este que será usado para recuperar toda a trajetória do ativo no *blockchain*. Nesse ponto, os dados fornecidos pelo Produtor de vinhos são adicionados ao bloco gêneses, enriquecendo-o com informações específicas sobre a produção de vinhos.

Ao término desse processo, o bloco gêneses é oficialmente criado e incorporado a *blockchain*, estabelecendo um registro validado e autenticado da criação do ativo pelo Produtor de vinho.

Com o primeiro bloco da rede *blockchain* criado, surge a possibilidade de consultar seu histórico. Essa consulta é efetuada por meio de uma requisição à API, utilizando o ID único do ativo e o endereço do servidor web. Essas informações são consolidadas de maneira prática em um QR Code, que é integrado à embalagem do produto, como apresenta a Figura 21. Nesse contexto, o Produtor de vinho, assumindo o papel de primeira entidade na cadeia de produção e responsável pela embalagem dos vinhos, também é encarregado de realizar as consultas ao *ledger*.

O Produtor de vinho, ao gerar e supervisionar a embalagem do produto, assume a responsabilidade adicional de rastrear a trajetória do vinho até o consumidor final. Dessa forma, o Produtor de vinho não apenas contribui para a criação do primeiro bloco, mas também desempenha um papel central no monitoramento e na verificação do histórico do produto ao longo de sua jornada na cadeia de suprimentos.

A Figura 26, Apêndice A, apresenta a consulta ao ativo, este possuindo as informações adicionadas pelo Produtor de vinho.

Figura 21 – QR Code para visualizar o histórico de transações.

Fonte: Autoria propria.

O Produtor de vinho vende seus vinhos para o (2) Distribuidor, o Distribuidor, por sua vez, realiza uma requisição POST para inserir seus dados na rede, como apresentado na Figura 22.

Figura 22 – Requisição POST pelo Distribuidor.

Fonte: Autoria propria.

A requisição POST realize a execução da função “Transferir Ativo”. Essa função tem como propósito a transferência de titularidade do ativo do Produtor para o Distribuidor. O fluxo operacional inicia com a emissão da requisição pelo Produtor, seguida pela validação por parte do Distribuidor.

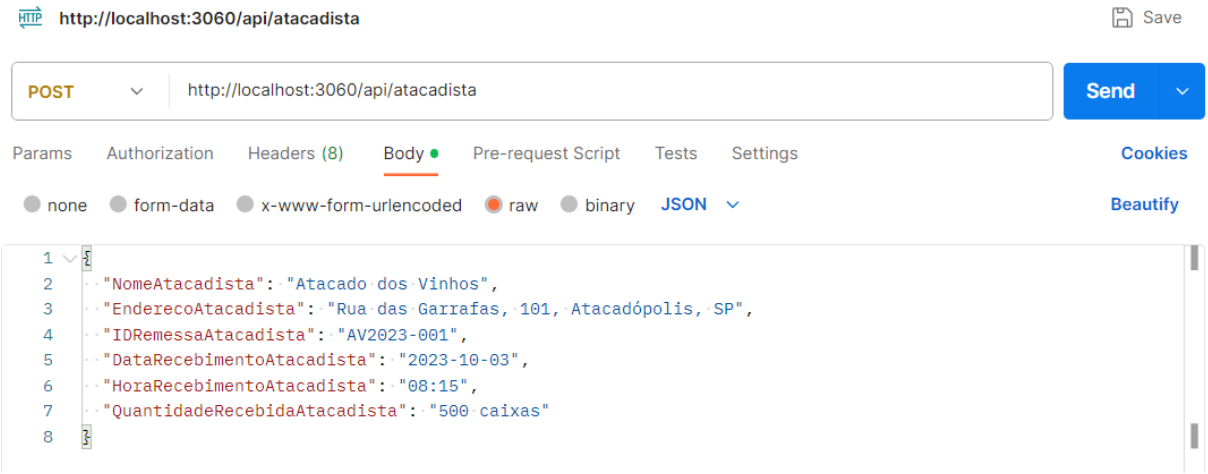
Após a validação, são inseridos dados pertinentes ao Distribuidor no bloco. Este processo engloba não apenas a inclusão dos dados, mas também a validação, sendo duplamente confirmada por meio da assinatura do Distribuidor em ambas as partes do bloco.

Este bloco resultante mantém o ID único ’item-001’ sendo designado como o 13º bloco na rede. Este ID único serve como uma referência exclusiva, enquanto a numeração sequencial (bloco 13) facilita a identificação na cadeia de blocos, conforme apresentado na Figura 27, Apêndice A.

A Figura 28, Apêndice A apresenta a consulta ao ativo, este possuindo as informações adicionadas pelo Produtor de vinho e Distribuidor, começando assim a formar o histórico do ativo.

O Distribuidor vende seus produtos para o (3) Atacadista, o Atacadista, por sua vez, realiza uma requisição POST para inserir seus dados na rede, como apresentado na Figura 23.

Figura 23 – Requisição POST pelo Atacadista.



Fonte: Autoria propria.

A requisição POST em foco conduz a execução da função “Transferir Ativo”, destinada à transferência de titularidade do Distribuidor para o Atacadista. O processo se inicia com a emissão da requisição pelo Distribuidor e, em seguida, é validado pelo Atacadista.

Posteriormente à validação, são introduzidos os dados relativos ao Atacadista no bloco. Esse procedimento abarca não apenas a inclusão dos dados, mas também a validação, confirmada mediante assinatura do Atacadista em ambas as partes do bloco.

O bloco resultante mantém o ID único ’item-001’ sendo designado como o 14º bloco na rede. Este ID exclusivo serve como referência, enquanto a numeração sequencial (bloco 14) facilita a identificação na cadeia de blocos, conforme apresentado na Figura 29, Apêndice A.

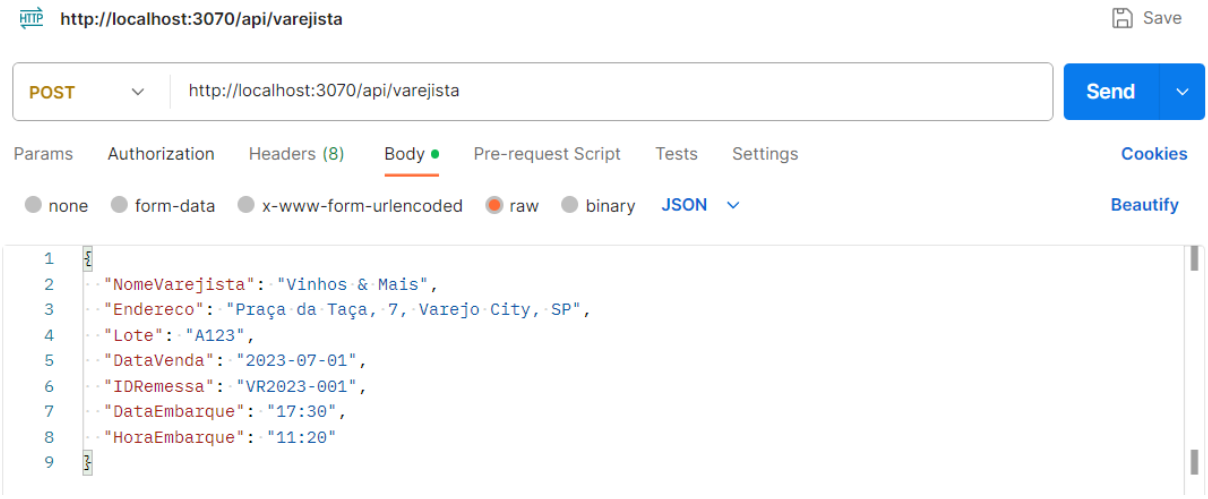
A Figura 30, Apêndice A apresenta a consulta ao ativo, este possuindo as informações adicionadas pelo Produtor de vinho, Distribuidor e agora Atacadista.

O Atacadista vende seus produtos para o (4) Varejista, este, por sua vez, realiza uma requisição POST para inserir seus dados na rede, como apresentado na Figura 24.

A requisição POST em foco conduz a execução da função “Transferir Ativo”, destinada à transferência de titularidade do Atacadista para o Varejista. O processo se inicia com a emissão da requisição pelo Atacadista e, em seguida, é validado pelo Varejista.

Posteriormente à validação, são introduzidos os dados relativos ao Varejista no bloco. Esse procedimento abarca não apenas a inclusão dos dados, mas também a validação, confirmada mediante assinatura do Varejista em ambas as partes do bloco.

Figura 24 – Requisição POST pelo Varejista.



Fonte: Autoria propria.

O bloco resultante mantém o ID único ’item-001’ sendo designado como o 15º bloco na rede. Este ID exclusivo serve como referência, enquanto a numeração sequencial (bloco 15) facilita a identificação na cadeia de blocos, conforme apresentado na Figura 31, Apêndice A.

A Figura 32, Apêndice A apresenta a consulta ao ativo, este possuindo as informações adicionadas pelo Produtor de vinho, Distribuidor, Atacadista e o Varejista. Dessa forma, o consumidor que tenha curiosidade em conhecer sobre a trajetória de seu vinho, poderá realizar somente verificando o QR Code no rótulo.

Essa abordagem visa promover a transparência dos dados e oferecer uma visão abrangente da jornada do ativo na cadeia de suprimentos, essa transparência não apenas atende às curiosidades dos consumidores, mas também beneficia todas as entidades envolvidas, uma vez que promove a confiança ao proporcionar uma compreensão clara e verificável da trajetória do ativo ao longo de sua vida útil.

5 CONCLUSÃO

O presente trabalho teve sua origem na exploração da tecnologia *Blockchain*, motivado pelo objetivo de aplicá-la a desafios reais. Em consonância com esses objetivos, identificou-se a cadeia de suprimentos de vinho como um campo propício, dada a existência de problemas como falsificação de rótulos e adulterações de embalagens.

A revisão do artigo de (Biswas, 2017) proporcionou *insights* valiosos, como: identificação das entidades envolvidas, arquitetura da cadeia de suprimentos, sequência operacional, e a implementação em um *framework Blockchain*. No entanto, a ausência de informações detalhadas sobre implementação e código-fonte limitou a possibilidade de replicação.

Com base nessas informações, desenvolveu-se a arquitetura, delineando as entidades relevantes. A fase de implementação no *framework* foi desafiadora, exigindo compreensão da arquitetura do sistema e a escolha de uma estrutura exemplar. Apesar das dificuldades, foi possível criar uma cadeia de suprimentos *blockchain* envolvendo quatro organizações, embora a expansão para uma quinta tenha se mostrado mais complexa, resultando na decisão de prosseguir com quatro organizações.

O trabalho cumpriu os objetivos estabelecidos inicialmente, definindo uma arquitetura para a utilização de um *framework Blockchain* e realizando sua implementação, utilizando o Hyperledger Fabric. Através da coleta de dados e testes de funcionamento, pôde-se validar a proposta desse trabalho, que apesar de não ser um sistema completo, abre caminho para futuras implementações e complementos nessa área de aplicação, como a cadeia de vinhos.

Além disso, a implementação da tecnologia *Blockchain* na cadeia de suprimentos de vinho ofereceu uma série de ganhos substanciais. A descentralização proporcionou uma transparência sem precedentes, permitindo uma visão holística e em tempo real de cada estágio do processo. A rastreabilidade, ancorada na natureza imutável dos registros, melhorou a autenticidade do produto final, atendendo às demandas dos consumidores por origens transparentes e éticas.

A segurança criptográfica robusta da *blockchain* mitigou riscos de fraudes e adulterações, enquanto a automação facilitada por contratos inteligentes simplificou operações, reduzindo erros humanos e acelerando fluxos de trabalho, resultando em eficiência operacional e redução de custos.

Visando trabalhos, podem ser construídas simulações do sistema em uma rede *Local Area Network* (LAN), com configurações de rede definidas para cada servidor representando uma entidade. Além disso, a criação de uma página web destinada tanto às entidades quanto aos consumidores visa proporcionar uma interação mais amigável. A adição de novas entidades à rede *blockchain*, apesar de enfrentar desafios ao expandir para mais de quatro, permanece como um objetivo a ser abordado.

REFERÊNCIAS

ABEYRATNE, S. A.; MONFARED, R. P. Blockchain ready manufacturing supply chain using distributed ledger. **International journal of research in engineering and technology**, v. 5, n. 9, p. 1–10, 2016.

ADAMASHVILI, N. *et al.* Blockchain-based wine supply chain for the industry advancement. **Sustainability**, MDPI, v. 13, n. 23, p. 13070, 2021.

ATLAM. Technical aspects of blockchain and iot. *In*: **Advances in computers**. [*S.l.*]: Elsevier, 2019. v. 115, p. 1–39.

BANERJEE, A. Blockchain technology: supply chain insights from erp. *In*: **Advances in computers**. [*S.l.*]: Elsevier, 2018. v. 111, p. 69–98.

BERMAN, B. Strategies to detect and reduce counterfeiting activity. **Business Horizons**, Elsevier, v. 51, n. 3, p. 191–199, 2008.

BHUTTA, M. N. M.; AHMAD, M. Secure identification, traceability and real-time tracking of agricultural food supply during transportation using internet of things. **IEEE Access**, IEEE, v. 9, p. 65660–65675, 2021.

BISWAS. Blockchain based wine supply chain traceability system. p. 56–62, 2017.

BOISSIEU, E. de *et al.* The use of blockchain in the luxury industry: supply chains and the traceability of goods. **Journal of Enterprise Information Management**, Emerald Publishing Limited, 2021.

BUTERIN, V. *et al.* A next-generation smart contract and decentralized application platform. **white paper**, v. 3, n. 37, p. 2–1, 2014.

CHOHAN, U. W. The double spending problem and cryptocurrencies. **Available at SSRN 3090174**, 2021.

COULOURIS, G. *et al.* **Sistemas Distribuídos-: Conceitos e Projeto**. [*S.l.*]: Bookman Editora, 2013.

CROSBY, M. *et al.* Blockchain technology: Beyond bitcoin. **Applied Innovation**, v. 2, n. 6-10, p. 71, 2016.

DANESE. Designing blockchain systems to prevent counterfeiting in wine supply chains: a multiple-case study. **International Journal of Operations & Production Management**, Emerald Publishing Limited, 2021.

EMBRAPA. **Brasil terá o primeiro açúcar mascavo rastreado com tecnologia blockchain**. 2022. Disponível em: https://www.embrapa.br/busca-de-noticias/-/noticia/71508414/brasil-tera-o-primeiro-acucar-mascavo-rastreado-com-tecnologia-blockchain.

ETHEREUM. **The Merge**. 2023. Disponível em: https://ethereum.org/en/roadmap/merge/.

FERRETTI. On the ethereum blockchain structure: A complex networks theory perspective. **Concurrency and Computation: Practice and Experience**, Wiley Online Library, v. 32, n. 12, p. 5493, 2020.

GARG, N.; YADAV, P. Comparison of asymmetric algorithms in cryptography. **J. Comput. Sci. Mob. Comput.(IJCSMC)**, v. 3, p. 1190–1196, 2014.

GERVAIS, A. *et al.* On the security and performance of proof of work blockchains. *In*: **Proceedings of the 2016 ACM SIGSAC conference on computer and communications security**. [*S.l.*: *s.n.*], 2016. p. 3–16.

GREENSPAN, G. *et al.* Multichain private blockchain-white paper. **URI: http://www. multichain. com/download/MultiChain-White-Paper. pdf**, v. 85, 2015.

GUIDELINE, G. A. Wine supply chain traceability. 2008.

HYPERLEDGER. **What is Hyperledger Fabric**. 2022. Disponível em: https://hyperledger-fabric.readthedocs.io/en/latest/blockchain.html#what-is-hyperledger-fabric.

IFTEKHAR, A. *et al.* Application of blockchain and internet of things to ensure tamper-proof data availability for food safety. **Journal of Food Quality**, Hindawi, v. 2020, 2020.

KOLVART. Smart contracts. *In*: **The Future of Law and etechnologies**. [*S.l.*]: Springer, 2016. p. 133–147.

LIMA, L. G. **A Utilização de Blockchain para controle da cadeia de distribuição de combustíveis derivados: Proposta de modelo de negócio**. 2021. Tese (Doutorado) — PUC-Rio, 2021.

MALIK, A. *et al.* Supply chain management- an overview. **International Journal of Logistics and Supply chain management**, v. 2, p. 97–101, 01 2010.

MANN, S. *et al.* Blockchain technology for supply chain traceability, transparency and data provenance. *In*: **Proceedings of the 2018 international conference on blockchain technology and application**. [*S.l.*: *s.n.*], 2018. p. 22–26.

MENEZES, L. D. **Blockchain e cartórios: uma solução viável?** 2020. Tese (Doutorado) — Universidade de São Paulo, 2020.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. **Decentralized Business Review**, p. 21260, 2008.

PENARD, W.; WERKHOVEN, T. van. On the secure hash algorithm family. **Cryptography in context**, Wiley Newyork, p. 1–18, 2008.

PPLWARE. **Criptografia simétrica e assimétrica. Sabe a diferença?** 2010. Disponível em: https://pplware.sapo.pt/tutoriais/networking/criptografia-simetrica-e-assimetrica-sabe-a-diferenca/.

SALEH, F. Blockchain without waste: Proof-of-stake. **The Review of financial studies**, Oxford University Press, v. 34, n. 3, p. 1156–1190, 2021.

SEGENDORF, B. What is bitcoin. **Sveri gesRiksbankEconomicReview**, v. 2014, p. 2–71, 2014.

STALLINGS, W. **Criptografia e segurança de redes. Princípios e práticas, ch. 6**. [*S.l.*]: Pearson Prentice Hall, 2006.

SWAN, M. **Blockchain: Blueprint for a new economy**. [*S.l.*]: "O'Reilly Media, Inc.", 2015.

SZABO, N. The idea of smart contracts. **Nick Szabo's papers and concise tutorials**, v. 6, n. 1, p. 199, 1997.

TAPSCOTT, D.; TAPSCOTT, A. **Blockchain revolution**. [*S.l.*]: Senai-SP Editora, 2018.

TSE, D. *et al.* Blockchain application in food supply information security. *In*: IEEE. **2017 IEEE international conference on industrial engineering and engineering management (IEEM)**. [*S.l.*], 2017. p. 1357–1361.

VUJIČIĆ. Blockchain technology, bitcoin, and ethereum: A brief overview. *In*: IEEE. **2018 17th international symposium infoteh-jahorina (infoteh)**. [*S.l.*], 2018. p. 1–6.

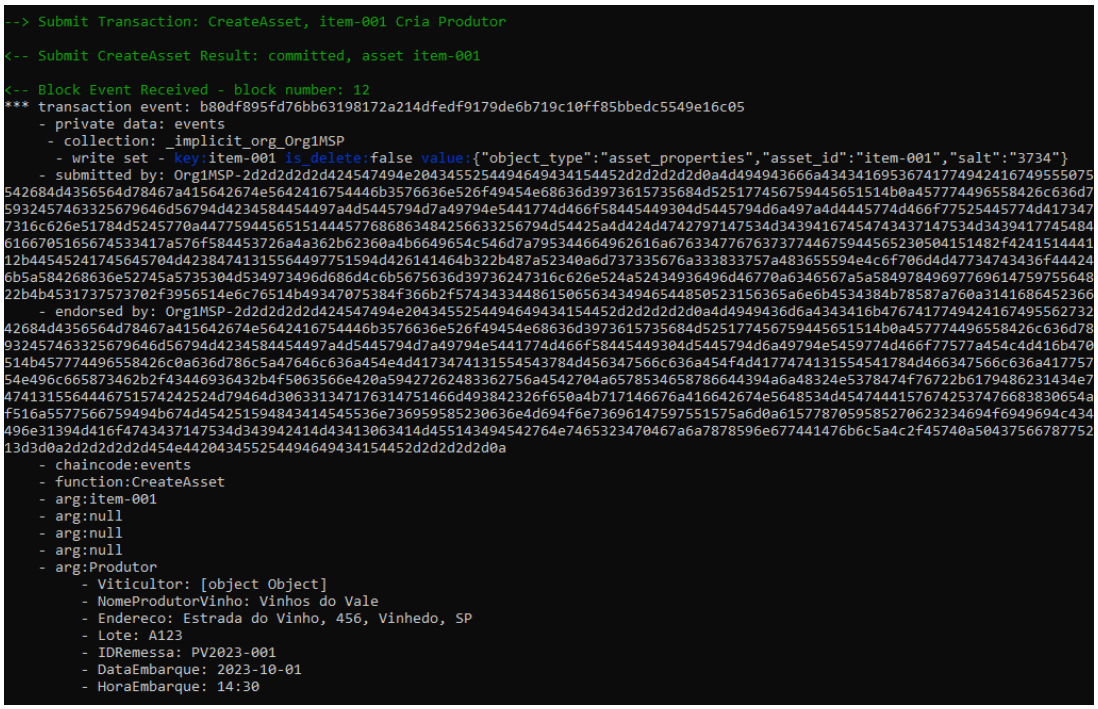
WACKEROW, P. **Proof-of-Stake (POS)**. 2022. Disponível em: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

YANO, M. *et al.* **Blockchain and Crypto Currency: Building a High Quality Marketplace for Crypt Data**. [*S.l.*]: Springer Nature, 2020.

APÊNDICE A – Detalhes de Implementação

A Figura 25, apresenta a execução da função “Criar Ativo”, pelo Produtor de vinho, procede à assinatura digital dos dados gerados, com a validação da assinatura é realizada novamente pelo Produtor de vinho. O bloco é designado como o 12º bloco na rede *blockchain* e recebe o identificador único ’item-001’, este que será usado para recuperar toda a trajetória do ativo no *blockchain*. Ao término desse processo, o bloco gêneses é oficialmente criado e incorporado a *blockchain*, estabelecendo um registro validado e autenticado da criação do ativo pelo Produtor de vinho.

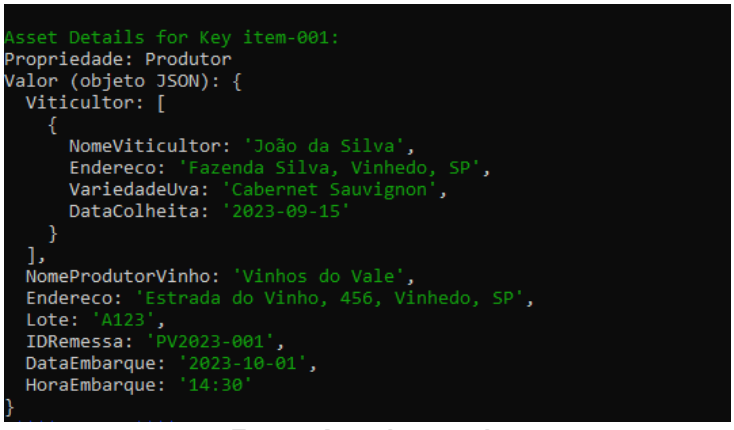
Figura 25 – Inserção do bloco gênese pelo Produtor de vinho a rede.



Fonte: Autoria propria.

A Figura 26, apresenta a consulta ao ativo, este possuindo as informações adicionadas pelo Produtor de vinho.

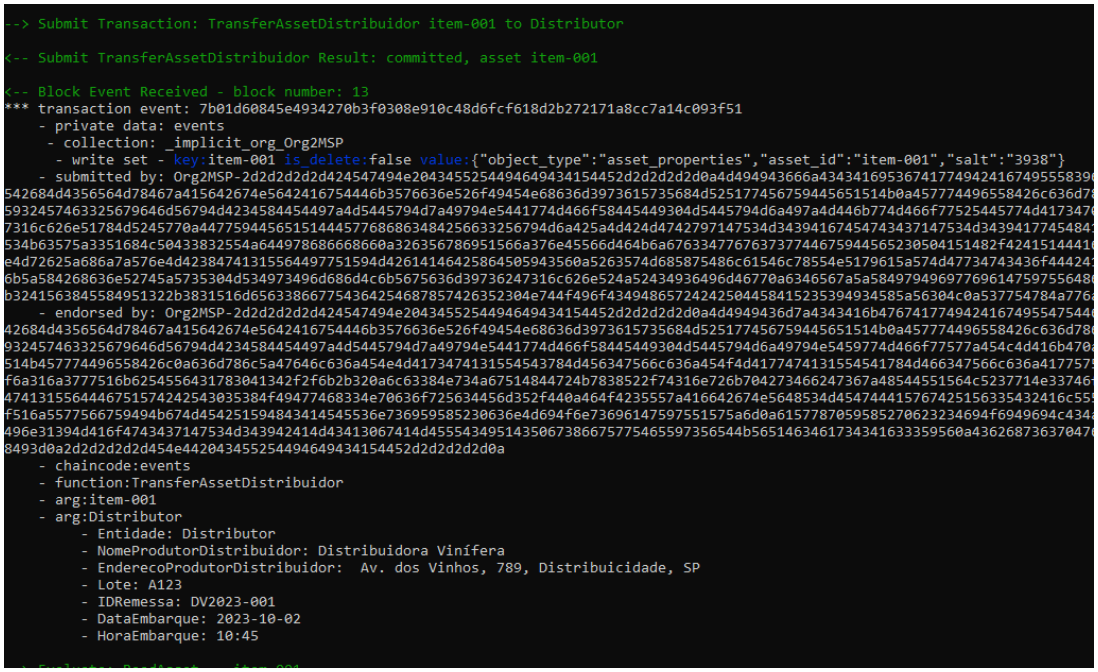
Figura 26 – Leitura do histórico da rede — Produtor de vinho.



Fonte: Autoria propria.

A Figura 27, apresenta a execução da função “Transferir Ativo”. Essa função tem como propósito a transferência de titularidade do ativo do Produtor para o Distribuidor. O fluxo operacional inicia com a emissão da requisição pelo Produtor, seguida pela validação por parte do Distribuidor. Após a validação, são inseridos dados pertinentes ao Distribuidor no bloco. Este bloco resultante mantém o ID único ’item-001’ sendo designado como o 13º bloco na rede. Este ID único serve como uma referência exclusiva, enquanto a numeração sequencial (bloco 13) facilita a identificação na cadeia de blocos.

Figura 27 – Transferência de propriedade de Produtor de vinho para Distribuidor e acréscimo de informações.

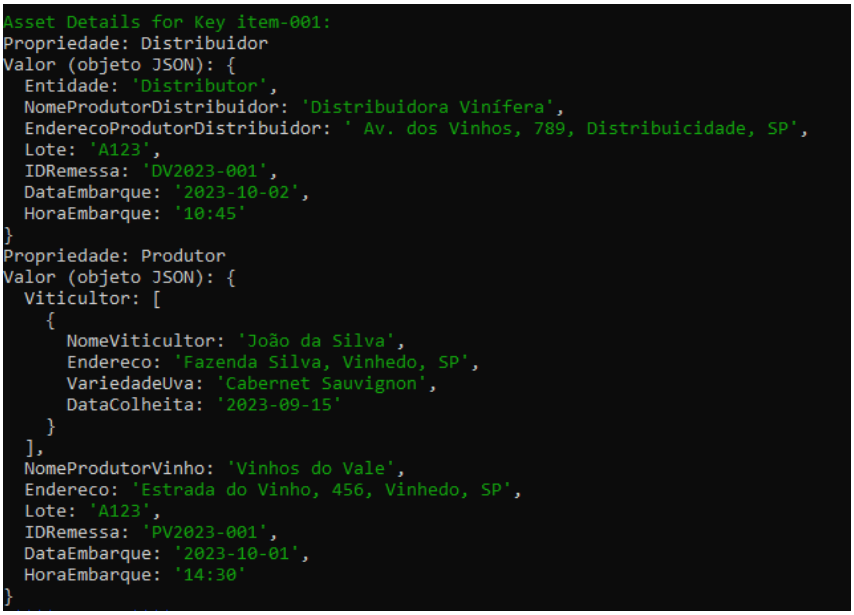


Fonte: Autoria propria.

A Figura 28, apresenta a consulta ao ativo, este possuindo as informações adicionadas pelo Distribuidor.

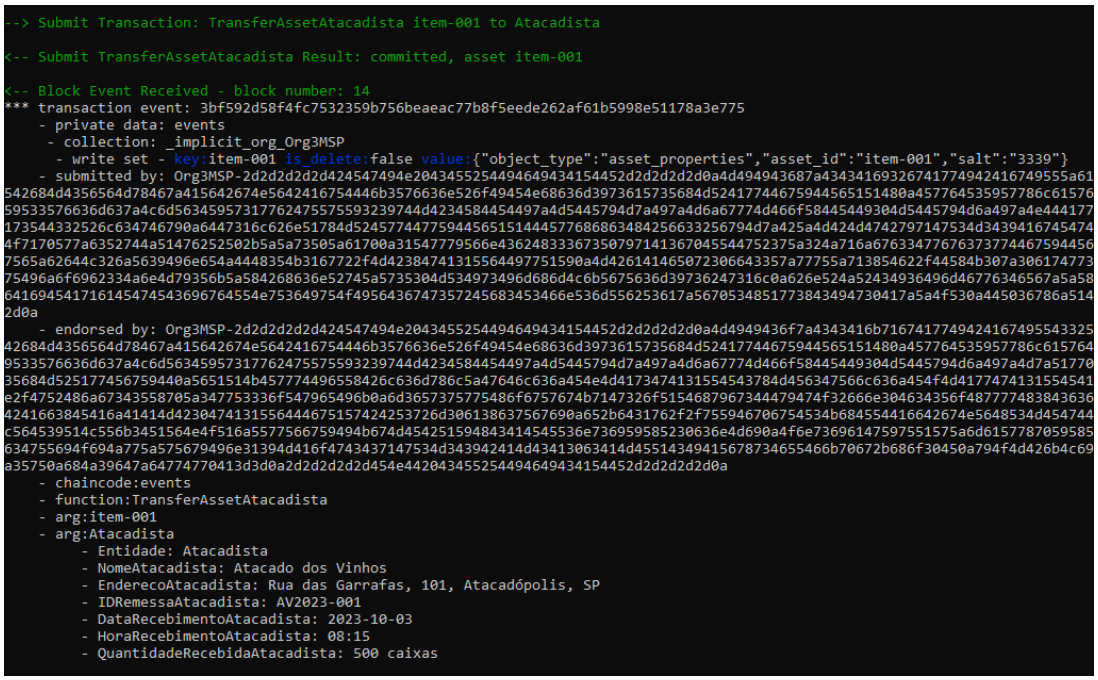
A Figura 29, apresenta a execução da função “Transferir Ativo”. Essa função tem como propósito a transferência de titularidade do ativo do Distribuidor para o Atacadista. O fluxo operacional inicia com a emissão da requisição pelo Distribuidor, seguida pela validação por parte do Atacadista. Após a validação, são inseridos dados pertinentes ao Atacadista no bloco. Este bloco resultante mantém o ID único ’item-001’ sendo designado como o 14º bloco na rede. Este ID único serve como uma referência exclusiva, enquanto a numeração sequencial (bloco 14) facilita a identificação na cadeia de blocos.

Figura 28 – Leitura do histórico da rede — Distribuidor.



Fonte: Autoria propria.

Figura 29 – Transferência de propriedade de Distribuidor para Atacadista.

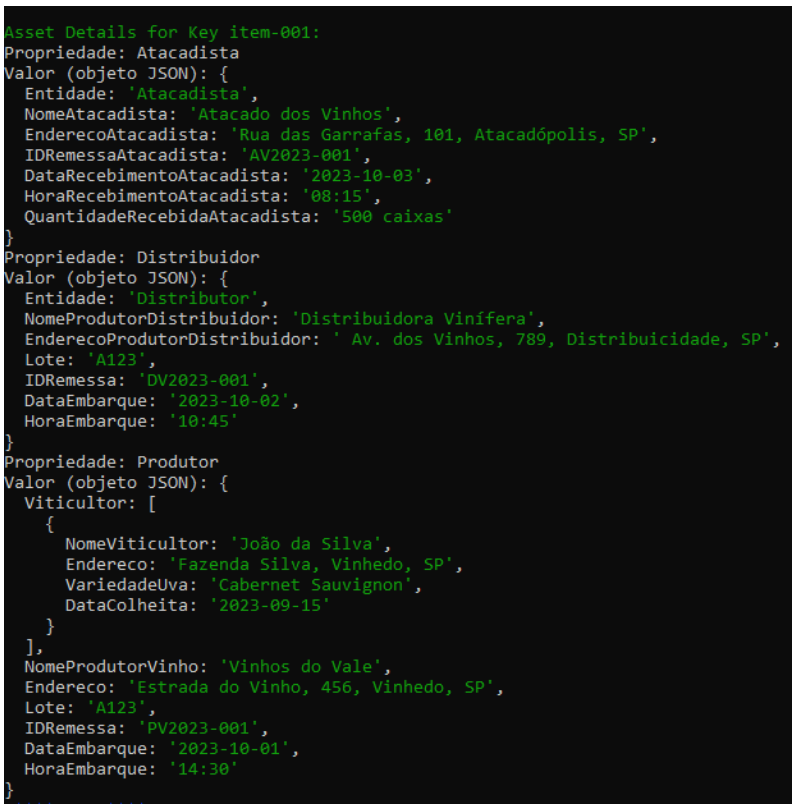


Fonte: Autoria propria.

A Figura 30, apresenta a consulta ao ativo, este possuindo as informações adicionadas pelo Atacadista.

A Figura 31, apresenta a execução da função “Transferir Ativo”. Essa função tem como propósito a transferência de titularidade do ativo do Atacadista para o Varejista. O fluxo operacional inicia com a emissão da requisição pelo Distribuidor, seguida pela validação por parte do Varejista. Após a validação, são inseridos dados pertinentes ao Varejista no bloco. Este bloco resultante mantém o ID único ’item-001’ sendo designado como o 15º bloco na rede. Este ID

Figura 30 – Leitura do histórico da rede - Atacadista.

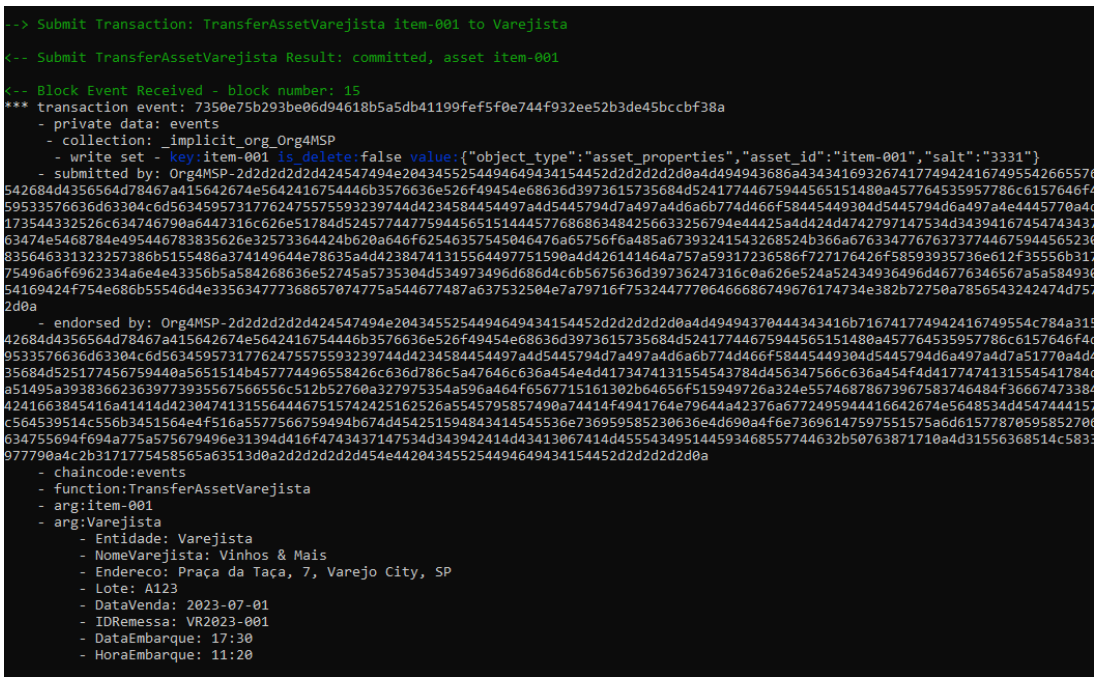


Fonte: Autoria propria.

único serve como uma referência exclusiva, enquanto a numeração sequencial (bloco 15) facilita a identificação na cadeia de blocos.

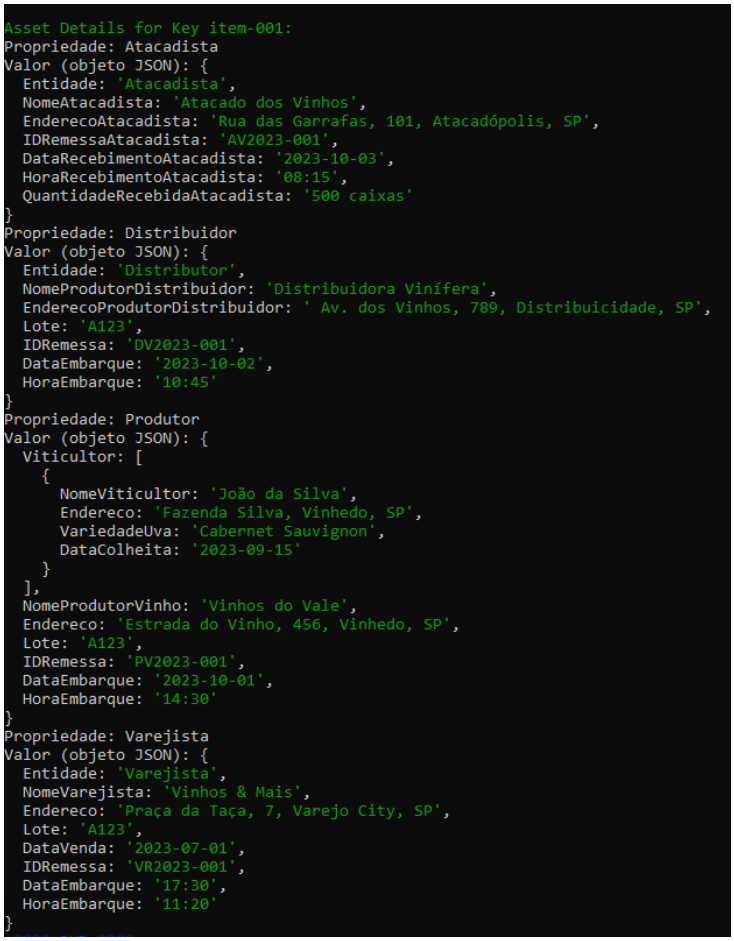
A Figura 32, apresenta a consulta ao ativo, este possuindo as informações adicionadas pelo Varejista.

Figura 31 – Transferência de propriedade de Atacadista para Varejista.



Fonte: Autoria propria.

Figura 32 – Leitura do histórico da rede - Varejista.



Fonte: Autoria propria.

APÊNDICE B – Principais funções utilizadas

Dentre as funções essenciais implementadas no chaincode da rede de cadeia de suprimentos, destacam-se as operações de criar, transferir e ler. Cada uma desempenha um papel crucial na construção e manutenção da integridade da cadeia de suprimentos. A seguir, detalhamos cada uma dessas funções:

B.0.1 `CreateAsset`

A função `CreateAsset` é a etapa inicial na cadeia de suprimentos e na rede. Quando um produtor inicia o processo de criação, ele fornece informações iniciais, define o proprietário do ativo e a atribui um ID único. Ao longo da jornada do ativo na rede, outros participantes preenchem os dados adicionais. O código-fonte pode ser observado na Listagem 1, que representa a implementação desta função:

Listagem 1 – CreateAsset.

```
async CreateAsset(ctx, id, distribuidor, atacadista, varejista, owner,
produtor) {

    const asset = {
        ID: id,
        Owner: owner,
        Produtor: produtor,
        Distribuidor: distribuidor,
        Atacadista: atacadista,
        Varejista: varejista
    };
    await savePrivateData(ctx, id);
    const assetBuffer = Buffer.from(JSON.stringify(asset));

    ctx.stub.setEvent('CreateAsset', assetBuffer);
    return ctx.stub.putState(id, assetBuffer);
```

Fonte: Autoria própria (2023).

B.0.2 `TransferAssetDistribuidor`

A função `TransferAssetDistribuidor` representa a transferência de propriedade de um ativo do produtor para o distribuidor na cadeia de suprimentos, definindo o novo proprietário e os detalhes do distribuidor. O código-fonte pode ser observado na Listagem 2, que representa a implementação desta função:

Listagem 2 – TransferAssetDistribuidor.

```
async TransferAssetDistribuidor(ctx, id, newOwner, distribuidor) {
    const asset = await readState(ctx, id);
    asset.Owner = newOwner;
    asset.Distribuidor = distribuidor;
    const assetBuffer = Buffer.from(JSON.stringify(asset));
    await savePrivateData(ctx, id);

    ctx.stub.setEvent('TransferAssetDistribuidor', assetBuffer);
    return ctx.stub.putState(id, assetBuffer);
}
```

Fonte: Autoria própria (2023).

B.0.3 `TransferAssetAtacadista`

A função `TransferAssetAtacadista` representa a transferência de propriedade de um ativo do distribuidor para o atacadista na cadeia de suprimentos, definindo o novo proprietário e os detalhes do atacadista. O código-fonte pode ser observado na Listagem 3, que representa a implementação desta função:

Listagem 3 – TransferAssetAtacadista.

```
async TransferAssetAtacadista(ctx, id, newOwner, atacadista) {
    const asset = await readState(ctx, id);
    asset.Owner = newOwner;
    asset.Atacadista = atacadista;
    const assetBuffer = Buffer.from(JSON.stringify(asset));
    await savePrivateData(ctx, id);

    ctx.stub.setEvent('TransferAssetAtacadista', assetBuffer);
    return ctx.stub.putState(id, assetBuffer);
}
```

Fonte: Autoria própria (2023).

B.0.4 `TransferAssetVarejista`

A função `TransferAssetVarejista` representa a transferência de propriedade de um ativo do atacadista para o varejista na cadeia de suprimentos, definindo o novo proprietário e os detalhes do varejista. O código-fonte pode ser observado na Listagem 4, que representa a implementação desta função:

Listagem 4 – TransferAssetVarejista.

```
async TransferAssetVarejista(ctx, id, newOwner, varejista) {
    const asset = await readState(ctx, id);
    asset.Owner = newOwner;
    asset.Varejista = varejista;
    const assetBuffer = Buffer.from(JSON.stringify(asset));
    await savePrivateData(ctx, id);

    ctx.stub.setEvent('TransferAssetVarejista', assetBuffer);
    return ctx.stub.putState(id, assetBuffer);
}
```

Fonte: Autoria própria (2023).

B.0.5 `queryAssetByKey`

Para ler o histórico de dados do ativo, utiliza-se a função `queryAssetByKey`. Esta função deve ser realizada por uma das entidades da cadeia de suprimentos, a qual, possuiu o contrato inteligente relacionado à cadeia e o ID do ativo. O código-fonte pode ser observado na Listagem 5, que representa a implementação desta função:

Listagem 5 – queryAssetByKey.

```
async queryAssetByKey(ctx, assetKey) {
    const assetBuffer = await ctx.stub.getState(assetKey);

    if (!assetBuffer || assetBuffer.length === 0) {
        return null;
    }
    const assetString = assetBuffer.toString('utf8');
    const asset = JSON.parse(assetString);

    if (asset.dados_adicionais) { return asset; }
    else{ return asset; }
}
```

Fonte: Autoria própria (2023).